ENISA Threat Landscape 2015

JANUARY 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

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.

Authors

Louis Marinos (louis.marinos@enisa.europa.eu), ENISA, Adrian Belmonte, ENISA (contribution Attack Vectors and SDN), Evangelos Rekleitis, ENISA (contribution Big Data).

Contact

For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

The author would like to thank the members of the ENISA ETL Stakeholder group: Paolo Passeri, Consulting, UK, Pierluigi Paganini, Chief Security Information Officer, IT, Paul Samwel, Banking, NL, Tom Koehler, Consulting, DE, Stavros Lingris, CERT, EU, Jart Armin, Worldwide coalitions/Initiatives, International, Thomas Häberlen, Member State, DE, Neil Thacker, Consulting, UK, Margrete Raaum, CERT, NO, Shin Adachi, Security Analyst, US, R. Jane Ginn, Consulting, US, Lance James, Consulting, US, Polo Bais, Member State, NL. 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. Thanks go to ENISA colleagues who contributed to this work by commenting drafts of the report. Special thanks to Jakub Radziulis, iTTi and his colleagues for the support in information analysis.

Table of Contents

Executive Summary

For yet another year the 2015 edition of the cyber-threat landscape features a number of unique observations, the main one being the *smooth advancement of maturity*. As a matter of fact, cyber-space stakeholders have gone through varying degrees of further maturity. While the friendly agents – the good guys – have demonstrated increased cooperation and orchestrated reaction to cyber-threats, hostile agents – the bad guys – have advanced their malicious tools with obfuscation, stealthiness and striking power.

On the defenders' side, improvements have been achieved in coordinated campaigns to disturb operations of malicious infrastructures, strengthen the legal/governmental cyber-defence framework and develop more efficient products. In particular:

- Performing orchestrated actions to take down malicious infrastructure but also to analyse incidents and improve attribution.
- Strengthening governmental awareness, cyber-defence expenses, capabilities and level of cooperation among states.
- Performing exercises, development of threat intelligence, proliferation of information sharing, tools and products to enhance awareness, preparedness and efficiency of defence.
- Focusing on research and development to accommodate developments of the cyber-threat landscape to existing protection measures and methods and tools.

These are qualities that have been consistently developed throughout 2015 and have reached a momentum that allows for a persistent course of action.

Adversaries have achieved considerable advances too. No Snowden or Heartbleed-like events have been reported. Instead, cyber-threats have undergone significant evolution and just as in 2014, significant breaches have covered front pages of media. And exactly this is an alerting fact: seemingly, cyber-threat agents have had the tranquillity and resources to implement a series of advancements in malicious practices. In particular:

- Performing persistent attacks based on hardware, far below the "radar" of available defence tools and methods.
- Achieving enhancements in the provision of "cyber-crime-as-a-service", tool developments for non-experts and affiliate programmes.
- Highly efficient development of malware weaponization and automated tools to detect and exploit vulnerabilities.
- Campaigning with highly profitable malicious infrastructures and malware to breach data and hold end-user devices to ransom.
- Broadening of the attack surface to include routers, firmware and internet of things.

Details for all the above-mentioned points can be found in the ENISA Threat Landscape 2015 (ETL 2015). Top 15 cyber-threats together with threat trends, trends of threat agents and trends for emerging technologies have been assessed and presented in this report. This material delivers evidence upon which the consequences for the development of cyber-defences can be based.

Lessons learned and conclusions summarise our experience from this year's threat landscape and draw a roadmap with aspects that need to be addressed in the future by policy, businesses and research. An overview hereof is as follows:

Policy conclusions:

- Make threat intelligence collection, management and sharing an inherent part of the national cyber-defence capabilities.
- Foster voluntary reporting and perform analysis of reported incidents and recycle results for better planning of defences.
- Disseminate cyber-threat knowledge to all players in cyber-space, including end-users.

Business conclusions:

- Simplify content of threat intelligence to achieve wider uptake in the stakeholder community.
- Elaborate on threat agent models and make it inherent part of threat intelligence.
- Create correlated, contextualized threat information to increase timespan of relevance.
- Continuously adapt protection and detection tools to the threats.
- Invest in better vulnerability management and exploitation of dark web.

Research conclusions:

- Develop applied statistic models to increase comparability of cyber-threat and incident information.
- Develop new models for seamlessly operated security controls to be included in complex, smart end-user environments.
- Develop trust models for the ad hoc interoperability of devices within smart environments.

Finally, regarding the overall highlights for the future cyber-threat landscapes, one should mention two overarching trends for defenders and adversaries respectively:

- The need for "*Streamlining and consolidation*" of existing policies, defences and cooperation to accommodate changes in threat landscape and
- Ongoing activities towards "*Consumerization of cyber-crime*", that is, making malicious tools available to everybody.

The figure below summarizes the top 15 cyber-threats and threat trends in comparison to the threat landscape of 2014.

Top Threats 2014	Assessed Trends 2013	Top Threats 2015	Assessed Trends 2014	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	➲	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	➲	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	➲	11. Data breaches	➲	↓
12. Information leakage	↑	12. Identity theft	➲	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

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

Table 1: Overview and comparison of cyber-threat landscapes 2015 and 2014

1. Introduction

This report, the ENISA Threat Landscape 2015 (ETL 2015), is the result of an analysis of cyber-threats that have been encountered in the last 12 months, that is, approximately between December 2014 and December 2015. ETL 2015 is the fourth in a series of reports issued yearly by ENISA. It provides an analysis of the state and the dynamics of the cyber-threat environment: the *Cyber-Threat Landscape*.

Just as previous threat landscape reports, ETL 2015 is the result of a comprehensive threat analysis that is based mainly on open source intelligence. The analysis is followed by a collation of threat information. In this process, cyber-incidents, cyber-threats, cyber-attacks, etc. are put in context to by means of correlated information. This is *cyber-threat intelligence* that is being created within ENISA: an amount of knowledge on the development of cyber-threats created on annual basis.

ETL 2015 is a significant part of this knowledge captured in the form of a report. It contains top 15 cyber-threats assessed in 2015, together with information on threat agents, attack vectors and threat trends for a number of emerging technologies. The information presented is accompanied with references to all relevant resources found. Though non-exhaustive, ETL 2015 includes a critical mass of published material that allows to underpin the assumptions made. At the same time, the collected material is a tool to the hands of interested individuals who need to deepen in the details of a certain matter presented in this report.

In the reporting period, material found on cyber-threats has increased quantity, quality and focus. This is due to the continuous improvement achieved in the area of threat intelligence and is a result of the increased demand and efforts invested, both by public and private organisations. In a similar manner as in ETL 2014, in ETL2015 we have processed ca. 380 resources. This number is rather representative for the search and analysis effort at ENISA than the available resources worldwide which were apparently much higher.

Besides open source information, in this report ENISA has used information provided by the MISP platform[1], by CERT-EU[2] and by also using threat intelligence of the cyber-security portal CYjAX[3], provided by means 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.

In comparison to previous ETLs, some minor changes have been made in the structure of this report. They regard the description part of current threats. In particular, for each cyber-threat described we attach a list of indicative mitigation controls, referred to as *mitigation vector*. This was a requirement communicated to us by stakeholders. Secondly, in 2015 kill chain information of the top 15 threats has not been adopted as it is identical with ETL 2014. To find information hereto, interested readers would need to revisit ETL 2014[29].

Just as in previous years, ENISA has consulted the ETL Stakeholder group that accompanies the threat analysis work. The group has provided valuable input, has supported the ENISA event on threat analysis

[1] http://www.misp-project.org/, accessed November 2015.
[2] https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html, accessed November 2015.
[3] https://www.cyjax.com/, accessed November 2015.

organised in 2015[4] and has reviewed ENISA material. Their support has definitely contributed to the quality of the material presented in this report.

1.1 Policy context

The Cyber Security Strategy of the EU[5] 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 new ENISA Regulation[6] 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*".

The ENISA Threat Landscape aims to make a significant contribution to the implementation of the EU Cyber Security Strategy by streamlining and consolidating available information on cyber-threats and their evolution.

1.2 Target audience

Information in this report has mainly strategic and tactical relevance[10] to cyber-threats and related information. Such information has long-term relevance of approximately up to one year. It is directed to executives, security architects and security managers. Nonetheless, provided information is also easily consumable by non-experts.

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

- The method part (see chapter 2) is targeting **security professionals** who may seek to find out how threat information relates to other topics of information security and information security management. Provided information may allow them to deepen in issues of threat intelligence, threat information collection and threat information analysis and/or find ways in integrating it with other security management disciplines.
- The current threat landscape is a compilation of information about top cyber-threats (see chapter 3). At the level of the threat description**, generalists** and **decision makers** can find non-technical information about the cyber threats. By going through details, issues assessed and sources related to the text, interested individuals and **security experts** might find detailed technical information.
- A generic description of cyber-threat agents explains developments in this area (see chapter 4). This information is good for all readers, **decision makers, security experts** and **non-experts**.
- The emerging threat landscape contains information for a wide range of skills (see chapter 6). The chapter targets mainly **security managers** and **security architects** who would like to understand the

[4] https://www.enisa.europa.eu/activities/risk-management/events/enisa-workshop-on-eu-threat-landscape, accessed November 2015.
[5] http://www.ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, accessed November 2015.
[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF, accessed November 2015.

trends ahead. The information provided is also potentially useful for **decision makers** as decision support information.

Besides these roles in the ETL target group, details provided on methodology, threats, issues, threat agents, attack vectors and trends are useful for **risk manager**. This kind of information is essential input to any risk assessment process.

Besides the information in this report, there are "side products" that might be interesting for a wide audience. On the occasion of the ENISA High Level Event[7], ENISA has produced a leaflet with a consolidated high level description of issues that resulted this year's threat assessment[8]. This material targets **decision makers** from both policy and business.

Another product of the ETL process is the ENISA threat taxonomy, a hierarchy of threats used as a point of reference to classify collected and processed information about threats and in particular cyber-threats[26]. Finally, in 2015 ENISA has produced two detailed threat assessments in two sectors. These *the thematic landscapes* have been issued for Big Data[362] and Software Defined Networks / 5G[320] and are published as separate reports.

1.3 Structure of the document

The structure of ETL 2015 is as follows:

Chapter 2 "*Purpose, Scope and Method*" provides some information regarding the threat analysis process as it is being performed within the ETL2015. Moreover, it refers to the information structures as used within our threat analysis and provides some information on used definitions.

Chapter 3 "*Top Cyber-Threats: The Current Threat Landscape*" is the heart of the ETL 2014 as it contains top 15 cyber-threats assessed in 2015. It provides detailed information on the threat with references to all relevant resources found, trends assessed and mitigation vectors for each threat.

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.

Chapter 5 "*Attack Vectors*" provides information on typical attack scenarios, steps and deployed cyber-threats and is supposed to complement the presented material by giving some initial information on the "How" of a cyber-attack.

Chapter 6 "The *Emerging Threat Landscape*" indicates assessed technology areas that will impact the threat landscapes in the middle-term. Ongoing developments in those areas will influence the ways attackers will try to achieve their aims, but also the way defences are going to be implemented.

Chapter 7 "*Food for thought: Lessons Learned and Conclusions*" is a summary of interesting issues encountered within the threat analysis and provides the conclusions of this year's ETL.

[7] https://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2015, accessed November 2015.
[8] https://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2015/cyber-7-seven-messages-to-the-edge-of-cyber-space, accessed November 2015.

2. Purpose, Scope and Method

In 2015, threat analysis and threat intelligence have gone through an impressive breakthrough, whereas the details of various aspects, phases and purposes/use cases have been analysed and documented. This has been done by means of various reports issued by various states[9], organisations[10] and vendors[11,12,13,14] (references are indicative due to the large number of related material). Threat intelligence in general has been considered as one of the key technologies in cyber-security[15]. These facts underline the importance of threat intelligence and in particular threat analysis in the context of management of cyber-security incidents. Following this trend, many services, products and practices have entered the market. Threat intelligence services in various degrees of "width and depth" have shown up.

Though quite massively deployed, threat intelligence is still a new area and as such, products and market are at an early maturity stage: both vendors and customers do not have common perceptions on the topic and how it can be integrated as service or product into the daily businesses. Moreover, there is a "spread" in existing offerings with regard to the kind of delivered information and protection offered on the one hand and on the other hand the customer prerequisites (e.g. technical and organisational). Nonetheless, predictions foresee a great potential for the threat intelligence market, reaching some 5 billion $ in 2020[16].

Research and development in the area of threat intelligence advances too. In the reporting period we have assessed the initiation of important programmes in the area of threat intelligence[17,18] and dynamic risk management[19] both in Europe and US.

While research and vendors are working on the state-of-the-art in the area of threat intelligence/threat analysis, ENISA has undertaken next steps for the improvement of methods used. This effort has ran in parallel to the information collection and analysis tasks and aimed at the development of available practices. In particular, ENISA efforts have been concentrated in the following areas:

- *Identification of the data structures used in the threat analysis process and threat landscaping*: A data model of the information household of the entire process of collection, analysis and description of cyber-threats, both for ETL and ENISA Thematic Landscapes has been developed.
- *Creation of a threat taxonomy*: Through the information collection and analysis activities of the previous years at ENISA, a threat taxonomy has evolved. This taxonomy is a multi-tool that can be used

[9] https://securityintelligence.com/us-government-to-establish-cyber-threat-intelligence-integration-center/, accessed November 2015.
[10] https://www.cpni.gov.uk/documents/publications/2015/23-march-2015-mwr_threat_intelligence_whitepaper-2015.pdf?epslanguage=en-gb, accessed November 2015.
[11] http://digitalshadows.com/threat-intelligence-a-buyers-guide-/, accessed November 2015.
[12] http://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf, accessed November 2015.
[13] http://threatintelligencetimes.com/about-us/, accessed November 2015.
[14] http://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/, accessed November 2015.
[15] http://darkmatters.norsecorp.com/2015/02/25/cisos-threat-intelligence-big-data-analytics-and-encryption-are-key-technologies/, accessed November 2015.
[16] http://www.marketsandmarkets.com/PressReleases/threat-intelligence-security.asp, accessed November 2015.
[17] https://ec.europa.eu/digital-agenda/events/cf/ictpd14/item-display.cfm?id=12676, accessed November 2015.
[18] http://www.gtri.gatech.edu/ctisl, accessed November 2015.
[19] http://www.mitigateproject.eu/, accessed November 2015.

in all phases of threat analysis. The development of a threat taxonomy has been a requirement communicated to ENISA in 2014 and it will be continued in 2016.

- *Initial identification of graphical support for the presentation of cyber-threat information*: Graphical elements for the representation of cyber-threats are an important issue that is currently addressed by market players in the threat analysis[20,21,22]. In 2015, ENISA carried out an initial assessment of graphical support for ETL.

Results achieved in these areas will be briefly discussed in the forthcoming chapters. This information might help readers to better understand the scope of ENISA's work, while at the same time providing information about the ENISA method. Information about the method may help interested parties in introducing threat analysis in their organisations. Such information may be used in multiple ways, such as; being the basis for requirements analysis; used for the evaluation of tools; used for the evaluation of services; taken as good practice for adjustments of own practices, etc.

2.1 Data structures used in the threat analysis process and threat landscaping

The information used within ENISA for threat landscaping has been identified in 2015 and has been represented by means of a data model. This is an initial step in order to create a data household of the entire information managed within the ENISA work, both regarding ETL but also the Thematic Landscapes, i.e. detailed threat landscapes in selected areas/technologies.

Although some of the data concerned have been created and maintained as distinct entities in the past, the entire ETL model has not been described as a whole. Yet, the identified ETL data model is comprehensive and covers all information, from the collection to the final documentation. The data model in its current form has been created in 2015 in an ex-post manner and is presented in the figure below (see Figure 1). It is worth mentioning that the blue under laid area covers the data used in ETL, while the yellow one stands for the data household of the thematic landscapes.

[20] http://cybermap.kaspersky.com/, accessed November 2015.
[21] https://www.fireeye.com/cyber-map/threat-map.html, accessed November 2015.
[22] http://map.ipviking.com/?_ga=1.98376799.153405815.1403529861#, accessed November 2015.

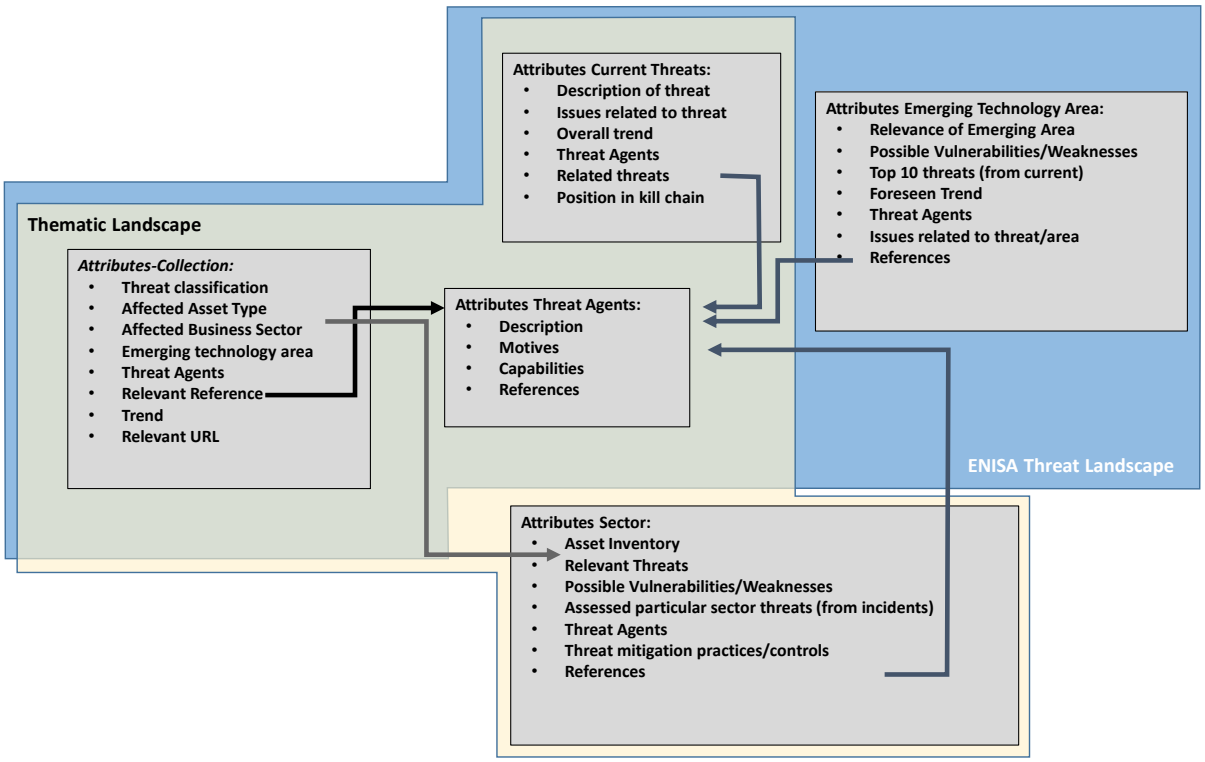

Figure 1: Data model covering all information managed within all phases of ETL

Knowing maintained data structures has manifold purposes: i) it clarifies the context and the interdependencies of used information, ii) it helps in defining storage structures of the information (e.g. tables/relations), iii) it clarifies data structures that can be imported / exported and iv) it helps in understanding how own data correspond to other approaches. All these four steps are essential in advancing the maturity of the used approach.

In order to assess level of "coverage" between this data model and STIX[23] - a data format that is being widely used for threat information - we have made a comparison at the level of data models. The detailed comparison can be found in Annex A: With this information at hand, the interfaces between ENISA's data and data from other threat intelligence sources can be defined (i.e. input/output data).

Finally, regarding the quality of produced cyber-threat information, it has to be underlined that the ETL is geared more towards strategic threat intelligence with some tactical parts, while thematic landscapes contain more tactical information. An excellent report describing role and scope of threat information is 10.In short, strategic and tactical threat information as follows[24]:

- *Strategic information* is used within forecasts of the threat landscape and emerging technological trends in order to prepare organisations by means of assessments, prospective measures and security

[23] https://stixproject.github.io/, accessed November 2015.
[24] https://www.first.org/resources/papers/conf2015/first_2015_marinos-louis-enisa-threat-landscape_20150630.pdf, accessed November 2015.

investments, as well as adaptation of existing cyber security strategies. It is created and consumed by humans and has a life span of some months (ca. one year).

- *Tactical information* consists of condensed information describing threats and their components, such as threat agents, threat trends, emerging trends for various technological areas, risks to various assets, risk mitigation practices, etc. This information is important for stakeholders engaged in maintenance of security controls. It is created by humans and machines and has a life span of weeks/months.

2.2 Threat taxonomy

Threat taxonomy is a classification of threats. The purpose of such a taxonomy is to establish a point of reference for threats encountered, while providing a possibility to shuffle, arrange and detail threat definitions. To this extend, a threat taxonomy is a living structure that is being used to maintain a consistent view on threats on the basis of collected information.

The current version of ENISA Threat Taxonomy (ETT) has been developed over the past years as an internal tool used in the collection and consolidation of threat information. When collecting information on various threats, it is very convenient to store similar things together. To this extend, a threat taxonomy has been generated. It is worth mentioning that the initial structure has been updated/consolidated with various sources of threat information. Most of threat information included was from existing threat catalogues the area of information security and in particular risk management. An overview of consolidated threat catalogues can be found here[25]. Hence, besides cyber-threats the ENISA threat taxonomy (ETT) contains also physical threats that can cause harm to information technology assets.

As until now the ETT has been used for collection and consolidation of cyber-threat information, only the cyber-threat part of the taxonomy has been maintained and developed further. Although all information security threat areas are part of the ETT, those that are not related to cyber have not evolved over the time.

In 2015, ENISA has created a consolidated version of these threats, has added some short descriptions to these threats and has decided to make this material publicly available as a spread sheet[26]. The figure below shows this taxonomy in form of a mind map, together with some symbols indicating its possible use-cases (see Figure 2).

[25] http://opensecurityarchitecture.org/cms/images/OSA_images/TC_Comparison.pdf, accessed November 2015.
[26] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information, accessed January 2016.

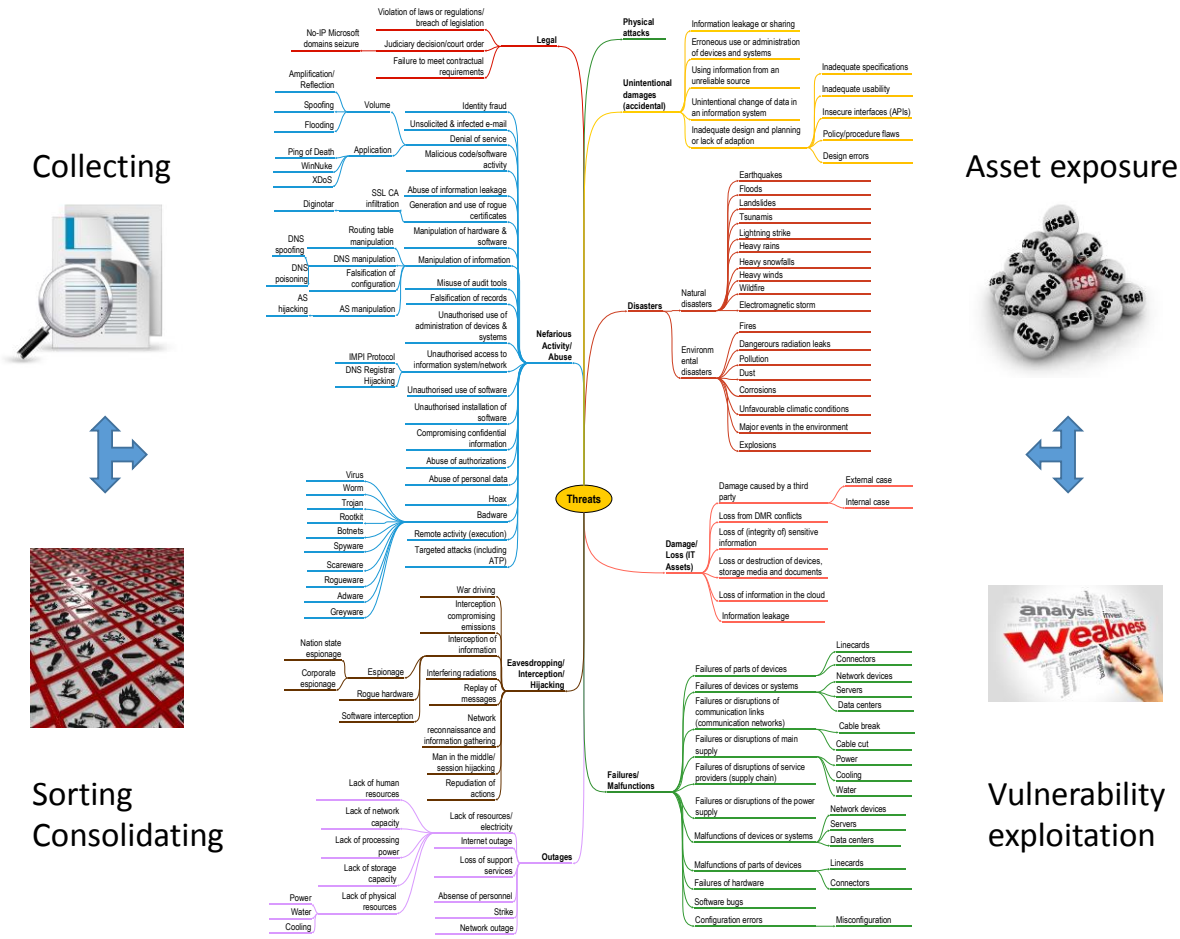

Figure 2: ENISA Threat Taxonomy and its use-cases

In short, the indicated use-cases for the threat taxonomy are:

- *Collection*: When information is being collected, findings can be grouped around a certain cyber-threat, although this is often not clearly mentioned in the source text. In the collection phase is as a place to associate various findings under a common threat, putting thus information in context.
- *Sorting/Consolidation*: When sufficient information has been collected about a cyber-threat, a consolidated view about the state-of-play may be generated. This information might include trends, statistics and references. It is then subject to further grouping and prioritization (i.e. in form of one of the top 15 cyber-threats, possibly containing a number of detailed threats).
- *Asset exposure*: The threats of the taxonomy may be assigned to assets. This is being done in order to express the exposure of an asset to threats. Usually, threats explore weaknesses/vulnerabilities of assets to materialise. Hence, vulnerabilities/weaknesses may also be assigned to threats exploring them, either directly or indirectly through the assets.

The current version of ETT has been published as a separate deliverable this year[26]. Its development will be continued in 2016.

2.3 Graphical support

Graphical support of threat landscapes, threat information and threat intelligence is an area that has very large potential. In the reporting period we have seen various approaches to visualization of threats, as vendors try to provide more user-friendly access/navigation options to threat information. Besides visualisations of threats by means of web-applications[20,21,22], we have seen interesting interactive graphical approaches appearing on online versions of threat reports[27] that certainly provide a better readability/animation to the content of threat reports.

Though no extensive assessment has been done regarding available visualization approaches of threat intelligence tools/portals/information services, it seems that there is a general trend towards visualization of threat intelligence.

An interesting approach to the visualization of security and threat intelligence based on open source intelligence is Sinfonier[61]. Being developed for security intelligence, this approach provides graphical elements and mechanisms for collection, analysis and sharing of related information[28]. As such, it seems as particularly appropriate for threat information.

In 2015, ENISA has made some prototyping with graphical representation of strategic and tactical threat information. The prototype was based on graph database Neo4j and its basic visual user interface (neo4j-contrib/neoclipse). This effort will be continued in 2016 with the objective to visualize ETL information, whereas other technical options for the run-time environment will also be investigated.

2.4 Used definitions

The definitions used are identical to the ones of ETL 2014[32]. In order to visualize the relationships among all elements of risks, we use a figure taken from ISO 15408:2005 (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 further detailed through the ETL data model presented in Figure 1 above. 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:

---

[27] http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup, accessed November 2015.

[28] http://www.slideshare.net/rootedcon/sinfonier-003?ref=https://cdn.embedly.com/widgets/media.html?src=https%3A%2F%2Fwww.slideshare.net%2Fslideshow%2Fembed_code%2F33910506&src_secure=1&url=https%3A%2F%2Fwww.slideshare.net%2Frootedcon%2Fsinfonier-003&image=https%3A%2F%2Fcdn.slidesharecdn.com%2Fss_thumbnails%2Fsinfonier003-140424134953-phpapp01-thumbnail-4.jpg%3Fcb%3D1398366729&key=b7276e97d3f840f38fbdb95eb1242b10&type=text%2Fhtml&schema=slideshare, accessed November 2015.

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

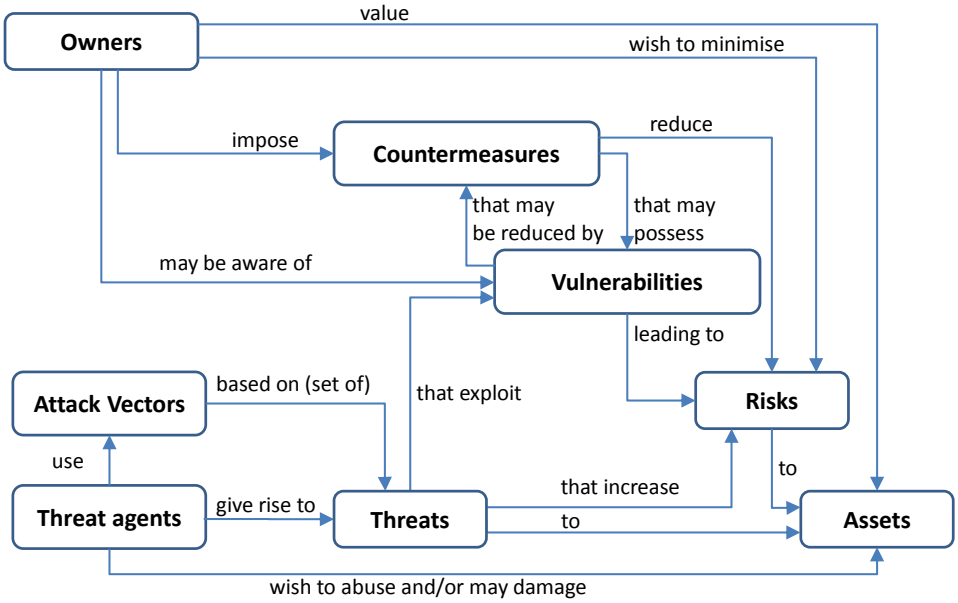

Figure 3: the elements of a risk and their relationships according to ISO 15408:2005

3. Top Cyber-Threats: The Current Threat Landscape

3.1 Content and purpose of this chapter

In this chapter the current threat landscape 2015 is presented. It consists of fifteen top cyber-threats, assessed during information collection and analysis activities. The current threat landscape covers information material that has been made publicly available in the time period November 2014 to November 2015. This time window is referred to as *reporting period* in the present report. For the sake of clarity, it should be noted that the sources analysed in this chapter are the ones detected via the ENISA open source intelligence gathering process. While non-exhaustive[29], they are considered as representative of the threats and incidents encountered during this period.

Following the trend of previous years, the material found online has increased. In the reporting period, numerous focused publications in important cyber-threats have been found. Examples are: insider threat, denial of service, data breaches and identity theft. At the same time, our team won the impression that the area of mobile computing had shown some stagnation regarding the level of coverage; some reports conclude that (fortunately) the mobile vector has not met expectations of cyber-security experts and did not seem to be preferred attack vector to breach user data[85] regarding growth potential. Instead, the attention of cyber-security experts has been drawn on incidents in the area of Internet of Things[137] and attacks at cyber-physical interfaces[30]. These are definitely upcoming areas of concern for the cyber-security community.

In this reporting period the cyber-security community has developed a better focus on particular areas of cyber-threats. Moreover, cyber-threat information and intelligence appears to become commonly maintained knowledge, especially at the level of cyber-threat information collection and dissemination organisations, such as CERTS (e.g. CERT-EU[31]). This increase in focus and maturity is very beneficial for all parties in the assessment of cyber-threats. Following this maturity, we have seen dedicated products for the mitigation of the assessed cyber-threats to start appearing in the market, such as web application firewalls[65].

It is indeed very fortunate to see threat analysis and assessment efforts converging with product development, thus leading to a robust, demand-driven market. This is one of the most interesting and positive observations in the reporting period: efforts invested in cyber-threat analysis and cyber-threat intelligence have led to interesting, well-shaped service and product offerings in the cyber-security market. This is a shift from vendor-driven market to a demand-driven one. It remains to be seen how the market will further evolve and how it will accommodate dynamics of the cyber-threat landscape.

As was the case in previous versions of the ETL, the threat prioritisation has been performed mainly by means of a combination of frequency of appearance/reference and number of incidents (i.e. “efficiency” of the threat). In some cases, for example, threats that were decreasing ranked higher or kept their position. This means that a higher efficiency of attacks based on this threat has been reported (e.g. botnets). In the

[29] Due to the vast amount of published threat information and the limited resources available, it is very likely that several publications on the topic of cyber-threats escaped our attention. Hence, if readers miss some publications known to them, these might be items that have not been spotted during information collection. Despite potentially undetected reports, we believe that the collected material is a sufficient sample to identify cyber-threat dynamics and trends.

[30] https://ec.europa.eu/digital-agenda/en/cyberphysical-systems-0, accessed November 2015.

[31] https://www.youtube.com/watch?v=a1yhQgx2aN8, accessed November 2015.

reporting period we have seen some reports classifying incidents according to impact and sector[92]. This is a very useful classification that should be used by more vendors, as it covers aspects of incidents that are important for decision making within various sectors (i.e. caused costs and consequences).

The ETL 2015 has been developed without any particular business or infrastructure scenario in mind. As such, when used within a particular business environment, it is necessary to put ETL information in the context of that business area. Usually, this should be done by assessing the importance of business, as well as human and IT assets of the organisation. Based on this information, a risk assessment will provide evidence for the threat exposure of the assets at stake, hence allowing for a prioritization of the threats according to the environment of that business area. The cyber-threats discussed below serve as input to such a prioritisation.

The description of cyber threats consists of i) a short text explaining the whereabouts of the threat, ii) a list of findings, iii) the trend observed in the reporting period, iv) other related threats that are used in combination with a threat, and v) a list of authoritative resources. In an attempt to keep the size of this report moderate, in this year's report the kill-chain information of each threat has not being included. It is identical to the previous year's ETL[32]. Instead, in this year's ETL, the description of each cyber-threat is followed by a short, indicative list of mitigation options. This list comprises an initial collection of controls, whose implementation would mitigate the threat, that is, reduce the exposure to the threat. This addition has been done after requirements communicated to ENISA by the reader community of ETL. In future ETL versions this type of information might be more extensive.

This chapter is concluded by a visualized comparison between the current threat landscapes of the ETL 2014 and the ETL 2015. This will help readers to easily understand the changes of the current threat landscape in this time period.

3.2 Malware

In the reporting period malware remains number one cyber-threat. In 2015 current advances in sophisticated malware show their potential: Equation Group uses hardware re-programming allowing for installation of malicious information (e.g. URLs to malware droppers) in the firmware of hard discs[33,34]. This infection method is difficult to detect and disinfect, as it resists hard disc formatting and operating system re-installation. Hardware that has been infected with this method may need to be entirely replaced, if used for sensitive tasks (e.g. governments). Albeit mobile malware may not have reached expected levels of growth, it continues being a serious concern. Total number of mobile malware grew 17% in Q2 2015, exceeding 8 million samples, while in 2015, the growth of new mobile malware samples was about 50% more than in previous year[35]. It is interesting that in the area of mobile malware, sharing methods are topped by manual sharing, followed by fake offerings and fake "Likes" that lead to malicious URLs (i.e. droppers)[36]. The Android platform holds the lion's share with over 95% of mobile malware. Finally, one

[32] Interested individuals may find the kill-chain information for the various cyber-threats in last year's ETL: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport.

[33] http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage, accessed September 2015.

[34] https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/, accessed September 2015.

[35] http://www.mcafee.com/mx/resources/reports/rp-quarterly-threats-aug-2015.pdf?view=legacy, accessed September 2015.

[36] https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence-report-08-2015-en-us.pdf, accessed September 2015.

should mention the availability of tools that enable technically novices to create own malware variants, thus further lowering the thresholds for the deployment of malware attacks[37].

In the reporting period we have assessed that:

- Rather than complexity, cyber-criminals are focussing on efficiency. In the reporting period we have seen the revival of infection techniques employed almost 20 years ago: Microsoft Office documents infected with Visual Basic macros[38,39] and subsequently downloading malware. This method stands for the other extreme to highly sophisticated attacks encountered in 2015, such as Equation Group and Duku 2[40], allegedly emanating from high capability threat agents.
- It is interesting that CONFICKER, a more than 7 years old work still leads the PC infection statistics (37% of infections according to[41]). This is another impressive evidence that adversaries maintain "old good" methods as far as they continue paying back. The second most popular malware (Kilim) is based on social media misuse. This is an evidence for increasing use of social media as one of the main sources to lure users.
- Use of malicious URLs showed a sharp increase, compared to malicious e-mail attachments. This is due to the shift of infection tactics by using social engineering methods to craft spam/phishing attacks[42]. Interestingly, rate of malware transporting e-mails has been reduced.
- It is worth mentioning that the observed drop in mobile malware families is an indication that level of innovation slows down, and/or that existing families provide a good basis for abuse of available devices – including mobile Internet of Things devices[43]. Apparently, existing malware families suffice to create a significant growth of this threat.
- Malware continues increasing by ca. one million new samples per day. The total increase of malware samples till Q2 is 12%[35]. By the end of 2014, total number of available malware samples was estimated by 1.7 billion. Consequently, by the time of publication of this report, the overall number of malware would reach the 2 billion threshold.
- Current malware statistics provide the following information[44]:
  - Top 5 countries in which IT resources are infected by malware are: Bangladesh and Vietnam with ca. 60%, followed by Pakistan, Mongolia and Georgia with ca. 58% each.
  - Top countries hosting online malware resources are: Russia ca. 50%, US ca. 12%, The Netherlands ca. 8%, Germany ca. 5% and France ca. 3%.

---

[37] http://securityaffairs.co/wordpress/41714/cyber-crime/govrat-platform.html, accessed November 2015.
[38] http://betanews.com/2015/03/06/down-but-not-out-vba-malware-makes-a-comeback-in-microsoft-office/, accessed September 2015.
[39] http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-Q2-EN.pdf, accessed September 2015.
[40] https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf, accessed September 2015.
[41] https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2014, accessed September 2015.
[42] http://www.cert.pl/PDF/Report_CP_2014.pdf, accessed September 2015.
[43] http://www.symantec.com/security_response/publications/threatreport.jsp, accessed September 2015.
[44] https://securelist.com/analysis/quarterly-malware-reports/71610/it-threat-evolution-q2-2015/, accessed September 2015.

- Top countries with the risk of online infection are: Russia ca. 39%, Kazakhstan ca. 37%, Ukraine ca. 35%, Syria ca. 24% and Belarus ca. 33%. It is interesting that the majority of those countries suffer some kind of crisis (political/military).

- Malware types detected in the reporting period are topped by potentially unwanted software (aka RiskTool) with ca. 44 %, followed by AdWare with ca. 19%, Trojan at ca. 12%, Trojan.SMS 8% and Trojan.Spy 7%. Followed by Backdoor, Ransomware and Downloader/Dropper, all around 1%[44]. While other repots mention slightly different findings such as Memory Dumper, Remote Access Tool (RAT), Downloader, Keylogger, Click Fraud/Malvertising, Backdoor, Persistence and Botnet being in the top 8 list[116].

- Apps and consequently app stores remain main target for "packaging" and spread of malware. Yet in 2015, we have seen successful attempts to overcome vetting processes of official app stores, led by recent Apple store hack that has affected possibly thousands of apps[45], potentially used by hundreds of millions of users[46,47]. Android app stores suffered similar incidents in the reporting period[48]. A technique for patching existing software and introducing malicious code has been become the main method to distribute Trojans[49,50].

Observed current trend for this threat: *increasing*

Related threats: Web based attacks, Web application attacks, Exploit kits, Spam, Phishing, Botnets, Data Breaches, Ransomware, Cyber espionage.

Authoritative Resources 2015: "Internet Security Threat Report 20" Symantec[43], "THREAT REPORT H2 2014" F-Secure[41], "Threats Report" August 2015 McAfee[35].

Mitigation vector: The mitigation vector for this threat contains the following elements:

- Patching of software and firmware to the latest version supported by the vendor.
- Whitelisting of applications to define legitimate software as authorised and block the execution of rogue software.
- 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.

[45] http://thehackernews.com/2015/09/ios-malware-cyber-attack.html, accessed September 2015.
[46] http://www.nytimes.com/2015/09/21/business/apple-confirms-discovery-of-malicious-code-in-some-app-store-products.html?_r=1. Accessed September 2015.
[47] http://www.japantimes.co.jp/news/2015/09/23/business/tech/app-store-hack-slow-foreign-connections-lack-support-apple-led-developers-use-risky-pirated-tools/#.VgqCvaP6jI8, accessed September 2015.
[48] http://blog.trendmicro.com/trendlabs-security-intelligence/setting-the-record-straight-on-moplus-sdk-and-the-wormhole-vulnerability/, accessed December 2015.
[49] https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/, accessed September 2015.
[50] https://blog.lookout.com/blog/2015/11/04/trojanized-adware/, accessed December 2015.

- Use of available tools on malware analysis as well as sharing of malware information and malware mitigation (i.e. MISP)[51].
- Development of security policies that specify the processes followed in cases of infection. Involve all relevant roles, including executives, operations and end-users.
- Update of malware mitigation controls regularly and adapt to new attack methods/vectors.

3.3 Web based attacks

Web based attacks are that rely on the web as a means to detect exploits and finally install malware. In order to achieve this objective, both web servers and web clients are in the focus of cyber criminals. Web based attacks include malicious URLs, compromised web pages (aka watering hole attacks), drive-by attacks, web backdoors and browser exploits. The core element of web based attacks remain malicious or bad URLs. These are URLs that have been compromised and/or contain malware or redirect to malware with the objective to infect end-user devices. With hundreds of millions of malicious URLs[53], this threat is the main instrument to deploy malicious code attacks and score at the second position of malicious online objects with ca. 32% (directly following AdWare[49]). The continuous increase of web based attacks is an indication about changes in tactics regarding infection methods, in particular the increasing role of social scams[52].

In this reporting period we have assessed that:

- Changes in tactics for infection campaigns have been observed[53]. In particular, sending malicious objects via e-mail attachments has declined in recent years. Instead, social (Facebook) scams, downloaders, redirects and phishing are gaining in importance[43,52]. It is expected that use of these methods will continue growing in the future. The role of browser exploits as a basic web based attack vector becomes apparent from the fact that browser exploits top the list as payload of the most frequently accessed malicious URLs[117,54].
- An obfuscation method used within this threat is to misuse web shells of servers using SSL and install drive-by download malware on those machines. In this case, communication between compromised server and victim devices is encrypted, thus difficult to trace. Other methods used to obfuscate is to use chains of URL re-directs that are often changed. These redirect chains lead to few high-end servers maintained by the cyber-criminals. Using permanently changing redirection URLs, make the discovery of their servers a difficult to achieve task. While 90% of bad URLs are used for spam, their characteristic is that they change within hours or minutes, making their filtering difficult[53].
- Another interesting development in the area of web based threat has been observed in 2015: malvertising campaigns use browser plugins that are bundled within “unwanted software” packages. In order to evade detection, some 4000 different names and 500 domains are being used for these plugins and used URLs. Moreover, the URL encoding scheme has been changed and normal web traffic has been used[52] instead. This tactic has proven its efficiency by increases in the number of infections.

[51] http://www.misp-project.org/, accessed November 2015.
[52] http://www.cisco.com/web/offers/pdfs/cisco-msr-2015.pdf, accessed October 2015.
[53] https://www.webroot.com/shared/pdf/Webroot_2015_Threat_Brief.pdf, accessed October 2015.
[54] https://www.sophos.com/en-us/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf?cmp=70130000001xKqzAAE, accessed October 2015.

- Ca. 58 thousand malicious URLs per day are detected at the level of CERTs[42]. This sums up to 20 million malicious URLs yearly. Given the fact that ca. 90% of those change daily/hourly, we end up with few hundreds millions of bad URLs. Blacklisting those and keep the list up to date with reliable data is a challenge, but also important to reduce malware infection[53]. It has been reported that some 80 thousand IPs are added to blacklists on a daily basis[53]. Many products/offerings have been developed in this area, including open source blacklists[55,56,57,58]. An overview of available open source blacklist offerings can be found in 59.
- A view on web based attack statistics unveils important details behind web based attacks. Top five categories of web sites exploited are: technology, hosting, blogging, business and anonymizer (i.e. services providing anonymity). The most common threats found is browser exploit, followed by virus and phishing[43]. While clicking on mailed malicious link is also considered as belonging to the top infection vectors[85]. Malicious URL is considered to be the second on the top 20 list of malicious objects online[44].
- Regarding the geography of malicious URLs, there have been some changes between 2014 and 2015. While US remains the first county hosting malicious URLs (with ca. 40% of those), in 2015 France (ca. 8%) and Germany (ca. 4%) have been replaced from second and third place by Russia (ca. 6%) and Portugal (ca. 3%). The Netherlands retained the fourth position with ca. 2% of global malicious URLs[42,117]. Interestingly, countries with the highest rate in clicking of malicious URLs are US (ca. 30%), Japan (ca. 20%) and Taiwan (ca. 4%)[117]. It is argued that the sequence of countries is related to the wealth of citizens/market and/or the availability of protection measures against abuse of web infrastructure components.

Observed current trend for this threat: *increasing*

Related threats: Malware, Exploit Kit, Phishing, Web application attacks, Spam, Botnet, Ransomware.

Authoritative Resources 2015: ”Internet Security Threat Report 20” Symantec[43] , “A Rising Tide: New Hacks Threaten Public technologies”, TrendLabs 2Q 2015 Security Roundup, Trend Micro[117], “CERT POLSKA REPORT 2014”, CERT.PL NASK 2015[42], “WEBROOT 2015 THREAT BRIEF”, WEBROOT APRIL 2015[53].

Mitigation vector: The mitigation vector for this threat contains the following elements[43]:

- 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.
- Filtering web browser traffic to detect obfuscated web based attacks.
- 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).

[55] http://www.brightcloud.com/services/web-classification.php, accessed October 2015.
[56] https://www.fireeye.com/blog/threat-research/2008/11/the-case-against-url-blacklists.html, accessed October 2015.
[57] http://urlblacklist.com, accessed October 2015.
[58] http://www.surbl.org, accessed October 2015.
[59] http://dsi.ut-capitole.fr/documentations/cache/squidguard_en.html#contrib, accessed October 2014.

- Patching of software and firmware to the latest version supported by the vendor.
- Whitelisting of applications to define legitimate software as authorised and block the execution of rogue software.
- Removing functions from web browsers that are not necessary for business processes, like Adobe Flash plugin.

3.4 Web application attacks

Given the fact that application are increasingly web enabled, that is, are open to web access or are using web resources, attacks to applications from within the web has become a major attack vector. This attack vector is referred to as web application attacks. There is a variety of attack methods to web applications, and, as applications architectures encompass additional components, the window of opportunity for web application attacks increases. Hence, "traditional" web application attacks such as cross-site scripting and SQL-injection (SQLi) exposures that were reported to be at a decreasing rate in 2014, have increased in 2015[60]. Similarly, manipulation of libraries used Software Development Kits (SDK), abuse of transported data, data leakages, abuse of vulnerabilities and evasion of vetting processes of app stores became main attack methods. All this makes web application attacks an important tool for malware injections but also for information leakage and data breaches. In the reporting period we have seen a few compromises in apps that have already passed vetting checks[46,47], while currently developed analysis techniques shed additional light to weaknesses that are "built in" in apps[61].

In the reporting period we have assessed that:

- The window of availability of web vulnerabilities in various sectors is quite large. In many sectors, a significant part of web sites (ranging from 30-55%) seem to be always vulnerable, while the part that rarely contains vulnerabilities is rather low (ranging from 18-ca. 40%). The most exposed sector seems to be public administration, with low number of vulnerabilities but very large window of remediation. The sectors with the less vulnerabilities and most efficient vulnerability remediation are arts, entertainment and education[62].
- It is worth mentioning that attacks tactics differ among web applications found on web pages and mobile applications[63]. While in mobile applications attacks are based on the quality of code, attacks on web pages abuse more often the environment of the application. On the other hand, abuse of errors (i.e. error code messages) is an attack method mainly surfaced in web applications. However, the general trends regarding attacks are similar in both web and mobile applications: abuse of APIs follows abuse of environment and abuse of security features[63]. These statistics go along the lines of generally assessed vulnerability likelihood of web applications. Here, we find at the top positions: transport layer protection, information leakage, XSS, brute force, content sniffing, cross-site request forgery and URL redirection[62].
- Application attacks are a significant part in DDoS attacks. In such DDoS attacks, SQL injection and local file inclusion (LFI) are the prevailing attack vectors (especially in HTTP)[60], while attacks on Java play a

[60] http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed6.pdf, accessed December 2015.
[61] http://sinfonier-project.net/, accessed October 2015.
[62] https://www.whitehatsec.com/press-releases/featured/2015/05/21/pressrelease.html, accessed October 2015.
[63] http://www.asial.com.au/documents/item/113, accessed October 2014.

very minor role (ca. 1%)[82]. Moreover, it is worth mentioning that SQL reflection attacks are an important attack vector in DDoS[64].

- In the reporting period we have seen Shellshock- a threat that has appeared in 2014 - reaching top position in web application attacks, especially the ones encountered over HTTPS. In total, Shellshock toped the web application attack statistics (ca. 40%), followed by SQLi (ca. 28%) and LFI (ca. 18%)[82].
- US almost monopolizes the countries targeted by web application attacks by "attracting" ca 80% of attacks worldwide. Given the fact that US is followed by Brazil (7%) and China (4%), the rest of the world shares ca. 9% of the volume of DDoS attacks on web application. In particular these statistics show that for European countries this threat is of very low relevance[82].
- Yet quite known in the security area, it is interesting to refer to evidence found reports about the efficiency of vulnerability remediation in accordance to the roles accountable for possible incidents. The biggest vulnerability remediation rates have been achieved when board of directors and executive management have been accountable for breaches. Interestingly, when breach accountability was with security department, the lowest remediation rates have been achieved[62]. It is worth noticing that the largest remediation rates of vulnerabilities are achieved when compliance is the driver, while vulnerability remediation due to a risk oriented posture is delivering lowest remediation rates.
- One can conclude that web application attacks is an area that is highly dynamic, multi-faceted and that has potential to climb further to the top cyber security threats. Especially countries with a certain wealth should expect attacks targeting applications with financial background.

Observed current trend for this threat: *increasing*

Related threats: Denial of Service, Web based attacks, Information leakage, Malware, Botnets, Data breaches.

Authoritative Resources 2015: "Website Security Statistics Report 2015" WhiteHat SECURITY[62], "akamai's [state of the internet] / security Q2 2015 report"[82], "2015 Web Application Attack Report (WAAR)", IMPREVA[60], "Cyber Risk Report 2015", HR Security Research[63].

Mitigation vector: The mitigation vector for this threat contains the following elements[120]:

- Formulation of security policies for the development and operation of applications.
- Installation of Web application firewalling (WAF)[65].
- Performance of traffic filtering to all relevant channels (web, network, mail).
- Performance of input verification.
- Deployment of bandwidth management.
- Performance of regular web application vulnerability scanning and intrusion detection.

3.5 Botnets

Botnets are one of the most important infrastructure components for the deployment of various types of cyber-attacks. Botnets consist of command and control (C&C, or C2) servers and a large number of infected

[64] https://blogs.akamai.com/2015/02/plxsert-warns-of-ms-sql-reflection-attacks.html, accessed October 2015.
[65] http://www.darknet.org.uk/2015/11/modsecurity-open-source-web-application-firewall/, accessed November 2015.

computers – usually some hundreds of thousand - that participate in the attack and can be remotely managed. Being of such an importance for cyber-crime, they are in the focus of cyber-defenders: as in previous years, in the reporting period we have seen a lot of developments regarding this cyber-threat. Globally coordinated takedowns from law enforcement have contributed to the declining trend of this threat[66], while the efficacy of this method continues being controversially discussed in the cyber-security community[67]. Cyber-criminals have continued improving methods and technology to create difficultly detectable botnets. Beyond the use of encryption and TOR, new variants of Gameover Zeus botnet, for example, have abandoned peer-to-peer (P2P) networks (upon a weakness of P2P the takedown has been performed). They also deploy domain generation algorithm (DGA) to establish C2C communication over malicious, short lived domains[68]. Moreover, attackers seem to always look for new opportunities to abuse weaknesses in order to install botnet functionality in various IT-devices[69,70].

In the reporting period we have assessed that:

- Botnet prevention policies range from take downs to individual holistic end-point protection. Both methods are quite challenging, given the inherent property of botnets to morph. Botnet takedowns are very effective in reducing this threat, at least for a certain period. The reduction of this threat in 2015 is attributed to law enforcement takedowns. Some methods for takedowns have been encountered in relevant reports[71]. The ones that are publicly known are global coordinated law enforcement takedowns[66]. In a recent cyber-security event, during the debate about efficacy of takedowns, FBI has informed that law enforcement would like to obtain enough capabilities to achieve takedowns as a quick response to botnets, by also involving other players[72]. Other players in cyber-protection argue that the best defence seems to be a unified web security solution with real time inspection functions for all kinds of data exchanged, while capitalizing on available collected, consolidated, correlated, validated and shared information[73].
- In the reporting period it has become clear that botnets are one of the most important business cases for cyber-criminals (aka botnet-for-hire) and the main element in cyber-crime consumerization. To this extend, botnets are the first item that has reached market maturity in the area of Cybercrime-As-A-Service. In the reporting period we have seen prices between USD 20 and 40 for one hour per month DDoS attacks performed via botnets, aiming at increasing attack amplification/attack bandwidth. The fact that between 20 and 40% of the DDoS attacks have botnet fingerprint[81], is indicative for the level of adoption of botnets for cyber-attacks. Enabling big impact attacks at low costs is the main driver for the increasing use of this tool[81]. At the same time this is a major concern of cyber-security experts and business users.
- Market forces dictate the existence and offered functionality of botnets. Botnet owners create such infrastructures for short period of time, take them down and go online again. The resilience of botnets has been effectively demonstrated with the ZeroAccess botnet: after the coordinated law enforcement

[66] http://www.interpol.int/News-and-media/News/2015/N2015-038, accessed October 2015.
[67] http://www.scmagazineuk.com/botnet-takedowns-are-they-worth-it/article/428021/, accessed October 2015.
[68] https://www.cloudmark.com/releases/docs/threat_report/cloudmark-security-threat-report-15q2.pdf, accessed October 2015.
[69] https://www.incapsula.com/blog/ddos-botnet-soho-router.html, accessed October 2015.
[70] https://www.bluecoat.com/security-blog/2015-01-09/botnet-internet-things, accessed October 2015.
[71] http://www.level3.com/~/media/files/white-paper/en_secur_wp_botnetresearchreport.pdf, accessed October 2015.
[72] http://swisscyberstorm.com/presentations/alan_neville.pdf, accessed October 2015.
[73] http://www.secureworks.com/assets/pdf-store/other/banking-botnets-persist-2015.pdf, accessed October 2015.

take down, the botnet has been revived (around 15th January 2015) performing a distribution of click-fraud templates[74,75]. Yet, this is not the only revived botnet. This fact comes in support of botnet takedown critics[76] . Other botnets disappear, such as Rustock and Srizbi[116]. Short time after Gameover Zeus takedown, researchers identified new variant of the botnet. It has the same code as Gameover Zeus without P2P functionality (the weakness upon which the botnet has been taken down)[73]. Instead, for backend and C2 communications it uses domain generation algorithm (DGA[77]).

- Some key figures regarding botnets contribute towards understanding their importance and role. In the reporting period, a single botnet (Nidol) is responsible for ca. 60% of all application layer attacks[81]. The average lifetime of a botnet is estimated with ca. 38 days[71]. The average size of a single botnet is ca. 1700 infected servers. In 2015, ca. 600 to 1000 C2s has been identified. Each one, in turn, consists of few hundreds of thousands of infected computers[71]. Moreover, botnets can be created in a short period but reach considerable sizes, as it was the case with the botnet of SOHO[78] or MrBlack[79] routers. Together with the information presented in the bullets above, it becomes apparent that it is difficult to identify all existing botnets (both active and inactive ones), or to hinder the creation of new ones. From this point of view, establishing a holistic security protection at the endpoints seems to be a good defence strategy.
- It has been argued, that botnet operators are in favour of using rogue virtual machines for their C2 server infrastructure. This is a shift from infecting legitimate servers with bot malware. In this way they use technological advantages of virtualized platforms, those being performance, efficient management and scaling, lower risk of detection, stability of could service, etc. The high density of botnets in areas with VM hosting providers (i.e. US), might be a phenomenon resulting this trend[71]. Statistics about countries from which C2 traffic originates show that top 10 countries such attacks originated from are: US, Ukraine, Russia, The Netherlands, Germany, Turkey, France, UK, Vietnam and Romania[71]. Though not fully representative, these statistics give an overview of geographic locations with high botnet density.

Observed current trend for this threat: *decreasing*

Related threats: Denial of Service, Web application attacks, Web based attacks, Malware, Data breaches.

Authoritative Resources 2015: "SAFEGUARDING THE INTERNET LEVEL 3 BOTNET RESEARCH REPORT", Level (3) COMMUNICATIONS[71], IMPREVA | incapsula "Q2 2015 Global DDoS Threat Landscape"[81], "Banking Botnets Persist Despite Takedowns", April 2015, Dell SecureWorks[73].

Mitigation vector: The mitigation vector for this threat contains the following elements:

- Installation and configuration of network and application firewalling.
- Performance of traffic filtering to all relevant channels (web, network, mail).

---

[74] https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf, accessed October 2015.
[75] https://www.hkcert.org/my_url/en/blog/15042801, accessed October 2015.
[76] http://searchsecurity.techtarget.com/news/4500256186/Dridex-malware-returns-despite-DoJ-arrests?utm_medium=EM&asrc=EM_NLN_49188856&utm_campaign=20151028_Dridex%20banking%20Trojan,%20botnets%20wreaking%20havoc%20again%20despite%20DOJ%20takedown_oeckerson&utm_source=NLN&track=NL-1820&ad=903816&src=903816, accessed October 2015.
[77] https://en.wikipedia.org/wiki/Domain_generation_algorithm, accessed November 2015.
[78] https://www.incapsula.com/blog/ddos-botnet-soho-router.html, accessed October 2015.
[79] http://www.extremetech.com/computing/205525-anonymous-may-have-hijacked-thousands-of-routers-for-zombie-botnet, accessed October 2015.

- Installation and maintenance of IP address blacklisting.
- Performance of Botnet Sinkholing[80].
- Performance of updates in a regular basis in orchestration with vulnerability management.

3.6 Denial of service

Also in 2015, DDoS attacks continue to be an important tool for cyber threat agents. Our analysis for this cyber threat is based mainly on data of providers of DDoS protection solutions, CERTs and threat intelligence organisations. The trends that have been unambiguously assessed are increased volumes and further optimization of attack practices[81,82]. Increase in the volume has been observed due to more attacks; but with lower average bandwidth as in the previous year[82]. Yet, in this year the average duration of the attacks has increased. A second change in the attack profile is related to the used infrastructure: there is a trend of replacing powerful equipment of the past (i.e. server-based botnet) with low end devices such as network router. In many cases, such devices have been selected from purely secured home-based components, including Internet of Things devices (i.e. home routers, various internet connected devices, embedded systems, etc.). In such environments, the use of the Universal Plug and Play Protocol is being misused by means of SSDP reflectors. This protocol has achieved a high percentage in the DDoS statistics within a year, being second but almost at the same level with SYN attacks. It is remarkable to see a warning issued by a law enforcement agency, in particular FBI, about the risks emanating from Internet of Things environments[83]. This is considered as the right step towards awareness raising. Finally, in the reporting period we have seen a new monetization attempt based on DDoS: cyber-criminals request ransom in order to stop DDoS attacks that they have launched against an organisation[84].

In the reporting period we have assessed that:

- DDoS statistics provide strong evidence about the dynamics behind this cyber-threat. Compared to similar period of 2014, significant increases in all parameters of DDoS have been encountered, in particular: over 130% increase in total number of attacks, over 120% increase in application level attacks, over 130% increase in infrastructure level attacks and 100% increase in attacks over 100 Gpbs[82]. Decreases in the average bandwidth and average volume of attacks can be attributed to changes in the attack tactics, rather than to any other defence-related aspects.
- Regarding the statistics of DDoS attacks targets, it has been reported that the sectors Gaming, Software and Technology and Internet providers are at the top 3 positions with ca. 35%, 27% and 13% respectively. Financial, retail and public sector are rather low with shares of ca. 8%, 2,5% and 1,5% of DDoS attacks[81]. On the other hand, incident information indicates that public, retail and financial organisations lead the victim statistics[85]. This fact may lead to obvious conclusions about the posture regarding DDoS defences of the latter sectors and/or about incident reporting tactics of victim organisations.

[80] http://la.trendmicro.com/media/misc/sinkholing-botnets-technical-paper-en.pdf, accessed October 2015.
[81] https://www.incapsula.com/blog/ddos-global-threat-landscape-report-q2-2015.html, accessed September 2015.
[82] https://www.stateoftheinternet.com/resources-cloud-security-2015-q2-web-security-report.html, accessed September 2015.
[83] http://www.ic3.gov/media/2015/150910.aspx, accessed September 2015.
[84] http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks/, accessed November 2015.
[85] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf, accessed September 2015.

- DDoS botnets have demonstrated the agility of adversaries in adapting their practices. While ca. 60% of the DDoS bots in 2014 identified themselves as search engine impersonator bots, this technique has been almost entirely abandoned in 2015, after defences (IP based verification techniques) have been developed[81,86]. It is interesting that in the reporting period, DDoS bots user agent variants (i.e. crawler variants that mimic legitimate user agents) have demonstrated a diversity that was not present in 2014: while in 2014 most common user agents covered ca. 90% of all attacks, in 2015 the most common ones have been found in ca. 43%[81]. Moreover, it is assumed that slow, longer lasting DDoS attacks are used to attract the attention of security teams and achieve malware infections and data exfiltration[87].
- A significant change has happened in the reporting period with regard to the used DDoS attack vectors. In 2015, single vector attacks (i.e. attacks to a single component of infrastructure layer or application) are in the majority (ca. 56%) while multiple vector attacks (i.e. attacks to multiple component of infrastructure layer or application) account for ca. 44% of the attacks. The former attack vector seems to be part of a "hit and run" tactic, a short attack that serves reconnaissance purposes of the victim's defences[81]. While multi-vector, long-duration attacks may target victims with the objective of creating damage in their systems.
- The growing cyber-crime tools market provides DDoS-as-a-service offerings. Depending on bandwidth and attack mix, prices from ca. 20 to 40 $ are common for ca. 1 hour per moth usage of DDoS botnets. There is evidence that ca. 40% of the DDoS traffic is generated by such DDoS-for-hire offerings[81,82]. It is important to underline that such services deliver to any non-specialized individual tools to perform powerful DDoS attacks at affordable prices. This fact introduces a risk potential to IT infrastructures and services that is very difficult to calculate.
- Studies performed in the reporting period have given an insight into the impact resulting a successful DDoS attack and the costs connected hereto[88,89]. As regards the impact, ca. 2/3 of victims had temporarily lost access to critical information, 1/3 have been unable to carry out main businesses and another 1/3 had lost business opportunities/contracts[88]. The costs of DDoS attacks have been calculated with 40.000$ per hour, while average costs of successful DDoS attacks may range from 40 – 500 K $. Ca. 1/3 of responders calculate costs per hour being between ca. 5 and 20K $. Costs are in analogy to the company size. These figures reflect remediation costs resulting a successful attack.

Observed current trend for this threat: *increasing*

Related threats: Botnets, Web Application Attacks, Web Based Attacks, Malware, Data Breaches, Identity theft, Information leakage.

Authoritative Resources 2015: "akamai's [state of the internet] / security Q2 2015 report"[82], IMPREVA | incapsula "Q2 2015 Global DDoS Threat Landscape"[81].

Mitigation vector: The mitigation vector for this threat contains the following elements[120]:

---

[86] http://www.youngupstarts.com/2015/08/21/q2-2015-ddos-trends-the-fall-of-search-engine-impersonators/, accessed September 2015.

[87] http://www.computerweekly.com/news/4500253349/Most-DDoS-attacks-hiding-something-more-sinister-Neustar-warns, accessed September 2015.

[88] https://media.kaspersky.com/en/B2B-International-2014-Survey-DDoS-Summary-Report.pdf, accessed September 2015.

[89] http://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf, accessed September 2015.

- Creation of a DoS/DDoS security policy including a reaction plan to detected incidents.
- 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, etc.)[90].
- 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.
- Regular reassessment needs and checking of effectiveness of implemented controls, as well as new developments.

3.7 Physical damage/theft/loss

There is not much to say about this rather trivial threat. The impressive fact about this (certainly non-cyber) threat is that it continues to be one of the leading causes for data breaches and identity theft. For this very reason, we have heighten its rank in the top 15 threat in comparison to the previous years. The increasing trend, however observed so far seems to slow down coming to a slight increase[128] to almost stable[126] in 2015. In some particular sectors such as in healthcare however, the increasing trend keeps up. This fact underlines the necessity to keep an eye on this threat by introducing mitigation controls in a sector-dependent fashion. The numbers assessed about this threat are probably affected by US incidents, as US imposes reporting obligation for physical loss. Such cases are making up a considerable part of the Identity Theft Resource Centre[91]. Naturally, the majority of loss incidents happens in the work space (ca. 55%), while ca. 22% involve vehicles[85]. These trivial facts should be part of permanent awareness measures aiming at the reduction of this threat (see also mitigation methods for this threat below).

In the reporting period we have assessed that:

- Although physical theft/loss caused by own employees is reported as the 3rd most serious reason for data breaches[85], if seen in common with theft caused by external partners, this threat is potentially at the first position, especially in particular sectors like healthcare, public/government and financial[126]. Even in global statistics about materialized threats, it ranks at ca. the 7th position[85].
- It seems that the reporting regarding physical theft/damage/loss will need some more systematic classification: in the reporting period, some researchers have seen manipulation of physical access[85] to cyber-assets belonging to this category, while others have discriminated among employees and outsiders and cases of loss (e.g. portable device loss vs. physical loss and stationary device loss[126]). This can be seen as an inconsistency in handling incidents emanating from same or similar groups (i.e. insiders). Putting this wright might help to better scrutinize the necessary controls in order to increase their efficiency.
- Physical theft/damage/loss is maybe one of the most usual causes in areas with very sensitive data, such as health and government. In particular in government, if loss of devices, physical loss and stationary device loss are subsumed under the same category, they rank as first in the breach methods (over 50%), far above hacking (ca. 17%)[126]. This is in fact also the case for the areas healthcare and

[90] http://www.arbornetworks.com/news-and-events/press-releases/2015-press-releases/5351-arbor-networks-10th-annual-worldwide-infrastructure-security-report-finds-50x-increase-in-ddos-attack-size-in-past-decade, accessed November 2015.
[91] http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf, accessed October 2015.

finance. Combined with available statistics of recent global cyber-threats, theft of devices by staff and by external partners - if taken together – it reaches 4th position in the statistics. As such, a loss is far more likely than network intrusion and denial of service[92]! In total, researchers report that ca. 23% of companies experience loss of mobile devices[93].

- It is impressive to see how often well known, rather baseline controls fail, when it is being reported about findings of confidential data on sold hardware[94,95]. This is a typical case of physical loss that has happened through negligence of basic data protection rules. Though mitigation of such risks is rather simple, the failures demonstrate that physical loss of confidential data is rather an underestimated threat that might have significant impact.

Observed current trend for this threat: *stable*

Related threats: Information leakage, Identity theft, Data Breach

Authoritative Resources 2015: "Follow the Data: Dissecting Data Breaches and Debunking Myths" Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015 Data Breach Records[126].

Mitigation vector: The mitigation vector for this threat contains the following elements:

- Use of encryption in all information storage and flow that is outside the security perimeter (devices, networks). This will eliminate the impact from this threat.
- Establishment of well communicated procedures for physical protection of assets, covering the cases of loss, damage and theft.
- Use of asset inventories to keep track of user devices and remind owners to check availability.
- Consideration of transferring the risks from this threat to an insurance.
- Installation of processes to reduce the time for the management of theft/damage/loss incidents.
- Implementation of off-site storage regimes, when applicable.

3.8 Insider threat

Insider threats continue to stay in focus during 2015. In this period, this threat has been considerably analysed and taken into account in the analysis of cyber security incidents. In the reporting period we have seen some major contributions, all of those being mentioned in the list of authoritative resources of this cyber-threat. Coming to expand the viewpoints of previous years, the insider threat now encompasses unintentional actions that have led to security incidents[96]. Together with a more holistic view on the involved agents/individuals, performed analysis regarding insider threat became more comprehensive and holistic[85,97]. And this is quite natural, given that ca. one third of cyber security incidents are attributed to unintentional and intentional activities of insiders. Surveys have shown that in encountered/analysed

[92] http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf, accessed October 2015.
[93] http://media.kaspersky.com/pdf/b2b/A_Best_Practice_Guide_to_Mobile_Security_MDM_and_MAM_2015.pdf, accessed October 2015.
[94] http://www.focus.de/digital/computer/computer-experten-finden-private-daten-auf-gebraucht-verkauften-geraeten_id_4997087.html, accessed October 2015.
[95] http://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/daten-kopierer-speichern-100.html, accessed October 2015.
[96] http://www.raytheoncyber.com/spotlight/ponemon/pdfs/3P-Report-UnintentionalInsiderResearchReport-Ponemon.pdf, accessed October 2015.
[97] http://www-05.ibm.com/at/businessconnect/assets/files/Security-XForce_Report.pdf, accessed October 2015.

security incidents it is often difficult to discriminate between careless, erroneous and intentional insider activities. Finally, the increased rates of both cyber-espionage and social engineering activities, the insider threat comes to a new light; they open up a large variety of exploitation channels for all kinds of misuse based on insider knowledge[97].

In the reporting period we have assessed that:

- Classifications of insiders foresees the following roles: current and former employees, current and former providers/contractors/consultants, current and former suppliers and business partners, customers[98]. A common characteristic of all insider threat actors is that they all have physical or remote access to information assets of the organisation, including hard copies[99]. In all these cases, particular emphasis has to be given to privileged users: over half of incidents led to data breaches are attributed to this user category[85]. Moreover, surveyed individuals have declared that privileged user control and insider threat in the context of APT are the top concerns, especially in cloud environments[100]. Finally, malicious insiders seem to abuse digital access rights in order to access to physical and logical company assets[97].
- According to a survey, the top five reasons for the materialization of insider threat (both intentional and unintentional) seem to be: reduced care of employees when dealing with sensitive data; insufficient training to apply security policies; increased work load and multitasking leading to reduced attention to security policies; inconvenience of security policies often making users ignore them, and users do not take security seriously[96].
- The impact of materialised insider threat is usually higher than that of most other threat agents, eventually with the exception of cyber-espionage. Although insider threat has so serious consequences, 75% of responders within a survey said that they will resolve insider incidents internally, without invoking police[101]. Let alone that many companies do not have an insider threat prevention program. This attitude will lead to eternalization of insider threat, as potential threat agents may repeatedly commit their atrocity within other victim organisations.
- Significant increases in incidents of insider threat may be explained by the fact that these incidents are increasingly analysed, as opposed to the time before Snowden. Other explanations of the increase are due to increasing monetization opportunities created by cyber-criminals or cyber-espionage. They might serve as a motive for insiders to offer their knowledge[102]. Another plausible source for insider threat are Bring Your Own Device and open Wi-Fi regimes that are not accompanied with effective security measures[103]. Finally, a plausible reason seem to be the increasing pressure to workers that is materialized by increased workloads and multitasking: both giving grounds to oversee security policies.
- In many cases of insider misuse attribution has been made after forensic investigations based on user actions and evidence found in user devices. Although such activities usually take place long after the threat agent has left the company, they provide intelligence about the various cases and can be used as lesson learned in order to establish appropriate protection policies[85]. Advances in data analysis and

[98] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html, accessed November 2015.
[99] http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html, accessed October 2015.
[100] http://www.vormetric.com/campaigns/insiderthreat/2015/, accessed October 2015.
[101] http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf, accessed October 2015.
[102] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf, accessed October 2015.
[103] https://www.lancope.com/resources/infographics/reality-insider-threats, accessed October 2015.

user behaviour pattern recognition are good mitigation approaches[104]. However, their implementation should not kill innovation, create fear and hinder progress in the organisation[105].

Observed current trend for this threat: *increasing*

Related threats: Malware, Data breaches, Information leakage, Identity theft, Physical theft/damage/loss, Phishing, Web application attacks, Web based attacks.

Authoritative Resources 2015: "The Unintentional Insider Risk in United States and German Organizations" Ponemon Institute LLC, July 2015[105], "Malicious or inadvertent, an insider threat to your enterprise "crown jewels" can cause significant damage. Explore ways to fight insider threats", IBM X-Force Threat Intelligence Quarterly, 2Q 2015[97], "Follow the Data: Dissecting Data Breaches and Debunking Myths" Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015 Data Breach Records[126].

Mitigation vector: The mitigation vector for this threat contains the following elements[97,106]:

- Definition of a security policy regarding insider threats.
- Use of identity and access management (IAM) solutions.
- Implementation of identity governance solutions defining and enforcing role-based access control.
- Implementation/use of security intelligence solutions.
- Use of data-based behaviour analysis tools.
- Implementation of privileged identity management (PIM) solutions.

3.9 Phishing

Phishing is a means for cybercriminals to lure users by establishing fake confidence through reference to content that looks familiar, trustful. Main objective of phishing is to steal credentials and/or install malware on the victim's device. One can argue that phishing is the advancement of spam, as it is more targeted and thus potentially more efficient; albeit having a lot of commonalities with spam as regards the infrastructure used to implement it. In order to establish the desired fake confidence, phishing piggybacks with events that are familiar in the breaking news. Or it tries to mimic look-and-feel from trustful organisations, brands, services, persons, etc. As it is the case in most of the reports analysed[107,108,43], in the context of this section phishing is differentiated from spear-phishing - a more targeted method to lure individuals. Spear-phishing is covered under the threat cyber-espionage in this report (see section 3.16). There are some good news about phishing: in 2015, we have assess some reduction of the exposure to this threat, measured by reduction of average phishing campaigns (i.e. uptime of phishing servers). This success is attributed mainly to efficient mitigation methods[108]. Following the same trend as spam, phishing is for the second year in a slightly declining trend.

In the reporting period we have assessed that:

---

[104] http://www.information-age.com/technology/security/123459786/how-leverage-user-behaviour-analytics-insider-threat-profiles, accessed October 2015.
[105] https://community.websense.com/blogs/websense-news-releases/archive/2015/07/30/survey-finds-employee-negligence-is-leading-cause-of-insider-threats-in-the-u-s-and-germany.aspx, accessed October 2015.
[106] http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf, accessed November 2015.
[107] http://apwg.org/download/document/245/APWG_Global_Phishing_Report_2H_2014.pdf, accessed November 2015.
[108] https://securelist.com/files/2015/08/KL_Q2_2015_SPAM_REPORT_ENG.pdf, accessed November 2015.

- The average uptime of a phishing campaign is an important figure indicating the duration of the campaign in hours. In the reporting period, a reduction of the uptime has been observed, from ca. 32 to about 29 hours[108]. Given that nearly half of the users who open phishing scams click on them within the first hour[85], the first day of a phishing attack seems to be the most efficient for cyber-criminals. This underlines the important to further reduce the uptime window of phishing attacks through timely detection of the phishing server.
- Like spam, phishing infrastructure is set either by registering malicious domains or by infecting legitimate servers and misusing them as phishing sites. As regards servers, cyber-criminals use available vulnerabilities to infect legitimate machines with phishing content and C2 functionality to collect user data (after successful infection). As regards malicious domains, cybercriminals use either malicious top level domains (TLDs) or subdomains[109] or Internationalized Domain Names (IDNs)[110] or services called URL-shorteners[111]. There are various mitigation levels and maturities regarding these methods. As regards TLDs, many of those have phishing mitigation in place and achieve shortening the uptime. Yet the efficiency has not fully met expectations (i.e. median uptime increased), possibly due to some issues in the timely execution of measures. The use of subdomains has been stable, while the use of UL shorteners increased[107].
- As in all cyber-threats, statistics regarding phishing are very interesting: the distribution rates of registered malicious TDL domains are (ca.): .com 62%, .tk 12%, .pw 6,2%, .cn 3,4% and .net 2,7%. It is worth mentioning that ca. 28% of all phishing domains used are registered domains. As regards the subdomain abuse method, it is estimated to be used in ca. 6-7% of all phishing attacks. The geographical distribution of phishing domains is (ca.): United States 53%, Germany 5%, United Kingdom 4%, France 3% and The Netherlands 3%[112].
- As regards the statistics of attacked industries (i.e. brand names used in phishing to lure victims), ca. 42% of phishing attacked Global Internet Portals, social networking sites 15%, banks 13,5%, Online Stores 8% and e-payment ca 6%. Top 3 targeted brands were (ca.): Yahoo with 29%, Facebook with 10% and Google with 5,5%[44]. This is slightly different as the statistics of 2014[108] with reduction of bank and e-payment phishing but increase of social media phishing scams.
- In a study that has been published in the reporting period, one can find a detailed analysis of costs related to phishing incidents[113] for a large company (i.e. 10.000 employees). It is interesting to see that the majority of costs are related to productivity losses encountered. The method followed includes, among other things, costs from loss of credentials, as well as potential malware infection and productivity costs. The per capita cost is estimated with ca 380$, whereas a training mitigation measure worth ca. 3,7$ per user would bring ca. 50% mitigation of this threat.
- Obviously, user habits are decisive for the failure or the success of phishing mitigation. It has been argued that user awareness may achieve ca. 5-10% phishing detection[85]. On the other hand, phishing tactics are decisive for the success of a campaign: a slow, persistent campaign that includes some messages leads at a rate of 90% to a success[85]. Obviously this is a spear-phishing-like attack tactic. On the other hand, untrained users are falling victims of phishing campaigns irrespectively of the awkwardness of the malicious URL. Therefore putting brand names in the domain or URL name is not a

[109] https://en.wikipedia.org/wiki/Subdomain, accessed November 2015.
[110] https://en.wikipedia.org/wiki/Internationalized_domain_name, accessed November 2015.
[111] https://en.wikipedia.org/wiki/URL_shortening, accessed November 2015.
[112] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf, assessed November 2015.
[113] http://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf, accessed November 2015.

necessary followed tactic. This makes cheap, non-obfuscated domain names fully appropriate for malicious use (e.g. hackerstuff.tk, professionalhacker.pw)[107].

Observed current trend for this threat: *Stable to slightly decreasing*

Related threats: Identity theft, Information leakage, Malware, Web based attacks, Web application attacks, Data Breach.

Authoritative Resources 2015: "Global Phishing Survey: Trends and Domain Name Use in 2H2014, An APWG Industry Advisory", APWG May 20105107, "Kaspersky SPAM AND PHISHING IN Q2 2015", Kaspersky Lab, August 2015[108], "Internet Security Threat Report 20" Symantec[43].

Mitigation vector: The mitigation vector for this threat contains the following elements[120,108,112]:

- Implementation of awareness training targeted to phishing
- Performance of secure gateway e-mail-filtering
- Performance of sender identity and DNS verification
- Detection and deletion of malicious attachments
- Scan received and clicked URLs upon malicious characteristics
- Implementation of fraud and anomaly detection
- Implementation of multiple controls for critical financial transactions

3.10 Spam

Spam, one of the oldest cyber-threats, is still a "baseline" tool for cybercriminals. Although spam is in a declining trend since some years now, its importance in the malicious arsenal remained at least almost equal: new methods of "weaponization" of this threat make it a serious threat. In the reporting period we have assessed that spam is an effective means for malware distribution. Ca. 6% of overall spam volume included malicious attachments or links[116]. Moreover, in the same period malicious Office documents and ransomware were among the distributed malicious objects[116,108,43]. Traditionally, spam had piggybacked with various national and international events/happenings. Just as phishing, in 2015 spam has abused events like the earthquakes in Nepal, the Olympic Games in Rio de Janeiro, various national elections and an abuse of recent google algorithm update[108]. On the other hand, spam is a typical representative for successes in coordinated international mitigation of cyber-threats: the falling spam numbers are results of botnets takedowns and efficient mail filtering and bad address blacklisted through vendors and governmental agencies.

In the reporting period we have assessed that:

- Spam has continued its declining trend. In 2015 a drop of ca. 7% has been assessed by the middle of 2015 (from ca. 60% in 2014 to ca. 53% of all mail traffic in 2015)[43,108]. It is very likely that this trend will keep up till the end of the year. Top spam categories were: healthcare, stock market, malicious content, dating and adult content[116]. Regarding the sources of spam, top countries are US with ca. 14,5% of spam, Russia with ca. 8% and China with ca 7%. This is a significant change since 1Q 2015, where US, Germany and China led the top spam source countries. Expectedly, these statistics are in analogy with those regarding botnets, given the fact that ca. 70% of spam is generated by bots (see also section 3.5).
- Just as botnets operators do, spammers try to massively create bad URLs that are at low or no cost and redirect to a smaller number of pages that are more laboriously structured[68]. Such low cost URLs are

shorteners (see also methods in phishing, section 3.9 **Error! Reference source not found.**) or redirection services[114]. Such ULRs are abandoned any time they are detected and/or blacklisted. While they create own shorteners, they prefer using existing (hacked) shorteners or URLs, as they hold high reputation (e.g. Twitter's t.co or lately bit.ly ones)[68]. It is worth mentioning that spammers also use IP addresses for mass mail distributions. Such IPs are represented by the octal or hexadecimal in order to fool spam filters[108].

- As already mentioned, although decreasing in number, the weaponization of spam has made progress: the rates of malware or malicious URL inclusion in spams has quadrupled since the last 2-3 years[97]! Moreover, there have been some interesting developments regarding the payload of spam: macro viruses – a ca. 15 years old malicious method- has been reused, designed to download malicious code[43,108]. This method came to surprise defenders, as such a "revival" was not expected. Another "highlight" was the relatively high level of ransomware through fake resumes sent to small-medium-enterprises[68].
- Migration of spam to mobile platforms continued in 2015. The use of Email-to-SMS gateways has been misused by spammers in order to transmit malware, scams and phishing messages to device users. The only information that is necessary is the phone number of victims. SMS messages as attack method can cause harm, as through the interconnection of apps, SMS messages can open applications on the mobile device (i.e. mobile browser) and subsequently exploit the device[43]. Here again, we see how a relatively old technology (SMS) can be misused to deploy their campaigns, mainly in the areas of adult content, Payday Load, Bank phishing and rogue pharmacy[43].
- Just as many other cyber-threats, spam is being offered as a service. Such operators undertake the weaponization of the spam according to the needs of their customers. As it is the case with other cyber-threats, prices around spam dropped too. For example one thousand stolen e-mail addresses are being offered between 0,5 to 10 $. Distribution to one million verified e-mails costs between USD70 and 100[43].

Observed current trend for this threat: *decreasing*

Related threats: Malware, Identity theft, Information leakage, Web based attacks, Web application attacks, Data Breach.

Authoritative Resources 2015: "Kaspersky SPAM AND PHISHING IN Q2 2015", Kaspersky Lab, August 2015[108], "Internet Security Threat Report 20" Symantec[43], : "2015 TRUSTWAVE GLOBAL SECURITY REPORT" Trustwave[116].

Mitigation vector: The mitigation vector for this threat contains the same elements as phishing ([120,108,112]), with some additional controls[116,68]:

- Use of a security e-mail gateway with regular (possibly automated) maintenance of filters (anti-spam, anti-malware, policy-based filtering).
- Block of executables found in mail attachments.
- 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 questions such as, 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.

[114] https://en.wikipedia.org/wiki/URL_redirection, accessed November 2015.

3.11 Exploit kits

Being developed over the few last years, exploit kits have taken a dominant position in the cyber-threat landscape. They are an automated means for the deployment of malware and hold a key role in infection vectors: they check available vulnerabilities in the targeted environment and install the appropriate malware that exploits the detected vulnerabilities. Exploit kits have mutated to one of the main tools for installation of malware. They are developed and managed in orchestration with available (zero-day) vulnerabilities, malware, malicious URLs, droppers and C&C infrastructures. Besides the establishment of relevant infrastructures, the interplay among malicious tools and threat agents establishes also a human infrastructure capable of continuously advancing attack methods and tools. It is impressive to see which innovation steps have been made to enhance sophistication, but also to increase the impact achieved in attack campaigns based on exploit kits. These developments led to an increase of 67% in exploit kit detections in the reporting period[117].

In the reporting period we have assessed that:

- At the example of Angler, the most prevalent exploit kit, one can assess the sophistication[115] level achieved. The list is quite long: quick incorporation of vulnerabilities to be exploited; memory resistant malware to evade anti-virus detection; obfuscation of virus scanners through use of cipher for payload; antivirus detection capabilities; recognition of operating system and virtualization platforms; transit encryption of payload; permanent change of locations with exploit kit code; obfuscation of code delivery methods for browser exploits[116].
- Malicious activities involving exploit kits have increased about 67% (i.e. exploit kit detections in 1H2015[117]), whereas Angler deployment numbers have tripled. It is interesting that the most affected countries cover ca. 80% of cases. These are Japan (ca. 50%), US (ca. 22%) and Australia (ca. 6%). This means that the rest of the globe has relatively low exposure to this threat!
- The wide deployment of exploit kits in cyber-crime shows how fast the gap created by the arrest of Blackwhole developer has been re-filled. After almost two years, the exploit kit activity has not only recovered, but also achieved immense growth. In the reporting period, four of the exploit kits cover ca. 90% of exploit kit detections (Angler, Magnitude, Nuclear, Neurtino)[117].
- It is impressive to see the speed of adoption of new vulnerabilities in exploit kits. Apparently, the popularity and efficiency of Angler lies in the fact of quick integration of announced vulnerabilities. Other exploit kits do not lay far behind: Angler covers 11 vulnerabilities, Magnitude and Nuclear 9 and Neutrino 8[117]. One might say that some “specialization” is recognisable: 10 of 11 Angler vulnerabilities concern Adobe vulnerabilities. It is worth mentioning that Java vulnerabilities continue with declining detection rates in 2015[118].

[115] https://threatpost.com/analyzing-angler-the-worlds-most-sophisticated-exploit-kit/110904/, accessed October 2015.
[116] https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf, accessed October 2015.
[117] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_a_rising_tide.pdf, accessed October 2015.
[118] http://www.cisco.com/assets/global/DE/unified_channels/partner_with_cisco/newsletter/2015/edition2/download/cisco-annual-security-report-2015-e.pdf, accessed October 2015.

- The deployment of attacks involving exploit kits has shown its potential, especially when attacks are crafted with the "right mix of cyber threats"[119]. According to this publication, 10 million users have been potentially be infected in 10 days. Compromised domains in Japan may be an explanation for the large number of detections in that geographical area. In general it is estimated that the return on investment for exploit kit and ransomware schemes is about 1425%[116]!
- Being one main tool for malware weaponization and delivery, exploitation and installation, exploit kit use-cases and deployment models vary according to roles taken or agreed upon by cyber-criminals in the entire attack lifecycle[120]. For example, exploit kit developers might establish a cooperation with the user of the kit, if they are allowed to deliver own malware, hence indirectly co-profiting from the launched campaign.
- Due to the skills required for development and use of exploit kits, a trust relationship between developer and user of the kit needs to be developed. Usually, such relationships are developed within underground fora/blogs.
- Efficiency of exploit kits depend on the number, severity and age of the build-in vulnerabilities to be exploited. To this extend, exploit kit developers are often parts of vulnerability discovery, acquisition and exploitation chain. In 2015, it has been reported that US Commerce Department would treat software vulnerabilities as weapons[121], in order to be in the position to prosecute cyber-criminals.

Observed current trend for this threat: *increasing*

Related threats: Web based attacks, Malware, Phishing, Web application attacks, Spam, Ransomware.

Authoritative Resources 2015: "2015 TRUSTWAVE GLOBAL SECURITY REPORT" Trustwave[116], "2015 NTT GROUP GLOBAL THREAT INTELLIGENCE REPORT" Solutionary[120], "A Rising Tide: New Hacks Threaten Public technologies", TrendLabs 2Q 2015 Security Roundup, Trend Micro[117].

Mitigation vector: Exploit kits infect systems based on their vulnerabilities. Exploit kit themselves are installed as malware. Hence the mitigation vector for this threat contains elements found in malware:

- Performance of updates in a regular basis in orchestration with vulnerability management.
- 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.

3.12 Data breaches

Data breaches are the result of successful attempts to compromise confidential information, that is, information that is protected by organisations and is important for their businesses/operations. By putting the focus on cyber-space, under data breaches we consider data losses that are materialized via cyber-threat agents. As opposed to the year 2014 that was the "*year of the data breach*", 2015 could be

[119] http://securityaffairs.co/wordpress/38943/cyber-crime/malvertising-campaign-10m-users.html, accessed October 2015.
[120] https://www.solutionary.com/threat-intelligence/threat-reports/annual-threat-report/ntt-group-global-threat-intelligence-report-2015/, accessed October 2015.
[121] http://recode.net/2015/05/21/u-s-aims-to-limit-exports-of-undisclosed-software-flaws/, accessed October 2015.

characterised as being a year of "*smooth data breach routine*". In 2015 the number of breaches remained stable (eventual very slight decrease), while there was a considerable drop in the number of breached records of ca. 40%[122]. In the reporting period we have seen quite some reports providing information on the threat agents behind data breaches. This is a positive development in general, albeit the numbers of attribution are not yet at levels similar to other crimes. Another positive development in this the fact that data breaches are more strongly put in the context of other cyber-threats. That is, the interplay of the confidential information loss with other cyber-threats has become subject of analysis (i.e. before and after the breach[85]).

In the reporting period we have assessed that:

- Despite advancements in data collection, data filtering and forensic analysis, for over 50% of the breaches it is not clear how many records have been compromised[122]. Though the reasons for this are unknown, this indicates the low level of analysis efforts invested in incident management and in data breaches in particular. When seen in combination with fact that ca. one third of attacks are of unknown kind[123], it is evident that the current statistics lack precision.
- Protection against data breaches needs to undergo a serious reconsideration. End-user expectations about data losses[124], solutions currently operated and efficiency of the controls make the diversification between perceptions and reality clear: data protection strategies need to be developed around the data and not around a perimeter[122]. This in imperative given the high level of data flow in modern IT environments (i.e. cloud, virtualization, BYOD).
- Identity information is number one breached data type (over 50%). This is the reason for looking at related cyber-threats separately in ETL (see chapter 3.13). Identity loss is followed by loss of financial access information (credentials) (over 20%), followed by existential data (confidential data or intellectual property) (over 10%) user credentials (over 10%) and nuisance data (3%)[122,126]. Top three affected sectors are government, health and technology (making up ca. 80% of the breaches)[122]. Some spread in statistics can be observed regarding the sector education (2nd position in *126* with ca 14% of breaches vs. 7th position in *122* with ca. 7% of the breaches).
- Statistics about threat agents involved in breaches show that malicious outsider (aka cyber-criminal) is the first detection with over the half of data breach incidents[122,125] (ca. 60%). Accidental loss, malicious insider, hacktivism and state sponsored espionage are following with ca. 20%, 12&, 2% and 2% respectively. These numbers are similar in some breach reports[43] with some small deviation in the numbers and threat agent groups[126].
- From the analysis existing data breach incidents numerous lessons are learned and conclusions are drawn. Their analysis goes up to the identification of their root causes and – when possible – to the final attribution. This knowledge/intelligence helps security professionals in the development of

[122] http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf, accessed September 2015.
[123] http://www.hackmageddon.com/2015/08/10/july-2015-cyber-attacks-statistics/, accessed October 2015.
[124] http://www.computerweekly.com/news/4500254985/Most-UK-workers-believe-data-theft-is-inevitable?utm_medium=EM&asrc=EM_EDA_48336546&utm_campaign=20151007_Most%20UK%20workers%20believe%20data%20theft%20is%20inevitable_&utm_source=EDA, accessed October 2015.
[125] It seems that this percentage is similar to the one of total cyber-attacks attributed to the same threat agent group. Though this might be accidental, it may also be in analogy to the total "engagement" of this threat agent group in cyber-threats. See also 123.
[126] http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data, accessed October 2015.

better protection. For this reason, legislators consider making security incident reporting mandatory, at least for incidents above a certain impact threshold. ENISA plays already a role in incident reporting in the Telecommunication sector[127].

- Discussions about impact thresholds for incident reporting will need to take place, together with acceptable models for the calculation of data breach monetization. Together with a "normalization" of data breach statistics, such measures will allow for the homogenization of data breach information. A homogenisation of the reporting, classification and analysis of incidents is needed. This will facilitate reporting and analysis of data breaches, as they will be put into a common context and will be classified accordingly.
- Evidence in 2015 has indicated that the speed of breach discovery is much lower than the speed to compromise a system[85]. One necessary step in increasing discovery of breaches is to increase the dissemination speed of knowledge derived by thorough analysis efforts.
- Based on estimations from 2014, in 2015 the cost of data breach has been assessed with ca. 2 to 4.3 million Euros for large businesses (an increase of 233% in 2014) and ca. 100k to 430k Euros for small businesses (an increase of +273% in 2014)[128,129,130]. At the same time, due to the large number of breached data in the underground market, the prices of stolen records have fallen significantly (ca. 75% in 2015)[126].

Observed current trend for this threat: *stable*

Related threats: Malware, Physical damage/theft/loss, Web Based Attacks, Web Application Attacks, Phishing, Spam, Insider threat, Information leakage, Identity theft.

Authoritative Resources 2015: "2015 DATA BREACH INVESTIGATION REPORT" Verizon[85], "2015 First Half Review" Findings from the BREACH LEVEL INDEX, gemalto[122], "Follow the Data: Dissecting Data Breaches and Debunking Myths" Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015 Data Breach Records[126], "Internet Security Threat Report 20" Symantec[43].

Mitigation vector: It is worth mentioning that 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[43]:

- Performance of data classification to assess and reflect the level of protection needed according to data categories and adapt the level of protection to the value of the data.
- Implementation of Data Loss Prevention solutions to protect data according to their class both in transit and in rest.
- Usage of encryption of sensitive data, both in transit and in rest.
- Reduction of access rights to data according to principle of least privileges.
- Development and implementation of security policies for all devices used.

[127] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2014/at_download/fullReport, accessed October 2015.
[128] http://www.pwc.co.uk/audit-assurance/publications/2015-information-security-breaches-survey.jhtml, accessed October 2015.
[129] http://www.propertycasualty360.com/2015/10/16/hacked-the-cost-of-a-cyber-breach-in-5-different-i?page=2, accessed October 2015.
[130] http://www.ponemon.org/blog/2014-global-report-on-the-cost-of-cyber-crime, accessed October 2015.

- Performance of updates in a regular basis in orchestration with vulnerability management.
- Implementation of malware protection and insider threat protection policies.

3.13 Identity theft

Identity theft is a special case of data breach. It is about theft of IDs of all kinds, that is, identity information of users. Misuse cases of this information is manifold: credentials give access to services and data that can be misused, identity related data can be used to pretend being a user of a service, identity data can be used in creating user profiles, etc. This threat represents the consumer part in breached data and is of particular importance because its misuse will directly affect customers[131], who will eventually been asked to take corrective actions[132]. In any case, a direct monetization of stolen identity information is obvious. This information is interesting to all kinds of threat agents as it can be misused in multiple ways, and as such, is a very desirable asset that can cause significant impact to end users. Given the increasing use of identity information in many important areas of life like health, finance, energy and transportation, users can be severely impacted if their identity data is misused. For this reason, incidents related to identity are often mandatorily reported[133]. As a matter of fact, statistics show that stealing personally identifiable information (PII) is at the top of reported data breaches[126]. This threat overlaps with other threats mentioned in this report. Identity theft is part of data breaches and can be materialized via information leakage, phishing or malware.

In the reporting period we have assessed that:

- According to NIST[134], personally identifiable information (PII) consists of any combination of: Full name, Home address, Email address (if private from an association/club membership, etc.), National identification number, Passport number, IP address (in some cases), Vehicle registration plate number, Driver's license number, Face, fingerprints, or handwriting, Credit card numbers, Digital identity, Date of birth, Birthplace, Genetic information, Telephone number, Login name.
- Information theft seems to be an important element in incidents in medical/healthcare industry. In the reporting period identity theft in this sector has received particular attention, from the side of defenders[135], victims[136] and vendors[126]. In the reporting period there is a significant increase in healthcare information breaches. If seen in combination with developments in the internet of things/wearables it is obvious that this threat opens up great misuse potential in the area of healthcare[137].
- Statistics in the area of identity theft shows that the threat is almost stable in the reporting year in US[138]. Nonetheless, identity theft in healthcare has increased, making up one third of breached information, sector-wise [126]. Besides healthcare, other affected sectors are retail (ca. 15%), government (ca. 13%), financial and education (ca. 10% each) [126]. Identity information (i.e. PII) is the

[131] http://rsagroup.com/rsagroup/en/home/Customer-Notice#.Vjxe0E3ovI8, accessed November 2015.
[132] http://help2.talktalk.co.uk/oct22incident, accessed November 2015.
[133] http://www.idtheftcenter.org/, accessed November 2015.
[134] http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf, accessed November 2015.
[135] http://www.reuters.com/article/2015/02/11/us-usa-healthcare-cybersecurity-analysis-idUSKBN0LF22H20150211#s2bKMeJaDt88F8AS.97, accessed November 2015.
[136] http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html, accessed November 2015.
[137] http://news.verizonenterprise.com/2015/06/wearable-security-phishing-healthcare-networkfleet/, accessed November 2015.
[138] http://hosted.verticalresponse.com/358216/5b657da747/1746749985/0f7bdaadc2/, accessed November 2015.

number one information type breached, accounting for ca 30% of all breached data types. Top three methods used to breach identity information are information leakage, malware and loss of device, accounting for more than 70% of all cases[126].

- In the meantime, various states and user/consumer organisations have understood the potential of this cyber-threat and provide information[139] on how to proactively protect identity[140,141] and how to behave when identity theft has occurred[142,143]. These offerings provide useful hints, raise awareness raising and inform about available tools at a great quality.
- Identity is an enabling factor for many applications that will emerge in the area of Internet of Things, virtualization, mobile devices and services, etc. Interoperability of identities is an area where a lot of international activities are focussing on[144,145]. At the same time, identity theft can be facilitated by vulnerabilities introduced through complexity in interoperable systems. Some leading companies in the mobile communication sector try to address interoperability with OpenID[146]. The threat of identity theft is fully counter-productive with regard to such engagements, and weakens consumer trust to online services.

Observed current trend for this threat: *stable*

Related threats: Information leakage, Phishing, Physical loss/damage/theft, Malware, Web based attacks, Web application attacks, Spam.

Authoritative Resources 2015: "Follow the Data: Dissecting Data Breaches and Debunking Myths" Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015 Data Breach Records[126].

Mitigation vector: The mitigation vector for this threat contains the following elements[140]:

- All physical identity documents and copies hereof should be adequately protected against unauthorised access. This should include documents in transit, such as ones sent via mail delivery services.
- Identity information should not be undisclosed to unsolicited recipients and their requests. Such unsolicited requests may arrive via online requests, by phone, mail or in person.
- Users should be aware of accidentally disclosing their identity data by using it in crowded places, for example by means of their devices or by means of publicly available ATMs and POS devices.
- Transactions documented by means of bank statements or received receipts should be checked regularly upon irregularities.

[139] Please note that the references provided are representative and non-exhaustive. There is a large number of resources of this sort in the internet.
[140] https://www.usa.gov/identity-theft, accessed November 2015.
[141] http://www.pc-magazin.de/ratgeber/identitaetsdiebstahl-schutz-passwort-diebstahl-online-sichern-ratgeber-3075587.html, accessed November 2015.
[142] https://www.identitytheft.gov/, accessed November 2015.
[143] http://www.ndr.de/nachrichten/netzwelt/Identitaetsdiebstahl-im-Netz-was-tun-hilfe,identitaetsdiebstahl102.html#anchor5, accessed November 2015.
[144] https://www.secureidentityalliance.org/, accessed November 2015.
[145] http://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/, accessed November 2015.
[146] http://alexandra.dk/sites/default/files/arrangementer/rump-session/oidc_dt_20140202.pdf, accessed November 2015.

- Install content filtering to filter out unwanted attachments, mails with malicious content, spam and unwanted network traffic.
- Install end-point protection by means of anti-virus programs but also block execution of files appropriately (e.g. block execution in Temp folder).
- Ensure good quality of credentials and secure methods for their storage.

3.14 Information leakage

Information leakage is about inconspicuous divulgence of small amounts of information through abuse of technical systems or through fraudulent activities. Information leakage is the data breach of individual records, that is, of small but important pieces of information. Information leakage is considered as being a different cyber threat from data breaches because stolen information differs not only quantitatively but also the qualitatively from breached data. The weaknesses that are being abused in information leakage are usually related to malfunction of technical components[147] or application functions. Such functions are misused to silently include malware in used products and services[148,149,150]. The cyber-threat information leakage causes theft of personally identifiable information (PII)[151]. In turn, PII can be used for fraud, installation of malware, misuse and data breaches. In 2015, leakage has been identified to be in the top 10 risks in web applications by OWASP[152]. Particularly attractive for adversaries are leakages in cryptographic functions, as they would reveal used secret keys. In 2014 we have seen such a threat by means of the Heartbleed attack[153]. Though none leaks of this format have been encountered in 2015, information leakage is still a major tool for threat agents as it can contribute to collection of large amounts of personal information and/or confidential data (including credentials). In the era of big data, this information has value also outside black markets[154].

In the reporting period we have assessed that:

- Scientific work has shown that unexplored weaknesses of software systems might be used for malicious purposes. Exploring existing software and infrastructure components is particularly relevant in the area of open source. In the reporting period, weaknesses in the implementation of dual IPv6 and IPv4 stacks have been demonstrated[155]. They have led to leaks via VPN clients, for all OS tested. This indicates that explorative approaches regarding leaking of critical information may carry fruits in

[147] http://electronicdesign.com/embedded/common-embedded-vulnerabilities-part-2-information-leaks, accessed November 2015.
[148] http://www.cbronline.com/news/enterprise-it/software/whatsspy-public-can-leak-your-whatsapp-info-to-strangers-110215-4509890, accessed November 2015.
[149] http://securityaffairs.co/wordpress/41483/digital-id/whatsapp-collects-call-metadata.html, accessed November 2015.
[150] http://www.v3.co.uk/v3-uk/analysis/2430510/dridex-banking-malware-security-experts-urge-public-to-be-wary-of-cyber-threat, accessed November 2015.
[151] https://en.wikipedia.org/wiki/Personally_identifiable_information#Examples, accessed November 2015.
[152] https://www.owasp.org/images/c/c3/Top10PrivacyRisks_IAPP_Summit_2015.pdf, accessed November 2015.
[153] http://heartbleed.com/, accessed November 2015.
[154] http://www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html, accessed November 2015.
[155] http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf, accessed November 2015.

various software technology and infrastructure scenarios. Given current drivers in corporate and state sponsored cyber-espionage it is obvious that such leakage scenarios are of high relevance[156].

- Often unknown to the owners of various devices, both the device operating system and installed applications may transmit data that – if needed – they can be used to identify the owner. In any case, the data collected can serve as an anonymous user profile. By default, for example, mobile phones transmit with every interaction information on version of the operating system, apps and browser used, together with (unique) identification number of the device[157], but also cookies and surfing habits. These information bits can be put together to form personalized content and context.
- The large percentage of PII in breached data shows the huge interest of cyber-criminals in this type of data, motivated through its immediate monetization opportunities. Statistics regarding data stolen from businesses and individuals, show that PII are comprise ca. 70% of stolen/breached information[126]. Not all breached PIIs have been compromised via information leakage theat. However, given that information leakage reported as the top cause of breaches[62], it is evident that most of lost PIIs have been obtained via this cyber-threat.
- Popular leakage channels remained error messages, together with improper time, state and session management[158]. In particular, security features, environment, encapsulation, input validation, errors, time and stated, code quality and API abuse are enlisted as top exploits in for the threat of identity theft[158]. In the reporting period exploits abused by this threat have increased. Vendors try to minimize leaks in memory management by issuing advisories[159] and/or blogs[160] to be followed by developers.
- Some experts have debated about the importance/impact of information leakage, arguing that if "something you have" is being leaked/compromised it is not so bad, as information about "who you are" is being leaked. Simply because the former can be replaced, eventually at moderate costs; the latter, however cannot be so easily replaced[117]. Especially if it is connected to biometric characteristics of users. In that case it can never be recovered[161].

Observed current trend for this threat: *increasing*

Related threats: Identity theft, Web based attacks, Web application attacks, Data Breach.

Mitigation vector: The mitigation vector for this threat contains the following elements[147,162]:

- 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.

---

[156] http://resources.infosecinstitute.com/the-top-five-cyber-security-vulnerabilities-in-terms-of-potential-for-catastrophic-damage/, accessed November 2015.
[157] http://dc.bluecoat.com/Mobile_Malware_Report, accessed November 2015.
[158] http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/, accessed November 2015.
[159] https://www-01.ibm.com/support/knowledgecenter/SS7K4U_8.5.5/com.ibm.websphere.base.doc/ae/ctrb_memleakdetection.html, accessed November 2015.
[160] http://stackoverflow.com/questions/31351379/how-do-i-fix-a-memory-leak-in-java, accessed November 2015.
[161] https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf, accessed November 2015.
[162] https://www.prot-on.com/tips-to-prevent-information-leaks-in-your-company, accessed November 2015.

- Performance of static analysis of application code to identify weaknesses in programming. This analysis should be done both for source and object code.
- 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.

3.15 Ransomware

Cyber-threat-wise, 2015 could be characterized as the year of ransomware. In this year, ransomware was almost doubled, reaching highest levels ever[112]. This unique increase is attributed to the fact that current ransomware variants (i.e. CTB-Locker) are difficult to detect and they come together with an aggressive phishing campaign that has led to these infection levels[112]. Current versions of ransomware use all advances of anonymization and encryption to successfully hide their traces. The abbreviation CTB in the name of CTB-Locker is indicative for the features used within this malware. CTB stands for: **C**urve - referring to elliptic curve crypto, **T**or – referring to the anonymization network and **B** – referring to bitcoin. As shown in the statistics, the ransomware threat hits citizens that are believed to be wealthier, hence primarily from North America and Europe. Ransomware is a counter-example regarding the effectiveness of taking down botnets[163]: the takedown of Gameover Zeus has certainly affected the distribution of Cryptolocker. However, after a relatively short period of a few months we have seen an infection boost with new ransomware generations introducing further technical advantages.

In the reporting period we have assessed that:

- Defence regarding ransomware should be end-point oriented. This is because just like most of malware, ransomware infections happen at user level. Given that end-point virus protection cannot defend all possible infection vectors related to this threat, additional defences need to be developed. Nevertheless, focus of defence controls is always the end-user, that is, they need to be end-point centric[164]. This does not mean parallel defences thwarting important cyber-crime infrastructure components should left out of focus[165].
- The recovery from a ransomware infection is generally not possible. Encrypted data can only be recovered via the use of cryptographic key used by the malware. And usually this is at the possession of the cyber-criminals. In some exceptional cases, successful law enforcement take downs have allowed access to cryptographic keys used. In such a case[166], for example, in cooperation with a

[163] http://www.computerworld.com/article/2490343/malware-vulnerabilities/massive-botnet-takedown-stops-spread-of-cryptolocker-ransomware.html, accessed November 2015.
[164] http://learn.avecto.com/cyber-threats-report-2015, accessed November 2015.
[165] http://blogs.cisco.com/security/talos/angler-exposed, accessed November 2015.
[166] http://thehackernews.com/2015/04/ransomware-removal-decrypt-tool.html, accessed November 2015.

security vendor, a tool has been developed to recover user data[167]. Other examples exist as well[168,169]. Such solution are very welcome, yet it is questionable if they are suitable for all kinds of users, i.e. if all users can afford not having access to their data till such a solution is eventually being offered after a successful law enforcement operation.

- Besides the fact that total ransomware has doubled in the reporting period, it is interesting to see that new ransomware types appeared in H1 2015 has quadrupled[35]. Crypto-ransomware (i.e. ransomware that encrypts files) has reached almost 50% of all ransomware with an increasing trend[170]. Ransomware campaigns continue targeting wealthy countries, US and Europe hold over 50% of the infections, while 85% of CTB-Locker infections hit in North America and Europe (50% and 35% respectively)[35]. Targets of infection campaigns are end-users (ca. 50%), enterprises (ca. 25%) and small businesses (ca. 14%)[170]. Recently, a detailed report[171] on CryptoWall has assessed the revenue from a single ransomware to be some over 300 million $.
- A remarkable novelty that has taken place in 2015 has been the establishment of cooperation among cyber-criminals by means of "affiliate programmes", a sort of crime-ware-as-a-service approach[172]. It has been established/communicated in the context of CTL-Locker ransomware. The idea behind this model is to contribute with own tools and infrastructure to ransomware campaigns and share the profits. Cyber-security experts argue that the success of CTL-Locker is due to this affiliate programme[112].
- Future developments expected in the area of ransomware will be made to maximise profit of this already lucrative business. Efforts are going be invested in improving infection rates by combining available infrastructures and establishing alliances through affiliate models. Stealthiness and obfuscation methods will be refined while available functions will be combined with existing and new vulnerabilities to move to web server sector[173]. Existing approaches are already available and are expected to be part of new ransomware variants, together with advances in encryption methods used[174]. Around the end of the reporting period, a new version of CryptoWall has appeared that implements evasion of detection even from second generation firewalls[175]. Finally, due to the fact that available tools to configure and disseminate ransomware are easy to use, less skilled cyber-criminals may use them more efficiently[176]. One can mention hereto an available ransomware-as-a-service tools that have been released and allow everyone to launch a ransomware campaign[177,178].

---

[167] https://blog.kaspersky.com/coinvault-ransomware-removal-instruction/8363/, accessed November 2015.
[168] http://www.decryptcryptolocker.com/, accessed November 2015.
[169] http://blogs.cisco.com/security/talos/teslacrypt, accessed November 2015.
[170] https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/rpt-trendlabs-2015-1q-security-roundup-bad-ads-and-zero-days-reemerging-threats-challenge-tr.pdf, accessed November 2015.
[171] http://cyberthreatalliance.org/cryptowall-report.pdf, accessed November 2015.
[172] http://www.darkreading.com/partner-perspectives/intel/franchising-ransomware/a/d-id/1321148, accessed November 2015.
[173] http://www.theregister.co.uk/2015/02/03/web_ransomware_scum_now_lay_waste_to_your_backups/, accessed November 2015.
[174] http://news.softpedia.com/news/researchers-discover-powerful-encryption-capable-ransomware-that-works-offline-495747.shtml, accessed November 2015.
[175] http://www.theregister.co.uk/2015/11/09/cryptowall_40/, accessed November 2015.
[176] https://www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html, accessed November 2015.
[177] http://securityaffairs.co/wordpress/41950/cyber-crime/fakben-ransomware-as-a-service.html, accessed November 2015.
[178] http://securityaffairs.co/wordpress/39753/cyber-crime/orx-locker-raas.html, accessed November 2015.

Observed current trend for this threat: *increasing*

Related threats: Phishing, Spam, Malware, Exploit kits, Botnet, Web based attacks, Web application attacks.

Authoritative Resources 2015: "Bad Ads and Zero Days: Reemerging Threats Challenge Trust in Supply Chains and Best Practices", Trend Micro Trend Labs 1Q 2015 Security Roundup[170], "Winning the digital security battle: Cyber threat analysis from the Avecto Malware Labs", AVECTO Whitepaper[164], "Threats Report" May 2015 McAfee[112], "Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat", Cyber Threat Alliance[171].

Mitigation vector: The mitigation vector for this threat contains the following elements, again not overlap free with measures mentioned in other cyber-threats:

- 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 back-up 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 whitelisting to prevent unknown executables from being executed at the end-points.

3.16 Cyber-espionage

Cyber-space evolves to the battlefield of the future. Nation states are currently within an arms race w.r.t. cyberspace capabilities[179]. In the reporting period, cyber-espionage operations have continue increasing and advancing in sophistication. State sponsored operations have made headlines in the reporting period. We would like to highlight few important operations in the area of cyber-espionage, namely the Sony[180] and TVMonde[181] attacks, the Bundestag breach, the disclosure of Equation Group activities[182] and the OPM data breach[183]. Although these cyber-espionage cases are just the tip of the iceberg, they take precedence over cyber-attack methods and impact:

- The Sony and TV5Monde attacks had a destructive/disruptive impact, as both cases the victim organisation was unable to operate for days/weeks due to the cyber-attack.
- The Bundestag hack[184] highlights that physical conflicts as they happened in the Eastern Europe also find their effect in the cyber-world.
- The equation group attack has demonstrated the power of attacks to cyber-physical (i.e. hardware) sub-systems.

[179] http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech, accessed November 2015.
[180] https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack, accessed December 2015.
[181] http://www.bbc.com/news/world-europe-33072034, accessed December 2015.
[182] https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf, accessed November 2015.
[183] https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach, accessed November 2015.
[184] http://securityaffairs.co/wordpress/37535/cyber-crime/russians-hacked-bundestag.html, accessed December 2015.

- The OPM hack has led to a loss (and eventually misuse) of biometric information of a large number of US public servants, a loss that cannot be recovered, as this information is unique.

Another interesting consequence of cyber-espionage is related to the blurriness in the limits between state-sponsored and industrial espionage: when big multinational players are involved, national capabilities may be used in campaigns involving hostile activist groups, competitors, and industrial espionage[120]. The grey area between state-sponsored (i.e. Advanced Persistent Threat – APT) and targeted campaigns (i.e. targeted attacks/advanced targeted attacks) is subject of discussions[185,186,187]. Following the practice of other key cyber-security players[43,85,200], we consider targeted attacks as being part of this threat, though knowing that not all targeted attacks may have espionage background. Considering targeted attacks as being part of this cyber-threat, leads to further enlargement the scope of cyber-espionage, establishing thus an overlap with activities of other threat agents[188,43].

In the reporting period we have assessed that:

- Though being assumed for some years now[189], in 2015 the cyber security community has encountered a case where manipulations are made persistent by hiding themselves in embedded software, that is, in firmware or hardware-device programming[182]. This incident has impacted the cyber-security community because it adds a new quality to cyber-attacks: they are very difficult to detect and survive operating system re-installation. In other words, the most efficient remediation of this attack would be to replace affected devices. Some similar attacks have been developed by researchers to demonstrate ways to hide malicious code in hardware[190]. On the other hand, this threat shows that there is no device that can be considered as trusted[191]. And it unveils the potential risks that are behind cyber-physical systems, i.e. systems making up the transition from the cyber to the physical world[192]. Though not new[193,194,195], this threat appears in a totally new context when seen in combination with interconnected applications and anonymization network/services. In times of increasing interoperability and integration of devices and services, this fact may have an impact that exceeds

[185] http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference/, accessed November 2015.
[186] http://securityaffairs.co/wordpress/40228/cyber-crime/targeted-attacks-vs-advanced-persistent-threats.html, accessed November 2015.
[187] https://www2.fireeye.com/ciso-guide-next-generation-threats.html?x=FE_WEB_IC, accessed November 2015.
[188] Knowing that targeted attacks are used also outside espionage campaigns, we dedicate in this report two special chapters with analysis of attack vectors used within APT and targeted attacks.
[189] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11416985/Millions-of-computers-may-be-compromised-by-US-spyware-report.html, accessed November 2015.
[190] http://arstechnica.com/security/2015/05/gpu-based-rootkit-and-keylogger-offer-superior-stealth-and-computing-power/, accessed November 2015.
[191] http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf, accessed November 2015.
[192] http://dp8hsntg6do36.cloudfront.net/55ad80d461646d4db7000005/531bc5de-3185-49d1-ae1d-2e4acb580efelow.mp4, accessed November 2015.
[193] http://www.darkreading.com/risk-management/intelligence-agencies-banned-lenovo-pcs-after-chinese-acquisition/d/d-id/1110950?, accessed November 2015.
[194] http://www.bbc.com/news/business-19879864, accessed November 2015.
[195] http://www.wsj.com/articles/u-s-navy-looks-to-replace-ibm-servers-for-security-after-lenovo-purchase-1432047582, accessed November 2015.

expectations of all involved roles in cyber-space. And it will keep a lot of actors in IT busy for the coming years[196,197,198].

- If one makes the extreme, yet not fully irrelevant assumption, that no device is un-hackable, the issue of secure storage/secure device comes into a new light. And given the fact that data stored in such storages is usually of very high value/confidentiality, one can easily assess the impact of such losses. In the reporting period, a data breach of biometric data[161,183] has shown the potential of high capability actors such as cyber-espionage. Such breaches are indicative for other trusted devices that are needed in order to perform critical services, such as e-health systems, smart grids, industrial control, etc.
- Targeted attacks are an important vector during initial phases of infiltration. They are usually materialized through spear-phishing attacks. These are targeted phishing attacks that are customized to reach a specific user community. The customization is implemented by means of social engineering and especially crafted malware[43,120]. In 2015 spear-phishing attacks have become more targeted: while their number was increasing, the number of mails per campaign was reduced. Probably this is an indication about narrower victim groups[43], and thus bigger specialization[199]. From the efficiency point of view, it is argued that spear-phishing attacks may bring 10 times the revenue of one thousand phishing mails[200].
- Statistics are indicative for the high potential behind this threat and the high level of exposure organisations have: the majority of incidents regarding this threat had no attribution[85]. This is indicative for the relatively low risk/likelihood of involved threat agents to be caught. Expectedly, top types of industries being targeted are manufacturing, public administration, professional, information and utilities[85]. The types of threat agents involved in cyber-espionage are: state-sponsored 87%, organised crime ca. 1%, competitor ca. 1% and former employees ca. 1%[201]. Looking at the installation vectors underlines the key role of spear-phishing: top three infection methods used in cyber-espionage are e-mail attachment, malicious e-mail link, and drive-by attack. They cover ca. 85% of the cases! Finally, it is worth mentioning that cyber-espionage is at the third position impact-wise, whereas for small-medium-businesses holds the first position[202].
- Obviously, zero-day vulnerabilities are a very strong tool in the hands agents with advanced capabilities and as such very desirable. There is evidence that nation states invest in exploring new vulnerabilities[203]. Consequently, driven by the needs in cyber-espionage and cyber-crime, there is a market for zero-day vulnerabilities[204,205,206]. The regulation of zero-day vulnerabilities appears to be a

---

196 https://securityledger.com/2015/09/nist-framework-tackles-cyber-physical-security/, accessed November 2015.
197 http://www.securityweek.com/our-rising-dependency-cyberphysical, accessed November 2015.
198 http://www.pcworld.com/article/2954817/security/researchers-develop-astonishing-webbased-attack-on-a-computers-dram.html, accessed November 2015.
199 https://www.invincea.com/2015/08/white-paper-1h-2015-advanced-endpoint-threat-report/, accessed November 2015.
200 https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html, accessed November 2015.
201 http://www.mcafee.com/hk/security-awareness/articles/mcafee-labs-threats-predictions-2015.aspx, accessed November 2015.
202 http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf, accessed November 2015.
203 http://www.pcworld.com/article/2947572/cyberespionage-group-pawn-storm-uses-exploit-for-unpatched-java-flaw.html, accessed November 2015.
204 http://www.wired.com/2015/04/therealdeal-zero-day-exploits/, accessed November 2015.
205 https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/, accessed November 2015.
206 https://grahamcluley.com/2015/09/researcher-demands-fireeye-pay/, accessed November 2015.

logical consequence of the developments in underground markets and developments in cyber espionage[207,208].

Observed current trend for this threat: *increasing*

Related threats: Phishing, Malware, Exploit kits, Botnet, Spam, Physical damage/loss/theft, Insider threat, Web based attacks, Web application attacks, Information leakage, Identity theft, Data Breach.

Authoritative Resources 2015:"Internet Security Threat Report 20" Symantec[43], "2015 DATA BREACH INVESTIGATION REPORT" Verizon[85]

Mitigation vector: Due to the comprehensive nature of this threat, it would contain several mitigation measures found in other threats of this report. Following advice found[209210], 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[211].
- 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[212].
- Implementation of need to know principle for access rights definition and establishment of controls to monitor misuse of privileged profiles[213].
- Establishment of content filtering for all inbound and outbound channels (e-mail, web, network traffic).

[207] https://www.lawfareblog.com/proposed-us-export-controls-implications-zero-day-vulnerabilities-and-exploits, accessed November 2015.
[208] http://moritzlaw.osu.edu/students/groups/is/files/2015/06/Fidler-Second-Review-Changes-Made.pdf, accessed November 2015.
[209] https://www.linkedin.com/pulse/44-proactive-counter-espionage-roadmap-lydia-k-phd-lkcyber-?trk=hp-feed-article-title-share, accessed November 2015.
[210] http://www.asd.gov.au/infosec/mitigationstrategies.htm, accessed November 2015.
[211] http://www.asd.gov.au/publications/protect/application_whitelisting.htm, accessed November 2015.
[212] http://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm, accessed November 2015.
[213] http://www.asd.gov.au/publications/protect/restricting_admin_privileges.htm, accessed November 2015.

3.17 Visualising changes in the current threat landscape

In comparison to the ETL 2014, there have been significant changes in the assessed cyber-threats. To facilitate the visual comparability of 2015's results, in the figure below an overview of 2014 and 2015 is given. The figure depicts changes both in threat trends but also in their ranking for all assessed cyber-threats.

Top Threats 2014	Assessed Trends 2013	Top Threats 2015	Assessed Trends 2014	Change in ranking
16. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
17. Web-based attacks	↑	2. Web based attacks	↑	→
18. Web application /Injection attacks	↑	3. Web application attacks	↑	→
19. Botnets	↓	4. Botnets	↓	→
20. Denial of service	↑	5. Denial of service	↑	→
21. Spam	↓	6. Physical damage/theft/loss	➲	↑
22. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
23. Exploit kits	↓	8. Phishing	➲	↓
24. Data breaches	↑	9. Spam	↓	↓
25. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
26. Insider threat	➲	11. Data breaches	➲	↓
27. Information leakage	↑	12. Identity theft	➲	↑
28. Identity theft/fraud	↑	13. Information leakage	↑	↓
29. Cyber espionage	↑	14. Ransomware	↑	↑
30. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

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

Table 2: Overview and comparison of Current Threat Landscapes 2014 and 2015

4. Threat Agents

4.1 Threat agent models

As regards threat agents, in the reporting year one has to repeat conclusions of the past: the issue is rather under-illuminated. In 2015, some important players in cyber-security have come to the same conclusion, asking for a better analysis of threat agents and better attribution of cyber-incidents[214].

One should wonder, however, if and which organisations may be in the position to improve attribution of incidents. While the capability maturity regarding this task is surely rather low in many organisations, some vendors may be in the position to support. Yet, costs and impact from analysis of the incident and the attribution are two factors that might be the spoilsports. How much are the costs of forensic analysis? Can companies afford paying someone to support in attribution? What to do with the results? A critical mass on experience in these areas will be necessary in order for decision makers to proceed with incident attribution.

Before going to attribution, it is argued that the cyber-security community needs to understand the whereabouts of the threat agents out there. And this involves many aspects, starting from proactive activities, such as threat agent modelling, to reactive ones, mainly related to attribution of incidents or analysis of currently active threat agent groups. In the reporting period, some progress has been made in both areas. This progress can be summarised as follows:

- A remarkable contribution to threat agent modelling has been assessed my means of a detailed analysis of threat agent motivation. This work provides strong incentives about drivers behind threat agents and helps understanding their rationale[215]. This is considered as a contribution to proactive threat agent identification.
- Some other contributions in the area identification of contemporary threat agents have been published in scientific[216], media[217] and other[218] publications. These have analysed online/real-time information found in underground fora, chat rooms and market places and draw conclusions about behaviour of cyber-criminals.
- Finally, significant information has been found on the topic of insider threat. Incidents caused by insiders have been analysed and more detail insights into the structure and motivations of this threat agent group have been published. This is also a result of reactiveness, that is, “ex post” analysis of incidents[97].

Given these developments, in this chapter we discuss the current stay-of-play in analysis of cyber threat agents and provide a short discussion including proactive vs. reactive considerations. The current situation in threat agent analysis is graphically represented in the following picture:

---

[214] https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2014, accessed November 2015.
[215] http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf, accessed November 2015.
[216] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7165944&filter%3DAND(p_IS_Number%3A7165923), accessed November 2015.
[217] http://www.telegraph.co.uk/technology/internet-security/11568376/Unmasked-the-six-hacker-tribes-you-need-to-watch-out-for.html, accessed November 2015.
[218] http://www.iss.europa.eu/uploads/media/Brief_2_cyber_jihad.pdf, accessed November 2015.

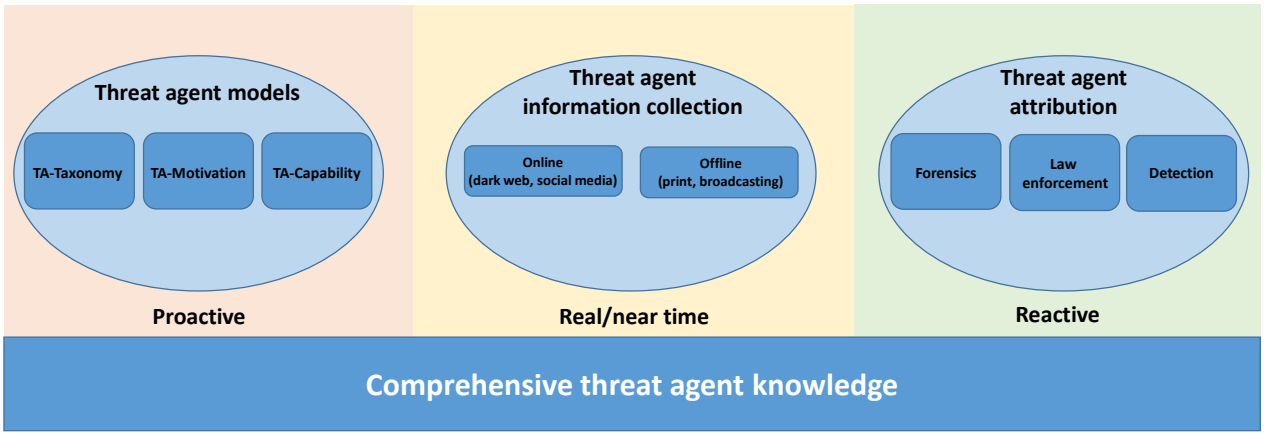

Figure 4: Content of comprehensive threat agent knowledge

Turning this figure to words it means that comprehensive knowledge about threat agents would consist or three categories of knowledge:

- *Proactive knowledge*, consisting of a threat agent model covering all relevant parameters, such as distinct threat agent groups, capabilities and skills, motivation, interactions/interrelationships among the groups, etc. Purpose of this knowledge is to be taken into account during threat or risk assessments in order to evaluate threat exposure of assets. The current state-of-play with regard such knowledge is rather initial. Besides a well-developed threat agent model[219], no much open source information has been found in 2015. We believe that this area deserves further elaboration.
- *Real/near-time knowledge*, consists of contemporary information collected from online sources (web, dark web, social media, etc.), print and broadcasting media. Existing approaches found demonstrate results from the dark web[216]. However, information on this matter, if existing, it is kept confidential, i.e. it might not be widely accessible as open source information. Examples of this knowledge are institutions of which stolen credit cards are being offered online. This kind of knowledge would be very useful for both security operations and security planning and threat/risk assessment. The unavailability of this knowledge is barrier vis-à-vis its wider use. In this field the state-of-play can be characterised as initial too. A lot more need to be done with regard to methods and tools for information and knowledge discovery in the dark net.
- *Reactive knowledge* is an outcome of analysis of incidents that have gone through successful attribution. Reactive knowledge helps understanding threat agent groups, their motivations and attack methods and is provided by vendors, law enforcement organisations or security agencies after analysis of security incidents. Though some of the incidents in the reporting year have led to attributions/arrests (indicatively[220,221222]), not much is known about the involved threat agents. Nonetheless, in 2015 significant consolidated information about insider threat has been published by

[219] https://communities.intel.com/servlet/JiveServlet/previewBody/1151-102-1-1111/Threat%20Agent%20Library_07-2202w.pdf, accessed November 2015.
[220] http://www.independent.co.uk/news/uk/home-news/talktalk-cyber-attack-fourth-person-arrested-over-hack-a6720331.html, accessed November 2015.
[221] http://edition.cnn.com/2015/10/15/politics/malaysian-hacker-isis-military-data/, accessed November 2015.
[222] http://www.bbc.com/news/technology-34504317, accessed November 2015.

some vendors [96,100,103]. Information about insiders and their motivation have led to detailed knowledge of this group. Reactive threat agent knowledge would be very useful for threat/risk assessment and security operations. The area of reactive knowledge needs further elaboration too. Though some information exists in this field, lessons learned by attributed incidents are not collected and systematically maintained. It would be very beneficial if a central repository with lessons learned by analysed incidents would be made available to security professionals.

Concluding, one may again underline the importance of threat agent knowledge for the threat landscape and in particular in threat and risk assessment. Advancements in this area would be another step towards facilitation of proper development of defences to cyber-threats. These advancements should go hand in hand with a better incorporation of threat agent knowledge at all levels of planning and operation of security controls (i.e. methods, processes and tools). Certainly an interesting task for research and standardisation organisations.

4.2 Overview of threat agents

Threat agent activities and published material found in the reporting period allow for a more detailed/precise threat agent knowledge. This is the case for some of the threat agent groups mentioned in previous ETLs, in particular cyber-criminals, insiders, hacktivists and cyber-spies. Obviously, these are the threat agent types mostly analysed/discussed in 2015 and are allegedly top initiators of cyber-incidents[223,85]. In this section we will concentrate on the threat groups where some developments have been documented, while threat groups with less dynamics will not be further developed. With this method we aim at keeping the length of this ETL moderate and avoid redundancies. Interested readers may refer to ETL2014[224] for additional information on the threat groups.

Before going into the whereabouts of each threat agent group, overall trends should be taken into account. Some important trends of the threat landscape that have explicit influence of threat agent activities are:

- *Consumerisation of cyber-crime*: the offering of inexpensive cyber-crime services is a reality. Prices for stolen data and for cyber-crime-as-a-service are in a falling trend (see also 3.10). Cyber-crime "franchising" with affiliate programmes have been seen in the wild[172]. Ransomware as-a-service is another impressive example of the consumerisation trend[177]. Even code signing certificates have become important tool for malicious applications[225]. Cyber threat agents are in the position to achieve maximum impact at low prices. This increases the risk level.
- *Low entry level barriers for technically novices*: it was never easier to launch a ransomware campaign, to make a successful SQL injection or to launch a phishing campaign[226]. These are strong fact towards enabling motivated[215] individuals to become cyber-criminals at any time[227].
- *Level of exploitation of dark net*: the dark net and dark web reminds currently the internet of the 90s: it is used only by geeks and the access to it requires some technical knowledge. In addition to that, the content of dark web is considered as evil and some technical obstacles have been implemented to de-motivate untrusted visitors sniffing in their business[216]. This reduces the possibility to "harness" dark

[223] http://www.hackmageddon.com/category/security/cyber-attacks-statistics/, accessed November 2015.
[224] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport, accessed November 2015.
[225] http://securityaffairs.co/wordpress/40866/cyber-crime/code-signing-certificates.html, accessed November 2015.
[226] http://siliconangle.com/blog/2015/10/27/15-year-old-script-kiddie-arrested-in-talktalk-hacking-investigation/, accessed November 2015.
[227] http://resources.infosecinstitute.com/25-ways-to-become-the-ultimate-script-kiddie/, assessed November 2015.

web. At the same time, information discovery in dark web is far behind compared to that of the internet. These are negative factors allowing dark web to be hideout of threat agents.

- *Low rates of attributions*: it is still difficult to get the bad guys in cyber-space[191]. Attribution levels in cyber-space are very encouraging for threat agents. In many thousands of (known) incidents, data breaches and after huge amounts of profit, only a few attributions have been made. And in cases of espionage, almost none has been arrested. This makes threat agents in cyber-space one of the professions with relatively low risks[228].

Before going into the details of threat agent groups, one might observe an overlap among some threats and threat agent groups used (e.g. insider threat vs. insider agent, or cyber espionage threat vs. cyber spy agents). This is not necessarily a redundancy content-wise: while in the threats we refer to the means with which threats are deployed (e.g. tools, methods, vectors), in the threat agents we refer more to motivations and capabilities.

According to incident statistics, top threat agent groups in 2015 are: cyber-criminals (including online social hackers), insiders, hacktivists, cyber-spies (nation states and corporations) and cyber warriors[223].Taking into account all above trends and developments in the area of threat agents, new details assessed for the threat agents are:

Cyber-criminals: While the description of this threat group from last year is still valid totally[224], one can mention some additional facts regarding this group. Firstly it should be noted that operated infrastructures, malicious tools / software and attack methods have continue advancing[229][230]. Obfuscation (non-exhaustively)[231,232,233] and hiding of viral high potential and high effort servers has advanced too[234]. Moreover, collaboration patterns such as affiliate programmes enhance the spread and depth of performed attacks[112]. Their motivation is mainly based on monetisation. This makes them perfect "candidates" for what has been reported as "espionage-as-a-service"[217]; some information found attests participation of ca. 10% of cyber-crime in espionage campaigns[201]. It is worth mentioning that information available on this threat agent seem to be primarily product of proactive (i.e. modelling) and secondarily of reactive approaches (i.e. analysis of incidents). A more balanced quality covering all three possible approaches would increase the value of information on this threat group.

Insiders (Employees): Insiders are a pretty well analysed threat agent group in the reporting period. The classification within this group has been made more detailed. Available classification of insider foresees the following insiders: current and former employees, current and former providers / contractors / consultants, current and former suppliers and business partners and customers[98]. It is important to understand who of those are privileged users. To this subgroup the majority of breaches has been attributed[100]. Irrespectively if they are internal or external, an abuse of credentials has taken place. It is

[228] http://www.digitaltrends.com/computing/how-the-fbi-hunts-down-cyber-criminals-around-the-globe/, accessed November 2015.
[229] http://www.telegraph.co.uk/news/uknews/crime/11930627/Cyber-criminals-drain-20m-from-UK-bank-accounts-using-particularly-virulent-virus.html, accessed November 2014.
[230] http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html, accessed November 2015.
[231] https://securityintelligence.com/an-example-of-common-string-and-payload-obfuscation-techniques-in-malware/, accessed November 2015.
[232] https://www.owasp.org/index.php/Bytecode_obfuscation, accessed November 2015.
[233] http://www.excelsior-usa.com/articles/java-obfuscators.html, accessed November 2015.
[234] http://blog.trendmicro.com/trendlabs-security-intelligence/adapting-to-change-how-command-and-control-servers-remain-hidden-and-resilient/, accessed November 2015.

quite interesting that besides monetization and revenge, convenience is one of the top reasons for the misuse of access rights[85]. This means that bypassing existing restrictive settings (eventually security controls) is a main reason for misuse of privileged accounts. Another interesting finding regarding this threat agent group is that most often misused credentials are those of end-users/customers, cashiers, finance and executives are following. Sys-admins are actually very low at ca. 9th position[85]. An additional risk that has to be encountered regarding insiders, is the interest other threat agent groups might have to "recruit" insiders for their malicious purposes, eventually through monetization[235]. Current information on insider threat agents originates partially from reactive analysis of related incidents and mainly from modelling. A significant resource of insider threat agent is CERT SEI Carnegie Mellon University[236], besides dedicated product/tool offerings[237]. All in all, investigation and protection against this threat agent group has reached a good maturity.

Online social hackers: Online social hacking has continue increasing in 2015. This is due to the increased role of phishing attacks that are specially crafted for a certain target group[238]. Information from social networking delivers important information to this attack vector[239]. Given that necessary tools for this kind of attacks are widely available[240], it is very easy for motivated individuals to take over this role. Nevertheless, highly sophisticated social engineering attacks can be deployed[241]. Available knowledge regarding this group is based on reactive approaches, that is, is based on analysis of incidents.

Cyber spies (Nation states, Corporations): This threat agent group has not changed with regard to motivation and course of actions[242,243]. There have been interesting developments in the capabilities of this group. It is very interesting to see advances in attack vectors used, as those will affect defence strategies in the future. The highlight of these advancements is the expansion of the attack surface to include cyber-physical systems[191]. This tactic will reduce traceability of attacks and will enhance efforts to recover from such attacks[33]; as such it is a real breakthrough. It is expected that defences are going to be developed in this area[244]. After being aware of these tactics, the cyber-security community has identified various other impressive methods to abuse cyber-physical properties of systems[245]. It is worth mentioning that In the

[235] https://www.lancope.com/blog/know-your-enemy-motivations-and-methods-insider-threat, accessed November 2015.
[236] http://www.cert.org/insider-threat/, accessed November 2015.
[237] http://www.varonis.com/products/datadvantage-insider-threats/?utm_source=google&utm_medium=cpc&utm_term=%2Binsider%20%2Bthreats&utm_content=Insider+Threats&utm_campaign=DatAdvantage+v2&gclid=CMqcq9WoiskCFSIOwwodqZ4ENg, accessed November 2015.
[238] https://securityintelligence.com/social-engineering-attackers-deploy-fake-social-media-profiles/, accessed November 2015.
[239] http://edition.cnn.com/2015/10/07/politics/iran-hackers-linkedin/, accessed November 2015.
[240] http://social-hacks.com/, accessed November 2015.
[241] http://www.crn.com/news/security/300077701/pentagon-data-breach-shows-growing-sophistication-of-phishing-attacks.htm, accessed November 2015.
[242] http://www.cio.com/article/3003192/iranian-cyberespionage-group-attacked-over-1600-high-profile-targets-in-one-year.html, accessed November 2015.
[243] http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025, accessed November 2015.
[244] http://www.darkreading.com/partner-perspectives/intel/defending-cyber-physical-systems-from-attack-chains/a/d-id/1319676?, accessed November 2015.
[245] https://blog.kaspersky.com/when-going-offline-doesnt-help/9078/, accessed November 2015.

reporting period, bilateral agreements between US and China on cyber warfare have led to arrest of Chinese cyber-spies[246].

Hacktivists: The landscape around this threat agent group remained "stable" in 2015 as regards motivation and capability levels. They continue hacking and disseminating information from organizations or people in power in order to embarrass them and to raise public awareness about alleged wrongdoings. They promote freedom of expression and openness of internet. Some campaigns have been assessed during this year[247,248] that fully comply with the activism attitude of this threat agent group. Some discussion/protests have taken place regarding the legal practice of sentencing hacktivists with the same rules as terrorists[249]. It was interesting to see Anonymous in the reporting period starting an operation against ISIS by defacing jihadist web sites and identifying 10.000 twitter and Facebook accounts used for ISIS recruitment purposes[250]. A similar announcement has been done with regard to the terroristic attacks in Paris[251], an event that may lead to a sort of "alliance" between hacktivists and security agencies[252]. In such campaigns, hacktivists turn having same targets as nation states, a fact that apparently does not always pleases the nations involved in such conflicts. However, to team up with hacktivists against a common target might be a viable reinforcement of striking power in cyber-space[253]. Finally, assessment shows that hacktivist groups may shift their focus and start a profession by means of commercial offerings stemming from activist experience[254].

Cyber fighters: Being nationally motivated, threat agents from this group may move in the interstellar space between cyber terrorists, activists and espionage. Recent announcements about Syrian Electronic Army, for example deliver evidence about this[255]: key players assumed behind this organisation still have or had close relationships to the Syrian government. A similar situation is assumed for groups like Yemen Cyber Army and Iranian Cyber Army[256]. Another interesting attack that has been encountered was motivated by terroristic attack at Charlie Hebdo[257]. The activities of the group can be assigned somewhere between this threat agent group and cyber-terrorists.

---

[246] http://www.techtimes.com/articles/94188/20151013/china-arrested-hackers-on-us-request-cyberespionage-tension-defused.htm, accessed November 2015.
[247] http://www.dw.com/en/anonymous-hacktivist-explains-why-group-is-targeting-saudi-arabian-government/a-18758195, accessed November 2015.
[248] http://www.theguardian.com/technology/2015/nov/06/anonymous-ku-klux-klan-name-leak, accessed November 2015.
[249] http://www.commondreams.org/news/2015/02/03/jailed-anonymous-hacktivist-was-watchlisted-fbi-arrest, accessed November 2015.
[250] http://thecryptosphere.com/2015/03/20/anonymous-vs-isis-the-ongoing-skirmishes-of-opisis/, accessed November 2015.
[251] https://www.youtube.com/watch?v=w49NCXhq0YI, accessed November 2015.
[252] http://www.spiegel.de/netzwelt/netzpolitik/anonymous-wie-hacker-die-is-propaganda-ausschalten-wollen-a-1063067.html, accessed November 2015.
[253] http://www.ibtimes.co.uk/isis-us-government-should-team-anonymous-fight-islamic-state-1490446, accessed November 2015.
[254] http://ghostsecuritygroup.com/, accessed November 2015.
[255] http://motherboard.vice.com/read/the-syrian-electronic-armys-most-dangerous-hack, accessed November 2015.
[256] http://motherboard.vice.com/read/theres-evidence-the-yemen-cyber-army-is-actually-iranian, accessed November 2015.
[257] http://www.bbc.com/news/technology-30850702, accessed November 2015.

Cyber terrorists: In this reporting period we have seen ISIS coming into the landscape. National security and cyber experts try to assess their striking power in the cyber space[258,259]. It has to be noted that the use of modern internet technology has been established as a communication channel and as channel for recruitment, and is being build up constantly[218,260]. To this extend, they have acted rather as social online hackers (see threat agent group above). Nonetheless, it seems that ISIS is trying to employ hackers to maintain their social networking infrastructure, that is, to operate the recruitment campaigns over social networks. Moreover, like other malicious agents, terrorists are interested in anonymous financial transaction both for collecting and distributing money[261]. This makes them acquiring resources to manage this task. Yet, terrorists using the internet for their purposes does not equals cyber-terrorism. However, by increasingly engaging in cyber-space and give the availability of cyber-crime-as-a-service, one can assume that they would be in the position to launch cyber-attacks. At the time being, experts do not believe ISIS might have significant cyber-terrorist capabilities.

Script kiddies: It is obvious that a lot of information is available in the internet to allow for launching cyber-attacks. Currently, available services make it easy to launch attacks[262,263], create own malware and ransomware. Through the increased consumerization of cyber-crime, this threat agent group might get involved in more security incidents. This developments bear increased risks that young individuals might be engaged in hacking just for the fun of it. Or even cause cyber incidents with unknown outcomes. This is a reality that might attract not only kids. In the reporting period we have assessed a major incident allegedly caused by a teenager (i.e. TalkTalk data breach)[264]. Cyber-security communities try through competitions to channel available hacking skills to positive directions[265]. These are internationally welcome initiatives that go at the right direction[266].

The figure below is an evolution of ETL2014[32] and shows and overview of threat agent groups by covering developments assessed in 2015.

[258] http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race, accessed November 2015.
[259] http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html, accessed November 2015.
[260] https://news.siteintelgroup.com/Jihadist-News/is-supporter-suggests-method-to-avoid-twitter-suspension.html, accessed November 2015.
[261] http://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856, accessed November 2015.
[262] http://resources.infosecinstitute.com/25-ways-to-become-the-ultimate-script-kiddie/, accessed November 2015.
[263] http://arstechnica.com/security/2015/07/advanced-spyware-for-android-now-available-to-script-kiddies-everywhere/, accessed November 2015.
[264] http://siliconangle.com/blog/2015/10/27/15-year-old-script-kiddie-arrested-in-talktalk-hacking-investigation/, accessed November 2015.
[265] http://www.theregister.co.uk/2015/10/23/european_cyber_security_challenge_2015/, accessed November 2015.
[266] https://haxogreen.lu/, accessed November 2015.

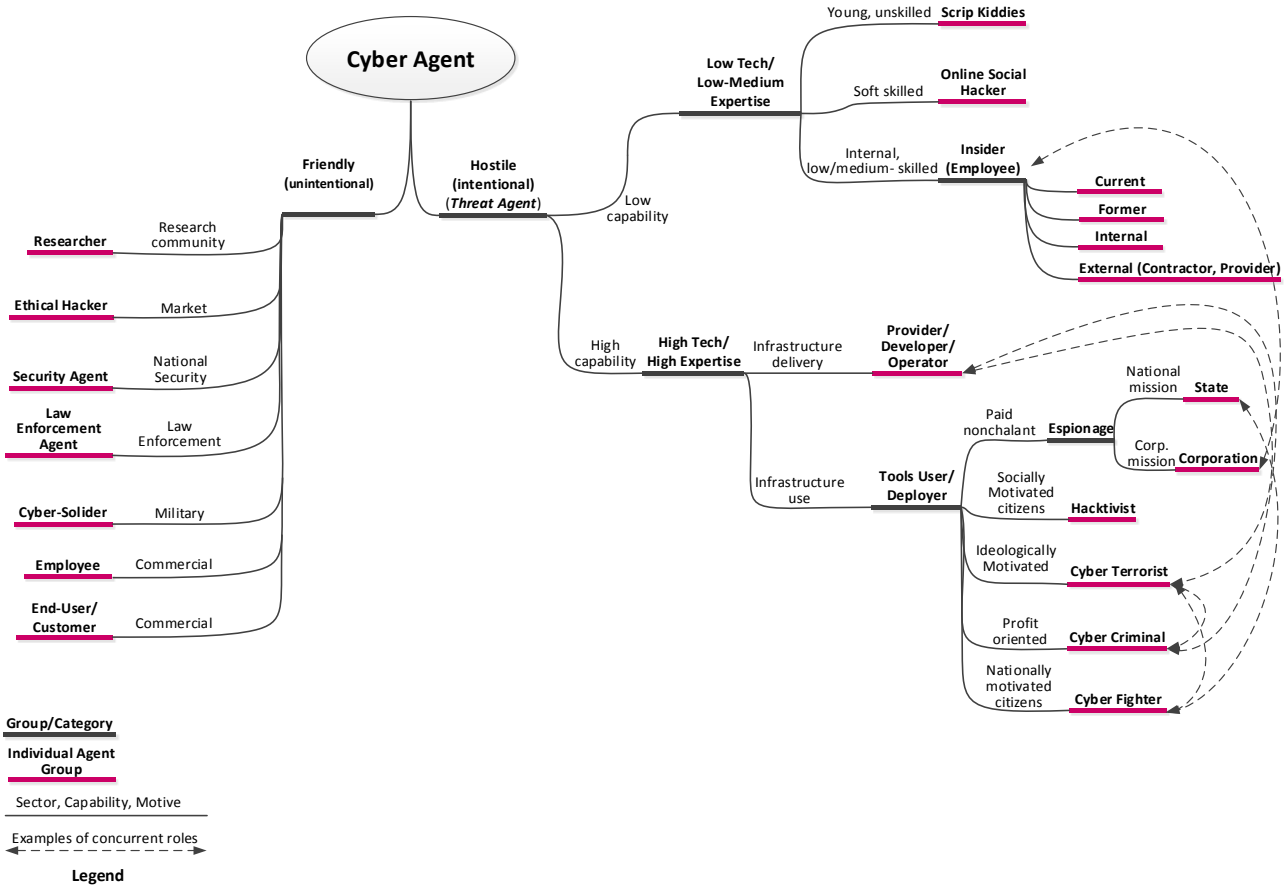

Figure 5: A proactive model as overview of threat agents

Concluding the discussion on threat agent groups, one should underline again the need to invest efforts in the area of proactive, real/near time and reactive approaches to threat agent identification.

Moreover, we believe that it might be very beneficial to consider how friendly cyber-agent/action groups might be created and mobilized to play an active role in cyber-defence. Drawing parallels to civil protection, it is argued that the cyber-security community should consider mobilizing voluntary groups of citizens willing to participate in national cyber-defence initiatives. Besides the feasibility of implementation, the mode and roles of potential involvement of action groups could be examined. Such an activity would be part of the countermeasure to cyber-threats putting the society at risk.

4.3 Threat Agents and top threats

The involvement of the above threat agents in the deployment of the identified top threats is presented in the table below (see Table 2). The purpose of this table is to visualize which threat agent groups are involve in which threats. The target group of this information are individuals who wish to assess possible threat agent involvement in the deployment of threats. This information might be useful when assessing which capability level can be assumed behind the top threats and thus support in decisions concerning the strength of the implemented security measures.

	Threat Agents								
	Cyber criminals	Insiders	Online social hackers	Nation States	Corporations	Hacktivists	Cyber Fighters	Cyber terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓			✓	✓	✓	✓	✓	✓
Web application attacks	✓			✓	✓	✓	✓	✓	✓
Botnets	✓			✓	✓	✓	✓	✓	✓
Denial of service	✓			✓	✓	✓	✓	✓	✓
Physical damage/ theft /loss	✓	✓		✓	✓			✓	
Insider threat	✓	✓		✓	✓			✓	
Phishing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Spam	✓		✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓			✓	✓	✓			✓
Data breaches	✓	✓		✓	✓	✓	✓	✓	✓
Identity theft	✓	✓		✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ransomware	✓		✓						✓
Cyber espionage		✓		✓	✓				

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

Table 3: Involvement of threat agents in the top threats

The above table indicates, for example, that ransomware is a threat that originates primarily from cyber-criminals but due to the availability of tools can be performed by less knowledgeable groups such as script kiddies and social hackers. Colours indicate primary and secondary involvement of threat agent group in the threat.

5. Attack vectors

All of the assessed cyber-threats are launched by means of a "workflow" that consists of the steps attackers undertake to materialize the threat. This workflow is called attack vector. An attack vector may be composed of one or more threats, while some steps of the attack may not be malicious at all. They may, for example, consist of reconnaissance, access to available services with the purpose of profiling, luring to visit a site, making fake offers, etc. One can say that while cyber-threats describe the "what", attack vectors provide information about the "how" of a cyber-attack.

The information regarding an attack vector is just as intuitive as the definition of risk: a threat agent uses tools (i.e. cyber-threats) to abuse weakness of some assets, thus obtaining access to these assets with the final aim to achieve their malicious objectives (illegal profit/fraud, theft of valuable data, sabotage, etc.). Attack vectors consist of steps. Each step might include an asset, its weakness/vulnerability, the tool to exploit the vulnerability and move forward to the next assets with the final consequence of a successful attack.

We consider attack vector as being of great importance in the understanding the modus operandi of cyber-threat agents. Having this information, defenders will be in the position to understand the details of the attack and put in place defences to eliminate vulnerabilities, eventually by implementing some security controls or adapting existing ones.

Information-wise, attack vectors greatly overlap with kill-chains. Kill-chains provide a generic classification scheme that can accommodate the method of an attack. Given the use of kill-chains within ENISA threat landscapes, we still use kill-chains as a reference model to describe attack vectors. In assessed reports, attack vectors are also explained via graphical means, this is a very useful and intuitive way to represent attack vectors.

In this ETL three attack vectors have been analysed, namely i) attacks against cyber-physical systems, ii) advanced persistent threat (APT) attacks and iii) targeted attacks. These three attack types have been selected because they are very prevalent and combine some threats as the deployed from high capability threat-agents. As such are good examples to understand attack tactics and eventually adapt appropriate defences.

For the description below we use some elements to structure presentations: Description is a generic description of the attack; relation to kill-chain shows how the attack unfolds; specializations describe attack variants found; existing sources provides with references to sources found: finally a list of involved threat agents is provided.

5.1 Attacks against cyber physical systems

Description: "A cyber-physical system (CPS), also referred to as "smart systems", is a system of collaborating computational elements controlling physical entities. Unlike more traditional embedded systems, a full-fledged CPS is typically designed as a network of interacting elements with physical input and output instead of as standalone device".[267] Through the developments in industrial systems[268], the amount of devices, services, connectivity, integration and diversity within CPS is constantly growing. Besides multiple devices, many different systems and supporting processes for industrial automation, home control, smart grids, smart transportation, etc. are part of CPS. One can argue that CPS is the

[267] https://en.wikipedia.org/wiki/Cyber-physical_system, accessed November 2015.
[268] https://en.wikipedia.org/wiki/Industry_4.0, accessed November 2015.

industrially oriented Internet of Things. This diversity makes CPS prone to various kinds of attacks[269]. Due to the role of such industrial, medical or home environments, a successful attack will have severe impact.

CPS structure implies that successful attacks targeting a part of CPS systems will affect a wider range of components/functions but also possibly managed physical phenomena. This might have severe economical, health and environmental losses. Objective of CPS attacks encountered in the reporting period were not data exfiltration and data breach. They were primarily targeting manipulation of engineered systems in order to affect the processes. Data exfiltration and leakage were secondary objectives. On the long term, however, it is estimated that offenders may manipulate sensors to affect integrity of input/output with the objective to achieve physical damage[244].

Relation to kill-chain: Attacks on CPS will need to explore weaknesses of all involved components, including parts of the processes of the managed physical phenomena. Such weaknesses may be related to software or hardware assets, but also physical and human aspects. The reconnaissance phase will include all these elements. If intrinsic aspects of the managed phenomena are well understood by attackers, weaponization will eventually laborious, yet feasible due to high capability agents usually involved in such attacks. Depending on the initial weakness to be exploited, installation will take place with digital means, mainly through properly crafted phishing[244]. Once the system is compromised and the malware is successfully installed, the attackers can proceed to "command and control" the compromised device by establishing a communication channel. This is the point of differentiation with non-physical attacks: With fully access to the system or device they can monitor or perform actions with direct physical effects (*actions on objectives).*

Specificities/specialisations: The main specific characteristic of this kind attacks is the direct impact on physical world. Compromising CPS may lead to attacks on critical systems and, when coordinated with other attacks, could increase the impact to threaten human life. The characteristics of a CPS attack will depend of the targeted industry, system, environment and connectivity of the attacked system. Attacks on CPS sometimes involves skillsets that go beyond hacking. Specific knowledge about the targeted system or architecture is sometimes needed for develop especially crafted software (or malware) as well. An attacker would need to have some knowledge of the control systems running, especially in highly specific systems (i.e. SCADA). However, due to the relatively long supply chains involved in such industrial systems, knowledge/intelligence about the managed phenomena and involved components might be easy to obtain[244], for example by stealing information or using social engineering techniques.

Finally, another specialization is the occasional use of attacks to supply chain both as knowledge acquisition and primary attack method. A manipulation or vulnerability included in a delivered (standard) ICT component by a supplier can be used as backdoor to numerous prospective (malicious) uses within industrial systems[244].

Existing representations overviews/resources: On attack vectors of CPS attacks, the following information was found (indicative):

- Equation Group Hard drive firmware hacking [270][271][272][273]

[269] http://www.greenbuildermedia.com/internet-of-things/hacking-the-internet-of-things, accessed November 2015.
[270] http://www.wired.com/2015/02/nsa-firmware-hacking/, accessed November 2015.
[271] https://blog.kaspersky.com/equation-hdd-malware/7623/, accessed November 2015.
[272] https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf, accessed November 2015.
[273] https://securelist.com/files/2015/02/Fanny_4.jpg, accessed November 2015.

- Jeep Cherokee: Remote car hacking [274][275][276][277]
- Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities[278]
- Cyber-Physical Attacks Against Vessel Tracking System [279][280]

Involved adversaries: Adversaries involved in CPS attacks are mainly engaged in espionage or sabotage activities undertaken by nation states or cyberterrorist .In some cases, cyberattacks [281] or coordinated activities has been performed by cybercriminals or hacktivists.

5.2 Targeted attacks

Description: Targeted attacks are malicious attacks that are aimed to a specific individual, company, system or software based on some specific knowledge regarding the target[282]. These attacks are not widespread, but rather are designed to actively pursue and compromise a target infrastructure. Based on such knowledge, adversaries proceed to craft specific messages or other artefacts to lure the victim. When arriving at the victim end, due to the familiarity that has been built (i.e. reference to a familiar personal, organisational process/matter) the message is not recognized as malicious, increasing the chances for the victim to "bite" the bait and allowing the initial infection.

Relation to kill-chain: Targeted attacks usually covers all phases of a kill chain. Usually a target attack starts with reconnaissance: the threat actor identify, collect and gather publicly available information in order to be able to customize their attack in a successful manner. In this initial phase, actors aims to obtain valuable and strategic information in many different areas such IT environment, organizational structure or personal information. The information gathered can range from the business applications and software to the roles and relationships that could exists in the organization. Is possible to find the utilization of social engineering techniques to obtain information like recent events, work-related issues concerns, and other areas of interest for the intended target for the creation of more convincing artefacts to perform the infection (weaponization). The delivery takes place by means of the time point the victim "bites the bait" and can be done through different methods depending on the organization, resources and the target.After the malicious artefact is executed, the exploitation takes place: Exploit code executes the payload and exploits vulnerability in an application component to execute specific commands in the context of end-user system. Eventually, if the exploitation is successfully executed, the malicious artefact performs an installation, usually by downloading a piece of malware on on the end-user system that may establish a communication channel (command and control) with the adversary in order to perform different actions on objective (data exfiltration, lateral movement, obtaining company information)[283].

---

[274] https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/, accessed November 2015.
[275] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, accessed November 2015.
[276] http://www.darkreading.com/jeep-hack-0day-an-exposed-port/d/d-id/1321642?_mc=RSS_DR_EDT, accessed November 2015.
[277] http://files.tested.com/photos/2014/05/06/61092-screen-shot-2014-05-06-at-3.png, accessed November 2015.
[278] https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf, accessed November 2015.
[279] https://securityledger.com/2014/12/research-finds-cyber-physical-attacks-against-vessel-tracking-system/, accessed November 2015.
[280] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais, accessed November 2015.
[281] http://thehackernews.com/2015/07/smart-city-cyber-attack.html, accessed November 2015.
[282] http://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks, accessed November 2015.
[283] http://searchsecurity.techtarget.com/feature/Targeted-Cyber-Attacks, accessed November 2015.

Specificities/specialisations: Threat actors may use varied methods to infiltrate a target's infrastructure. Common methods include customized spear phishing email, zero-day or software exploits, and watering hole techniques. Attackers also utilize instant-messaging, social engineering components and social networking platforms to entice targets to click a link or download malware[284].These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim's defences. Several of these attacks may be crafted to fit a particular sector[285,286,287,288]and may be based on hypes from breaking news, political events, crises, conflicts, etc.[289,290].

Existing representations overviews/resources: On attack vectors of targeted attacks, the following information was found:

- Targeted attack generic[291,292].
- Pawn Storm: an example Spear Phishing targeted attack[293].
- Targeted attack through SMS[294].
- Carnabank: Target attack to bank institutions with spear phishing and dropper[295,296].

Involved adversaries: All kinds of adversaries can be involved in targeted attacks: cyber-criminals, online social hackers, hacktivists, nation states, corporations, employees, cyber fighters, cyber terrorists, script kiddies

5.3 Advanced Persistent Threats (APT)

Description: Advanced Persistent Threats refer to a diverse set of stealthy processes targeting a specific entity and performed by threat agents with high capacities. They are usually encompassed in specific campaigns against particular organizations or sectors. The main intentionality of an APT attack is to steal data rather than causing any damage to the network and, in order to be successful, requires a high level of stealthiness over a prolonged duration of operation (i.e. years/months)[297].

[284] https://en.wikipedia.org/wiki/Targeted_threat, accessed November 2015.
[285] http://www.bankinfosecurity.com/cyber-attacks-target-energy-firms-a-8068/, accessed November 2015.
[286] http://www.computing.co.uk/ctg/news/2428596/banking-energy-and-education-sectors-most-targeted-by-cyber-attacks, accessed November 2015.
[287] http://www.theinquirer.net/inquirer/news/2428385/uks-education-energy-and-financial-services-under-cyber-attack, accessed November 2015.
[288] http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/, accessed November 2015.
[289] http://www.geekrepublic.org/netflix-credentials-targeted-phishing-campaign/, accessed November 2015.
[290] http://www.threatgeek.com/2015/06/cve-2014-4114-tracing-the-link.html, accessed November 2015.
[291] http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/targeted-attack-campaigns-and-trends-2014-annual-report, accessed November 2015.
[292] http://sjc1-te-ftp.trendmicro.com/images/tex/graphs/targeted-attack-components.jpg, accessed November 2015.
[293] http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts, accessed November 2015.
[294] https://securityintelligence.com/gone-phishing-how-to-prevent-sophisticated-attacks/, accessed November 2015.
[295] http://news.softpedia.com/news/Ongoing-Cyber-Attack-on-Banks-Worldwide-Creates-Billion-Dollar-Loss-473391.shtml, accessed November 2015.
[296] http://i1-news.softpedia-static.com/images/news2/Ongoing-Cyber-Attack-on-Banks-Worldwide-Creates-Billion-Dollar-Loss-473391-2.jpg, accessed November 2015.
[297] http://en.wikipedia.org/wiki/Advanced_persistent_threat, accessed December 2015.

The high capabilities shown by the threat agents are usually evidenced through a high degree of orchestration, planning and use of specially crafted malware and extensive knowledge of the victim[298]. In fact, the degree of capabilities and resources demonstrated within such attacks can mainly be attributed to teams with large resources and budget, not usually concerned with costs or direct economic revenue, as you can find in other cybercriminal groups. It is assumed that only state sponsored espionage can explain the provision of such an amount of resources.

Relation to kill-chain: By design, an advanced persistent threat (APT) uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term mission[299]. It is correct to say that an APT is operating in the full spectrum of computer intrusion and covering, therefore, all the phases of kill-chain[300] (reconnaissance, weaponisation, delivery, exploitation, installation, command and control, action on objectives)[301].

As a targeted attack, the threat agent performs different actions in order to obtain knowledge about the internal composition of the target organization: Personnel, organizational information, possible weaknesses, etc. to prepare an attack in a successful manner. Recognized attack vectors include infected media[302], supply chain compromise, and social engineering including combination of different attacks[303]. The purpose of these attacks is to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period[304]. For this purpose, different approaches has been found depending on the target's posture: From APT's using publicly available exploit against a well-known vulnerability to APT's which researches new vulnerabilities and develop custom exploits[305]. Once established a communication inside the network the attacker will usually proceed map the organization's defences and will deploy multiple kill-chains to ensure the persistence and will obtain the final actions on objectives[306].

Specificities/specialisations: APTs are also targeted attacks that are initiated by threat agents with high capabilities. They are not opportunistic or casual intruders, the adversary is formally tasked to accomplish a mission and it is organized, well-funded and motivated. Main specificity of APT is the long duration of the attack.

Another important characteristic is the differentiation between campaigns and objectives: depending of the target organization an APT attack will vary, modifying different aspects such attack vector or malware

[298] http://www.zdnet.com/article/black-vine-anthem-hackers-share-zero-days-with-rival-cyberattackers/, accessed November 2015.
[299] http://www.symantec.com/theme.jsp?themeid=apt-infographic-1, accessed November 2015.
[300] https://blogs.mcafee.com/mcafee-labs/intel-security-protecting-customers-takes-precedence-seeking-headlines/, accessed November 2015.
[301] https://en.wikipedia.org/wiki/Advanced_persistent_threat#mediaviewer/File:Advanced_persistent_threat_lifecycle.jpg, accessed November 2015.
[302] https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf, accessed November 2015.
[303] http://i1-news.softpedia-static.com/images/news2/HeartBeat-Advanced-Persistent-Threat-Aimed-at-South-Korean-Government-2.jpg, accessed November 2015.
[304] http://www.theinquirer.net/inquirer/news/2403740/chinese-hacker-group-has-been-spying-on-governments-for-a-decade-says-fireeye, accessed November 2015.
[305] http://blog.trendmicro.com/trendlabs-security-intelligence/analysis-of-cve-2015-2360-duqu-2-0-zero-day-vulnerability/, accessed November 2015.
[306] http://apac.trendmicro.com/cloud-content/us/images/icons/icon_atp-diagram-lifecycle.png, accessed November 2015.

used. Hence, each APT campaigns might have unique peculiarities in the preparation and execution of the attack[307,308,309,310](indicative list of a recent APT campaigns).

Existing representations overviews/resources: On attack vectors of APT attacks, the following information was found (indicative):

- The Dukes[311,312].
- Advanced Persistent Threat Generic [313,314,315,316].
- Turla APT Group [317].
- Equation Group APT [318].
- Cyberspionage APT Group [319].

Involved adversaries: Adversaries involved in APT attacks are mainly related to espionage or sabotage, in the past years different nation states were involved in APT attacks and, in a lesser extent, large companies. In other cases has been found APT attack actions coordinated or supported externally by cybercriminals or hacktivists or even specialized companies.

[307] https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf, accessed November 2015.
[308] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf, accessed November 2015.
[309] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf, accessed November 2015.
[310] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf, accessed November 2015.
[311] http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/seven-years-of-cyber-espionage-f-secure-unveils-the-dukes/, accessed November 2015.
[312] https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf, accessed November 2015.
[313] http://securityaffairs.co/wordpress/33999/cyber-crime/apt-and-avt-techniques.html, accessed November 2015.
[314] http://www.netswitch.net/apt-advanced-persistent-threat-what-you-need-to-know/, accessed November 2015.
[315] http://www.trendmicro.com.au/apt/stages/index.html, accessed November 2015.
[316] http://securityaffairs.co/wordpress/33999/cyber-crime/apt-and-avt-techniques.html, accessed November 2015.
[317] http://digital-era.net/turla-apt-group-abusing-satellite-internet-links/, accessed November 2015.
[318] https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf, accessed November 2015.
[319] http://research.zscaler.com/2015/08/chinese-cyber-espionage-apt-group.html, accessed November 2015.

6. Emerging Threat Landscape

In this chapter threat trends and security issues related to a number of emerging technology areas are presented. This part of the document constitutes the *Emerging Threat Landscape*. It presents the way identified cyber-threat may affect technology areas that are coming up and make up the state-of-the-art in new technological developments.

For the various areas discussed, top 10 cyber-threats are enlisted with the intention to demonstrate what the most likely exposures for the coming period will be. These cyber-threats have been assessed by the information collection effort and are an indication for the threat landscape of a particular technology area. Obviously, the assessed threat exposure will be related to some weaknesses of these technologies. Adversaries will be explore those weaknesses by exposing them to the assessed cyber-threats. Due to the emergence nature of these technologies, new exploitations will take place in the future that cannot be predicted by now. The presented material is thought of as identifying possible exposure trends.

Besides the identification of the threat exposure of each emerging technology area, a number of security issues relate to that area are also identified. These issues concern security issues emerging from various properties but also use-cases of the technology area. These issues regard highlights/conclusions/open problems that have come to our attention during the analysis of material found and/or interactions with experts within and outside ENISA. Although not exhaustive, these issues might constitute focal points for future ENISA work. For example, related issues in the area of Network Virtualisation and Software Defined Networks mentioned in last year's report have been addressed by means of a Thematic Landscape that has been developed in 2015 in that area[320]. Similarly, some of the areas that are covered in this chapter may be the subject of more detailed threat assessments within 2016, depending on feedback from ENISA stakeholders.

In 2015, emerging areas from last ETL reports have been kept. Only one has been abandoned, namely Trust Infrastructure. This is due to the fact that this area has received particular attention within ENISA, mainly through its engagement in the eIDAS activities[321].

The emerging technology areas considered in this ETL are:

- *Cloud Computing*: being an important component in modern application architectures, cloud computing is being considered within emerging technologies as main target of cyber-threats. This is mainly due to the vast number of potentially valuable information stored and/or processed. As such, it bothers security experts and users in the future. Development of security controls, innovative cloud usage, new attack scenarios are emerging security matters for this technology.
- *Mobile Computing*: Mobile computing is still an area with high innovation potential. Mobile devices continue to be platforms for the migration of application logic, covering in particular the user interaction part. Moreover, mobile platforms as such offer a big potential for innovative applications, while they are acting as a convergence/integration channel for various interconnected gadgets. We are going to see a lot of mobile-based innovation happening in the areas of smart environments, smart transportation, mobile-health, etc. As already shown by the current threat landscape, such environments will be favourite targets for cyber-criminals.

[320] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/sdn-threat-landscape, accessed January 2016.
[321] https://www.enisa.europa.eu/activities/identity-and-trust/library/presentations/june2015/06%20Gorniak%20TSP-CAB%20ENISA, accessed November 2015.

- *Cyber Physical Systems (CPS)*: Cyber-physical systems represent the "melting point" between the physical and cyber worlds. Every time software is used to manage a physical process or physical phenomena are bridged with each other via software, a cyber-physical interface is available. The integration of the physical, engineered systems with software environments enforces users to bridge existing silos, such as security and safety, product quality with performance and availability, efficiency with smart functions. These and other issues pose challenges to cyber-security.
- *Internet of Things (IoT)*: Interconnected devices forming ad hoc networks as part of some application are an area of growth and innovation. IoT can be considered as a special case of CPS, when interconnected devices cope with some physical phenomena, i.e. managing home environment, be part of assisted living, etc. IoT is an implementation of pervasive/ubiquitous computing, leading to the challenge of blurry/unstable security perimeter. IoT will force the cyber-security community to develop new approaches for securing IoT functions and data.
- *Big Data*: Besides IoT, big data is considered as the next avenue of IT innovation. By collecting data from various infrastructures, applications, storage and IT-environments - often as IT side-products- enables data collectors to draw conclusions that are themselves products. In this way, vast unstructured and initially unrelated data can be put in context and provide valuable conclusions that can be part of other products/services. As such, big data may be used to synthesize information that is security relevant, confidential, personal, etc. As such big data has a great security relevance.
- *Network Virtualization and Software Defined Networks (SDN / 5G)*: This technology will impact the area of networks in a similar way cloud computing affected traditional computing. Hardware and software network components are integrated into a virtual entity that can be operated and managed seamlessly, without paying any attention to physical elements of the network. Major investments are currently made in this area worldwide. The security challenges for this technology are going to be considerable and of a new quality.

It should be noted that, just as cyber-threats, the above areas are not completely independent or overlap free. Mobile computing and cloud computing, for example, are parts of IoT environments. Similarly, SDN/5G networks might be composed of ad hoc networks of smart components, or their management might be based on big data. Assessing threat trends according to those areas, however, allows for a better establishment of the context of each threat and helps assessing threat trends and security issues in that area. It is worth noticing that some predictions for 2016 that have been developed around the end of the reporting period use also these areas as clustering of cyber-security developments and draw similar conclusions[338,54 ,191,90].

In the following sections a short discussion including highlights in each particular area is given. For each area, whenever applicable, the top 10 threats have been assessed. In addition to the emerging threats, for each area we provide a number of important issues regarding developments/challenges in cyber-security that are seen as relevant for the particular area. It should be noted that these threat trends are not always result of detailed assessments. This is because of the emerging nature of these areas. Hence, both the prioritisation and assessed trends are predictive and as such rather indicative for each particular area.

References to resources indicate the sources used for the assessment. With this information, interested readers can have a deeper insight into the relevant matter.

6.1 Cloud computing

Cloud computing is a reality for many businesses. Besides using the cloud for their data and databases, this platform comes increasingly packaged in many end-user applications in all areas, such as web conferencing, telephony, office applications, etc. And this tendency will keep up in the future, as cloud is

inherent part in mobile environments, smart environments, Internet of Things[338], jut to mention the main emerging ones. Many users perceive cloud as secure place, as it provides security controls that seem to cover mainstream cyber-threats. It seems that majority of cloud users see security/compliance issues as main criteria for selecting a cloud solution[322].

On the other hand, many businesses, without performing any risk assessment with regard to the ratio data-value vs. threat exposure, and without checking existing security controls, trust cloud services. This is a risky situation, typical in outsourcing ventures. This is certainly not a weakness of the cloud technology per se, but of the security posture of cloud users. Fact is, that due to the confidential nature of data stored/processed in the cloud, they will sooner or later attract the attention of a wide spectrum of threat agents with a wide spectrum of capabilities.

Despite ongoing discussion about cloud security, cloud environments have increased security maturity. Various providers and associations are going through a continuous improvement of security practices[323]. They offer controls for malware analysis, audit, forensics, identity management, etc. At the same time, encountered incidents have been analysed[324] and existing controls are being adapted to accommodate changes of the threat landscape.

Top emerging threats to cloud computing are:

	Emerging Threat	Threat Trend
1.	**Malicious code**	↑
2.	**Web based attacks**	↑
3.	**Web application attacks**	↑
4.	**Botnets**	↑
5.	**Denial of Service**	↑
6.	**Insider threat**	↑
7.	**Data breaches**	↑
8.	**Cyber espionage**	↑
9.	**Identity Theft**	↑
10.	**Information leakage**	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 4: Emerging threats and their trends in the area of cloud computing

[322] https://hbr.org/resources/pdfs/comm/verizon/19319_HBR_Report_Verizon_Cloud_6.pdf, accessed November 2015.
[323] https://cloudsecurityalliance.org/research/, accessed November 2015.
[324] https://en.wikipedia.org/wiki/2014_celebrity_photo_hack, accessed November 2015.

Besides the above emerging threat landscape, the following issues have been identified:

- Attention to risk exposure from cloud usage gained by executives. This is a positive development, given that the highest remediation rates are achieved if the board is accountable for security[62]. One thing that needs the attention of decision makers, however, is the discrepancy between risk perception and risk reality. It has been reported that perceived cloud related risks are in most case higher than real ones[325]. This can be costly and misleading.
- More and more business application come with integrated cloud support. It has been reported that in an average company there are few hundreds cloud enabled applications installed[326]. With this huge number of cloud applications operated, it is essential to check cloud upon enforcement of security policies with regard to storage, communication, authentication, confidentiality, etc. In most of the cases, however, it can be assumed that there is no assurance that security policies and controls have been or can be checked upon enforcement.
- Just as customers request cloud provider to adapt their security controls to the threat environment, users of cloud should check adoption/balance between own and could offered controls. In areas where a mismatch exists, customers need to close the gaps by advising the cloud provider. In some reports this is expressed by means of a better "enterprise adoption"[325] and should concern both parties (i.e. customer and cloud provider). Whatever the degree of adoption is, the emerging threat landscape makes it necessary to assess the use of encryption, key management, mutual transparency regarding existing controls and commonly agreed security architecture development paths.
- One point that should not left out from the emerging landscape of cloud computing is its role in the current trend of the consumerization of cyber-crime. In the reporting period we have seen threat agents using advantages of cloud computing, for example to set up botnets[71]. By taking as given that the trend of cyber-crime-as-a-service will continue, the cyber-security and cloud community should pay attention on cloud usage for this purpose. One cannot exclude the use of private clouds for this purpose that might be already available in the dark net[327].

6.2 Mobile computing

In the reporting period mobile computing has started receiving the attention it deserves: departing from the mobile as "hype" and come to mobile as a tool at the hands of end-users. An initial signal in this direction came from Verizon[85], stating that "mobile is not a preferred vector for data breaches". Similarly, infections with "real" malware shown very low levels (0,03%)[85]. So, what is wrong? Do low number of misuse cases come to contradict predictions? The answer to this question has to do with the comparison of reality vs. expectations. Apparently mobile computing is a clear cut case of a vague reality assessment: expectations of security experts about wrong things to happen with mobile could not meet reality. The mismatch between reality and expectation is big.

On the other hand, in the same period other reports speak about high levels of misuse of mobile apps[328]. 8 and 7% are the rates for malicious apps coming from China and Taiwan, respectively. Malicious apps bothered us this year during the incident with Apple Store[46,47]. Such apps are reportedly collecting user

[325] http://enterprise-encryption.vormetric.com/rs/vormetric/images/Cloud-and-BigData-Edition-2015-Vormetric-Insider-Threat-Report-Final.pdf, accessed November 2015.
[326] https://resources.netskope.com/h/i/66292735-netskope-cloud-report-emea-edition-april-2015-infographic, accessed November 2015.
[327] http://www.computerweekly.com/news/2240239259/Darknet-technologies-have-legitimate-security-uses-says-researcher, accessed November 2015.
[328] http://www.marblesecurity.com/enterprise/, accessed November 2015.

information such as private data, contact databases, browser data etc. It seems that one solid misuse case for mobile devices is the collection of personal data.

Another report in 2015 concludes that the main monetization vector in the area of mobile computing seems to be malvertisement[329]. Another realistic misuse case of mobile is given due to its role in expanding the security perimeter: through spyware and traffic monitoring, identities and information can be leaked. That information can be used for data breaches by means of a secondary attack vector.

It seems that these misuse-scenarios of mobile will be the ones to be more aggressively abused in the future. To this extend, top emerging threats to mobile computing are:

Emerging Threat	Threat Trend
1. Malware	↑
2. Physical Theft/Loss/Damage	→
3. Web application attacks	↑
4. Phishing	→
5. Web based attacks	↑
6. Information Leakage	↑
7. Identity Theft	↑
8. Data breaches	↑
9. Ransomware	↑
10. Botnets	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 5: Emerging threats and their trends in the area of Mobile Computing

Besides the above emerging threat landscape, the following issues have been identified:

- Mobile computing is in most of the cases in co-existence with cloud storage and wireless networking. Definitely vast part of mobile devices use network services to synchronize stored information with cloud services or other computers. In many cases wireless networks like WLAN/Bluetooth/GSM are used for data transfer. The reason for that may be both lack of physical network ports due to size of mobile device and convenience of transferring data wirelessly instead of connecting cables. Interception of the air interface is far easier for attacker. These are typical security perimeter issues that will continue bothering us in 2016.
- Despite argumentation about "not being a preferred vector for data breaches"[85], leakage of personal data from mobile phones is a data breach. One should not forget that in the era of big data, collecting few tens of records from tens of millions of devices constitutes a "medium to large" data breach. If this

[329] https://securelist.com/files/2015/10/KLReport-IT-threat-evolution-Q3-2015_EN.pdf, accessed November 2015.

information is collected on a regular basis, the damage is huge. An additional dimension towards impact of such breaches is due to the fact that mobile data can be permanently updated and hence it does not turn obsolete after some time elapses. Another important issue regarding this leakage is that it is almost unavoidable: despite protection measures there will always be a weak point that will allow for information leakage.

- In their role as a secondary channel to a banking attack, mobiles act as a platform to steal banking credentials. In the reporting period this malicious activity has shown a significant increase and reflects another important misuse area for mobile computing, namely identity theft within two factor authentication processes. Hereto, we see malicious activities regarding spyware, SMS-Trojans and baking Trojans[329] continue bothering security experts.
- The emerging threat landscape for mobile computing will move towards prevailing usage scenarios of mobile devices: they are end-user handhelds and thus good for advertisement; they help in collecting accurate data about user habits; they serve as secondary channel for authentication and m-commerce; and they communicate a great deal of data to storage systems. Adware will continue growing, yet the impressive growth will probably speed down. Information collection will continue aggressively[191], as big data techniques mature. And attacks to credentials and identity will continue, as far as windows of opportunity are available that allow their misuse, especially in baking. Given that mobiles are often backed up, we might not see much of ransomware for mobiles.

6.3 Cyber physical systems

For the sake of this chapter, the definition of cyber-physical systems from last year's ETL will be used: Cyber physical systems are engineered systems that interact with computing equipment being seamlessly integrated to control, manage and optimize physical processes in a variety of areas from traditional engineering science[330]. In essence, a cyber-physical interface exists when a piece of software controls a physical phenomenon, such as temperature, pressure, movements of a robot, industrial processes, etc. Usually, such interfaces are implemented through embedded software programmed within a device and is being used by applications/operating systems via software drivers. To this extend, cyber-physical interfaces do exist in any device: a hard disc drive, for example is a cyber-physical system where the physical device is being controlled by software.

As already mentioned, in 2015 we have seen an important incident that has abused embedded software to load malware[182]. Such attacks are very difficult to detect and recover from. In the particular example, the hack survives reinstallation of the operating system and disk formatting. Yet, it is obvious that this resistance in defence measures are typical for embedded software, as it is not subject of any available information security control.

In the reporting period some important developments have taken place in this area, such as a draft of a cyber-physical framework to establish the basis for further discussion in this area[331]. Other reports position cyber-physical systems within industrial systems[332]. These is important step as they allow for the

[330] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport, accessed November 2015.
[331] http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf, accessed November 2015.
[332] https://www.bmwi.de/BMWi/Redaktion/PDF/I/industrie-4-0-und-digitale-wirtschaft,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, accessed November 2015.

development of standard reference architectures, common understanding and a vocabulary for CPS. Also the attention of research and development initiatives are on CPS[333].

At the level of end consumer, CPS has strong extensions in the areas of smart environments, smart transportation, e-health, but also interconnected devices. From the application point of view, consumer related applications are summarized by means of the emerging area Internet of Things (see chapter 6.4). From the physical interface point of view, smart environments are part of the present chapter.

Top emerging threats to cyber physical systems are:

	Emerging Threat	Threat Trend
1.	**Malware**	↑
2.	**Cyber espionage**	↑
3.	**Physical damage/theft/loss**	↑
4.	**Insider threat**	↑
5.	**Web based attacks**	↑
6.	**Web application attacks**	↑
7.	**Phishing (as instrument to infect IT and affect CPS)**	↑
8.	**Spam (as instrument to infect IT and affect CPS)**	↑
9.	**Denial of Service**	↑
10.	**Information leakage**	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 6: Emerging threats and their trends in the area of cyber physical systems

Besides the above emerging threat landscape, the following issues have been identified:

- Both US and EU are advancing in CPS during 2015. NIST CPS framework is a positive step towards establishment of standards in this area, including security. In Europe, series of projects have been initiated in the area of embedded systems[334]. Taking into account activities of NIST, one might argue that US are a bit ahead of EU in the settlement of standards, whereas there is a balance in the by means of research and development activities.
- As regards security issues, a major concern in the area of cyber-physical systems is the alignment of security policies between the security and physical worlds. Potential mismatches may lead to critical situations resulting failures of security controls in either environments. For example, blocking a user account after a number of login failures might not be tolerable for the physical environment, if this

[333] https://ec.europa.eu/digital-agenda/en/cyberphysical-systems-0, accessed November 2015.
[334] http://ec.europa.eu/digital-agenda/en/embedded-systems, accessed November 2015.

user is engaged in a physical process production process that needs to be managed[335]. Many such examples may be found if the security requirements of the physical system will be compared to the ones of the IT system.

- Maintenance of integrity is a fundamental qualitative issue in the interface between the cyber and physical space: none of the intermediate levels should modify values that need to be passed through. Irrespectively in which directions, any modification of input/output received from /transmitted to the physical world would mean a hazard for the entire process. Similar manipulations have taken place through Stuxnet[336].
- Equally important as integrity will be issues of availability. Both the physical system and the cyber-counterpart will need to contain balanced access control mechanisms. Similar balance needs to be established for issues of confidentiality: functions allowing data discovery in industrial systems should be subject to protective measures that are implemented at the levels of the IT systems in change (e.g. network levee, application level). Finally physical characteristics of the controlled components may allow to malicious users to damage the equipment[337]. This may turn information about the physical process implemented subject to confidentiality rules. The interplay of between cyber and physical is not obvious, as there are typical silos that need to be bridged in order to achieve this objective[331] (e.g. security vs. safety, resilience vs. reliability, etc.).
- Just as it is the case in IoT, in cyber-physical system components are going to join and leave a system on an ad hoc basis. Given the importance of components in the performance of processes in the engineered system in question, trust functions need to be developed for the interacting components. Depending on the importance of the process (e.g. gas distribution) and the role of the component (e.g. pressure meter), it might be necessary to establish a trusted communication. As of today, no components exist that support such functions (i.e. in the context of cyber-physical communication)[191].

6.4 Internet of things (IoT)

As far as cyber-threats is concerned, Internet of Things was one of the main fields in the 2015's landscape. This was quite foreseeable already in 2015. And it is foreseeable that this trend is going to continue for 2016[338,191]. The drivers behind this trend are: i) besides the proliferation of IoT devices in home environments, one can observe an increased role of wearables in the area of health; ii) the increased use of wireless connectivity among devices is of all kinds in various sectors of life is here to stay (i.e. such as interconnected sensors[339], automotive[340341] and smart environments); iii) interaction of all components with mobile and cloud platforms a key of their architecture design.

The attacks that have taken place in 2015 have abused weaknesses in basic security controls. Malware attacks have led to a takeover of routers to form botnets[69,70]. The abused weaknesses are due to missing or ill-configured security controls and practices. On the other hand, although privacy of IoT was and remain a

[335] http://www.securityweek.com/cyberphysical-security-next-frontier, accessed November 2015.
[336] https://en.wikipedia.org/wiki/Stuxnet, accessed November 2015.
[337] http://www.networkworld.com/article/2968432/microsoft-subnet/cyber-physical-attacks-hacking-a-chemical-plant.html, accessed November 2015.
[338] http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf , accessed November 2015.
[339] http://www.esp8266.com/, accessed November 2015.
[340] http://www.mcafee.com/ca/resources/white-papers/wp-automotive-security.pdf, accessed November 2015.
[341] https://en.wikipedia.org/wiki/Vehicular_ad_hoc_network, accessed November 2015.

concern[342,343], not much privacy breaches/incident have been assessed in 2015. However, in 2015 identity information has topped types of breached data. And such data have been breached from mobile devices, in particular in the area of health. In addition, with the proliferation of big data techniques, information "crumbs" found in ad hoc wireless networks will be valuable input in profile building.

An additional dimension related to IoT are cyber-physical security issues addressed within this report (see chapters 3.16 and 6.3). When exploring cyber-physical systems of a smart home environment, for example, one might be in the position to create the perfect ransomware[344]; or be in the position to generate severe impact to the house lord by impacting vital functions of the building (i.e. electricity, heat, etc.).

IoT security issues definitely relate with the complexity resulting the convergence of multiple platforms and applications into a system-of-systems. Sensors are wirelessly interconnected with mobile gadgets, these gadgets communicate with storage and applications hosted in the cloud; these systems may be managed by users over mobile devices. In these cyclic dependencies among components, exploits may have amplification effect on impacts throughout the entire chain of interrelated components. These and similar security issues are subject of ENISA work to be released in 2016 in the area of Smart Cities[345] and Transportation[345]. This work is based on a threat assessment based on the present threat landscape.

Top emerging threats to internet of things/interconnected devices/smart environments are:

	Emerging Threat	Threat Trend
1.	**Malware**	↑
2.	**Botnets (abusing IoT components as botnet nodes and/or C2 servers)**	↑
3.	**Identity theft**	↑
4.	**Web based attacks**	↑
5.	**Physical theft/damage/loss**	↑
6.	**Phishing**	↑
7.	**Insider threat**	↑
8.	**Information leakage**	↑
9.	**Web application attacks**	↑

[342] http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf, accessed November 2015.
[343] https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, accessed November 2015.
[344] http://www.csoonline.com/article/2960787/cyber-attacks-espionage/report-iot-is-the-next-frontier-for-ransomware.html, accessed November 2015.
[345] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices/at_download/fullReport, accessed December 2015.

	Emerging Threat	Threat Trend
10.	**Denial of Service**	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 7: Emerging threats and their trends in the area of Internet of things, interconnected devices and smart environments

Besides the above emerging threat landscape, the following issues have been identified:

- Though the exploitations we have seen till now are just of reduced scope and impact, it is a matter of time to see attacks affecting more than one levels/components of an IoT scenario. Particular impact may be created to denial of service attacks to devices that are critical for human health, i.e. in assisted living systems[346]. It is worth mentioning that due to the long chain of dependencies between involved/interconnected components, single points of failure and weakest link exploitation of IoT components are to be taken care of[347].
- Just as it is the case in the web, where commercial players are gathering information about user behaviour, IoT will be a premium place to collect consumer data about intimate, highly marketable information on habits of individuals. This information will be equally interesting for malicious agents aiming at understanding the habits of the victims, including the ones interested in physical assets (i.e. e burglars).
- Security and privacy considerations of entire IoT systems may arise sometime after their implementation, when the interplay of components has been set within a certain application scenario. Willing to fulfil such requirements ex-post, might be very costly, especially when individual components involved do not support functions to implement those requirements[348]. In monolithic legacy applications, though difficult, adding additional security controls was more feasible, even by adding them as external to the application at stake. This will not be so easy with interconnected components, mainly due to the ever changing perimeter.
- From incident statistics becomes evident that human error and insider threats, if taken together, are sufficient to top the list of cyber-threats. Given the fact that IoT will be used mainly by cyber-novices and, given the relatively large number of "insiders" within a smart environment (i.e. smart home), it needs not much prediction skills to find the prime source of IoT abuse. These are going to be users and all insiders surrounding them.
- Gradual proliferation of IoT applications will pose additional requirements to the internet infrastructure. Surveys refer to bandwidth issues for various families of components, starting from WiFi frequencies to network traffic, server and application processing capabilities[342]. This will be the case for cloud environments that will be main information storage components.
- When various sensors and components join or leave an ad hoc (wireless) network, it is necessary to check level of trust. According to that level, they might be allowed (or not) to access parts of the available services and data. Though some infrastructures support security functions and establish trust

[346] http://www.demorgen.be/technologie/anonymous-probeert-ehealth-te-hacken-b8614dbe/, accessed November 2015.
[347] https://securelist.com/analysis/publications/72595/surviving-in-an-iot-enabled-world/, accessed November 2015.
[348] https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers, accessed November 2015.

levels[349], trust functions are not based on device properties but rather on functions of the infrastructure. Although it is a remarkable offering, infrastructure-based security measures might significantly increase operation costs of IoT applications.

- But there are also positive developments in this area. It is remarkable that IoT security offerings are appearing in the market[349]. Moreover, numerous research and development programmes have been kicked off, taking care of security in IoT[350]. Security vendors provide information related to IoT vulnerabilities and attack methods[347] to create awareness among users.

6.5 Big data

This is the third consecutive year big data appear in ETL's emerging technologies. In past reports[224] the business side and threat intelligence point of view have been discussed; both areas continue to be heavily developed. According to estimates, it is believed that "*the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020*"[351], becoming a significant economic drive. Scientific big data continue to proliferate and many agencies and institutions in Europe and worldwide have or will launch big data projects to facilitate scientific data analysis and exploitation[352] (e.g. the European Centre for Nuclear Research (CERN) – Worldwide LHC Computing Grid[353], the European Space Agency big data Initiative[354] [355], the UK Data Service[356] etc.).

Big data technologies have already been deployed within national security applications, an important force behind current and future big data research and development[357]. Operations such as fighting terrorism; assisting in combat; gathering and analysing intelligence from heterogeneous sources, including battlefield data and open sources; casual model predictions; or even preventing army suicides[358] are expected to significantly benefit from big data analytics. Big data seems to be the solution as data has exceeded the capability of unassisted human analysts to understand, analyse and make predictions.

As predicted in last year's ETL the abundance of big data usage is not without concerns. Attacks are showing an increase trend in both number, sophistication and impact, but given the loose definition of the term and the unwillingness of affected organizations to disclose attack data, accurate estimates are not easy to come up with[359] [360]. The European Commission Business Innovation Observatory's reports[361] notes that "*nearly all large organisations experience security breaches or data leaks, sometimes with disastrous consequences. Information from the UK Information Commissioner's Office shows that local government data leaks*

[349] http://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/iot-system-security-wp.pdf, accessed November 2015.
[350] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-iot-2016-2017.html#c,topics=callIdentifier/t/H2020-IOT-2016-2017/1/1/1&callStatus/t/Forthcoming/1/1/0&callStatus/t/Open/1/1/0&callStatus/t/Closed/1/1/0&+identifier/desc, accessed November 2015.
[351] http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, accessed Nov 2015.
[352] http://byte-project.eu/10-big-data-initiatives-an-insight-into-the-big-data-landscape/ accessed Nov 2015.
[353] http://home.cern/scientists/updates/2015/09/big-data-takes-root accessed Nov 2015.
[354] https://earth.esa.int/web/guest/content/-/article/big-data-from-space-news accessed Nov 2015.
[355] http://www.copernicus-masters.com/index.php?anzeige=press-2015-01.html accessed Nov 2015.
[356] https://www.ukdataservice.ac.uk/about-us/our-rd/big-data-network-support accessed Nov 2015.
[357] http://www.defenseone.com/reports/harnessing-big-data/122177/ accessed Nov 2015.
[358] http://www.apa.org/monitor/2015/04/army-suicide.aspx accessed Nov 2015.
[359] http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/, accessed Nov 2015.
[360] http://www.zdnet.com/article/big-hacks-big-data-add-up-to-blackmailers-dream/, accessed Nov 2015.
[361] http://ec.europa.eu/growth/industry/innovation/business-innovation-observatory/case-studies/index_en.htm, accessed Nov 2015.

increased by 1609% over the last five years, while other public organisations showed a 1380% rise. In addition, private organisations recorded a 1159% surge in data leaks".

Given that big data are extremely novel and high tech ICT systems, with little time to mature against cyber-attacks, these numbers are directly relevant and indicative of the future. Additionally, as more and more businesses and organizations venture into the big data field, attackers will have more incentives to develop specialized attacks against big data technologies; e.g. web application attacks exploiting injection to NoSQL databases and Semantic Web tools, to further equip their tactics. Given the importance of big data, in the reporting period ENISA has developed a threat assessment for big data by means of a big data thematic landscape[362].

One further point for consideration is the interrelation between big data and other technologies; such as cloud computing and IoT. More and more it becomes the norm to build big data on top of cloud infrastructure to "*to meet certain infrastructure requirements, such as cost-effectiveness, elasticity, and the ability to scale up or down*"[363], whereas IoT is considered a 'big' producer/provider of raw big data that are generated at exceedingly higher speeds and bigger volumes. It is obvious that lack of security in supporting or providing technologies and systems has the potential of adversely affecting big data systems.

Finally, one should note that privacy remains a thorny issue in the area of big data: the LIBE Committee states that there is an "*increased collection and processing of personal data for various - and often unaccountable - purposes*"[364]. ENISA has invested some work in the area of privacy and big data by means of a report overview on privacy enhancing technologies and tools for big data analytics[365].

Top emerging threats to big data are:

	Emerging Threat	Threat Trend
1.	**Web application attacks (to big data systems)**	
2.	**Identity theft**	
3.	**Malware (to affect big data systems)**	
4.	**Insider threat**	
5.	**Phishing**	
6.	**Information leakage (of information stored as big data)**	
7.	**Cyber espionage**	
8.	**Data breaches**	

[362] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/bigdata-threat-landscape, accessed January 2015.
[363] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6842585, accessed Nov 2015.
[364] http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282015%29536455, accessed Nov 2015.
[365] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection/at_download/fullReport, accessed December 2015.

	Emerging Threat	Threat Trend
9.	**Denial of service (to components of big data system)**	↑
10.	**Legal threats[366] (due to non-conformance with privacy laws)**	↑

Legend: ↓ Declining, ➲ Stable, ↑ Increasing

Table 8: Emerging threats and their trends in the area of big data

Besides the above emerging threat landscape, the following issues have been identified:

- Big data and development of Security Incident and Event Management (SIEM) was hailed in previous ETL report for new acquisitions in the area of cyber security. Recently though critical voices have raised concerns on the effectiveness of more data, esp. given the fact that many attacks exploit well known vulnerabilities[367,368]. A good balance between exploring new technologies for threat intelligence, cost and actually making good use of the generated knowledge is essential.
- Mobile phones with their apps and sensors are a major contributor to the generation of big data but issues arise when this collection does not result from informed consent. Apps in mobile phones have been criticised for covert data collection. A recent research funded by DARPA shows that "*63% of the external communication made by top-popular free Android applications from Google Play has no effect on the user-observable application functionality*"[369]. Moreover, more than half of the calls could not be attributed to analytics.
- According to the director of NSA, the Office of Personnel Management data breach that resulted in 21.5 millions of stolen records of federal workers, including 5.6 million people's fingerprints [370], shows a new trend toward using big data analytics. Breached data can be used within big data to collect information about the individuals behind biometrical data. It has become clear that "*increasingly data has a value all its own and that there are people actively out there interested in acquiring data in volumes and numbers that we didn't see before*"[371]. Such data breaches, which affected 7% of the USA population, can give an edge to adversaries to correlate with other data. With the results they will be in the position to launch personalized and highly efficient phishing attacks, especially if combined with personal information and biometrics[372].
- One remarkable element of the big data state-of-play is the issue of perception: when is data big enough to be big data? Besides debates on this topic, it important to understand the "threshold" of scale to change the context from data to big data. In many reports, for example, threats related to data are referred within big data context. In the ENISA threat assessment in the area of big data[365], we found ourselves debating about what threat exposure is inherent to big data and how this is

[366] Although this threat is not a cyber-threat per se and is not addressed in this report, it is a direct consequence of misuse resulting correlation of information, often performed within processing of big data.
[367] http://www.theregister.co.uk/2015/11/16/security_black_hat_europe_keynote/, accessed Nov 2015.
[368] https://www.blackhat.com/eu-15/briefings.html#what-got-us-here-wont-get-us-there, accessed Nov 2015.
[369] https://people.csail.mit.edu/mjulia/publications/Covert_Communication_in_Mobile_Applications_2015.pdf, accessed Nov 2015.
[370] http://www.reuters.com/article/2015/07/09/us-cybersecurity-usa-idUSKCN0PJ2M420150709, accessed Nov 2015.
[371] http://freebeacon.com/national-security/cybercom-big-data-theft-at-opm-private-networks-is-new-trend-in-cyber-attacks/, accessed Nov 2015.
[372] http://economictimes.indiatimes.com/news/defence/us-big-data-breaches-offer-treasure-trove-for-hackers/articleshow/47567896.cms, accessed Nov 2015.

differentiated in the case of "non-big" data. While this can be easily differentiated when speaking about big data systems, it is fairly difficult if data are in flow or in a temporary storage.

6.6 Network Function Virtualization, Software Defined Networks and 5G

5G[373] represents the next major phase of mobile telecommunication systems and network architectures beyond the current 4G standards. It aims at extreme broadband and ultra-robust, low latency connectivity, to enable the programmable connectivity for the Internet of Things[374]. Despite the significant debate on the technical specifications and the technological maturity of 5G, which are under discussion in various fora[375], 5G is expected to affect positively and significantly several industry sectors ranging from ICT to industry sectors such as car and other manufacturing, health and agriculture in the period up to and beyond 2020.

5G will be driven by softwarization of network functions, known as *Software Defined Networking* (SDN) and *Network Function Virtualization* (NFV). The key concept that underpins SDN is the logical centralization of network control functions by decoupling the control and packet forwarding functionality of the network. NFV complements this vision through the virtualization of these functionalities based on recent advances in general server and enterprise IT virtualization.

Considering the technological maturity of the technologies that 5G can leverage on, SDN is the one that is moving faster from development to production. For this reason, in the reporting period ENISA has developed a specific threat assessment in this area[320].

Though not yet met in the wild, incidents related to SDN, NFV and 5G will orient themselves towards lower level threats and weaknesses (i.e. concerning low technological network layers) that will then affect higher level of components and functions. Concrete impacts on these components are difficult to assess at the time being. To this extend, we follow a "bottom-up" approach by estimating threats that exploit more "traditional" network components that will be extrapolated to assumed SDN/NFV levels. A more detailed view on these threats and their mitigation can be found in 320.

Top emerging threats to NFV, SDN and 5G are:

	Emerging Threat	Threat Trend
1.	**Insider threat**	↑
2.	**Malware**	↑
3.	**Physical damage/theft/loss**	↑
4.	**Web application attacks**	↑
5.	**Denial of service**	↑
6.	**Phishing**	↑
7.	**Identity theft**	↑

[373] www.5g-ppp.eu/roadmaps, accessed November 2015.
[374] http://ioeassessment.cisco.com/, accessed November 2015.
[375] http://www.3gpp.org/news-events/3gpp-news/1734-ran_5g, accessed November 2015.

	Emerging Threat	Threat Trend
8.	**Information leakage**	↑
9.	**Cyber espionage**	↑
10.	**Data breaches**	↑

Legend: ↓ Declining, ➲ Stable, ↑ Increasing

Table 9: Emerging threats and their trends in the area of network functions virtualisation, SDN and 5G

Besides the above emerging threat landscape, the following issues have been identified:

- Despite allowing better performance and monitoring, centralisation of control or logically centralised control it is a big concern in SDN security. By having the entire network intelligence concentrated in one single point, it is single point of failure. At the same time it has multiple threat exposures and represents a high-value asset to attackers[376]. Compromising this point means, effectively, compromise the whole network by facilitating the launch of further attacks, exploitations or even reprogramming the entire network. The effects of having SDN as a potential target are more devastating that using traditional networks. The threat landscape is continuously evolving and the deployment of architectural components of SDN can lead to new security threats and vulnerabilities.
- Likewise, the programmability aspect of SDNs includes new features that do not exists in the previous conception of traditional-closed administrative domains. Such functions, however, may introduce in addition to the traditional attack vectors[377], vulnerabilities and risks that did not previously exists. A common management and network policy enforcement layer multiplies the impact of such vulnerabilities to big number of components, increasing dangerously the attack and threat surface.
- Security within the SDN paradigm is a challenge, as all layers, sub-layers and components need to communicate according to strict security policies. Some of the new challenges on protecting SDN relies on the main features of this paradigm: centralization, abstraction and programmability. Efforts and advances are being done in order to improve the trust between third party applications and the controller, a better cross domain connection, implementing correct isolation of traffic and resources and integrating and improving the compatibility of legacy protocols[378].
- Security and dependability are becoming the top priorities for SDN[379]. Flexibility provided by SDN can enhance the security by facilitating the implementation of a number of security controls for the entire managed network. For example, centralization as a single point of control and monitoring, enables more consistent enforcement and control of security policies through fewer and uniformly accessible controllers. In the same manner the deployment of different virtual devices (firewalling, packet filtering, IDS, IPS, load balancing, etc.) can provide a better Quality of Service (QoS), resilience and protection. Finally, automation will allow to facilitate quicker response to malware or DDoS attacks by isolation or reaction to changes of the network state, while maintaining the high-level policies in place.

[376] http://umexpert.um.edu.my/file/publication/00001293_118473.pdf, accessed November 2015.
[377] http://arxiv.org/pdf/1406.0440.pdf, accessed November 2015.
[378] https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf, accessed November 2015.
[379] https://www.ietf.org/proceedings/87/slides/slides-87-sdnrg-2.pdf, accessed November 2015.

7. Food for thought: Lessons Learned and Conclusions

7.1 Lessons learned

ETL work conducted in 2015 has allowed us to further deepen our knowledge in threat collection and threat analysis. The experience gained is at the level of the process and of the content, both important components of the development of the threat landscape. Regarding the use of our tools to perform the task of threat analysis, we come to a number of points that are summarised below as *Lessons from the ETL process*. Lessons learned from the developments in the threat landscape are summarized by means of the section *Lessons from the analysed content*.

Lessons from the ETL process:

The collection of points below stem from own experience gained during the information collection and analysis activities at ENISA. Moreover, issues identified during the year in the ETL workshop[4], but also discussions with experts within various ENISA dissemination activities flow in these points. In particular:

- Less information exchange is needed, not more. But the right information needs to be found. It must be at the right quality, level and context. The existence of large amount of information alone is not beneficial, if the interrelations and proper presentation of correlated information cannot be captured.
- Threat analysis has commonalities with big data: the discovery of context out of massive data is decisive. Context makes threat information meaningful, useful and durable for some period of time. To this extend, threat information quality is more important than quantity.
- Development of threat intelligence is a laborious task. Using sharing platforms like MISP[1] makes clear how much effort is required to consolidate large amount of information into a usable entity that balances degree of technical detail, with degree of abstraction and usable information content.
- Due to diversification in available tools and procedures, it seems that the life-cycles for the creation of operational, tactical and strategic intelligence diverge. This affects the quality of produced information and poses additional challenges in creating single context throughout all three levels of intelligence.
- At the time being, creation of strategic and tactical threat intelligence seems to be possible only manually. Automation of this task seems viable only for information persistence of identified information and interconnections. The creation of context needs a great deal of human intervention.
- A standardized way for referring to threats, threat categories and threat terminology is necessary.
- The speed of reaction to cyber threats is an issue that deserves further consideration. However, given the remediation speed of vulnerabilities being one to two years, the life span of strategic and tactical intelligence with less than 12 months seems to be sufficient. This means that dissemination work is critical.
- The right presentation of threat information will be critical for the dissemination across the relevant stakeholders. New interactive presentation approaches will need to emerge.
- Often, threat statistics within various reports are selected ad hoc and difficult to compare. This disallows the consolidation of findings under a common qualitative and quantitative denominator.

Lessons from the analysed content:

- It seems that threat intelligence and threat information is a good instrument for segmentation of features of security products. When expressing available product capabilities with regard to mitigation of threats, it will help users understanding the nature of provided protection and the necessity of a

product. To this extend, threat information may be used as an additional instrument toward a user-driven security market.

- Analysis of incidents makes clear that in most of the cases even basic security controls are not in place or fail to provide assumed protection. It is important to develop/propose baseline security controls for various areas/sectors/scenarios and support small-medium organisations in operating them.
- Single user and small-medium organisations are in a vicious cycle: they do not have basic security measures in place and are not aware of the dynamics of the cyber-threat landscape. The cyber-security community will need to make thoughts of how to brake this cycle.
- Vulnerabilities are getting too old: 80% of the vulnerabilities in the wild are getting 1-2 years old before they are remediated. With such a life span, attempts to reduce exposure to cyber-threats becomes a pointless effort. Apparently, efforts are necessary to help users understanding the notion of vulnerability and how to manage it.
- Phishing is one of the most common vectors leading to malware installation. And it constantly gains momentum. Phishing mitigation is efficient when humans are aware. Training humans is a cost effective method that is worth and should be applied in a much wider manner.
- It seems that consumerization of cyber-crime (aka cyber-crime-as-a-service) is a model that will develop further. The cyber-security community will need to elaborate on methods to disable the development of this market.
- The dark net is a place that is unexploited as to knowledge base with regard to cyber-threats and activity of threat agents. A lot more effort will be necessary in order to better explore dark nets to enhance cyber-threat intelligence[380].
- Penetration of IT technology to the physical systems though Internet of Things and Industry 4.0 creates strong links within sectors with differentiating viewpoints with regard to operation processes, business cases, roles, security practices, etc. Now, more than ever is time to identify and break silos, especially the ones related to security.
- Treat agents is still an area with big potential: while some threat agent modelling means have been developed, no threat agent models are widely available. Attribution lags behind and information sharing about threat agents is at a very low maturity.

7.2 Conclusions

The development of the cyber-threat landscape in 2015 has been impressive in one thing: the smoothness of its development without big “hypes” in the media. Cyber-threats have evolved while following two extremes. Effective simplicity, achieved with a series of “low-tech” highly efficient infection methods. And effective complexity, achieved with next generation malware and attack vectors. Our conclusions in 2015 have been divided into three categories: policy conclusions, business conclusion and research conclusions.

Policy conclusions:

- Development of support models for weak links in cyber-space is a competitive advantage. Public authorities would need to foster end-point protection by:

[380] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf, accessed November 2015.

  - Issuing market guidance based on cyber-threat mitigation measures. This is particularly important for interconnected systems used for the management of vital/critical physical phenomena (Internet of Things).
  - Develop end-user trainings that are based on the current threat landscape and are free of technical details.
  - Disseminate threat mitigation good practices.
- Intensify and re-engineer available incident and data breach report schemes to effectively capture information about cyber-threats and involved threat agents. Results from this scheme should be disseminated to stakeholders by means of lessons learned from security breaches.
- In a similar manner to emergency and crisis-management, public sector should examine the feasibility of mobilizing citizens to support community in cyber-defence. Such roles would be similar to civil-protection, and would be activated in cyber-crises.
- Develop threat intelligence for the governmental organisations and apply state-of-the-art cyber-threat intelligence approaches within all relevant authorities.

Business conclusions:

- The cyber-threat landscape needs to be disseminated to all kind of stakeholders. Cyber-threat information needs to be made consumable by executives, non-expert user and end-users. It needs to become non-technical and translated into concrete actions to be undertaken.
- Businesses in the area of cyber-security need to elaborate on threat agent models and create threat agent intelligence based on proactive, real/near-time and reactive information. This kind of information is of high value in risk assessment and in the definition of protection requirements.
- Businesses in the area of technology should look for ways to extract/discover information from dark net/dark web. This might include crawlers, data mining tools, pattern matching tools, etc. The objective would be to develop a better understanding about the dynamics of dark net and collect information about threat agents.
- Given the longevity of vulnerabilities in cyber-space, it seems that current vulnerability management practices are not efficient. Businesses in the cyber-security sector should find methods to support users in managing vulnerabilities at end-points.
- Not more, but better quality information about threats is needed. Organisations should focus on creation of context from incident and cyber-threat data. This context should be structured and shared according to individual needs of target groups.

Research conclusions:

- Research in applied statistics and metrics for impact of incidents as well as statistic models for threats according to detection and materialization levels are necessary. They contribute to the comparability of cyber-threats and can provide homogeneous quantitative evidence for the threat landscape.
- Research on new models for the seamless and intuitive operation and management of security controls is necessary. Such models would target technically novices who will need to user ubiquitous computing applications in home environments, e-health and transportation. Hiding the complexity while keeping the efficiency of security controls is a means to reduce exposure in these emerging technology areas, especially in cases that they might impact human life.

- Research is necessary in order to develop trust models for the establishment of ad hoc interconnections among devices in application scenarios, in particular related to the Internet of Things and Industry 4.0. Access to and exchange of confidential information will be performed on the basis of the trust level negotiated.

Annex A: Comparison ENISA and STIX data models

Attributes-Collection:		
STIX	Description	ENISA
-	-	High level Threat
incident:Title	The Title field provides a simple title for this Incident.	Threat
incident:Description	This field characterizes a single cyber threat Incident.	Threat Detail
incident:Affected_Asset	The Affected_Assets field is optional and characterizes the particular assets affected during the Incident.	Affected Asset Type
-	-	Affected Business Sector
-	-	Emerging technology area
Threat Actor	ThreatActors are characterizations of malicious actors (or adversaries) representing a cyber-attack threat including presumed intent and historically observed behaviour.	Threat Agent
incident:Information_Source	The Information_Source field details the source of this entry.	Relevant Reference
incident:Information_Source	The Information_Source field details the source of this entry.	Trend
incident:Information_Source	The Information_Source field details the source of this entry.	Relevant URL
Attributes Threat Agents:		
STIX	Description	ENISA
ta:Description	The Description field is optional and provides an unstructured, text description of this ThreatActor.	Description
ta:Motivation	The Type field characterizes the motivations of this threat actor. It may be used multiple times to capture multiple motivations.	Motives
ta:Intended_Effect	The Intended_Effect field specifies the suspected intended effect for this Threat Actor.	Capabilities
ta:Information_Source	The Information_Source field details the source of this entry.	References
Attributes Current Threats:		
STIX	Description	ENISA
incident:Description	This field characterizes a single cyber threat Incident.	Description of threat
incident:Intended_Effect	The Intended_Effect field specifies the suspected intended effect of this incident.	Issues related to threat
incident:Information_Source	The Information_Source field details the source of this entry.	Overall trend
incident:Attributed_Threat_Actors	The Attributed_Threat_Actors field identifies ThreatActors asserted to be attributed for this Incident.	Threat Agents
incident:Related_Indicators	The Related_Indicators field identifies or characterizes one or more cyber threat Indicators related to this cyber threat Incident.	Related threats
ttp:Kill_Chains	The Kill_Chains field characterizes specific Kill Chain definitions for reference within specific TTP entries, Indicators and elsewhere.	Usage in kill chain
et:Vulnerability / et:Weakness	The Vulnerability field identifies and characterizes a Vulnerability as a potential ExploitTarget. / The Weakness field identifies and characterizes a Weakness as a potential ExploitTarget.	Possible Vulnerabilities/Weaknesses
-		Foreseen Trend
-	-	Issues related to threat/area
et:Information_Source	The Information_Source field details the source of this entry.	References
Attributes Sector:		
STIX	Description	ENISA
-		Asset Inventory

ttp:Behavior	Behavior describes the attack patterns, malware, or exploits that the attacker leverages to execute this TTP.	Relevant Threats
ttp:Exploit_Targets	The Exploit_Targets field characterizes potential vulnerability, weakness or configuration targets for exploitation by this TTP.	Possible Vulnerabilities/Weaknesses
-		Assessed particular sector threats (from incidents)
Threat Actor	ThreatActors are characterizations of malicious actors (or adversaries) representing a cyber-attack threat including presumed intent and historically observed behaviour.	Threat Agents
ttp:Handling	Specifies the relevant handling guidance for this TTP. The valid marking scope is the nearest TTPBaseType ancestor of this Handling element and all its descendants.	Threat mitigation practices/controls
ttp:Information_Source	The Information_Source field details the source of this entry.	References

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

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