ENISA Threat Landscape Report 2017

15 Top Cyber-Threats and Trends

FINAL VERSION

1.0

ETL 2017

JANUARY 2018

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries on this paper, please use enisa.threat.info@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank the members of the ENISA ETL Stakeholder group: Pierluigi Paganini, Chief Security Information Officer, IT, Paul Samwel, Banking, NL, Jason Finlayson, Consulting, IR, Stavros Lingris, CERT, EU, Jart Armin, Worldwide coalitions/Initiatives, International, Thomas Häberlen, Member State, DE, Neil Thacker, Consulting, UK, Shin Adachi, Security Analyst, US, R. Jane Ginn, Consulting, US, Andreas Sfakianakis, Industry, NL. The group has provided valuable input, has supported the ENISA threat analysis and has reviewed ENISA material. Their support is highly appreciated and has definitely contributed to the quality of the material presented in this report. Moreover, we would like to thank CYjAX for granting access pro bono to its cyber risk intelligence portal providing information on cyber threats and cyber-crime.

ISBN 978-92-9204-250-9, ISSN 2363-3050, DOI 10.2824/967192

Table of Contents

Executive Summary

2017 was the year in which incidents in the cyberthreat landscape have led to the definitive recognition of some omnipresent facts. We have gained unwavering evidence regarding monetization methods, attacks to democracies, cyber-war, transformation of malicious infrastructures and the dynamics within threat agent groups.

But 2017 has also brought successful operations against cyber-criminals. Law enforcement, governments and vendors have managed to shut down illegal dark markets, de-anonymize the Darknet and arrest cyber-criminals. Moreover, state-sponsored campaigns have been revealed and details of technologies deployed by nation states have been leaked. Mostly remarkable though is the manifestation of the cyberthreat landscape within framework programmes that are about to be established in the financial sector: cyberthreats make up the basis for the development and implementation of red and blue teaming activities in financial sector, both within Member States and across Europe.

But the cybersecurity community is still far from striking the balance between defenders and attackers. Although 2017 has reached records in security investments, it has also brought new records in cyber-attacks of all kinds, data breaches, and information loss. From this perspective, one may argue that there is a market failure in cyber-security; that is, the increased defence levels and expenses cannot successfully reduce levels of cyberthreat exposure.

Whether this is due to a segmented cyber-security market, lack of awareness or capabilities and skills, are topics of vivid discussions in the corresponding communities. The fact is however, that in 2017 we have seen a significantly increased amount of information on cyber-security incidents, cyberthreats and related matters to attract the attention of all kinds of media. This trend is indicative for the high level of interest assigned by media to cybersecurity issues.

In summary, the main trends in the 2017's cyberthreat landscape are:

- Complexity of attacks and sophistication of malicious actions in cyberspace continue to increase.
- Threat agent of all types have advanced in obfuscation, that is, hiding their trails.
- Malicious infrastructures continue their transformation towards multipurpose configurable functions including anonymization, encryption and detection evasion.
- Monetization of cybercrime is becoming the main motive of threat agents, in particular cyber-criminals. They take advantage of anonymity offered by the use digital currencies.
- State-sponsored actors are one of the most omnipresent malicious agents in cyberspace. They are a top concern of commercial and governmental defenders.
- Cyber-war is entering dynamically into the cyberspace creating increased concerns to critical infrastructure operators, especially in areas that suffer some sort of cyber crises.
- Skills and capabilities are the main concerns for organisations. The need for related training programmes and educational curricula remains almost unanswered.

All these trends are assessed and analysed by means of the content of the ENISA Threat Landscape 2017 (ETL 2017). Identified open issues leverage on these trends and propose actions to be taken in the aras of policy, business and research/education. They serve as recommendations and will be taken into account in the future activities of ENISA and its stakeholders. An overview of identified points is as follows:

Policy conclusions:

- Policy makers need to take into account elements of the cyberthreat landscape in policy making actions. First legislative actions towards this direction have been assessed in 2017; they are indicative for the importance cyberthreat assessment can play in understanding current state-of-play in cyberspace; the cyberthreat landscape is a very important parameter in the definition of defence strategies.
- Policy makers need to launch discussions about the whereabouts of lawful interventions in cyber-space. The main concern is to avoid influencing the cyberthreat landscape in a negative manner. The measures taken should not enlarge threat exposure, thus affecting the threat landscape.
- Skills, capabilities and knowledge on cyberthreats need to be better developed. Policy makers need to take measures to ensure that education and research obtains the necessary means to achieve this goal.

Business conclusions:

- After some years of development and deployment, vendors need to re-assess the usefulness of cyberthreat intelligence and eventually develop more efficient means for its adoption via the wider stakeholder community.
- Automation of cyberthreat intelligence needs to further advance to include strategic and tactical intelligence. This information should be interfaced with existing security management and protection practices. The aim should be to group available market offerings, instead of fragmenting it.
- Threat information maturity models need to be established. They should include indicators showing the effects of threat information usage in the final organisation-wide risk mitigation strategy.

Research/educational conclusions:

- Malware tactics, attack vectors and malicious infrastructure are in a continual transformation. Research is necessary to understand these trends as early as possible and adapt defences. The use of innovative approaches, artificial intelligence and machine learning techniques may support researchers towards this task.
- Research has to support policy in developing lawful intervention technologies and methods that do not negatively affect the cyberthreat landscape.
- Research is necessary in order to showcase use of cyberthreat intelligence in various disciplines and sectors. Moreover, research is required in order to elaborate on the structure and role of various forms of threat intelligence within security management practices.
- Education needs to combine available skillsets and develop curricula for cyberthreat intelligence. This requires innovative actions that will lead to the creation of knowledge that spans more than one discipline. Policy will need to create the environment for these innovations.

In the last chapter of this document (see chapter 6.1), a number of important issues leading to the above conclusions are mentioned; this chapter provides more elaborated conclusions. It is proposed to consider these issues and identify their relevance by reflecting them to the own situation and elaborate on these issues accordingly.

The figure below summarizes the top 15 cyber-threats and threat trends in comparison to the threat landscape of 2016.

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware		→
2. Web based attacks	↑	2. Web based attacks		→
3. Web application attacks	↑	3. Web application attacks		→
4. Denial of service	↑	4. Phishing		↑
5. Botnets	↑	5. Spam		↑
6. Phishing	➲	6. Denial of service		↓
7. Spam	↓	7. Ransomware		↑
8. Ransomware	➲	8. Botnets		↓
9. Insider threat	➲	9. Insider threat		→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss		→
11. Exploit kits	↑	11. Data breaches		↑
12. Data breaches	↑	12. Identity theft		↑
13. Identity theft	↓	13. Information leakage		↑
14. Information leakage	↑	14. Exploit kits		↓
15. Cyber espionage	↓	15. Cyber espionage		→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Figure 1: Overview and comparison of the current threat landscape 2017 with the one of 2016.

1. Introduction

This is the 2017's version of the ENISA Threat Landscape (ETL 2017) yearly report. It is the sixth in a series of ENISA reports analysing the state-of-the-art in cyberthreats based on open source material[1]. This report is the result of a one-year long collection, analysis and assessment activity of cyber-threat related information found in the public domain. The time span of the ETL is ca. December 2016 to December 2017 and is referred to as the "reporting period" throughout the report.

As part of the annual improvement process, some adaptations have been applied to the ETL 2017. These have their source in various reasons such as: discussions with internal/external experts, increase of efficiency in generating the report, advancements in collection and dissemination of information and establishment of better coherence among various ENISA material on cyber-threats. In overview, the changes performed to this year's ETL are:

- *Adaptation of the description of cyber-threats*: In ETL 2017 we have slightly changed the structure of the template used for the presentation of the assessed cyberthreats. The new template aims at better reflecting the whereabouts of the cyber-threat. The structure is explained in chapter 3.
- *Development of an ETL web application*: In 2107 ENISA has developed a web application to visualise the ETL contents in an easily understandable and easily navigable form for a wide range of stakeholders, including non-experts. A description of the ETL web application can be found in chapter 2.3.1.
- *Establishment of an event on CTI as a community forum*: in 2017, following an idea and request coming from stakeholders, ENISA has organized the first event in the area of Cyber Threat Intelligence (CTI) addressing the European community (experts, vendors, users). A description of the event can be found in chapter 2.3.2.
- *Development of a first version of CTI maturity model*: In 2017, ENISA has performed initial work towards the development of a maturity model for CTI[2]. This work has emerged within a work aiming at the identification of gaps in current Threat Information Sharing Tools. (TIS tools). Given the interest of the community and the availability of resources, this work will be continued in 2018.

As regards the channels used for information collection, ENISA has used information provided by the MISP platform[3], by CERT-EU[4] and by also using threat intelligence of the cyber-security portal CYjAX[5], granted as access pro bono to ENISA. Confidential information found in these platforms has just been taken into account in our analysis without any disclosure or reference to this material.

Last but not least, it is worth mentioning that in 2017 ENISA has initiated a tighter liaison with the EU agencies touching upon cyber-security: this involves the European Defence Agency (EDA), CERT-EU and

[1] It is worth mentioning, that in this chapter some parts of the ETL 2016 text have been reused, in particular regarding the sections policy context and target group. These two topics are considered mostly identical to the previous landscapes. Some changes have been added to policy context to reflect recent developments in EU–regulations.
[2] The report is going to be published by ENISA end of January 2018.
[3] http://www.misp-project.org/, accessed November 2017.
[4] https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html, accessed November 2017.
[5] https://www.cyjax.com/, accessed November 2017.

EC3. This has been implemented by means of discussions for a more enhanced cooperation among all four organisations[6].

The links to these institutions existed already at a working level. ENISA has a tight cooperation with CERT-EU in the area of threat information. This is implemented by means of mutual reviews of cyber-threat assessments, use of CERT-EU services and by of intensive personal communication. This allows maintaining a high level of coherence in mutual views on cyber-threat assessment. Moreover, ENISA capitalizes on valuable comprehensive threat information that CERT-EU delivers to its partners.

While with EC3 and EDA working relationships do exist, in this year the cooperation in the area of CTI has been advanced by means the ENISA CTI event that was commonly supported by all four institutions[14]. It is planned to continue the cooperation in the area of CTI both by means of events and information exchanges.

1.1 Policy context

The Cyber Security Strategy of the EU[7] underscores the importance of threat analysis and emerging trends in cyber security. The ENISA Threat Landscape contributes towards the achievement of objectives formulated in this strategy, in particular by contributing to the identification of emerging trends in cyber-threats and understanding the evolution of cyber-crime (see 2.4 regarding proposed role of ENISA).

Moreover, the ENISA Regulation[8] mentions the need to analyse current and emerging risks (and their components), stating: "*the Agency, in cooperation with Member States and, as appropriate, with statistical bodies and others, collects relevant information*". In particular, under Art. 3, Tasks, d), iii), the new ENISA regulations states that ENISA should "*enable effective responses to current and emerging network and information security risks and threats*".

ETL is also related to the context of NIS Directive[9], as it contributes towards provision of cyber-threat knowledge needed for various purposes defined in NIS-Directive (e.g. article 69). Moreover, it comprises a comprehensive overview of cyber-threats and as such it is a decision support tool for EU Member States and can be used in various tasks in the process of building cyber-capabilities.

Of particular interest is, however, the important role of threat landscaping and threat intelligence within the proposed new ENISA regulation/ ENISA mandate[10]. Article 7.7 foresees that "*The Agency shall prepare a regular EU Cybersecurity Technical Situation Report on incidents and threats based on open source information, its own analysis, and reports shared by, among others: Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact (in accordance with NIS Directive Article 14 (5)); European Cybercrime Centre (EC3) at Europol, CERT EU.*". ENISA's work in the area of threat analysis (as exemplified by this report) largely satisfies this requirement, while articles 9 and 10 state the role of emerging cyber-threats both to perform long term analysis and feed research initiatives. Despite the fact that this proposal may be modified during the review process, the role of threat analysis assigned by this draft regulation is indicative for its future importance.

---

[6] https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/12/08/eda-enisa-ec3-and-cert-eu-discuss-enhanced-cooperation, accessed December 2017.
[7] http://www.ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, accessed November 2017.
[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF, accessed November 2017.
[9] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, accessed November 2017.
[10] https://www.enisa.europa.eu/news/enisa-news/european-commission-proposal-on-a-regulation-on-the-future-of-enisa, accessed November 2017.

1.2 Target audience

Information in this report has mainly strategic and tactical relevance[11] to cyber-threats and related information. Such information has relevance of approximately up to one year. It is directed to executives, security architects and security managers. Nonetheless, the information provided is also of use by non-experts. For all these target groups, ENISA has developed a web application that will facilitate the use of the ETL information.

Looking at the details provided by this report and ETL in general, one can discriminate among the following information types and target groups:

- The first part of the document that can be found in chapter 1 is a description of the current state-of-play in cyber threat intelligence (CTI). It reflects discussions performed in 2017 with the ENISA Threat Landscape Stakeholder Group (ETL SG) and within the ENISA event on Cyber Threat Intelligence in the EU (CTI EU) [14]. This information targets **security professionals** or **scholars** interested in open/emerging issues of CTI.
- The top cyber-threats may find a wider group of potential stakeholders who are interested in understanding the threat landscape in general means or would like to deepen into particular threats and their aspects. Hence **decision makers**, **security architects**, **risk managers**, **auditors** clearly belong to the target group. And again, **scholars** and **end-users** who wish to get informed about the where-about of various cyber-threats may find this material useful. Last but not least, ETL 2017 can be a useful tool for **professionals of any speciality** who are interested in understanding the state-of-play in the area of cyber-threats.

Besides the information on cyber-threats, ETL is offering an overview of the entire cybersecurity threat "ecosystem", by covering the relationships of various objects, such as threat agents, trends and mitigation controls. These interconnections make up the context of cyber-threats and can be used in various other activities, such as any kind of security assessment, identification of protection needs or categorization of assets.

Together with ETL 2017, interested readers may find a series of publications analysing cyber-threats based on contemporary incidents. These reports are published as Cybersecurity Infonotes[Error! Bookmark not defined.] are issued in a biweekly basis.

1.3 Structure of the document

The structure of ETL 2017 is as follows:

Chapter 2 "*Cyber Threat Intelligence and ETL*" provides an overview of recent developments in cyber-threat intelligence positions the ETL and summarizes some cyber-threat intelligence issues that are seen as emerging.

Chapter 3 "*Top Cyber-Threats*" is the heart of the ENISA Threat Landscape. It provides the results of the yearly threat assessment for the top 15 cyber-threats.

Chapter 4 "*Threat Agents*" is an overview of threat agents with short profiles and references to developments that have been observed for every threat agent group in the reporting period.

[11] https://www.cpni.gov.uk/documents/publications/2015/23-march-2015-mwr_threat_intelligence_whitepaper-2015.pdf?epslanguage=en-gb, accessed December 2017.

Chapter 5 "*Attack Vectors*" provides an overview of important attack vectors that have led to the most important incidents in 2017.

Chapter 6 "*Conclusions*" concludes this year's ETL. By synthesizing a generic view from the assessed cyber-threats, it provides some policy, business and research recommendations.

2. Cyber Threat Intelligence and ETL

2.1 Cyber Threat Intelligence: State-of-Play

Cyber Threat Intelligence is an area where a lot of development is to be expected, maybe in a more substantial and eventually more silent way. This is the case in all areas of CTI: development of tools, development of CTI methods/approaches, integrating CTI with other security disciplines, etc. While these developments go on, CTI starts finding its way to the organisation. More mature approaches have already managed to find open doors in the ICT-Department and in some cases in the executive management. It is remarkable that CTI ranks at the 5th position of the top most helpful defences[12]. However, a vast majority of security professionals (over 50%) think that the threat landscape evolves much faster than they can strategically and tactically assess it[13].

During this reporting period, ENISA has assessed the need to bring together various CTI experts in Europe for the first time by means of a dedicated workshop[14]. The workshop has found significant acceptance by the relevant community and has provided a series of interesting conclusions[49]. Besides the conclusions that have been drawn (see chapter 2.2 below), CTI experts supporting ENISA have identified the following CTI areas of interest for the coming period:

- **CTI sharing** is key for all kinds of players involved in the creation, dissemination and consumption of threat intelligence. CTI information sharing is one of the main areas for activity in order to establish an efficient CTI usage. At the same time, the potential of CTI sharing is considered as very high. There are a lot of CTI sharing issues to be still resolved by the relevant communities. Some examples are:
  - Options/standards for formatting CTI information;
  - Quality and usability issues of CTI information;
  - Incentives for CTI information sharing;
  - Legal issues of CTI information sharing;
  - Current sharing practices;
  - Current information sharing platforms (MISP, CIF, etc.)
  - Future trends in CTI information sharing;
  - Maturity models for CTI and CTI sharing functions;
  - Limitations of available tools.
- **Active defence** is considered as an effective strategy to make launching of various cyber-threats costly and inefficient. Based on available cyber-threat intelligence, active defence may reverse the "asymmetry" of many cyber-threats/cyber-attacks and create additional obstacles to adversaries. Active defence is a new area that is characterized by defence tactics aiming at disrupting cyber-attacks. This can be achieved by developing innovative approaches in disrupting malicious infrastructures or by developing offensive capabilities towards attack methods of adversaries. Indicative topics to be covered are:

[12] https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910, accessed November 2017.
[13] http://www.marketwired.com/press-release/cyber-pros-point-to-perfect-storm-as-security-fundamentals-face-crisis-2239435.htm, accessed November 2017.
[14] https://www.enisa.europa.eu/events/cti-eu-event, accessed November 2017.

- Purpose and objectives of active defence;
- Areas of applicability of active defence;
- Active defence elements/processes;
- Active defence methods & frameworks;
- Active defence tools;
- Intelligence-led active defence;
- Legal issues with regard to active defence.

- Adapted to the needs of various user groups, usage scenarios and differentiated user capability and maturity levels, **automation methods of CTI** play an important role. Their uptake will affect the level CTI will penetrate the cyber-security field. Indicatively, various issues to be discussed in this area are:
  - CTI elements (current, desired, future, etc.);
  - Formulation of CTI program requirements (understanding the needs, manage expectations, leverage on available resources);
  - Purpose/use cases of CTI information; target groups (e.g. security, technical, non-technical, decision maker);
  - CTI modelling, taxonomies, frameworks and workflow issues;
  - Integrating/Mapping CTI to related internal processes and available governance and control structures (e.g. SOC, Hunting, SIEM, Red teaming, Risk Governance, Compliance, etc.);
  - Tailoring CTI information to own needs;
  - Identify role of CTI in internal value creation processes and integrated it in decision making (i.e. tools for the board, HR, etc.);
  - Legal aspects of CTI;
  - The role of CTI in coverage of legal/compliance requirements.
- Cyber Resilience requires a defense in depth approach containing several layers of defense. However, implementing multiple layers of defense everywhere is too costly. It is therefore necessary to identify the most effective practices for protection using the Kill Chain[15] or Diamond model[16] approaches as guidelines for the incorporation of threat intelligence. Some indicative topics when in **embedding CTI in security organization** are:
  - CTI elements (current, desired, future, etc.);
  - Formulation of CTI program requirements (understanding the needs, manage expectations, leverage on available resources);
  - Purpose/use cases of CTI information; target groups (e.g. security, technical, non-technical, decision maker);
  - CTI modelling, taxonomies, frameworks and workflow issues;
  - Integrating/Mapping CTI to related internal processes and available governance and control structures (e.g. SOC, Hunting, SIEM, Red teaming, Risk Governance, Compliance, etc.);
  - Tailoring CTI information to own needs;
  - Identify role of CTI in internal value creation processes and integrated it in decision making (i.e. tools for the board, HR, etc.);

[15] https://en.wikipedia.org/wiki/Kill_chain, accessed November 2017.
[16] http://www.activeresponse.org/the-diamond-model/, accessed December 2017.

- Legal aspects of CTI;
- The role of CTI in coverage of legal/compliance requirements.

- **CTI capabilities and skills** is one of the most important aspects for the usage of CTI as tool in all concerned organisations, networks of stakeholders, interested businesses, education. Main parameter for the identification of capability level and skill profiles will be the proportionality of CTI usage in organisations and the required maturity level.
  - Turning CTI information from a capability to knowledge for various stakeholders;
  - CTI use cases;
  - Proportionality of CTI usage and related skill sets (especially low-cost CTI options and tools);
  - CTI analyst's skillset;
  - CTI tradecraft for various use cases;
  - CTI curricula and methods for integrating CTI "lessons learned" in education;
  - Using CTI for awareness purposes.

CTI capacity building is yet another major issue in the utilization of CTI. CTI capacity building covers issues related to education, training and research. Main parameter for the identification of skill profiles will be the proportionality of CTI usage in organisations and the required maturity level.

2.2 CTI Issues: An Overview

Given recent developments in the area of CTI but also discussions with CTI experts, we have identified some issues that need further elaboration. These have been also discussed in the ENISA event organised in 2017[Error! Bookmark not defined.]. Below we present the issues that seem to be the most important for the attention of the target group of this report and the CTI community, in particular:

- **Adoption of CTI** in the organisation seems to be an important, yet not sufficiently matured practice. Though the topic has been sufficiently investigated by governmental players[17,18,19] and vendors[20,21,22,23] its practical implementation in organisations is lagging. It has been argued, that there is a discrepancy between complexity of cyberthreats and skills. Together with lack of strategic and tactical understanding of the landscape, this leads to a low level of adoption of CTI and low level of integration in the organisation. In many occasions, CTI experts praise the importance of integrating CTI and risk management activities, while investing in automated tools and skills[24]. The details of CTI adoption are visible in some surveys that ran in the reporting period[12,25]. There is a lot of work to be done for CTI adoption, in particular its integration with risk management, including the development of key

[17] https://www.crc-ics.net/research.html, accessed November 2017.
[18] https://www.slideshare.net/dgsweigert/cyber-threat-intelligence-integration-center-ondi, accessed November 2017.
[19] http://www.tno.nl/media/9419/innovating-in-cyber-security.pdf, accessed November 2017.
[20] https://www.surfwatchlabs.com/threat-intelligence-products/purchase, accessed November 2017.
[21] https://www.slideshare.net/Splunk/enterprise-security-featuring-uba-67591180, accessed November 2017.
[22] https://www.eclecticiq.com/resources/white-paper-threat-intelligence-maturity-model, accessed November 2017.
[23] https://www.recordedfuture.com/cyber-threat-intelligence-team/?utm_source=hs_email&utm_medium=email&utm_content=58479321&_hsenc=p2ANqtz--q5-6dn7AqvsG_B1j7oaVVP5tvixpO9W-gowIODnRLgmcAoI3iUXAPSHNgtshlgjS6O9GPTornqF-gcDK07k7GZbJaNbMPYA1p1BA4XuFLL2nGbKM&_hsmi=58479321m, accessed November 2017.
[24] https://www.business.att.com/cybersecurity/docs/vol4-threatlandscape.pdf, accessed November 2017.
[25] https://www.redseal.net/files/PR/2017%20Resilience%20Report%20Executive%20Summary%20FINAL.pdf, accessed November 2017.

performance indicators for threat intelligence (see also bullet "*Creation and consumption of CTI within organisations*" below).

- **Automated support of strategic and tactical CTI is limited**. Existing tools depend on standards, in particular on the ingest side[26]. Despite the existence of various standards for structuring threat information, however, it has been reported that CSV[27] is still the most commonly used standard. This shows the relatively low need for (pre-) structure formats dictated by CTI standards. Although CTI standards are used for ingest, generated feeds are mostly packed in more efficient, simple CSV files. In many cases of massive data processing the use of CSV may be connected with performance issues. Moreover, the non-contextualized nature of CSV may be another of the main reasons for its use. Another reason for the use of standards seems to be connected with the available skills. Nonetheless, research has shown that CTI tools are mostly data collection and mining engines and are NOT providing analysis functions. This turns big parts of cyberthreat intelligence to manual activities that are often generating closed source results[28]. It is indicative that – for example – from the STIX available threat intelligence related constructs indicators of compromise is the most popular type of exchanged information. In the ENISA CTI event it has been debated about the use of formats and in particular the use of feeds vs. contextualized information.
- **Creation and consumption of CTI within organisations** are two fairly complex tasks. Firstly, it is often the case that CTI is not properly created: its contextualization according to the business processes and valuable assets[29] is often neglected. This, reduces the relevance of CTI with regard to realistic Modus Operandi for the particular business/organisation. Although CTI is being already considered as an important tool, CTI professionals often feel overwhelmed by the amount of data to be processed and the speed incidents are taking place. Given the usually limited resources to leverage on CTI information and the relatively low maturity level in CTI adoption, organisations cannot fully benefit from CTI information, or the benefits do not become visible at all levels. Finally, given the fact that most of the tools are in the position to process large amounts of data up to indicators of compromise (IOC), CTI information at higher contextual levels is not present at all.
- Due to limited maturity, integration, automation, etc., **skilled resources** are the last bastion for successful CTI[30]: they perform a significant part of the analysis needed and produce actionable intelligence out the information generated by tools. Given the fact that tactical and strategic CTI is mainly a manual activity, CTI remains valid within an organisation and serves its requirements. The same is true for outsourced CTI: if it is not adapted by the provider, the recipient will need to adapt it to their business environment. Prerequisite in both cases is the knowledge of business, operational processes, and further requirements, such as those emerging from other relevant workflows of the organisation (e.g. security management requirements).
- The **right CTI for an organisation** is the one based on their business and organisational requirements. CTI cannot be outsourced if it is not clear to the organisation what is its scope. Like most of the investments, CTI development should be based on own requirements and not tools. In most cases, "build-in" workflow and requirements of tools are the common denominator of consolidated market requirements and may not correspond to own needs. In the task of finding a proper CTI approach, organisations will need to take into account the three key elements of a company's quality system,

[26] https://www.rsaconference.com/writable/presentations/file_upload/pst-w08-cyber-threat-intelligence-sharing-standards.pdf, accessed November 2017.
[27] https://www.ietf.org/rfc/rfc4180.txt, accessed November 2017.
[28] https://wi2017.ch/images/wi2017-0188.pdf, accessed November 2017.
[29] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016, accessed November 2017.
[30] https://www.itproportal.com/features/mobilizing-people-power-against-cyber-threats/, accessed November 2017.

namely people, processes and products. One typical example of the role of processes in the identification of a threat landscape is the new EU roaming act. Through elimination of roaming costs, users do not use Wi-Fi anymore (in many cases slower than 4G). This leads to massive increases in mobile infrastructure that poses new management and availability risks[31]. Last but not least, identification of desired level of CTI capability is key for investments in that topic.

- Currently, there are several **types of Cyber Threat Information** depending on the scope and the degree of details of the provided content. Variations in content may occur according to the purpose of the analysis, often manifested through the scope of the threat assessment. The scope may include the size of the collected data sample and/or the specific area of the analysis. Law enforcement agencies, for example, issue threat reports that focus on cyber-crime, and in particular such that relates to fraud, abuse of humans, IPR preaches and any other crime that is covered by criminal law[32]. Other types of CTI content may be related to service provisioning and may even consists of real-time adaptations of operated controls[33]. Others may be related to awareness raising and adaptation of security policies, just like the ENISA Threat Landscape. Besides generic threat analysis and landscapes, there are also thematic CTI sources, yet those are usually closed source and are subject to sector-oriented CTI exchange activities and ISACs[34]. It is extremely relevant for an organisation to identify the kind of CTI that needs to consume and understand the content and scope of various offerings in the market.
- **Simplicity of consumed CTI information** is key for its deployment. All stakeholders involved in the supply-chain of CTI will need to take care to simplify the structure of their results, should those be thought of to be consumed by humans. Given the structure, updatability and visualization requirements of CTI, simplification of CTI presentation is a complex task. Though data science is inherently part of threat analysis process, in many cases the issuers of CTI do not invest required resources to materialise simplification. Currently, existing CTI and threat information sharing tools invest in visualisation[35]. Given the proliferation of CTI (both open and closed source), it is expected that some improvements will be experienced in this area. Nonetheless, significant work needs to be made in this area. ENISA has also invested resources in this area. The followed approach is discussed in some detail in chapter 2.3.1 below.
- It is important to **develop means (e.g. in form of KPIs) to show the influence of CTI in assets protection** in the organisation. Due to loose usage scenarios (imprecise CTI use cases, varying CTI-content, etc.) and not properly interconnected to cyber security related practices (ISMS, Risk Management, SIEM, threat hunting, etc.), it is not clear what the indicators for successful CTI usage are. This makes unclear to decision makers how CTI contributes to the general risk mitigation in the organisation. Assuming an increasing role of CTI[12], the relevant community will need to identify key performance indicators for CTI with regard to interrelated disciplines, such as security operations, risk management, incident management, business owners, vulnerability management, etc. As far as this is not done, it will not be easy to enhance maturity demonstrate CTI role in the organisation.

[31] https://researchcenter.paloaltonetworks.com/2017/10/sp-secure-mobile-roaming-just-time-roam-like-home/, accessed November 2017.
[32] https://www.europol.europa.eu/iocta/2017/index.html, accessed November 2017.
[33] https://www.slideshare.net/cisoplatform7/security-strategy-and-tactic-with-cyber-threat-intelligence-cti-69859022, accessed November 2017.
[34] https://www.fsisac.com/, accessed November 2017.
[35] http://www.misp-project.org/, accessed November 2017.

- There are a lot of unexplored dependencies between CTI and other disciplines. This is a conclusion that has emerged by training organisations trying to analyse the knowledge modules behind CTI[36]. Among the most important modules of CTI belong: computer science regarding automation, incident management and information security, machine learning and artificial intelligence; Data science regarding data discovery, consolidation, data normalization and augmentation, data mining, statistics, visualization, data storage techniques, etc.; criminology including forensics, intelligence collection, threat agent analysis. Good practices, methods and tools in every of these categories would also be relevant. It is obvious that due to its complexity, full CTI capability can only be developed by combining multiple skills. Resources for such a setup are usually available at the level of nation states or big multinational companies. The training skills required to teach CTI may even go beyond the knowledge that is available within a single educational institution. Available CTI trainings cover some parts of the above mentioned areas[37]. We believe that the existence of complete CTI curricula will still need some time, depending on CTI market maturity progress.
- Development of **maturity models for CTI** will be useful. Such models will help both users and providers measure the maturity of their approaches/good practices and tools. Such maturity models exist to some extent[38,39]. Given recent developments in CTI, those models might need to be updated/consolidated to embrace developments in the area of threat information (sharing) platforms and workflows connecting the various cyber security related disciplines (see also discussion with KPIs above). ENISA does currently initial work towards such a maturity model. It that has evolved within an attempt to define requirements of Threat Information Sharing Platforms. The related paper will be published by ENISA end of January 2018.

2.3 ENISA approaches to CTI dissemination

In the reporting period ENISA has implemented a few instruments to facilitate dissemination of various available materials in the area of threat information/threat intelligence. While one of the implemented instruments serves as a dissemination tool for ETL and related information, some tools to facilitate CTI-Stakeholder communication have been implemented. In this section both tools are being described in short.

2.3.1 ETL Web App[40]

In 2017, ENISA has developed a web application that allows for the visualization of results both of the ENISA Threat Landscapes and Thematic Landscapes. In both areas, the application allows for displaying results published in various years and for various thematic/sectorial landscapes. The aims of the application are as follows:

Increase usability and accuracy of available information. Currently available ETL information (mainly the contents of yearly reports), is monolithic in nature and document-like organized. Splitting this document into its constituent parts enables a selective reading, while it allows users to better explore its contents, including the large amount of references. But most importantly, the content of additional thematic

[36] https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/current-training-educational-opportunities/, accessed November 2017.
[37] https://www.sans.org/course/cyber-threat-intelligence, accessed November 2017.
[38] https://www.digitalshadows.com/blog-and-research/cater-for-your-threat-intelligence-needs/, accessed November 2017.
[39] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf, accessed November 2017.
[40] https://www.etl.enisa.europa.eu, accessed November 2017.

assessments comes to gain from the threat landscapes by demonstrating the exposure of assets and the methods for reducing this exposure through controls.

Allows for better information discovery. Having the information in self-contained modules facilitates the precision searches. Through a comprehensive search function, users are in the position to search from the summary of all supported information according to the object type and its content. Through the interconnections of the stored (and found) objects, users may navigate the information by means of its related (contextually relevant) objects.

Allows for user interaction with the published material. Through the implementation of user experience functions, the application allows users to login and provide contributions of any type to the various stored/retrieved information objects. While both anonymous and logged-in users may access the same information, logged-in users may interact with the stored information and contribute to the information collection. By using authentication functions of linkedin[41], facebook[42] and google[43], no user data need to be managed locally.

GUI allows for usage by multiple stakeholders. As ETL and related documents are targeting non-technical users, the developed GUI has been designed to be usable for user that are agnostic to threat information/threat intelligence. Being totally uniform for both mobile and web applications, it allows users to have identical look and feel in all types of devices, both for the web app and the mobile app. This has been achieved by using hybrid software development technology/environment[44].

Transition from a page-based to **a more modular documentation approach**. Through the ETL app, ENISA intends to establish an approach that allows online editing and publishing of smaller information portions/modules. In this way, ENISA may respond more quickly to assessed changes of the cyberthreat landscape, while at the same time disseminate available CTI information to stakeholders. We believe that this possibility will contribute towards a more dynamic communication of CTI knowledge to the stakeholder community.

Integrate and disseminate material from all relevant sources. The ENISA app may serve as a dissemination platform for information from various stakeholders. Besides external stakeholders, ENISA internal material will be also put in the context of cyberthreats, such as ENISA cyber security infonotes[45], training[46] in malware analysis, mobile malware, etc. Moreover, cyberthreat objects be used as consolidation point for the developments in a particular threat. This information may be created in cooperation with other EU bodies, e.g. CERT-EU.

Allows for the **visualization of material that spans more than one year**. The ETL app will cover material that has been created in various years. Examples are older ETLs and Thematic Landscapes. This will allow users to increase the usability of older ENISA information, always in the context of threats, assets and all related objects hereto, just as it is foreseen in the meta-model that is used as basis for this threat landscape (see chapter 2.4).

Use of the same storage model for ETL process and ETL application. The data model used for the ETL work and for the storage of data within the ETL app are identical. This allows for a smooth transfer of

---

[41] https://developer.linkedin.com/docs/signin-with-linkedin#, accessed November 2017.
[42] https://developers.facebook.com/docs/facebook-login/, accessed November 2017.
[43] https://developers.google.com/api-client-library/php/auth/web-app, accessed November 2017.
[44] https://clearbridgemobile.com/mobile-app-development-native-vs-web-vs-hybrid/, accessed November 2017.
[45] https://www.enisa.europa.eu/publications/info-notes#c5=2007&c5=2017&c5=false&c2=infonote_publication_date&reversed=on&b_start=0, accessed 2017.
[46] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#dynamic, accessed November 2017.

homogeneous information between the ETL process (collection, analysis, assessment) and the objects supported by the ETL app. This fact facilitates both the work of ENISA and the better understanding of the stored information by interested stakeholders.

The following figure (see Figure 2) presents the "look and feel" of the developed web app. It presents three main screenshots of the app: a screenshot of the ETL (Threats) (first left), a screenshot of the Thematic Landscapes (Assets) (center) and a snapshot with the search and user interaction menus (right).

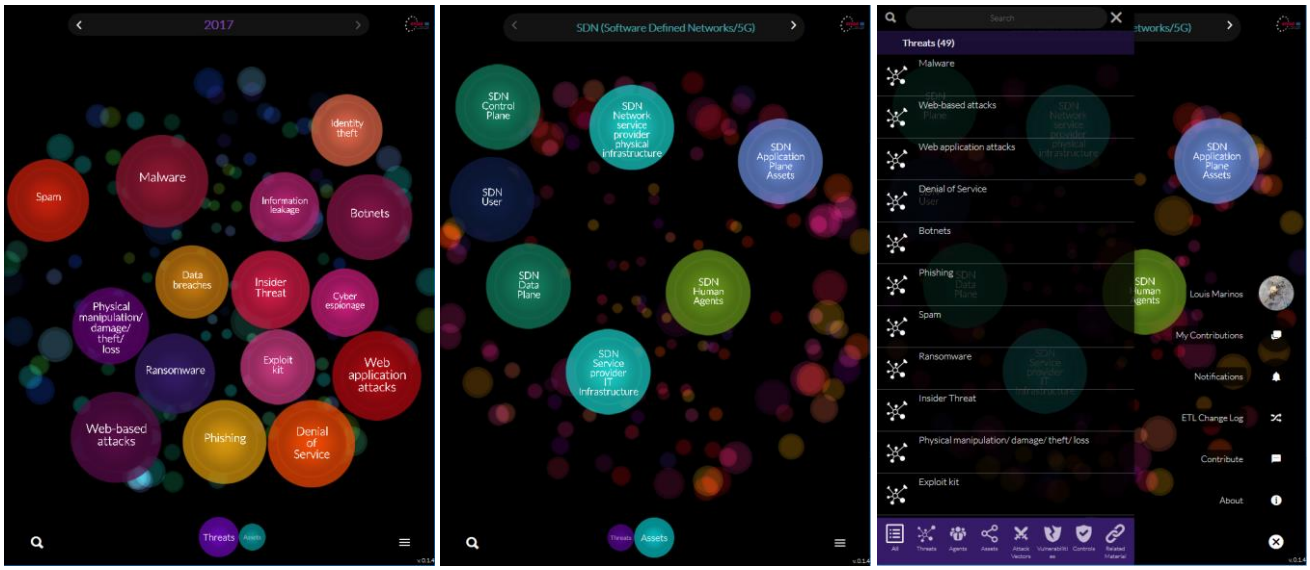

Figure 2: Screenshots of the ETL app (etl.enisa.europa.eu)

With the ETL app, ENISA offers another public domain CTI platform that provides cyberthreat information including asset exposure and possible mitigation controls. It thus covers the full spectrum of information needed to implement proper protection policies for various assets. Just as with the material around ETL, it provides support to end-users willing to find some guidance for protecting their assets. The (only) additional effort that needs to be done is to assess the value of assets according to their role in business processes.

2.3.2 CTI EU

In the reporting period ENISA has organized an event for the European CTI community[14]. By implementing received stakeholder requests, we have created with this event a forum for various actors and users of CTI to voice their needs, concerns, plans, etc.

By assessing a list of various interesting areas via the ENISA Threat Landscape Stakeholder Group, we have organized parallel session for 5 topics. Aim was to enforce discussions among participants on these hot topics, instead of having only frontal presentations from a few acknowledged experts.

Besides the discussions in the various sessions, the attempt to have a continuous dialog has been undertaken. ENISA has created a chat-URL to facilitate discussions among the participants[47].

The results of the event (participant presentations and conclusions) can be found here[48].

[47] https://cti-chat.enisa.europa.eu, accessed November 2017.
[48] https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-presentations, accessed November 2017.

2.4 Scope and used definitions

The method used for the development of ETL has been documented in previous landscapes. Indicatively we would like to mention chapter 2.6 of ETL 2016 (see chapter "*Scope and definitions*")[49]. For this reason, in ETL 2017 we do not refer to the method and model underlying the creation of the present report. Interested readers will need to consider the material mentioned above.

The definitions used in this study are identical to the ones of ETL 2016[49]. In order to visualize the relationships among all elements of risks, we use a figure taken from ISO 15408:2005[50] (see Figure 3). This figure has a level of granularity that is sufficient to illustrate the main elements of threat and risk mentioned in this report. The entities "Owner", "Countermeasures", "Vulnerabilities", "Risks" and partially "Assets" are not taken into account in the ETL. They appear in the figure in order to show their context with regard to threats. The notion of attack vector is being displayed in this figure and is covered in the present report (see chapter 5).

One should note that the entities *threat agent* and *threat* presented in Figure 3 are part of the ETL data model. This is quite natural as these entities make up the kernel of ETL.

As regards risks, we adopt the definition according to the widely accepted standard ISO 27005: "*Threats abuse vulnerabilities of assets to generate harm for the organisation*". In more detailed terms, we consider risk as being composed of the following elements:

Asset (*Vulnerabilities, Controls*), **Threat** (*Threat Agent Profile, Likelihood*) and **Impact**.

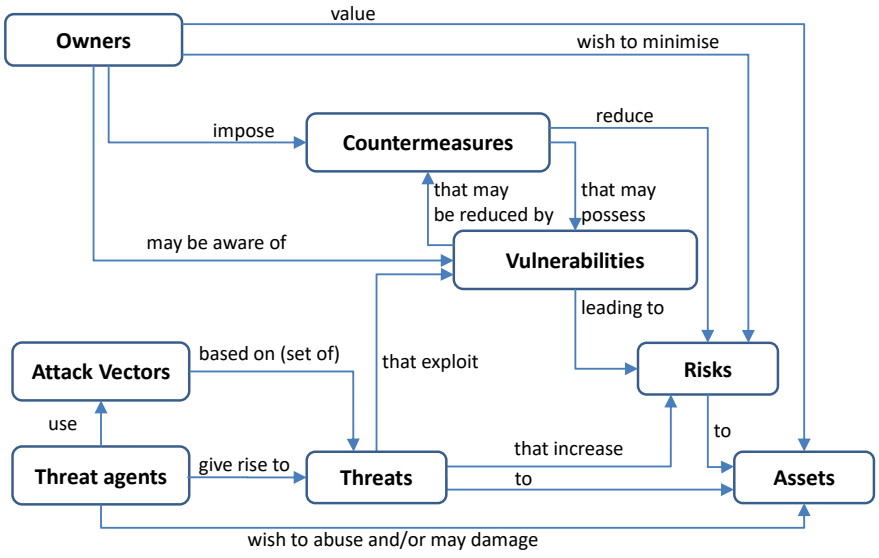

Figure 3: The elements of risk and their relationships according to ISO 15408:2005

As a final note we would like to state that the above data model is identical to the one used within the ETL application (see also chapter 2.3.1), and in particular both for storage and display purposes.

[49] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016, accessed November 2017.
[50] https://www.iso.org/standard/40612.html, accessed November 2017.

3. Top cyber-threats

This chapter is a presentation of the current threat landscape 2017. It is the result of the collection, analysis and assessment effort that has taken place in the entire year 2017. The source of the collected information is the public domain - almost exclusively Open Source Intelligence (OSINT). As in all ENISA landscapes, the time window of information collection is from ca. December 2016 till December 2017. It is being considered that the collected information and the performed assessment cover most of the remarkable events and developments that have are relevant to cyberthreats. However, we do not claim exhaustiveness in the information collection[51].

Continuing the trend of previous years, incidents but also advancements in defence and attack tactics have increased in the reporting period. Among the many interesting developments in 2017, ransomware attacks have dominated the threat landscape. A further remarkable development is the massive increase of phishing/spear phishing: it has now covered the gaps created by lawful takedowns of malicious infrastructure components such as botnets and exploit kits. The success of these methods is manifested by the new record in data breaches that has been encountered in 2017[414].

The information collection exercise conducted in 2017 involved tight cooperation with CERT-EU, the ENISA stakeholder group and provided pro-bono access to a threat intelligence portal of CYjAX[52] (CYjAX Security Portal). Moreover, malware information has been taken into account through the malware information sharing platform MISP. Though the information taken into account contained some classified information, this material has not been disclosed. It has just been taken into account during the analysis process, e.g. in the validation of performed assessments.

The presentation of the fifteen top cyberthreats has been revamped in this ETL. The structure of the description template has been changed in order to accommodate:

- a short description of the cyberthreat as it has appeared in the reporting period;
- a list of interesting points with remarkable observations for this cyberthreat;
- trends and main statistics including geographical information, when relevant;
- top threats within this threat category;
- specific attack vectors used to launch this threat;
- mitigation actions;
- kill chain for this cyberthreat and
- authoritative references;

It has to be noted that according to the findings and the nature of each threat, some of the above elements might be slightly different or missing. Moreover, kill-chains and mitigation actions (vectors) have been reused from previous year's ETL, adapted accordingly with new evidence as deemed necessary.

[51] Due to the surging number of information on cyber-security incidents and threats and the limited available resources, it is likely that many articles, reports, white papers, etc. have escaped our attention. It may also be the case that missing reports have been intentionally left out from our references because they had significant overlaps with used references.

[52] https://www.cyjax.com/, accessed November 2017.

The fifteen top threats assessed are the ones that have dominated the threat landscape. Though no new threat has been encountered, there are quite some changes in the ranking. These changes reflect the developments that cyberthreats have undergone. Some interesting observations regarding the presented cyberthreats and their ranking are as follows:

- It is considered that data breaches and identity theft are not typical cyber-threats. Rather, they are consequences of successful threats (i.e. actions on objectives, if formulated according to the kill-chain). In other words, in order to breach information, one has to successfully launch one or some of the other cyber-threats addressed in this chapter. As such, data breach and identity theft are maintained in our top list because they are found throughout the analysed material.
- The presented 15 cyber-threats do not all belong to different distinct threat categories. Hence, they represent instances from 12 threat types, according to the threat taxonomy used[53]. Ransomware, for example, is a specialization of the threat type malware. Hence, for this threat all malware protection measures apply, plus some that are special for the specialized threat, i.e. in this case ransomware. The same is true for Identity Theft: it is a special category of Data Breach. Nonetheless, it is handled separately because this threat is launched by special malicious artefacts.
- Cyber espionage is merely a motive than a cyber-threat. This cyber-threat is maintained because it unites almost all of the other cyber-threats in addition to some high-capability threats that are specially crafted by state-sponsored organisations, such as advanced hacking tools, vulnerability discovery and combination of military/law enforcement intelligence methods.
- The ranking in the list is indicative. A cyberthreat is assigned a ranks according to the role it has played in the threat landscape. The position is based on the number of incidents, impact and role played for other cyberthreats. Sharing the same ranking is not foreseen in our list. This leads to the interesting situation where - although a threat increases - it is being ranked lower just because another cyberthreat has been ranked higher, impacting thus the ranking of the cyberthreat below it.

As a final remark, we would like to state that ENISA has developed a web based tool[54] as a means to deliver cyberthreat information in a quicker and more efficient manner. This tool will allow for a better, more intuitive use of the ETL information, while allowing for the storage and interconnection of various ENISA results in a multiannual manner (see also chapter 2.3.1).

[53] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy, accessed November 2017.
[54] https://etl.enisa.europa.eu, accessed November 2017.

3.1 Malware

3.1.1 Description of the cyberthreat

Once again, in 2017 malware is the most frequently encountered cyberthreat. It continued its constant evolution in terms of sophistication and diversity, albeit its frequency has stagnated. In 2017 some Anti-Virus (AV) vendors detected more than 4 million samples per day[55], or more than 700 million samples in Q1 2017[56], while hundreds of ready-to-use anti-debugging and anti-analysis tools can be purchased from the black market. Mobile malware has demonstrated a descending evolution in terms of unique samples, with an average of 1,3 million samples in Q1 and Q2 of 2017 compared with 1,5 million in Q3 of 2016, but experts reported a rise in terms of mobile malware sophistication[57]. 2017 can be characterized as the year of big and highly mediatized online leaks of tools and exploits. These have allegedly been developed by a state intelligence agency[58] and used in WannaCry and NotPetya outbreaks. Also, a diversification of infection vectors have been observed, with a special emphasis on compromising the supply chain and update mechanisms of some well-known and widely used software such as CCleaner[59] and MeDoc[60].

3.1.2 Interesting points

The identified interesting points for malware are as follows:

- **The rise of click less infections**. The WannaCry outbreak is a representative example of the trend to use remote execution exploits (like EternalBlue) and RDP brute force attacks as infection vectors, achieving worm capabilities and eliminating the need for a user action (e.g. to click or open a malicious URL or file)[61].
- **"Living of the Land" and fileless attacks[62]**. Fileless malware is being used in attacks by both targeted threat actors and cybercriminals in general – helping to avoid detection and make forensic investigations harder. Kaspersky Lab's experts have found examples in the lateral movement tools used in the Shamoon attacks, in attacks against Eastern European banks, as well as in the hands of a number of other APT actors[63].

  Attackers are increasingly making use of tools already installed on targeted computers, like PowerShell, PSExec, or WMI, or are running simple scripts and shellcode directly in memory. Creating fewer new files on the hard disk, or being completely fileless, means less chance of being detected by traditional security tools and therefore minimizes the risk of an attack being blocked. Using simple and clean dual-use tools allows the attacker to hide in plain sight among legitimate system administration work[64].

---

[55] https://www.avira.com/en/threats-landscape, accessed September 2017.
[56] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf, accesses September 2017.
[57] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed September 2017.
[58] https://blog.rapid7.com/2017/04/18/the-shadow-brokers-leaked-exploits-faq/, accessed September 2017.
[59] https://blog.avast.com/update-to-the-ccleaner-5.33.6162-security-incident, accessed September 2017.
[60] http://blog.talosintelligence.com/2017/07/the-medoc-connection.html, accessed September 2017.
[61] https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/, accessed September 2017.
[62] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/increased-use-of-powershell-in-attacks-16-en.pdf, accessed September 2017.
[63] https://usa.kaspersky.com/about/press-releases/2017_destined-for-deletion-apts-harness-wipers-and-fileless-malware-targeted-attacks, accessed September 2017.
[64] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf, accessed September 2017.

- **Network spreading through worm capabilities**. The success of WannaCry and NotPetya outbreaks, in terms of infections, is inspiring attackers to revisit worms to propagate their infections more rapidly. Right after those outbreaks, other malware variants appeared and used the EternalBlue vulnerability. This vulnerability is denoted by entry CVE-2017-0144 and DoublePulsar exploits from the Shadow Brokers released as part of their campaigns[65]. Among them were Adylkuzz, Uiwix, and EternalRocks.
- **Wipers** are being harnessed by targeted threat actors, both for cyber-sabotage and for deleting tracks after cyberespionage operations. An evolved generation of Wipers was used in the new wave of Shamoon attacks. The subsequent investigation led to the discovery of StoneDrill and its code similarities to the NewsBeef (Charming Kitten) group. A StoneDrill victim was found in Europe
- **The rise of script-based malware[66].** Scripting techniques used by malware are a widely embraced tactic by attackers. Some malware employ these techniques during their entire operations and others for a specific purpose. McAfee Labs[66] has seen script-based malware increase during the last two years, as cybercriminals continue their search for ways to deceive users and evade detection.
- Just as in other years, we have seen in 2017 malicious functions being packaged within **Potentially Unwanted Programs (PUPs)**. While legitimate browser developers like Firefox and Chrome are making efforts to tighten security, the adware industry is creating its own custom browsers without any built-in security features and bundling them along with adware applications. They will shamelessly replace your own browser as the default browser and expose you to the greater risks of using such a browser.
- **Escalation of ad wars boosts malware delivery[67].** Fake advertisements are here to stay, too, with an increasing number of ad networks that take a user's browsing session hostage, whether to deliver malware, scams, or endless surveys. It is alarming that in 2017, such adware has been delivered through top-tier sites. It seems that there is a race between ad users trying to block malvertising and advertisers who try to install telemetry functions to trace user feedback. Advertisers have new methods to bypass ad blockers, but those will be followed by updated ad-blocking software that blocks them again. Cross-site scripting detection is yet being integrated in ad-blockers to detect injections of malicious modules.
- **Hardware and firmware threats an increasing target for sophisticated attackers.** In the reporting period we have seen some very impressive cases of hardware vulnerabilities[68,69,70]. Though it is not yet known if some malware exploits these vulnerabilities, their level and depth in the hardware architecture makes it quite difficult to detect and prevent from. Reportedly, vendors have already respond to these vulnerabilities. However, the level of patching will be difficult to assess for long time from now.
- **Hybrid Attacks[71].** Attackers are creating all the time new and more complex techniques for attacking and compromising their targets. For example, they are combing two different attacking methods, one of them more noisy than other one, in order to deceit all security mechanism. When things like this is

[65] https://blogs.cisco.com/security/talos/adylkuzz-uiwix-eternalrocks, accessed September 2017.
[66] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sept-2017.pdf, accessed September 2017.
[67] https://www.mcafee.com/ca/resources/reports/rp-threats-predictions-2017.pdf, accessed September 2017.
[68] https://www.blackhat.com/docs/us-17/wednesday/us-17-Matrosov-Betraying-The-BIOS-Where-The-Guardians-Of-The-BIOS-Are-Failing.pdf, accessed November 2017.
[69] https://security-center.intel.com/advisory.aspx?intelid=intel-sa-00086&languageid=en-fr, accessed November 2017.
[70] https://arstechnica.com/information-technology/2017/11/intel-warns-of-widespread-vulnerability-in-pc-server-device-firmware/, accessed November 2017.
[71] http://arrka.com/index.php/2017/09/20/malware-trends-2017/, accessed November 2017.

happening and minimum two attack methods are launched in tandem, the focus will be to restore the affected service while the real targeted malware goes at least temporarily undetected and can do real damage. For example, BrickerBot[208,238] is a such malware: it is using compromised routers and wireless access points against other Linux-based devices. After that the malware is brute forcing using common username and password combinations on devices that have the Telnet exposed to the internet. If it finds a successful credential it will launch commands to overwrite the data stored on the device's mounted volumes.

- **MacOS and Linux malware is growing[72]**. In 2016 was observed in statistics a rising of the overall number of malware programs for macOS doubled within the Q1 of 2017. Also, Linux systems suffered a marked increase in the recorded attacks.
- **The long life of DGA.** A lot of important malware campaigns are using domain-generation algorithms (DGAs) to make them hard to be detected using pseudo-random generation of domain names. DGA generated domains have a short lifetime but can sometimes last for months, which makes heuristic blocking more challenging as a defending mechanism. Most likely this trend is because the attackers are under pressure to conduct attacks able to avoid the defense mechanism and remain undiscovered for a long period of time. Also, this is a mechanism which helps the attackers to avoid blocklists, but not so fast that defenders manage to block all new domains. In most cases, the algorithms used by the malware that generate DGA domains are using only two elements when creating domains: the length of the domain name and the possible top-level domains it can use.
- **Supply chain attacks: one compromised vector can affect many organisations.** Similar with enterprises which are looking to save time and money all the time, attackers are searching new ways to make their attacks more and more efficient. As the Cisco partner RSA discovered, supply chain attacks can offer maximize the impact with a minimal effort invested by the criminals. In the case that RSA handled, the attackers inserted malicious codes into legitimate software typically used by system administrators to analyse Windows system logs. The compromised software was available for download at the vendor's website. The result was maximized because one compromised vector—the vendor site—could then spread the threat to many more enterprise networks, simply by allowing users to download the compromised software.

3.1.3 Trends and main statistic numbers[73]

- With about 22 million new malware samples in the first quarter of 2017 it looks like the number of malware files will continue to decline[74];
- Businesses are experiencing far more threats in 2017: In the first quarter of 2017, businesses encountered far more malware than they experienced in Q1 2016[75];
- In Q1 of 2017, there's been a clear trend towards more traditional viruses for Windows, the share of which in the malware distribution compared to 2016 is increasing from 37 to 46%. The number of Windows Trojans also considerably increased in the first quarter of 2017, climbing from 23 to over 30%. This trend is also followed by the number of detected ransomware samples, growing by one-third to

[72] https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf, accessed September 2017.
[73] https://blog.barkly.com/ransomware-statistics-2017, accessed September 2017.
[74] https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017, accessed September 2017.
[75] https://www.malwarebytes.com/pdf/white-papers/MalwareTrendsForSMBQ12017.pdf, accessed September 2017.

1.55% and is seeing a decline in Internet worms, which with a percentage drop from 25 to 6% are clearly among the losers in the malware market[76];

- Mac users were kept busy dealing with more malware in Q2 than they had seen in all of 2016[77];
- Clearly, ransomware continues to dominate the Windows malware scene, with an evolution from 55% in January 2017 to 75% in July 2017[78];
- **The overall trend of malware in 2017 was STABLE to slightly declining.** Yet malware has the most detections from all other threats.

3.1.4 Top Malware threats

In the reporting period, the following key malware vectors have been assessed:

RDP attacks spreading CrySIS ransomware increase 2x
First WannaCry variant described as run-of-the-mill
Microsoft releases security update MS17-010, patching vulnerability CVE-2017-0144 (EternalBlue)
Shadow Brokers leak EternalBlue and other NSA exploits AES-NI ransomware claims to be utilizing EternalBlue Adylkuzz cryptocurrency mining malware utilizes EternalBlue
WannaCry utilizes EternalBlue and worm capabilities to infect 400,000 computers QakBot banking trojan triggers mass Active Directory lockouts with modified worm capabilities
NotPetya utilizes EternalBlue and system tools to spreadorebrect ransomware mimics NotPetya's use of PsExec forlateral movement Spike in SamSam ransomware attacks utilizing RDP to spread
Emotet banking trojan adds worm capabilities TrickBot banking trojan adds worm capabilities
Eternal Blues scanner identifies 166,000 hosts vulnerable to EternalBlue Rapid7 scan identifies over 4 million exposed RDP endpoints

[76] https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf, accessed September 2017.
[77] https://www.malwarebytes.com/pdf/white-papers/CybercrimeTacticsAndTechniques-Q2-2017.pdf, accessed September 2017.
[78] https://www.malwarebytes.com/pdf/white-papers/CybercrimeTacticsAndTechniques-Q2-2017.pdf, accessed September 2017.

3.1.5 Specific attack vectors

In the reporting period the prevailing attach vector for malware infections was phishing[79]. Phishing has been reported to be responsible for 90-95% of successful attacks worldwide. Through the use of obfuscation, phishing mails manage to evade end-point detection. Of particular interest (because very sophisticated) are CEO phishing mails/fraud. It is considered that the human link is still a weak link in the phishing infection vector. It is imperative to increase awareness measures to increase user vigilance.

Besides phishing, attempts continue to spread malware by using the common attack vectors like malvertising, spam emails, exploit kits, etc.

3.1.6 Specific mitigation actions

The mitigation actions for this threat include (in overview, detailed descriptions can be found here[80]):

- Reliance on only end-point or server malware detection and mitigation is not sufficient. Malware detection should be implemented for all inbound/outbound channels, including network, web and application systems in all used platforms (i.e. servers, network infrastructure, personal computers and mobile devices).
- Establishment of interfaces of malware detection functions with security incident management in order to establish efficient response capabilities.
- Use of available tools on malware analysis as well as sharing of malware information and malware mitigation (i.e. MISP[3]).
- Development of security policies that specify the processes followed in cases of infection. Involve all relevant roles, including executives, operations and end-users.
- Understanding of capabilities of various tools and development of solutions (e.g. multi-scanner/multichannel approaches to cover gaps.
- Regular update of malware mitigation controls and adaptation to new attack methods/vectors.
- Regular monitor of antivirus tests[81,82].

3.1.7 Kill Chain

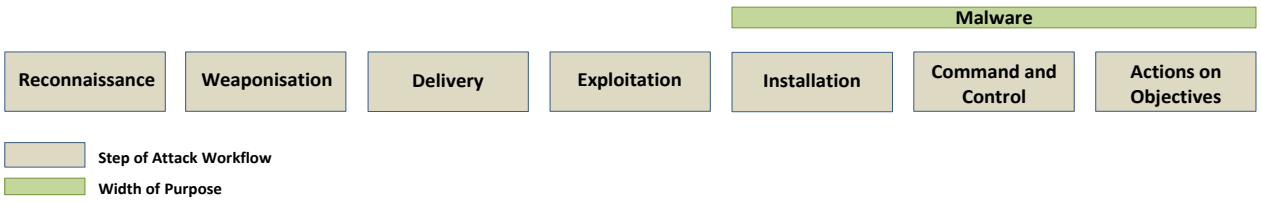

Figure 4: Position of Malware in the kill-chain

[79] https://www.infosecurity-magazine.com/news/phishing-remains-top-attack-vector/, accessed November 2017.
[80] https://zeltser.com/malware-in-the-enterprise/, accessed November 2017.
[81] https://www.av-test.org/en/, accessed November 2017.
[82] https://www.av-comparatives.org/dynamic-tests/, accessed November 2017.

3.1.8 Authoritative references

"Labs Threats Report June 2017", McAfee[83]; "IT threat evolution Q2 2017", Securelist[84]; "Internet Security Threat Report", Symantec[85]; "McAfee Labs Threat Report, September 2017", McAfee[86]; "Cybercrime tactics and techniques", Malwarebytes[87]; "Cisco 2017 Midyear Cybersecurity Report", Cisco[88].

[83] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf, accessed October 2017.
[84] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed October 2017.
[85] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf, accessed October 2017.
[86] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sept-2017.pdf, accessed September 2017.
[87] https://www.malwarebytes.com/pdf/white-papers/CybercrimeTacticsAndTechniques-Q2-2017.pdf, accessed October 2017.
[88] https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html, accessed October 2017.

3.2 Web-based attacks

3.2.1 Description of the cyberthreat

In the context of the present report, web based attacks are those that make use of web-enabled systems and services such as browsers (and their extensions), websites (including Content Management Systems), and the IT-components of web services and web applications. Examples of such attacks include web browser exploits (or their extensions), web servers and web services exploits, drive-by attacks, water-holing attacks, redirection and man-in-the-browser-attacks. This type of attack remained one of the most important threats in 2017[89] and is expected to stay so in the coming years, given the fact that web technologies and web components are of high importance in the digital world. Web-based attacks are very popular in combination with malware campaigns for infection, propagation or victims control purposes, banking malware being a relevant example in this sense[90]. Web-based-attacks have shown a substantial increase in 2017 and are about to reach levels similar to malware (in number of detected appearances).

3.2.2 Interesting points

The following interesting points have been identified:

- **Financial malware still relies on web-based attacks**. Most of the known financial malware (i.e. Zbot, Gameover Zeus, SpyEye, Ice IX, Citadel, Carberp, Bugat, and many others) use browser exploits, like the new arrival called Disdain[91]) and man-in-the-browser techniques.
- **First compromised browser extensions appear during the summer**. Several popular Chrome extensions (including the "Web Developer" extension – used by web developers and pen-testers) have been compromised. Attackers managed to "pawn" the author of the extensions probably through spear-phishing attacks. As most users tend to save credentials in the browser, experts warned affected users to change all credentials for web-services. The malware included in the "WebDeveloper" extension allowed the authors to load within the victim's browser java-script code served from a DGA Domain[92].
- **Popular messaging apps suffered web-based attacks to break encryption.** A couple of bugs were discovered[93] in both Telegram and WhatsApp that would allow an attacker to break the encryption used by both apps by compromising the device via web-based vectors.
- **Drive-by downloads relies on malicious JavaScript**. Two out of the top-ten most popular malware threats were malicious JavaScript[94], one major reason being that JavaScript malware can infect a computer without any interaction from the user (drive-by download attacks).
- **Web browser vulnerabilities still represent a big threat for users**. In a recent report[95] of the Google Zero Project it is shown that all well-known and used desktop browsers have associated security vulnerabilities, with Safari leading the top with 17 vulnerabilities and Chrome ending it with 2.

---

[89] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sept-2017.pdf, accessed October 2017.
[90] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed October 2017.
[91] https://www.intsights.com/blog/new-disdain-exploit-kit-may-signal-reemergence-of-the-popular-hacker-tool, accessed October 2017.
[92] https://www.proofpoint.com/us/threat-insight/post/threat-actor-goes-chrome-extension-hijacking-spree, accessed October 2017.
[93] https://blog.checkpoint.com/2017/03/15/check-point-discloses-vulnerability-whatsapp-telegram/, accessed October 2017.
[94] https://www.watchguard.com/wgrd-resource-center/security-report, accessed October 2017.
[95] https://googleprojectzero.blogspot.ro/2017/09/the-great-dom-fuzz-off-of-2017.html, accessed October 2017.

Moreover, at every bug bounty contest new vulnerabilities for browsers are discovered, which was the case also for Pwn2Own 2017 where Microsoft Edge was successfully exploited[96].

- **Water-holing attacks are on the rise**. More and more compromised websites are used to lunch water-holing attacks. Malware is downloaded in the websites visitor's machines without their knowledge, usually using exploit kits. Watering hole attacks in the early 2017 attempted to infect more than 100 organizations in 31 different countries[97], most of them being financial institutions. One of the biggest challenges emerging from this type of attack is that they are often difficult to investigate as they are very targeted. They are using different hopping points to select and infiltrate the victims. A common behaviour of such attacks is that users are infected or redirected to different landing sites only if they have a specific version of browser (or operating system), use an IP address assigned to a targeted organisation or are from a specific region.
- **Number of unique Malicious URL's is still very high**. According to reports[98], in Q2 of 2017 more than 33 million of unique malicious URL's responsible for spreading malware all over the globe were identified, with US (32%), Netherlands (20%), France (11%), Finland (10%) and Germany (8%) clearly on top countries when comes for hosting this kind of malicious resources.

3.2.3 Trends and main statistic numbers

- According to a 2017 survey[12], 48% of the faced threats entered the browser via web-based drive-by or download.
- 58% of malware distribution in manufacturing environments was via web-based downloads[99].
- Reports are saying that 79,209,775 unique URLs were recognized as malicious by web antivirus components in Q1[100] of 2017 and 33, 006, 783 in Q2[101] of 2017 (a significant drop).
- More than 50% of all cyber-attacks are targeting or rely on web-based technologies, while 38% of the attacks are using a browser of some sort with Adobe Flash and Oracle Java filling in till 50%.
- **The overall trend of web-based attacks in 2017 was INCREASING.**

[96] http://blog.trendmicro.com/pwn2own-2017-day-three-schedule-results/, accessed October 2017.
[97] https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0, accessed, October 2017.
[98] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed October 2017.
[99] https://www.nttcomsecurity.com/us/gtic-2017-q2-threat-intelligence-report/, accessed October 2017.
[100] https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/, accessed October 2017.
[101] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed October 2017.

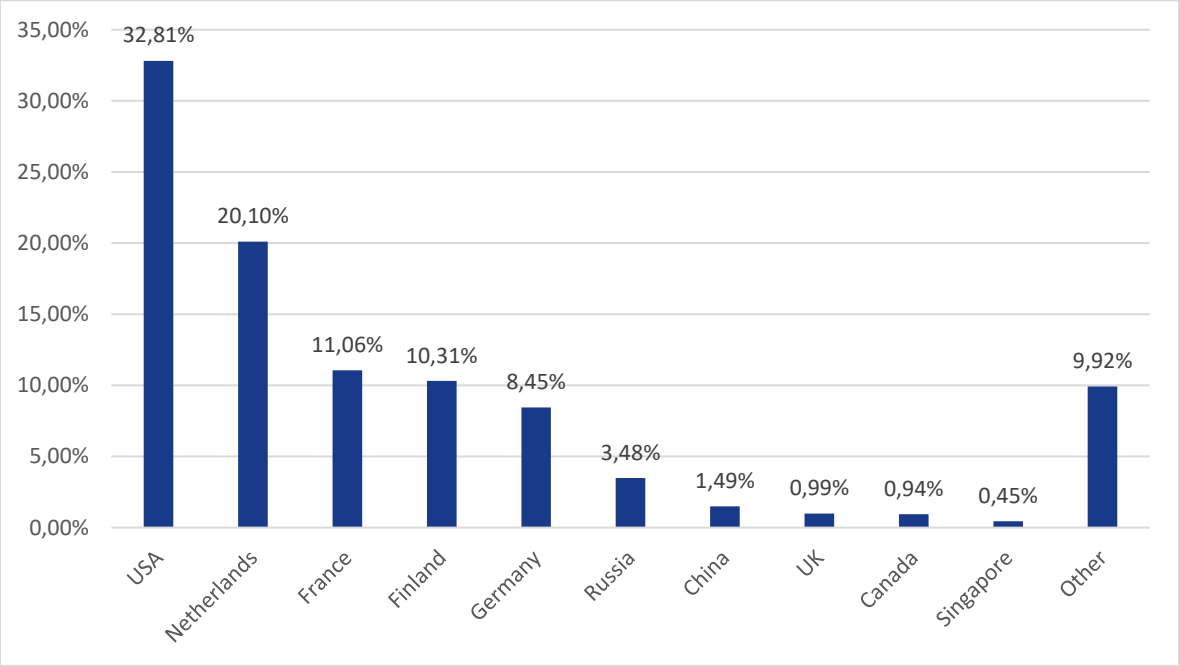

Figure 5: Distribution of web attack sources by country, Q2 2017[102]

3.2.4 Specific attack vectors

Browser exploits: are forms of malicious code that take advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach browser security to alter a user's browser settings without their knowledge. Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, Flash and other Web technologies and cause the browser to run arbitrary code.

Drive-by downloads: is a common method of spreading malware as cybercriminals look for insecure web sites to plant a malicious script into HTTP or PHP code on one of the pages. This script may install malware directly onto the computer of someone who visits the site, or it may take the form of an IFRAME that re-directs the victim to a site controlled by the cybercriminals. In many cases the script is obfuscated, to make it more difficult for security researchers to analyse the code. Such attacks are called 'drive-by downloads' because they require no action on the part of the victim — beyond simply visiting the compromised web site: they are infected automatically (and silently) if their computer is vulnerable.

Malicious URL's: are URL's created with malicious purposes, among them, to download any type of malware to the affected systems, which can be contained in spam or phishing messages, or even improve its position in search engines using Blackhat SEO techniques.

Water-holing: Is a malware attack in which the attacker observes the websites often visited by a victim or a particular group, and infects those sites with malware. A watering hole attack has the potential to infect the members of the targeted victim group through the use of specific configurations for the malware in order to be able to select the targets from the infected users (based on their IP for example).

A recent report[103] shows the top online threats associated with web-based attacks - malicious objects that are downloaded from a malicious/infected web page, in particular in the banking sector (see Figure 6).

[102] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed October 2017.
[103] https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/, accessed November 2017.

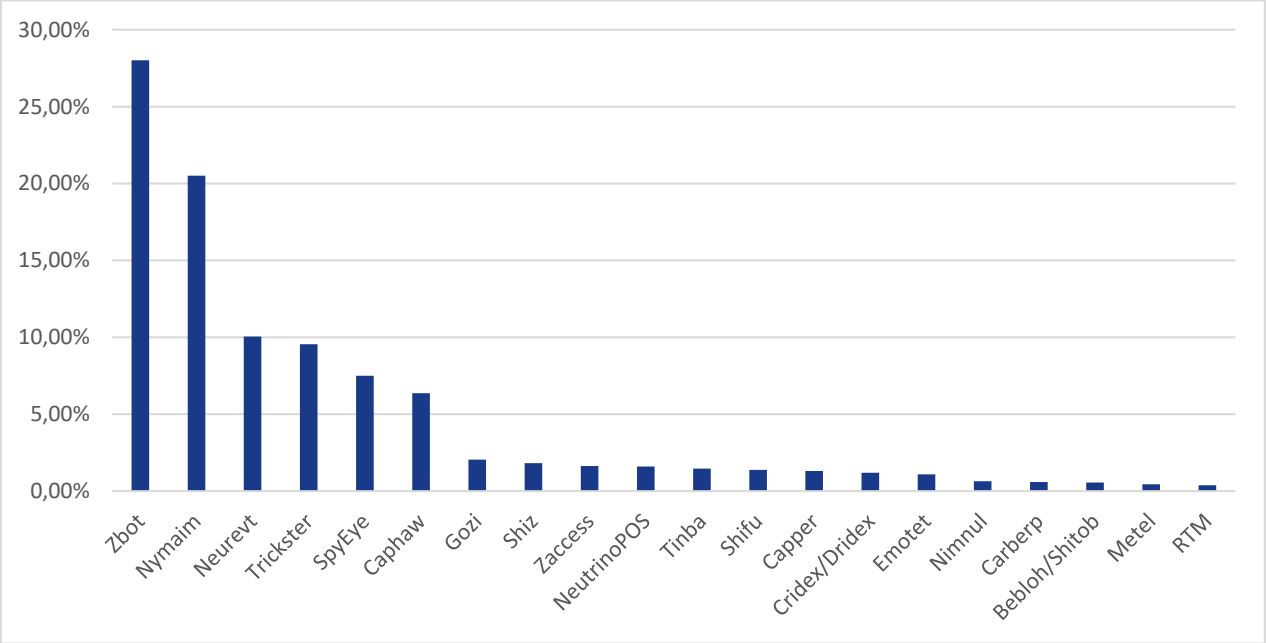

Figure 6: Top online threats in the banking sector

3.2.5 Specific mitigation vectors

The mitigation vector for this threat includes:

- Use of web browser protection mechanisms (sandboxing, antimalware extension) and changing default settings/configuration for a more secure utilisation (i.e. disabling unused features and extensions).
- Avoidance of utilisation of unnecessary browser plugins/extensions, in particular installation from untrusted sources.
- Web traffic filtering to detect and block malicious payloads and destinations (IP's, URL's).
- Utilisation of web traffic encryption technologies like SSL/TLS
- Regular updating/patching of web browsers and web server technologies and products
- Regular updating/patching of CMS based websites (like Wordpress or Joomla) and avoid the utilisation of third party plugins (usually responsible for most of the attacks against CMS's).
- Protection of end point from unpatched software containing known vulnerabilities.
- Avoidance of installation of malicious programs through potentially unwanted programs (PUPs).
- Monitoring of behaviour of software to detect malicious object, such as web browser plug-ins.
- Web address, web content, files and applications reputation solutions, blacklisting and filtering to establish risk-oriented categorization of web resources.
- Check application and web-browser settings in order to avoid unwanted behaviour based on default settings (esp. for mobile devices).

3.2.6 Kill Chain

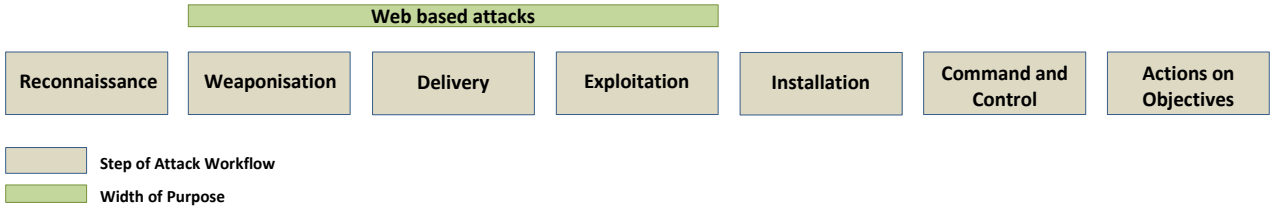

Figure 7: Position of Web based attacks in kill-chain

3.2.7 Authoritative references

"Threat Report September 2017", McAfee Labs[104]; "IT threat evolution Q1 2017. Statistics", Kaspersky Labs[105]; "IT threat evolution Q2 2017. Statistics", Kaspersky Labs[106]; "2017 Data Breach Investigations Report", 10th Edition, Verizon[107]

[104] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sept-2017.pdf, accessed October 2017.
[105] https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/, accessed October 2017.
[106] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed October 2017.
[107] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf, accessed October 2017.

3.3 Web application attacks

3.3.1 Description of the cyberthreat

Web application attacks are those attacks directed against available web applications, web services, and mobile apps. Such attacks try to abuse APIs that are incorporated in web applications. While not totally overlap free to the web-based attacks, these attacks take place within the scope of web application runtime environments and APIs. This type of attack is very popular, and is expected to stay so because most web apps and web services used are usually exposed and openly accessible. Web applications launched by government and financial organisations continue to represent tempting targets, just as they were in 2016. However, a slight drop in terms of the number of attacks has been assessed, compared to the number of attacks on web applications in 2016[108]. OWASP added this year two major additions to its top ten threats[109] that are relevant to this cyber threat. These are Insufficient Attack Protection and Under-protected APIs, including SOAP/XML, REST/JSON, RPC, GWT, and others. It is important to note that these APIs are often unprotected, and they contain numerous vulnerabilities. Attacks are targeting well-known resources and open-source or public-source based projects such as Wordpress plugins, Magento sites, etc. Their way of exploiting such resources are getting more efficient and once such a resource has a public vulnerability, scanners are build and deployed to scan and exploit them.

3.3.2 Interesting points

The following interesting points have been assessed for web application attacks:

- **SQL Injection is still an important threat for web applications**. Injection-type cyber-attacks (of which SQL Injection is one) are still the highest-ranked threat by the Open Web Application Security Project (OWASP). In the Top 10[110] OWASP lists API attacks are in the first position, while weak API protection ranks third.
- **Cross-site Scripting (XSS) on the rise**. XSS attacks grew 39% in Q1 of 2017 (the biggest jump since Q4 of 2015[111]), while XSS vulnerabilities are expected to grow 166% in 2017 (the biggest jump since 2012). Only in Q1 of 2017, the NIST database reported XSS vulnerabilities in certain versions of some of the top-tier software systems[112,113,114].
- **Content Management Systems vulnerabilities are still an important source of attacks**. The high adoption of CMSs for websites makes them very tempting for attackers as once a vulnerability discovered it can be used to attack a very large number of websites. News from February 2017 announced that WordPress (the most used CMS, with 70% of the market share) newly discovered vulnerability allowed hackers to infiltrate and vandalize around two million web sites[115]. A lot of CMS

[108] https://www.ptsecurity.com/upload/corporate/ww-en/analytics/WebApp-Attacks-2017-eng.pdf, accessed September 2017.
[109] http://sdtimes.com/owasp-adds-unprotected-apis-insufficient-attack-protection-top-ten-2017-release/, accessed October 2017.
[110] https://www.owasp.org/index.php/Top_10_2017-Top_10, accessed September 2017.
[111] https://snyk.io/blog/xss-attacks-the-next-wave/#high-profile-xss-vulnerabilities-are-not-a-thing-of-the-past, accessed September 2017.
[112] https://nvd.nist.gov/vuln/detail/CVE-2016-6037, accessed September 2017.
[113] https://nvd.nist.gov/vuln/detail/CVE-2017-8801, accessed September 2017.
[114] https://nvd.nist.gov/vuln/detail/CVE-2017-3008, accessed September 2017.
[115] http://www.cbronline.com/news/cybersecurity/breaches/wordpress-security-weak-spot-lets-hackers-infiltrate-and-vandalise/, accessed September 2017.

based websites are vulnerable due to the utilisation of vulnerable/outdated plugins/extensions like WP Statistics (WordPress plugin) found vulnerable to SQL Injection in June 2017[116].

- **The websites of government institutions and IT companies are still preferred targets[117]**, with an average number of 1,346 web-application-attacks in the IT sector, 1,184 in the government sector, 610 in the healthcare sector and 44 in education sector.

3.3.3 Trends and main statistic numbers

- Comparing Q1 of 2017 with Q4 of 2016, reports[118] mention 2% decrease in total web application attacks, 20% increase in attacks sourcing from the U.S. and 15% decrease in SQLi attacks;
- Q2 of 2017 saw an increase trend of web-app-attacks[119], with 5% increase in total web application attacks compared with Q1 of 2017, while SQLi attacks increased with 21%;
- 30% of total reported breaches involved attacks against web applications, while 93% of web application attacks were financially motivated and organized by criminal groups[120].
- A recent report[121] on web attacks measured 1.8 billion average daily attack volume, with 6,298 unique exploit detections, while 69% of firms saw severe attacks.
- **The overall trend of web application attacks in 2017 was INCREASING.**

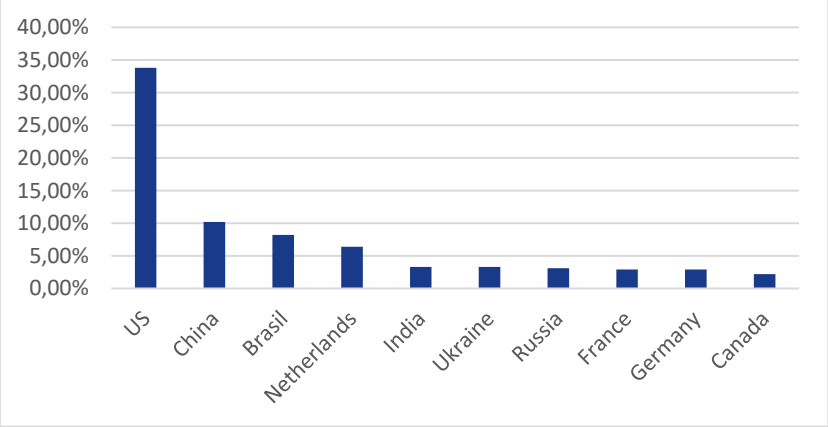

Figure 8: Top countries by source of attacks, Q2 of 2017[119]

3.3.4 Top web app attacks

As in previous years, the most prevalent web application attacks are SQL Injection (SQLi) attacks, Local File Inclusion (LFI), Cross-site Scripting (XSS), Remote File inclusion (RFI) and PHP injection (PHPi) or PHP Object Injection (for definitions of these attack types see[122]).

---

[116] https://blog.sucuri.net/2017/06/sql-injection-vulnerability-wp-statistics.html, accessed September 2017.
[117] http://blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html, accessed October 2017.
[118] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf, accessed October 2017.
[119] https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf, accessed October 2017.
[120] https://www.whitehatsec.com/resources-category/premium-content/web-application-stats-report-2017/, accessed October 2017.
[121] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Fortinet-Threat-Report-Q2-2017.pdf, accessed November 2017.
[122] https://www.acunetix.com/blog/articles/, accessed November 2017.

Assessed statistics for the use of each of these attacks can be found below.

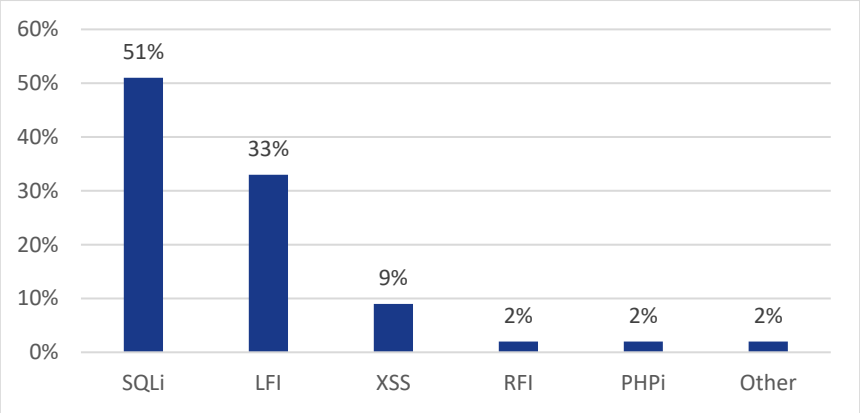

Figure 9: Web application attack vectors in Q2 2017[119]

3.3.5 Specific mitigation actions

The mitigation vector for this threat contains the following elements:

- Formulation of security policies for the development and operation of applications.
- Use of authentication and authorization mechanisms with a strength corresponding to the state-of-the-art.
- Installation of Web application firewalling (WAF)[123].
- Performance of traffic filtering to all relevant channels (web, network, mail).
- Performance of input verification.
- Deployment of bandwidth management[124].
- Perform regular web application vulnerability scanning and intrusion detection.
- Fix code vulnerabilities commonly found in production software earlier, during development.

3.3.6 Kill Chain

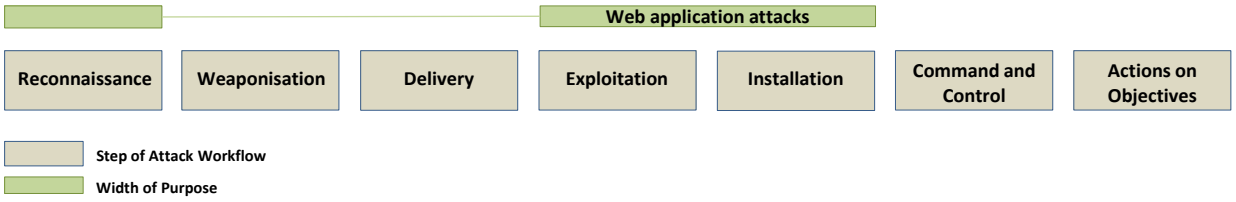

Figure 10: Position of Web application attacks in kill-chain

[123] http://www.darknet.org.uk/2015/11/modsecurity-open-source-web-application-firewall/, accessed November 2017.
[124] https://en.wikipedia.org/wiki/Bandwidth_management, accessed December 2017.

3.3.7 Authoritative references

"Web Application Attack Statistics: Q2 2017", Positive Technologies[125]; "State of the Internet / Security, Q1 2017 Report", Akamai[118]; "State of the Internet / Security, Q2 2017 Report", Akamai[119]; "2017 Application Security Statistics Report", WhiteHat Security[126]; "Threat Landscape Report Q2 2017", Fortinet[127]

[125] http://blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html, accessed October 2017.
[126] https://www.whitehatsec.com/resources-category/premium-content/web-application-stats-report-2017/, accessed October 2017.
[127] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Fortinet-Threat-Report-Q2-2017.pdf, accessed November 2017.

3.4 Phishing

3.4.1 Description of the cyberthreat

Phishing is a quite pervasive attack because it primarily uses social engineering to attack end users. Phishing is an important infection vector for all types of threat agents. It is becoming more and more sophisticated and targeted, which makes its detection increasingly difficult. A multilayer security approach has to be followed against phishing. Moreover, new solutions that involve machine learning should be considered in order to assist and enhance traditional security measures. According to recent reports[128,129,12] , in 2017, phishing campaigns have increased both in volume and sophistication. Phishing is highly used as the first step in cyber-attacks and is the most successful infection vector for data breaches and security incidents in both targeted and opportunistic attack tactics. In the reporting period the existence of phishing as a service[130] has been assessed. It is being used by cybercriminals and it utilizes full-fledged frameworks to perform phishing attacks. Phishing is related to most of the cyberthreats, e.g. botnets, malware, web based attacks, exploit kits, cyber-espionage, etc.

3.4.2 Interesting points

For phishing we have identified the following interesting points:

- **Targeted attacks[131]**. Originally, phishing attacks were being deployed through massive spam campaigns that indiscreetly targeted people. The goal was to trick a sufficient number of people to click on a malicious link or download a malicious attachment and ultimately harvest their credentials and install malware (or exfiltrate data) respectively. Nowadays, the goal remains the same but phishing attacks have become more targeted and sophisticated[132]. "Spear-phishing" is used to specifically target an individual or group of people. Spear-phishing is a phishing attack that is highly tailored to the target (usually based on all sorts of gathered public information, e.g. social media), which makes it difficult to determine its malicious nature. In a previous note[133] "Business e-mail compromise – BEC" was also described. This phishing technique (also known as "whaling"[134]) refers to spear-phishing attacks against C-level executives[135], usually with the aim to steal money from their organisations or to conduct cyber espionage. Spam and phishing are two cyber-threats that go hand in hand, while botnets[136] are usually employed to deliver them. It was recently reported[137] that there was an increase in targeted attacks where e-mails were masked as business correspondence. Spammers used details of real companies, e.g. e-mail subject message, logos, e-mail signatures etc., in order to impersonate them and "phish" their targets -reportedly[138] the B2B sector. Such targeted attacks usually aim to have financial gain; either by delivering ransomware (therefore asking for a ransom in order to decrypt valuable corporate

[128] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[129] https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf, accessed November 2017.
[130] https://www.netskope.com/blog/phishing-service-phishing-revamped/, accessed November 2017.
[131] https://www.enisa.europa.eu/publications/info-notes/phishing-on-the-rise, accessed November 2017.
[132] https://www.eff.org/deeplinks/2017/09/phish-future, accessed November 2017.
[133] https://www.enisa.europa.eu/publications/info-notes/how-to-avoid-losing-a-lot-of-money-to-ceo-fraud, accessed November 2017.
[134] https://www.insedia.com/articles/whales-guppies-when-a-company-s-top-bottom-1-are-equally-exposed, accessed November 2017.
[135] https://www.scmagazineuk.com/ceo-sacked-after-aircraft-company-grounded-by-whaling-attack/article/530984/, accessed November 2017.
[136] https://thehackernews.com/2017/10/peter-levashov-kelihos.html, accessed November 2017.
[137] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[138] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.

data), delivering spyware to steal financial information, or to compromise e-mail accounts of company employees[139] and perform various types of internal phishing and BEC[140] attacks. Moreover, such attacks have targeted industrial companies[141] from the metallurgy, electric power, construction, engineering and other sectors, in which cases the risk of unauthorised access and control of corporate networks and industrial equipment rises.

- **Phishing delivering malware**. As previously noted, phishing is widely used as the first step of a cyber-attack (initial infection vector) that aims to give an attacker a foothold on a target system. Phishing usually delivers a booby-trapped link or attachment (most often in the form of a document), which upon access/execution infects the target system with malware e.g. ransomware[142], banking Trojans, backdoors[143] etc. More precisely, a survey[12] showed that in 2017, 74% of the cyber-threats entered a system as an e-mail attachment or link.
- **Imposed urgency and compelling phishing attacks**. Phishing's success often relies on the sense of urgency it imposes to the victim. Phishing e-mails usually urge[144] the victim to take action upon something within a limited span, e.g. act upon an alleged data breach, act upon the delivery of a product, act upon a password expiration reminder etc. This phishing approach aims at the natural human tendency to take action, which might oversee the signs of abuse. Technology support scams[145] are similar attacks that aim to trick the users to download malicious software by using fake and deceiving system and error lookalike messages. Additionally, phishing attacks through malicious mobile applications that fake system pop-up notifications -in their effort to steal user credentials- are also considered[146] an upcoming threat. In one case[147] of a phishing attack, the threat actor sent fake notifications allegedly originating from software vendors, urging potential victims to update the respective software due to their systems being supposedly infected by WannaCry[148]. The link to the alleged update led to a phishing page hoping that victims would panic and access it. It is known that after major events, e.g. cyber-incidents, physical catastrophes, political/social events, etc., cyber criminals grasp the opportunity to initiate new spam and phishing campaigns. The sense of urgency imposed by phishing attacks is tied to quite compelling e-mails and fake websites that cleverly impersonate legitimate entities and third-party websites respectively. Often, these websites may look identical both content-wise and in terms of the domain name –which is found at the URL address bar of every browser. More precisely, phishers often use non-Latin characters[149] that look very similar to Latin letters but they can easily go unnoticed[150] to the untrained eye.

---

[139] http://blog.trendmicro.com/phishing-starts-inside/, accessed November 2017.
[140] https://securelist.com/nigerian-phishing-industrial-companies-under-attack/78565/, accessed November 2017.
[141] https://securelist.com/nigerian-phishing-industrial-companies-under-attack/78565/, accessed November 2017.
[142] https://www.darkreading.com/attacks-breaches/new-locky-ransomware-phishing-attacks-beat-machine-learning-tools/d/d-id/1330010, accessed November 2017.
[143] https://www.scmagazine.com/new-backdoor-targets-russian-businesses-in-apparent-spear-phishing-campaign/article/680268/, accessed November 2017.
[144] https://mediaserver.responsesource.com/press-release/85178/Q32017+Infographic.pdf, accessed November 2017.
[145] https://twitter.com/msftmmpc/status/918012087351283712, accessed November 2017.
[146] https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking, accessed November 2017.
[147] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[148] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst, accessed November 2017.
[149] https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers, accessed November 2017.
[150] https://gerryk.com/node/68, accessed November 2017.

- **Detection evasion**. In the past, spam campaigns used one or just a few phishing websites for the entire phishing campaign, which made it feasible for defenders to block the malicious domains. According to the data of a recent report[151], phishing campaigns rely on multiple and short-lived websites per campaign. This means that the life-cycle of a phishing campaign has become significantly smaller (in the magnitude of a few hours) and that traditional anti-phishing techniques, e.g. block lists, do not suffice against the ever-increasing number of malicious domains. In several instances, phishing e-mails were spotted[152] of being accompanied with password-protected archives as attachments. This tactic served a dual purpose. They created a false sense of security to the victims, implying that legitimate confidential data were exchanged and hence it was reasonable for the archives to be password-protected. Additionally, they evaded antivirus solutions since such files have to be extracted before they can be scanned by antivirus software. Phishers are always on the lookout for new techniques that will help them avoid detection. One more is the abuse of legitimate services.
- **Abuse of legitimate services**. Aside from direct e-mail phishing attacks, phishers leverage social media and legitimate websites too. Threat actors are in a constant research for ingenious ways of abuse/delivering phishing. As reported[153], "one of the phishers' tricks is to place pages of popular organizations on domains belonging to other popular organizations" in their effort to induce credibility to their phishing attacks. This makes the detection and mitigation even more difficult since legitimate sites are also used in the process. Threat actors mostly focus on involving popular websites in their phishing campaigns, hoping that they will have higher chances of success.

3.4.3 Trends and main statistic numbers

- According to recent data[154] "*an average of 1.385 million unique phishing sites are created each month with an astonishing high of 2.3 million in May of 2017*".
- The number of new phishing websites has increased dramatically, to an average of more than one million per month, making it impossible to block sites using static block lists[155], while the average lifecycle of a phishing website is now 4-8 hours, many with no inbound or outbound links, making web crawlers ineffective at finding such sites.
- In Q3 of 2017, the highest amount of phishing/spam has been detected in September: 59.56% of the entire mail traffic was spam. The average amount of spam total email traffic is ca. 58.02%. This is almost the same with previous quarter[156]. It is expected that spam and phishing will increase towards end of the year, as cyber-crime enters in the Christmas period.
- In a recent survey, 40% of respondents chose phishing, including spear phishing and whaling as the top threats with significant impact for the organizations[12].
- **The overall trend of phishing in 2017 was INCREASING.**

[151] https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf, accessed November 2017.
[152] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[153] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[154] https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf, accessed November 2017.
[155] https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf, accessed November 2017.
[156] https://securelist.com/spam-and-phishing-in-q3-2017/82901/, accessed November 2017.

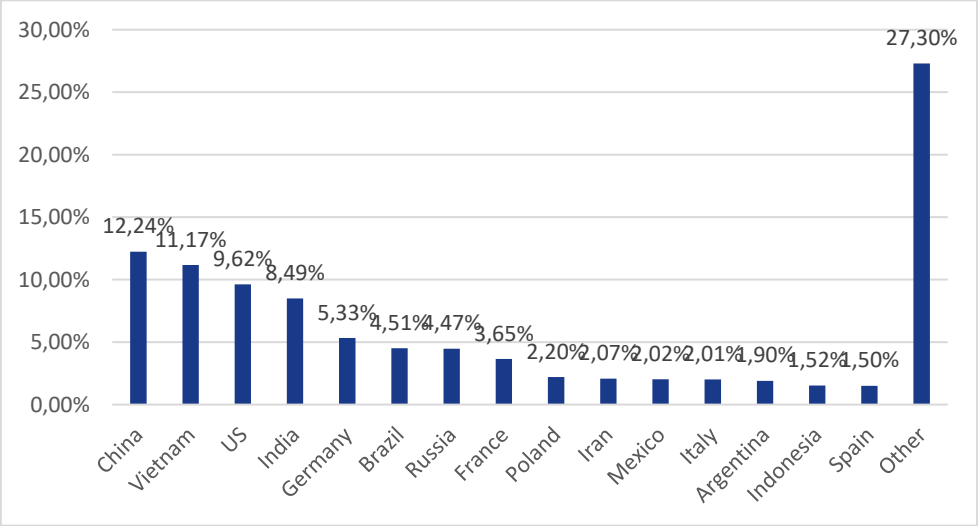

Figure 11: Top sources of spam by countries[157]

3.4.4 Top 10 Most-Clicked General Email Subject Lines[158]

- Official Data Breach Notification – 14%
- UPS Label Delivery 1ZBE312TNY00015011 – 12%
- IT Reminder: Your Password Expires in Less Than 24 Hours – 12%
- Change of Password Required Immediately – 10%
- Please Read Important from Human Resources – 10%
- All Employees: Update your Healthcare Info – 10%
- Revised Vacation & Sick Time Policy – 8%
- Quick company survey – 8%
- A Delivery Attempt was made – 8%
- Email Account Updates – 8%

3.4.5 Specific mitigation actions

- Organisations should educate their staff to identify fake and malicious e-mails and stay alerted. They should also internally launch simulated phishing attacks to test both their infrastructure and the responsiveness of their staff.
- Organisations should use specialised security e-mail gateways for filtering spam, which is heavily related to phishing campaigns.
- Do not click on links or download attachments if you are not absolutely confident about the source of an e-mail.
- Do not click on random links and especially short-links found in social media.

[157] https://securelist.com/spam-and-phishing-in-q3-2017/82901/, accessed November 2017.
[158] https://www.cybriant.com/2017/10/q3-2017-top-clicked-phishing-emails/, accessed December 2017.

- Avoid over-sharing personal information in social media, e.g. time of absence from office or home, flight information etc. as they are actively used by threat actors to collect information about their targets.
- Check the domain name of the websites you visit for typos, especially for sensitive websites, e.g. bank websites. Threat actors usually register fake domains that look similar to legitimate ones and use them to "phish" their targets. Looking only for an https connection is not enough.
- Do not click on "enable content" (which enables macros) in Microsoft Office documents. Macros are leveraged to download and install malware.
- Enable two factor authentication whenever applicable. Two factor-authentication can prevent account takeover.
- Use a strong and unique password for every online service. Re-using the same password in various services is a serious security issue and should be avoided at all times. Using strong and unique credentials in every online service limits the risk of a potential account takeover to the affected service only.
- In case of wiring money to an account, double check the bank information of the recipient through a different medium. Unencrypted and unsigned e-mails should not be trusted, especially for sensitive use-cases like these.
- Consider applying security solutions that use machine learning techniques[159] to identify phishing sites in real time.

3.4.6 Kill Chain

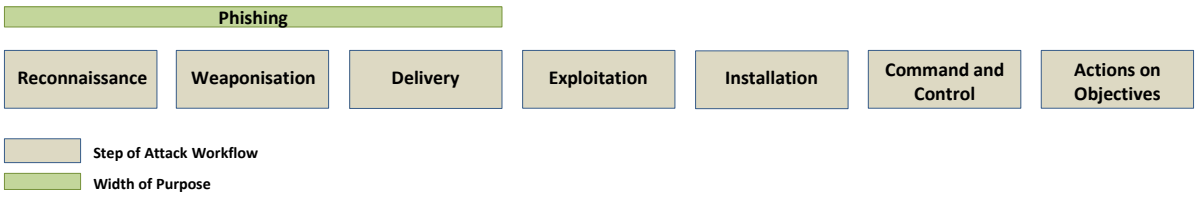

Figure 12: Position of phishing in the kill-chain

3.4.7 Authoritative references

"Phishing on the rise", ENISA[131]; "Spam and phishing in Q2 2017", Securelist[160]; "Spam and phishing in Q3 2017", Securelist[161]; "2017 Threat Landscape Survey: Users on the Front Line", SANS Survey[12].

[159] https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf, accessed November 2017.
[160] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[161] https://securelist.com/spam-and-phishing-in-q3-2017/82901/, accessed November 2017.

3.5 Spam

3.5.1 Description of the threat

Spam is one of the most prevalent and persistent cyber-threats, it dates back to the beginning of the Internet. Spam used to be and still remains the main means for malware delivery, through malicious attachments and malicious URLs. Spam accounts for more than half the volume of e-mails worldwide and is mainly distributed by large spam botnets. Most spam messages simply try to advertise products, typically in relation to healthcare or dating.

Although reduced in numbers, spam has gained in quality, e.g. by combining information to trick victims, and by using better obfuscation techniques to evade spam filtering. Despite spam reduction, spam messages still remain the most frequently used channel for cyber-criminals.

3.5.2 Interesting points

The following interesting points have been assessed:

- Last year, most of spam came from the Necurs botnet, which is currently considered the world's largest spam botnet[162]. However, in late December 2016, the network's activity almost completely ceased. As time showed, it was not just a temporary break as the volume of spam sent from this botnet remained at an extremely low level for almost the entire first half of 2017[163].
- In April 2017, the mastermind behind the Kelihos botnet was arrested in Spain. For many years Kelihos was responsible for millions of spam messages that carried banking malware and ransomware. The US Department of Justice acknowledged international cooperation between United States and foreign authorities, the Shadow Server Foundation, and industry vendors[164].
- A large Jaff ransomware wave came via spam the day before the WannaCry outbreak, and although it did not gain as much publicity, it continued for multiple days, affecting many users[165].
- At the start of Q2 2017, a wave of malicious mails imitating notifications from well-known delivery services was spotted, with Trojan downloaders sent out in ZIP archives[166].
- In Q2 2017, cyber criminals involved in spam distribution, tried to capitalize on public fears after the WannaCry ransomware outbreak struck in May[167].
- Threat agents started sending password-protected archives containing Microsoft Word or Excel documents with macros or JavaScript scripts embedded. This technique allowed them to bypass e-mail spam filters or other defensive measures in place.
- Several malware families discovered in July 2017 had added functionality that allowed them to send out spam, containing copies of themselves[168].

---

[162] https://securelist.com/spam-and-phishing-in-q1-2017/78221/, accessed November 2017.
[163] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[164] https://www.mcafee.com/mx/resources/reports/rp-quarterly-threats-jun-2017.pdf, accessed November 2017.
[165] https://www.malwarebytes.com/pdf/white-papers/CybercrimeTacticsAndTechniques-Q2-2017.pdf, accessed November 2017.
[166] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[167] https://www.kaspersky.com/about/press-releases/2017_snake-oil-in-q2-spammers-cashed-in-on-wannacry-epidemics, accessed November 2017.
[168] https://www.symantec.com/connect/blogs/latest-intelligence-july-2017, accessed November 2017.

- According to Spamhaus[169], up to 80% of spam is generated by a hard-core group of around 100 known persistent spam gangs whose names, aliases and operations are documented in Spamhaus' "Register Of Known Spam Operations (ROKSO)" database.
- A popular price comparison site was fined £80,000 (US$104,000) in July for spamming more than 7 million of its customers after they had specifically requested not to receive direct marketing emails from the company[170].
- Attackers are starting to use real companies and real people in their spams (impostor e-mail), trying to better reach their targets. They tend to use messages related to courier services, e-store notifications, etc.
- Spam started to evolve by moving from e-mail to social networks. By leveraging social networks to distribute their message, be it malicious or not, spammers manage to bypass e-mail service's filters, gaining a wider reach.

3.5.3 Trends and main statistic numbers

- In Q4 of 2017, the average daily spam volume was around 454 billion, representing around 85% of the total daily email volume[171].
- In Q1 2017, the percentage of spam in e-mail traffic amounted to 55.9%[172].
- Overall, in the second quarter of 2017, the percentage of spam in e-mail traffic grew slightly from the previous quarter. The number of e-mail antivirus detections increased by 17% in Q2 in comparison to Q1[173].
- The global spam rate for July 2017 was the highest seen since March 2015, increasing by 0.6% and reaching 54.9%[174].
- A massive spambot uncovered during August was found to contain approximately 711 million e-mail addresses while distributing variants of the Snifula family of information stealing Trojans[175].
- Spam statistics[176] shows that 88% of all spam is sent from botnets, with 91% of spam containing some form of URL, while 66% of all spam being related to pharmaceutical products.
- **The overall trend of spam in 2017 was INCREASING.**

[169] https://www.spamhaus.org/statistics/spammers/, accessed November 2017.
[170] https://www.symantec.com/connect/blogs/latest-intelligence-july-2017, accessed November 2017.
[171] https://www.talosintelligence.com/reputation_center/email_rep#global-volume, accessed November 2017.
[172] https://securelist.com/spam-and-phishing-in-q1-2017/78221/, accessed November 2017.
[173] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[174] https://www.symantec.com/connect/blogs/latest-intelligence-july-2017, accessed November 2017.
[175] https://www.symantec.com/connect/blogs/latest-intelligence-august-2017, November 2017.
[176] https://antispamengine.com/spam-statistics/, accessed November 2017.

3.5.4 Top Spam sources

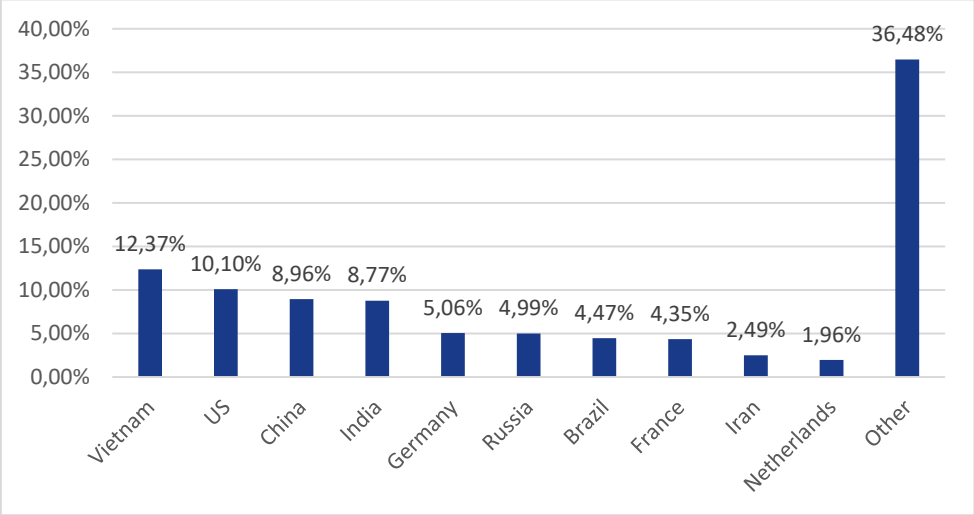

Figure 13: Top 10 Spam sources by country[177]

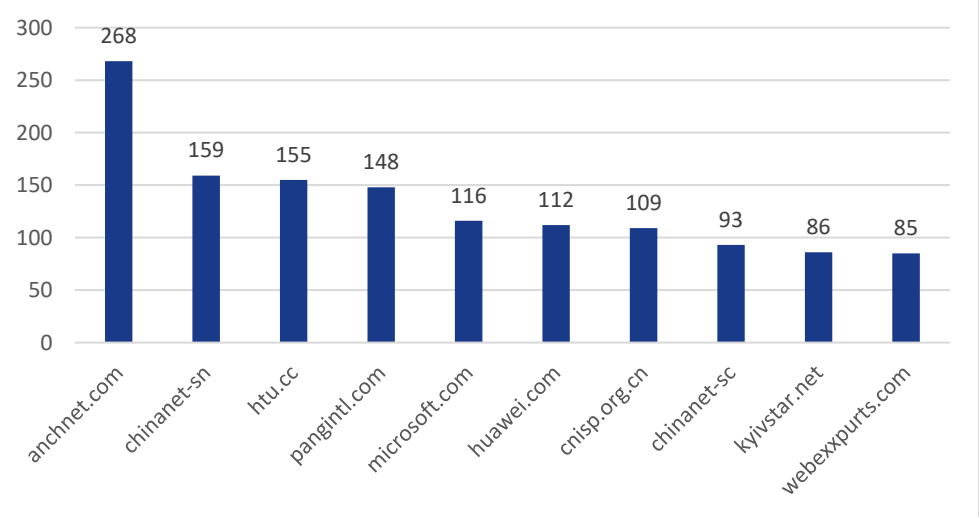

Figure 14: Top 10 Spam sources by ISPs[178]

3.5.5 Specific mitigation actions

The mitigation measures for spam and spam-based threats are the following:

- DKIM (Domain Keys Identified Mail), reputation filters, content filters, RBL and other measures have been successfully used in the past.
- Use of AI and specifically machine learning and anomaly detection techniques.
- Block of executables (and macros) found in mail attachments.

[177] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[178] https://www.spamhaus.org/statistics/networks/, accessed November 2017.

- Disable automatic execution of code, macros, rendering of graphics and preloading mailed links at the mail clients and update them frequently.
- Educate the users, e.g. to ask themselves, e.g. if they know the sender, if they feel comfortable with the attachment content and type, if they recognize the subject matter of the mail, etc.
- The most important threat (impostor e-mail) is still the most difficult to identify and mitigate as it does not rely on technical means but rather on social-engineering, and the abuse of the inherent trust in a known e-mail partner. Therefore, user awareness and training is the first step in fighting it. In that respect, there are training services that mimic tactics used by malicious actors. Such trainings aim to identify individuals that might fall for them and essentially educate them on how to recognise and counter similar attacks.

3.5.6 Kill Chain

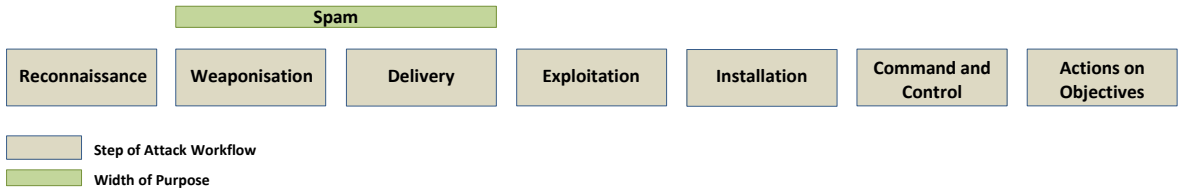

Figure 15: Position of Spam in the kill-chain

3.5.7 Authoritative references

"Spam and phishing in Q1 2017", SecureList[179]; "Spam and phishing in Q2 2017", SecureList[180]; "Latest Intelligence for July 2017", Symantec[181]; "Latest Intelligence for August 2017", Symantec[182]

[179] https://securelist.com/spam-and-phishing-in-q1-2017/78221/, accessed November 2017.
[180] https://securelist.com/spam-and-phishing-in-q2-2017/81537/, accessed November 2017.
[181] https://www.symantec.com/connect/blogs/latest-intelligence-july-2017, accessed November 2017.
[182] https://www.symantec.com/connect/blogs/latest-intelligence-august-2017, accessed November 2017.

3.6 Denial of Service

3.6.1 Description of the threat

Denial of Service (DoS) attacks, and especially the distributed ones (DDoS) remained an important threat for almost all kind of businesses with an online presence. The Mirai IoT botnet kept the headlines[183] in Q4 of last year, being responsible for the largest DDoS attacks in history in terms of bandwidth (over 1 Tbps) and exemplifying the expert's warnings about the impact of improperly secured IoT devise to the Internet health. It was the trigger for everyone to tackle seriously the problem, starting with IoT vendors that looked for improving security of the devices, continuing with sustained efforts form the cyber security community to patch compromised IoT devices and also seeing an intensified activity on the Law Enforcement side that led to some arrests[184]. Those efforts led to an overall reduction in volumetric DDoS attacks, but also a significant increase in the amount of traffic in reflection attacks was seen in late 2016 and Q1 of 2017, with a new reflection source[118] (CLDAP5) being added recently in the landscape which can have an multiplication factor of 70. The majority of attacks are still small relative to the largest Mirai attacks, but the number of attacks increased and in fact they don't need to be big to be effective. If we consider that many businesses lease uplinks to the Internet in the range of 1–10 Gbps, any attack exceeding 10 Gbps could be "big enough" and more than capable of taking the average unprotected business offline. In Q1 and Q2 of 2017, volumetric attacks accounted for roughly 99% of the overall attack traffic most likely because it's trivial for an attacker to launch a volumetric attack in comparison to the technical understanding needed to make effective use of application layer tools. In terms of predictions for 2017 and the following period, reports[185] are talking about the rise of Permanent Denial of Service (PDoS) for Data Center and IoT Operations, increased importance and sophistication of Telephony DoS (TDoS) attacks, and the rise of more segmented (and even personal) denial of service attacks combined with cyber-ransom (Ransom-DoS), with health systems being seen as a possible target. In fact, WannaCry and Petya outbreaks in Q2 of 2017 represented examples of how Ransomware and Denial of Service attacks can be combined.

3.6.2 Interesting points

The following interesting points have been identified:

- **DDoS attacks are on the rise**. According to research[186], over a third (33%) of organizations faced a DDoS attack in 2017, compared to just 17 % in 2016, a trend that shows a very rapid development in the cyber threat landscape which means that all businesses, regardless of size, are at risk of experiencing a DDoS attack.
- **"Pulse wave" DDoS attacks**. Instead of using a DDoS botnet to direct a sustained stream of denial of service traffic at a single target, some attackers are now using their attack infrastructure to direct short bursts of traffic at multiple targets - an assault dubbed pulse wave attacks[187]. In the most extreme cases, they lasted for days at a time and scaled as high as 350 Gbps.

[183] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet, accessed October 2017.
[184] https://threatpost.com/hacker-admits-to-mirai-attack-against-deutsche-telekom/127001/, accessed October 2017.
[185] https://security.radware.com/ddos-experts-insider/ddos-practices-guidelines/cyber-security-predictions-2017/, accessed October 2017.
[186] https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizations-continues-to-climb, accessed October 2017.
[187] https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html, accessed October 2017.

- **Multi-Vector DDoS Attacks Remain the Norm**. According to reports[188], 74% of DDoS attacks in Q2 of 2017 utilized at least two different attack types. For example, the Mirai botnet has the ability to launch multiple TCP and UDP flood attack types in addition to Layer 7 attacks.
- **DDoS-for-hire services are gaining traction**. While they are marketed as stressors – sites that stress-test legitimate targets, in fact some of these services don't actually validate that the request is made with the consent of the owner of the said target. One of these services was closely investigated by the known journalist Brian Krebs in January 2017[189] who's website was hit in late 2016 by one of the biggest DDoS attacks in terms of bandwidth.
- **DDoS as-a-service costs are getting lower**. The fact that Mirai's botnet source code has become publicly available didn't help much, lowering the threshold for obtaining a botnet even more. As an interesting development, some authors even attempted to calculate the costs of an one hour DDoS attack using resources form a cloud service provider and the conclusion was that the attacks can be made with no more than 4 US Dollars[190]. Some operators located in China offer such services using copy-cat websites that even include dashboards showing the number of attacks carried out and the number of online bots[191].
- **Bandwidth implicated in attacks is smaller than before but more efficiently used**. If in 2015 the most aggressive attack used in the ballpark of 500 Gbps[192], at the end of the previous year the attacks against OVH[193] topped 1Tbps and the Mirai botnet attack against Brian Krebs[194] site topped at 620 Gbps. This year the attacks tend to last less than an hour but they occurred in bursts[195], and this puts a supplementary strain on the technical personal of the affected entity.
- **The rise of DNS-based DDoS attacks**. After last year's well mediatized Dyn attacks[196], DDoS attacks continued to target DNS systems in 2017 when big media websites in France went down[197] due to such attacks.
- **The rise of extortion attempts under threat of DDoS (ransom DDoS)**. Armanda Collective[198] demanded 315.000 from seven South Korean banks in exchange for not disrupting their online service. This trend also worried Law Enforcement Agencies and they began to prosecute offenders more seriously as it happened in Great Britain[199]. The pay-out for such attacks vary from 5 to 200 bitcoins.

---

[188] https://www.verisign.com/assets/report-ddos-trends-Q22017.pdf, accessed October 2017.
[189] https://krebsonsecurity.com/tag/ddos-for-hire/, accessed October 2017.
[190] https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/, accessed October 2017.
[191] http://blog.talosintelligence.com/2017/08/chinese-online-ddos-platforms.html, accessed October 2017.
[192] https://www.abusix.com/blog/5-biggest-ddos-attacks-of-the-past-decade, accessed October 2017.
[193] https://amp.thehackernews.com/thn/2016/09/ddos-attack-iot.html, accessed October 2017.
[194] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, accessed October 2017.
[195] https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html, accessed October 2017.
[196] https://blogs.akamai.com/2016/10/dyn-ddos-attack-wide-spread-impact-across-the-financial-services-industry-part-1.html, accessed October 2017.
[197] https://www.bloomberg.com/news/articles/2017-05-10/french-websites-knocked-offline-in-cyber-attack-on-cedexis, accessed October 2017.
[198] https://www.bleepingcomputer.com/news/security/-1-million-ransomware-payment-has-spurred-new-ddos-for-bitcoin-attacks/, accessed October 2017.
[199] https://www.theregister.co.uk/2017/04/25/british_malware_author_2_years_jail_titanium_stresser/, accessed October 2017.

- **Bitcoin exchanges under fire**. According to reports[200], a new trend can be seen in outages affecting bitcoin exchanges and marketplaces starting with June 2017. This type of attacks seems correlated with currency value fluctuations and have exponentially grown due to the rise in value of bitcoin – hitting an all-time high of $2,995 USD on June 11, 2017.
- **DDoS are sometimes used to cover up other types of attacks[201]**. According to a research, in the first half of 2017, 53% of entities affected by a DDoS attack claimed that it was used as a smokescreen to hide other types of attacks: malware infection (50%), data leak or theft (49, network intrusion or hacking (42%), or financial theft (26%).

3.6.3 Trends and main statistic numbers

- For the first time in recent years, in Q2 of 2017 no large attacks exceeding 100 Gbps were observed[119], with PBot (a botnet based on decades-old PHP code) being responsible for the biggest attack seen in that period (75 Gbps).
- China is the top attacking country with more than 60%[202] (in 2016 according to Kaspersky labs the percent was 71.60) while United States is the top target with well over 90% of the targets[203].
- Most of the DDoS botnet C&C servers continue to be located mostly in South Korea[204] - 66.5% in Q1 of 2017, compared with 59% in 2016.
- Another important trend shift has been the comeback of Windows based DDoS bots from 25% to almost 60 %, mostly due to Yoyo, Drive and Nitol bots[204].
- Reflection attacks continued to comprise most DDoS attack vectors and accounted for 57% of all mitigated attacks. Of all DDoS reflection attacks in Q2 of 2017, 33% used DNS reflectors attacks, 28% used NTP reflectors, 17% used CHARGEN reflectors, and 12% used SSDP reflectors. Overall reflector count across all vectors is lower than at the same time last year.
- The most targeted industry seems to be the gaming industry with more than 80 % of the volume of traffic[205]. Of note are attacks against financial and banking sectors in Central Europe and Nordic countries and also against Gulf States Energy, Transportation and Media sectors.
- In terms of types of businesses affected by DDoS attacks, 20% were very small businesses, 33% were SMBs and 41% percent were enterprises, proving again that all types of organizations are exposed to this risk[206].
- **The overall trend of denial of service attacks in 2017 was INCREASING.**

[200] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/cryptocurrencies-trade-under-fire/, accessed October 2017.
[201] https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizations-continues-to-climb, accessed October 2017.
[202] https://securelist.com/ddos-attacks-in-q3-2017/83041/, accessed November 2017.
[203] https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html, accessed October 2017.
[204] https://securelist.com/ddos-attacks-in-q1-2017/78285/, accessed October 2017.
[205] https://www.cyberscoop.com/akamai-ddos-q2-2017/, accessed October 2017.
[206] https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizations-continues-to-climb, accessed October 2017.

3.6.4 Top 5 most dangerous DDoS attacks

An important resource that describes top 5most salient types of DDoS attacks (techniques) mentions the following[207]:

- **Advanced Persistent DoS (APDoS)**. This type of attack is characterized by persistence over extended periods of time, explicit motivation, and by a combination of massive network layer DDoS attacks, focused application layer (HTTP) floods, repeated application layer attacks (SQLI, XSS).
- **DNS Water Torture Attacks**. Targets organisation's DNS servers and involves a flood of maliciously crafted, DNS lookup requests. The potential impact of this attack was suddenly realized when Mirai botnet was used to launch its own DNS query flood.
- **SSL-Based Cyber Attacks**. SSL-based DDoS attacks take many forms and usually are similar with standard ones, only they further complicate the challenge by encrypting traffic and forcing exhausting of resources do to encryption and decryption processes.
- **Permanent Denial of Service (PDoS)**. A permanent denial-of-service (PDoS) attack is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of the system (e.g. BrickerBot[208])
- **IoT Botnets**. Botnets are one of the fastest growing and fluid threats facing cyber security experts today and introduced the 1Tbps DDoS era.

3.6.5 Specific attack vectors

According to reports on Q1[118] and Q2[119] of 2017, the top four infrastructure DDoS related attacks were the same in the beginning of 2017 as in 2016: UDP fragments, DNS floods, NTP floods, and CHARGEN attacks dominated, as shown in Figure below.

Other statistics on DoS attack type by protocol in Q2 2017[209] shows that attacks using UDP and TCP protocols have increased, but attacks using HTTP protocol have decreased by 13x, compared with the same quarter of 2016.

[207] https://blog.radware.com/security/2017/09/2017-5-most-dangerous-ddos-attacks/, accessed October 2017.
[208] https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/, accessed October 2017.
[209] https://www.cdnetworks.com/sg/resources/CDNetworks_DDoS%20Attack%20Trends_Q2%202017_ENG_final_20170821-2-.pdf, accessed October 2017.

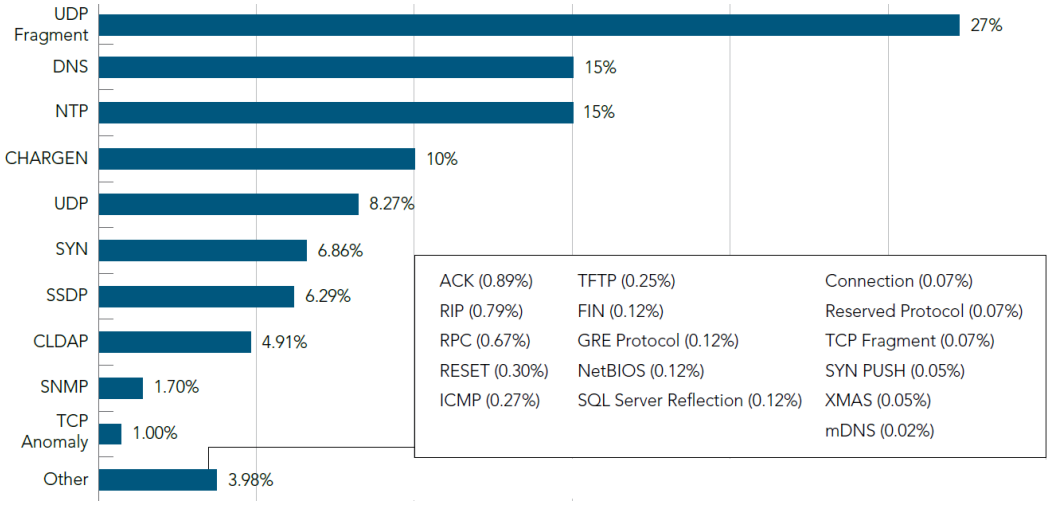

Figure 16: DDoS Attack Vector Frequency, Q2 2017[119]

3.6.6 Specific mitigation actions

The mitigation vector for this threat contains (detailed list can be found here[210]):

- Creation of a DoS/DDoS security policy including a reaction plan to detected incidents.
- Use of ISPs who implement DDoS protection measures[211].
- Consideration of using a managed solution for DDoS protection.
- Selection of a technical DoS/DDoS protection approach (e.g. Firewall based, Access Control Lists (ACLs), Load-balancer, IPS/WAF, Intelligent DDoS mitigation systems (IDMS) at network perimeter, Cloud-based DDoS mitigation service[212Error! Bookmark not defined.], etc.)[213].
- Assessment and documentation of roles of all third parties involved in the implemented protection DoS/DDoS approach. Regular test of reaction time and efficiency of involved roles.
- Establishment of interfaces of implemented solution with company operations to collect and process information from DoS/DDoS protection and incidents.
- Development of preparedness for identifying attacks that happen under the cover of DDoS. An intrusion prevention system (IPS) is the basis for the identification of other intrusion attempts.

[210] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/iot-devices-threat-spreading/, accessed October 2017.
[211] http://security.stackexchange.com/questions/134767/how-can-isps-handle-ddos-attacks, accessed November 2017.
[212] https://geekflare.com/ddos-protection-service/, accessed November 2017.
[213] https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf, accessed November 2017.

3.6.7 Kill Chain

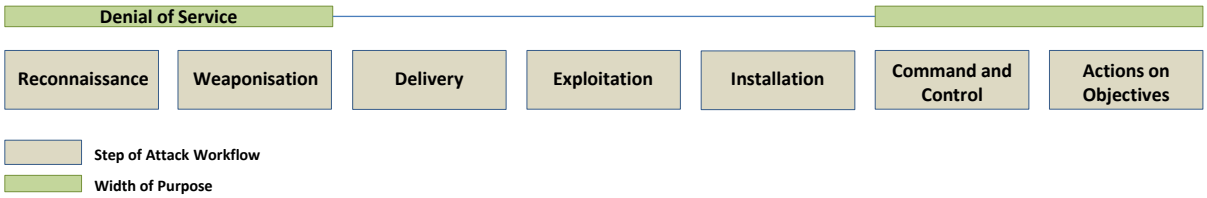

Figure 17: Position of Denial of Service in the kill-chain

3.6.8 Authoritative references

"State of the Internet / Security, Q1 2017 Report", Akamai[118]; "State of the Internet / Security, Q2 2017 Report", Akamai[119]; "Global DDoS Threat Landscape Q1 2017", Imperva[214]; "2017's 5 Most Dangerous DDoS Attacks & How to Mitigate Them", Radware[215].

[214] https://www.incapsula.com/collateral/2017-q2-ddos-threat-landscape.pdf, accessed October 2017.
[215] https://blog.radware.com/security/2017/09/2017-5-most-dangerous-ddos-attacks/, accessed October 2017.

3.7 Ransomware

3.7.1 Description of the threat

Over the last years, ransomware remained a prominent threat. Ransomware hit the headlines multiple times and for good reason; its profitability not only remained high, but kept growing. While traditional malware such as banking Trojans, spyware, and keyloggers require cybercriminals to go through multiple steps before making profit, ransomware make it a seamless and automated process. Moreover, low capability threat agents e.g. script kiddies, can easily jump into this "business" by using ransomware frameworks through what is known as "Ransomware as a Service" (RaaS), which make digital theft easy. If a company suffered an infection during Q1 2017 regardless of whether it was via a spam email or an exploit kit, it is more likely to have been caused by ransomware than any other malware. More precisely, roughly 60%[216] of malware payloads were ransomware, with the rest being a mix of ad fraud malware and other types of malware.

3.7.2 Interesting points

The identified interesting points for ransomware are as follows:

- **The growth of targeted attacks**. In early 2017, researchers assessed a trend towards more targeted attacks against businesses[217]. On the contrary, massive attacks to users seem to be of lower priority. The attacks primarily focused on financial organisations worldwide while experts encountered cases where payment demands amounted to over half a million dollars. This trend is alarming as ransomware actors orchestrate their attacks against new and potentially more profitable targets.
- **The rise of ransomware-as-a-service**. In Q1 of 2017, as a result of several attacks powered by ransomware-as-a-service, ransomware incidents started to grow again after a few months of decline[218]. A representative example is "Philadelphia"[219], a ransomware released and maintained by a group called "The Rainmaker Labs", currently sold for $389 on the Darknet.
- **Ransomware is targeting server technologies[220]**. Ransom attacks against MongoDB databases are a continuation of the so-called MongoDB Apocalypse that started in late December 2016 and continued until the first months of 2017[221]. During those attacks, multiple threat agents scanned the Internet for exposed and unprotected MongoDB databases, wiped their content, and replaced it with a ransom demand. Most of these exposed databases were test systems, but some contained production data and a few companies ended up paying the ransom; only to later find out they had been scammed and attackers never had their data. Ransom attacks also spread to other server technologies, such as ElasticSearch, Hadoop, CouchDB, Cassandra, and MySQL servers.

---

[216] https://www.malwarebytes.com/pdf/labs/Cybercrime-Tactics-and-Techniques-Q1-2017.pdf, accessed September 2017.
[217] https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-ransomware-actors-focusing-on-targeted-attacks-against-businesses, accessed December 2017.
[218] https://blogs.technet.microsoft.com/mmpc/2017/09/06/ransomware-1h-2017-review-global-outbreaks-reinforce-the-value-of-security-hygiene/, accessed September 2017.
[219] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/RaaS-Philadelphia.pdf, accessed September 2017.
[220] https://www.enisa.europa.eu/publications/info-notes/ransom-attacks-against-unprotected-internet-exposed-databases
[221] http://www.securitynewspaper.com/2017/09/04/massive-wave-mongodb-ransom-attacks-makes-26000-new-victims/, accessed December 2017.

- **The rise of ransomware impostors and media impact**. WannaCry and NotPetya, the last two high-profile ransomware outbreaks, failed to earn money but showcased a worrying destructive potential. Experts[222] concluded that they were never meant to decrypt files and should be classified as "wipeware". Nevertheless, their media impact was inversely proportional with their profit. News kept rolling on media channels and hit headlines for several days. Especially, due to the high profile victims (Ukraine, Maersk, etc.).
- **The increase in sophistication**. In May 2016, security researchers discovered Petya[223] ransomware. Petya not only encrypts data stored on a computer, but also overwrites the hard disk's master boot record (MBR), making infected computers unable to boot into the operating system. In June 2017, a modified version of Petya, called NotPetya, was identified. NotPetya used multiple spreading techniques: the update mechanism of a legitimate third-party Ukrainian software product called M.e.Doc, a modified version of the EternalBlue exploit that was also used by WannaCry one month earlier[224], local network propagation techniques using built-in Microsoft tools (WMI and PSEXEC), and credential capturing using custom tools similar to Mimikatz[225]. One of the most important aspects about WannaCry and NotPetya is that, unlike traditional ransomware, they used leaked exploits (supposedly being developed by the US intelligence agency[226]) as attack vectors. WannaCry and NotPetya are examples of high-profile, global-scale, and potentially government-sponsored attacks that aimed at creating chaos.
- **Mobile Ransomware Increased in 2017[227].** Last year, it was the year of ransomware and no signs of decline were observed. Moreover, the volume of mobile ransomware grew 3.5 times during the first few months of the year. The number of mobile ransomware files detected reached 218,625 during Q1 of 2017. Additionally, ransomware targeting all types of devices or systems continued to grow, and 11 new families made their appearance in Q1 of 2017. Finally, the United States was the country that was mostly impacted by mobile ransomware in Q1 of 2017, while the most widespread ransomware threat was Svpeng.
- **Ransomed medical devices: a new threat.** Integration between IT and operational technology (OT) is a trend seen in our increasingly interconnected world, including the healthcare sector[228]. Threat researchers warn that targeting medical devices with ransomware and other malware is only going to rise in the future. They called this attack vector "MEDJACK", or "medical device hijack." The potential damage is clear if we consider that the average small to midsize hospital with five or six operational units has between 12,000 and 15,000 devices that can be potentially compromised.

3.7.3 Trends and main statistic numbers[229]

- 6 in 10 malware payloads were ransomware in Q1 2017

---

[222] Study on "Tracking Ransomware End to End" presented at Black Hat USA 2017 conference by researchers of Google, UC San Diego, New York University (NYU), and the blockchain analysis firm Chainalysis.
[223] https://www.kaspersky.com/about/press-releases/2017_petrwrap-criminals-steal-ransomware-code-from-their-peers, accessed September 2017.
[224] https://securelist.com/schroedingers-petya/78870/, accessed September 2017.
[225] https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/, accessed September 2017.
[226] https://www.symantec.com/connect/blogs/equation-has-secretive-cyberespionage-group-been-breached, accessed September 2017.
[227] https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-reports-mobile-ransomware-dramatically-increased-in-q1-2017, accessed September 2017.
[228] http://www.networkiq.co.uk/ransomware-medical-devices-medjack/, accessed December 2017.
[229] https://blog.barkly.com/ransomware-statistics-2017, accessed September 2017.

- There were 4.3 times more new ransomware variants in Q1 2017 compared to Q1 2016
- 15% or more, of businesses in the top 10 industry sectors have been attacked by ransomware
- 71% of the companies targeted by ransomware attacks, have been infected by ransomware
- Phishing emails carrying ransomware dropped nearly 50% in Q1 2017
- Two thirds of ransomware infections in Q1 2017 were delivered via RDP
- The average ransom demand has risen to $1,077
- 1 in 5 businesses that paid the ransom never got their files back
- 72% of infected businesses lost access to data for two days or more
- Global ransomware damages are predicted to exceed $5 billion in 2017
- **The overall trend of ransomware in 2017 was INCREASING.**

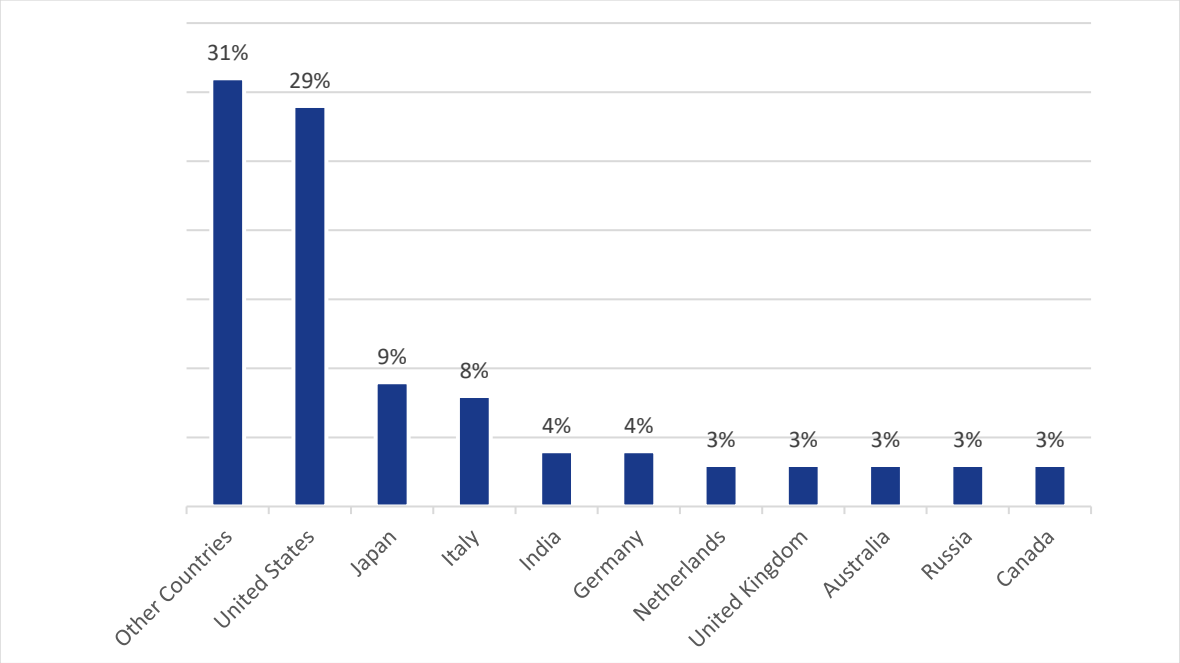

Figure 18: Top 10 countries by ransomware detections[230]

3.7.4 Top 5 ransomware threats[230]

- **Cerber**. Appearing first in March 2016, Cerber is one of the most widely spread ransomware families of the past year, distributed through spam and exploit kit campaigns. Spam campaigns have employed JavaScript (JS.Downloader), and Microsoft Word macro (W97M.Downloader) downloaders. Additionally, in a number of campaigns, Cerber was delivered directly as a compressed attachment. Recent variants have incorporated additional functionality such as Bitcoin wallet-stealing functionality.
- **Jaff** is a relatively recent arrival on the ransomware landscape but made an immediate impact. It is being spread by major malicious spam campaigns mounted via the Necurs botnet. The ransomware is downloaded by a malicious macro which is itself dropped by a .pdf attachment. Early variants of the ransomware appended encrypted files with a .jaff file extension. More recent variants use an extension

[230] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf, accessed November 2017.

of .sVn. Interestingly, before Jaff begins encrypting files, it checks the language setting of the infected computer. If it finds that the language is set to Russian, it will delete itself.

- **Sage** is an evolution of older ransomware known as CryLocker. It has been highly active over the past year and has been distributed through a wide variety of channels including the Trojan.Pandex spamming botnet, the Trik botnet, and the RIG exploit kit.
- **GlobeImposter.** Another recent arrival, GlobeImposter has managed to make an impact. Mostly, due to being distributed by a major malicious spamming operation known as Blank Slate, which has been linked to a number of ransomware families. GlobeImposter began by encrypting files with the .crypt file extension, but reports indicate that it is now using as many as 20 different file extensions.
- **Locky.** First appeared in early 2016, Locky has since been an ongoing ransomware menace. The malware is mainly spread through major spam campaigns, but at times Locky has also been distributed through a number of exploit kits. Locky has experienced periodic dips in activity, such as when the Necurs spamming botnet went quiet in early 2017. Locky invariably reappears with new campaigns as happened in August 2017.

3.7.5 Specific attack vectors

In 2017, we observed a not so common attack vector for delivering ransomware, namely the exploitation of a vulnerability (as described in chapter 5). More precisely an SMB vulnerability on Windows systems was exploited to deliver ransomware. Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147 and CVE-2017-0148.

In 2017, ransomware was also spread using more common attack vectors like spam emails, exploit kits, etc. For the entire list please of attack vector, see chapter 5.

3.7.6 Specific mitigation actions

The mitigation vector for ransomware contains the following elements:

- Exact definition and implementation of minimum user data access rights in order to minimize the impact of attacks (i.e. less rights, less data encrypted).
- Availability of reliable back-up off-line schemes that are tested and are in the position to quickly recover user data.
- Implementation of robust vulnerability and patch management.
- Implementation of content filtering to filter out unwanted attachments, mails with malicious content, spam and unwanted network traffic.
- Installation of end-point protection by means of anti-virus programs but also blocking execution of files (e.g. block execution in Temp folder).
- Use of policies for the control external devices and port-accessibility for all kinds of devices.
- Use of whitelisting to prevent unknown executables from being executed at the end-points.
- Invest in user awareness esp. with regard to secure browsing behaviour[231].
- Follow recent ransomware developments and prevention proposals in this[232] resource.

[231] http://theconversation.com/its-easier-to-defend-against-ransomware-than-you-might-think-57258, accessed November 2017.
[232] https://www.nomoreransom.org/prevention-advice.html, accessed November 2017.

In addition to the protective measures, there are a few important actions to be considered in order to minimize ransomware attack damages:

- Regular system backups (tested);
- Vulnerability patching as soon as a patch becomes available;
- Train users to avoid common security pitfalls, like phishing and social engineering attacks.

In the fight against malware additional mitigation actions need to be considered. Please find the full list of mitigation actions in the chapter on malware (see chapter 3.1.6 above).

3.7.7 Kill Chain

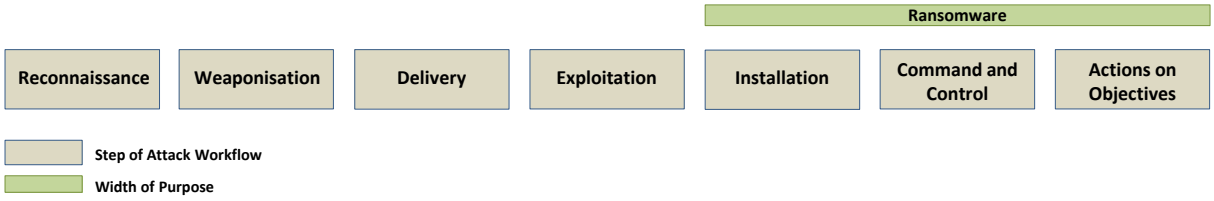

Figure 19: Position of Ransomware in the kill-chain

3.7.8 Authoritative references

"2017, State of Malware Report", Malwarebytes[233]; "KSN Report: Ransomware in 2016-2017", Securelist[234]; "Internet Security Threat Report – Government, June 2017", Symantec[235];

[233] https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf, accessed November 2017.
[234] https://securelist.com/ksn-report-ransomware-in-2016-2017/78824/, accessed November 2017.
[235] https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf, accessed November 2017.

3.8 Botnets

3.8.1 Description of the threat

Internet of Things botnets were considered as the second most important threat in 2017, after in late 2016 an enormous DDoS attack[236] performed using Mirai Botnet impacted a DNS Service provider called DYN. Moreover, it has been estimated that in 2017 another around 8.4 billion of things will be connected to the Internet. A big percentage of those devices have been assumed to be vulnerable and – when compromised - they can become part of botnets. Given the Mirai botnet in 2016, one of the biggest concerns of 2017 was the Internet of things (IoT) botnets engaged in DDoS attacks[237]. Yet, in this year there have been only a couple of events that confirmed these expectations[247, 238, 239]. Another important aspect is that IoT botnets were observed to be part of new botnet-based ransomworms like Hajime[240]. Devil's Ivy was an assessed vulnerability that could lead to new bit IoT botnets[241]. Finally, a interesting, yet alarming development was the detection of pulse wave DDoS attacks[187] (see also chapter 3.5). It has been assessed that technology used to achieve this kind of attacks doubles output speed of the botnet.

3.8.2 Interesting points

The identified interesting points for botnets are as follows:

- **Virtual Machines Could Be Turned into Botnets[242].** Big cloud providers like Microsoft or Google warned businesses that cyber criminals are targeting virtual machines deployed via the cloud to compromise them, turn them into zombies – part of botnets in order to be used in further attacks.
- In the first quarter of 2017 was observed an increase in botnet malware usage and tools like Ursnif, DELoader and Zeus Panda[243].
- Necurs[244] is one of the most active botnets in 2017 which affects mainly Asian and European countries. This botnet is formed by 7 smaller botnets put together using the same malware and it is used for sending large spam campaigns through email.
- Botnets are used in fake advertising[245]: attacker are developing bot networks which are used in creating fake popular accounts of pages on the Internet in order to attacks users who want to pay for advertising. Unfortunately, the advertisers don't get the exposure they were really paying for.

---

[236] https://www.cybersecurity-insiders.com/most-dangerous-cyber-security-threats-of-2017/, accessed November 2017.
[237] https://www.strozfriedberg.com/blog/2017-prediction-criminals-harness-iot-devices-botnets-attack-infrastructure/, accessed November 2017.
[238] https://arstechnica.com/information-technology/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/, accessed November 2017.
[239] https://research.checkpoint.com/new-iot-botnet-storm-coming/, accessed November 2017.
[240] https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things, accessed November 2017.
[241] https://www.wired.com/story/devils-ivy-iot-vulnerability/, accessed November 2017.
[242] https://biztechmagazine.com/article/2017/01/microsoft-warns-hacked-virtual-machines-are-very-real-threat, accessed November 2017.
[243] https://www.esecurityplanet.com/threats/q1-2017-saw-a-massive-surge-in-botnet-malware-activity.html, accessed November 2017.
[244] https://www.blueliv.com/research/necurs-one-of-the-worlds-biggest-botnets-today/, accessed November 2017.
[245] https://imptrax.com/blog/botnets-in-2017-everything-you-need-to-know, accessed November 2017.

- In late 2017 it has been discovered that a new massive botnet dubbed IoTroop[246] is forming by accumulating Internet of Things systems and smart devices such as IP Wireless cameras.
- Reaper[247] – the Mirai's successor has shown up to alert security-researchers. The botnet has been spotted in Q3 was found to share similarities and components with Mirai but with a key difference: Instead of primarily guessing the passwords of the devices, it uses known security weaknesses/vulnerabilities in the code of those insecure devices. Reaper infects IoT devices like: DLink, Goahead, JAWS, Netgear, Vacron, Linksys or Avtech. Approximately 100 DNS open resolvers were Integrated in this Malware, so DNS amplification attack can be easily carried out.
- Hackers are racing for enslaving more and more IoT devices. Once the Mirai botnet source code was published in late 2016, cybercriminals worldwide are about to create their own botnets and soon after they started the race to infect as much as possible vulnerable IoT devices. This has led to the introduction of malware that can expunge other malware from controlling the device[248].

3.8.3 Trends and main statistic numbers

- In first quarter of 2017 was revealed a 69.2%[249] increase of malware usage in comparison with the previous quarter. Malware tools like Ursnif, DELoader and Zeus Panda were used to leverage phishing emails and transform the targets into zombies – botnets members.
- Necurs, one of the most active botnets in 2017 has more than 1.5 million infected computers under its control.
- The Reaper[250] IoT botnet infected a million networks and has been assessed as a serious threat to the whole internet[251].
- Regarding Reaper were done some statistic[252] about its activity. So, was estimated that over 2 million of vulnerable devices are waiting to be infected only in one c2 queue. Also, was estimated that around 10k of active bots are controlled daily by one c2.
- As of 27 November 2017. the world's worst botnet infected countries are: China, India, Russia Federation, Brazil, Vietnam, Argentina, Iran, Islamic Republic of, Thailand, United States, Indonesia[253].
- The top four largest botnets to date are: 1 – BREDOLAB, 2 – MARIPOSA, 3 – CONFICKER, 4 – MARINA BOTNET.[254]
- **The overall trend of botnet population activity in 2017 was INCREASING.**

[246] https://research.checkpoint.com/new-iot-botnet-storm-coming/, accessed November 2017.
[247] https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/, accessed November 2017.
[248] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/iot-devices-threat-spreading/, accessed October 2017.
[249] https://www.esecurityplanet.com/threats/q1-2017-saw-a-massive-surge-in-botnet-malware-activity.html, accessed November 2017.
[250] https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/, accessed November 2017.
[251] https://thehackernews.com/2017/10/iot-botnet-malware-attack.html, accessed November 2017.
[252] http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/, accessed November 2017.
[253] https://www.spamhaus.org/statistics/botnet-cc/, accessed November 2017.
[254] https://themerkle.com/top-4-largest-botnets-to-date/, accessed November 2017.

3.8.4 Top botnets attacks

- At the start of 2017 Twitter[255] discovered that there were over 350.000 fake accounts which all were part of one botnet. More, other accounts which were part of smaller bot networks were found, bringing the total of fake accounts to over half a million.
- After three months of inactivity at the beginning of this year, Necurs[256] reappeared in March and resumed its activity with mass mailing spam campaigns spreading in most cases ransomware.
- In July 2017[257] an unnamed 29-year-old man pleaded guilty in a German court to charges related to Deutsche Telekom's routers became infected with a modified version of the Mirai malware.
- In late 2016 and yearly 2017 was performed a massive DDoS attack that reached 650 Gbps (Gigabit per second) using Leet Botnet[258].

3.8.5 Specific attack vectors

Botnets have a couple of particularities when it comes to attack vectors: the attackers are using common compromising/infections techniques in order to create the zombie networks; subsequently they are using them in conducting various other attack types, such as malware infection, sending phishing/spam and performing DDoS attacks.

3.8.6 Specific mitigation actions

Because most of the botnets are used to perform DDoS attacks, it is very important to take into consideration the mitigations for DDoD (see chapter 3.6.6 above). Moreover, mitigation vectors for this threat include:

- Installation and configuration of network and application firewalling.
- Performance of traffic filtering to all relevant channels (web, network, mail).
- Installation and maintenance of IP address blacklisting.
- Performance of Botnet Sinkholing[259].
- Performance of updates in a regular basis in orchestration with vulnerability management.
- Orchestration of controls both at host and network level as described in this resource[260].
- A standard for invalid traffic detection methods has been developed[261]. Accredited organisations may support in detection and filtering of fraudulent traffic[262].

[255] https://imptrax.com/blog/botnets-in-2017-everything-you-need-to-know, accessed November 2017.
[256] https://www.symantec.com/connect/blogs/necurs-mass-mailing-botnet-returns-new-wave-spam-campaigns, accessed November 2017.
[257] https://thehackernews.com/2017/07/mirai-botnet-ddos.html, accessed November 2017.
[258] http://www.securityweek.com/massive-attack-new-leet-botnet-reaches-650-gbps, accessed November 2017.
[259] http://la.trendmicro.com/media/misc/sinkholing-botnets-technical-paper-en.pdf, accessed October 2015.
[260] https://www.shadowserver.org/wiki/pmwiki.php/Information/BotnetDetection, accessed November 2015.
[261] http://mediaratingcouncil.org/GI063015_IVT%20Addendum%20Draft%205.0%20(Public%20Comment).pdf, accessed November 2017.
[262] https://www.whiteops.com/press-releases/white-ops-mrc-accreditation, accessed November 2017.

3.8.7 Kill Chain

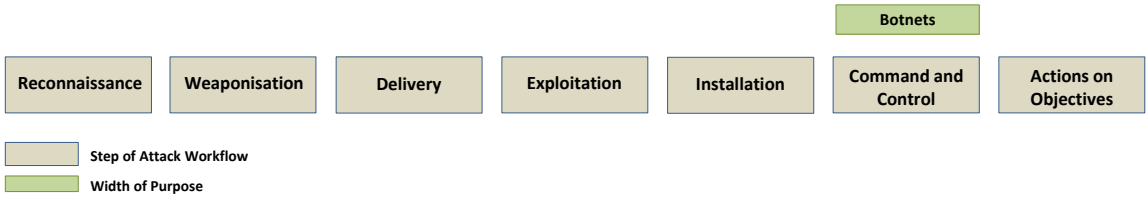

Figure 20: Position of Botnets in the kill-chain

3.8.8 Authoritative references

"State of Malware Report", Malwarebytes[263]; "Threats Report", McAfee[264]; "Threat Landscape Report", Fortinet[265]; "2017 Data Breach Investigations Report", Verizon[266];"The Evolution of Botnets", Cyren[267]; "A New IoT Botnet Storm is Coming", CheckPoint[268].

[263] https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf, accessed November 2017.
[264] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf, accessed November 2017.
[265] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Fortinet-Threat-Report-Q2-2017.pdf, accessed November 2017.
[266] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed November 2017.
[267] https://www.cyren.com/tl_files/downloads/Botnet_Evolution_Infographic.pdf, accessed November 2017.
[268] https://research.checkpoint.com/new-iot-botnet-storm-coming/, accessed November 2017.

3.9 Insider threat

3.9.1 Description of the cyberthreat

As a definition[269], insider threat refers to the threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of an organisation. Insider threats have been a major risk to governments and organisations around the world for many years. Still, they continue to play an important role in the threat landscape, since it is difficult for most organisations to distinguish them from benign activity. Even advanced external adversaries aim at abusing insiders to compromise an organisation. Insider incidents may be deliberate or inadvertent, whereas the latter is the most frequent form of insider abuse (e.g. via phishing). Given organisations' increased focus on robust perimeter security and locked-down systems, insiders are identified as a good potential attack vector. Tackling insider threats by enabling qualified detection and mitigation measures, requires a combination of different techniques. Such techniques originate from the technical, sociological, and the socio-technical domain.

3.9.2 Interesting points

The identified interesting points for insider threat are as follows:

- **Insider threat is perceived as a rising trend**. 56% of security professionals say insider threats have become more frequent in the last 12 months, while 42% of organisations expect a cyber-security budget increase over the next year[270].
- **Losses due to insider threat are largely unknown**. Relatively, only few respondents of a recent survey[271] were able to quantify either real or potential losses due to an insider threat. This could explain why insider threats are a concern but not a priority. It is known that organisations often do not spend money in an area if they cannot quantify the losses first.
- **Privileged users pose the biggest threat**. According to a recent survey[272], privileged users, such as managers with access to sensitive information, pose the biggest insider threat to organizations (60%), followed by contractors and consultants (57%), and regular employees (51%).
- **The enemy within**. In 60% of cases, insiders withhold data in the hope of cashing it out in the future. But, sometimes it might be the case of taking data to a new employer or starting a rival company (15%)[273].
- **Top challenge in terms of detection**. According to reports[274], right after the detection of advanced/unknown threats and lack of security staff, the detection of rogue insider attacks is the third of the top 3 challenges that SOCs (Security Operations Centres) face.

[269] https://www.dni.gov/files/documents/FOIA/DF-2016-00161.pdf, accessed November 2017.
[270] http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017_Haystax_FINAL.pdf, accessed November 2017.
[271] https://www.sans.org/reading-room/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890, accessed November 2017.
[272] http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017_Haystax_FINAL.pdf, accessed November 2017.
[273] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed November 2017.
[274] http://www.cybersecurity-insiders.com/wp-content/uploads/2017/02/2017-Threat-Hunting-Report.pdf, accessed November 2017.

- **Health care sector is targeted**. Healthcare organisations, more than ever, need to pay attention to insider threats. 2017 kicked off with figures suggesting that 59.2% of breached patient records were the result of insider attacks[275].

3.9.3 Trends and main statistic numbers[276,277,Error! Bookmark not defined.]

- Recent figures[278] related to the health care sector show that 29% of the incidents reported to The U.S. Department of Health and Human Services (HHS) were the result of malicious insiders or insider errors.
- Over 75% of organisations estimate insider breach remediation costs could reach $500,000, while 25% believe the cost exceeds $500,000 and can reach in the millions.
- 74% of organisations feel vulnerable to insider threats — an increase of 7% over last year's survey. However, less than half of all organisations (42%) have the appropriate controls in place to prevent an insider attack.
- 53% majority of a survey responders have confirmed insider attacks against their organisation in the previous 12 months.
- 56% of organizations leverage insider threat analytics, an increase of 20% compared to last year.
- According to a recent report, organisations are shifting their focus to the detection of insider threats (64%), followed by deterrence methods (58%), analysis and post breach forensics (49%).
- The use of user behaviour monitoring is accelerating, as 88% of organisations deploy some method of monitoring users.
- Concerning resources dedicated to countering insider threats, only 29% of the organisations declare that they have a dedicated team for that threat, while 60% say that they use their usual security resources when insider threats/attacks occur[279].
- **The overall trend of insider threat in 2017 was STABLE.**

3.9.4 Top IT assets vulnerable to insider attacks

A recent report shows that the following IT assets are most vulnerable to insider attacks[280].

[275] https://post-healthcare.com/31-health-data-breaches-disclosed-in-january-as-hhs-fines-for-late-reporting-d72c533034fa, accessed November 2017.
[276] http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017_Haystax_FINAL.pdf, accessed November 2017.
[277] https://www.cybersecurity-insiders.com/portfolio/insider-threat-report/, accessed November 2017.
[278] https://post-healthcare.com/31-health-data-breaches-disclosed-in-january-as-hhs-fines-for-late-reporting-d72c533034fa, accessed November 2017.
[279] https://www.sans.org/reading-room/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890, accessed November 2017.
[280] http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017_Haystax_FINAL.pdf, accessed November 2017.

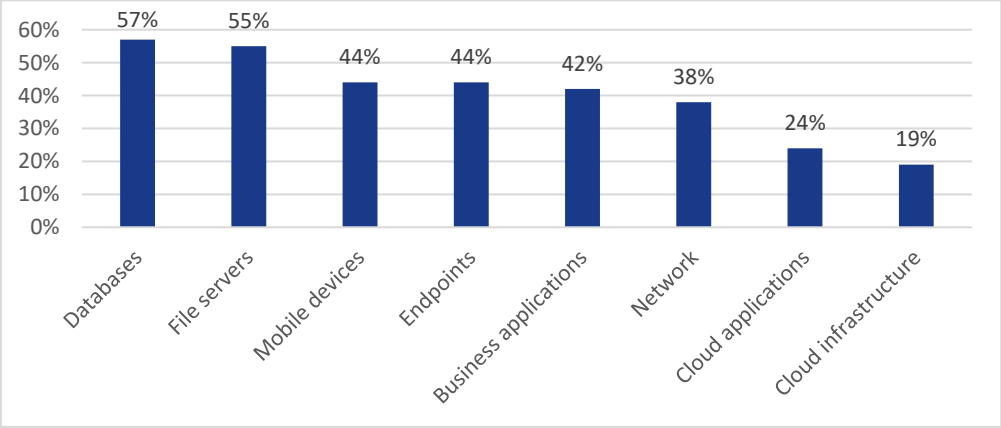

Figure 21: IT assets vulnerable to insider attacks

3.9.5 Specific attack vectors

A recent survey[281] reveals cybersecurity professionals perceive the following, as the top enablers for insider attacks. For more information about attack vectors please see chapter 5.

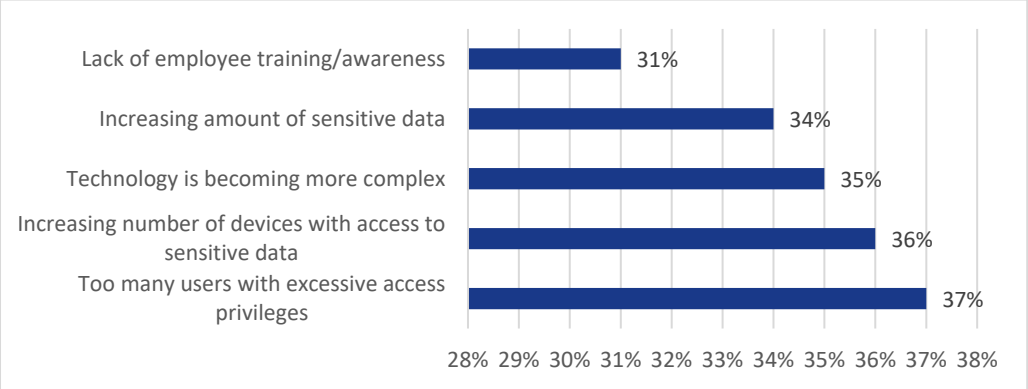

Figure 22: Top enablers for insider attacks

3.9.6 Specific mitigation actions

The mitigation vector for this threat contains the following elements[282]:

- Definition of a security policy regarding insider threats, in particular based on user awareness, one of the most effective controls for this type of cyber-threat[283].
- Use of identity and access management (IAM) solutions by also implementing segregation of duties (e.g. according to defined roles).
- Implementation of identity governance solutions defining and enforcing role-based access control.
- Implementation/use of security intelligence solutions.

[281] https://www.cybersecurity-insiders.com/wp-content/uploads/2016/09/Insider-Threat-Report-2018.pdf, accessed November 2017.
[282] http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf, accessed November 2015.
[283] https://www.forcepoint.com/resources/reports/forcepoint-2016-global-threat-report, accessed October 2017.

- Use of data-based behaviour analysis tools.
- Implementation of privileged identity management (PIM) solutions.
- Implementation of training and awareness activities
- Implementation of audit and user monitoring schemes.

3.9.7 Kill Chain

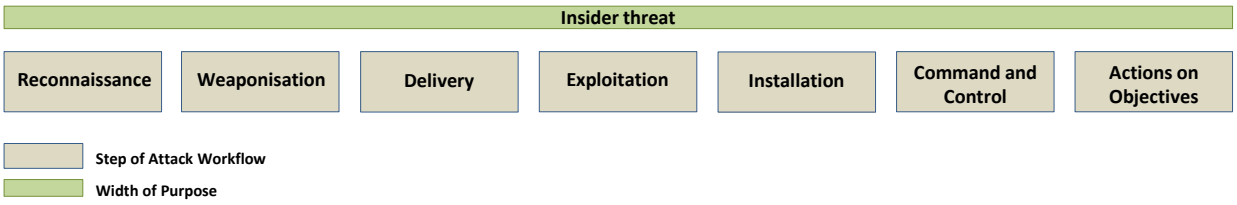

Figure 23: Position Insider threat in kill-chain

3.9.8 Authoritative references

"2017 Data Breach Investigations Report", Verizon[284]; "Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey", SANS[12]; "Insider Threat – 2018 Report", Cybersecurity Insiders[285]; "Insider Attacks - Industry Survey", Haystax[286].

[284] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed November 2017.
[285] https://www.cybersecurity-insiders.com/wp-content/uploads/2016/09/Insider-Threat-Report-2018.pdf, accessed November 2017.
[286] http://haystax.com/wp-content/uploads/2017/03/Insider_Threat_Report_2017_Haystax_FINAL.pdf, accessed November 2017.

3.10 Physical manipulation/damage/theft/loss

3.10.1 Description of the cyberthreat

Though not always a technical/cyber threat, physical manipulation/damage/theft/loss continues to have severe impact on all kinds of digital assets. Physical loss and theft used to be the most important causes of data breaches[287], and while hacking or malware took their place in 2017, they remain one of the major causes of data breaches[288].

3.10.2 Interesting points

The identified interesting points for physical manipulation/damage/theft/loss are as follows:

- A last year's survey[289], which polled IT professionals across various industries, revealed that IT theft in the office accounts to 23%, while more than half of the survey participants do not utilize physical locks for their IT devices.
- Although protection by means of storage encryption would suffice to mitigate the risks emanating from data breaches, it's being reported[290] that only 41% of companies currently have a consistent enterprise-wide encryption strategy.
- Given the increased number of IoT and mobile devices, and also the increase of cloud services, securing the perimeter will remain one of the challenges of cyber-security professionals.
- Physical attacks also pose a high risk for critical infrastructures[291], which are very often attacked by physical means. Physical threat is persistent and needs more attention from both users and companies, especially because it has the potential to surpass the efficiency of all other complex security measures.
- **Drilled ATMs - new ways of physical intervention**. Reports[292] speak about several cases of ATMs compromised by physical intervention, e.g. a perfectly round hole about 4 cm in diameter drilled near the PIN pad. Experts found that some ATMs are easy to drill due to the plastic parts they incorporate. Moreover, a 10-pin header connected to a bus that interconnects all of the ATM's components, can be used to take control of the machine.
- **The black market of stolen phones is lowering**. It seems that complex security measures taken lately by the smartphones vendors to block the utilization of stolen devices are paying off. Reports[293] mention that the number of smartphone thefts has been halved in 2017 as compared to 2009.
- **The rise of SCAM targeting the owners of stolen smartphones.** Thieves use a SCAM to trick the owners of the phones to reveal necessary data for unlocking stolen phones: they send an SMS to the victim saying their phone was found and they try to convince them to click on a fake URL to provide

[287] https://documents.trendmicro.com/assets/rpt/rpt-2017-Midyear-Security-Roundup-The-Cost-of-Compromise.pdf, accessed November 2017.
[288] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed November 2017.
[289] https://www.kensington.com/a/283005, accessed November 2017.
[290] https://gets.thalesesecurity.com/pdf/ponemon-global-encryption-trends-study-infographic.pdf, accessed November 2017.
[291] https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf, accessed November 2017.
[292] https://www.kaspersky.com/blog/sas-2017-atm-malware/14509/, accessed November 2017.
[293] http://www.mobilenewscwp.co.uk/2017/03/13/nearly-half-million-brits-phones-stolen-last-year/, accessed November 2017.

confidential data in order get the phone back[294].Though being related to phishing, this attack is based on the loss of property.

- **Telecom infrastructure is still preferred by thieves**. Copper thieves have now gone after all kinds of targets, and telecom infrastructure is one of them[295]. They recently added the backup batteries that keep cellular towers working to their list. This is a real and serious threat considering the role of this infrastructure in case of emergencies.

3.10.3 Trends and main statistic numbers

- According to a recent report[296], physical actions were present in 8% of breaches – a lowering trend;
- In the first half of 2017, 18% of data breaches were caused by accidental loss[297];
- The average person now loses 1.24 items a year and less than half of those are ever recovered, while 70% of people have lost a data storage device, and 7.5% of people have lost their laptop in the last 12 months [298];

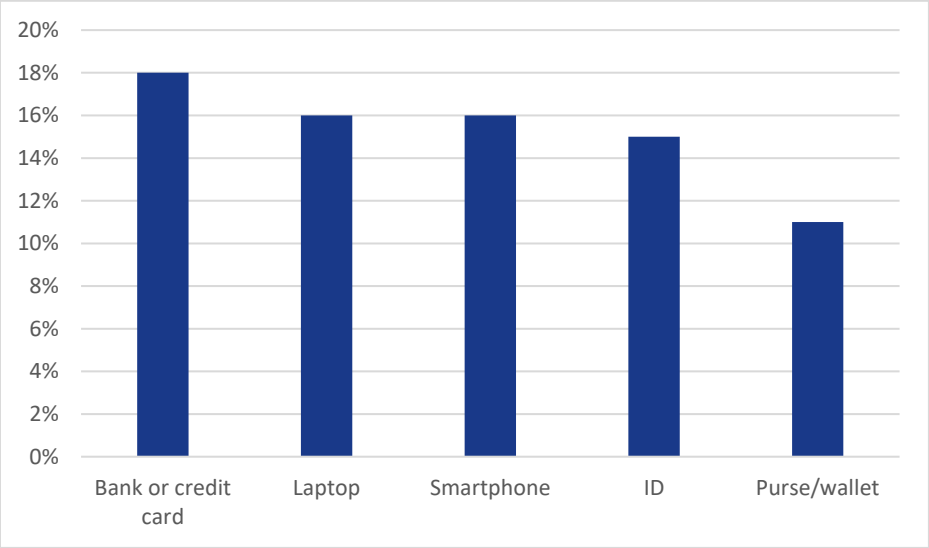

Figure 24: Items lost by people in the last 12 months

- **The overall trend of physical manipulation/damage/theft/loss in 2017 was STABLE (slight increase).**

3.10.4 Specific mitigation actions

- Use of encryption in all information storage and flow that is outside the security perimeter (devices, networks, cloud services, etc.). This will eliminate the impact from this threat.
- Use asset inventories to keep track of user devices.

[294] http://abc7chicago.com/technology/new-smartphone-scam-targets-owners-of-stolen-phones/2089537/, accessed November 2017.
[295] http://www.lfpress.com/2017/08/29/london-crime-opp-probes-thefts-of-backup-batteries-and-copper-wire, accessed November 2017.
[296] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed November 2017.
[297] http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf, accessed November 2017.
[298] http://mozy.com/about/news/reports/lost-and-found/, accessed November 2017.

- Limit access to areas with sensitive info or equipment[299].
- Implement well documented physical security policies and integrate physical security measures with digital ones to obtain a holistic approach.
- Consider using insurance to cover losses connected to both physical and related cyber- risks.
- Develop user guides for mobile devices (smartphones, tablets, laptops, etc.) and use good practices[300].

3.10.5 Kill Chain

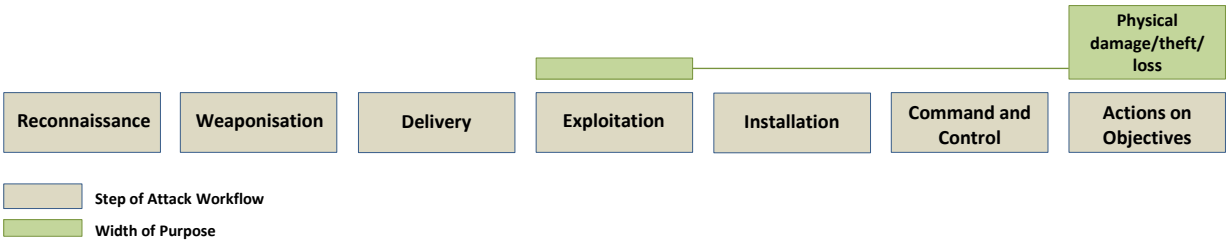

Figure 25: Position of Physical manipulation/damage/theft/loss in the kill-chain

3.10.6 Authoritative references

"2017 Data Breach Investigations Report", Verizon[301]; "Survey: IT Security & Laptop Theft", Kensington[302]; "2017 Global Encryption Trends", Thales[303]

[299] http://blog.securitymetrics.com/2017/02/5-tips-to-boost-business-physical-security.html, accessed November 2017.
[300] http://transition.fcc.gov/cgb/consumerfacts/lostwirelessdevices.pdf, accessed November 2017.
[301] https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf, accessed November 2017.
[302] https://www.kensington.com/a/283005, accessed November 2017.
[303] https://gets.thalesesecurity.com/pdf/ponemon-global-encryption-trends-study-infographic.pdf, accessed November 2017.

3.11 Data Breaches

3.11.1 Description of the cyberthreat

Data breaches are successful incidents that have led to loss of data and are encountered ex-post: that is, when a data breach is being assessed, the successful incident has already happened. Just as security incidents, successful data breaches are supposed to be much more than we know of. In the past year, data breach preparedness became a critical objective for most companies. Data breach is not a cyberthreat per se. It is rather a collective term for successfully launched cyberthreats. Hence, the avoidance of data breaches is related with the implementation of defences that span the entire cyberthreat landscape. Defenders must keep an eye on both known and new threats so that they can address them with an incident response plan, along with comprehensive data breach preparation.[304].

3.11.2 Interesting points

The following interesting points have been identified for data breaches:

- Researchers made a top five of trends seen in data breaches that dominated in 2017[305]:
  - The high number of data breaches based on weak or stolen/broken passwords expedite the end of password as a means for protection.
  - There is a transition from espionage to nation-state cyber-attacks.
  - Most organisations, targeted by new, sophisticated attacks, will come from the healthcare sector.
  - Cyber criminals turn to payment-based attacks such as ransom attacks.
  - Multinational companies will be the most affected by international data breaches.
- According to researchers[320], cybercriminals will continue selling user credentials on the dark web. Reusing passwords will expose companies to the risk of becoming the target of repeating unauthorized log-ins; notifying users about successful logins may prevent information from being misused.
- Once the new E.U. General Data Protection Regulation (GDPR) goes into effect in 2018, damages made by data loss will have significant repercussions. According to researchers, new regulations will also take effect in Canada. Australia may also apply a data breach bill as well.
- Although user credentials remain popular targets, the overall number of data breaches affecting this type of records has decreased during the first half of 2017[306].

3.11.3 Trends and main statistic numbers

- This year the number of confirmed successful attacks increased by 25%, with more incidents still coming to light[307].

[304] https://www.cio.com/article/3155724/security/5-data-breach-predictions-for-2017.html, accessed November 2017.
[305] https://www.cio.com/article/3155724/security/5-data-breach-predictions-for-2017.html, accessed November 2017.
[306] https://www.opswat.com/blog/11-largest-data-breaches-all-time-updated, accessed December 2017.
[307] https://www.riskbasedsecurity.com/2017/07/over-2200-data-breaches-disclosed-so-far-in-2017-exposing-over-six-billion-records/, accessed November 2017.

- Insider threats may be involved in fraud, theft of valuable information or sabotage. In most cases (60%), insiders will trade data for cash. Other observed attempts of insiders are: cases of unsanctioned snooping (17%), taking data to a new employer or to start a rival company (15%)[308].
- 8.1% of cybersecurity breaches were related to the government or military sector.
- 7.4% of data breaches are related to educational institutions.
- 61% of the data breach victims in this year's report are businesses with under 1,000 employees.[309]
- About 95% of phishing attacks that led to a breach were followed by unwanted software installation.[310]
- At the end of June, 2017, there were 2,200 data breaches disclosed exposing over 6 billion records[311].
- The biggest 10 breaches exposed 5.6 billion of the 6 billion records compromised[312].
- 35.4% of the data breaches targeted entities from Medical and Healthcare sectors[313].
- **The overall trend of data breaches in 2017 was INCREASING.**

3.11.4 Top Data breaches

The table below enlists some of the most sever data breaches:

Organisation	Description
DU Group DU Caller	(Web) 2,000,000,000 user phone numbers, names and addresses were inappropriately made accessible in an uncensored public directory
NetEase, Inc.	(Hacking) 1,221,893,767 e-mail addresses and passwords were stolen by hackers and were sold on the Dark Web by DoubleFlag
River City Media, LLC	(Web) 1,374,159,612 names, addresses, IP addresses, and e-mail addresses, as well as an undisclosed number of financial documents, chat logs, and backups were exposed by a faulty rsync backup
Deep Root Analytics	(Web) Approximately 198,000,000 voter names, addresses, dates of birth, phone numbers, political party affiliations, and other demographic information were exposed in an unsecured Amazon S3 bucket
Edmodo	(Hacking) 77,000,000 user e-mail addresses, usernames, and bcrypt hashed passwords with salts were stolen by hackers through undisclosed means
EmailCar	(Web) 267,693,854 e-mail addresses and phone numbers were exposed in an unsecure MongoDB installation and were later dumped on the Internet

[308] http://www.nationalinsiderthreatsig.org/pdfs/Insider%20Threats%20Incidents-Could%20They%20Happen%20To%20Your%20Organization.pdf, accessed December 2017.
[309] https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf, accessed November 2017.
[310] https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf, accessed November 2017.
[311] https://www.riskbasedsecurity.com/2017/07/over-2200-data-breaches-disclosed-so-far-in-2017-exposing-over-six-billion-records/, accessed November 2017.
[312] https://pages.riskbasedsecurity.com/hubfs/Reports/2017%20MidYear%20Data%20Breach%20QuickView%20Report.pdf?t=1506112909072&utm_campaign=2017%20MidYear%20Data%20Breach%20QuickView%20Report&utm_source=hs_automation&utm_medium=email&utm_content=54529893&_hsenc=p2ANqtz--lCW5WPTdHKj202vJ-NmAJn0xvdwxRNBTfnvGybbPxN3DigKfpKXaajge0oV4Cq5HYauocBrqHszSR_qG7DPFhqI21ng&_hsmi=54529893, accessed November 2017.
[313] https://revisionlegal.com/data-breach/2017-security-breaches/, accessed November 2017.

Tencent Holdings Ltd	(Hacking) 129,696,449 e-mail addresses and passwords were stolen by hackers and were sold on the Dark Web by DoubleFlag
National Social Assistance Programme (India)	(Web) Roughly 135,000,000 Aadhaar numbers and 100,000,000 linked bank account numbers, as well as names, caste, religion, addresses, phone numbers, photographs, and assorted financial details were leaked on government web portals
Youku	(Hacking) 91,890,110 user accounts with usernames, e-mail addresses and MD5 encrypted passwords were compromised by hackers and offered for sale
Yahoo Japan	(Hacking) 23,590,165 e-mail addresses and passwords were stolen by hackers and were sold on the Dark Web by DoubleFlag
Equifax	143 million customers of the credit reporting service had their personal and financial information stolen. The hack occurred over several weeks between May and June 2017 and was disclosed in late July. Since the first reports, Equifax reported that an additional 2 million customers were affected by the hack. The Equifax data breach has subjected Equifax to government investigation.

Table 1: Sequence of Data breaches in 2017

3.11.5 Specific attack vectors

Patterns and attack vectors seen in 2017 regarding data breaches:

- **SQL Injection Attack[314].** This type of attack remains the most popular and commonly used web application attack.
- **Phishing Attacks.** Attackers target companies by trying to impersonate a partner or a vendor through an e-mail that asks users to take an action that would give the phisher an access point to critical data or information.
- **Insider threat and privilege misuse[315].** This category includes any kind of unauthorised or malicious use of organisational resources. It can be the result of both the actions of an insider or an external attacker, using compromised credentials, or a combination of both.
- **Physical theft and loss**. This refers to intentional or unintentional loss due to physical attacks.

3.11.6 Specific mitigation actions

Due to wide nature of threats that can lead to a data breach, mitigation controls mentioned overlap with other cyber-threats. The mitigation vector for this threat contains the following elements (see also[316]):

- Performance of data classification to assess and reflect the level of protection needed according to data categories.
- Implementation of Data Loss Prevention solutions to protect data according to their class both in transit and in rest, especially in cases of large data transfers and use of USB devices.
- Usage of encryption of sensitive data, both in transit and in rest.
- Reduction of access rights to data according to principle of least privileges.

[314] https://www.bitsighttech.com/blog/attack-vectors-types-of-security-breaches, accessed November 2017.
[315] https://www.solarwindsmsp.com/blog/top-10-cyberattack-vectors-and-how-mitigate-them-part-1, accessed November 2017.
[316] https://zeltser.com/malware-in-the-enterprise/, accessed November 2017.

- Development and implementation of security policies for all devices used.
- Performance of updates in a regular basis in orchestration with vulnerability management.
- Develop new policies to enforce the use of stronger passwords and the use of two-factor authentication.
- Limit the amount of sensitive information stored on web-facing applications.
- Implementation of malware protection and insider threat protection policies.
- Organisations that plan in advance greatly reduce their legal, reputational and financial impacts. A holistic plan should cover two distinct parts of a data breach incident -assessment of the privacy incident and development of an appropriate breach response.
- Enforce security awareness within your company creating and maintaining training courses. Train your employees to identify and report suspicious e-mails or to call IT if they notice anything unusual with their computers.

3.11.7 Kill Chain

Kill chain is not relevant for this threat: this is a "composite" threat, that is, consisting of many cyberthreats spanning the entire phases of the kill chain.

3.11.8 Authoritative references

"2017 Data Breach Investigations Report", Verizon[317]; "M-Trends 2017", FireEye[318]; "Cost of Data Breach Study", IBM[319]; "Data Breach Industry Forecast", Experian[320].

[317] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed November 2017.
[318] https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html, accessed November 2017.
[319] http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf, accessed November 2017.
[320] https://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf, accessed November 2017.

3.12 Identity Theft

3.12.1 Description of the cyberthreat

Identity theft is a cyberthreat in which the attacker aims at obtaining confidential information that is used to identify a person or even a computer system. Such confidential information may be: identifiable names, addresses, contact data, credentials, financial data, health data, logs, etc. Subsequently, this information is abused to impersonate the owner of the identity. Identity theft is a special case of data breach. It is the result of successful attacks through other cyber-threats that target identity information. Fraudsters acquire identity data in various ways: hacking, dark web shopping, exploiting personal information on social media, social engineering etc. With more and more data breaches being exposed -like the famous Equifax data breach, which exposed the personal data of 143 million U.S consumers[321]- we assume that identity theft is a serious threat and will probably remain so in the coming years. Reports[322] suggest that identity fraud attempts are increasing every year, and reached high levels in 2017. For example, in the UK, identities are being stolen at a rate of almost 500 per day. The frequent massive data breaches in combination with the low prices of identity information on the black market makes identity theft easy and affordable for low capability threat agents.

3.12.2 Interesting points

The interesting points for this threat are:

- **Personal information remains a popular commodity**. Credit card data is available in online marketplaces starting from $10 - $20, while other highly detailed personal information records (referred to as "fullz" in the black market slang language) are offered for as low as $10[323].
- **Increase in old-fashioned stealing techniques**. The widespread adoption of EMV credit cards (a global standard for cards equipped with computer chips and the technology to authenticate chip-card transactions, which is adopted by major companies such as Europay, Mastercard and Visa) will likely force fraudsters to resort to other methods to steal financial data, like dumpster diving, check washing, and mail theft[324].
- **Information about identity theft/fraud is still insufficient in the EU space**. As in the previous years, important information about countering identity theft and fraud originates from the US[325,326,327], with the UK[328] covering the subject a bit more comprehensively.
- **Identity theft risk is underestimated**. Many people underestimate the general risks of identity theft and their personal exposure[329]. Most are only somewhat concerned about the security of their personal information online, with 62% saying it is a minor concern they worried about sometimes, and 17% saying that they don't worry about it at all.

---

[321] https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do, accessed November 2017.
[322] https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels, accessed November 2017.
[323] https://www.secureworks.com/resources/rp-2017-state-of-cybercrime, accessed November 2017.
[324] http://www.idtheftcenter.org/Identity-Theft/the-2017-identity-theft-and-fraud-predictions.html, accessed November 2017.
[325] https://wallethub.com/edu/states-where-identity-theft-and-fraud-are-worst/17549/, accessed November 2017.
[326] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime, accessed November 2017.
[327] https://www.asecurelife.com/category/personal-security/identity-theft/, accessed November 2017.
[328] https://www.cifas.org.uk/, accessed November 2017.
[329] https://www.experian.com/blogs/ask-experian/survey-findings-are-consumers-making-it-easier-for-identity-thieves/?pc=prt_exp_0&cc=prt_0817_itpsurvey, accessed November 2017.

3.12.3 Trends and main statistic numbers

- According to one of the UK's leading fraud prevention services[330], a record of 89,000 identity frauds were recorded in the first semester of 2017 – a 5% growth compared to the same period of 2016.
- 25% of the respondents of a recent survey[331] declared that they shared their credit card number or PIN with friends and family, and 20% would allow a friend or family member to use their personal information to help them get a job or credit.
- The most common types of identity theft are the following:

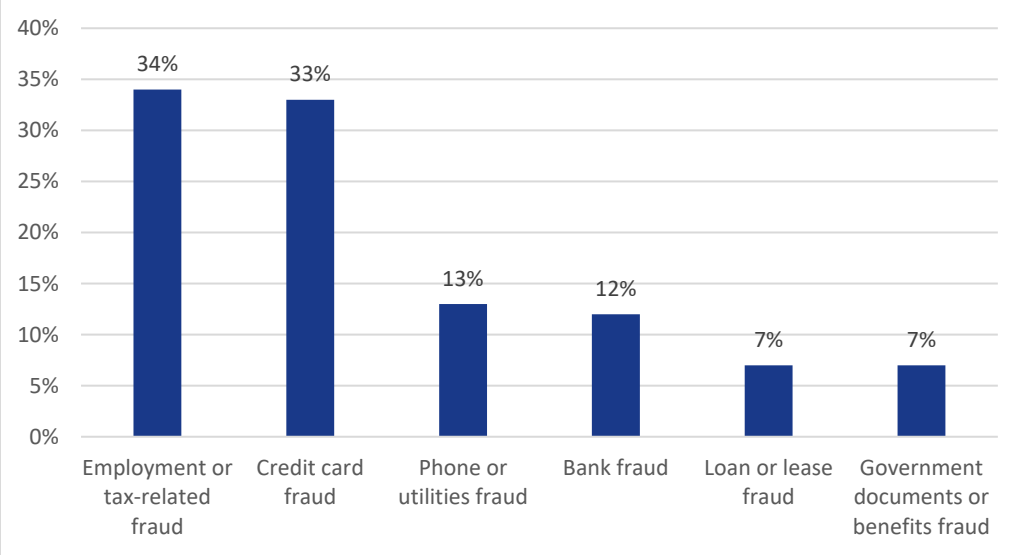

Figure 26: Most common types of identity theft[332]

- **The overall trend of identity theft follows the trends of data breaches and in 2017 was INCREASING.**

3.12.4 Top 5 identity theft threat

- **Skimmers**. An identity theft method where, fraudsters place these devices (skimmers) over card readers at checkout registers, gas stations or ATMs. Skimmers store credit and debit card information and fraudsters can then use this data to make counterfeit cards, use them for online purchases, or sell them on the black market.
- **Dumpster divers**. Fraudsters dig through trash or mailbox, looking for bank statements, copies of tax returns and other documents that have personal information.
- **Phishers**. Phishers use authentic-looking e-mails and websites to trick users to click on a link or open an attachment that will download malware onto their computers and leave confidential information vulnerable.
- **Hackers**. These threat agents install malware on computer networks, legitimate websites, and by extension to user systems, and steal personal information.

[330] https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels, accessed November 2017.
[331] https://www.experian.com/blogs/ask-experian/survey-findings-are-consumers-making-it-easier-for-identity-thieves/?pc=prt_exp_0&cc=prt_0817_itpsurvey, accessed November 2017.
[332] https://www.lifelock.com/education/how-common-is-identity-theft/, accessed November 2017.

- **Telephone impersonators**. Fraudsters may contact a bank's call center many times, each time gaining a different piece of information until they have enough information to impersonate an actual bank customer and gain account access.

3.12.5 Specific attack vectors

As described in chapter 5, the human element is one of the most common attack vectors used by threat agents. According to a recent survey[333], some of the most common information that people unknowingly make available online and can be abused are:

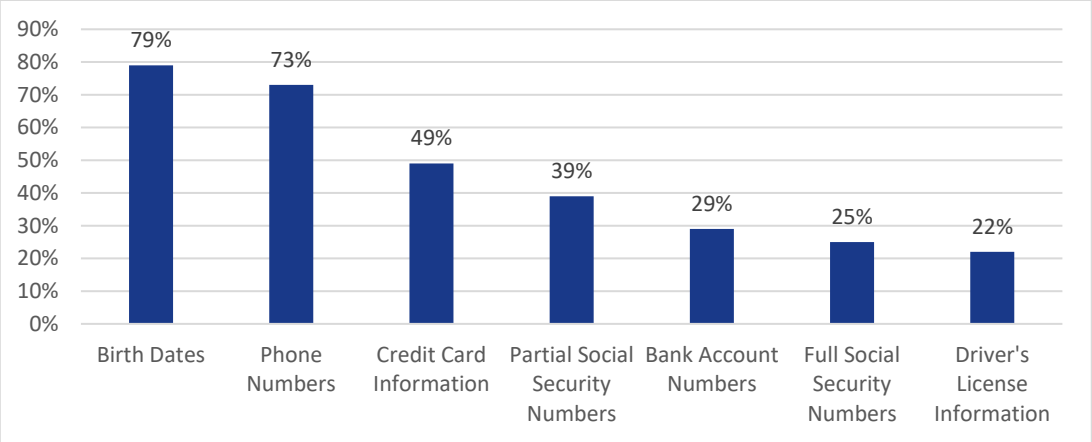

Figure 27: Types of exposed information

3.12.6 Specific mitigation actions

- Adequately protect all identity documents and copies (physical or digital ones) against unauthorised access;
- Properly configure privacy settings across all the social media channels you use, including the use two factor authentication.
- Identity information should not be disclosed to unsolicited recipients and their requests by phone, email or in person.
- Password protect devices, ensure good quality of credentials, and secure methods for their storage.
- Users should pay attention when using public Wi-Fi networks, as fraudsters hack or mimic them. If one is used, it should be avoided accessing sensitive applications and data. A trusted VPN service should be used when connecting to public Wi-Fi networks.
- Transactions documented by means of bank statements or received receipts should be checked regularly upon irregularities.
- Content filtering to filter out unwanted attachments, mails with malicious content, spam and unwanted network traffic should be installed.
- Install end-point protection by means of anti-virus programs but also block execution of files appropriately (e.g. block execution in Temp folder).

[333] https://www.experian.com/blogs/ask-experian/survey-findings-are-consumers-making-it-easier-for-identity-thieves/?pc=prt_exp_0&cc=prt_0817_itpsurvey, accessed November 2017.

- Ensure good quality of credentials and secure methods for their storage.
- Use of Data Loss Prevention (DLP) solutions. A detailed guide for DLP can be found here[334].
- A detailed list of practical identity theft mitigation controls can be found also here[335].

3.12.7 Kill Chain:

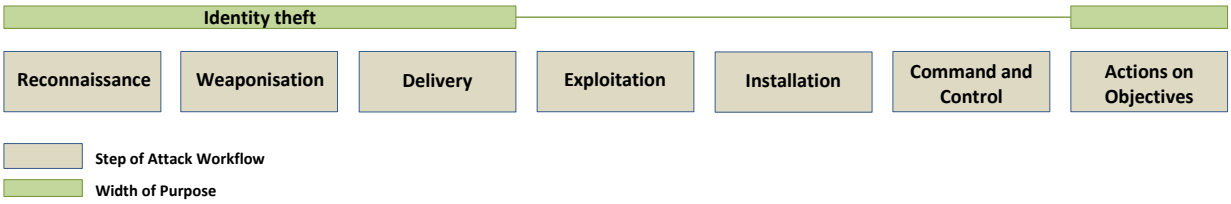

Figure 28: Position of Identity theft in the kill-chain

3.12.8 Authoritative references

"Identity fraud soars to new levels", CIFAS[336]; "2017 State of Cybercrime Report", SecureWorks[337]; "ITRC 2017 Identity Theft and Fraud Predictions", ITRC[338]

[334] http://www.mcafee.com/us/resources/reports/rp-data-protection-benchmark-study-ponemon.pdf, accessed October 2016.
[335] http://www.asecurelife.com/ways-to-prevent-identity-theft/, accessed November 2017.
[336] https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels, accessed November 2017.
[337] https://www.secureworks.com/resources/rp-2017-state-of-cybercrime, accessed November 2017.
[338] http://www.idtheftcenter.org/Identity-Theft/the-2017-identity-theft-and-fraud-predictions.html, accessed November 2017.

3.13 Information leakage

3.13.1 Description of the cyberthreat

One of the major cyber-security threats of 2017 is the various types of information leaks, from personal data collected by Internet giants and online services, to business data stored in companies' IT infrastructures[339]. When security breaches become headlines on blogs or newspapers, they tend to be about hostile actors or the catastrophic failure of technologies. But often the reality is that despite the impact or the scope of a breach, it is usually caused by an action, or failure of someone inside the organisation[340].

3.13.2 Interesting points

The identified interesting points for information leakage are as follows:

- **Take into consideration the basics.** Getting the basics done well can determine the biggest and most efficient impact on insiders: updating software automatically closes that open vulnerability before a hacker can use it to compromise a network. Enforcing strong standards and policies for user identities and passwords means stealing credentials is much harder[341].
- **Focus on the most important assets**. Cyber criminals target what an organisation values most. So identify the most-valuable systems and data, and then give them the strongest defences and the most frequent monitoring.
- **We're only human, and at exactly the wrong time**. Human error is one of the most important factor in breaches, and trusted but unwitting insiders are to blame. From misaddressed emails to lost devices to confidential business data sent to insecure personal emails, mistakes can be very costly. The riskiest of these are well-meaning IT admins, whose complete access to company infrastructure can turn a small mistake into a catastrophe.
- **Mobile applications can expose sensible information[342]**: Coding errors can put mobile device users at risk by exposing personal data. For example in November 2017, was identified a coding error in many GPS apps published by Telenav Inc. or in AT&T Navigator app pre-installed on many Android which allow hackers to access credentials for text messaging. The credentials were hardcoded in the app by the developers.

3.13.3 Trends and main statistic numbers

- About 78% of users considered to quit social networks, part of them being concerned about technology companies spying on them.
- Information leakage incidents have evolved in terms of frequency, volume and sophistication[343].

---

[339] https://www.bloomberg.com/news/articles/2016-12-21/data-leaks-from-social-networks-threat-in-2017-kaspersky-says, accessed November 2017.
[340] https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company, accessed November 2017.
[341] https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company, accessed November 2017.
[342] https://www.reuters.com/article/us-cyber-mobile-vulnerability/mobile-app-errors-expose-data-on-180-million-phones-security-firm-idUSKBN1D91ZA?rpc=401&, accessed November 2017.
[343] http://thelibrary.solutions/library/newsletters/2017-cyber-attack-trends%20Mid-Year%20Report%20(EN).pdf, accessed November 2017.

- Privacy leakage resulting from mobile applications will increase in the future[344]. This is supported by latest threats, involving mobile applications downloaded from application stores that sent personal details back to the application developer or exposed embedded credentials.
- One of the biggest concerns in 2017 related to BYOD was information leakage (69%)[345].
- **The overall trend of information leakage in 2017 was INCREASING.**

3.13.4 Top data leaks threats[346]

- **Cloudbleed.** In February, Cloudflare Internet Infrastructure announced that a platform error has caused a leakage of potentially sensitive customer data. Cloudflare provides security services to approximately six million customer websites, although leakages were rare and involved only small pieces of data from an enormous amount of information.
- **198 Million Voter Records Exposed.** Unfortunately, it is not unusual for electoral data to get publicly exposed. On June 2017, a publicly accessible database containing personal information for 198 million American voters was found.
- **Macron Campaign Hack.** In May 2017, two days before the French presidential election, hackers dumped a significant amount of data online – about 9GB of emails were leaked from the front-runner party (Emmanuel Macron's party). The timing of the leakage seemed orchestrated to give Macron a minimal response time and capacity to respond, since French presidential candidates have no right to speak to the public two days before the election. The authenticity of the leaks was soon questioned by Macron's party.
- A misconfiguration on a cloud server of **Verizon** led to the details being posted online: phone numbers, names and pin codes of six million customers which were left online for around nine days.

3.13.5 Specific attack vectors

The primary attack vector in information leakage is insiders. This term is used to describe a person with an interest to exfiltrate important information on behalf of a third-party entity.

Other common attack vectors used by this threat are misconfigurations and vulnerabilities. For more attack vectors please see the dedicated chapter (chapter 5) in this report.

3.13.6 Specific mitigation actions

The mitigation vector for this threat contains the following elements[347]:

- Avoidance of clear-clear text information, especially when stored or on the move.
- Performance of dynamic analysis of application code, both by means of automated or manually performed code scans and input/output behaviour.
- Performance of static analysis of application code to identify weaknesses in programming. This analysis should be done both for source and object code.

[344] http://www.iisp.gatech.edu/sites/default/files/documents/2017_threats_report_finalblu-web.pdf, accessed November 2017.
[345] https://www.herjavecgroup.com/wp-content/uploads/2017/06/Cybersecurity-trends-2017-survey-report.pdf
[346] https://tld.mcafee.com/exploit_kits.html, accessed November 2017.
[347] https://www.prot-on.com/tips-to-prevent-information-leaks-in-your-company, accessed November 2015.

- Performance of manual code reviews at a certain level of code details, whereas more detailed analysis should be done tool-based.
- Perform classification of processed/transmitted/stored information according to the level of confidentiality.
- Use of technology tools to avoid possible leakage of data such as vulnerability scans, malware scans and data loss prevention tools.
- Identification of all devices and applications that have access/they process confidential information and application of steps above to secure devices and applications with regard to information leakage threats.

3.13.7 Kill Chain

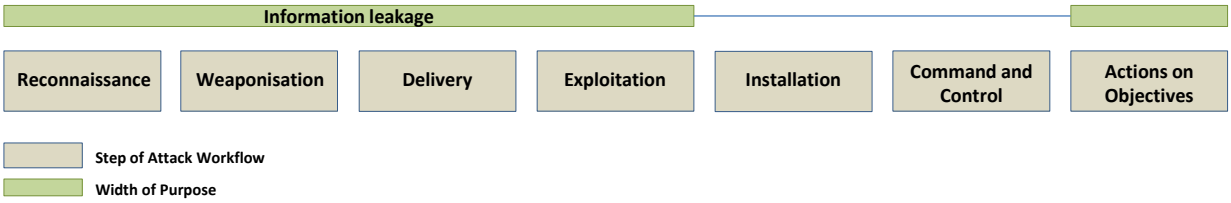

Figure 29: Position Information leakage in the kill-chain

3.13.8 Authoritative references

"Global Data Leakage Report H1 2017", InfoWatch[348]; "2017 Data Breach Investigations Report", Verizon[349]; "Global Cyber Attack Trends 2017", CheckPoint[350]; "Cybersecurity Trends", SpotLight[351].

[348] https://infowatch.com/analytics/leaks_monitoring/request#, accessed November 2017.
[349] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed November 2017.
[350] http://pages.checkpoint.com/global-cyber-attack-trends-2017-11.html?utm_source=blog&utm_medium=cp%20website&utm_campaign=CM_BLG_17Q3_WW_Global%20Trends%20Report%202017%20Blog, accessed November 2017.
[351] https://www.alertlogic.com/resources/industry-reports/cybersecurity-trends-2017-spotlight-report/, accessed November 2017.

3.14 Exploit kits

3.14.1 Description of the cyberthreat

Exploit kits include a collection of ready-made exploits usually planted in compromised websites or used in malvertising campaigns. Exploit kits have the ability to identify exploitable vulnerabilities in a user's browser or web application[352] and automatically exploit them. They often target browser add-ons such as Java and Adobe Flash. Exploit kits have been reduced, but they have not completely gone away. Recent reports suggest that important exploit kit families like Angler, Neutrino, and Nuclear that were once often found in the wild and represented a big part of the threat landscape, will not be used at all in the future. Even if Angler, which dominated the landscape in early 2016 was disrupted, exploit kits as a whole continued to be a threat to unprotected and unpatched IT environments. In 2017, some of the most important malware campaigns (from malvertising to high level attacks), used exploit kits to compromise their targets worldwide[353]. Because exploit kits were and are a reliable tool to deliver malware, it is not a new thing that ransomware continues to use them as infection vectors.

3.14.2 Interesting points

The identified interesting points for exploit kits are as follows:

- The Disdain exploit kit is available for rent on a daily, weekly, or monthly basis for prices starting of $80. A security researcher, has discovered a new version of Disdain that is offered for rent on underground forums by a malware developer using the pseudonym of Cehceny[354].
- Exploit kits have been a threat for a long time, and though recently in decline, they are still an infection vector that should be addressed. Their infection mechanism does not usually require user interaction, and they often compromise an operating system without using a malicious portable executable being run by the browser, thus making detection in early stages very difficult[355].
- One of the most used exploit kits remains RIG -in comparison to others that disappeared or became very localised threats. RIG was used in various campaigns, each of them having different characteristics, thus making it something more than a single threat. This was also supported by the variety of payloads used which included various kinds of ransomware and other kinds of malware.
- Despite including complex filtering mechanisms to hide their malicious activities, threat actors that use exploit kits found that scaling up their attacks can pose many detection risks for the deployed payloads. This may answer why the trend of using exploit kits will decline and exploit kits will be used at a minimum, with mere focus on the geographical regions where they cannot be monitored by researchers[356].
- **Exploit kits will give way to 'human kits'.** As their name says, exploit kits are powered by the existence of reliable exploits for high risk vulnerabilities found in most used applications. Taking into consideration that in the last several years both the total number of disclosed vulnerabilities and

[352] https://blog.malwarebytes.com/threat-analysis/2017/03/exploit-kits-winter-2017-review/, accessed November 2017.
[353] https://blogs.technet.microsoft.com/mmpc/2017/01/23/exploit-kits-remain-a-cybercrime-staple-against-outdated-software-2016-threat-landscape-review-series/, accessed November 2017.
[354] http://securityaffairs.co/wordpress/62021/malware/disdain-exploit-kit.html, accessed November 2017.
[355] https://www.virusbulletin.com/uploads/pdf/magazine/2017/201709-vbweb-comparative.pdf, accessed November 2017.
[356] https://www.proofpoint.com/us/threat-insight/post/cybersecurity-predictions-2017, accessed November 2017.

exploits created for them decreased, cyber criminals changed their business model and implicitly their arsenal in order to achieve their goals by attacking human weaknesses instead.

- **Exploit kits used ransomware as a payload.** A few years ago exploit kits were delivering malware such as downloaders, worms, infostealers and botnets. Since ransomware became more profitable in 2016 and 2017, cyber criminals started using exploit kits to spread them. Namely, Locky, Cerber, CrypMIC, BandarChor, TeslaCrypt ransomware families and others.
- **RIG remains the most active exploit kit.** Even if the overall traffic has been decreasing over the past several months, RIG remains the primary spreading mechanism for various ransomware and it recently started dropping cryptocurrency mining software[357] too.
- **New exploit kit was discovered. Terror EK** includes more sophisticated mechanisms like Metasploit payloads as well as other EKs, most notably Sundown and Hunter. It still uses Sundown exploit packages, though some large changes have been made to the infection cycle[358].
- **The Disdain EK is a brand-new exploit kit that first appeared in early August.** It shares code with Terror EK and uses the same URL pattern, but has also many distinct features. The Disdain campaign is spread using a gate that is also distributing the RIG EK. Many of the gate domains campaign used the format "campngay##" with a two-character top-level domain[359].

3.14.3 Trends and main statistic numbers[360]

- No major changes observed in exploit kit-related infections[361]. This is in part due to the lack of fresh and reliable exploits in today's drive-by landscape. RIG EK remains the most popular exploit kit at the moment used both in malvertising and compromised websites campaigns. Its primary payloads are ransomware. For example, accordingly with research studies[362] the most common malware in March 2017 were HackerDefender and Rig EK in first and second place, each impacting 5% of organizations worldwide, followed by Conficker and Cryptowall, each impacting 4% of organizations worldwide.
- In 2017, we saw that exploit kits increasingly used social engineering. Advanced groups, including those using EKs and malvertising will continue to shift their attention to other attacking tools and will put more effort into social engineering[363].
- Starting in April 2017, a significant decrease in using Rig exploit kit (EK) was seen. After two major campaigns, EITest and pseudo-Darkleech, stopped using EKs[364].
- Based on the exploit kit trends we observed over the last year, exploit kits will continue to be used less frequently on the long term. Most probably the first place will be taken by phishing e-mails containing malicious attachments, and malicious scripts, which have been proven to be very reliable in the past year.

---

[357] https://www.zscaler.com/blogs/research/top-exploit-kit-activity-roundup-spring-2017, accessed November 2017.
[358] https://www.zscaler.com/blogs/research/top-exploit-kit-activity-roundup-spring-2017, accessed November 2017.
[359] https://www.zscaler.com/blogs/research/top-exploit-kit-activity-roundup-summer-2017, accessed November 2017.
[360] https://blog.barkly.com/ransomware-statistics-2017, accessed September 2017.
[361] https://blog.malwarebytes.com/threat-analysis/2017/03/exploit-kits-winter-2017-review/, accessed September 2017.
[362] https://blog.checkpoint.com/2017/04/13/marchs-wanted-malware-list-exploit-kits-rise-popularity/, accessed September 2017.
[363] https://www.proofpoint.com/us/threat-insight/post/cybersecurity-predictions-2017, accessed November 2017.
[364] https://researchcenter.paloaltonetworks.com/2017/06/unit42-decline-rig-exploit-kit/, accessed November 2017.

- Exploit market disruption: The most used exploit kits in the world - Angler, Magnitude and Nuclear declined and even disappeared, leading to a shakeup of the exploit kit market[365].

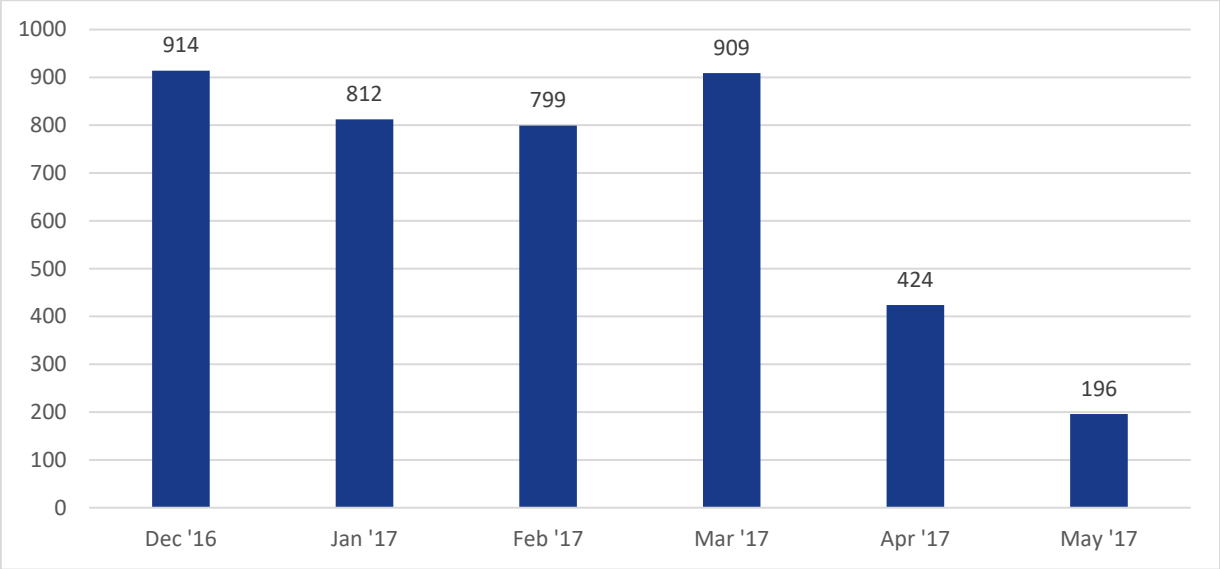

Figure 30: Hits for Rig EK from December 2016 through May 2017

- **The overall trend of exploit kits in 2017 was DECREASING.**

3.14.4 Top 10 exploit kit threats[366]

- **Neutrino Exploit Kit.** Neutrino and its predecessor Neutrino-v are popular exploit kits that appeared increased in mid-2016. They are known for using watering hole and malvertising techniques to infect users with various malware.
- **RIG Exploit Kit.** RIG is spread via suspicious advertisements that have been inserted in compromised legitimate websites. The VIP version of the exploit kit, RIG-v, appeared in 2016 and used new URL patterns.
- **Empire Pack Exploit Kit.** The exploit kit, also referred to RIG-E, appeared in September 2016 and exploited vulnerabilities in Microsoft and Adobe software.
- **Sundown Exploit Kit.** Also referred to as the "Beta Exploit Pack," Sundown is known for distributing remote access Trojans (RATs) using phishing e-mails. Sundown was updated in late 2016 when it started using steganography to conceal its exploit code.
- **Bizarro Sundown Exploit Kit.** The exploit kit was first disclosed in October of 2016 and it is a predecessor of the Sundown exploit kit.
- **Magnitude Exploit Kit.** Also known as Popads, Magnitude used malvertising to infect victims visiting compromised websites.

[365] https://www.trustwave.com/Company/Newsroom/News/2017-Trustwave-Global-Report-Reveals-Cybersecurity-Trends/, accessed November 2017.
[366] https://tld.mcafee.com/exploit_kits.html, accessed November 2017.

- **Terror Exploit Kit.** The exploit kit was discovered in late 2016 and is related to the Sundown exploit kit. Both use similar pieces of code. The main focus of this exploit kit is to turn infected systems into miners for the Monero cryptocurrency.
- **Nebula Exploit Kit**. Nebula, a re-brand of the Sundown exploit kit, is available for rent for $2,000.00 a month on an underground forum and offers support to both Russian and English speaking clients.
- **KaiXin Exploit Kit.** The exploit kit is reported to have origins in China and targets users who visit compromised Korean websites.
- **CK Exploit Kit.** The exploit kit was first undisclosed in 2012 and infected users with drive-by-downloads primarily on Chinese and Korean websites.

3.14.5 Specific attack vectors

The primary infection method with an exploit kit is a drive-by download attack[367]. This term is used to describe a process where one or several pieces of software get exploited while the user is browsing a site.

Exploit Kits in their basic sense introduce malicious code onto a web server allowing an attacker to turn the web server into a mechanism to deliver malicious code[368]. For more information about attack vectors please see chapter 5.

3.14.6 Specific mitigation actions

Exploit kits are infecting systems based on the existence of detected vulnerabilities. Exploit kit themselves are installed as malware. Hence, in addition to the mitigation below, mitigation vector for malware also applies (see chapter 3.1.6 above):

- Performance of updates in a regular basis in orchestration with vulnerability management, especially regarding web infrastructure components.
- Malware detection should be implemented for all inbound/outbound channels, including network, web and application systems in all used platforms (i.e. servers, network infrastructure, personal computers and mobile devices).
- Use of a security e-mail gateway with regular (possibly automated) maintenance of filters (anti-spam, anti-malware, policy-based filtering), as well as content filtering to filter out unwanted attachments, mails with malicious content and spam.
- Follow various vendor good practices[369].

[367] https://blog.malwarebytes.com/threats/exploit-kits/, accessed November 2017.
[368] https://www.sans.org/reading-room/whitepapers/detection/neutrino-exploit-kit-analysis-threat-indicators-36892, accessed November 2017.
[369] http://documents.trendmicro.com/assets/guides/executive-brief-exploits-as-a-service.pdf, accessed November 2017.

3.14.7 Kill Chain

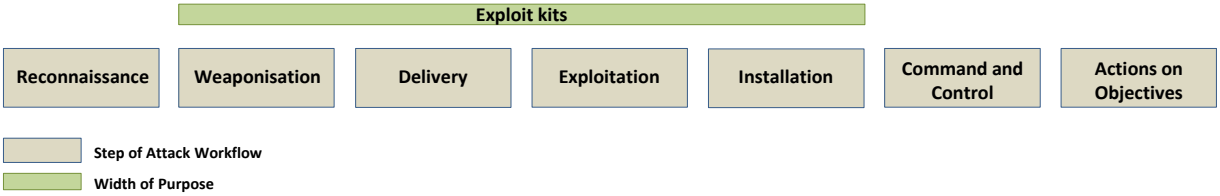

Figure 31: Position of Exploit kits in the kill-chain

3.14.8 Authoritative references

"Cybercrime tactics and techniques Q2 2017", Malwarebytes[370]; "Internet Security Threat Report", Symantec[371]; "2017 Midyear Security Roundup: The Cost of Compromise", Trend Micro[372]; "Ransomware: A declining nuisance or an evolving menace?", Microsoft[373]; "Terror Evolved: Exploit Kit Matures", Talos[374]; "2017 Annual Threat Report", SonicWall[375]

[370] https://www.malwarebytes.com/pdf/white-papers/CybercrimeTacticsAndTechniques-Q2-2017.pdf, accessed November 2017.
[371] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf, accessed November 2017.
[372] https://documents.trendmicro.com/assets/rpt/rpt-2017-Midyear-Security-Roundup-The-Cost-of-Compromise.pdf, accessed November 2017.
[373] https://blogs.technet.microsoft.com/mmpc/2017/02/14/ransomware-2016-threat-landscape-review/, accessed November 2017.
[374] http://blog.talosintelligence.com/2017/05/terror-evolved-exploit-kit-matures.html, accessed November 2017.
[375] https://starcom.tech/wp-content/uploads/2017/05/SonicWall-Threat-Report_Visual-Summary.pdf, accessed November 2017.

3.15 Cyber-Espionage

3.15.1 Description of the cyberthreat

In 2017 a lot of researchers revealed that global organisations consider cyber espionage (one of) the most serious threat to their business[12,376,377]. That's most probable because of the increase of public discussions and media coverage about cyber-espionage. For example, there are several reports about the alleged Russian involvement in the US Democratic National Committee (DNC) breach and their efforts to influence the US presidential election in favour of Donald Trump[378]. Over the next period, cyber experts expect to see a growth in cyber-espionage due to geopolitical triggers, economic sanctions, but also due to strategic nation goals. Bad actors ranging from organised crime to nation-states, are creating new techniques and tools to try and steal intellectual property and secrets. These adversaries usually fall in the category of APTs – Advanced Persistent Threats. APTs represent a collection of processes, tools and resources used by certain groups in order to covertly infiltrate specific networks, remain stealthy in the systems over a long period of time, and exfiltrate data or perform other destructive actions.

3.15.2 Interesting points[379,380]

The identified interesting points for cyber-espionage threat are as follows:

- Cyber-espionage attacks for subversive purposes. For example, attacks during or prior to elections became very important and represent a new form of high-profile targeted attacks.
- The traditional form of targeted attacks - economic espionage has reduced in some cases. For example, Chinese espionage campaigns dropped considerably as a result of a mutual agreement with the US to not target intellectual property.
- Private organisations that are running sensitive activities or support government systems are just as likely to be attacked, as public institutions.
- In the reporting period, less zero-day vulnerabilities have been identified/announced; their place was taken by the penetration testing tools used to identify existing vulnerabilities. Moreover, phishing messages attacking weaknesses (systems, humans) have been used as infection vectors.
- One of the most used tactics in this category is 'denial and deception' –the practice of using a fake identity to get investigators off the trail.
- Nation-states use means to anonymise attacks. This makes attribution extremely difficult.
- State-sponsored hackers are characterized for their dedication and time spent to compromise a specific target.
- Many countries are actively recruiting well skilled security professionals, and a lot of news appear on a daily basis about it: from China's army of hackers, to Ukraine's power grid being taken down by Russian cyber spies etc.

[376] http://newsroom.trendmicro.com/press-release/company-milestones/cyber-espionage-tops-list-most-serious-threat-concern-global-busine, accessed December 2017.
[377] https://www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf, accessed November 2017.
[378] https://www.theguardian.com/us-news/2017/jun/23/obama-cia-warning-russia-election-hack-report, accessed December 2017.
[379] http://www.information-age.com/state-sponsored-hacking-123462535/, accessed November 2017.
[380] http://www.information-age.com/cyber-threat-new-face-espionage-123462346/, accessed November 2017.

3.15.3 Trends and main statistic numbers[381]

- 20% of global organisations consider cyber espionage the riskiest threat to their business, with a quarter (26%) struggling to keep up with the rapidly evolving threat landscape.
- 20% of US companies have suffered a cyber-espionage attack in past year.
- **The overall trend of cyber espionage in 2017 was INCREASING.**

3.15.4 Top cyber espionage attacks[382]

- Called **CopyKittens (aka Rocket Kittens)**[383], this cyber espionage group has been active since at least 2013 and targeted organisations and individuals, including diplomats and researchers, from Israel, Saudi Arabia, Turkey, the United States, Jordan and Germany. Last year a new espionage campaign - dubbed **"Operation Wilted Tulip"**[384]**-** was identified of being conducted by this group**.**
- **APT33**[385] cyber espionage group attacks in 2017: in September 2017, it was discovered that this group was behind the alleged spying of companies from the US, Middle East, and Asia. Most of the companies are connected to the petrochemical industry, military, and commercial aviation.
- **APT32**[386] (OceanLotus Group) is a Southeast Asian cyber espionage group threatening multi-national companies operating in Vietnam. In 2017, it was discovered that this group conducted a campaign against two subsidiaries of US and Philippine consumer products corporations, located in Vietnam.
- **APT28**[387] (also known as, Fancy Bear, Pawn Storm, Sofacy Group, Sednit and STRONTIUM) is a cyber-espionage group most probable sponsored by the Russian government. Recently, a new campaign was uncovered being conducted by this group in early July, against multiple companies in the hospitality industry, including hotels in at least seven European countries and one Middle Eastern country.
- **APT29**[388] known also as Cozy Bear, is a Russian hacker group believed to be associated with Russian intelligence. In 2017, it was identified that this group targeted a couple of public institutions from Norway: Ministry of Defence, Ministry of Foreign Affairs, and the Labour Party. Also, it was identified that Dutch ministries, including the Ministry of General Affairs, were targeted by this group in 2017.
- **APT17**[389] is a China-based threat group that has conducted network intrusions against U.S. government entities, the defence industry, law firms, information technology companies, mining companies, and non-government organisations. Researchers speculate that the **CCCleaner** attack was powered by a nation-state actor, likely the Chinese APT17 group.

---

[381] http://newsroom.trendmicro.com/press-release/company-milestones/cyber-espionage-tops-list-most-serious-threat-concern-global-busine, accessed November 2017.
[382] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ec, accessed November 2017.
[383] https://thehackernews.com/2017/07/opykittens-cyber-espionage.html, accessed November 2017.
[384] http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf, accessed November 2017.
[385] Advanced Persistent Threat 33 (APT33) is a hacker group identified by FireEye as being supported by the government of Iran, accessed November 2017.
[386] https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html, accessed November 2017.
[387] https://en.wikipedia.org/wiki/Fancy_Bear, accessed November 2017.
[388] https://en.wikipedia.org/wiki/Cozy_Bear, accessed November 2017.
[389] https://attack.mitre.org/pre-attack/index.php/Group/PRE-G0025, accessed November 2017.

3.15.5 Specific attack vectors

In cyber espionage attacks, threat agents often use complex pieces of malware. But in most cases common spreading and infecting methods, e.g. phishing, are used. For more details about attack vectors please see chapter 5.

3.15.6 Specific mitigation actions

Due to the comprehensive nature of this threat, it would contain several mitigation measures found in other threats of this report. Following advice found[390], baseline mitigation controls for this threat are:

- Identification of mission critical roles in the organisation and estimation of their exposure to espionage risks. Based on business information (i.e. business intelligence), risks to businesses and level of espionage risks are being evaluated.
- Creation of security policies that accommodate human resource, business and operational security controls to cater for risk mitigation regarding loss of human resources and business assets. This will include rules and practices for awareness raising, corporate governance and security operations.
- Establishment of corporate practices to communicate, train and apply the developed rules and keep operational parts defined up and running.
- Development criteria (KPIs) to benchmark the operation and adapt it to upcoming changes.
- Depending on the risk level assessed, whitelisting for critical application services should be developed.
- Vulnerability assessment and patching of used software should be performed regularly, especially for systems that are in the perimeter, such as web applications, web infrastructure and office applications.
- Implementation of need to know principle for access rights definition and establishment of controls to monitor misuse of privileged profiles.
- Establishment of content filtering for all inbound and outbound channels (e-mail, web, network traffic).

3.15.7 Kill Chain

Kill chain is not relevant for this threat: this is a “composite” threat, that is, consisting of many cyberthreats spanning the entire phases of the kill chain, just as Data Breaches (see chapter 3.11.7).

3.15.8 Authoritative references

“Internet Security Threat Report”, Symantec[391]; “APT Trends report Q3 2017”, Securelist[392]; “McAfee Labs 2017 Threats Predictions”, McAfee[393]; “Cyber Espionage Tops the List as Most Serious Threat Concern to Global Businesses in 2017”, Trend Micro[394]; “Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations”, FireEye[395].

---

[390] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf, accessed September 2017.
[391] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf, accessed November 2017.
[392] https://securelist.com/apt-trends-report-q3-2017/83162/, accessed November 2017.
[393] https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf, accessed November 2017.
[394] http://newsroom.trendmicro.com/press-release/company-milestones/cyber-espionage-tops-list-most-serious-threat-concern-global-busine, accessed November 2017.
[395] https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html, accessed November 2017.

3.16 Visualising changes in the current threat landscape

This chapter provides a visualization of the changes assessed in 2017's landscape in comparison to the one of the previous year (see Figure 32). Besides changes in ranking, the figure also displays the trends identified for each threat. The interesting phenomenon of having some threats with stable or decreasing trend climbing up the ranking, is mostly due to the fact that, albeit stagnation/reduction, the role of this threat in the total landscape has grown, for example through volume of infections, identified incidents, breaches attributed to the threat, etc. Similarly, other threats with increasing trend are lowered in the ranking. This is due to threats climbing to higher positions of the ranking, inevitably leading to lowering all other threats below.

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware		→
2. Web based attacks	↑	2. Web based attacks		→
3. Web application attacks	↑	3. Web application attacks		→
4. Denial of service	↑	4. Phishing		↑
5. Botnets	↑	5. Spam		↑
6. Phishing	➲	6. Denial of service		↓
7. Spam	↓	7. Ransomware		↑
8. Ransomware	➲	8. Botnets		↓
9. Insider threat	➲	9. Insider threat		→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss		→
11. Exploit kits	↑	11. Data breaches		↑
12. Data breaches	↑	12. Identity theft		↑
13. Identity theft	↓	13. Information leakage		↑
14. Information leakage	↑	14. Exploit kits		↓
15. Cyber espionage	↓	15. Cyber espionage		→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 32: Overview and comparison of the current threat landscape 2017 with the one of 2016.

4. Threat Agents

4.1 Threat agents and trends

The developments in the area of threat agents/actors has advanced in analogy to the developments of the entire threat landscape: complexity, sophistication and advancements in capabilities have been observed for most of the threat agent groups. While the race between good and bad guys continues, advancements in obfuscation and masquerading of threat agents make it more difficult to understand who-is-who. This difficulty has led to an alerting phenomenon: the user community cannot differentiate between the bad and the good, thus loosing trust to commercial and even institutional players in cyber-space[396,397].

By looking at the trends/advancements of threat agents, it is noticeable that:

- Threat agents have permanently tried to pretend to belong to another group than the genuine one. In 2017 we have seen masquerading techniques[398] to be omnipresent in many campaigns. In the meantime, they can be considered as a standard practice for almost all threat agent groups. Some simple techniques such as: imitating origin, imitating intention, smokescreens, use of similar tools[399] and code segments, are typical examples[407] hereof.
- Threat agent masquerading at various levels of sophistication have been assessed. Expectedly, state sponsored actors are best in fooling researchers about their actual motives/origin.
- While responsible disclosure has reduced the number of zero-day vulnerabilities, there is evidence that both low and high capability actors are very active in the discovery of zero-day vulnerabilities that allow them to successfully exploit their targets[400],[401].
- Evasion techniques advanced too: more and more malicious attacks make use of anonymity platforms, use of strong encryption and stealth functions (file-less, sand-box evasion, sophisticated code obfuscation).
- If combined with capabilities such as dissemination of fake news and influence of people through social media campaigns, existing attack obfuscation methods may turn attribution almost impossible, at least for advanced threat agents.
- There are still too few investigations on the kill chain phase “actions on objectives”, meaning that the final exploitation (i.e. the finally exploited asset) is in most of the cases remains unclear. This hinders identification of final intention/motivation and thus the profiling activities of threat agent groups.

From the defender’s side, one should appraise advancement achieved, such as:

[396] http://limn.it/whos-hacking-whom/, accessed November 2017.
[397] http://www.nybooks.com/daily/2017/07/19/hacking-the-vote-trump-russia-who-helped-whom/, accessed November 2017.
[398] https://theintercept.com/2017/10/04/masquerading-hackers-are-forcing-a-rethink-of-how-attacks-are-traced/, accessed November 2017.
[399] http://www.zdnet.com/article/hackers-are-re-using-free-online-tools-as-part-of-their-cyber-espionage-campaigns/, accessed November 2017.
[400] https://cybersecurityventures.com/zero-day-vulnerabilities-attacks-exploits-report-2017/, accessed November 2017.
[401] https://www.schneier.com/blog/archives/2017/07/zero-day_vulner.html, accessed November 2017.

- In the reporting period (and slightly before) the notion of threat agent has been further addressed, noticeably by some very detailed and well written resources[402,403,404,405,406,407].
- Threat agents becomes an important counterpart of thematic assessments[408]. This will lead to more detailed threat agent models and will contribute to improvement of protection. It is worth mentioning, that threat agent groups are the central element for developing defences (e.g. protection from Russian cyber-criminal groups).
- Law enforcement has demonstrated some sophisticated, yet risky ways to prosecute cyber-criminal offences by launching or taking over operation of market places in the darknet[409]. For the first time we have seen reports about take-overs/masquerading campaigns from law enforcement with the objective to get multiple threat agent groups. The objective was to use vacuums in underground markets to catch sellers and consumers of illegal stuff. The Dutch police –for example – in order to catch illegal sellers and buyers, has introduced and operated a dark market known as Hansa Market, right after the takedown of Alpha Market in June 2017[410].
- While vulnerability discovery is being performed by a bigger number of actors in cyber-space, the practice of adopting responsible disclosure has reduced the number of zero-day vulnerabilities.
- It has been observed that various additional criteria for the assessment of the threat agents have been mentioned in published reports. Aspects like activity time window, comparison to diplomatic and political activities/tensions, commercial interests and geopolitical issues are taken into account[411].

The above mentioned points largely demonstrate the trends in CTI with regard to the threat agents:

- Though threat agents are ahead of defenders, threat agent profiling has not yet enjoyed the attention it deserves in CTI.
- The gap between low and high capability threat agents seem to increase. This has been already assessed in various surveys, where defenders classify high capability agents as the most prevalent threat in cyber-space.
- Through the entrance of additional high capability actors in the cyber-space, it is expected that the above mentioned observations/trends will be further amplified.

---

[402] https://www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf, accessed November 2017.
[403] https://cdn.securelist.com/files/2016/10/Bartholomew-GuerreroSaade-VB2016.pdf, accessed November 2017.
[404] https://www.f-secure.com/documents/996508/1030745/callisto-group, accessed November 2017.
[405] https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/, accessed November 2017.
[406] https://www.swiftinstitute.org/wp-content/uploads/2017/10/SIWP-2016-004-Cyber-Threat-Landscape-Carter-Final.pdf, accessed November 2017.
[407] https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2017.html, accessed November 2017.
[408] https://www.safety4sea.com/wp-content/uploads/2017/09/UK-Cyber-Security-Code-of-Practice-for-ships-2017_09.pdf, accessed November 2017.
[409] http://www.dw.com/en/norwegian-newspaper-reveals-australian-police-ran-child-porn-site-childs-play-for-11-months/a-40865610, accessed November 2017.
[410] https://krebsonsecurity.com/2017/07/after-alphabays-demise-customers-flocked-to-dark-market-run-by-dutch-police/, accessed November 2017.
[411] https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html, accessed November 2017.

- The lack of human resources and transparency in threat agent engagement may amplify the movements of threat agents among the various groups, especially the high capability ones (i.e. state-sponsored, cyber-criminals, researchers, law-enforcement).

Some of the above points are taken up in the conclusions of this report (see chapter 6.2).

4.2 Top threat agents and motives

In this chapter we present an outline of top threat agent groups. It includes observations about their motives and main trends assessed with regard to their capabilities. This is a complementary view to the threat assessments (including tools, methods and tactics) presented within the top cyber-threats (see chapter 3) and the attack vectors (see chapter 5).

Just as in previous threat landscapes, we consider the following threat agents' groups: cyber-criminals, insiders, cyber-spies, hacktivists, cyber-offenders, cyber-fighters, cyber-terrorists and script-kiddies. It should be noted that the sequence of mentioning is according to their engagement in the threat landscape[412,413].

The assessed cyber threat agent groups are as follows:

In 2017, **Cyber-criminals** remained the most active threat agent group in cyber-space, being responsible for at least two third of the registered incidents[412]. They demonstrated very firm activity towards monetization. This has been manifested by the concentration on quite narrowly targeted ransomware attacks to victims with high monetization potential. Consequently, a concentration of high value victims has been manifested by an increase of incidents and data breaches in the business sector[414]. Instead of starting massive attacks to wide user segments with low end malicious tools, threat agents proceed with selection of high value targets and tailor their artefacts to those attacks. The massive increases of spear fishing attacks and advancements in relevant attacks are a clear indication towards this trend (whaling[415], attacks based on google searches[416]). Despite the ransomware trend in 2017, cyber-criminals continued with more "traditional" fraudulent activities: ad-fraud remains at high levels as a low risk with fairly good turnovers[417]. Cyber-crime makes significant income from related services that are sold as "Crime-as-a-Service". These are based on breached data. The permanent increase in data breaches for a consecutive year is a clear indication for the interest of cyber-criminals in monetizing stolen information[418]. As regards the monetisation actions of this threat agent group, there have been some important developments, summarized nicely by this source[419]. As a final note in this short assessment, one should mention alleged intensive interactions among cyber-criminals and cyber-spies[420]. An outstanding piece of threat agent

[412] http://www.hackmageddon.com/, accessed November 2017.
[413] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed November 2017.
[414] http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReportSummary_2017.pdf, accessed November 2017.
[415] https://www.csoonline.com/article/3234716/phishing/types-of-phishing-attacks-and-how-to-identify-them.html, accessed November 2017.
[416] http://www.spyware-techie.com/zeus-panda-trojan-spreads-through-google-search?utm_source=hs_email&utm_medium=email&utm_content=58308840&_hsenc=p2ANqtz--2nxbblBq0U3oBDBs4xmmZS3Nymyg8KWgt-20bJZhVWaQJJf5X5KAy3XHSm581Zq27eySy-I5w6ZFMCC_Rm_u8WikfDzISKy85i-WS5atS1twCZNk&_hsmi=58308840, accessed November 2017.
[417] https://insider.integralads.com/monetising-ad-fraud-fraudsters-perspective/, accessed November 2017.
[418] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf, accessed November 2017.
[419] https://www.rsaconference.com/writable/presentations/file_upload/spo2-r11_the-malware-monetization-machine.pdf, accessed November 2017.
[420] https://www.theregister.co.uk/2017/10/05/fog_of_cyberwar/, accessed November 2017.

assessment w.r.t. WannaCry[405] seen in the context of recent investigations[421] is indicative for the fuzziness in the interaction of threat agent groups.

Insider threat (see also description as cyber threat) and with it the corresponding threat agent group **insider** score quite high in the threat landscape 2017[422]. This is similar to the developments in 2016: while insiders score quite high in the perception of defenders[423], we see in 2017 for the first time evidence that malicious insider activity has declined[424]. This decline concerns both inadvertent and intentional actions. Just as it is the case with cyber-criminals, insiders aim primarily at financial gain: they try to monetize their malicious activities, both directly and/or indirectly by selling them in dark markets. Insiders (both intentional and inadvertent) have the lion's share in the financial and health care sectors[425] with 58% and 71% of incidents respectively. In the case of inadvertent insider threat agents, it is necessary to consider compromised accounts or end-points that have been infected and are controlled by other threat agents (merely criminals and state-sponsored agents). The high percentages of inadvertent actions can also be explained via the increased exposure of this group to spear phishing attacks, in particular within the reporting period[425]. This fact needs to be seriously taken into account and eventually be attributed to the threat agent group that is behind such attacks. This will help defenders in the definition of more efficient mitigation controls towards activities of this threat agent group. Another very interesting aspect regarding this threat agent group is an analysis for the reasons leading to high exposure levels[422]: in order to speed up with productivity, insiders tend to neglect security policies. As a result, they stay logged on for long time, send files to personal accounts, they are writing down passwords and store data on media that are external to the organisation.

According to reported incidents in 2017 **Nation States** have become the third most active threat agent group with over 20% of incidents[413,412]. Given the advanced capabilities of this group, performed attacks are often difficult to identify and defend. This means that it is very likely that the actual activity of this group may be much higher as indicated by the incident statistics. The fact that states are increasingly developing cyber-capabilities contributes to a higher activity of this threat agent group[426,427,428]. As regards the targets of state-sponsored activities, manufacturing and public administration top the list. This reflects the genuine interest of nation states in industrial espionage and state secrets[413]. This threat agent group plays an important role in the cyber-space: they invest heavily in cyber-attack tools[429], while promoting innovative approaches for both attack methods and defences. In the reporting period there has been strong evidence that state-sponsored actors have used for a long time zero-day vulnerabilities[430,431,]. Let alone speculations about involvement of nation-states in identified vulnerabilities[432]. These developments are reflected in the expectations of defenders: Blackhat attendee survey shows that state sponsored actors

[421] http://www.independent.co.uk/news/world/asia/north-korea-responsible-wannacry-ransomware-microsoft-brad-smith-cyber-attack-nsa-a8000166.html, accessed November 2017.
[422] https://www.bomgar.com/resources/whitepapers/secure-access-threat-report, accessed November 2017.
[423] https://www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf, accessed November 2017.
[424] https://www2.trustwave.com/2017-Trustwave-Global-Security-Report.html, accessed November 2017.
[425] https://www.ibm.com/security/data-breach/threat-intelligence, accessed November 2017.
[426] https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/, accessible November 2017.
[427] http://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/, accessed November 2017.
[428] https://www.cybersecurityintelligence.com/blog/which-countries-are-ready-for-cyberwar-2763.html, accessed November 2017.
[429] https://wikileaks.org/vault8/, accessed November 2017.
[430] https://wikileaks.org/ciav7p1/cms/, accessed November 2017.
[431] https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance, accessed November 2017.
[432] http://www.zdnet.com/article/nsa-krack-vulnerability-security-experts/, accessed November 2017.

are rather the most feared cyber-attackers. In this category we subsume zero-day vulnerably (20%), high sophisticated attack skills (11%) and strong backing/financing by organized crime or nation-states (17%)[423]. Concluding the assessment of this threat agent group one has to mention recent allegations for mutual espionage campaigns based on Kaspersky's anti-virus software[433]. Though such activities are assumed to exist since years, in 2017 it has been used as an argument to ban Kaspersky products from US public authorities/government[434]. This dispute has created a great deal of discussions and analysis in the cybersecurity domain[435,436] and is indicative for the big role of cyber-espionage in all domains, from commerce to politics to diplomacy.

Hacktivists have had remarkable activity in 2017. Triggered by some political events, hacktivists have performed defacement and data theft/leakage campaigns against primarily governments/public sector organisations and companies. This threat agent group is in the top 5 security issues at the attention of defenders[423]. In this threat agent group individuals of various levels of capability can be found[437]. As regards their activities, they concentrate on defacement, propaganda and media attractive DDoS attacks[39]. It is assumed that this threat group uses available Cyber-Crime-as-a-Service (CCaaS) offerings for their attacks. This group has a rather clear motive for attacks, this being political motivation. Expectedly, this motive attracts other threat agents - in particular nation-states – who often use the hacktivist/anonymous facade to achieve political objectives[403]. An important resource found on financial threat landscape argues that hacktivists threat is considered as being very low for banks, either because sophisticated hackers have seen that the risk of hacktivist is too high for the impact achieved; or because the generation with the available skills has concentrated in other lucrative activities and do not want to risk being caught just for political protest[438]. Besides some interesting successful attacks in Vietnam[439], major hacktivist activity in this year is still ongoing and has connected with the independency movement in Catalonia[440,441], with political developments in Turkey[442] and some minor protest in Greece[443].

Cyber-fighters remain in the landscape being nationally or religiously motivated groups[403,408]. Given the developments in Syria and the refugee crisis, it is considered likely that radicalized individuals may create tensions in ethnical communities. Those, in turn, may start malicious activities in the cyberspace. Yet, reports see them as mingling with supporters of terrorist groups, extremist activists[403], but also supporting

---

[433] https://www.technologyreview.com/the-download/609100/israeli-spies-spied-russian-spies-spying-on-american-spy-plans-via-kaspersky/, accessed November 2017.
[434] https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152_story.html?utm_term=.440345781d1d, accessed November 2017.
[435] https://www.reuters.com/article/us-usa-cyber-kaspersky-congress/about-15-percent-of-u-s-agencies-found-kaspersky-lab-software-official-idUSKBN1DE28P, accessed November 2017.
[436] https://securelist.com/investigation-report-for-the-september-2014-equation-malware-detection-incident-in-the-us/83210/, accessed November 2017.
[437] https://security.radware.com/ddos-knowledge-center/ddos-chronicles/anatomy-of-a-hacker/, accessed November 2017.
[438] https://www.swiftinstitute.org/papers/forces-shaping-the-cyber-threat-landscape-for-financial-institutions/, accessed November 2017.
[439] http://news.softpedia.com/news/chinese-hacktivists-attack-vietnamese-airports-506778.shtml, accessed November 2017.
[440] https://www.washingtonpost.com/news/democracy-post/wp/2017/10/18/the-great-catalonian-cyberwar-of-2017/?utm_term=.576805622abb, accessed November 2017.
[441] https://twitter.com/UnitedSecAnon/status/932762199843536896, accessed November 2017.
[442] https://latesthackingnews.com/2017/06/24/20749/, accessed November 2017.
[443] http://greece.greekreporter.com/2017/09/27/anonymous-boasts-of-hacking-bank-of-greeces-confidential-documents/, accessed November 2017.

nation-states that still support their political opinions[408]. All these opinions are definitely valid and reflect the blurriness in the identification of interactions among various threat agent groups. This situation explains also the variety in motives and capabilities that have been assessed for such groups. Their activities range from defacements and DDoSing (i.e. just as hacktivists)[444,445] to more sophisticated hacking campaigns[446],[447] (i.e. similar to nation-states activities). Some argue that the capabilities of Islamic cyber-fighters are rather low[448] and that Syrian Electronic Army has disbanded during the Syrian war[449]. A typical government affiliated group is the Iranian Cyber Army that has quite long activity record in cyberspace[450].

Cyber-terrorism is a motive that is often part of the security policy of relevant organisations such as public organisations, industries, critical sectors, etc. Yet, threat assessments published in 2017 downplay the threat emanating from terrorist activities in cyberspace, merely because cyber capabilities of terrorists are assumed to be rather low[451]. As far as jihadist activities in cyberspace is concerning, there is not more than activities of ISIS sympathising groups. Those are more of the hacktivist type as described above, thus covering mainly defacements and DDoS attacks. Going beyond hacking activities, it assumed that cyber-terrorists are interested in developing capabilities in cryptocurrencies, just because the need means to hide their funds from the international financial system and perform money laundering[451]. Moreover, terrorists may be interested in using dark markets to purchase cyber-crime services, weapons[452], drugs[453], etc. As a final note it should be mentioned that terroristic cyber-threat may emerge from other groups politically extremist group such as nationalistic and left extremists[454].

The threat agent group **script kiddies** has been addressed in 2017 assessments mostly for completeness reasons. Though theoretically some threats can originate from this group, due to its low capabilities, and average motivation, they usually do not go beyond simply structured, low impact cyber-attacks[32]. This threat agent group, however, may be interesting to consider when analysis vitas of hackers from other threat agent groups: he example of Marcus Hutchings[405] demonstrates how a scrip kid activity may mature to a full-fledged attack. Equally interesting is the potential of this threat agent group when misusing available hacking tools[455]. It is important that society offers interested teenagers the possibility to channel potential interest in cyber-space through cyber-challenges. Just as in previous years, such challenges have

[444] http://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html, accessed November 2017.
[445] http://www.zone-h.org/archive/notifier=Southern%20Yemen%20Cyber%20Army?zh=1, accessed November 2017.
[446] https://www.vice.com/sv/article/avnbv4/speaking-with-the-sea-about-hacking-the-onions-twitter-account, accessed November 2017.
[447] https://motherboard.vice.com/en_us/article/mgbn58/this-is-how-the-syrian-electronic-army-hacked-the-washington-post, accessed November 2017.
[448] http://www.newsweek.com/isis-cyber-jihadis-are-garbage-hacking-top-researcher-says-670972, accessed November 2017.
[449] https://intelligenceobserver.com/2017/02/26/syrian-electronic-army-highly-likely-disbanded-in-2016/, accessed November 2017.
[450] https://thebuckleyclub.com/the-rising-iranian-cyber-threat-15028b76e0f9, accessed November 2017.
[451] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf, accessed November 2017.
[452] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017, accessed November 2017.
[453] https://www.thesun.co.uk/living/3688057/captagon-isis-drug-chemical-courage-sleep-disorders-terrorists/, accessed November 2017.
[454] https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2016, accessed November 2017.
[455] https://www.theregister.co.uk/2017/04/21/windows_hacked_nsa_shadow_brokers/, accessed November 2017.

been organized with great success. ENISA is involved in the EU-Cyber Challenge that is one of the biggest in Europe[456].

Some of the above points are taken up in the conclusions of this report (see chapter 6.2).

4.3 Threat Agents and top threats

The involvement of the above threat agents in the deployment of the identified top cyber-threats is presented in the table below (see Table 2). The purpose of this table is to visualize which threat agent groups are involved in which threats. This information is targeted towards stakeholders who are interested in assessing possible threat agent involvement in the deployment of threats. This information might be useful in identifying the capability level can be assumed behind the top threats and thus support in decisions concerning the strength of the security controls that are implemented to protect valuable assets. The table below is very similar to the one of ETL 2016[49], apart from some minor changes/adaptations based on the engagement of threat agents in 2017's incidents.

The table visualizes the various capability levels of various threat agent groups: threat agents who are the source of many primary threat actions are the ones with higher capabilities, while with ones with more secondary or no cyber-threat assignment are possess lower capabilities.

[456] https://www.europeancybersecuritychallenge.eu/index.html, accessed November 2017.

	THREAT AGENTS							
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-fighters	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓		✓
Phishing	✓	✓	✓	✓	✓	✓		
Spam	✓	✓	✓	✓				
Ransomware	✓	✓	✓	✓		✓		✓
Insider threat	✓		✓	✓		✓	✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓		✓	✓
Exploit kits	✓		✓	✓		✓		
Data breaches	✓	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓		✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓		✓		

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

Table 2: Involvement of threat agents in the top cyber-threats

In this table we differentiate between threats that are typically deployed through a group (primary group of a threat) and threats that are secondarily deployed by a group. This differentiation is being graphically through the colours of the check symbols in the table (see also Legend in Table 2).

5. Attack Vectors

5.1 Introduction

"The deployment of the different cyber threats assessed in the previous chapters is done by the use of one or more attack vectors. *Specifically, an **attack vector** is a means by which a threat agent can abuse of weaknesses or vulnerabilities on assets (including human) to achieve a specific outcome"*[457].

The description of an attack vector is important in order to understand the various cyber threats, tactics, techniques and procedures (TTP) used by threat agents that were described earlier. It also provides defenders the opportunity to implement appropriate defences.

In this ETL report the main attack vectors identified in various security incidents have been categorised (see 5.2). Despite the list below is extensive it is not exhaustive. Out of the identified attack vectors, five common attack vectors are analysed. Namely "*Attacking the human element", "web and browser based attack vectors*", "*Internet exposed assets*", "*Exploitation of vulnerabilities/misconfigurations and cryptographic/network/security protocol flaws*", and "*Supply-chain attacks*".

For each attack vector, we present a brief description, introducing the attack vector. Then, we present security incidents involving this attack vector, setting the context around it and we pinpoint to cyber threats related with the respective attack vector.

5.2 Attack vectors taxonomy

Below is a categorisation of attack vectors:

1. **Attacking the human element**
   - Social engineering
   - Phishing/spear-phishing/business email compromise(BEC)/whaling/spam through e-mail/social media/online services
     - Malicious attachments in e-mails
     - Malicious URLs in e-mails and social media
     - Microsoft office attack vectors (macros etc)
   - Scams
     - Customer/tech support scams
     - Phone scams (Vishing)
     - SMS scams (Smishing)
   - Social media/public Internet information gathering
2. **Web and browser based attack vectors**
   - Drive-by downloads
   - Drive-by mining (cryptojacking)
   - Malicious scripts/URLs
   - Exploit-kits
   - Malvertising
   - Web application attacks (SQL injection)
   - Browser based attacks

[457] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

- Malicious browser add-ons (updates)
- Compromised/fake websites

3. **Internet exposed assets**
   - Unprotected assets exposed on the internet
   - Default/weak service credentials
   - Password reuse
4. **Exploitation of vulnerabilities/misconfigurations and cryptographic/network/security protocol flaws**
5. **Supply-chain attacks**
6. **Network propagation/lateral movement**
7. **Active network attacks**
   - DNS attacks (DNS hijacking/poisoning)
8. **Passive network attacks**
   - Wifi-Sniffing
9. **Data leakage**
10. **Smokescreen attacks**
11. **Mobile app stores**
12. **Malicious USB devices**
13. **Card skimming**

5.3 Attacking the human element

The human element poses one of the most significant attack vectors. Threat agents aim to exploit people through social engineering attacks, phishing, spear-phishing/BEC/whaling attacks delivered via e-mail, social media and Internet services, online scams, social media and public information gathering etc. Phishing is usually the first step in most cyber-attacks before gaining foothold into a system or stealing data. Examples of how phishing is used as an attack vector are illustrated in the figure below:

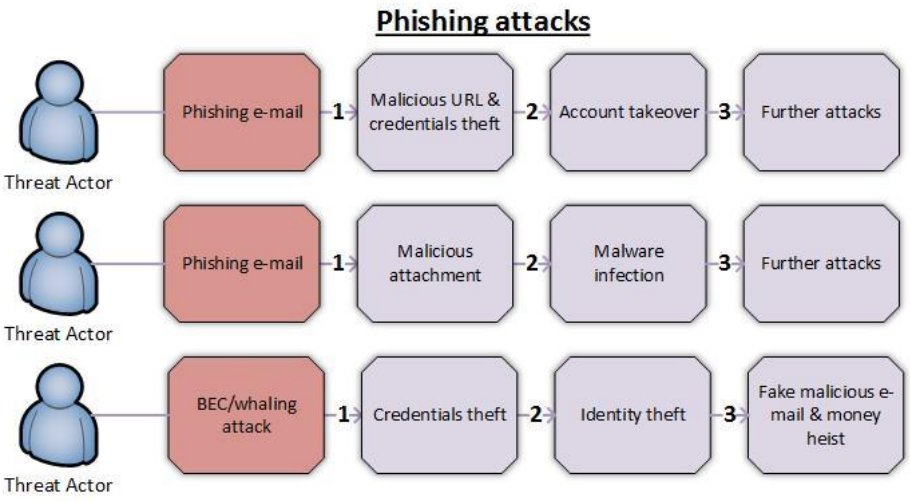

Figure 33: Examples of phishing attacks[458]

Example security incidents related to this attack vector:

[458] https://www.enisa.europa.eu/publications/info-notes/phishing-on-the-rise

- E-mails pretending to come from a bank delivered the banking Trojan Trickbot via a malicious attachment[459]. This is a very common scenario of delivering malware and ransomware. The e-mails are usually very well constructed and compelling, thus they often manage to deceive people.
- Tech support scams rely on social engineering: They use fake error messages to trick users into calling hotlines and paying for unnecessary tech support services or downloading malware. One of the latest trends in this area is the use of websites that automatically open the default phone call app of a mobile device with the phone number ready to be dialled[460].
- A fake WhatsApp application with 1 million downloads was found in Google's play store[461]. The malicious app appeared to have been developed by WhatsApp Inc, the legitimate owner of the app but in fact it wasn't. The threat agent behind the app managed to deceive the users by adding a hidden space (in Unicode) at end of the company's name, masquerading the app as a WhatsApp Inc app. Similar deception techniques have been used in phishing attacks[462].

Related cyber threats:

Phishing, Spam, Malware, Ransomware, Data Breaches, Identity Theft

5.4 Web and browser based attack vectors

Web is a major attack vector for threat agents. Compromised/fake websites delivering exploit kits, drive-by downloads, malicious advertisements or cryptomining scripts[463] are only a few of the common web attack vectors. In most cases threat agents seek to infect user systems with ransomware and malware, steal data and sensitive information, or abuse their system resources. Moreover, browser based attacks that include malicious browser add-ons[464] are also a common attack vector. A simple malvertising attack, which is a widely used attack vector for delivering malware is illustrated below:

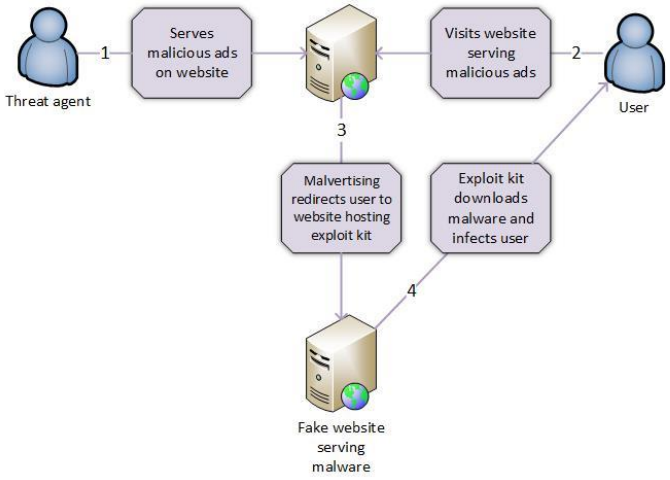

Figure 34: A malvertising attack

[459] https://myonlinesecurity.co.uk/more-fake-natwest-emails-deliver-trickbot-banking-trojan/
[460] https://blogs.technet.microsoft.com/mmpc/2017/11/20/new-tech-support-scam-launches-communication-or-phone-call-app/
[461] https://www.theregister.co.uk/2017/11/03/fake_whatsapp_app
[462] https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers
[463] https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser
[464] https://www.enisa.europa.eu/publications/info-notes/malware-in-browser-extensions

Example security incidents related to this attack vector:

- A malvertising campaign was used to redirect browsers to malicious websites that hosted the Terror exploit kit[465] and served a Trojan. Another malvertising campaign has been used to deliver Matrix ransomware[466]. A slightly different malvertising campaign redirected users to a fake page urging them to download a browser or a Flash update but instead served them Kovter, a multipurpose malware dropper[467].
- A new attack vector that is used in Q4 of 2017 is cryptojacking[463], i.e. the unauthorised execution of cryptomining scripts in browsers. Threat agents are using cryptojacking as an attack vector in order to mine cryptocurrency coins by exploiting user system resources instead of using their own.

Related cyber threats:

Exploit kits, malware, ransomware, web application attacks, phishing, data breaches

5.5 Internet exposed assets

Threat agents systematically target Internet exposed services that are unprotected or ill-protected and use them as an attack vector to steal data, deliver malware, or perform ransom attacks[468]. Misconfiguration and negligence are often the reasons behind the unprotected and Internet exposed services. At the same time, password reuse, default/weak passwords are also well-known attack vectors that are leveraged by threat agents. Examples of attacks against Internet exposed services as well as password reuse attacks are illustrated below:

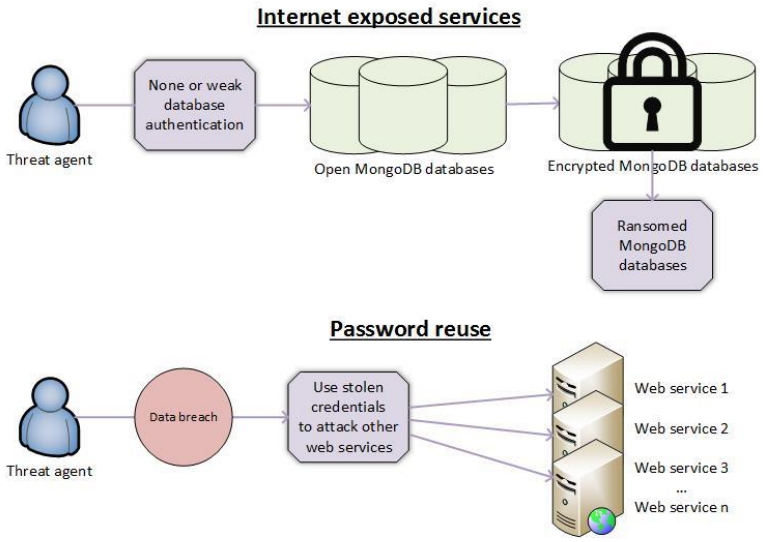

Figure 35: Ransom attacks against MongoDB Databases, password reuse

Example security incidents related to this attack vector:

[465] https://threatpost.com/malvertising-campaign-redirects-browsers-to-terror-exploit-kit/
[466] http://securityaffairs.co/wordpress/64920/malware/matrix-ransomware-malvertising.html
[467] https://www.bleepingcomputer.com/news/security/malvertising-group-spreading-kovter-malware-via-fake-browser-updates/
[468] https://www.enisa.europa.eu/publications/info-notes/ransom-attacks-against-unprotected-internet-exposed-databases

- Several cases of unprotected online storage buckets have been identified, potentially leading to serious data breaches. Anyone could have access to these data buckets by simply entering the appropriate URL address in their browser. The leaks range from voter data[469][470] to corporate data[471] and can be impactful if they end-up in the wrong hands.
- Credentials that are leaked from data breaches are usually used by threat agents to attack other online services. Credentials possibly leaked from the Kickstarter data breach were used to hijack Coinhive's website DNS settings[472].

Related cyber threats:

Data breaches, information leakage, identity theft, ransomware, web-based attacks, botnets

5.6 Exploitation of vulnerabilities/misconfigurations and cryptographic/network/ security protocol flaws

Vulnerabilities[473] and misconfigurations are quite common attack vectors and are usually exploited in order to gain foothold into a system. Cryptographic, network and security flaws are less common but are usually severe since they usually introduce a large attack surface and are quite impactful.

Example security incidents related to this attack vector:

- Wannacry[474] is the notorious ransomware that wreaked havoc to thousands of organisations and users around the world in May 2017. Wannacry's success was based on the fact that it used a leaked NSA exploit against a Microsoft Windows SMB vulnerability. Interestingly, in this attack, the threat agent used another attack vector as well to further spread the malware, namely "Network propagation/lateral movement" based on 5.2.
- KRACK[475] is an attack against the WPA2 security protocol found in Wi-Fi enabled devices. The vulnerability is actually a flaw in the protocol, likely affecting all correct implementations. ROCA[476] is another flaw in a widely used cryptographic library used by a known semiconductor manufacturer. The flaw affects various devices, such as Estonian smart IDs. In both cases the potential impact of these flaws is significant due to their wide reach.

Related cyber threats:

Data breaches, ransomware, Information leakage, cyber espionage, physical manipulation/damage/theft/loss, botnets, web application attacks, web-based attacks

5.7 Supply-chain attacks

Supply chain attacks[477] refer to the compromise of a particular asset e.g. the infrastructure of software or hardware provider, with the aim to indirectly damage a specific target or targets. Supply chain attacks

[469] https://www.enisa.europa.eu/publications/info-notes/voter-data-left-exposed-on-open-internet-facing-system
[470] https://www.upguard.com/breaches/the-rnc-files
[471] https://www.upguard.com/breaches/cloud-leak-accenture
[472] https://www.theregister.co.uk/2017/10/24/coin_hive_hacked_password_reuse/
[473] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits
[474] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst
[475] https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability
[476] http://securityaffairs.co/wordpress/64401/breaking-news/roca-vulnerability-cve-2017-15361.html
[477] https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks

abuse the inherent trust between end-users and the respective providers. Such attacks are typically used as a first step out of a series of attacks. Examples of supply-chain attacks are illustrated below:

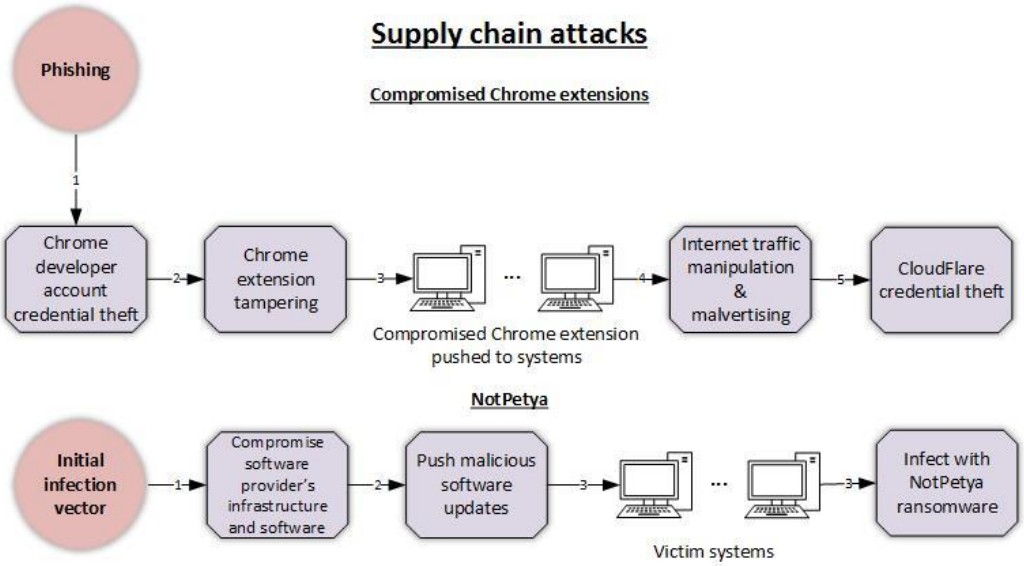

Figure 36: Examples of supply chain attacks[477]

Example security incidents related to this attack vector:

- NotPetya malware spread to systems that had "M.E.Doc" an accounting software, installed. The incident investigation[478] revealed that the threat agent behind the attack compromised the software provider's infrastructure, tampered with the software, and pushed the tampered version of the software to the provider's clients, as a legitimate software update. This software update was responsible for infecting victim systems with the "NotPetya" malware.
- Version 5.33 of CCleaner tool was compromised by a threat agent with the aim to gather information in regards to the infected systems and deliver malware to them[479].
- Chrome browser extensions were compromised through phishing attacks targeting the developers of the extensions[480]. The compromised extensions served malicious advertisements to all systems that had them installed. Furthermore, the malicious extensions aimed at stealing CloudFlare credentials from victim systems.

Related cyber threats:

Data breaches, ransomware, malware, cyber espionage, web-based attacks, web application attacks

5.8 Aftermath of this year's ransomware attacks

Concluding the chapter on attack vectors, we would like to provide the assessment that has been performed on the occasion of this year's ransomware attacks. This assessment provides and analysis on the "incubation environment" of this (and similar) attacks. Though relevant with other parts of the

[478] http://blog.talosintelligence.com/2017/07/the-medoc-connection.html
[479] http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
[480] https://www.proofpoint.com/us/threat-insight/post/threat-actor-goes-chrome-extension-hijacking-spree

document (e.g. ransomware threat), we provide this discussion in this chapter because we consider it as enabler for a series of attack vectors.

The 2017's ransomware attacks have definitely demonstrated the impact on critical functions a cyber-attack may have. For the security specialists, however, WannaCry[474] was the occurrence of already predicted attacks with already expected medium to high impact. The following analysis is not based on technical details and targets both security savvy and non-technical audience. In this realm, one may observe that:

- Abuse of vulnerabilities may create huge impact. This motivates numerous agents in cyber space to work on vulnerability discovery.
- A zero-day vulnerability (i.e. unknown vulnerability) together with the code to abuse it is already considered as cyber-weapon[481].
- Due to its potential destruction power, a vulnerability is a very valuable piece of knowledge. There is a flourishing market for unknown vulnerabilities.
- Legitimate owners of cyber-weapons (e.g. nation-states) need to understand that whenever a cyber-weapon (or its parts) are leaked, a great misuse potential is released.
- When a vulnerability or code abusing it is being leaked, the main part of the cyber weapon is available to the public and can be used for multiple purposes, multiple times.
- The misuse options emanating from a leaked vulnerability are many. They may affect availability, confidentiality or integrity of systems and data.
- While loss of availability is easily noticeable, loss of confidentiality or integrity are outcomes that are not easily noticeable.
- Software vendors respond quickly to unknown vulnerabilities with fixes. Even in managed IT-environments, however, the installation of fixes does take too long to avoid massive failures. Various attacks have demonstrated this.
- The use of software and in particular operating systems that are non-supported by the vendor is very risky. In such cases, discovered vulnerabilities are not corrected/patched by the vendor, at least timely. Such systems offer a wide attack surface; hence it is a matter of time when such systems will be successfully attacked.
- In many cases, the availability and efficiency of security policies cannot mitigate such risks. This is because security policies may not eliminate the occurrence of ALL the above observations.

In the case of WannaCry, we have experienced occurrence of almost all these circumstances. It must be clear, that this may have happened/still happens/will happen with various other vulnerabilities that are available in the wild. Not to mention available unpublished vulnerabilities that are in possession of various cyber-threat agents as we speak.

Though the impact of WannaCry was big, it is not a unique incident of this sort. In summer 2016 we have seen the Mirai[482] botnet that had many similar characteristics in common with WannaCry: it was based on

[481] http://www.dailymail.co.uk/news/article-4509428/Hackers-adapted-NSA-cyber-weapon-EsteemAudit.html, accessed November 2017.
[482] https://en.wikipedia.org/wiki/Mirai_(malware), accessed November 2017.

leaked code that was abusing weaknesses of internet routers and it had affected routers using default credentials.

WannaCry has affected availability of systems and this is just one possible outcome of a known vulnerability. Loss of availability is immediately noticeable. There are hundreds of other possible outcomes, related for example to the integrity or confidentiality of services/data. They might have been implemented already, driven by motives that are different as monetization.

The conclusions that can be drawn from this assessment are also not unknown to the security community and are often stated/discussed. Despite its negative consequences, this incident gives a fair chance to revisit these conclusions and put them in the context of users, experts, lawyers and politicians, in particular:

- Avoid the use of outdated, non-supported, non-managed software and services.
- Liaise among related players to investigate options for optimization of security controls to maximize protection and minimise the effects of cyber-attacks.
- Revisit responsible vulnerability disclosure and investigate technical and legal implementation options.
- Follow-up on vulnerability markets, vulnerability analysis activities, engagement of individuals or groups in vulnerability hunting, etc.
- Check available legal frameworks for their suitability for launching lawful responses to large scale cyber-attacks.
- Discuss the liabilities that arise from the lawful development and possession of cyber-weapons.
- Investigate liability for use of non-supported software in professional and private environments.
- Expand available legislation with rules for the possession and use of cyber-weapons.
- Debate on criteria for the characterization of attacks in order to be in the position to identify appropriate defence responsibilities and defence measures.

6. Conclusions

6.1 Main cyber-issues ahead

This chapter provides a summary of the most important issues implied by the assessments of 2017's cyberthreat landscape. These issues are considered to be ahead of us, that is, they constitute the main future challenges. Although some causality may be evident in the sequence of the points below, they are not listed according to any priority scheme in mind. Moreover, these issues/challenges are indicative with regard our threat assessment. As such they are not exhaustive: various other predictions and assessment reports refer to additional future issues and trends[483,484,485,486,522]. Those will need to be taken into account in order to obtain a complete picture on future predictions. The main issues/challenges are as follows:

With the advancing digitization, numerous applications are popping up. They leverage on new business ideas, technologies and infrastructure models. They use IoT devices and sensors, novel platforms, big data analytics, etc. In addition to the technological components, novel methods and algorithms are utilized. Mostly, such applications use components and know-how that span various disciplines, combining thus IT-knowledge and sector-oriented workflows and processes. In most of the cases, **cyber-security and data protection issues are not taken care of during development or deployment** of such systems. Rather, security is integrated later, when the systems enter operations. This is a critical omission: weaknesses that are built-in cannot always be removed ex-post. Nor can be efficiently covered via security measures that protect the perimeter of such infrastructures. Though this is a rather common observation in many reports, it still remains as root cause of many incidents. The cyberthreat landscape is still heavily affected by this kind of weaknesses of modern infrastructures.

In recent years, and especially in 2017, we have seen a **gradual development of malicious practices** that have impacted the way threat agents conduct their crimes. This shift in methods and tactics has led to a transformation of malicious infrastructures and services towards more aggressive[487] and innovative[488] methods. In particular: malware contains all necessary "intelligence" and functions to autonomously detect vulnerabilities, scan the network, encrypt and adjust to the target environment. This turns, for example, the very role of exploit kits to be obsolete. The reduced availability of vulnerabilities has led to advancements in phishing practices. Malware incorporates command and control functions; this reduces the role of botnet infrastructures in infection and target exploitation activities. It is necessary to study these changes of malware, attack vectors and malicious infrastructures more thoroughly and develop corresponding adaptations of defence methods for all types of assets.

Increasing digitalization goes along with a massive increase of data. This data starts becoming one of the most important assets for the transformation of organisations. Using data analytics, one can discover and

[483] https://sensorstechforum.com/cyber-threat-landscape-will-change-2018/, accessed November 2017.
[484] https://www.ibm.com/security/data-breach/threat-intelligence, accessed November 2017.
[485] https://blog.malwarebytes.com/malwarebytes-news/2017/02/2016-state-of-malware-report/, accessed November 2017.
[486] https://nakedsecurity.sophos.com/2017/11/03/2018-malware-forecast-learning-from-the-long-summer-of-ransomware/, accessed November 2017.
[487] https://www.publictechnology.net/articles/news/cyber-attacks-bolder-and-more-aggressive-ever-says-cyber-security-centre, accessed December 2017.
[488] https://arstechnica.com/information-technology/2017/03/smart-tv-hack-embeds-attack-code-into-broadcast-signal-no-access-required/, accessed December 2017.

leverage on the value of this data[489]. But there is also going to be misuse of this data: both criminals and state-sponsored agents are going to try to **get access to this data and explore their value by using analytics** too[490]. In the reporting period we have seen the massive impact of malicious use of social media analytics[491]. The adoption of new technologies like data analytics - eventually based on Artificial Intelligence and Machine Learning -open new avenues to extract knowledge out of data, thus opening opportunities for cyber-criminals to abuse big data. If cyber-crime develops data analytics capabilities, new forms of abuse will be developed[492]. Given that these new forms of abuse may be based on knowledge (i.e. more complex entities), they will be more difficult to detect than the ones that are based just on individual data (e.g. credit card data, identity data, etc.).

With more and more states starting activities for the lawful surveillance of encrypted traffic, there is going to be continuously flourishing **market for identification of weaknesses and vulnerabilities**[493]. Current "demand" on vulnerabilities from cyber-crime actors and state-sponsored actors will amplify this trend[494]. On the other hand, vulnerabilities and exploits are considered as cyber-weapons. In 2017 we have seen the consequences of zero day vulnerabilities falling in the wrong hands[495]. The use and misuse of these vulnerabilities will need to be clarified[496]. Currently assessed initial discussions reveal the real dimension of this topic[497,498]. Elements to be discussed are how the vulnerabilities are obtained, how they are stored, used, and how they may be patched after their disclosure and/or deployment.

State-sponsored and military capabilities that are currently developed will be very eager to test their tools, weapons and attack capabilities. In 2017 first "cyberwar ranges" have been sighted[499,500]. Such initiatives are important for simulation of cyberwarfare. Nonetheless, testing available cyber weapons under real conditions will be very desirable. Hence, it in being considered likely that state-sponsored high capability agents are going to **look for "cheap cyber-shooting ranges"** in areas with relatively low governance (both political and technical), areas suffering crisis, war, etc[501]. Combined with advanced obfuscation techniques, this might create additional incidents, threats and "noise" in the cyberthreat landscape[502]. Some risks are

[489] https://www.mckinsey.com/global-themes/digital-disruption/whats-now-and-next-in-analytics-ai-and-automation, accessed November 2017.
[490] https://www.information-management.com/news/cyber-espionage-emerges-as-top-data-security-threat, accessed November 2017.
[491] https://www.theguardian.com/technology/2017/mar/04/cambridge-analytics-data-brexit-trump, accessed November 2017.
[492] http://www.access-ai.com/news/1708/microsoft-executive-warns-ai-fascists-dream-ripe-abuse/, accessed November 2017.
[493] https://resources.trendmicro.com/rs/945-CXD-062/images/Frost-and-Sullivan_2016-Global-Public-Vulnerability-Research-Market.pdf, accessed November 2017.
[494] https://resources.trendmicro.com/rs/945-CXD-062/images/Frost-and-Sullivan_2016-Global-Public-Vulnerability-Research-Market.pdf, accessed November 2017.
[495] https://en.wikipedia.org/wiki/EternalBlue, accessed November 2017.
[496] https://www.hsdl.org/?view&did=800768, accessed November 2017.
[497] http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf, accessed November 2017.
[498] https://www.wired.de/collection/life/wie-soll-deutschland-den-umgang-mit-sicherheitsluecken-regeln, accessed November 2017.
[499] https://www.azcwr.org/, accessed November 2017.
[500] https://www.c4isrnet.com/show-reporter/ausa/2017/10/12/heres-what-the-pentagons-persistent-cyber-training-platform-might-look-like/, accessed November 2017.
[501] http://www.sueddeutsche.de/digital/cyber-angriff-auf-die-ukraine-it-forscher-cyberwaffe-russischer-hacker-schaltete-stromnetz-von-kiew-aus-1.3543072, accessed November 2017.
[502] http://www.bbc.com/news/technology-42056555, accessed November 2017.

seen in the way that other players in the cyberspace will react on such incidents; they may create impressions in multiple levels (policy, diplomacy, experts, vendors, etc.).

There is evidence **that there are quite some large scale activities towards scrutinizing the cyber space** (i.e. parts of the internet infrastructure and services offered) by high capability agents (i.e. nation states, large businesses and corporations, military organisations)[429,503]. Such activities may create organized protest and coordinated activities from various society groups such as consumer associations, socially motivated groups, human rights organisation activists, minorities, etc. These protests may lead to new developments in the open source community with regard to anonymity and privacy tools, but also towards the creation of citizen protest and pressure groups. Though such reactions are usually positive for the establishment of social values and equilibria, they might have an impact on the state-of-play with regard to existing cybersecurity tools, practices and levels of technology adoption. It is meaningful from both policy and technology point of view to follow developments hereto[504].

But a reverse trend to the above has also been assessed: one-sided, not neutrally investigated cyber-incidents like state-sponsored conflicts[505], accusations among cyber-actors[434,506], grey area cases in cyber space[405,507], etc. may **cause a "cyber-saturation" to users**. This can only have negative impact on user trust, level of technology adoption and use of security controls. On the other hand, such cases may lead to a fragmentation of infrastructures, policy domains, security markets, etc.[508] Such developments may happen on initiative of nation states in an attempt to disconnect from the influence or on protest of user groups who abstain from using available applications and services[509]. All these are very negative developments towards democracy, human rights as well social and economic prosperity[510].

Cyberthreat Intelligence capabilities and training are two areas that need to be better looked at. Currently, cyberthreat capabilities are limited to vendors and big organisations. Yet, the level of maturity is still low[511]. The community needs to develop maturity models for cyberthreat intelligence and translate them to tangible governance, activities, skillsets and good practices. This will be an important milestone in increasing the deployment of cyberthreat intelligence to more organisations. Education may take up such material[512] and experience and transform it to comprehensive programmes towards the development of the necessary skill sets. Given the interdisciplinary nature of this area, innovative actions in research and education may be developed that will allow for a cross sector cooperation to cover all aspects of cyberthreat intelligence.

---

[503] https://www.nytimes.com/2017/09/24/world/asia/china-internet-censorship.html, accessed November 2017.
[504] https://www.weforum.org/agenda/2016/12/freedom-on-the-net-2016-where-are-social-media-users-under-pressure/, accessed November 2017.
[505] https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/, accessed November 2017.
[506] http://www.telegraph.co.uk/news/2017/03/09/russian-hackers-could-behind-wikileaks-cia-revelations-hacking/, accessed November 2017.
[507] https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.f07543845f99, accessed November 2017.
[508] https://www.cfr.org/blog/internet-fragmentation-exists-not-way-you-think, accessed November 2017.
[509] https://www.lexology.com/library/detail.aspx?g=1dc3e56e-6966-48ac-9b33-6b26251b10fe, accessed November 2017.
[510] http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1570, accessed November 2017.
[511] https://folk.uio.no/vasileim/publications/CTI_Mavroeidis&Bromander_2017.pdf, accessed November 2017.
[512] https://www.sans.org/course/cyber-threat-intelligence, accessed November 2017.

Given the multifaceted security issues and methods, **in the cybersecurity domain there is a great segmentation of product market and approaches**. The market assumes that the customer will purchase solutions and take care to make them coexist in harmony and meet their purpose in an effective manner. In organisations with low to average maturity level in cybersecurity – assumedly the larger part of the user domain – this is not feasible. Current statistics show clearly the market failure in cybersecurity: although cybersecurity investments grow, number of incidents grows too. And it seems that we are far from an equilibrium (i.e. stable investments and stable/decreasing number of incidents). Experts argue[513,514,515] that it is necessary to perform dovetailing of existing approaches in a manner that is transparent to the user. This integration needs to be performed both at technical and methodological levels. User should just express their requirements and do not bother weather their implementations are fit for purpose. Rather, the used product/service will be in the position derive a defence strategy and create the necessary protection.

State-sponsored agents are investing in adoption of new technologies, notably Artificial Intelligence and Machine Learning[516]. Their main concern is to be in the position to manage speed of discovery in large data volumes, such as collected digital communication data, social media data, etc. Both for the civil society and for the sake of international transparency, it would be very constructive for the mutual trust to apply in cyber space similar rules to the ones applied to the transparency of arm trade[517518,519]. Given the fact that this may take long time to be fulfilled, it might be advantageous to regularly assess/estimate the levels of engagement of various nation-states in scrutinising the cyber space[520,521]. This information should be made available to the wide public in order to create awareness about the level of engagement and level of offensive/defensive capabilities.

Attacks on infrastructures to obtain data, misuse processes and available resources **will continue targeting the weakest links**, those being low-end devices or such that are not under robust management and maintenance regimes[522]. IoT devices are going to be one of the elements under attack with this respect. Such supply chain attacks are considered to be the future of cyberthreat landscape development in 2018[522]. Although such attacks may sound trivial, it has been assessed that in most cases are performed by threat agents with high to very high capabilities[523]. Though the exposure to such attacks is difficult to

[513] https://ec.europa.eu/digital-single-market/en/news/comprehensive-approach-evolving-cyber-threats, accessed November 2017.
[514] http://www.digitalistmag.com/cio-knowledge/2017/07/27/global-ransomware-attack-highlights-need-for-comprehensive-cybersecurity-05236100, accessed November 2017.
[515] http://www.govtech.com/policy/States-Take-a-Comprehensive-Approach-to-Improving-Cybersecurity.html, accessed November 2017.
[516] https://phys.org/news/2017-09-swamped-spy-agencies-artificial-intelligence.html, accessed November 2017.
[517] https://www.bloomberg.com/news/articles/2017-07-20/we-need-cyberwar-rules-of-engagement-now, accessed November 2017.
[518] https://www.amnesty.org/en/press-releases/2017/09/geneva-as-global-arms-trade-surges-states-greenlight-reckless-harmful-deals/, accessed November 2017.
[519] https://www.essarp.org.ar/wp-content/uploads/2017/05/GA6-Ensure-transparency-of-investments-in-the-arms-trade.pdf, accessed November 2017.
[520] https://www.scmagazine.com/experts-not-surprised-by-cias-leaked-cyber-weapons-but-stunned-agency-failed-to-protect-them/article/642924/, accessed November 2017.
[521] https://fas.org/sgp/crs/row/R44912.pdf, accessed November 2017.
[522] https://cdn.securelist.com/files/2017/11/KSB_Predictions_2018_eng.pdf, accessed November 2017.
[523] https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks, accessed November 2017.

reduce, there are numerous ways to raise the level of defences[524,525]. However, if the attacks are launched by threat agents with high level of capabilities, it a matter of time for their attacks to succeed. It seems that durable defences for this kind of attacks need to be developed, maintained and properly disseminated[526].

6.2 Conclusions

In this section the conclusions of this year's ETL are being presented. They are divided in three categories, namely policy, business and research/education. This differentiation is indicative for the type of actors that would need to take up actions to cope with the points made below. Though there is a large variety of organisations matching each of these categories, they are not further specified in this report. This would go beyond the scope/purpose of this document. We believe, however, that it is quite straightforward for interested readers to understand what type of organisation would be relevant for the points made in each category, especially when national, sectorial and educational peculiarities are being taken into account.

Policy conclusions

- Recent developments in lawful interventions in cyber-space make clear the need to regulate various critical elements of the threat landscape such as: state support of vulnerability discovery and use, methods for recovery of encryption keys, lawful methods for hacking, etc. These issues will require the development of practices regarding procedural, technical and legal aspects.
- In order to increase efficiency of cyberspace protection, programmes/frameworks that take into account cyberthreat intelligence need to be developed. Similar practices are already under development in the financial sector[527]. Additional critical sectors should be envisaged.
- Policy makers need to investigate methods for establishing necessary transparency in ways state-sponsored actors perform their operations. This would correspond to existing parliamentarian control of military and intelligence services in European democracies[528,529].
- Policy makers should check whether changes in threat landscape may influence policy-making[530] and vice-versa[31]. This would mean that in principle the cyberthreat landscape is being consulted in policy making activities.
- Political forces will need to be inclusive in policy making activities regarding the cyberspace: all related civil/society/consumer groups and interests need to be taken into account. This will be advantageous for a better public applicability/acceptance of produced legislation.

---

[524] http://www.sdcexec.com/article/12369570/protecting-supply-chains-against-cyber-attacks, accessed November 2017.
[525] https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252, accessed November 2017.
[526] https://www.asd.gov.au/infosec/mitigationstrategies.htm, accessed November 2017.
[527] https://www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf, accessed December 2017.
[528] https://de.wikipedia.org/wiki/Parlamentarisches_Kontrollgremium, accessed December 2017.
[529] https://de.wikipedia.org/wiki/Wehrbeauftragter_des_Deutschen_Bundestages, accessed December 2017.
[530] https://arstechnica.com/tech-policy/2017/03/group-sues-dhs-ic-over-digital-device-border-search-records/, accessed December 2017.

- The development of better cyber-defences requires new combination of skills and knowledge. Policy needs to create proper conditions that will lead to better education in the area of cybersecurity and in particular in cyberthreat intelligence.

Business conclusions

- Businesses will need to develop defence strategies that: are based on cyberthreat intelligence, correspond to their maturity/capability level and their sector.
- Vendors need to develop and offer training programs to CTI users according to their maturity and capability levels.
- Existing CTI automation solutions need to be adapted to various CTI maturity and capability levels, to cover sectorial needs economics.
- Currently, the available material on cyberthreats has reached volumes that cannot be managed by end users. The need to better structure available threat intelligence according to types of landscapes and sectors is evident. Vendors will need to create cyberthreat information that is better focussed and better consumable by end-user groups.
- Provided cyberthreat information will need to serve a purpose within organisations. It is necessary to create key performance indicators (KPIs) for the use and role of CTI in the overall protection/risk reduction objectives of organisations.
- Automation of various phases of cyberthreat intelligence tradecraft need to be developed. In particular, automation of cyberthreat intelligence with focus on strategic and tactical issues needs to advance further.

Technical, Research, Educational conclusions

- Understand emerging trends in malware, attack and malicious infrastructure tactics and adapt defences accordingly. Potential use of machine learning and artificial intelligence methods may be accounted for.
- In 2017 we have seen new attack practices, both from security researchers as well as from threat agents. It is necessary to develop new controls that are better suited for modern attack practices. Emerging technologies may be adopted to provide necessary functions and capabilities.
- The cybersecurity community needs to elaborate on technical solutions that will allow for lawful interventions in cyberspace that do not jeopardise privacy and security properties of user data (i.e. confidentiality, integrity and availability of information).
- Educational programmes need to be developed to cover identified gaps in the matter of Cyberthreat Intelligence (CTI). For this purpose, organisations that possess the necessary knowledge will need to (re-)shape the corresponding skill profile and combine capabilities to develop comprehensive education curricula.
- The various use cases of cyberthreat intelligence need to be better understood and better incorporated into good practices. This includes understanding the content and type of threat information required and ways for its delivery.

- Maturity models for CTI need to be developed. These will complement use cases of CTI and will be used as guidance for the adoption and implementation of needed maturity levels by various types of CTI users.
- Various types of threat landscapes (containing corresponding CTI) will need to be developed that suit various use cases, maturity levels and sectors. Such landscapes will flow into various activities for the assessment of available security level (e.g. through red or blue teaming).

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-250-9
ISSN: 2363-3050
DOI: 10.2824/967192