ENISA

CURRENT THREAT + LANDSCAPE EMERGING

ETL 2014

ENISA Threat Landscape 2014

Overview of current and emerging cyber-threats

December 2014

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu

https://t.me/learningnets

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.

Author

Louis Marinos, ENISA
E-mail: Louis.marinos@enisa.europa.eu

Contact

For contacting the editors please use resilience@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The author would like to thank the members of the ENISA ETL Stakeholder group: Martin Dipo Zimmermann*, Consulting, DK, 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, Klaus Keus, 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. Moreover, we would like to thank Welund Horizon Limited for granting free access 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 ENISA colleague Anna Sarri for her support in information analysis.

* In memory of Martin Dipo Zimmermann who has left us on 16.12.2014.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2014

Reproduction is authorised provided the source is acknowledged.

ISBN: 978-92-9204-112-0, ISSN: 2363-3050, DOI: 10.2824/061861

https://t.me/learningnets

Executive summary

No previous threat landscape document published by ENISA has shown such a wide range of change as the one of the year 2014. We were able to see impressive changes in top threats, increased complexity of attacks, successful internationally coordinated operations of law enforcement and security vendors, but also successful attacks on vital security functions of the internet.

Many of the changes in the top threats can be attributed to successful law enforcement operations and mobilisation of the cyber-security community:

- The take down of GameOver Zeus botnet has almost immediately stopped infection campaigns and Command and Control communication with infected machines.
- Last year's arrest of the developers of Blackhole has shown its effect in 2014 when use of the exploit kit has been massively reduced.
- NTP-based reflection within DDoS attacks are declining as a result of a reduction of infected servers. This in turn was due to awareness raising efforts within the security community.
- SQL injection, one of the main tools used to compromise web sites, is on the decline due to a broader understanding of the issue in the web development community.
- Taking off-line Silk Road 2 and another 400 hidden services in the dark net has created a shock in TOR community, both at the attackers and TOR users ends.

But there is a dark side of the threat landscape of 2014:

- SSL and TLS, the core security protocols of the internet have been under massive stress, after a number of incidents have unveiled significant flaws in their implementation .
- 2014 can be called the year of data breach. The massive data breaches that have been identified demonstrate how effectively cyber threat agents abuse security weaknesses of businesses and governments.
- A vulnerability found in the BASH shell may have a long term impact on a large number of components using older versions, often implemented as embedded software.
- Privacy violations, revealed through media reports on surveillance practices have weakened the trust of users in the internet and e-services in general.
- Increased sophistication and advances in targeted campaigns have demonstrated new qualities of attacks, thus increasing efficiency and evasion through security defences.

In the ETL 2014, details of these developments are consolidated by means of top cyber threats and emerging threat trends in various technological and application areas. References to over 400 relevant sources on threats will help decision makers, security experts and interested individuals to navigate through the threat landscape.

Lessons learned and conclusions may be useful for all stakeholders involved in the reduction of exposure to cyber threats. Opportunities and issues in the areas of policy/business and technology have been identified to strengthen collectively coordinated actions towards this goal. In the next year, ENISA will try to capitalize on these conclusions by bringing together expertise to improve information collection capabilities and to apply lessons learned to various areas of cyber security.

The figure below summarizes the top 15 assessed current cyber-threats and threat trends for emerging technology areas. More details on the threats, emerging technology areas, threat agents and attack methods can be found in this report.

https://t.me/learningnets

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Compu-ting	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtuali-sation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

Table 1: Overview of Threats and Emerging Trends of the ENISA Threat Landscape 2014[1]

[1] Please note that the ranking of threats in the emerging landscape is different than the one in the current landscape. The rankings of emerging threat trends can be found in the corresponding section (see chapter 6). Arrows that show a stability

https://t.me/learningnets

Table of Contents

Executive summary iii

1 Introduction 1

2 Purpose, Scope and Method 5

2.1 Quality of Content of Threat Information 5

2.2 End-user Needs with regard to Threat Information 6

2.3 Typical Practical Use Case for Threat Information 8

2.4 Content of this year's ETL and Terminology 9

2.5 Used definitions 10

3 Top Threats: The Current Threat Landscape 13

3.1 Malicious Code: Worms/Trojans 14

3.2 Web-based attacks 16

3.3 Web application attacks / Injection attacks 17

3.4 Botnets 18

3.5 Denial of Service 20

3.6 Spam 22

3.7 Phishing 23

3.8 Exploit Kits 25

3.9 Data Breaches 26

3.10 Physical damage/theft/loss 28

3.11 Insider threat 30

3.12 Information leakage 32

3.13 Identity theft/fraud 33

3.14 Cyber espionage 35

in a threat may be increasing in emerging areas. This is because current threat landscape includes all threats independently from particular areas.

https://t.me/learningnets

3.15 Ransomware/Rogueware/Scareware 37
3.16 Visualising changes in the current threat landscape 39

4 Threat Agents 41
4.1 Cyber-opportunity makes the thief 41
4.2 Overview of Threat Agents 42
4.3 Threat Agents and Top Threats 48

5 Attack Vectors 51
5.1 Attack Vectors within threat intelligence 51
5.2 Describing a Cyber-Attack though Attack Information 52
5.3 Targeted attacks 53
5.4 Drive-by-attacks 54
5.5 Strategic web compromise (watering hole attack) 55
5.6 Advanced persistent threat (APT) 56

6 Emerging Threat Landscape 59
6.1 Cyber Physical Systems as an emerging CIP issue 60
6.2 Mobile Computing 63
6.3 Cloud Computing 65
6.4 Trust infrastructures 67
6.5 Big Data 69
6.6 Internet of things/interconnected devices/smart environments 72
6.7 Network Virtualisation and Software Defined Networks 74

7 Food for Thought: Lessons Learned and Conclusions 79
7.1 Lessons learned 79
7.2 Conclusions 81

https://t.me/learningnets

1 Introduction

This ENISA Threat Landscape report for 2014 (ETL 2014) is the result of threat information collection and analysis of the last 12 months (December 2013 – December 2014), referred to in this document as the *reporting period*.

The ETL 2014 is a continuation of the reports produced in 2012 and 2013: it follows similar approaches for the collection, collation and analysis of publicly available information to produce the cyber-threat assessment. The report contains a description of the methodology followed, together with some details on use-cases of cyber-threat intelligence. The main contribution of the ETL 2014 lies in the identification of top cyber threats within the reporting period. Together with the emerging threat landscape, it makes up the main contribution towards identification of cyber-threats.

As in previous years, the ETL 2014 is based on publicly available material, the availability of which has grown substantially in the reporting period. Starting from ca. 150 references in 2012, we identified ca. 250 in 2013. In 2014, we identified over 400 sources containing information on cyber threats, whereas in all years we assume that our information collection detects ca. 60-70% of available material. This makes the ETL 2014 a unique comprehensive collection of information regarding cyber-security threats.

ENISA has performed information collection by means of internet searches, by using the information provided by the CERT-EU[2] and by using the web platform of Welund Horizon Ltd through free access granted to ENISA in the reporting period.

As is explained later in this report, the ETL 2014 has been expanded to include information on attack vectors, that is schematic representations on the course of attacks, indicating targeted assets and exploited weaknesses/vulnerabilities. Another new component in the ETL 2014 is the elaboration of use-cases of threat intelligence: by showing the various activities of threat analysis, we demonstrate how the information produced can be used within various phases of security management.

Another novelty of the ETL 2014 process is the involvement of stakeholders in the identification of issues as well as knowledge transfer and information sharing. In 2014, ENISA has established an ETL stakeholder group consisting of 13 experts from CERTs, vendors, Member States and users. This group has provided advice on various issues of threat analysis, including stakeholder requirements and state-of-the art developments in the area of threat intelligence.

Lessons learned and conclusions summarize the highlights of this year's threat assessment exercise and provide concluding remarks that are relevant for policy makers, businesses and cyber-security experts.

Policy Context

The policy context of the ETL 2014 with regard to relevant EU-regulations is identical to that of 2013 ETL. The Cyber Security Strategy of the EU[3] stresses the importance of threat analysis and emerging trends in cyber security. The ENISA Threat Landscape is an activity contributing 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).

[2] http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html, accessed November 2014.
[3] http://www.ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, accessed 28 Nov 2013.

https://t.me/learningnets

Moreover, the new ENISA regulation[4] 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.

Target audience

The target audience of the ETL 2014 remains very similar to that of previous versions of this report. It mainly targets cyber-security specialists and individuals interested in the development of cyber-threats. More precisely, these are cyber-security specialists working at the strategic, tactical and operational levels of security management. Threat and risk assessments may be the primary concerns of such individuals. They are busy with assessing the "external environment" and "internal environments"[5] in the framework of threat and risk assessments. In this year's ETL, we provide a more extensive view on the use-cases of a threat analysis process (see section 2.2). Besides the high level discussions provided within this document, security experts will be in a position to identify detailed issues on the assessed threats by means of numerous references to collected sources. This might make the ETL a useful tool for long term use as it comprises a sort of contextualized "directory" to cyber-threat sources.

As the ETL contains high level information about cyber threats and emerging technology areas, it is a good "entry point" to the subject of threat intelligence for non-experts. This target group will be interested in the descriptions provided and the consolidated presentations of cyber threats and threat trends. We have experiences, for example, that consolidated material of ETL 2013 has been used within German schoolbooks.

The ETL 2014 will be of interest for policy makers: current threats and threat trends may be an important input to policy actions in the area of cyber-security, national cyber-security preparedness and possible coordination and cooperation initiatives among threat collection organisations and other competent bodies.

Experience from previous ETL reports shows that media is an important target group of the ETL. The generic cyber-threat descriptions provided can be easily understood by non-security experts. Such descriptions help media to understand the dependencies and developments in that area. An area that enjoys particular media attention, the latest after revelations about state sponsored surveillance activities and related privacy risks for citizens world-wide.

Last but not least, by providing tactical and strategic guidance, The ETL 2014 could be used to support executive management decisions and orientation of asset protection policies. This makes the ETL 2014 potentially useful for ISMS activities.

Structure of this document

The structure of the ETL 2014 is as follows:

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF, accessed 28 Nov 2013.
[5] http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/rm-process/crm-strategy/scope-framework, accessed 30 Oct 2013.

https://t.me/learningnets

Chapter 2 "*Purpose, Scope and Method*" provides some information regarding the threat analysis process as it is being performed within the ETL 2014. Moreover, it refers to the information flow between threat analysis and relevant stakeholders, while it gives some information on use-cases for threat intelligence and used definitions.

Chapter 3 "*ETL 2014: Current Threat Landscape*" is the heart of the ETL 2014 as it contains top 15 cyber-threats assessed in 2014. It provides detailed information on the threat with references to all relevant resources found, trends assessed and the role of each threat within the kill-chain.

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*" contains some new content that has been adopted in this year's ETL. It 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.

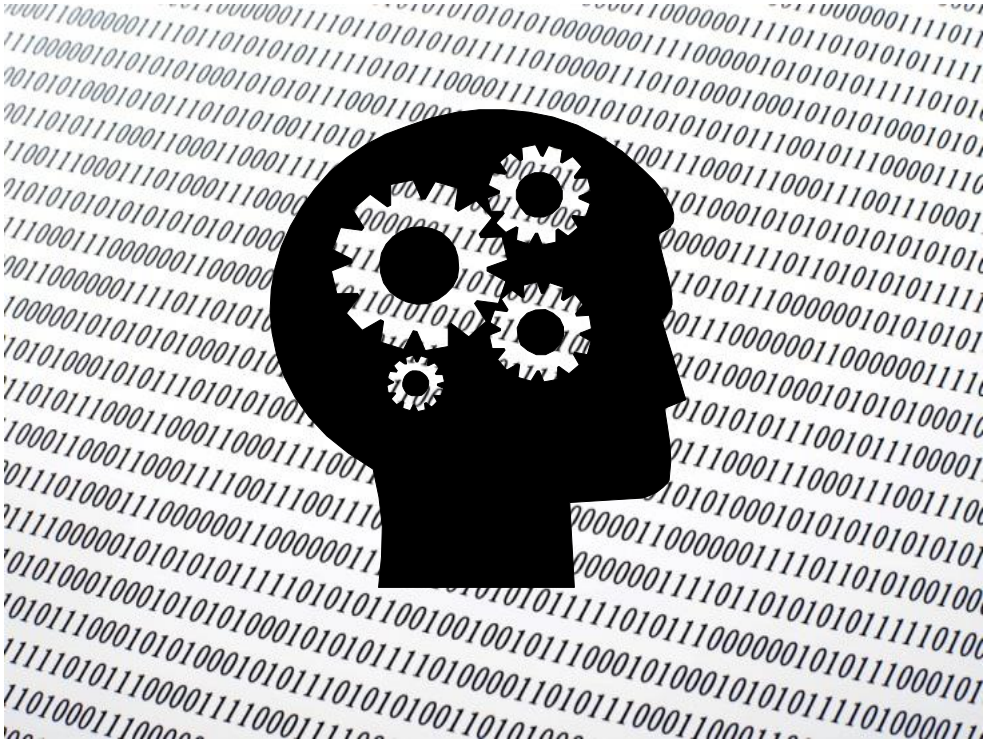
Chapter 6 "The *Emerging Threat Landscape*" indicates assessed technology areas that will impact the threat landscapes in the middle-term. Ongoing developments in those areas will influence the ways attackers will try to achieve their aims, but also the way defences are going to be implemented.

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.

As was the case in ETL 2013, the present document has been developed in a modular way. The chapters are as independent as possible to each other, thus allowing for an isolation of the addressed issues so that readers can concentrate on the topic of interest. This approach also allows for independent updates of the content, when deemed necessary (i.e. in cases of publication of additional threat assessment summaries within a year).

https://t.me/learningnets

ETL 2013: Purpose, Scope and Method



https://t.me/learningnets

2 Purpose, Scope and Method

Worldwide, the cyber threat landscape – and threat analysis in general – has been assigned a central role in practical Security Incident and Event Management (SIEM[6]). This is the case both in the relevant vendor market and within end-user organisations. A plethora of related services and good practices are available that are based on threat intelligence. They consist mainly of collection, aggregation and correlation of data. It has been recognised that information on cyber-threats should be THE parameter to actively adapt security protection practices towards a more agile management of security controls. Following these trends, in this year's ETL we have optimized threat collection and analysis practices, whilst at the same time better reflecting on the practical applicability of threat information in Information Security Management Systems (ISMS) and SIEM.

The purpose and positioning of the ENISA Threat Landscape (ETL) has been documented in ENISA's 2013 deliverable (ETL 2013[7]) and is still valid. Yet, based on advancements observed in the reporting period, a more detailed view on the purpose and potential use of the delivered information is provided in this chapter. This is done by paying attention to stakeholder requirements with regard to threat information/threat intelligence. These requirements have been assessed within the ENISA Threat Landscape Stakeholder Group (ETL SG), established in 2014 in order to advise ENISA on relevant matters.

In the rest of this chapter we discuss several important aspects of threat landscape such as:

- Quality and content of threat information;
- End-user needs with regard to threat information;
- Typical practical use case for threat information and,
- Content of this year's ETL and terminology.

2.1 Quality of Content of Threat Information

Numerous organisations create, assess and analyse information regarding cyber threats. Typically, such information may have varying levels of detail, structure and abstraction level. The differences are motivated by the purpose of the delivered information and the input data used to create it. In particular, the following types of threat information can be found:

Strategic (S): this is usually the highest level information about threats. Such 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 investments, as well as adaptation of existing cyber security strategies. These are typical ISMS activities and stakeholders interested in this level of information are mostly CISOs and CIOs.

Tactical (T): tactical threat 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 long-term maintenance of security infrastructures, mostly within security management activities. Hence, tactical threat information is also relevant to ISMS.

Operational (O): this is the most basic information about existing threats. It covers detailed technical information about threats, incidents, vulnerabilities, etc., and usually derived from detections at the

[6] http://en.wikipedia.org/wiki/Security_information_and_event_management, accessed November 2014.
[7] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport, accessed 30 Sept 2014.

https://t.me/learningnets

level of technical artefacts. It includes identification of cyber threats (e.g.. MD5 hash or Indicators of Compromise (IOC) [8]), its elements (vulnerability abuses, threat agents, attack vectors) and corresponding countermeasures (technical controls for the elimination/reduction of threat or threat exposure). This information is crucial for the day-to-day operation and maintenance of infrastructure on the technical level and comprises the main input to SIEM. This area is strongly supported by many standards and tools available on the market (both open source like MISP[9] or commercial like Threat Connect®[10]) which facilitate automatic (at least on some level) gathering and sharing information.

The diagram known as Pyramid of Pain [11] illustrates how to measure the trouble generated to adversaries by using threat intelligence. Taking this approach as a basis, one can argue that while operational information is related to the bottom layers of the pyramid, tactical information refers rather to the top levels. Whereas both tactical and strategic information constitute the transition from threat intelligence and SIEM to ISMS.

ETL contains mainly strategic and tactical information about cyber threats. Information collection, aggregation and analysis, however, is often based on all types of information found in the public domain. Operational information is used mainly as trigger to recognise/understand the whereabouts of cyber threats which are then consolidated by means of tactical and strategic issues. The main focus of ETL is on tactical and strategic guidance, this makes it more relevant to asset protection policies and practices.

2.2 End-user Needs with regard to Threat Information

It is important to analyse, understand and address end-user needs in the provision of cyber threat information. Given the novelty of (dynamic) threat analysis processes in SIEM and ISMS, the identification of possible use-cases that might suit end-user needs is at an early stage.

In the reporting period, ENISA has initiated a dialogue with threat information stakeholders by means of the ETL SG. Within this group, discussions have taken place in an attempt to understand the needs end-users have with regard to threat information. Moreover, the act of balancing threat information provision capabilities and end-user requirements/expectations has also been elaborated.

Being at an initial state of maturity of threat intelligence, matching user expectations/needs and threat information provision models seems to be a challenge ahead. In this chapter, an initial assessment of user requirements on threat information is presented. Additional information on how to balance "supply and demand" in the case of threat information/threat intelligence is currently in preparation.

End-users apply the threat assessment process mainly as a support process to SIEM and ISMS implemented according to adaptations that meet individual organisational requirements. Usually, the ISMS includes three components:

- Assessment (threats, vulnerabilities, impact, risks);
- Planning (security controls and procedures) and
- Operation (security controls and security policy enforcement).

In each of these component, and according to the capability level of the organisation, end-users may have different needs in relation to the threat assessment process. Some of them may only use threat

[8] http://www.openioc.org/, accessed December 2014.
[9] https://github.com/MISP/MISP, accessed December 2014.
[10] http://www.threatconnect.com/, accessed December 2014.
[11] http://detect-respond.blogspot.gr/2013/03/the-pyramid-of-pain.html, accessed November 2014.

https://t.me/learningnets

information in selected phases or even outsource threat intelligence to external organisations. At this point, cyber threat information provision models come into the scope.

Some users will need only to assess the level of threats to perform risk assessments for developing better business processes or to provide precise pricing of their products. In this case, it is sufficient for the threat information to be adopted from external sources. Subsequently this information is put in scope of the internal assessment exercise.

Similarly, not all phases of the threat assessment process are used within the operational activities of a SIEM. To operate security controls there is a need for collecting, collating and analysing data about threats that concern specific assets and threat exposure assumptions. Moreover, for SIEM activities not only data about the newest threats are needed; historical data are also useful in order to draw conclusions about the efficiency of implemented security controls and revisions of the security architecture.

Knowing the current context of received threat information (e.g. strategic, tactical or operational guidance), users can formulate the overall organisation policies concerning cybersecurity, plan appropriate security controls and, finally, manage investment decisions. In those three cases the most important issue for organisations is to possess and understand the context of cyber threat information. Depending on the origin of threat information and the internal capability level, this might be a challenge.

The interaction between the threat assessment process and user needs is presented in Figure 1 below: green areas correspond to the threat assessment process phases, blue areas correspond to described user needs. S, T and O abbreviations refer to threat information levels (Strategic/Tactical/Operational) and orange text indicates which stakeholder group is associated with which user need.

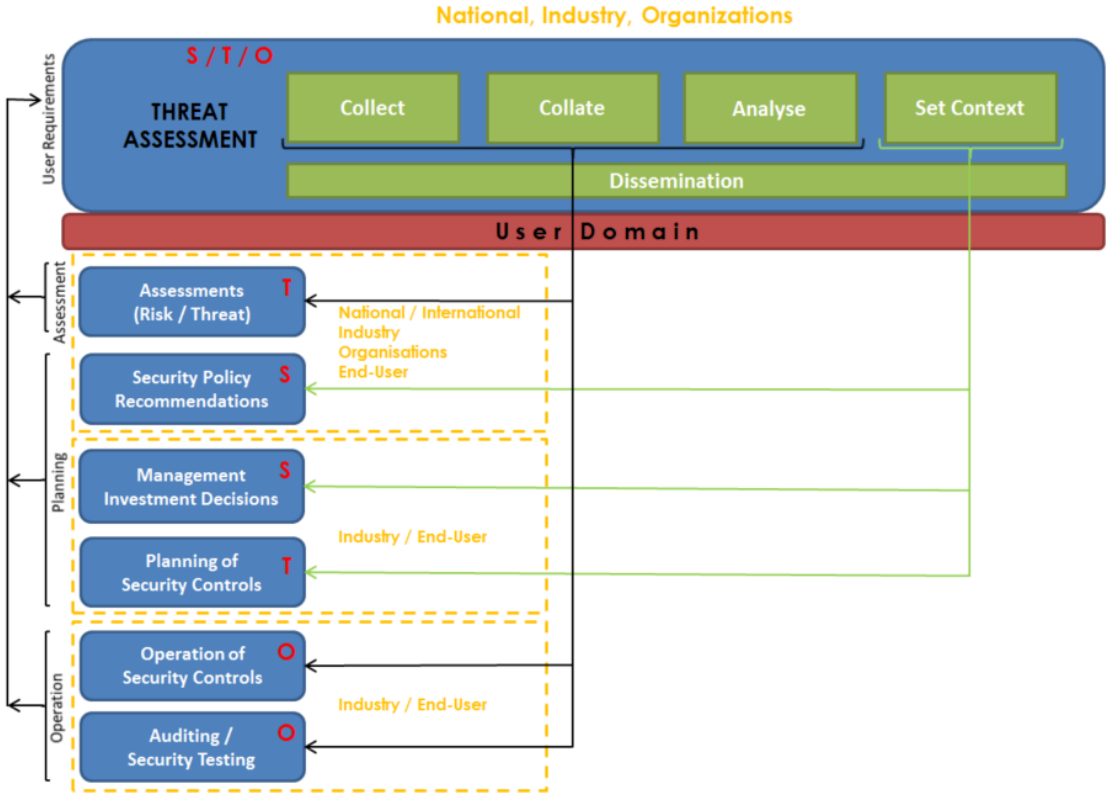


Figure 1: Threat assessment process – relation with user needs and ISMS activities

https://t.me/learningnets

Given the presented user requirements it becomes clear that ETL is delivering information for:

- Management decisions regarding expected evolution of cyber threats and in particular their relevance to emerging technology areas;
- Security policy recommendations, in particular through cyber threats, their potential impact on assets and the extrapolation of threats to emerging technology areas;
- Supporting information for risk assessments to be performed for valuable assets of the organisation, and
- Planning of security controls that will be in the position to reduce vulnerabilities that can be potentially abused by top cyber threats.

As a collateral product of ETL, but also of cyber threat information from other sources, one should mention the usefulness of this material in assessing the effectiveness of existing controls by utilising provided kill-chain[12] information. This approach is a typical practical example based on cyber threat information and is discussed in the forthcoming section (see section 2.3).

2.3 Typical Practical Use Case for Threat Information

In the present section we present a practical example for the use of threat information within the operational activities of an organisation. This example has been developed after feedback received from threat information users using threat information within both SIEM and ISMS. It is considered as a good practice in an agile management of security controls.

It is assumed that threat information consists of:

- Threat description including targeted assets;
- Threat details providing information on the "whereabouts" of an incident;
- Threat agents involved and
- Indicative information on attack vector (i.e. based on kill-chain).

Obviously, the more comprehensive the above information is, the more easily it can be integrated into the SIEM and ISMS activities. Nonetheless, structure and content of cyber threat information has to correspond to the internal capability and maturity level. In other words, threat information has to be structured in a way that can be efficiently consumed by internal security management process. This might be a challenging task to achieve, especially when internal capabilities are relatively low (e.g. SMEs willing to consume threat intelligence).

Figure 2 presents an indicative workflow of this use case: starting from a selection of the threat agent group to be addressed in the defence, it continues with the selection of relevant cyber threats and goes ahead up to the performance of corrective actions of existing protection. In this indicative workflow the importance of the kill-chain becomes apparent through its role within many steps.

It is worth mentioning that for the implementation of such a workflow some additional information will be necessary (i.e. asset inventories, vulnerability information, configuration data for existing security controls, etc.). Such information is one basic tool of ISMS within organisations.

Finally, as it is indicated in Figure 2, cyber threat information may be a useful tool for auditing existing security controls. This will allow using similar criteria, both for the implementation and efficiency check of available controls. Hence, this would contribute towards using a common terminology for

[12] http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html, accessed November 2014.

https://t.me/learningnets

implementing and controlling actions that are inherent to ISMS. This is a significant advantage for organisations, as differences in knowledge level between cyber security and other disciplines is often seen as a weakening factor for the life-cycle of security controls. For this reason, the use of a common threat taxonomy and common threat intelligence may be very beneficial.

The use cases around threat assessment/threat intelligence have been investigated in the reporting period quite thoroughly. In this context, we have made use of an authoritative resource in this area: "*How to Collect, Refine, Utilize and Create Threat Intelligence*", of Gartner Group[13]. The material published provides a comprehensive view on collection and analysis of threat information towards the creation of threat intelligence and comprises a very useful reading for information security professionals.

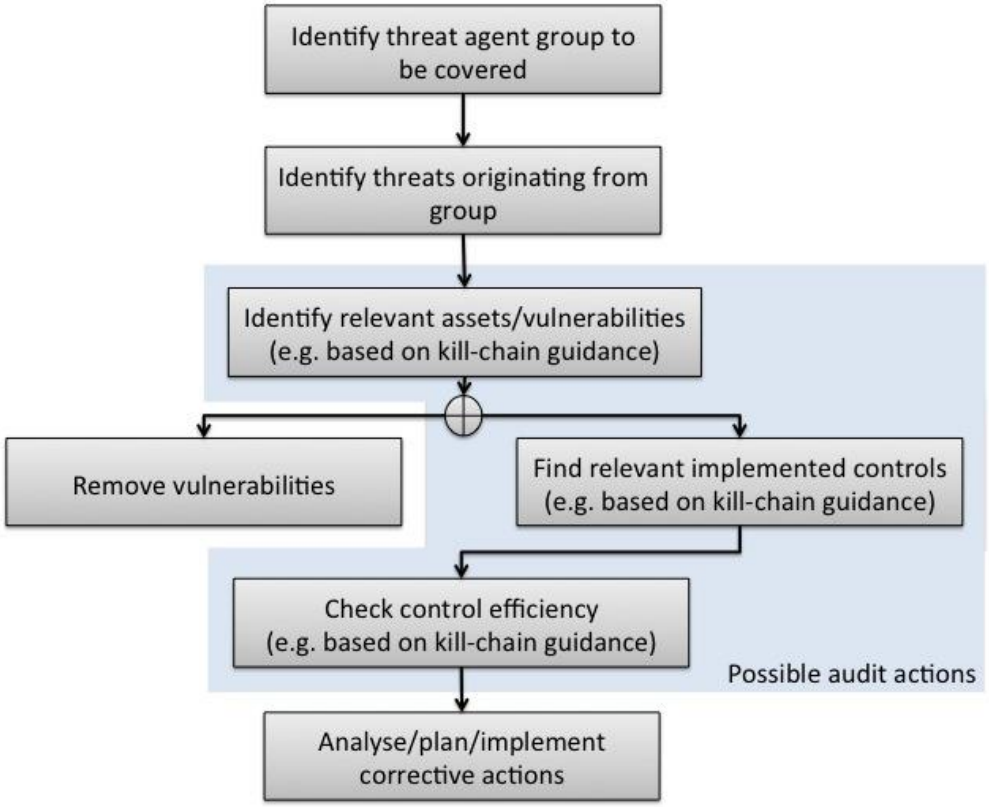


Figure 2: Indicative workflow of security management actions based on threat intelligence

2.4 Content of this year's ETL and Terminology

This version of the ETL covers all elements found in previous versions. In particular it provides:

- Information on top threats assessed in the reporting period (2014);
- Trends and issues of particular interest related to these threats;
- Kill-chain information per threat;
- Threat agents;
- Emerging threats in important technology areas;

[13] http://blogs.gartner.com/anton-chuvakin/2014/05/15/my-threat-intelligence-and-threat-assessment-research-papers-publish/, accessed October 2014.

https://t.me/learningnets

The details about structure and rationale of this information are the same as in last year's ETL [7] (see Chapter 2).

Following the developments in the area of cyber threat analysis and cyber threat landscape in general, this year's ETL has been expanded with information on attack vectors. This addition contributes towards a more clear separation between cyber threats and common tactical methods used to deploy an attack by combining various cyber threats.

The information on attack vectors added to the ETL 2014 is complementary to kill-chains: a kill chain provides generic guidance about which phases of an attack the threat can be deployed; while an attack vector provides information about the assets that can be targeted and the type of threat used per asset. In practice, within an attack vector several threats might be combined. E.g. in a Targeted Attack the cyber threats phishing, malicious URL and malware are being combined, targeting assets like human, web-browser, operating system, etc.

Finally, a new element added to this year's report is the explicit mentioning of authoritative resources. In each relevant section, a reference has been made to the authoritative sources found for a particular topic. This should facilitate information finding regarding the details of the particular topic. It should be noted that the term of authoritative source is used in order to indicate an information source that provides significant quantity of explanations/information in one topic. Hence, this term is not indicative for qualitative differences to other sources. Thus, reports that are referenced in the document but are not enlisted within authoritative resources are by no means of lower quality.

2.5 Used definitions

As in many complex areas, in cyber threat assessment wording matters. In this section we briefly present the terms used. Both within and outside this report, definitions facilitate the understanding of used terms; further, and equally importantly, consistent use of terms contributes towards better, quicker and more efficient knowledge transfer on cyber threats. This may enhance the response capabilities to cyber threats.

The definitions used are identical to the ones of ETL 2013. 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 most of the elements of risk mentioned in this section. It should be noted that "owner" refers to the owner of the asset; moreover, the issue of attack vector is displayed in this figure.

https://t.me/learningnets

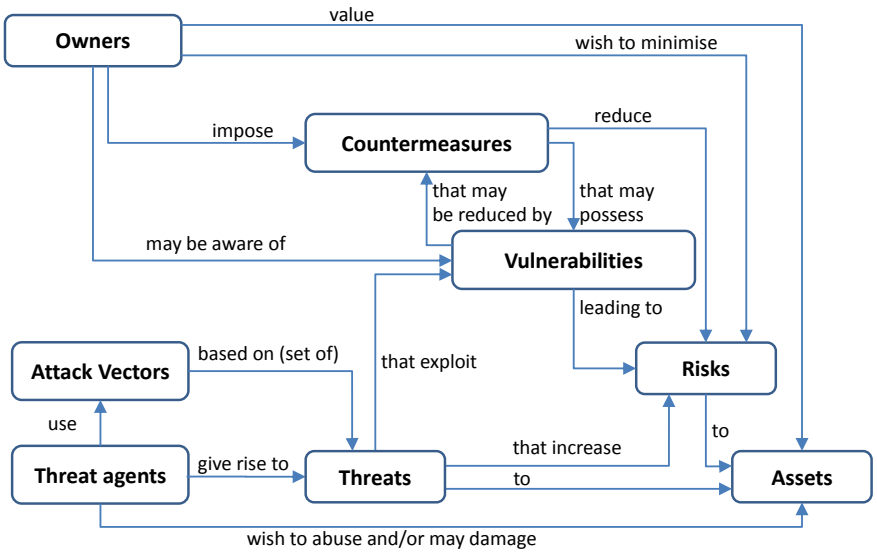


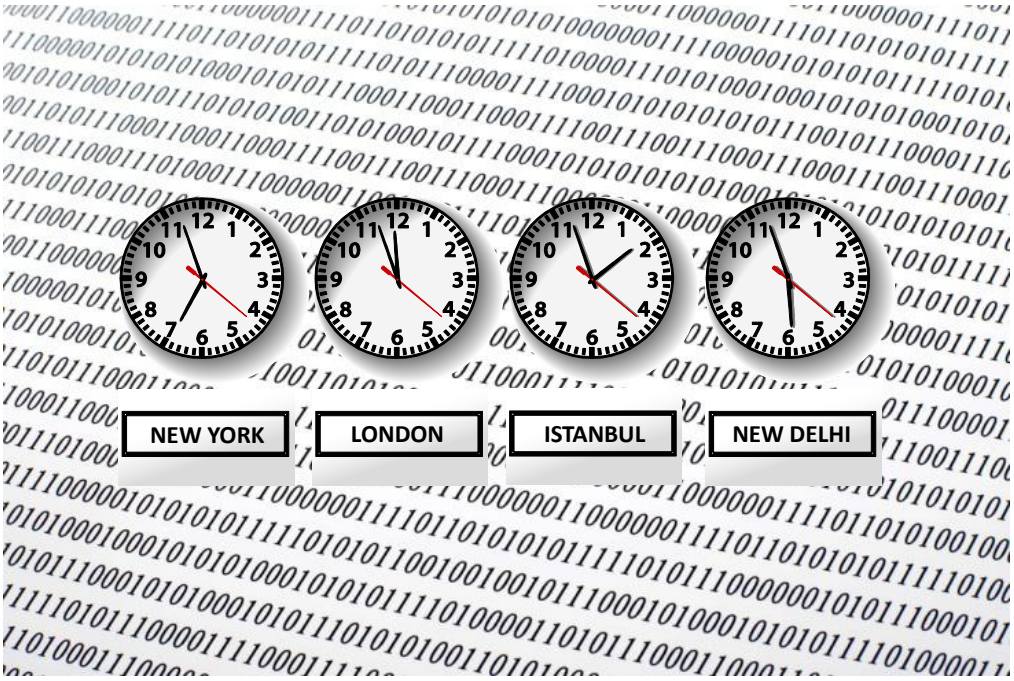
Figure 3: the elements of a risk and their relationships according to ISO 15408:2005

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

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

https://t.me/learningnets

ETL 2014: Current Threat Landscape



https://t.me/learningnets

3 Top Threats: The Current Threat Landscape

In the *Current Threat Landscape 2014,* related material published in the period between November 2013 and November 2014 has been compiled, thus covering approximately one year of cyber threat developments.

The amount of material published in the reporting period has increased significantly, both in terms of quantity and quality. From the material examined, we note that issued reports and published information have almost doubled since ETL 2013[14]. This is a strong indication of the important role assigned to threat information (i.e. threat intelligence) in the cyber-security community. While being a main component of SIEM, threat information plays and important role in ISMS because it can serve as an important instrument to implement more agile ISMS processes based on detections and reported incidents. This is a significant shift in security management, that has been traditionally based on one-off assessments that had taken into account a time restricted *snapshot* of the threat environment; and were often outdated shortly after they have been released.

Advances in the quality of published material has also been assessed. All organisations engaged in threat analysis have yet developed significant experience in the coverage of all facets of threat analysis and threat intelligence. This is indicated by the fact that the terminology used has converged, threat agents come into the focus and details of attack vectors started appearing in the reports. Although there is space for improvement, information available has reached a high maturity and span of coverage that was not available in the past couple of years.

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 than last year. This means that a higher efficiency of attacks based on this threat has been reported (e.g. botnets).

Knowing that this approach might not be free from ambiguity, it has nevertheless been selected as it delivers "*good-enough*" classification of threat importance and of threat trends. For example, it makes clear that worms/trojans, together with web-based attacks are detected the most, while detection of the insider threat is significantly lower. This approach is one among others, e.g. classification according to encountered incidents, according to breached assets, according to assessed impact etc. Discussions performed with members of the ENISA Stakeholder Group, led to the conclusion that it might be worthwhile examining various classification schemes and allowing the users of the threat landscape to select the one that best suits to their needs. This can be achieved by taking into account documented impact, relevant sectors, geographical spread, etc. In the presentation of the threats below, more frequent threats are mentioned first.

Having said that, it is worth mentioning that our aim was to present a priority of threats. However, users of this material who wish to use it as input to their assessments, will need to consider cyber-threats according to the ***scope*** of their assessment. This might require prioritisation according to relevant assets, vulnerabilities, impact level, etc. In such cases, the presented prioritisation might need to be changed to fulfil the needs of the scoping exercise.

[14] 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 known publications 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 threat dynamics and trends.

https://t.me/learningnets

The following threat descriptions consist 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, v) a list of authoritative resources and vi) the position of the threat in the attack workflow[15].

This chapter is concluded by a comparison between the current threat landscapes of the ETL 2013 and the ETL 2014. This will help readers to easily understand the changes of the current threat landscape in this time period.

3.1 Malicious Code: Worms/Trojans

In this reporting period, malware (worms/Trojans and Potentially Unwanted Programs – PUPs) tops the list of cyber threats, with worms and Trojans being the most common type of newly created malware[16,36]. It is interesting that in the reporting period, an observed increase of adware was observed, due to software delivered in form of bundled free software, the so called Potentially Unwanted Programs (PUPs)[17]. Besides topping the cyber threats in 2014, there are some additional interesting developments regarding malware. These developments concern: use of custom encryption for communication with C&C servers[167], file-less malware[18,19] , increase of spyware[20,21], provision of multi-platform capabilities[22], use of anonymity network TOR[23] and obfuscation /evasion techniques[24]. These advancements, together with the vast amount of malware variants per day (ca. 350.000), decreases the efficiency of existing signature based antivirus tools[44].

In this reporting period we have concluded that:

- Worms are over 19% of malware. Interestingly the Conficker worm – a six year old malware - is still the most commonly detected malware in domain computers (i.e. business environments). In PCs it is the number one detection (also referred to as DOWNADUP) [25,36].
- Due to its dynamics, complexity, sophistication and stealthiness, over 50% of malware stays undetected by antivirus products[44]. This indicated the need for multi-layered security

[15] Due to the scope of each cyber threat in ETL 2014, but also due the consolidation that is part of our analysis process, the kill chains of the threats is of generic nature. In other words, it might not correspond to the phases included in a particular detail threat assumed within this cyber-threat category. Rather it has been selected as a superset of phases found in all threats of this kind.

[16] http://www.pandasecurity.com/mediacenter/press-releases/malware-still-generated-rate-160000-new-samples-day-q2-2014/, accessed October 2014.

[17] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-turning-the-tables-on-cyber-attacks.pdf, accessed October 2014.

[18] https://blog.gdatasoftware.com/blog/article/poweliks-the-persistent-malware-without-a-file.html, accessed November 2014.

[19] http://www.faronics.com/news/blog/reboot-to-restore-new-fileless%E2%80%8B-malware-making-the-rounds-66/, accessed October 2014.

[20] http://www.heise.de/newsticker/meldung/FinFisher-Co-machen-harmlose-Katzenvideos-zur-Waffe-fuer-Cyber-Attacken-2293549.html?wt_mc=rss.ho.beitrag.atom, accessed November 2014.

[21] http://www.theguardian.com/technology/2014/nov/06/spyware-exports-licence-new-eu-rules-military-applications, accessed November 2014.

[22] http://www.tripwire.com/state-of-security/top-security-stories/mask-sophisticated-multi-platform-malware-espionage-operation/, accessed October 2014.

[23] http://threatpost.com/shedding-new-light-on-tor-based-malware/104651, accessed October 2014.

[24] http://www.fireeye.com/blog/technical/malware-research/2014/06/turing-test-in-reverse-new-sandbox-evasion-techniques-seek-human-interaction.html, accessed October 2014.

[25] http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft_Security_Intelligence_Report_Volume_16_English.pdf, accessed October 2014.

https://t.me/learningnets

solutions that perform malware detection at multiple levels of the infrastructure (i.e. network, application level, etc.) [26,27,44].

- In this reporting period, ca. 30% of malware used custom encryption to hide communication of stolen data[28]. It is interesting, that for this purpose SSL is not used due to the overhead related to certificates[28]. Besides securing communication, encryption has been also used in order to store modules of malware as encrypted data blobs that evade forensic functions[29].
- The increase in numbers of malware variants is a result of the availability of malware toolkits that can be found in the underground malware market[30]. Such tools offer obfuscation functions that allow for automated scanning of existing signatures and creation of new ones to evade antivirus detections[103].
- Open environments are the "paradise" of malware infections[44]. Due to access through a variety of users (obviously maintaining poor end-point security) academic, education and university environments were responsible for over 40% of malware detections. This demonstrates the difficulty in imposing security controls in such open environments.
- Sophistication of malware has been impressively demonstrated by means of existing banking Trojans. Such Trojans (e.g. the Italian and Turkish jobs[31]), have demonstrated a great deal of criminal energy and knowledge behind the attack: for example, as all sensitive components have been removed right after the investigation by law enforcement agencies had started[40]. Moreover, banking Trojans have been reused/reconfigured in order to steal user information[32]. Once installed, this malware can be re-configured to attack any kind of information, further to banking data. The efficiency in infection rates is illustrated by the fact that one in every 500 PCs is infected with this banking malware[33]. This corresponds to an increase by a factor of four within the reporting period and by a factor of 14,5 since mid-2012[40].
- Malware defence tactics need to be revised. While most of the tactics are mainly defending from "commodity malware"[34] new, more advanced approaches to malware defence need to be developed. They should not be based solely on detection at the end-points, but rather involving countermeasures at the level of network architecture. Another interesting measure for spyware control is its inclusion in the control list on dual use items[35] (together with surveillance equipment).

[26] http://online.wsj.com/articles/SB10001424052702303417104579542140235850578, accessed November 2014.
[27] http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/, accessed November 2014.
[28] http://www.websense.com/content/websense-2014-threat-report.aspx, accessed October 2014.
[29] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf, accessed November 2014.
[30] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf, accessed November 2014.
[31] http://bgr.com/2014/06/25/luuuk-trojan-online-banking-malware/, accessed October 2014.
[32] http://www.darkreading.com/operations/identity-and-access-management/new-citadel-attack-targets-password-managers/d/d-id/1317642, accessed December 2014.
[33] http://www.computing.co.uk/ctg/news/2370710/ibm-warns-over-proliferating-use-of-banking-trojans-in-enterprise-attacks), accessed October 2014.
[34] http://digital-forensics.sans.org/community/papers/grem/malwared-study-network-host-based-defenses-prevent-malware-accomplishing-go_3428, accessed November 2014.
[35] http://trade.ec.europa.eu/doclib/press/index.cfm?id=1166, accessed November 2014.

https://t.me/learningnets

Observed current trend for this threat: *increasing*

Related threats: Web application/Injection attacks, Exploit Kits, Botnets, Information leakage, Identity theft, Data breaches, Ransomware/Rogueware/Scareware, Phishing, Cyber espionage.

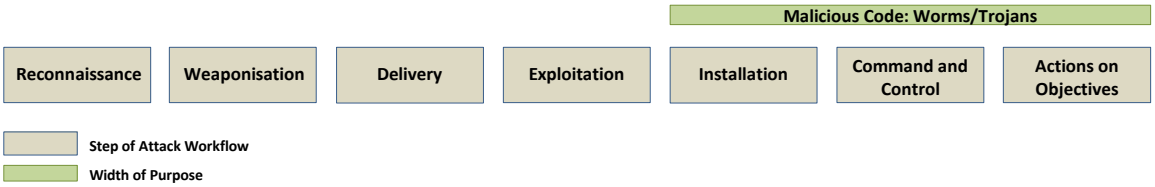


Figure 4: Position of Malicious Code: Worms/Trojans in attack workflow

3.2 Web-based attacks

Following existing reporting practices in this reporting period, the threat named *Web-based attacks* covers all available techniques regarding redirection of web browsers to malicious web sites where further malware infections may take place[36]. In 2013, this kind of attack has been referred to as "drive-by-downloads". As was the case with other threats, in the reporting period a shift has been assessed regarding this threat. This was due to widening of the scope of redirections (e.g.. disseminated via phishing messages), deployment of additional techniques in mobile devices/mobile apps and a strong decline in the use of the exploit kit Blackhole (after the arrest of its developers[37]). Nonetheless, available vulnerabilities in web browsers are still most often exploited in order to achieve a redirection to malicious sites (i.e. malicious URLs). The primary surface for exploitation are vulnerabilities of the Java programming environment and browser exploits[36,38,39].

In this reporting period we have assessed that:

- Web-based attacks are facilitated by the fact that malicious URLs are easy to implement. In this reporting period some 145 million unique URLs have been recognized as malicious (responsible for 39% of web attacks). The malicious URL is by far the first malicious object detected (72,9%)[40].
- It seems that short-lived domains further facilitate the creation of malicious URLs. According to reports found[41], ca. 0,4% of short life domains are malicious and have a life-cycle of ca 48 hours. These are ca. 2 million URLs every second day that are used for drive-by-communication, botnets and malware hosting. This reduces the usefulness of blacklists and increases maintenance effort. Therefore, in addition to blacklists, end-users need also to introduce intrusion detection combined with end-device security (i.e. Anti-Virus and Web Antimalware).
- Web-based attacks take the first position in the threat landscape in North America and Europe. In other continents, they are positioned in the lower middle field of top threats, following malware[36]. Assuming a higher spread of online services in North America and

[36] http://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf, accessed October 2014.
[37] http://www.pcworld.com/article/2070360/12-suspected-cybercriminals-arrested-in-russia-along-with-blackhole-creator.html, accessed October 2014.
[38] http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html, accessed October 2014.
[39] http://www.infosecurity-magazine.com/news/web-loving-malware-doubles-in-2013/, accessed October 2014.
[40] https://securelist.com/files/2014/08/KL_Q2_IT_Threat_evolution_EN.pdf, accessed October 2014.
[41] http://www.csoonline.com/article/2599806/data-protection/spotting-web-threats-in-the-confusion-of-short-lived-hostnames.html, accessed October 2014.

https://t.me/learningnets

Europe, it seems that web browsers are the main targets. Country statistics might be seen as a validation of this assumption: 88% of malicious web resources are located in Europe and North America[36].

- Although Java exploits have declined, Java is still by far the most exploited web software by this threat. Ca. 90 percent of web exploits are Java related. Among the reasons for these rates is the fact that a large amount of web sites (over 70%) use Java versions that are unsupported (e.g. Java 6)[42].
- While malicious URLs is the most widely detected malicious object, they are responsible for ca. 39% of detected infections. Malware infections scored higher[40]: several hundreds of millions of infections took place via viruses/worms/Trojans. This led us to consider web attacks as the second threat in the row in the ETL 2014.

Observed current trend for this threat: *increasing*

Related threats: Malware: Worms/Trojans, Web application attacks/Code Injection, Exploit Kits, Ransomware/Rogueware/Scareware, Cyber espionage.

Authoritative Resources: "*F-Secure Threat Report H1 2014"*[36], "*Kaspersky IT THREAT EVOLUTION Q2 2014"*[40].

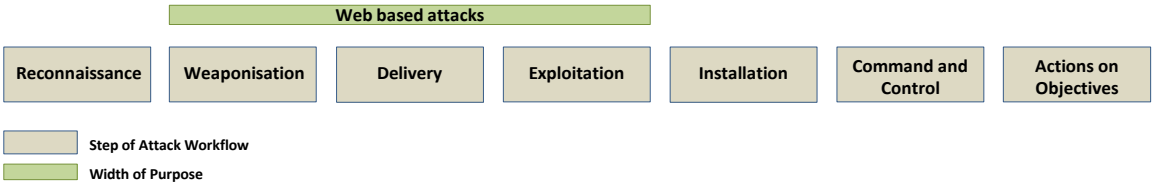


Figure 5: Position of Web-based attacks in attack workflow

3.3 Web application attacks / Injection attacks

Web application attacks consist mainly of feeding vulnerable servers and/or mobile apps with malicious inputs or unexpected sequences of events with the objective to inject malicious code, alter site content or breach information. In the area of web application attacks, some interesting developments are worth noticing: firstly, a slight reduction of vulnerable applications has been identified[43]. This is due to the fact that application developers have understood issues with SQL injection and have managed to reduce the attack surface. Moreover, app stores seem to do a good job in testing apps on malicious activities. Despite more efficient coding practices, in the reporting period web application vulnerabilities have increased slightly.

Yet, despite proportionally less SQLi incidents, a large amount of web applications are still vulnerable (over 90%[43]). Top web application threats are XSS, information leakage, authentication and access control, insecure object references, SQLi[44,45,46]. Interestingly, in recent surveys, the majority of CISOs (51%) are concerned about risks emanating from application vulnerabilities[47], while they see application threat exposure increasing.

[42] http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html, accessed October 2014.
[43] http://www.cenzic.com/downloads/Cenzic_Vulnerability_Report_2014.pdf, accessed October 2014.
[44] http://www.nttcomsecurity.com/en/services/managed-security-services/threatintelligence/, accessed October 2014.
[45] http://info.whitehatsec.com/rs/whitehatsecurity/images/statsreport2014-20140410.pdf, accessed October 2014.
[46] http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed5.pdf, accessed December 2014.
[47] https://www.owasp.org/index.php/CISO_Survey_2013:_Threats_and_risks, accessed October 2014.

https://t.me/learningnets

In this reporting period we have assessed that:

- A reduction of web application attack surfaces has been identified: Areas where flaws were understood by developers are: SQLi, Clickjacking and Cross Site Request Forgery (CSRF)[48].
- Besides injection attacks on web applications, mobile apps are exposed to additional threats. This is due to an inherent shift of architectural principles from web applications to mobile applications: this allows an attacker to deploy traditional web application threats in new unconventional ways[49]. As a result, reverse engineering or modifications the app's binary code [50] are possible. Moreover, in the reporting period an injection method known as Fragment Injection has been detected[51].
- Web application attacks are the second threat in the area of cloud computing surfaced by cloud hosting providers[75].
- Web application/Injection attacks are expected to develop in the coming years. This is mainly due to possible attacks to mobile devices, in combination with new web technologies, i.e. HTML5. Cross Device Scripting (XDS) is such an attack, which is assessed by experts to become a very serious threat in the future[52].
- Java is still by far the most exploited web software. Ca. 90 percent of web exploits are Java related. Among the reasons for these rates is the fact that a large amount of web sites (over 70%) use Java versions that are unsupported (e.g. Java 6)[53].

Observed current trend for this threat: *increasing (flat)*

Related threats: Web-based attacks, Data Breaches, Worms/Trojans, Botnets, Exploit Kits.

Authoritative Resources: NTT Group *"GLOBAL THREAT INTELLIGENCE REPORT 2014"*[44], WhiteHat Security "*2014 Website Security Statistics Report*"[45], IMPREVA *"WEB APPLICATION ATTACK REPORT #5"*[46].

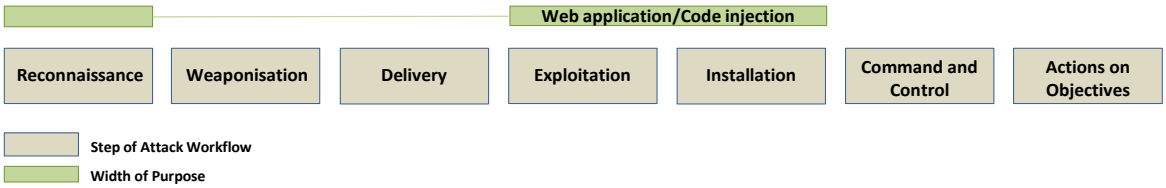


Figure 6: Position of Web application/Injection attacks in attack workflow

3.4 Botnets

In this reporting period a lot of dynamic changes happened in the area of botnets. Firstly however, one should mention the successes in taking down botnets. The takedown of ZeroAccess botnet has

[48] http://www.aspectsecurity.com/the-2014-state-of-developer-application-security-knowledge-report-landing-page, accessed October 2014.
[49] https://www.owasp.org/index.php/Architectural_Principles_That_Prevent_Code_Modification_or_Reverse_Engineering, accessed October 2014.
[50] https://www.owasp.org/index.php/Mobile_Top_10_2014-M10, accessed October 2014.
[51] http://securityintelligence.com/new-vulnerability-android-framework-fragment-injection/#.VES0vaP6gnM, accessed October 2014.
[52] http://www.cis.syr.edu/~wedu/Research/paper/code_injection_most2014.pdf, accessed October 2014.
[53] http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html, accessed October 2014.

https://t.me/learningnets

been performed as a globally coordinated action with the involvement of law enforcement (German BKA), industry (Microsoft, Symantec) and governments (Netherlands, Latvia, Luxembourg and Switzerland)[54,55]. Activities like this have led to a reduction of PC based botnets. On the other hand, attackers have changed strategies and moved away from botnet-driven PC infections[42]. In particular, they seem to work on building up web server based botnets. The advantage of this approach lies in the superior performance of web server machines: one web server zombie performs better than hundreds of PCs and is far easier to administrate[73]. Other forms of botnets that emerged in the reporting period include hardware based botnets abusing internet of things devices[56]. Speculations about the existence of cloud based botnets do also exist, following a demonstration of feasibility from the scientific community[57].

In the reporting period we have assessed that:

- All in all, botnet activity has been a very serious cyber-threat: it accounted for 34% of attacks and has thus ranked at 1st position of attack statistics[44]. However, due to successful law enforcement takedowns, the number of botnets has dropped in the reporting period (number of infected computers went down form ca. 3.5 million to ca. 2.3 million[55]). However, newer forms of botnet infections have shown up, which will lead to an increase of infected devices. As in other areas of malware, infected mobile devices will significantly contribute to the increase of botnet nodes[58].
- Botnet takedowns are quite controversial[59;60;61]. Firstly it is a matter of fact that through incorporated resilience mechanisms, total takedown of a botnet is not feasible[55]. While disruption of a botnet may give hard times to cybercriminals, the fact that the botnet still exists will give them the opportunity to build it up again, by potentially advancing structure and functions[36]. This might be at least a risk equal to the existence of the disrupted botnet, as experts argue. It has been reported, that during the takedown operation of ZeroAccess botnet its operators fixed a weakness in the protocol to disrupt the ongoing takedown campaign[55].
- Other forms of botnets seem to be in place consisting of smaller devices that are networked such as routers[62], sensors and Internet of Things devices[63]. The creation and operation of such botnets can be performed by means of an available toolkit that supports a variety of devices[64].
- Sophistication and stealthiness of botnets improved in this reporting period. The use of short life domains (ca. 2 million with a life shorter than 48 hours) are being used for various

[54] https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report, accessed October 2014.
[55] http://www.symantec.com/security_response/publications/threatreport.jsp, accessed October 2014.
[56] http://securityaffairs.co/wordpress/28642/cyber-crime/spike-botnet-runs-ddos.html, accessed November 2014.
[57] http://www.wired.com/2014/07/how-hackers-hid-a-money-mining-botnet-in-amazons-cloud/, accessed October 2014.
[58] http://www.theinquirer.net/inquirer/news/2322028/24-000-android-devices-are-hit-by-xxxxapk-mobile-botnet, accessed October 2014.
[59] https://www.damballa.com/microsoft-dcu-strike-three-now-what-2/, accessed November 2014.
[60] http://www.computerweekly.com/news/2240215443/RSA-2014-Microsoft-and-partners-defend-botnet-disruption, accessed October 2014.
[61] http://www.judiciary.senate.gov/imo/media/doc/07-15-14VixieTestimony.pdf, accessed November 2014.
[62] http://www.welivesecurity.com/2014/03/04/more-than-300000-wireless-routers-hijacked-by-criminals-in-global-attack/, accessed October 2014.
[63] http://www.incapsula.com/blog/ddos-threat-landscape-report-2014.html, accessed October 2014.
[64] http://www.csoonline.com/article/2687653/data-protection/new-toolkit-seeks-routers-internet-of-things-for-ddos-botnet.html, accessed October 2014.

https://t.me/learningnets

malicious activities, including botnet communication[41]. Such sources are difficult to detect and takedown. Moreover, advanced botnet infections techniques aggravate botnet detection[65].

Observed current trend for this threat: *decreasing (number only; while efficiency has significantly increased)*

Related threats: Web application attacks / Injection attacks, Malicious code, Exploit Kits, Phishing, Spam, Denial of Service, Ransomware/Rogueware /Scareware.

Authoritative Resources: Symantec "*INTERNET SECURITY THREAT REPORT APPENDIX 2014*"[30].

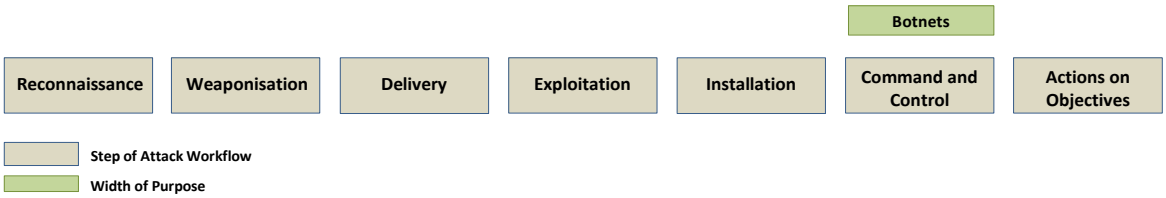


Figure 7: Position of Botnets in attack workflow

3.5 Denial of Service

In this reporting period, DDoS attacks continued to be a strong tool of adversaries. As with other threats, DDoS has evolved in many ways. Firstly, bandwidth has continued its growing trend: in 2014 (Q1-Q2) the average bandwidth of attacks is ca. 70% higher than in 2013, whereas a peak of ca. 240% higher has been observed[63, 66,67]. There are various reasons for this development. Firstly, reflection attacks have been more efficient in that they take advantage of multiple protocols (NTP, SNMP, DNS), with SNMP reflection demonstrating a comeback[67]. They bear the advantage that they can be performed without any involvement of botnets. Secondly, the use of server-based botnets (often hosted on performant web/cloud based servers) are more difficult to detect can be stealthy until their activation[68]. This is a shift away from PC-based botnets that significantly increases performance and C2 management[67]. Finally, one should mention the increased complexity of DDoS attacks: by attacking at the infrastructure and transport layer (i.e. TLS) (layers 3 and 4) and application layer (layer 7), a change of attack vectors in the course of single attack campaigns make their detection difficult[69].

In the reporting period we have assessed that:

- DDoS attacks are evolving by gaining in sophistication, stealthiness and unpredictability. Volumetric, asymmetric, computational, and vulnerability-based attacks are now in the arsenal of threat agents[70]. Moreover, attack bandwidth continues growing (peak 325 Gbps this year), while time windows of attacks become smaller (i.e. reduction of their duration).

[65] http://www.tomsguide.com/us/java-botnet-mac-linux-pc,news-18260.html, accessed October 2014.
[66] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf, accessed November 2014.
[67] http://www.prolexic.com/knowledge-center-dos-and-ddos-attack-reports.html, accessed October 2014.
[68] http://www.spiegel.de/netzwelt/web/ddos-mit-ntp-grosse-attacke-mit-gefaelschten-statusabfragen-a-953079.html, accessed October 2014.
[69] http://www.bankinfosecurity.com/whitepapers/analyst-report-idc-analyst-connection-ddos-prevention-time-for-w-1112, accessed October 2014.
[70] https://f5.com/solutions/enterprise/reference-architectures/ddos-protection, accessed October 2014.

https://t.me/learningnets

- Most DDoS attacks have been launched in combination with another attack, thus used as "smokescreening" to distract defenders from the collateral attacks happening in parallel[71,72]. In particular, the main objectives of collateral attacks assessed are: Virus and Malware installation/activation (49%), data theft (25,53%), loss of intellectual property (19,15%) and financial theft (10,64%)[71].
- Volumetric attacks will continue to be the main attack type in the future. Efficient reflection attacks and performant server-based botnets ease the deployment of such attacks[69,73]. The trend of SSDP reflection growth should be observed carefully and measures to reduce this exposure should be implemented[74].
- The trend of declining application attacks is continued in 2014. Nevertheless, they have picked up during the 2nd quarter. It is worth mentioning that application layer attacks are a strong tool as they may create significant impact and such attacks are difficult to detect and defend against. Along with reconnaissance attacks, brute force attacks and vulnerability scans these attacks may open new avenues of misuse of web applications through adversaries[75].
- In the reporting period, DDoS attacks to SSL have been detected. These are difficult to detect without decrypting and analysing SSL traffic[69,76]. This sort of attack continues to grow. Although SSL attacks increase computational load[77], together with weaknesses regarding SSL[78] they provide a considerable attack surface for this technology.
- After big increases at the beginning of 2014, NTP reflection attacks are on the decline as a result of awareness raised within the security community that led to reduction of servers to be abused (reduction of servers responding to monlist requests)[79,80].

Observed current trend for this threat: *increasing*

Related threats: Botnets, Web-based attacks, Data breaches, Malware: Worms/Trojans.

Authoritative Resource: "*Prolexic Quarterly Global DDoS Attack Report Q2 2014*"[67], "*NSFOCUS DDoS Threat Report 2013*"[73], *Incapsula "20013-2014 DDoS Threat Landscape Report*"[63], *Symantec "The continued rise of DDoS attacks"*[66].

[71] http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf, accessed October 2014.
[72] http://www.csoonline.com/article/2365062/disaster-recovery/code-spaces-forced-to-close-its-doors-after-security-incident.html?utm_source=CSO&utm_medium=LinkedIn, accessed November 2014.
[73] http://en.nsfocus.com/SecurityReport/NSFOCUS%20DDoS%20Threat%20Report%202013.pdf, accessed October 2014.
[74] http://www.scmagazine.com/ssdp-reflection-ddos-attacks-on-the-rise-akamai-warns/article/377754/, accessed October 2014.
[75] http://www.rackspace.com/knowledge_center/sites/default/files/whitepaper_pdf/ALERT-LOGIC-CLOUD-SECURITY-REPORT-Spring-2014.pdf, accessed October 2014.
[76] http://www.slideshare.net/BlueCoat/infographic-stopattackshidingunderthecoverofsslencryption, accessed October 2014.
[77] http://www.arbornetworks.com/asert/2012/04/ddos-attacks-on-ssl-something-old-something-new/, accessed October 2014.
[78] http://www.symantec.com/connect/blogs/ssl-30-vulnerability-poodle-bug-aka-poodlebleed, accessed October 2014.
[79] http://www.stateoftheinternet.com/downloads/pdfs/2014-state-of-the-internet-threat-advisory-ntp-amplification.pdf, accessed October 2014.
[80] http://openntpproject.org/, accessed November 2014.

https://t.me/learningnets

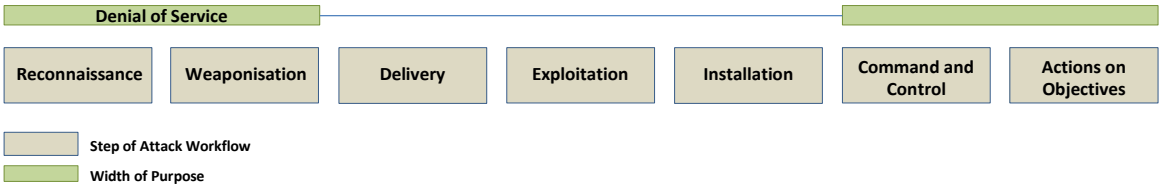


Figure 8: Position of Denial of Service in attack workflow

3.6 Spam

In this reporting period spam decreased, although its malicious intent remains constant[42]. The impressive drop of spam compared with volumes of 2010-2011 is related to take downs of large spam bots and successful spam blocking practices[25]. However, spam is still a serious cyber threat[166]: ca. 75% of messages are unwanted. Phishing comprises only ca. 4% of the entire spam volume[25]. From available statistics and spam volumes, it is assumed that quite some spam bots might exist in geographic areas where Window XP is still operated[81]. Another characteristic of spam are unexpected waves that come and go. In March 2014, spam numbers have been detected that are the highest of the last two and a half years[81]. Just as for phishing, spammers piggyback on international events that obtain media attention[82] in order to lure their victims. Speed of spread is one important element for spams: spam messages based on breaking news sent immediately after an event, thus making recipients believe that the message is authentic (admittedly an overlapping method with spear phishing, see section 3.6). Finally, it is worth mentioning that spam is rather well understood as an e-mail threat. In the reporting period, however, we have seen increased spam disseminated over channels that are non-typical for this threat, such as Social media spam[83], mobile apps, SMS, etc[84]. This "mutation" of spam opens new opportunities for attackers to increase the efficiency of their campaigns and achieve better infection rates.

In this reporting period we assessed that:

- Top themes for spam worldwide are: Bank Deposit/Payment Notifications, Online Product Purchase, Attached Photo, Shipping Notices, Online Dating, Taxes, Facebook, Gift Card or Voucher, PayPal[42].
- Although rather stable, image spam is an important tool of adversaries. As being typical for spam, however, some voluminous image spam activities have been detected in the period between December 2013 and January 2014. It is argued that images are an interesting content for spammers, as most spam filters are text based. Thus, spam images might evade spam-detection capabilities[81].
- In the reporting period spam has been assessed as a serious mobile threat[85,86]. Through parallel campaigns started both in social media and mobile applications, spammers try to

[81] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=WGL03050USEN#loaded, accessed October 2014.
[82] http://securelist.com/blog/58260/the-world-cup-spammers-set-their-sights-on-goal/, accessed October 2014.
[83] http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf, accessed October 2014.
[84] https://securelist.com/analysis/quarterly-spam-reports/67851/spam-and-phishing-in-the-q3-of-2014/, accessed December 2014.
[85] http://www.pandasecurity.com/mediacenter/news/whatsapp-scam/, accessed October 2014.
[86] http://www.pcadvisor.co.uk/news/software/3331146/new-whatsapp-charging-hoax-surfaces/, accessed October 2014.

https://t.me/learningnets

create user confidence about the trustworthiness of their messages. Through convolution of messages through various channels, it may become difficult for users to detect malicious purpose of messages.

- In social media we have seen significant spam increase rates[83]. It has been assessed that during first half of 2013 social spam volume has increased by 355% (one every 200 messages), with Facebook and YouTube leading the list of spam distribution social platforms (one every 100 messages). It is impressive that the number of spam messages increases faster than that of comments in social media[83].
- With the proliferation of mobile devices, text messages (SMS) are also misused as a spam channel. Spam text messages often aim at infecting mobile devices with malware (i.e. via malicious URLs) or just as a reconnaissance mechanism to identify valid telephone numbers (eventually connected to IDs in cloud services of providers, such as Apple-Cloud IDs)[87].

Observed current trend for this threat: *decreasing*

Related threats: Web-based attack, Phishing, Malicious code, Exploit Kits, Botnets.

Authoritative Resources: "*IBM X-Force Threat Intelligence Quarterly 2Q 2014*"[81], regarding spam in social media: "*NEX GATE 2013 STATE OF SOCIAL MEDIA SPAM*"[83].

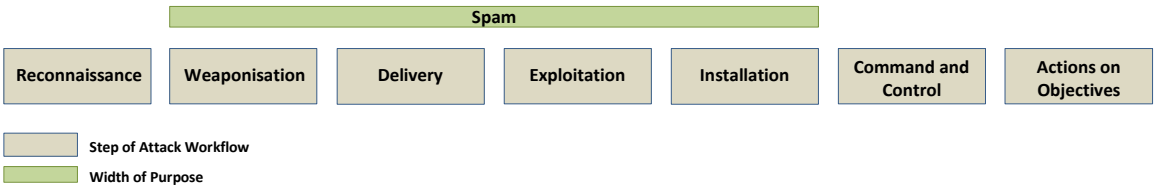


Figure 9: Position of Spam in attack workflow

3.7 Phishing

Phishing has definitely advanced in the reporting period, mainly through technical deception[88]. Attackers often combine spoofed e-mails and counterfeited web sites to lure users to malicious sites with the very objective of infecting end-user devices. The second component of phishing is social engineering. Both components gain in efficiency from availability of breached data in the underground market[89,92]. The ultimate malicious aim is to steal/intercept user names and passwords and financial credentials[90]. In addition to these advancements, it is remarkable that phishing volumes in the reporting period have been quite high[106] (Q2 2014 has been the second highest number since Q2 2012). The premium target of phishing activities are payment services, financial and retail services and crypto-currencies. Malicious URLs found in phishing messages demonstrate an increase of distribution

[87] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-mobile-cybercriminal-underground-market-in-china.pdf, accessed October 2014.
[88] http://blog.trendmicro.com/trendlabs-security-intelligence/new-phishing-technique-outfoxes-site-owners-operation-huyao/, accessed November 2014.
[89] http://krebsonsecurity.com/2011/04/epsilon-breach-raises-specter-of-spear-phishing/, accessed October 2014.
[90] http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf, accessed October 2014.

https://t.me/learningnets

of PUPs (adware, spyware) [91] . Targeted phishing campaigns combining personal identifiable information (PII) is known as spear phishing[92].

In this reporting period we have assessed that:

- Some interesting data regarding phishing are: Europe is the region with the lowest infection rates due to phishing messages. US is the number one country hosting phishing-based Trojans. Supposedly, this is due to the fact that the biggest part of the .com domain is hosted in the US[90].
- The proliferation of new technologies - usually bearing vulnerabilities and weak security controls - may lead to information theft/leakage. When misused within a spear phishing message, attacks can become extremely efficient and very difficult to defend[93,94]. Defending this threat will be a significant challenge, as it is obvious that when possessing information from the user's intimate environment, it will be very easy to fool them. Smart Cities, smart vehicles will constitute another big potential of phishing abuse[95]. In the reporting period ENISA has produced a detailed threat landscape and good practice guide for smart homes[409], that further elaborates on these issues.
- In order to understand the importance of phishing as cyber-threat, one needs to have a look at the rankings of seriousness of cyber-attacks: in some reports, phishing is in the 3rd position behind web based attacks and DDoS[96]. This fact demonstrates the importance of this threat for adversaries.
- It is common, that attackers may craft spear phishing messages by collecting publicly available information on victims. Social networking sites are the main source of information collection. This usually takes place during initial phases of targeted attacks, i.e. external reconnaissance[97].
- Social networking is also an important target for phishing. According to phishing statistics, Social Networking sites are the third target of phishing behind payment and financial systems[98].
- Defence of phishing/spear phishing is based mainly on appropriate end-user behaviour and awareness[99]. This defence is difficult to achieve, as following phishing trends, enrolment of end-user and awareness raising might be time-consuming and costly. Some information found in the reporting period provides a deeper insight into the topic[100].

Observed current trend for this threat: *increasing*

Related threats: Web-based attacks, Malicious code: Worms/Trojans, Identity theft, Data breaches.

[91] https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/GData_PCMWR_H1_2014_EN_v2.pdf, accessed November 2014.
[92] http://www.symantec.com/connect/blogs/phishing-post-mega-breach-how-loss-pii-only-start-your-customers-problems, accessed October 2014.
[93] http://www.proofpoint.com/about-us/press-releases/01162014.php, accessed October 2014.
[94] http://www.rand.org/pubs/research_reports/RR604.html, accessed October 2014.
[95] http://blog.kaspersky.com/a-week-in-the-news-april-1/, accessed October 2014.
[96] http://www.bitpipe.com/detail/RES/1412725269_735.html, accessed October 2014.
[97] http://www2.fireeye.com/rs/fireye/images/fireeye-real-world-assessment.pdf, accessed October 2014.
[98] http://blog.phishlabs.com/banks-epayment-top-list-of-phishing-kit-targets, accessed October 2014.
[99] http://ijraonline.com/Published%20Papers/1(1)36-39.pdf, accessed October 2014.
[100] http://www.darkreading.com/how-to-successfully-phish-your-own-firm/d/d-id/1139511?, accessed November 2014.

https://t.me/learningnets

Authoritative Resources: APWG "*Phishing Activity Trends Report 2nd Quarter 2014*"[90].

Figure 10: Position of Phishing in attack workflow

3.8 Exploit Kits

Exploit kits are a major tool of threat agents. They are automated tools, mainly detecting vulnerabilities at user end-devices and then downloading and managing malicious content accordingly[101]. The area of exploit kits has undergone significant developments in the reporting period, being thus maybe the best example of threat landscape dynamics. Around the end of reporting period of ETL 2013, the developer of Blackhole, of one of the prevailing exploit kits was arrested[102]. Since then, we have been in the position to observe a realignment of the exploit kit "market". Within 2014, Blackhole has almost disappeared from the landscape (currently estimated ca 3% of exploit kit market, while previously covering ca. 44%[103]). Cyber-criminals have almost immediately adapted to breaking news and have changed to other exploit kits[104]. Though not yet reaching the same level of usage, new exploit kits have come to fill the void left by Blackhole. In addition, in the reporting period we have seen cyber-criminals increasing the sophistication of exploit kits. Examples are: checked vulnerabilities in the victim's systems that are considerably newer, while it has become possible to infect hosts by injecting malware directly into existing processes[105], instead of downloading the payload by means of files. It is expected that exploit kit usage will continue to be a main threat leading to infections on the Web. Despite a contemporary decrease, the potential to see increased usage of exploit kits in the future is quite big[106].

In the reporting period we have assessed that:

- Like almost all cyber threats, exploit kits become more complex/sophisticated. In the reporting period we have seen exploit kits infecting targets with file-less malware, using TOR[107] communication between installed malware and C&C. Publication of exploit kit source code allows more malware authors to create more innovative, new attack patterns[103].
- It has been assessed, that organisations deploying vulnerability management show significantly lower infection rates from exploit kits than those without. Yet, vulnerability management based on manual processes (i.e. excel lists) seems to be weaker than more mature solutions based on formal methods.

[101] http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf, accessed October 2014.
[102] http://threatpost.com/blackhole-exploit-kit-author-arrested-in-russia/102537, accessed October 2014.
[103] http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf, accessed October 2014.
[104] http://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2013.pdf, accessed October 2014.
[105] http://www.securityweek.com/malware-injected-directly-processes-angler-exploit-kit-attack, accessed October 2014.
[106] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-vulnerabilities-under-attack.pdf, accessed December 2014.
[107] http://www.isssource.com/new-exploit-kit-using-tor/, accessed October 2014.

https://t.me/learningnets

- The average age of vulnerabilities used within exploit kits has been reduced significantly. While some years ago the average age of exploit kit vulnerabilities were at about two years, recent tools contain many actual vulnerabilities of one year average age. This is considered as another indication of increased sophistication of these malicious tools[44]. Other indications of increase sophistication are found in the Angler Exploit Kit that integrates Microsoft Silverlight vulnerabilities and uses gzip and Pack200, a compression method specially optimized for JAR archives[104]. Further indications for the creativeness of adversaries are redirects that have led Yahoo users to an exploit kit that exploited Java vulnerabilities and had installed malware including ZeuS, Andromeda and Dorkbot/Ngrbot[28]. Another innovation are DNS hijacks that redirected users to exploit kits[55].
- The new order in the area of exploit kits, especially after the arrest of Blackhole developer, is reflected in the available exploit kit statistics[103], according to which their spread is: Neutrino 24%, Unknown kit 21%, Redkit 19%, SweetOrange 11%, Styx 10%, Glazunov/Sibhost 5%, Nuclear 4% , Blackhole/Cool 3%, Other 3%, while Angler exploit kit seems to gain momentum[104].
- As security researchers argue, the possibility of the source code of Blackhole being published does exist. It is being argued, that publication of source code *helps malicious actors mask their trails from investigators* and detection[55]. This is due to improvements that may be implemented in existing malicious code. This was already the case with BlackPOS[108].

Observed current trend for this threat: *decreasing*

Related threats: Web-based attacks, Web application attacks/Code Injection, Malicious code: Worms/Trojans, Phishing, Ransomware/Rogueware /Scareware.

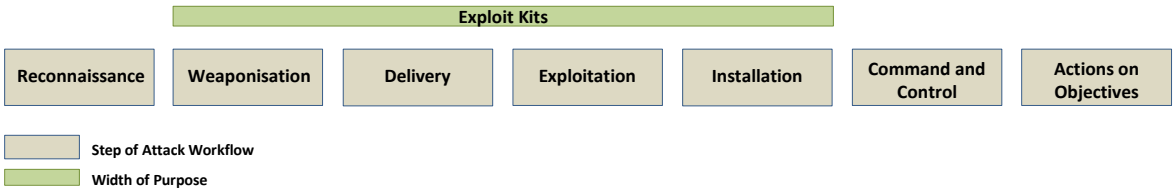


Figure 11: Position of Exploit Kits in attack workflow

3.9 Data Breaches

Due to significant increase of this type of threat, 2014 has good chances to become the *year of the data breach*. Data breach data assessed up to the authoring period of this report (Oct-Dec 2014) have already demonstrated an increase of ca. 25% over the same period in 2013[109,110,111]. In the reporting period many kinds of data breaches have surfaced. Most of those have had significant impact, at least within media and businesses: many have concerned large numbers of consumer information[112], others

[108] http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q4-2013.pdf, accessed October 2014.
[109] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html, accessed October 2014.
[110] http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf, accessed December 2014.
[111] http://www.computerweekly.com/news/2240235603/Films-leaked-online-after-Sony-Pictures-hack?asrc=EM_EDA_36999404&utm_medium=EM&utm_source=EDA&utm_campaign=20141201_Films%20leaked%20online%20after%20Sony%20Pictures%20hack_, accessed December 2014.
[112] http://www.forbes.com/sites/maggiemcgrath/2014/10/02/jp-morgan-says-76-million-households-affected-by-data-breach/, accessed October 2014, (indicative, selected as the latest found in the media).

https://t.me/learningnets

a small numbers of celebrities[113]. But not only personal data are subject to this threat: valuable information, mostly with financial impact is considered to be prime target of cyber-criminals, e.g.. Bitcoins[114,115]. Data breaches are the result of successful cyber-attacks, materialised cyber threats, or erroneous unintentional user activities, all leading to disclosure of confidential information. Due to their impact but also long term consequences, data breaches are among the most thoroughly managed and investigated cyber incidents. This is due to the fact that relevant national and international regulations force operators of IT systems - especially in the area of Critical Infrastructure – to report data breaches[116,117,118]. It is expected that more and more sectors will be obliged to join data breach reporting schemes in the near future.

In this reporting period we have assessed that:

- According to extensive data breach reports, the causes of data breaches are: Weak passwords, Vulnerable networks and application, Malware, Phishing, Incorrect user authentication, Insider threat, Tampering, Database errors[119,120]. This motivates the identified need for two factor authentication[121]. An observed deviation of data breach statistics/causes can be found in various reports[122,123,124]. It should be clear that data breach reports depend on the context/subject area in scope. Readers would need to understand the particular context and decide on the level of concern for their organisation.
- Breached information is an important tool for adversaries. This information is being utilized in a variety of cyber-attacks with intentions ranging from fraud to targeted attacks based on personal information and is available over underground markets[125]. This leads to a continuous abuse of this information, long after the occurrence of the breach. Hence, making the aftermath of a data breach is an important task for evaluating its impact and reduce long term costs from potential customer regress claims.
- Breached data are subject to monetisation through adversaries[101]. As a consequence, lost or stolen information will be misused over a longer time frame than the time needed to process/manage the incident. Additional costs should be calculated for assaults on businesses as the data is being offered in underground markets[17].

[113] http://www.mirror.co.uk/3am/celebrity-news/celebrity-4chan-shock-naked-picture-4395155, accessed October 2014.
[114] http://www.theguardian.com/technology/2014/feb/25/bitcoin-exchange-mtgox-offline-amid-rumours-of-theft, accessed October 2014.
[115] http://www.ibtimes.co.uk/bitcoin-investment-firm-collapses-due-alleged-hacking-management-disappears-1470779, accessed October 2014.
[116] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/proposal-for-one-security-framework-for-articles-4-and-13a/at_download/fullReport, accessed December 2014.
[117] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058, accessed December 2014.
[118] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, accessed December 2014.
[119] http://www.verizonenterprise.com/DBIR/, accessed October 2014.
[120] http://www.datasurer.com/8-common-reasons-of-data-breach/, accessed November 2014.
[121] http://www.computerworld.com/article/2476642/data-security/financial-firms-not-offering-two-factor-authentication.html, accessed November 2014.
[122] http://www.privacyrisksadvisors.com/news/beazley-announces-findings-from-analysis-of-1-500-data-breaches/, accessed October 2014.
[123] http://www.symantec.com/connect/blogs/symantec-intelligence-report-may-2014, accessed October 2014.
[124] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013/at_download/fullReport, accessed October 2014.
[125] http://www.csoonline.com/article/2691735/malware-cybercrime/what-to-do-in-the-aftermath-of-the-jpmorgan-breach.html, accessed October 2014.

https://t.me/learningnets

- Still relatively large unspecified/unknown number of data breach incidents are hindering cybersecurity specialists and law enforcement in understanding the whereabouts of successful attacks[126]. It will be necessary that additional data breach reporting schemes will enter into force[127].
- The security preparedness of businesses for new technologies are still in early maturity phases. Existing security mechanisms and processes are struggling to adapt to new technological developments such as cloud and mobile, especially with regard to data ownership in off-premises environments. Given the inevitable trend that data breaches will happen in cloud and mobile, the availability and maturity of multilayered security controls should be increased[128].
- A study regarding information loss has indicated that over 50% of data breaches is attributed to "sloppiness" of end-users with regard to security controls/procedures[129].
- Recent US data breach statistics show that most breaches have been reported in the area of medical/healthcare (ca. 42%)[130]. Businesses score second with 32% of reported incidents. Yet, data breaches in businesses have the lion's share as regards the amount of records stolen (ca. 82%). It is interesting to observe the interest of cyber-criminals in medical/health information. This is a strong indication that this sort of information will be premium target, in particular with the proliferation of assisted living and e-health systems within smart environments (see also section 6.6 on internet of things).

Observed current trend for this threat: *increasing*

Related threats: Malware: Worms/Trojans, Identity theft, Information leakage, Phishing, Web application attacks / Injection attacks, Web based attacks, Exploit Kits, Botnets.

Authoritative Resources: "*2014 Verizon Data Breach Investigations Report*"[119].

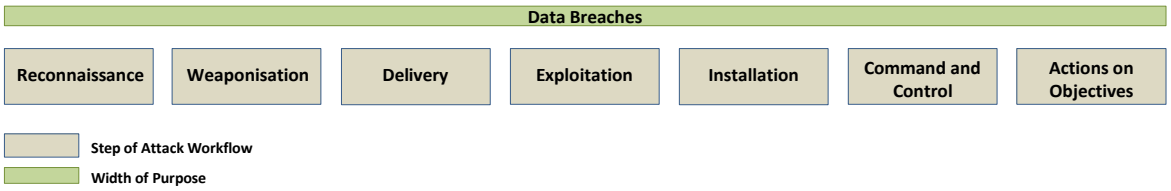


Figure 12: Position of Data Breaches in attack workflow

3.10 Physical damage/theft/loss

Physical damage, theft or loss of devices is an important cause leading to various cyber-security incidents, mainly data breaches and identity theft. Though not being necessarily related to cyber-space, damage, theft or loss of user devices exposes all information stored at the user's end; and this

[126] http://www.lka.niedersachsen.de/download/71603/Bericht_zu_Kernbefunden_der_Studie.pdf, accessed October 2014.
[127] http://www.europarl.europa.eu/document/activities/cont/201405/20140515ATT84137/20140515ATT84137EN.pdf, accessed October 2014.
[128] http://searchcloudsecurity.techtarget.com/news/2240231264/Experts-Expect-cloud-breaches-to-endanger-data-privacy?utm_medium=EM&asrc=EM_NLS_34415200&utm_campaign=20140924_Inevitable%20cloud%20breaches%20threatening%20data%20privacy_mbacon&utm_source=NLS&track=NL-1820&ad=896194, accessed October 2014.
[129] http://capgemini.ft.com/web-review/sloppiness-to-blame-for-more-data-losses-than-hacking-study-claims_a-41-648.html, accessed October 2014.
[130] http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf, accessed November 2014.

https://t.me/learningnets

information is highly relevant for device and application security. In the reporting period, we have seen device theft or loss to be the 3rd most important reason leading to data breaches[131], following hacking (1st position) and accidental exposure (2nd position). By summarizing all available reports[122,123], processed, one can argue that theft/loss is between second and third cause for data breaches. This looks reasonable, if one takes into account that one in seven devices gets lost[132]. Taking into account advances in hardware tampering techniques[133,134], code analysis[135] and bypassing security controls, it is evident that this threat plays an important role for cyber-adversaries, including targeted attacks.

In this reporting period we have assessed that:

- More than 3 million smart phones were stolen in the US last year alone. Taking into account that 34% of device owners do not use any security controls to protect information and that around 50% are using their devices for business purposes[136], this is the best demonstration of the potential efficiency of this threat.
- Inevitably, physical damage and theft is highly likely to happen in areas with social, political or military crises. In the reporting period we have seen few physical damage events with significant impact in crisis areas[137]. In such cases, besides availability issues, additional risks emerge from unencrypted storage devices.
- Physical damage may have non-human causes[138] such as force majeure, extreme weather and physical phenomena. The later has been identified a significant cause of outages in the telecommunications sector[124].
- Assessments indicate that loss of devices and documents is more often reported than theft. Interestingly, most assets have been stolen more frequently from corporate environments than various other locations (homes, cars, transportation, etc.). This might clarify the three most popular vectors reported for theft, namely: disabling existing protection controls, bypassing existing protection controls and privilege abuse[119]. All these vectors are related mainly to corporate locations.
- Statistics on device theft/loss indicate that at the first position are mobile user devices (i.e. smart phones, tablets), followed by laptops, documents, desktop, flash drive and disk drive[119].
- Though not led to device theft or loss, one of the most important consequences of access to physically unprotected assets in the reporting period was the fraud on ATMs[139]. In those cases, physical access to the ATM machines are key to manipulation of ATMs in order to initiate fraudulent activities[140].

[131] http://www.symantec.com/connect/blogs/data-breaches-put-focus-endpoint-security, accessed October 2014.
[132] http://blogs.absolute.com/lojack-for-laptops/2014/07/1-7-experience-device-loss-theft-travelling/, accesses October 2014.
[133] http://www.v3.co.uk/v3-uk/news/2344962/nsa-seen-tampering-with-cisco-kit-to-add-surveillance-tools, accessed October 2014.
[134] http://resources.infosecinstitute.com/hacking-atms-new-wave-malware/, accessed October 2014.
[135] http://securityintelligence.com/how-to-hack-a-mobile-app-its-easier-than-you-think/#.VE9qjqNBuLM, accessed October 2014.
[136] http://blogs.cisco.com/security/securing-mobile-data-in-the-event-of-device-loss-or-theft/, accessed October 2014.
[137] http://resources.infosecinstitute.com/russia-ukraine-information-warfare/, accessed October 2014.
[138] https://www.youtube.com/watch?v=1ehFiErtjW0, accessed October 2014.
[139] http://www.bankinfosecurity.com/atm-fraud-c-245, accessed October 2014.
[140] http://www.bankinfosecurity.com/hacking-atms-no-malware-required-a-7460, accessed November 2014.

https://t.me/learningnets

- Available attacks on mobile phones allow an attacker to exploit data leakage vulnerabilities when app developers place sensitive information or data in a location on the mobile device[50]. An adversary having physical access to the device (through theft or loss) can use existing tools to perform this attack. Hence, protection of mobile devices against theft or loss should be a priority for owners.

Observed current trend for this threat: *increasing*

Related threats: Insider threat, Data breach, Information leakage, Identity fraud/theft.

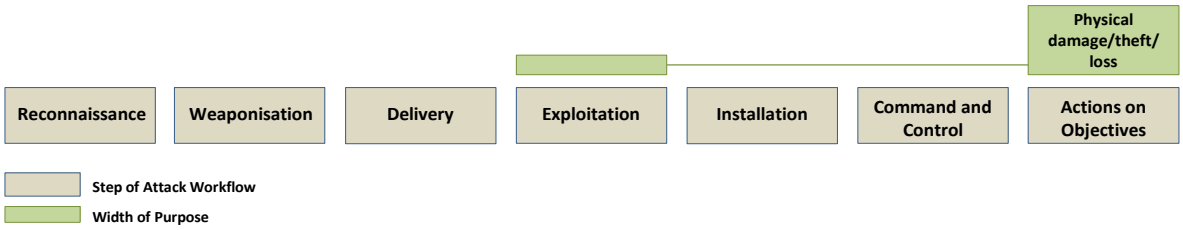


Figure 13: Position of Physical damage/theft/loss in attack workflow

3.11 Insider threat

As an aftermath of the Snowden revelations, in this reporting period a significant effort has been invested in the analysis of the insider threat. Reports on the insider threat have been issued, mainly on the initiative of or commissioned by governmental organisations or organisations enrolled in national security and military defence[141,142,143,144,145]. Although these reports mainly focus on malicious insider user activities, analysis of incidents indicates that a significant amount of insider threats stem from unintentional user errors/mistakes, unintentional displacement of information and loss/theft[124]. Whatever the grounds for insider threat materialisation might be, usually, they lead to significant impact for the organisation. This explains significant CISO concerns assessed: more than half of organisations believe that they are vulnerable to this threat[142]. On the other hand, more than half of security professionals consider insider threats as being difficult to prevent. Admittedly, the insider threat is not mainly a technical issue. Together with the high impact of such attacks, it is evident that this threat is a significant concern, both for technical experts and executives.

In the reporting period we have assessed that:

- The insider threat is being primarily noticed by means of technical controls (e.g. via analytics regarding printer logs, intranet logs, unauthorised access attempts, outbound web traffic to mistrusted sites, etc.). But technology is just one part of the problem. Being a part of the organisation, measures that go beyond technological solutions need to be sought.

[141] http://scadahacker.com/library/Documents/Insider_Threats/DHS%20-%20Risks%20to%20US%20Critical%20Infrastructure%20from%20Insider%20Threat%20-%2023%20Dec%2013.pdf, accessed October 2014.
[142] http://www.vormetric.com/sites/default/files/ap_Vormetric-Insider_Threat_ESG_Research_Brief.pdf, accessed October 2014.
[143] http://www.trustedcs.com/resources/whitepapers/Ponemon-RaytheonPrivilegedUserAbuseResearchReport.pdf, accessed October 2014.
[144] http://www.trustedcs.com/resources/whitepapers/RTN-PrivilegedUserAccessPUMA-RiskMitigationIIS2013-238WP.pdf, accessed October 2014.
[145] http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf, accessed October 2014.

https://t.me/learningnets

Technological solutions need to go hand in hand with HR, awareness and employee guidance processes[145].

- Materialised insider threats need particularly high efforts to contain. While average containment of cyber-attacks is ca. 30 days, insider attacks need on average ca. 60 days[146].
- Insider attacks are often bypassing existing security controls due to access rights but also due to available knowledge of the insider regarding existing protection. In addition, they are aware of weaknesses/vulnerabilities of the organisation that can be misused in order to successfully place an attack. Often, the best way to recognise an insider adversary is to keep an eye on people's behaviour to detect patterns of dissatisfaction[145].
- A considerable amount of insider incidents in organisations is a result of user error[143]. Given the assessed fact that over 50% of data breaches are due to user sloppiness, one can argue that significant damage is caused due to ignorance. Hence, a better remediation of insider threat might be achieved by better user training. Over 48% of organisations participating in a survey on insider threat have not provided any security training to their employees[147]. Among the most frequent user errors are misdelivery, that is, sending information (paper or digital) to wrong recipients[119]. Misdelivery is followed by publishing error, disposal error, misconfiguration and malfunction[119].
- Information types that have been breached by insiders are: intellectual property (63%), customer data (50%), unknown (24%) and financial records (22%)[147]. Top 5 activities of insider misuse assessed are: privilege abuse (88%), non-approved hardware (18%), bribery (16%), e-mail misuse and data mishandling (11%)[119].
- A very thorough risk assessment of the insider threat[141] has impressively demonstrated that no operator of critical systems can afford having the required level of protection to properly mitigate insider threats. This report underlines also the potential for the combination of insider threat with guidance from external threat agents, an issue that is often underestimated by organisations. All in all, this report penetrates the issue of insider threat at a considerable depth.
- It seems that there is a gap between perception and reality about insider threat. Analysis of real incidents shows that insider threats are in second position as cause of all incidents, but are far less than outsider threats which is at the first position[148] (insider threat only 8% of all incidents).

Observed current trend for this threat: *stable/ slight increase*

Related threats: Malicious code, Data Breaches, Information leakage, Identity theft, Physical damage/theft/loss, Phishing, Web-based attacks, Web application attacks / Injection attacks.

Authoritative Recourses: DHS "*National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat*"[141],"*2013 Vormetric/ESG Insider Threats Survey*"[142], "*Privileged User Abuse & The Insider Threat*"[143].

[146] http://www8.hp.com/us/en/hp-news/press-release.html?id=1815969#.VE4cGaNBvZ4, accessed October 2014.
[147] http://www.websense.com/assets/reports/report-ponemon-2014-part2-exposing-cybersecurity-cracks-en.pdf, accessed October 2014.
[148] https://www.riskbasedsecurity.com/reports/2014-MidYearDataBreachQuickView.pdf, accessed October 2014.

https://t.me/learningnets

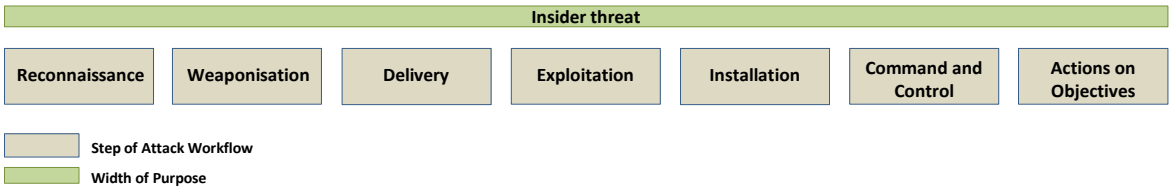


Figure 14: Position of Insider Threat in attack workflow

3.12 Information leakage

Information leakage relates to a set of threats that emerge due to unintentional or maliciously triggered revelation of valuable information (personal data, credentials, security related information, etc.) to an unauthorised party. Such information is then abused as is, or within other threats and attacks. Information leakage is different from data breach, in that it mainly concerns exploitation of technical and organisational weaknesses to obtain information that is then fed to other attacks. Data breach, on the other hand, is the threat of compromising of confidentiality of massively stored business information. In the reporting period we have experienced leakage incidents, one of which – Heartbleed - has been classified by the security community as "*one of the most serious to affect the Internet*"[149,150]. However, some months later, another leakage vulnerability of SSL has been found[151]. Concluding one can say that increased complexity of internet architectures (i.e. web and application services) as well as decentralisation and virtualisation of processing, open doors to information left-overs during processing. This information is targeted by this threat.

In this reporting period we have assessed that:

- Heartbleed was a serious blow to OpenSSL, one of the basic components of secure communication in the internet. Though good guidance was given to remove the vulnerability, delays, update errors and even non-corrections of the used SSL version have been observed. Yet, this incident has demonstrated the complexity in losing trust to a basic security component: certificates need to be re-issued and dependencies of existing software need to be analysed and fixed. It is expected that this incident will continue bothering security experts for some time[150]. A second leakage incident related to SSL is indicative for the continuous attempt to challenge the security of trust functions of the internet[151].
- Among application vulnerabilities (XXS, Information leakage, Session Management, etc.), none has demonstrated an increase similar to information leakage, which has nearly doubled in comparison to 2012. It is assumed that this was due to accidental leakage of sensitive information through data transmission error messages[43]. Others argue that due to increased complexity and low level of awareness for a good error handling, information storage and application architecture issues, information leakage will increase[152]. In the reporting period, information leakage weaknesses have been assessed to be within the top three in application vulnerabilities[45].

[149] http://www.theverge.com/2014/4/8/5594266/how-heartbleed-broke-the-internet, accessed October 2014.
[150] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=WGL03057USEN#loaded, accessed October 2014.
[151] https://community.rapid7.com/community/infosec/blog/2014/10/14/poodle-unleashed-understanding-the-ssl-30-vulnerability, accessed October 2014.
[152] http://www8.hp.com/us/en/hp-news/press-release.html?id=1571359#.VFCVzaNBsnO, accessed October 2014.

https://t.me/learningnets

- Social media remain a major channel for information leakage that can be used in other (e.g. targeted) attacks[153]. Creating awareness with regard to social media/networking applications can be considered as a "work in progress" area[154]. Important personal information can be found in social media such as: copies of driver licenses, ID cards, passports, registration cards, school ID cards or credit cards[155].
- Due to the need to transfer information among servers, mobile applications, cloud servers, etc. it is necessary to introduce/use security controls to avoid data exfiltration for data that are on the move or reside in end-devices that are not properly managed, at least security wise. Such controls need to be positioned at all components interacting by means of application scenarios, both within and outside the organisation[156].
- A relevant study shows that over 50% of tested applications exhibit weaknesses regarding information leakage related to application, its implementation, user data, etc. Moreover, over 30% of applications are prone to information leakage due to poor error handling. This fact opens windows for abuse through information leakage threat[152]. This indicates an increased need for secure application development practices.
- Among the most common leaks found in applications are: information found in comments (e.g. filename), cookie retrieval, internal IP addresses and server versions[152].

Observed current trend for this threat: *increasing*

Related threats: Web application attacks, Data Breach, Phishing, APT / Espionage, Web-based attacks.

Authoritative Recourses: "*IBM X-Force Threat Intelligence Quarterly, 3Q 2014*"[150], HP "*Cyber Risk Report 2013*"[152], White Hat Security "*2014 Website Security Statistics Report*"[45].

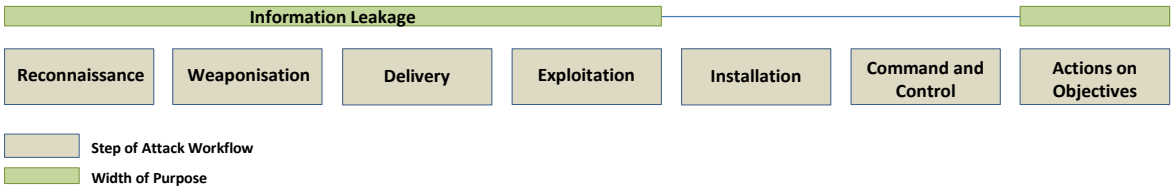


Figure 15: Position of Information Leakage in attack workflow

3.13 Identity theft/fraud

Often characterised as an attack vector, identity theft is a cyber-threat that aims at collecting user identity information including credentials, personal profiling, details of financial identification/authentication methods, credit card information, various access codes, technical identification data, etc. This information is referred to as Personal Identifying Information (PII). As such, identity theft is not overlap free with data breach and information leakage threats (see Annex B in[119]). This threat is considered individually, because PII is a valuable asset that is often targeted in cyber space by means of specific tools and attack vectors. As a matter of fact, PII can be part of a data

[153] http://www.academia.edu/6179116/Social_Information_Leakage_Effects_of_Awareness_and_Peer_Pressure_on_User_Behavior, accessed October 2014.
[154] http://research.itpro.co.uk/content34207, accessed October 2014.
[155] http://www.cert.pl/PDF/Report_CP_2013.pdf, accessed October 2014.
[156] http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-de_lancaster_executive_report.pdf, accessed October 2014.

https://t.me/learningnets

breach, just as PII can be subject of information leakage. Relevant sources on this topic[157,158,159] underline the importance of identity theft and fraud as a consumer issue: following an observed irregularity in financial transactions, credit card information or other identification information, consumers consider their identity being compromised and/or used for fraud. Accordingly, they proceed with notification to corresponding/competent organisations (e.g. Identity Theft Resource Centre in the US[160]). To this extent, identity theft/fraud is an important term for consumers who have experienced a successful attack that has revealed their PII.

In this reporting period we assessed that:

- Increasing numbers of identity theft/fraud[161] incidents have led to consumer mistrust in using digital means for performing financial transactions. Over 50% of consumers have expressed their concerns about reclaiming their identity in case they fall victim of this threat. This is double the number assessed in 2011[157]. This concern is justified, as they constantly hear news and reports about fraud in the areas financial, medical/health, taxation, POS, etc. It is understandable that the trust to the protection offered by their service providers vanishes[157].
- Both emerging, yet security immature innovations but also older pieces of technology in the area of home environments will become targets for identity theft: due to weakly implemented or operated security controls, a variety of PII will flow through a number of interacting components. Potential areas of PII to be exposed is entertainment, gaming, medical and consumer information[94].
- An increased activity in the area of identity theft has been assessed by national authorities. Threat agents have deployed more sophisticated methods, such as keyloggers, virtual kidnapping using ransomware and phishing attacks, to perform identity theft and fraud targeting small medium enterprises but also larger organisations[180].
- The role of interoperable identities increases together with the interoperability of applications in the consumer market[162]. While delivering advancements in application usability and user comfort, interoperable identities may introduce significant risks if one of those identities will be subject to identity theft. Through the interoperability, the adversary may obtain access to a number of other credentials by breaching only one[94].
- Businesses need to be prepared to manage customer reports on identity theft and fraud, as this threat has been assessed to be at the first position of overall customer complains, (increasing by 14% within 2013-2014[158)]. Especially identity fraud in the area of medical care is on the rise: in a survey on medical identity fraud, it has been estimated that ca. 2 million US citizens will spend over $12 billion as consequence of identity fraud[159,55].

[157] http://www.aciworldwide.com/-/media/files/collateral/global-consumers-losing-confidence-in-the-battle-against-fraud-report, accessed October 2014.
[158] http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf, accessed October 2014.
[159] https://www.privacyrights.org/sites/privacyrights.org/files/ID%20Experts%204th%20Annual%20Patient%20Privacy%20&%20Data%20Security%20Report%20FINAL.pdf, accessed October 2014.
[160] http://www.idtheftcenter.org/, accessed October 2014.
[161] http://time.com/2953428/data-breaches-identity-theft/, accessed October 2014.
[162] http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050742.hcsp?dDocName=bok1_050742, accessed October 2014.

https://t.me/learningnets

- Top types of PII breached between October 2013 and September 2014 are: real names, government ID numbers and home addresses[163]. Reports on identity fraud referring to US territory assess the following information targeted: government documents (34%), credit cards (17%), phone or utilities fraud (14%) and bank fraud (8%)[158].

Observed current trend for this threat: *increasing*

Related threats: Data Breach, Information leakage, Phishing, Web application attacks / Injection attacks, Web based attacks, Malware.

Authoritative Recourses: "*Consumer Sentinel Network Data Book*"[158], Ponemon "*Fourth Annual Benchmark Study on Patient Privacy & Data Security*"[159], Aite "*Global Consumers: Losing Confidence in the Battle Against Fraud*"[157].

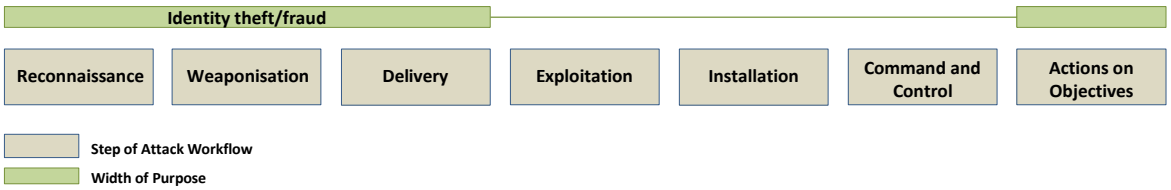


Figure 16: Position of Identity Theft/Fraud in attack workflow

3.14 Cyber espionage

This threat has been introduced in the top threats due to the significant amount of incidents attributed to nation states and corporations (see also section 4.2 on Threat Agents).With this cyber threat we would like to refer mainly to APT (Advanced Persistent Threat) and to Targeted Attacks, knowing that the later kind of attacks is not only deployed within espionage campaigns[164]. Moreover, from assessed material it becomes clear that APT is nothing more than a targeted attack that is being initiated by a threat agent with very high capabilities and resources. It is also clear, that cyber espionage consists of a combination of threats mentioned in this chapter. Hence, just as other threats in the present chapter, the cyber espionage threat is not overlap-free with other threats mentioned. To this extent, this threat refers rather to certain tools and tactics that match the profile of espionage threat agents: cyber espionage is rather a tactical approach than technical[165]. As it is the case with some reports found, cyber espionage is worth classifying according to campaigns encountered[165]. Whatever the classification of this threat might be, it assumes a high level capability and corresponding motivation. Moreover, this kind of attack and especially the reconnaissance phases may persist over a very long time period, while attribution is very difficult, especially in case of state sponsored espionage. In the reporting period we have seen cyber espionage on the rise: reports about incidents state a growth that is close to 3% compared to last year[166].

In this reporting period we have assessed that:

[163] http://www.symantec.com/connect/blogs/symantec-intelligence-report-september-2014, accessed October 2014.

[164] Due to the terminology diffusion regarding what is a threat and what is an attack vector, in ETL 2014 we have introduced an extra chapter on the topic of attack vectors to further analyse this matter (see Chapter 5 "*Attack Vectors*").

[165] http://about-threats.trendmicro.com/resources/threat-intelligence/targeted-attack-trends/rpt-targeted-attack-trends-2h-2013.pdf, accessed October 2014.

[166] http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf, accessed October 2014.

https://t.me/learningnets

- Quite some targeted attack campaigns have demonstrated an increase in focus, sophistication and persistence[55]. We have seen attacks more narrowly tailored, addressing a reduced number of recipients and organisations but increasing significantly in frequency. Spear phishing and Strategic Web Compromise[167] (SWC, aka Watering Hole) are important tools used for initial phases of the attack (i.e. reconnaissance, weaponisation and delivery). Spyware Trojans, Bootkits[40] and remote access trojans[168] (RAT) are often used malware in the phases exploitation and persistence[55,169].
- Statistics show important trends observed in the reporting period[55]: there is an increase of industry sectors targeted (11%) (i.e. wider campaigns). While the number of recipients targeted has decreased (62%) (i.e. more targeted campaigns). Average duration of targeted attacks increased (105%) (i.e. more persistent campaigns); and number of detected campaigns increased significantly (472%).
- The observed cascade of sophistication, complexity and capability levels start with advanced persistent threat, go over to targeted attacks and end at cyber-criminals. With the advancement of attacks, technology used today within APT and targeted attacks, will be adopted over time by cyber-criminals[167,169,170].
- New attack methods that can be used in targeted and advanced persistent threat attacks emerge in the area of research[171]. It can be assumed that advancements in new methods will arise in the military and national security sectors[172].
- The volume of attacks by industry sector shows that the most popular targets of targeted attacks are: governments (80%), computer/IT (4%), followed by Aerospace, Industrial, Electrical, Telecommunications and Military (3% each)[55,169]. This fact clearly manifests the areas of interest and motives behind cyber-espionage, being collection of intelligence regarding political, strategic, technological and industrial developments.
- Primarily within APTs but also targeted attacks, involved adversaries have demonstrated the ability to evade existing controls, at least automated ones[145]. It is therefore advisable to consider strengthening defences at the level of human-based controls, such as trainings regarding phishing and spam and awareness raising measures in general.

Observed current trend for this threat: *increasing*

Related threats: Phishing, Web based attacks, Malware, Exploit Kits, Information leakage, Web application attacks, Data breaches, Botnet, Spam, Physical Damage/Theft/Loss, Insider threat.

Authoritative Resources: Trend Micro "*Targeted Attack Trends 2H 2013 Report*"[169], Symantec "*2014 Internet Security Threat Report, Volume 19*"[55].

[167] http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf, accessed October 2014.
[168] http://news.softpedia.com/news/Advanced-Android-Remote-Access-Trojan-Aimed-at-Hong-Kong-Protesters-460684.shtml, accessed November 2014.
[169] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf, accessed October 2014.
[170] https://www.virusbtn.com/files/StewartCross-VB2013.pdf, accessed November 2014.
[171] https://www.dropbox.com/s/607xa16yz6yjpsa/Air-Hopper-MALWARE-final-e.pdf, accessed October 2014.
[172] http://www.net-security.org/secworld.php?id=17544, accessed October 2014.

https://t.me/learningnets

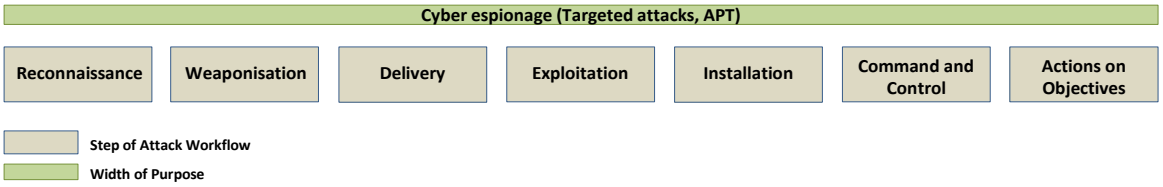


Figure 17: Position cyber espionage in attack workflow

3.15 Ransomware/Rogueware/Scareware

Although ransomware belongs to the family of malware threats, it has been considered as an individual threat due to its assessed dynamics. In the reporting period we have seen ransomware gaining importance as a malicious tool. Though some reduction of this threat has been expected after law enforcement success of last year (Police Virus[173], Zeus-Botnet[174]), a significant revival of this threat has been assessed, in particular for mobile devices. Equally significant is the fact that ransom shows growth potential due to updates performed in corresponding malicious tools, especially regarding distribution, encryption and used payment methods. It seems that ransomware has gone through improvements adopted from malware[17]. Moreover, it seems reasonable to speculate on the potential entrance of a ransomware development kit in the cyber-crime market [175,36]. Although ransom decreased in the reporting period, the inclusion of mobile devices and the new features mentioned above, create the impression that this threat will be increased in the future.

In this reporting period we have assessed that:

- Advancements in functionality of ransomware have shown up after the announcement of a Trojan encryption tool for sale in underground market for Android. Right after this announcement, the first mobile malware embracing this functionality was detected. By the end of second quarter of 2014, some 47 versions on the Trojan have been detected[40]. All ransom attempts have used social engineering techniques to exert pressure on the victims[40].
- For the communication with the C&C server, one version of the Trojan has used the TOR network. Although the use of the anonymity network is seen as an advancement, researchers argue that this increases detectability both of the malware and the underlying botnet[176]. It remains to be observed how TOR functionality usage within malware will evolve over the time.
- It is interesting to observe how protective functions of mobile devices have been misused to block phones and require a ransom: by attacking the Apple ID on iOS devices, adversaries managed to completely block the device and as money to unlock the device[177].
- Thee ransomware threat can create damage, especially to businesses, while it is highly profitable for cyber-criminals. As opposed to the past, available anonymous payment schemes such as MoneyPack and QIWI VISA Wallet, facilitate cash flow to the cyber-criminals. The

[173] http://pandalabs.pandasecurity.com/operation-ransom-police-virus-authors-arrested/ , accessed October 2014.
[174] http://www.techradar.com/news/internet/web/microsoft-and-fbi-team-up-to-take-down-gameover-zeus-botnet-1251609, accessed October 2014.
[175] http://arstechnica.com/security/2014/01/researchers-warn-of-new-meaner-ransomware-with-unbreakable-crypto/, accessed October 2014.
[176] http://www.ccdcoe.org/cycon/2014/proceedings/d3r2s3_casenove.pdf, accessed October 2014.
[177] http://blog.kaspersky.com/ransomware_targets_ios_osx/, accessed October 2014.

https://t.me/learningnets

encryption used is impossible to break (RSA 2048 encryption used within Cryptolocker[178] and its evolution Ransomcrypt[179]). Research has shown that ca 3% of victims pay a ransom[180].

- In the reporting period Fake Antivirus has bothered security experts, in particular in the mobile area. It is remarkable that a fake antivirus named "Virus Shield" has been downloaded over 10.000 times, thus getting into the top paid list in the first week of appearance[17].

Observed current trend for this threat: *decreasing*

Related threats: Malware, Phishing, Exploit Kits, Botnets.

Authoritative Resources: "*Kaspersky IT THREAT EVOLUTION Q2 2014*"[40], Symantec "*LATIN AMERICAN + CARIBBEAN CYBER SECURITY TRENDS*"[180].

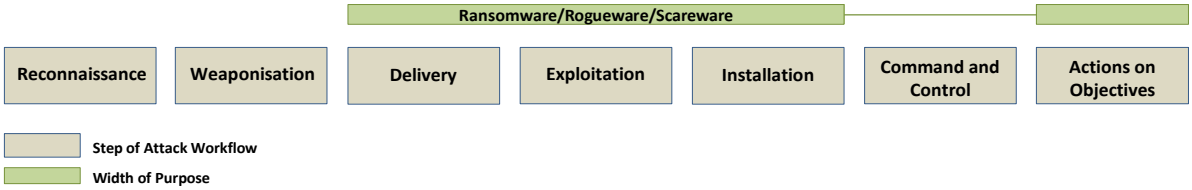


Figure 18: Position of Ransomware/Rogueware /Scareware in attack workflow

[178] http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report_2013.pdf, accessed October 2014.
[179] http://www.f-secure.com/v-descs/trojan_w32_ransomcrypt.shtml, accessed October 2014.
[180] http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf, accessed October 2014.

https://t.me/learningnets

3.16 Visualising changes in the current threat landscape

In comparison to the ETL 2013 there have been interesting changes in the current threat landscape. To facilitate comparability with the results of 2013, the figure below shows the changes in the threat landscape for 2014. The figure shows changes regarding both the trends and the ranking of assessed cyber threats.

Top Threats 2013	Assessed Trends 2013	Top Threats 2014	Assessed Trends 2014	Change in ranking
1. Drive-by downloads (renamed to Web-based attacks)	↑	1. Malicious code: Worms/Trojans	↑	↑
2. Worms/Trojans	↑	2. Web-based attacks	↑	↓
3. Code Injection	↑	3. Web application /Injection attacks	↑	→
4. Exploit Kits	↑	4. Botnets	↓	↑
5. Botnets	→	5. Denial of service	↑	↑
6. Physical Damage/Theft/Loss	↑	6. Spam	↓	↑
7. Identify Theft/Fraud	↑	7. Phishing	↑	↑
8. Denial of Service	↑	8. Exploit kits	↓	↓
9. Phishing	↑	9. Data breaches	↑	↑
10. Spam	→	10. Physical damage/theft /loss	↑	↓
11. Rogueware/Ransomware / Scareware	↑	11. Insider threat	→	(NA. new threat)
12. Data Breaches	↑	12. Information leakage	↑	↑
13. Information Leakage	↑	13. Identity theft/fraud	↑	↓
14. Targeted Attacks (renamed to Cyber espionage, merged with Watering Hole)	↑	14. Cyber espionage	↑	→
15. Watering Hole (threat consolidated with other threats/attack vector)	↑	15. Ransomware/Rogueware/ Scareware	↓	↓

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

Table 2: Overview and comparison of Current Threat Landscapes 2014 and 2013

https://t.me/learningnets

ETL 2014: Threat Agents

https://t.me/learningnets

4 Threat Agents

4.1 Cyber-opportunity makes the thief

Opportunity has been long ago recognised as a basic element of practical crime theory[181]. These approaches build on the old saying "opportunity makes the thief." In cyber-crime the situation is not much different. In the reporting period we have seen cyber threat agents looking for opportunities to better target their attacks and more easily fool their victims. The examples are self-speaking: international sport events, specially crafted phishing attacks based on personal profiles/habits, targeted campaigns to find weak links, etc.

Considering the opportunity factor in cyber-crime might be an important tool for defenders in order to understand motivation and techniques that are likely to be used. By taking into account the issue of opportunities in cyber-crime, it can be concluded that:

- *Cyber-crime opportunities often have location and time relevance*: It is typical that, as ordinary criminals, cyber criminals seek to abuse collective mind-sets that are formed within big events[182,183,184]. Moreover, events with international political impact are main triggers for cyber-crime, especially hacktivism, cyber-fighters and state sponsored espionage[185,186,187,188].
- *Cyber-crime tries to increase opportunity specificity*: cyber-crime seeks for specific opportunities that increase success rates. In the reporting period we have experienced a shift towards more targeted attacks to sets of opportunities that are concentrated to exploiting specific weaknesses. Hence, instead of looking for victims in the wild, cyber attackers concentrate their attacks on set of users, e.g. by abusing breached information[189].
- *Cyber-crime produces opportunities for cyber-crime*: The emergence of underground markets for hacking tools and hacked information (i.e. cyber-crime as a service) shows clearly that cyber-crime leads to cyber-crime. Cyber-crime underground forums, cyber-crime market places and offerings are a clear indication hereto[190].
- *Social and technological changes create cyber-crime opportunities*: Building the basis of cyber-crime for years now, social and technical changes are THE opportunity abused, especially in phases

[181] http://skywallnet.com/data_server/CA/OMT_PP_CP.pdf, accessed October 2014.
[182] http://gadgets.ndtv.com/internet/news/anonymous-threatens-cyber-attack-on-fifa-world-cup-sponsors-533657, accessed October 2014.
[183] http://www.ibtimes.co.uk/sochi-olympics-2014-cyber-threats-mean-there-no-privacy-winter-olympics-1435387#channel=f32fe627f65f00c&origin=http%3A%2F%2Fwww.ibtimes.co.uk, accessed October 2014.
[184] http://www.eweek.com/security/world-cup-spurs-cyber-attacks-digital-protests.html, accessed October 2014.
[185] http://au.ibtimes.com/articles/565988/20140911/isis-islamic-state-al-qaeda-caliphate.htm#.VDZLpqP6jZ4, accessed October 2014.
[186] http://learningenglish.voanews.com/content/hong-kong-protesters-fight-cyber-attacks/2477307.html, accessed October 2014.
[187] http://www.computerweekly.com/news/2240223145/Syrian-hacktivists-find-new-way-to-target-Reuters?asrc=EM_ERU_30745331&utm_medium=EM&utm_source=ERU&utm_campaign=20140624_ERU%20Transmission%20for%2006/24/2014%20(UserUniverse:%20919769)_myka-reports@techtarget.com&src=5262223, accessed October 2014.
[188] http://securityaffairs.co/wordpress/18294/security/fireeye-nation-state-driven-cyber-attacks.html, accessed October 2014.
[189] http://www.computerweekly.com/news/2240232029/JP-Morgan-breach-affects-7-million-small-businesses?asrc=EM_MDN_34980641&utm_medium=EM&utm_source=MDN&utm_campaign=20141008_MasterCard%20launches%20cyber%20hacking%20protection%20software_, accessed October 2014.
[190] http://securityintelligence.com/underground-cybercrime-exploits-for-sale/#.VDY-ZqP6jZ4, accessed October 2014.

https://t.me/learningnets

of growth, mass deployment/marketing and end of support. Knowing that, introduction of social and technical changes should be "secure by design". In the reporting period we have seen some EU-Member States introducing security in early stages of technology adoption[191,192] in order to effectively reduce the window of this opportunity.

Yet not always feasible and obvious, with some awareness, these opportunities could be recognised by defenders, thus contributing to situational prevention. In cyber-space this might mean adapting defences, level of preparedness and expectations.

Looking at ways to better understand the methods used for opportunity emergence and opportunity exploitation, might lead to a better cyber-defence. It is considered appropriate to more systematically analyse this field and capitalized on existing experience from the area of criminology[193].

4.2 Overview of Threat Agents

In the reporting period, we have seen evidence for the existence of almost all of threat agents described in previous ETLs[194]. Hence, the same group of threat agents will be maintained, by introducing a ranking according to attribution statistics found.

Generally speaking, some trends in the way threat agents place their attacks have been identified in the reporting period: the most active threat agents seem to perform more targeted attacks. Speaking in terms of opportunities, cyber threat agents are more effective in finding means for identification of windows of opportunities. This is a new trend: cyber-criminals can better target their attacks and be more successful in exploitation of vulnerabilities, while using more effectively malicious tools and attack methods.

One reason assumed for this trend is advancements in capabilities of finding vulnerabilities (technical/human). Breached/leaked information is considered as main tool to achieve this goal. Secondly, advancements in attack techniques allow certain types of attacks to "fly under the radar" by leaving no traces behind[195,196]. Finally, new attack practices combined with reconnaissance attacks on web applications (e.g. smokescreening[197]) increase their efficiency, while reducing detections. These tactics have led to the changes of threat landscape assessed within the ETL 2014.

[191] https://blog.cyberwar.nl/2014/07/cyber-security-assessment-netherlands-4/, accessed October 2014.
[192] https://www.cyberstreetwise.com/cyberessentials/#downloads, accessed October 2014.
[193] http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf, accessed October 2014.
[194] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport, accessed October 2014.
[195] http://www.pcworld.com/article/2601140/hackers-make-driveby-download-attacks-stealthier-with-fileless-infections.html, accessed October 2014.
[196] http://rt.com/news/175912-critroni-ransomware-tor-network/, accessed October 2014.
[197] http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf, accessed October 2014.

https://t.me/learningnets

In this chapter we provide an overview of the threat agents. In 2014, few elaborated descriptions were found on this topic[198,199,200,201,202,203,204]. However, no significant changes in the typology of Threat Agents could be observed. All in all, data collected in 2014 provides some additional information, yet not much differing from previous reporting periods.

However, it should be mentioned that this observation regards publicly available information. There are reports that law enforcement agencies work on profiling cyber criminals[205]. Yet this information is kept confidential and as such not accessible for this report.

In order to better understand Threat Agents, advancements in attribution are necessary. Attribution of incidents to various groups is difficult and laborious. In most cases attribution can be performed with the cooperation of various players triggered through law enforcement. Attribution of incidents to threat agents is an area that has significant development potential.

Moreover, observation of relevant underground market and its dynamics helps in understanding important dependencies among various Threat Agents as well as their product and technology level. It is worth mentioning that in the reporting period significant insights into the relevant market for cyber-crime tools and stolen data has been found (Authoritative Resource: *Report of Rand National Security Research Division "Markets for Cybercrime Tools and Stolen Data"*[206]).

The above developments aim at the validation of Threat Agent description and provide additional details regarding motives and capabilities. While the threat agents from ETL 2013 still remain relevant, the details assessed this year provide the basis for a ranking based on statistical information from incidents (mainly reported incidents[207] and data breaches[208]). The top five attributions of incidents refer to the target groups: Cybercriminals, Hacktivists and Cyber Espionage, Insider Threat and Cyber War. Accordingly, major threat agents identified are as follows (prioritised):

Cybercriminals: This threat agent group is the most widely known as its objective is to obtain profit from illegal/criminal activities in cyberspace. In the reporting period, most of the observed incidents have been attributed to this group. The main motivations behind their activities are intelligence and monetisation. One main characteristic is the availability of large time and money budgets, while being technically highly skilled and very well equipped. Often they use high-performance computing resources and might be part of highly organised groups (i.e. organised crime in Far East and Eastern Europe). Given existing crime opportunities and profitability of cybercrime, it is expected that organised crime groups will increasingly engage in this field.

---

198 https://www.nccgroup.com/media/481272/2014-04-09_-_security_of_things_-_an_implementers_guide_to_cyber_security_for_internet_of_things_devices_and_beyond-2.pdf, accessed October 2014.

199 http://researchcenter.paloaltonetworks.com/2014/05/how-well-do-you-understand-your-cyber-adversary-part-1/, accessed October 2014.

200 http://researchcenter.paloaltonetworks.com/2014/05/well-understand-cyber-adversary-part-3/, accessed October 2014.

201 http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf, accessed October 2014.

202 http://technical.cloud-journals.com/index.php/IJACSIT/article/download/Tech-136/pdf, accessed October 2014.

203 http://www.darkreading.com/perimeter/infographic-the-many-faces-of-todays-hackers/a/d-id/1317039?_mc=RSS_DR_EDT, accessed November 2014.

204 http://www.informationweek.com/security/attacks-and-breaches/9-notorious-hackers-of-2013/d/d-id/1113140, accessed November 2014.

205 http://triblive.com/news/editorspicks/6449644-74/hackers-bukh-criminals#axzz3FjI4gCyZ, accessed October 2014.

206 http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf, accessed October 2014.

207 http://hackmageddon.com/, accessed October 2014.

208 http://www.symantec.com/connect/blogs/symantec-intelligence-report-may-2014, accessed October 2014.

https://t.me/learningnets

Cybercriminals are typically involved in fraud regarding all kinds of sectors engaged in cyber-space: e-finance, e-commerce, e-payment, ransomware, cybercrime-as-a-service[209], delivery and development of malicious tools and infrastructures. Taking into account aspects of the cybercrime market, one can discriminate among some specialized roles (often building hierarchical structures)[193,206]. Such roles are administrators, specialized experts in various areas of cybercrime, intermediaries, brokers and vendors. In the figure provided in this section, roles at the "productive" end of the cybercrime are depicted by means of providers/developers/operators.

The cybercriminal market allows its suppliers/customers to obtain the means needed for their hostile activities, such as knowledge, tools and breached data. By taking as given that this group possesses significant monetary resources, it should be considered as being in the position to occupy additional workforce in order to enhance capabilities[210]. Finally the utilisation of anonymisation, encryption and virtual currencies, allows cyber criminals to move in a "dark market", hence impeding detection and attribution efforts.

Online Social Hackers: given the important role of phishing and stalking in targeting cyber-attacks, this group is considered as part of criminal activities in cyber space[211,212]. Therefore this threat agent group plays a key role when deploying cyber threats. Online social hackers are skilled with social engineering knowledge, are in the position to analyse and understand behaviour and psychology of social targets, thus evading privacy of potential victims. Main tools used are analysis of social engineering information, profiling of user (e.g. by using loggers, social media accounts, breached data). Even when not using high-tech methodologies and tools, activities of this threat agent group may cause significant privacy impact especially in areas of identity theft, collection of confidential personal data, user credentials, cyber bullying, etc.[213,214]. The capabilities of this group can be characterised as low to medium as regards the use of technology. However their social engineering skills are high. With increasing use of social networking, it is expected that the importance of this group in cyber-attacks will play a significant role, as phishing is becoming an important tool for placing cyber-attacks.

Hacktivists: Hacktivists is a threat agent group that has enjoyed great media attention, as they are politically motivated activists. Their motivation emerges mainly from political ideology, they proclaim social justice and sincerity and aim at propaganda and influence in political decision making. According to their motive and ideological direction, they can dynamically form groups/subgroups, usually lacking a central organisation structure. Typical reasons for their mobilisation are political decisions, political/social crises and assumed injustice and unfairness towards social groups. Their reactions are triggered during riots, international sport events and other major events with international attention. In the reporting period we have seen quite few engagements of this target agent group in

[209] http://www.computerweekly.com/news/2240231663/Service-model-driving-cyber-crime-says-Europol-report, accessed October 2014.
[210] http://www.smh.com.au/technology/technology-news/silk-road-mastermind-ross-william-ulbricht-tripped-up-by-careless-online-mistake-20131003-2utky.html, accessed October 2014.
[211] http://www.reuters.com/article/2014/10/03/jpmorgan-cybersecurity-idUSL2N0RY1CC20141003, accessed October 2014.
[212] https://www.europol.europa.eu/sites/default/files/publications/iocta2014_summary_findings_and_recommendations.pdf, accessed October 2014.
[213] http://www.pandasecurity.com/mediacenter/social-media/people-hack-social-media-accounts/, accessed October 2014.
[214] http://hackerspace.lifehacker.com/social-hacking-for-introverts-1554859929, accessed October 2014.

https://t.me/learningnets

corresponding occasions[215,216,217,218]. The main malicious activities of this group include: DDoS attacks, leakage, defacement, hacking[219].

Due to the dynamics behind this group, it is difficult to give it a sharp profile: in some cases, threat agents of other groups – e.g. script kiddies - join hacktivists activities in order to co-protest or to serve other purposes (e.g. express their sympathy, perform knowledge transfer, provide tools, etc.). Due to these dynamics, alleged hacktivist activities might be a façade used by groups with different motives[220].

Targets are selected in such a way, that media attention to successful cyber-attacks creates high visibility (e.g. government sites, big companies, media, public and private infrastructure components, etc.). Typical actions of successful attacks include publishing of breached data and video messages to maximize public attention. Defence costs against threats of hacktivists are considered as moderate. In the reporting period it has been reported for first time that security agencies have performed counter-attacks to defend hacktivist activities[221].

Nation States: The Snowden revelations in 2013-2014 have shed a new light in hostile activities that emerge as part of national security and intelligence/counter-intelligence regimes of nation states. The true dimension behind the potential of this threat agent group is a main ongoing focus of media since then (here few indicative references due to the large amount[222]). In the reporting period the state-sponsored espionage threat has created concerns to media[223], security experts[224,225,226] and industry alike, while has ranked at third position in attribution of cyber-incidents.

In the meantime, various nation states have developed cyber-intelligence capabilities[227]. Due to non-transparent policies and regimes, it can be assumed that all countries with such capabilities could potentially be involved in cyber-attacks, with a significant part being in the area of intelligence/counter-intelligence. Even within allies, no clear no-spy policies exist[228]. Taking into account resources and budget availability, hostile cyber-activities of nation states are a severe threat that can cause high defence costs, while creating severe impact both at governmental and corporate levels. Main targets of this threat agent group are state secrets, military secrets, data on intelligence, as well as threatening the availability of critical infrastructures. The degree to which performed attacks

[215] http://www.efinancialnews.com/story/2012-07-02/hacktivists-target-russian-banks-over-sochi-olympics?ea9c8a2de0ee111045601ab04d673622, accessed October 2014.
[216] http://motherboard.vice.com/read/anonymous-strikes-world-cup-sponsors-and-brazil-government, accessed October 2014.
[217] http://www.dawn.com/news/1130703, accessed October 2014.
[218] http://news2share.com/start/2014/10/01/anonymous-declares-war-against-hong-kong/, accessed October 2014.
[219] http://pastebin.com/4Bwr8jwL, accessed October 2014.
[220] http://www.dailymail.co.uk/news/article-2582071/Several-NATO-websites-hacked-cyber-attack-linked-crisis-Crimea.html, accessed October 2014.
[221] https://edri.org/hacktivists-targeted-british-spies/, accessed October 2014.
[222] http://www.spiegel.de/suche/index.html?suchbegriff=Spionage, accessed October 2014.
[223] http://www.matthewaid.com/post/98627215806/state-sponsored-spyware-systems-and-the-growing, accessed October 2014.
[224] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf, accessed October 2014.
[225] http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf, accessed October 2014.
[226] http://usa.kaspersky.com/about-us/press-center/press-blog/kaspersky-lab-research-energetic-bear, accessed October 2014.
[227] http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf, accessed October 2014.
[228] http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html, accessed October 2014.

https://t.me/learningnets

are successful can be considered as rather high. As it is the case with espionage in general, nation state activities aim at the creation of intelligence, strategic, psychological and political advantages[229].

Corporations: The growth of activities in corporate espionage follows the trends in state-sponsored cyber-espionage: it grows by targeting corporate information[230,231,232]. The aim is to collect business intelligence, stealing competitive information (e.g. research results, analyses, innovation ideas, planned procurements etc.), breach intellectual property rights (IPR), or even cause damage/sabotage to competitors. Being significantly budgeted and having sufficient knowledge, potential attacks from this threat agent group could cause high costs[233]. Generally speaking, corporations may be involved in reconnaissance activities, intrusion and data breach. Being in close cooperation with state, industrial espionage may use existing state cyber-resources to achieve their objectives [234] . Moreover, corporations may engage salaried threat agents from other groups to achieve their objectives.

Employees (current, ex, internal and external): motivated by extortion, revenge, sabotage or profit, this group has a significant role in the materialisation of cyber threats, especially those that lead to data breaches[235]. Referred to as Insider Threat, this threat group embraces both own and contracted employees, i.e. staff, contractors, operational staff, former employees, etc. Threats emanating from this target group may be both intentional and unintentional (i.e. i.e. lax handling of security procedures, user error or even malicious intent). ENISA incident reporting, for example, has shown that in the telecommunication sector Human Error and Third Party Failure are within the top 5 causes for large outages[236]. The effort required to protect assets against such threats can be quite high[237]. Therefore it is important to identify employee unhappiness, spot knowledge-gaps and get alerted when attacks abuse publicly unknown vulnerabilities[202].

Cyber Fighters: Cyber fighters are groups of nationally motivated citizens who possess significant striking power. Their attacks are politically motivated and, in a similar manner to hacktivists, are concentrating mainly to sabotage, by often publishing of breached data and video messages to maximize public attention. Such groups might have strong feelings when their political, national or religious values seem to be threatened by another group and are capable of launching cyber-attacks. To certain extent, such groups may be supporters of totalitarian regimes and, rightly or wrongly, act on behalf of their supporting parties (i.e. governments) by contributing to national activities in the cyber-space[238,239].

[229] http://en.wikipedia.org/wiki/Cyber_spying, accessed October 2014.
[230] http://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/, accessed October 2014.
[231] http://www.vice.com/en_uk/read/corporate-espionage-gavin-haynes-284, accessed October 2014.
[232] http://www.dw.de/german-businesses-face-rising-threat-of-industrial-espionage/a-17798275, accessed October 2014.
[233] http://cybertinel.com/wp-content/uploads/2014/09/HARKONNEN-OPERATION-CYBER-ESPIONAGE1.pdf, accessed October 2014.
[234] http://www.reuters.com/article/2014/01/26/us-security-snowden-germany-idUSBREA0P0DE20140126, accessed October 2014.
[235] http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf, accessed October 2014.
[236] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013/at_download/fullReport, accessed October 2014.
[237] http://www.vormetric.com/resources/Infographics/the-2014-vormetric-insider-threat-report-european-edition, accessed October 2014.
[238] http://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background, accessed October 2014.
[239] http://cybershafarat.com/2014/10/13/post-9-abu-bahgat-hatem-deeb-syrian-electronic-army-leadership/, accessed October 2014.

https://t.me/learningnets

In the reporting period we have seen more systematic and well organised activities from this threat agent group[240,241,242,243]. Activities of this target group from this year are characterized by increased maturity and sophistication of attack methods used.

Cyber Terrorists: cyber terrorism continued to be controversially discussed in the reporting period[244]. In this time, more extensive descriptions of this threat agent group could be found[245]. Supposedly, cyber terrorists are targeting large-scale sabotage to harm national security and society, mainly aiming at critical infrastructure. Characteristic of this threat agent group is the indiscriminate use of violence in order to influence decisions/actions of states towards their politically or relationally motivated objectives. As a matter of fact, no publicly known incident has been attributed to this target group in the reporting period. Nevertheless, national cyber-security strategies rate cyber-terrorism risks quite high and have developed numerous defences for protection[246]. At the same time it has been recognised that risks from cyber-crime and not cyber-terrorism is the major threat for western countries[247]. In the reporting period we have seen some evidence that terrorists may use technology as means for improving their communication while avoiding state surveillance. Yet, according to the definition of this threat agent group this is not a hostile activity. However, such an engagement may lead to increasing knowledge of related tools that can be then used to launch attacks[248,249]. In this reporting period a report was found that gives an interesting overview of potential misuse of the Internet by terrorists. It provides a detailed list of use-cases, potential actions and tools[250].

Script Kiddies: This target group consists of young individuals who might be thrilled about achievements and skills of tech savvy individuals who assumedly gave a lesson to persons, organisations or brands considered outrageous. Although they are not be present in incident statistics in the reporting period, script kiddies are still considered as threat agents. The rationale behind this is, that due to the ease of obtaining malicious tools, tech savvy teenagers will purchase and use them[251]. Consequently, due to potentially low level of knowledge about the use of hacking tools, low threshold of self-control, overestimation of own skills and the consequences of their activities, script kiddies may achieve great impact. Although it is not expected that significant incidents will be attributed to this threat agent group, it is considered within the ETL 2014for the sake of completeness.

As a short ***reflection to forthcoming developments of the threat landscape***, it is recognised that emerging technologies might create the grounds for malicious activities targeting smaller user communities. This might lead to creation of new threat agent groups, even if the reach of their activity

[240] http://www.bankinfosecurity.com/ddos-attackers-announce-phase-4-a-5929/op-1, accessed October 2014.
[241] http://www.bloomberg.com/news/2014-03-24/three-things-you-should-know-about-the-syrian-electronic-army.html, accessed October 2014.
[242] http://sea.sy/index/en, accessed October 2014.
[243] http://www.securityweek.com/tunisian-hackers-target-governments-banks-theweekofhorror-cyber-attacks, accessed October 2014.
[244] http://www.internetjournalofcriminology.com/awan_debating_the_term_cyber-terrorism_ijc_jan_2014.pdf, accessed October 2014.
[245] http://resources.infosecinstitute.com/explaining-cyberterrorism/, accessed October 2014.
[246] http://www.washingtonpost.com/world/national-security/nsa-director-calls-for-stronger-deterrent-strategy-to-oppose-cyberattacks/2014/02/27/aabd3d92-9fd4-11e3-a050-dc3322a94fa7_story.html, accessed October 2014.
[247] http://threatpost.com/cyberespionage-not-cyber-terror-is-the-major-threat-former-nsa-director-says/105223, accessed October 2014.
[248] http://www.dailymail.co.uk/news/article-2751896/Islamic-State-jihadists-planning-encryption-protected-cyber-caliphate-carry-hacking-attacks-West.html, accessed October 2014.
[249] http://www.usnews.com/news/articles/2014/09/16/nsa-director-michael-rogers-talks-islamic-state-cybersecurity, accessed October 2014.
[250] http://www.computerweekly.com/ehandbook/Terrorist-use-of-the-internet, accessed October 2014.
[251] http://www.itnews.com.au/BlogEntry/396629,being-a-script-kiddie-easier-than-ever.aspx, accessed October 2014.

https://t.me/learningnets

is limited. In the area of Smart Homes, for example, activities of harassment, abuse, sabotage, bullying, etc. could be initiated from individuals as result of neighbourhood disputes, landlords and tenants, etc. Just as in the case of bullying, this kind of malicious activity may cost human lives and should not be left out of scope.

As no significant changes in threat agent profiles have been observed in the reporting period, we reuse the threat agent taxonomy of ETL 2013 in order to provide an overview (see Figure 19). It should be noted, that the threat agents mentioned in this chapter are depicted in the figure through the right hand branch, annotated as *Hostile Cyber Agent*, whereas the left hand branch of it stays for other agents who serve friendly tasks in cyber space.

Besides serving as an overview, this figure may be used in order to follow/comprehend eventual interactions among the different groups, such as possible "camp changes", concurrent roles or other interactions among them[252].

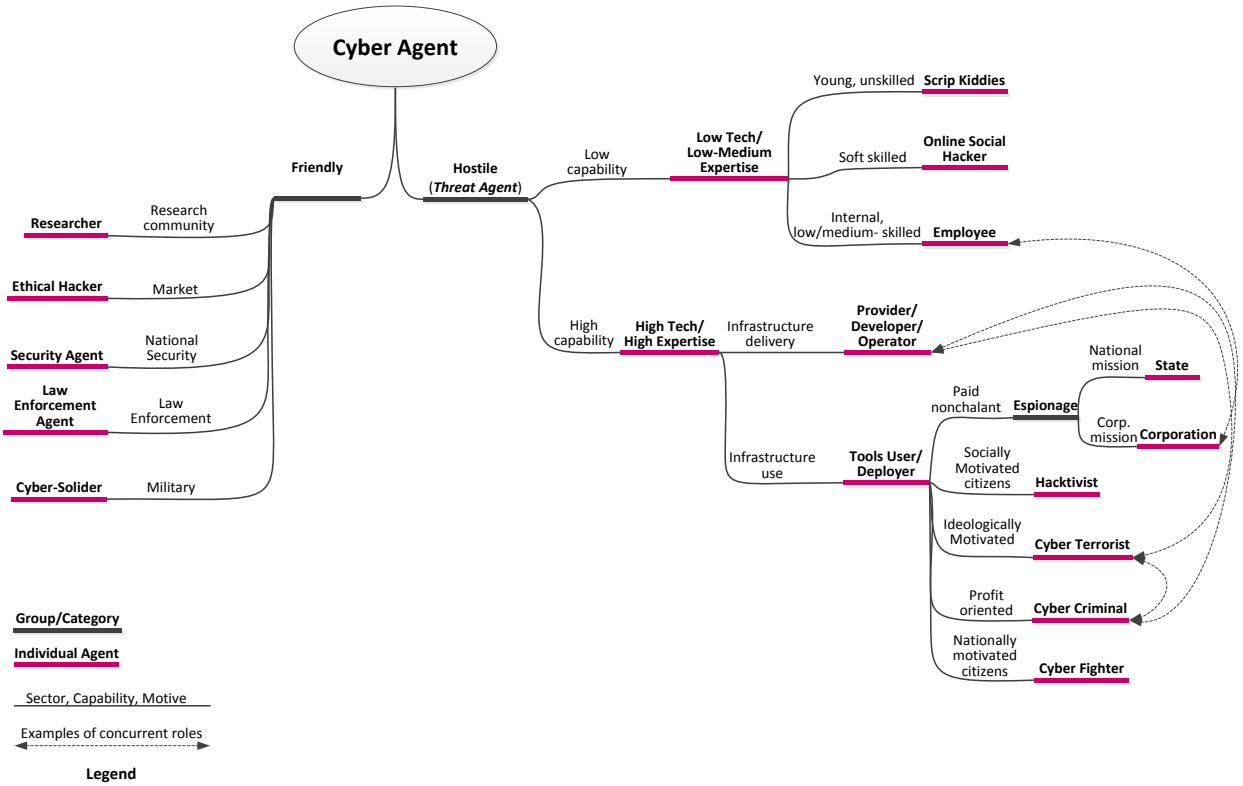


Figure 19: Overview of Agents in Cyber Space

Authoritative Recourses: National Cyber Security Centre, NL "*Cyber Security Assessment Netherlands 4*"[439]

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 3). The purpose of this table is to visualize which threat agent groups use 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

[252] http://motherboard.vice.com/read/how-an-fbi-informant-ordered-the-hack-of-british-tabloid-the-sun-1, accessed October 2014.

https://t.me/learningnets

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 (see section 2.4).

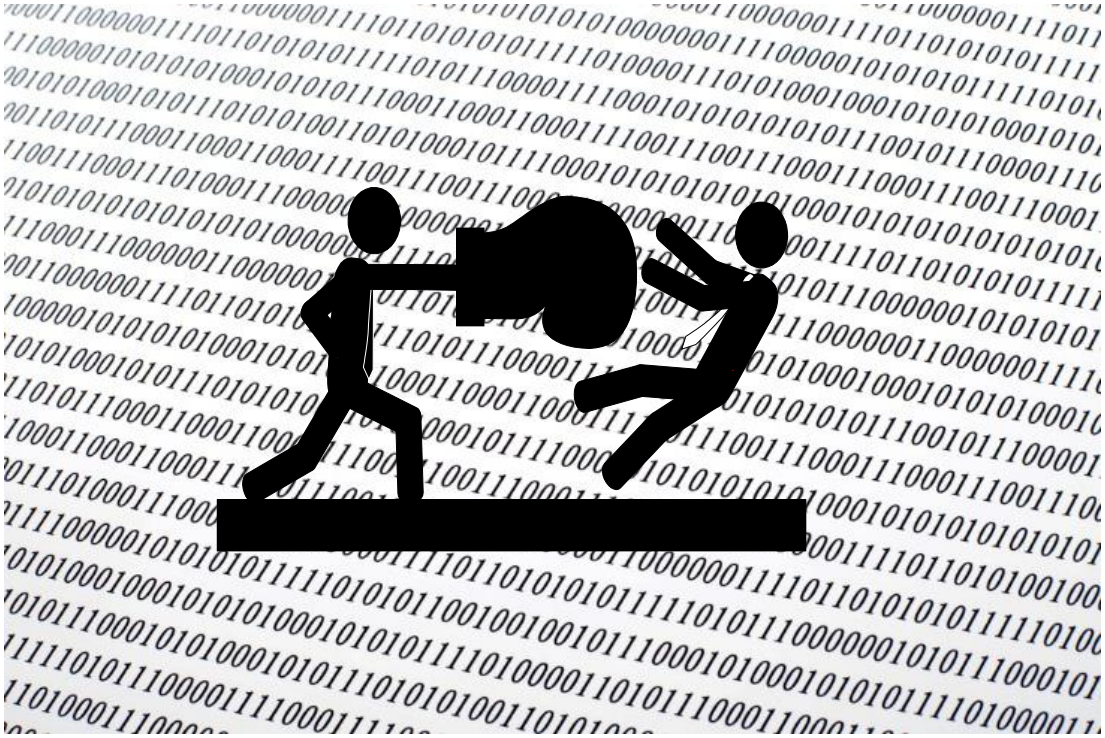
	Threat Agents								
	Corporations	Nation States	Hacktivists	Cyber Terrorists	Cyber Criminals	Cyber Fighters	Script Kiddies	Online Social Hackers	Employees
Malicious code: Worms/Trojans	✓	✓	✓	✓	✓	✓			✓
Web-based attacks	✓	✓	✓	✓	✓	✓		✓	
Web application /Injection attacks	✓	✓	✓	✓	✓	✓	✓		
Botnets			✓		✓				
Denial of service	✓	✓	✓	✓	✓	✓			
Spam				✓	✓	✓	✓	✓	
Phishing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Exploit kits		✓	✓	✓	✓	✓	✓		✓
Data breaches	✓	✓	✓	✓	✓	✓		✓	✓
Physical damage/theft /loss	✓	✓	✓	✓	✓	✓			✓
Insider threat	✓	✓	✓	✓	✓	✓			✓
Information leakage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity theft/fraud	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyber espionage	✓	✓							✓
Ransomware/ Rogueware/ Scareware					✓				

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. Similarly, Spam is a malicious tool deployed mainly by cyber-terrorists, cyber-criminals, cyber-fighters, script-kiddies and online social hackers.

https://t.me/learningnets

ETL 2014: Attack Vectors



https://t.me/learningnets

5 Attack Vectors

5.1 Attack Vectors within threat intelligence

In the ETL 2013[253], we have identified *attack workflow and attack patterns* as important pieces of information in order to better understand cyber threats. Such information will add value to identified threats, as every threat description will contain information on methods used to successfully deploy a specific threat. In this chapter we firstly position this information with regard to threats and explain its role. Moreover, we provide some information found on this matter by means of distinct attack methods assessed in the reporting period.

As already indicated in the used definitions (see section 2.6), in this year's ETL we have introduced **Attack Vectors** as an element of threat analysis. In the rest of this chapter, as an initial approach we use the term attack vector as synonymous with attack pattern and attack workflow. Knowing that these terms are already being used in threat modelling[254], we will not dive into details of such concepts for the time being[255]. Attack vectors will be considered rather from a practical point of view as an additional element for the understanding of cyber threats. To this extent, we will use the following simplistic definition of attack vectors:

If the assessed cyber threats are the malicious tools of threat agents, what are the ways these tools are used in order to harm assets? In other words: if the cyber threats are the "**what**", then what is the "**how**" to achieve a successful attack? The how reflected by the attack vector.

Knowing that this definition might be very simplistic and subjective, we use it for the time being as a sort of "pilot" to provide some information on attack vectors. Over time, this term will eventually mature further and become more comprehensive/inclusive. For the time being, however, we would assume attack vectors contain schematic information about the steps within an attack and the assets that have been compromised in order to achieve the malicious objectives (i.e. actions on objectives, as stated in kill chains).

Having stated this, we recognise that the concept of kill chains that is being used in the current threat landscape, is related to attack vectors. Within this work, we make the assumption that a kill-chain characterizes various phases of an attack vector. Hence, possible redundancies between kill-chain information and attack vector information should be tolerated for the time being. Another source of overlaps are assessed current threats: depending on the scope of each threat, it might be the case that some information from the attack vector (i.e. about the "how") is subsumed within the threat definition. Examples from the current document are the threats: web based attacks (including drive-by-download attack) cyber espionage (including APT and targeted attacks), exploit kits, etc. In other cases, a specific attack type is taken as synonymous to a threat (e.g. watering hole attack).

In order to gain information about attack vectors, an analysis of incidents needs to take place. Depending on the level of the detail achieved/published, various levels of attack vectors will be identifiable. The fact is, that attack vectors will be available for incidents that have been identified, reported and analysed, eventually by using forensic evidence. Given that not all incidents are analysed in this manner, it will not be always possible to provide this kind of information for assessed threats.

[253] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport, accessed November 2014.
[254] https://capec.mitre.org/, accessed November 2014.
[255] This is an activity that might be taken into account within discussions with relevant stakeholders in the coming year (2015).

https://t.me/learningnets

In the present chapter we deliver some preliminary information on the following attack vectors: Targeted attack, Drive-by-attack and Web strategic compromise (watering hole attack) and Advanced persistent threat (APT). These attack vectors have been selected as the most frequent and most documented ones.

Before going into these attack vectors, we will provide with a short discussion on the state-of-play of attack vector material found and the modalities used to describe attack vector information within ETL.

5.2 Describing a Cyber-Attack though Attack Information

The description of a cyber-attack is rather obvious: a threat agent uses tools (cyber threats) to abuse weakness of some assets, thus obtaining access to these assets with the final aim to achieve their malicious objectives (i.e. illegal profit/fraud, theft of valuable data, sabotage, etc.). This is identical to the content depicted in figure 1 "*Threats targeting an asset by trying to exploit vulnerabilities*" in chapter 2.2 of ETL 2013[256]. To this extent, an attack may be described as a set of steps. Each step might show an asset, its weakness/vulnerability, the tool to exploit the vulnerability and the consequences of a successful attack. 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). This is considered as a strong tool, especially for stakeholders with reduced threat analysis capabilities.

While information about the various steps of attacks were scarce in material found around 2010-2012, in 2013, many vendors/organisations have provided information about the attacks. Just as ETL 2013 and 2014, some organisations collecting threat intelligence have used kill-chains to provide general information about the phases of an attack supported by cyber threats[257,258,259,260,261,262] (references indicative and non-exhaustive). Kill-chains are definitely an important piece of information describing the "purpose" of a cyber threat. Yet, they do not give information about the assets at stake and vulnerabilities being abused. In some reports, a more detailed (mostly graphical) description of an attack is being provided[258,263,264,265,266,267] (references indicative and non-exhaustive).

Both kill-chains and graphical representations of attacks can be generic or campaign specific. This would allow for structuring attack vectors according to their specificity (i.e. generic category of drive-by-attack vs. specific drive-by-attacks within a certain campaign). Although structuring existing information in that way may be an interesting exercise, it might require significant effort. Apparently,

[256] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport, accessed November 2014.
[257] http://www.websense.com/content/websense-2014-threat-report.aspx, accessed October 2014.
[258] http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-de_lancaster_technical_report.pdf, accessed November 2014.
[259] http://www2.fireeye.com/rs/fireye/images/fireeye-real-world-assessment.pdf, accessed November 2014.
[260] http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf, accessed November 2014.
[261] http://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center, accessed November 2014.
[262] http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf, accessed November 2014.
[263] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf, accessed November 2014.
[264] http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf, accessed November 2014.
[265] http://www.fireeye.com/blog/wp-content/uploads/2014/02/greedywonk-campaign-v2.png, accessed November 2014.
[266] http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/, accessed November 2014.
[267] http://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/targeted-attacks, accessed November 2014.

https://t.me/learningnets

sticking to kill-chains seems to be a more feasible approach, as indicated by the relatively wide adoption of kill-chain within threat intelligence. A definite conclusion that can be drawn from this is, that the matter of attack vectors is at an early maturity level and requires more elaboration in the future.

Being a first pilot on attack vectors, the ETL 2014 will provide initial information on the attack vectors mentioned in section 5.1 consisting of: a generic description of the attack, threat agents involved and information sources found with some tags describing it (e.g. generic, campaign-specific, etc.). Due to the fact that we are at an early phase of our learning curve regarding this topic, the level of information provided could be characterized as initial. The material collected is not only from the reported period but also older. This allowed us to obtain a critical mass for the initial investigation of attack vectors.

Upon discussions with stakeholders and received feedback on this topic, we will consider expanding this information in the future by adding additional levels of description/details as deemed necessary.

5.3 Targeted attacks

Description: Targeted attacks are per definition attacks that are based on some specific knowledge regarding the target[268]. Based on this knowledge, adversaries craft specific messages or other artefacts to lure the victim. When arriving at the victims end, the malicious message is not recognised as such due to the familiarity that has been built in by the adversary (i.e. reference to a familiar personal, organisational process/matter). The victim "bites" the bait and an initial infection has been achieved.

Relation to kill-chain: Targeted attacks usually cover all phases of a kill-chain. A targeted attack starts with *reconnaissance* to obtain the initial knowledge about personal, internal, organisational and other characteristics of the victim. After that a *weaponisation* takes place (i.e. finding the right malicious artefact to perform the infection). The *delivery* takes place by means of the time point the victim "bites the bait". Then an *exploitation* takes place in that the malicious artefact finds a vulnerability to be exploited. Eventually, the malicious artefact perform an *installation* (i.e. malicious code) that may establish a communication channel with the adversary (i.e. *command and control*) to obtain the final *actions on objectives*.

Specificities/specialisations: A targeted attack may have many forms such as: spear phishing[269], watering hole attack (see dedicated description below), port attack, etc. Several of these attacks may be crafted to fit a particular sector[270,271,272]. Baits for targeted attacks may be based on hypes from breaking news, political events, crises, conflicts etc.

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

[268] http://marcoramilli.blogspot.gr/2014/07/cyber-intelligence-abusing-internet.html, accessed November 2014.

[269] http://usa.kaspersky.com/internet-security-center/definitions/spear-phishing?typnews=Social_media#.VGNAVaNBsnM, accessed November 2014.

[270] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf, accessed November 2014.

[271] http://www.securityweek.com/spear-phishing-hooked-businesses-big-and-small-2013-symantec-report, accessed November 2014 (provides as a summary of Symantec threat report).

[272] http://www.fireeye.com/blog/technical/malware-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html, accessed November 2014.

https://t.me/learningnets

- (Typical) Spear phishing attack[273],[274]
- Trend Alert campaign[275]
- Targeted attack data exfiltration[276]
- Targeted attack with dropper[277]

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.

5.4 Drive-by-attacks

Description: In a drive-by-attack, the victim visits a manipulated legitimate web site/page/application. Through the manipulation (i.e. injection) the victim's browser is redirected to a maliciously prepared site. It checks the victim's browser vulnerabilities and installs silently malware that exploits the discovered vulnerabilities. Other variations of drive-by-attacks use manipulated advertisements or other third party components referenced by Widgets[279]. Some sources refer to drive-by-downloads via viewing of an e-mails or pop-up[278]. Victims cannot visually recognise if a legitimate web site/page/application is compromised. This makes visual detection of drive-by-attacks by users impossible[279,280,281].

Relation to kill-chain: Drive-by-attacks have all phases of a kill-chain, apart from reconnaissance. *Weaponisation* happens via vulnerability scanning of victim's browser. Delivery is performed via downloaders, while *exploitation* takes place after the execution downloaded binaries[282]. According to exploits found, the malware downloads corresponding malicious code (usually a Trojan) that takes control of the victim's device (i.e. performing the phases *command and control* and *action on objectives*)[280].

Specificities/specialisations: Variations of drive-by attacks do exist, depending on the way a redirect is being implemented. Besides HTML manipulations, redirects can be implemented via manipulation of widgets (e.g. referring to advertisements). Further variations concern vulnerabilities exploited. Besides web browser, browser add-ons, operating system or third party applications may be exploited (Silverlight, Flash[283], PDF reader or video player).

[273] http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html, accessed November 2014.
[274] http://about-threats.trendmicro.com/RelatedThreats.aspx?language=tw&name=Anatomy%20of%20a%20Data%20Breach, accessed November 2014.
[275] http://www.fireeye.com/blog/technical/cyber-exploits/2013/05/targeted-attack-trend-alert-plugx-the-old-dog-with-a-new-trick.html, accessed November 2014.
[276] http://blog.trendmicro.com/trendlabs-security-intelligence/data-exfiltration-in-targeted-attacks/, accessed November 2014.
[277] http://news.softpedia.com/news/RARSTONE-RAT-Used-in-Targeted-Attacks-Against-Asian-Organizations-360843.shtml#sgal_0, accessed November 2014.
[278] http://en.wikipedia.org/wiki/Drive-by_download, accessed November 2014.
[279] http://www.imperva.com/Resources/Glossary?term=drive_by_downloads, accessed November 2014.
[280] http://blogs.sophos.com/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/, accessed November 2014.
[281] http://blogs.microsoft.com/cybertrust/2011/12/08/what-you-should-know-about-drive-by-download-attacks-part-1/, accessed November 2014.
[282] https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/provos/provos.pdf, accessed November 2014.
[283] https://blog.malwarebytes.org/exploits-2/2014/08/shining-some-light-on-the-unknown-exploit-kit/, accessed November 2014.

https://t.me/learningnets

Existing representations overviews/resources: On attack vectors of drive-by downloads, the following information was found (indicative):

- Drive-by-attack (also referred to as web malware attack)[284,285,286,287]
- Drive-by-attack (Darkleech malware) [288]
- Drive-by download (Flash file based)[289]
- Drive-by download (JS_WEBSTAR)[290]
- Drive-by download (Malvertising, DOUBLE CLICK Banner, advertisement)[291,292,293]

Involved adversaries: The following adversaries could run a drive-by attack: cyber-criminals, hacktivists, nation states, corporations, cyber fighters, cyber terrorists.

5.5 Strategic web compromise (watering hole attack)

Description: The watering hole attack is based on the infection of a legitimate web site that is being trusted/visited by a group of people that are under attack[294]. By visiting this compromised web site, visitors will be infected. To this extent, watering hole attacks are drive-by attacks (see 5.4) for a narrow group of victims. Watering hole attacks are also referred to as strategic web compromise (SWC)[295]. This attack is supposed to be complementary to spear phishing or other forms of phishing (i.e. are effective in case a group is resistant against such targeted attacks, see 5.3)[296].

Relation to kill-chain: The difference between SWC attacks and drive-by attacks, is that SWC starts with a *reconnaissance* in order to identify web sites that the target group uses/trusts. The rest continues as a drive-by attack: *weaponisation* happens via vulnerability scanning of victim's browser. Delivery is performed via downloaders, while *exploitation* takes place after the execution downloaded binaries. Subsequently, *installed* malware (usually Trojan or Remote Access Trojans – RAT) performs phases *command and control* and *action on objectives*[295].

Specificities/specialisations: Watering hole attacks are classified as targeted attacks (see 5.3). This is because through proper selection of the infected web site, adversaries may launch their attack on a specific group of users (e.g. developers, marketing, media teams etc.). The rest of the watering hole attack takes place as a drive-by download.

---

284 http://www.microsoft.com/security/assets/images/_security/sir_v11/keyfindings/rg_section_7_4.jpg, accessed November 2014.
285 http://sophos.files.wordpress.com/2014/03/webc2a0threatsc2a0infographic.pdf, accessed November 2014.
286 http://andyrussellcronin.files.wordpress.com/2012/02/drive-by-download-attack-example.png, accessed November 2014.
287 http://www.proofpoint.com/threatinsight/posts/the-invisible-drive-by-download-attack-I-attacker-infrastructure-how-it-works.php, accessed November 2014.
288 http://www.techweekeurope.co.uk/wp-content/uploads/2013/07/darkleech-1024x350.png, accessed November 2014.
289 http://blogs.cisco.com/security/far-east-targeted-by-drive-by, accessed November 2014.
290 http://about-threats.trendmicro.com/dumpImages/294201051312.jpeg, accessed November 2014.
291 http://blog.armorize.com/2010/12/hdd-plus-malware-spread-through.html, accessed November 2014.
292 http://securelist.com/blog/research/66415/gaps-in-corporate-network-security-ad-networks/, assessed November 2014.
293 http://www.invincea.com/wp-content/uploads/2014/10/Micro-Targeted-Malvertising-WP-10-27-14-1.pdf, accessed November 2014.
294 http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/137/watering-hole-101, accessed November 2014.
295 http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf, accessed October 2014., accessed November 2014.
296 http://en.wikipedia.org/wiki/Watering_Hole, accessed November 2014.

https://t.me/learningnets

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

- Strategic Web Compromise Activity (references including few campaigns)[295,297,298]
- Watering hole attack[299,300,301,302]
- Watering hole attack against Space Foundation[303]

Involved adversaries: Adversaries of SWC are almost identical to drive-by attacks: cyber-criminals, hacktivists, nation states, corporations, cyber fighters, cyber terrorists. However, incidents indicate a stronger engagement of threat agents with espionage aims (i.e. nation states, corporations).

5.6 Advanced persistent threat (APT)

Description: Advanced persistent threats refer to narrowly targeted campaigns that are performed from threat agents with high capabilities. Another characteristic of these attacks is their persistence: they usually run over a very long time period (i.e. years/months)[304]. The high capabilities are usually evidenced through a high degree of orchestration, use of advanced, specially crafted malware and extensive knowledge on details of the victim. These attacks are characteristic for espionage activities. This is due to the fact that the degree of capabilities demonstrated within such attacks can mainly be attributed to teams with large resources for preparation, reconnaissance, programming, vulnerability detection, computing power, etc. It is assumed that only state sponsored espionage can explain the provision of such an amount of resources.

Relation to kill-chain: Due to their advancement, size and quality, APTs cover the all phases of kill-chain (*reconnaissance, weaponisation, delivery, exploitation, installation, command and control, action on objectives*). Given their impact and importance, APT attacks have been analysed in a very detailed manner: the phases of APTs have been specified at a detail that goes beyond kill-chain phases[305,306,307,308].

Specificities/specialisations: APTs are also targeted attacks that are initiated by threat agents with high capabilities. Main specificity of APT is the long duration of attacks. Another important characteristic is the differentiation of APTs: by targeting a specific victim, APTs are quite different, especially regarding the malware used. Hence, each APT campaigns might have unique peculiarities in the preparation and

[297] http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/, accessed November 2014.
[298] http://www.fireeye.com/blog/technical/targeted-attack/2014/02/operation-greedywonk-multiple-economic-and-foreign-policy-sites-compromised-serving-up-flash-zero-day-exploit.html, accessed November 2014.
[299] http://www.symantec.com/connect/blogs/internet-explorer-zero-day-used-watering-hole-attack-qa, accessed November 2014.
[300] http://about-threats.trendmicro.com/de/webattack/137/Watering+Hole+101, accessed November 2014.
[301] http://zappytech.files.wordpress.com/2013/02/watering-hole.png, accessed November 2014.
[302] http://bvisible.ie/wordpress/wp-content/uploads/2013/04/Watering-Hole-Infographic1.png, accessed November 2014.
[303] http://eromang.zataz.com/2013/01/06/forgotten-watering-hole-attacks-on-space-foundation-and-rsf-chinese/, accessed November 2014.
[304] http://en.wikipedia.org/wiki/Advanced_persistent_threat, accessed November 2014.
[305] http://en.wikipedia.org/wiki/Advanced_persistent_threat#mediaviewer/File:Advanced_persistent_threat_lifecycle.jpg, accessed November 2014.
[306] http://hackmageddon.com/2011/10/13/apts-and-security-information-management/, accessed November 2014.
[307] http://piratehacks.com/wp-content/uploads/2013/04/Picture1.png, accessed November 2014.
[308] http://www.ibm.com/developerworks/library/se-aptplan/index.html, accessed November 2014.

https://t.me/learningnets

execution of the attack[309,310,311,312,313] (indicative list of recent APT campaigns). An interesting piece of information found in the reporting period provides some evidence on the efficiency of existing APT detection tools[314].

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

- Advanced Persistent Threat Stuxnet[315,316,317]
- Advanced Persistent Threat (Generic)[318],[319]
- APT28[320]
- RAT APT attack[321]
- APT NR4, 2011[322]

Involved adversaries: Adversaries involved in APT attacks are mainly engaged in espionage or sabotage activities, that is, mainly nation states and eventually large corporations. In some cases, such capabilities may be demonstrated in case of widely coordinated/orchestrated activities of cyber-criminals or hacktivists. An interesting APT analysis for EMEA including an analysis of involved threat agents can be found here[323].

[309] http://www.fireeye.com/blog/technical/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html, accessed November 2014.
[310] http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/11/darkhotel_kl_07.11.pdf, accessed November 2014.
[311] http://securelist.com/blog/research/67353/be2-custom-plugins-router-abuse-and-target-profiles/, accessed November 2014.
[312] http://www.novetta.com/files/5614/1329/6232/novetta_cybersecurity_exec_summary-3.pdf, accessed November 2014.
[313] http://www.symantec.com/theme.jsp?themeid=apt-infographic-1, accessed November 2014.
[314] https://blog.mrg-effitas.com/wp-content/uploads/2014/11/Crysys_MRG_APT_detection_test_2014.pdf, accessed December 2014.
[315] http://www.isssource.com/stuxnet-report-ii-a-worm%E2%80%99s-life/, accessed November 2014.
[316] http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, accessed November 2014.
[317] http://www.isssource.com/stuxnet-report-iv-worm-slithers-in/, accessed November 2014.
[318] http://net-founder.blogspot.gr/2011/02/advanced-persistent-threats.html, accessed November 2014.
[319] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_custom-defense-against-targeted-attacks.pdf, accessed November 2014.
[320] http://www.fireeye.com/resources/pdfs/apt28.pdf, accessed November 2014.
[321] https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23258/en_US/Diary_of_a_RAT_datasheet.pdf, accessed November 2014.
[322] http://www.symantec.com/threatreport/topic.jsp?aid=industrial_espionage&id=malicious_code_trends, accessed November 2014.
[323] http://www.fireeye.com/resources/pdfs/fireeye-emea-advanced-threat-report-1h2014.pdf, accessed November 2014.

https://t.me/learningnets

ETL 2014: Emerging Threat Landscape

https://t.me/learningnets

6 Emerging Threat Landscape

In this chapter ,threat trends for a number of emerging technology areas are presented. The content of this chapter constitutes the *Emerging Threat Landscape*. The information presented has been assessed by the analysis of relevant material. Besides security issues, emerging technology areas have been identified and the level of maturity with regard to cyber security has been assessed (e.g. in the area of network virtualisation). Thus, threat trends in emerging technology areas have been either directly mentioned in or have been implicitly assessed from the analysed material.

In the ETL 2014, some emerging areas from last year have been kept, while some new ones have been introduced. This occurred as a reaction to technological developments that have been identified in various application and technology areas in the reporting period. Moreover, focus shifts on emerging issues in well-established areas, as for example Critical Infrastructure Protection (CIP) have been reflected accordingly.

Besides establishing a connection between the threat landscape and emerging areas, this chapter identifies a number of security issues for each area that may be subject to security considerations in the middle term (i.e. 2015). 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, identified issues from last year's ETL have been taken into account within detailed threat landscapes that have been developed for smart environments[409] and internet infrastructure[324]. Similarly, some of the areas that are covered in this chapter may be the subject of more detailed threat assessments within 2015, depending on feedback from ENISA stakeholders (e.g. big data, network virtualisation or specific applications of smart environments, such as smart cities).

In particular, the emerging technology areas considered in this ETL are:

- *Cyber Physical Systems*: Cyber physical systems have been assessed as an emerging issue, especially within Critical Infrastructure Protection. With the current developments in areas relevant to CIP, it is important to understand the impact of engineered environments within the protection of critical goods, while assuring interoperability. A lot of innovations are expected to take place in this area in the future.
- *Mobile Computing*: The increasing role of mobile devices in the next generation IT architectures, but also the fact that they serve as a basis of technology convergence, makes them an important component both for users but also for operators of application services. As such, mobile devices are increasingly getting targeted by cyber-adversaries and this trend is going to keep up in the future.
- *Cloud Computing*: Being another important component of next generation IT, cloud computing is a technology that will bother users and security experts in the future. New/innovative usage models, attack scenarios and security control implementations will be in the focus of cyber-community in the future.
- *Trust Infrastructure*: Trust infrastructures and authentication infrastructures in particular are the most vital components of cyber-security. In the reporting period we have seen a lot of attacks on these components. These attacks result in dynamic changes, introduction of good practices and even innovations. Trust infrastructure is thus an evergreen of emerging cyber-security areas.

[324] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl, accessed December 2014.

https://t.me/learningnets

- *Big Data*: Though not yet completely explored, big data in the focus of cyber security for two reasons: firstly it is a valuable asset and as such is being targeted by cyber-attacks; secondly, it turns to become a very powerful tool for security professionals, as it significantly contributes to building intelligence about threats and incident management.
- *Internet of things/interconnected devices/smart environments*: While the growth of interconnected devices continues, smart environments and smart systems emerge in many sectors. Under this emerging area we consider all kinds of interconnected devices that build up a smart system, such as smart homes, smart buildings, smart cars, etc. The importance of this sector led ENISA to perform in 2014 a sector specific threat landscape in the area of smart homes and converged media[409].

It should be noted that the above areas are not completely independent or overlap free. Mobile computing, for example may be part of smart environments and have overlaps with trust infrastructures and cloud computing. 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 2015 that have been developed around the end of the reporting period draw similar conclusions[325,326].

In the following sections a short discussion with the highlights of each particular area is given prior to the emerging threat and trends 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. For each area, whenever applicable, the top 10 threats have been assessed. It should be noted that these threat trends are usually not the result of detailed assessments. This is because of the emerging nature of these areas. Hence, both the prioritisation and assessed trends are an estimation 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 Cyber Physical Systems as an emerging CIP issue

Cyber physical systems (CPS) 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. Examples of such areas are power supply, medical systems/healthcare, industrial systems and manufacturing, transportation, telecommunication and many others[327]. Being at the interface to physical production, distribution and deployment processes, CPS are vital for safety, resilience, security, adaptability, scalability. When combined with intelligent functions, CPS will bring great advantages for Critical Infrastructure Protection (CIP) and is considered as an emerging area that will have tremendous impact for innovation, availability of utilities and efficiency of use. To this extend, this emerging area has been selected in this year's ETL to reflect challenges in critical information infrastructure protection (CIIP) by covering the link to physical world, a source of impactful, yet difficult to manage security incidents.

Being at the transition point between physical and IT worlds, CPS will aim at illuminating the interplay between information technology and engineering. A typical example is security vs. safety: in numerous

[325] http://www.symantec.com/connect/blogs/threat-landscape-2014-and-beyond-symantec-and-norton-predictions-2015-asia-pacific-japan, accessed December 2014.
[326] http://www.informationsecuritybuzz.com/mcafee-lab-report-previews-2015-developments-exploits-evasion/, accessed December 2014.
[327] http://www.nsf.gov/pubs/2014/nsf14542/nsf14542.htm, accessed November 2014.

https://t.me/learningnets

discussions, for example in the area of Smart Grids, experts have debated about how safety issues, long matured in the engineering area, can be adopted/supported/reflected in security controls and vice versa. CPS seems a promising area that will facilitate transition between engineering and information technology, thus eliminating deficiencies stemming from (quite natural) mutual knowledge gaps between these disciplines.

In the consumer area, an important role in the interconnection of IT and physical worlds is attributed to internet of things and smart environments. In the industrial/engineering sector this role is attributed to Smart Grids and SCADA systems. This emerges from the necessity to efficiently manage/assist human life and achieve more efficient energy management and manufacturing processes. The developments in these areas have been dictated from strong market needs that can be saturated with the adoption of IT tools. Soon, other areas of interconnection between physical and IT world will achieve market maturity.

Top (preliminary[328]) emerging threats to CPS are:

	Emerging Threat	Threat Trend
1.	**Malicious code: Worms/Trojans**	↑
2.	**Web based attacks**	↑
3.	**Spam (as instrument to infect IT and affect CPS)**	↑
4.	**Phishing (as instrument to infect IT and affect CPS)**	↑
5.	**Physical damage/theft/loss**	↑
6.	**Insider threat**	↑
7.	**Cyber espionage**	↑
8.	**Identity theft**	↑
9.	**Web application attacks/Injection attacks**	↑
10.	**Information leakage**	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 4: Emerging threats and their trends in the area of cyber physical systems

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

[328] Assessed threats for this area are assumed by extrapolating threat landscapes of IoT, Smart Grid and SCADA, as initial CPS areas that have received attention from the cyber-security community. Due to the early stages of action in this area, these threats are rather indicative and of possibly restricted scope in comparison to the width and depth of this area.

https://t.me/learningnets

- Both in the US and in Europe the area of CPS has received considerable attention. Initial material towards strategies, innovation actions and research are in place[327,329,330,331,332,333,334]. Taking into account advancements in engineering sciences and activities within the EU, one might argue that CPS can be a favourable area for the creation of competitive advantages for European industry and research. To this extent, CPS is a distinct opportunity for Europe that should continue receiving the necessary attention from industry, academia and policy. The main focus should be on breaking silos and enabling the creation of proper grounds for the necessary interdisciplinary cooperation. Information found on the advancement of relevant activities leave the impression that the US is slightly ahead with regard to this area[335], as compared to EU at least at the coordination level. Though this might be quite natural (one country vs. many Member States), this does not mean that individual EU-Member States (e.g. Germany) are not in a more advanced stage in CPS[336].
- Taking a look at cyber security and CPS in performed/announced international events[337],[338] one can identify the following areas of interest/state-of-the-art that are indicative for upcoming developments (non-prioritized list): authentication and access control for CPS, availability, recovery and auditing for CPS, key management in CPS, legacy CPS system protection, lightweight crypto and security, vulnerability analysis for CPS, threat modelling for CPS, wireless sensor network security, intrusion detection for CPS, adaptive attack mitigation for CPS, trusted-computing in CPS, forensics for CPS. It is worth mentioning, the fact that these events are among the first organised in the area of CPS is indicative for the initial maturity of the entire topic.
- Although CPS is a rather new topic, this does not mean that in particular areas no progress is being achieved. The issue here is that this progress happens on a sector-by-sector basis, e.g. smart grids, smart homes, internet of things, smart vehicles, etc. This leads to a segmentation of the sectors and leads to a reduced interoperability among these sectors, a matter that is of great importance given the increased convergence, brought for example by technologies like mobile and cloud computing.
- The absence of common architectures and interfaces bears segmentation risks and thus market failure risk. Functional isolation of developed solutions with regard to an inevitable convergence becomes evident when looking at currently independent sectors that are necessary to create user centric experience. An example is the area of e-health: home care, assisted living, pharmaceutical, hospital systems and healthcare are still individual sectors, yet necessary to deliver a holistic service to ageing citizens. Failure to integrate through absence of a common reference

[329] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4281, accessed November 2014.
[330] http://ec.europa.eu/dgs/connect/en/content/cyber-physical-systems-european-ri-strategy, accessed November 2014.
[331] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/78-ict-01-2014.html, accessed November 2014.
[332] http://ec.europa.eu/digital-agenda/en/news/report-workshop-cyber-physical-systems-uplifting-europe%E2%80%99s-innovation-capacity, accessed November 2014.
[333] http://www.nsf.gov/pubs/2014/nsf14571/nsf14571.htm, accessed November 2014.
[334] http://www.nist.gov/cps/, accessed November 2014.
[335] http://www.nist.gov/cps/cps-pwg-webinar.cfm, accessed November 2014.
[336] https://www.cased.de/en/research/researchlabs/cyphyslab.html, accessed November 2014 (taken as just a representative but not unique EU case).
[337] http://icsd.i2r.a-star.edu.sg/cpss15/#CFP, accessed November 2014.
[338] http://www.cps-security.org/call-for-papers.html, accessed November 2014.

https://t.me/learningnets

architectures will create duplications of effort and weak links in among the sectors and within supply chain within sectors.

6.2 Mobile Computing

It is obvious that the importance of mobile computing and the value it holds for the end-user will keep growing in the near future[339]. The more interconnected devices are deployed, the more content and control is going to converge by means of mobile devices and platforms. Being a basic component of the mobile and interconnected ecosystem, mobile devices will continue to be the targets of cyber-criminals. It is expected that mobile device evolution rates will match the evolution rates of malicious activities being observed in the reporting period[340].

Following increases of threat sophistication, both interfaces and internal functions of mobile devices will be abused. But the main future trend will remain the abuse of mobile devices with respect to the entire mobile ecosystem, including cloud storage, app APIs, app internals (processed data and binary code [341]), abuse of vetting processes, stealth attacks, etc. The trend of migrating all malicious techniques from PC to mobile will continue, whereas attack specially crafted for mobile devices will show up. Such attacks have been impressively demonstrated by researchers[342,343].

Top emerging threats to mobile computing are:

	Emerging Threat	Threat Trend
1.	**Malware: Worms/Trojans (including malicious or unwanted functions of untrusted re-used code libraries[344])**	↑
2.	**Physical Theft/Loss/Damage**	↑
3.	**Phishing**	↑
4.	**Web application/Injection attacks**	↑
5.	**Web based attacks**	↑
6.	**Information Leakage**	↑
7.	**Identity Theft**	↑
8.	**Exploit Kits**	↑
9.	**Ransomware/Rogueware/Scareware**	↑

[339] http://www.computerweekly.com/news/2240233919/Societys-values-moving-from-Mono-to-Koto-says-Hitachi?asrc=EM_EDA_35964392&utm_medium=EM&utm_source=EDA&utm_campaign=20141103_Technology%20is%20changing%20society's%20values,%20says%20Hitachi_, accessed November 2014.

[340] http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/the-mobile-landscape-roundup-1h-2014, accessed November 2014.

[341] https://www.owasp.org/index.php/Mobile_Top_10_2014-M10, accessed November 2014.

[342] https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_wang-updated-8-23-13.pdf, accessed November 2014.

[343] http://www.cis.syr.edu/~wedu/Research/paper/xds_attack.pdf, accessed November 2014.

[344] http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-mobile-devices-security-perspective-30102014.pdf, accessed November 2014.

https://t.me/learningnets

	Emerging Threat	Threat Trend
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:

- Malware infection vectors that evade protection (i.e. sandbox) are for quite some time in the wild[345]. Yet, vicious mobile infection vectors are making their debut. Examples are: "implanting" vulnerabilities into a mobile device through rogue applications[346]; abusing synchronisation of mobile device with PC[347,348]; spread of malware that is tracking gestures[349]; misusing available functions to control the mobile device[350], abuse of loss protection controls[351], etc. Combined with advances that of general malware, these methods may deliver significant incidents in mobile devices, and not only: mobile devices are often the door to connected services such as cloud storage[352].
- The announced introduction of NFC-based payments via mobile devices will revive the payment market. Given a better penetration of mobile payments, cybercriminals are going to be target the payment platforms, eventually using attack scenarios from e-commerce and transaction based economy[353],[354]. It should not be a surprise to surface attacks that are attempt tampering of hardware, but also available authentication functions.
- Mobile security controls –both implementations and operation - need to reach the maturity of existing security controls for other non-mobile platforms. Moreover, they need to span limits of components of the mobile computing architecture and to seamlessly interoperate without introducing any security gaps[355]. Operators of mobile infrastructures and users need to understand and properly deploy them.
- Secure development of mobile apps moves again into the focus[356]. Application development of mobile apps needs to mature and follow maturity increases demonstrated in web application

[345] http://www.fireeye.com/blog/technical/malware-research/2014/06/turing-test-in-reverse-new-sandbox-evasion-techniques-seek-human-interaction.html, accessed November 2014.
[346] http://macsecurity.net/view/50/, accessed November 2014.
[347] http://www.australiansecuritymagazine.com.au/2014/06/kaspersky-discovers-new-android-ios-mobile-malware/, accessed November 2014.
[348] http://www.forbes.com/sites/thomasbrewster/2014/11/06/china-wirelurker-ios-malware/, accessed November 2014.
[349] http://securityaffairs.co/wordpress/21828/hacking/screenlogging-malware-can-log-swipe-gestures-mobile.html, accessed November 2014.
[350] http://www.wired.com/2014/07/hackers-can-control-your-phone-using-a-tool-thats-already-built-into-it/, accessed November 2014.
[351] http://www.troyhunt.com/2014/05/the-mechanics-of-icloud-hack-and-how.html, accessed November 2014.
[352] http://www.wired.com/2014/09/eppb-icloud/, accessed November 2014.
[353] http://www.slideshare.net/emcacademics/ecommerce-fraud-protecting-data-transactions-and-consumers, accessed November 2014.
[354] http://www.zdnet.com/researchers-use-shopping-cart-to-put-mobile-nfc-payment-theft-on-wheels-7000023584/, accessed October 2014.
[355] http://www.computerworld.com/article/2840355/gigamon-says-it-can-analyze-attacker-ssl-traffic-without-affecting-performance.html, accessed November 2014.
[356] https://www.owasp.org/index.php/OWASP_Guide_Project, accessed November 2014.

https://t.me/learningnets

development[357]. Besides secure app application and architecture practices, reuse of code libraries, and binary code protection will be two areas that will need to be further developed. Such advancements will reduce the attack surface for the leakage and identity theft threats. Finally, secure usage of identification and authentication and access control covering as much components as possible will increase data protection and data privacy in mobile environments.

6.3 Cloud Computing

Adoption of cloud computing solutions continues to grow. Trends identified in 2014 show that cloud plays a key role in next generation IT[358,359]. As indicated within this ETL report, mobile devices, cloud storage and Bring Your Own Device approaches are be the main components in the IT paradigm shift currently taking place[358]. Nonetheless, cloud computing has been massively put under pressure due to Snowden revelations, in particular regarding data protection issues of stored information[360]. Both state-sponsored surveillance and cyber-threat landscape regarding major components of the emerging next generation IT have impacted technology decisions[361]. As a result, a significant slowdown in the technology adoption with regard to next generation IT has been assessed. Moreover, it is estimated that these developments may cost cloud providers significant amounts[362]. But also policy has reacted on these developments: European Commission has created a framework to debate on issue of cloud computing, thus opting for updated strategies and requirements, in particular for public sector by means of the Digital Agenda[363].

Another concern regarding could computing is related to the complexity, flexibility and level of adoption for businesses. Inherent complexity of cloud computing, together with concerns about data protection, compliance, continuity[364] and insider threat in particular, are sources of additional concerns[365]. In particular, the management of such a massive chunk of infrastructure in a concentrated manner is a new challenge for users: possibility of human errors, misconfiguration and even insider threats pose significant risks to organisation[366].

Last but not least, just as businesses, cybercriminals have also recognised the advantages of cloud computing. Cost issues, better camouflage of malicious activities on legitimate sites and performance issues are key points for this[367]. It should be expected that this trend will continue beyond the reporting period and cloud providers would need to provide security controls and guide customers to develop their security strategies in accordingly.

Top emerging threats to cloud computing are:

[357] http://info.whitehatsec.com/rs/whitehatsecurity/images/statsreport2014-20140410.pdf, accessed November 2014.
[358] http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2014-state-cloud-survey, accessed November 2014.
[359] http://www.idc.com/getdoc.jsp?containerId=prUS24298013, accessed November 2014.
[360] http://nsaaftershocks.com/wp-content/themes/nsa/images/NSA-After-Shocks.pdf, accessed November 2014.
[361] http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf, accessed November 2014.
[362] http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0, accessed November 2014.
[363] https://ec.europa.eu/digital-agenda/en/news/european-cloud-strategy-0, accessed November 2014.
[364] https://www.owasp.org/index.php/Cloud-10_Business_Continuity_and_Resiliency, accessed November 2014.
[365] http://enterprise-encryption.vormetric.com/rs/vormetric/images/Global-Insider-Threat-WEB.pdf, accessed October 2014.
[366] http://www.brightcloud.com/pdf/CyberEdge-2014-CDR.pdf, accessed November 2014.
[367] http://www.solutionary.com/news-events/press-releases/2014/01/sert-threat-intelligence-report-q4-2013/, accessed November 2014.

https://t.me/learningnets

	Emerging Threat	Threat Trend
1.	**Malicious code: Worms/Trojans (targeting hosted information[368])**	↑
2.	**Web based attacks (on hosted information)**	↑
3.	**Web application /Injection attacks (on hosted information[358])**	↑
4.	**Botnets**	↑
5.	**Denial of Service**	↑
6.	**Insider threat (unintentional activity, information misplacement, misconfiguration errors)**	↑
7.	**Data breaches**	↑
8.	**Cyber espionage**	↑
9.	**Identity Theft**	↑
10.	**Information leakage**	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 6: Emerging threats and their trends in the area of cloud computing

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

- Given the current state-of-play in cloud computing, it seems that there is an emergence of multi-cloud strategies[369]. Multi-cloud strategies emerge from the need of agility, control (both technical and costs), data protection, performance, compliance, etc[370]. Implementation of multiple cloud strategies (also referred to as hybrid cloud), may require adaptation of network access to cloud providers and interoperability. In both cases, security controls of the organisation has to be optimised, also integrating security measures of the various providers (both cloud and network).
- Data breaches and surveillance are a major concern for decision makers in order to launch cloud based solutions. Complexity, performance and control are further issues to be surfaced. In remains to be seen how cloud provider and customers are going to master these challenges in order to address business concerns regarding reduced control over cloud computing, security and mobility. In particular given the fact that these technologies, may be vulnerable due to potential weak links in the supply chain[371]. Emerging security solutions including anonymity in the cloud[372]

[368] http://www.rackspace.com/knowledge_center/whitepaper/alert-logic-cloud-security-report-spring-2014-research-on-the-evolving-state-of-cloud, accessed November 2014.
[369] http://blog.equinix.com/2014/07/multicloud-management-strategies-the-hybrid-cloud-is-a-reality/, accessed November 2014.
[370] http://www.eweek.com/cloud/slideshows/developing-a-multi-cloud-strategy-10-factors-to-consider.html, accessed November 2014.
[371] http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf, accessed October 2014.
[372] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6732964, accessed November 2014.

https://t.me/learningnets

and uptake of encryption practices[373,374] are still subject of discussions and will be of concern to the community in the middle term. Finally, increased transparency and reduction of complexity in management of cloud resources will be a matter of concert, together with identity and access management/governance[366].

- Collected statistics regarding posture of cloud users regarding awareness of data protection[360] issues have shown that: some 50% are demonstrating an increased interest about location of data storage; ca. 55% have increased diligence regarding cloud activities/projects; some 50% have lost trust to public cloud services; while over 30% are changing procurement requirements and conditions with regard to could services.
- Unfortunately, for the same reasons as for legitimate users, cloud is an attractive platform for a variety of cyber-threat agents[367,375]. It provides a number of advantages that are serving malicious intent, including ease of site development to accommodate infection vectors, by at the same time evading IP blocking due to trusted origin (i.e. IPs of major cloud providers). Moreover, the inherent mobility of storage/applications to different clouds, adds another level of difficulty for defenders to locate and block malicious content. It is expected that through the use of encryption and anonymity, additional evasion mechanisms will be developed to abuse the cloud.

6.4 Trust infrastructures

With the term trust infrastructure we refer to systems, components, functions and data that implement security functions used to establish trust in the communication between systems and between systems and users. Examples of such functions are encryption, electronic signatures, challenge/response processes, etc. Trust infrastructure aims at the secure provision of these functions, the secure operation of involved components and secure storage of secret information. Proper functioning of trust infrastructures is key for the security in all kinds of electronic transactions, including the Internet. Consequently, any form of compromise or breach of such functions and data are a serious incident for digital trust.

In this reporting period we have seen serious incidents related to SSL (both OpenSSL and MS-TLS) a key component of the internet trust infrastructure[376,377,378]. Moreover, attempts to abuse tolerant requirements for purchasing SSL security certificates [379] and compromise the certificate infrastructure[380] have been detected. Besides SSL and certificate infrastructure, voices regarding the security level PGP have been raised[381]. All this is a warning on the trust level resulting current encryption, authentication and signing in the internet and e-mail communication. Taking into account

[373] http://www.infoworld.com/article/2608010/cloud-security/encryption-in-the-cloud-is-scarcer-than-you-think.html, accessed November 2014.
[374] https://www.thales-esecurity.com/knowledge-base/analyst-reports/encryption-in-the-cloud-english, accessed November 2014.
[375] https://www.europol.europa.eu/sites/default/files/publications/ec3_first_year_report.pdf, accessed November 2014.
[376] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=WGL03057USEN#loaded, accessed October 2014.
[377] https://community.rapid7.com/community/infosec/blog/2014/10/14/poodle-unleashed-understanding-the-ssl-30-vulnerability, accessed October 2014.
[378] http://arstechnica.com/security/2014/11/potentially-catastrophic-bug-bites-all-versions-of-windows-patch-now/, accessed November 2014.
[379] http://www.scmagazineuk.com/800-fake-companies-front-cybercrime-attack/article/369665/, accessed November 2014.
[380] http://securityaffairs.co/wordpress/22196/cyber-crime/fake-ssl-certificates.html, accessed November 2014.
[381] http://thehackernews.com/2014/08/cryptography-expert-pgp-encryption-is_19.html, accessed November 2014.

https://t.me/learningnets

that further attempts to compromise SSL and certification security infrastructure security might come up, effort needs to be invested in trust infrastructure to maintain a good level of trust. This will become important within the upcoming web of trust needed for Internet of Things, smart environments, payment, etc.

Top emerging threats to trust infrastructure are:

	Emerging Threat	Threat Trend
1.	**Web based attacks**	➲
2.	**Phishing (67% of cyber espionage campaigns start with a phishing attack[382])**	↑
3.	**Malware: Worms/Trojans**	↑
4.	**Web application attacks: Code Injection**	↑
5.	**Information leakage**	↑
6.	**Identity Theft**	↑
7.	**Physical theft/damage/loss**	↑
8.	**Denial of Service**	➲
9.	**Exploit kits**	↑
10.	**Cyber espionage**	↑

Legend: ↓ Declining, ➲ Stable, ↑ Increasing

Table 7: Emerging threats and their trends in the area of trust infrastructure

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

- Trust infrastructure is an area that is horizontal to many other emerging areas, in particular the ones covered in this chapter (i.e. mobile computing, Internet of Things, could computing, network virtualisation and cyber physical systems). As such, security of all other areas is highly dependent on trust infrastructures. Having such a central role in the chain of trust, it is evident that trust infrastructure will be a premium target for cyber-criminals. Hence, further leakage threats, abuse of trust between machines and users will be on the agenda of adversaries for the coming period.
- While encryption and anonymity seem to be the solution[383] for the observed reduction of trust in the internet communication and services, at least in the reporting period they have been rather the problem. We have seen an impressive erosion of basic security functions in this year, targeting both encryption[377,378,379] and potentially anonymisation functions[384,385].

[382] http://www.verizonenterprise.com/DBIR/, accessed October 2014.
[383] http://securityaffairs.co/wordpress/29781/social-networks/facebook-tor-hidden-service.html, accessed November 2014.
[384] https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous, accessed November 2014.
[385] http://securityaffairs.co/wordpress/30202/hacking/tor-traffic-analysis-attack.html, accessed November 2014.

https://t.me/learningnets

- Authentication models and in particular their technical implementations will need to be revisited. Based on existing good practices (i.e. financial sector[386]), requirements for increasing the security level of authentication functions might be considered. The wider adoption of two factor authentication, as introduced by leading IT-companies[387,388] is going to increase trust in existing authentication schemes. The consideration of non-repudiation schemes should also been taken into account.
- E-Mail encryption will need to be revisited. Existing encryption based on PGP receives a lot of fair criticism, mainly pointing out the need for modernisation of the used principles and available implementations[389]. Despite or even because of pending adoption of PGP by Google[390] and Yahoo[391], some discussion regarding the future potential of this standard after a mass deployment will serve the intended purpose.
- Internet of things and network virtualisation functions will bring big challenges in the establishment of trust between users and devices and among devices[392]. Risks related to interconnected identities will be in the focus, as interconnected devices will share data on behalf of users (i.e. implemented within the environments via chains of possibly interoperating mutually trusted identities). The attack potential to identities will rise, together with the potential impact of successful attacks.
- Attacks on authentication functions and open source functions will persist. Attacks to authentication functions hold the second position in OWASP top 10 risks list[393]. Regarding open source functions, as a lesson learned from Heartbleed attack, industry has formed the Core Infrastructure Initiative (CII)[394] that aims at taking care of open source code that is essential for computing (including security and trust functions). The aim of this organisation is to support the open source developer community with funding, thus achieving higher more security awareness and reduce the chances of bugs being introduced in the first place.

6.5 Big Data

In ETL 2013, big data has been addressed as an emerging technology, mainly from the business point of view and its future role as potential valuable asset. While this expectation for big data is still valid, in the reporting period this threat landscape, the cyber-security community has been focusing on the

[386] http://www.ecb.europa.eu/paym/t2s/progress/pdf/tg/crg/crg24/t2s_0466_bfd.pdf??ac7a536fed2f1643c5e52ac556e3061e, accessed November 2014.
[387] https://www.google.com/landing/2step/, accessed November 2014.
[388] http://www.zdnet.com/tutorial-facebook-2-factor-authentication-step-by-step-7000028372/, accessed November 2014.
[389] http://blog.cryptographyengineering.com/2014/08/whats-matter-with-pgp.html, accessed November 2014.
[390] http://googleonlinesecurity.blogspot.gr/2014/06/making-end-to-end-encryption-easier-to.html, accessed November 2014.
[391] http://www.pcworld.com/article/2462852/yahoo-mail-to-support-end-to-end-pgp-encryption-by-2015.html, accessed November 2014.
[392] http://www.nist.gov/nstic/gp-interoperability.html, accessed November 2014.
[393] https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management, accessed November 2014.
[394] http://www.linuxfoundation.org/programs/core-infrastructure-initiative, accessed November 2014.

https://t.me/learningnets

practical use of big data as a tool to build threat intelligence[395,396,404]. Several approaches and tools performing data analytics based on massive log and network traffic information have been released and took up an important role within Security Information and Event Management (SIEM)[397]. This development has turned SIEM approaches into powerful tools[398].

Notwithstanding the fact that currently the cyber security community views big data as a useful tool rather than a risk, big data growth is still being considered as a risk factor[399], especially given the upwards trend of data breach threat. After NSA revelations, the cyber-security community has realized that big data are at risk: one should consider raw data collected in a big style by national security agencies without establishing a proper transparency in their investigation activities.

Preparatory activities with regard to relevant regulation in the US have focused on big data by underlying its important role for society, but also stating risks to privacy and self-determination that are connected to this asset and related technologies[400]. Similar activities have been in the reporting period within the European Commission[401,402]. This is a very positive development, as this may help governmental/legal action to catch up in this area, being currently behind technological developments.

Top emerging threats to big data are[403]:

	Emerging Threat	Threat Trend
1.	**Data breaches**	↑
2.	**Information leakage**	↑
3.	**Identity theft/fraud**	↑
4.	**Insider threat**	↑
5.	**Cyber espionage**	↑
6.	**Physical damage/theft/loss**	↑
7.	**Phishing (as a tool to obtain access to big data)**	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

[395] http://www.shrm.org/hrdisciplines/safetysecurity/articles/pages/use-big-data-detect-cyber-crime.aspx, accessed November 2014.
[396] https://www-304.ibm.com/connections/blogs/predictiveanalytics/entry/big_data_analytics_and_the_digital_doppelganger?lang=en_us, accessed November 2014.
[397] ftp://ftp.software.ibm.com/la/documents/imc/la/commons/WGW03049_HR.pdf, accessed November 2014.
[398] http://www-03.ibm.com/security/solution/intelligence-big-data/, accessed November 2014.
[399] http://software.dell.com/documents/protecting-the-organization-against-the-unknown-whitepaper-27396.pdf, accessed November 2014.
[400] http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, accessed November 2014.
[401] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=3488, accessed November 2014.
[402] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6210, accessed November 2014.
[403] For this emerging area we have considered threats that target directly and/or may have an immediate impact on big data. From the top current threats we have identified seven as most relevant.

https://t.me/learningnets

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 SIEM is in the list for new acquisitions in the area of cyber security. Operating such a tool, however, will require significant skills in threat information collection, building up and maintaining threat intelligence and disseminating this information to relevant players within the organisation. Hence, the entire-lifecycle of SIEM might be quite expensive, while requiring adaptation of existing processes. Due to complexity and costs, it is very likely that smaller companies (i.e. SMEs) will not be in the position to afford such solutions.
- It is predicted that big data based SIEM technologies will be part of organisations defence strategy, growing form 8% currently to 25% in 2016[395]. Admittedly, current uptake of big data based security analytics is at an early phases of adoption and so is big data in general[400]. A few years will be required to understand technical and organisational exploitation of big data in general and in SIEM in particular. Current experience of early adopters of big data based SIEM are very positive, reporting advances in threat intelligence used to operate risk-based security controls[365].
- A survey[365] about use of big data in SIEM has shown that surveyed participants are concerned about protection of big data holding sensitive information (69%). 60% of participants were concerned violating data privacy by mixing data from different geographic areas; and ca 59% see data loss risks from wide distribution of big data. Moreover, in order to find relevant information among big amounts of data, top five use cases have been identified[404]: 1. Successful exploration of big data to understand it within decision making; 2. Holistic customer view by combining internal and external data; 3. Creation of security/intelligence context to achieve risk based protection in real time; 4. Achieve operational efficiency by analysing wide variety of data; and 5. Augment big data with traditional data warehouse capabilities.
- Within discussions with the ENISA ETL Stakeholder Group it has been identified that a challenge is to master the size of big data in order to timely spot threat patterns and achieve near-time responses. Another issue of concern regards data discovery: a very large amount of it contains information about already available intelligence. The challenge is to discover the parts that are related to new/unknown patterns that can attributed to malicious activities.
- Some additional interesting issues assessed within the reporting period with regard to big data are:
  - Smart environments will significantly contribute to production of big data. This kind of data will have high value, as it contains intimate life logging information of smart home users. Potential of misuse of this information by companies, adversaries and surveillance activities is a rather obvious conclusion.
  - While currently big data based SIEM use log, alert and incident information, it is expected that additional data will be included, such as configuration information, audit trails, web information, dark web information, etc. (an interesting visualisation can be found in[404] by

[404] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGW03020USEN&attachment=WGW03020USEN.PDF, accessed November 2014.

https://t.me/learningnets

means of a big data iceberg). Similar approaches are available within own developments of organisations and go currently through initial maturity steps.

6.6 Internet of things/interconnected devices/smart environments

Both the proliferation of mobile computing (see section 6.1) and the silent, yet considerable increase of interconnected things (i.e. Internet of Things)[405] pose challenges for cyber security. In particular interconnected devices from areas such as smart home, smart cities, smart vehicles[406], will exchange information that has high privacy/intimacy relevance. Moreover, functions available and data exchanged, when abused, may even impact human life [407, 408]. Given the complexity behind environments that take advantage of or are controlled by interconnected devices, security, trust and privacy issues are of major importance and pull the attention of end-users, industry, governments but also media.

Due to application scenarios implemented via interconnected devices in all relevant areas, the network of interconnected things is going to be dynamically shaped. That is, things will join and leave the network, different levels of trust will be maintained and various levels of information confidentiality need to be supported. The negotiating mode of interaction is a complex issue per se. By considering the existence of malicious motives in this interaction, it becomes apparent that attack potential grows and that prevention will be a great challenge. Let alone that security functions supported are rudimentary, yet immature. As an additional dimension to the technical one, one should calculate the immense potential that social engineering attacks may have. Information from private/intimate environments smart environments would turn a phishing message to a powerful attack that is difficult to defend[405,407]. Due to the importance of this area for cyber security, in the reporting period ENISA has performed a dedicated threat assessment by means of a threat landscape for of smart homes and converged media[409].

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

	Emerging Threat	Threat Trend
1.	**Malware: Worms/Trojans**	↑
2.	**Web based attacks**	↑
3.	**Phishing**	↑
4.	**Exploit kits**	↑
5.	**Information leakage**	↑
6.	**Insider threat (unintentional activity, information misplacement, misconfiguration errors)**	↑

[405] http://www.gtcybersecuritysummit.com/2015Report.pdf, accessed November 2014.
[406] http://www.gamingtechlaw.com/2014/11/top-5-takeaways-connected-cars.html, accessed December 2014.
[407] http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf, accessed November 2014.
[408] http://insct.syr.edu/wp-content/uploads/2014/03/Managing_Cybersecurity_Threats_Capstone.pdf, accessed November 2014.
[409] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/threat-landscape-for-smart-home-and-media-convergence/, accessed December 2014.

https://t.me/learningnets

	Emerging Threat	Threat Trend
7.	**Web application attacks / Injection attacks**	↑
8.	**Physical theft/damage/loss**	↑
9.	**Identity Theft**	↑
10.	**Denial of Service**	↑

Legend: ↓ Declining, ➲ Stable, ↑ Increasing

Table 9: Emerging threats and their trends in the area of Internet of things/interconnected devices/smart environments

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

- Internet of thinks and smart environments in particular consist of an increased number of interconnected sensors and devices. The increased number of interlinked functions and activity logs present and active will be a source of close, granular and intimate data on the activities and behaviour of inhabitants and visitors. Hence, when approaching or even connecting to such networks, emitted "data noise" from those devices may provide potential attack surface that can be misused in a great variety (e.g. phishing[410], misuse of trust, manipulation of information[405], denial of service[411], etc.). Moreover, due to the fact that smart environments are tightly related to personal consumption profiles, it is expected that they will be in the focus of individualized/targeted marketing and sales campaigns[412].
- The smart home is a point of intense contact between networked information technology and physical space. This will create new yet unknown threat and vulnerability models that are result of bringing together both the virtual and physical contexts. An example is the existence of assisted living for ageing population: through the ability to track movements into the home or city environment, this user group might be vulnerable to physical attacks[413]. Let alone attacks to medical records that are in general in the rise, due to their potential in fraudulent activities[414].
- The user interaction within smart environments will converge logically[415]. As regards the device to manage converged information, this will probably be a mobile device or TV-set. In both cases, these devices will attract the interest of adversaries. Having already sufficient cyber-threat capabilities for mobile devices (see also section 6.2), adversaries will be in the position to successfully attack important control functions of smart environments[416]. Given the fact that

[410] http://blogs.mcafee.com/consumer/internet-of-things-cyberattack, accessed November 2014.
[411] http://www.mostafafouda.com/Pub/Conf/2010.ICCES%2710.pdf, accessed November 2014.
[412] http://www.clickz.com/clickz/column/2347810/smart-homes-a-new-marketing-paradigm, accessed November 2014.
[413] http://www.igi-global.com/chapter/wireless-technologies-ambient-assisted-living/47126m, accessed November 2014.
[414] http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf, accessed October 2014.
[415] http://www.pocket-lint.com/news/127614-first-ios-in-the-car-integration-to-come-next-week-ferrari-volvo-and-mercedes, accessed November 2014.
[416] http://www.leaderpost.com/life/Hackers+show+auto+industry+trade+secrets/10425446/story.html, accessed December 2014.

https://t.me/learningnets

logical convergence of technology will happen via a variety of interfaces, intercepting data traffic will be yet another attack vector[417,418].

- Given economic factors in the development and manufacturing of internet of things components, weak implementation of security controls will be encountered[419]. Moreover, given the untested interplay of components of different classes and of different manufacturers, the effectiveness of existing security controls is uncertain. Certification certifications of devices with regard to the basis security characteristics - similar to the ones existing in the area of electrical, low voltage equipment[420] - might need to be developed in the middle term. Existing documents regarding certification of smart environments are either outdated or cover particular segments of the entire environments (e.g. CENELEC[421], IEC[422]).
- Current published ENISA incident statistic from the area of telecommunication, shows that ca. 20% of outages of professionally operated networks are caused by human errors [423] (e.g configuration mistakes). This is indicative for the role of humans in the configuration and operation of complex systems. Yet not being as complex as professional networks, interconnected devices and smart environment will constitute a significant challenge unexperienced users controlling them. Hence humans will remain the weakest link also within smart, interconnected environments[405].
- A further interesting issue within interconnected devices and smart environments is the possibility of conflicting interests among asset owners of the environment. For example, media content owners may view occupants' attempts to access licensed media content through alternate channels as a threat to their assets, whilst occupants may interpret digital rights management measures as barriers preventing them from accessing their assets. Different service providers and technology vendors may be in competition with each other for both bandwidth and data. Further conflicts may arise in cases of conflicts among owner and occupant: in cases of disputes, for example, occupants may have an interest in breaching privacy of owner; occupants may lock access to home appliances after leaving the house. Similar conflicts may arise within neighbourhoods. In such situations, additional threat agents to smart environments may emerge, whose motives and capabilities are difficult to foresee.

6.7 Network Virtualisation and Software Defined Networks

Network virtualisation (NV) is a technology based on combination of network hardware with software into a single virtualized system, i.e. a virtual network. Virtual networks are administered via a single software and offer network resource virtualisation [424], [425]. Network virtualisation exists in two

[417] http://www.spiegel.de/auto/aktuell/hacker-koennen-autos-ueber-funkverbindungen-aus-der-ferne-angreifen-a-985464.html, accessed November 2014.
[418] http://securityaffairs.co/wordpress/22070/hacking/can-hacking-tools.html, accessed November 2014.
[419] http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwordsm, accessed November 2014.
[420] http://www.ce-marking.org, accessed November 2014.
[421] http://www.ictsb.org/activities/Smart_House/Documents/Annex_Authent.pdf, accessed November 2014.
[422] http://webstore.iec.ch/preview/info_iec62045-1%7Bed1.0%7Den.pdf, accessed November 2014.
[423] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013/at_download/fullReport, accessed November 2014.
[424] http://en.wikipedia.org/wiki/Network_virtualization, accessed November 2014.
[425] http://searchsdn.techtarget.com/definition/network-functions-virtualization-NFV, accessed November 2014.

https://t.me/learningnets

variations, one being external virtualisation and the second internal virtualisation. While the former aims at the creation of virtual networks based on a number of physical networks (LANs), the latter supports emulating a network system with software. External virtualisation is mainly an administrative function that allows the creation of virtual networks (VLANs) out of a number of physical networks. Internal virtualisation is used to optimise efficiency of resources. Software defined networks (SDN) come to build upon network virtualisation: while network virtualisation created virtual networks, software defined networks come to perform changes to virtual networks according to user needs[426,427,428].

In a similar fashion to the virtualisation of computing through could, network virtualisation and SDN are the enablers for the development of a business model called network-as-a-service (NaaS)[429]. Hence virtualisation of network and SDN will be put at a similar basis to could computing, where network configuration and usage will be offered as an on-demand service. Combined with virtualized computing, NV and SDN will offer a perfect model for cost reduction and elasticity. While some argue that network virtualisation and SDN will bring advances to network security[430], there are concerns about security issues of such a virtual infrastructure[431,432]. All in all, one should note that security analysis (threat, risk assessment) of NV and SDN is still in early phases and standards and products are at early maturity stages. This is a reason for considering NV and SDN as an emerging security area.

Top (preliminary[433]) emerging threats to CPS are:

	Emerging Threat	Threat Trend
1.	**Denial of service attacks (central control plane, hypervisor, e.g. through packet flooding)**	↑
2.	**Malicious code: Worms/Trojans (infection of central control plane, switches)**	↑
3.	**Web application /Injection attacks (components of control functions written in Java Script)**	↑
4.	**Insider threat (intentional, unintentional)**	↑
5.	**Physical damage/theft/loss**	↑
6.	**Phishing (as instrument to infect IT, steal identity information)**	↑
7.	**Identity theft/fraud**	↑

[426] http://www.networkworld.com/article/2174268/tech-primers/understanding-the-differences-between-software-defined-networking-network-virtualizati.html, accessed November 2014.
[427] https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-sdn-nvf-solution.pdf, accessed November 2014.
[428] http://www.storagecraft.com/blog/network-virtualization-security-benefits-risks-best-practices/, accessed November 2014.
[429] http://www.cloudcomputingadmin.com/articles-tutorials/naas/naas-future-networking-cloud-based.html, accessed November 2014.
[430] http://www.networkworld.com/article/2606388/virtualization/how-network-virtualization-is-used-as-a-security-tool.html, accessed November 2014.
[431] http://searchsdn.techtarget.com/news/2240214438/SDN-security-issues-How-secure-is-the-SDN-stack, accessed November 2014.
[432] https://www.sdncentral.com/security-challenges-sdn-software-defined-networks/, accessed November 2014.
[433] Assessed threats for this area are assumed by extrapolating top threat to assets involved in NV and SDN. Due to the early stages of action in this area, these threats are rather indicative. More thorough assessments in those areas will need to be performed.

https://t.me/learningnets

	Emerging Threat	Threat Trend
8.	**Information leakage**	↑
9.	**Cyber espionage**	↑
10.	**Data breaches (network management information or network traffic being breached)**	↑

Legend: ↓ Declining, ➲ Stable, ↑ Increasing

Table 10: Emerging threats and their trends in the area of network virtualisation and SDN

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

- NV and SDN are based on centralisation of control of network covering management and data flow issues. As such, these components are single point of failure. Having the entire intelligence of the network concentrated at one position, failures may affect the entire network. Hence, denial of service attacks on a variety of underlying network components may affect the central control functions (e.g. through coupling over data exchange with network switches). Besides direct DoS attacks to the central control panel, flooding attacks may have similar failure effects[434].
- NV and SDN have taken care of security issues. However, the prevailing standard OpenFlow has not been developed with the "security by design" principle. Moreover, due to the complexity of the environment and multiplicity of supported devices, vulnerabilities found in network hard- and software may impact availability and functionality of the entire environment. Given the existing variety of vulnerabilities/attacks for network hardware[435] and software (references taken just as examples) [436,437], it is evident that careful selection and maintenance of network soft- and hardware are key for the security of the environment.
- NV and SDN technologies are a promise towards quality of service, performance and facilitation of network management. Yet, both existing standards and released technology are at early stages of adoption and maturity; they still include a lot of vendor own product philosophy and specificities. It remains to be seen what the uptake of this technology will be, what are going to be the prevailing business models and what kind of vulnerabilities, attack vectors and security issues in general will be surfaced. At the time being, the need for more detailed security assessments for this technology is rather evident.
- Although NV and SDN will bring new exploitation potential for network functions, they are also going to facilitate implementation of a number of important network security functions[430]: firstly, centralisation of control will increase coherency of management activities; virtual firewalling will allow for a better protection of network and application assets; more flexible packet filtering techniques will be implementable, for example regarding DDoS attack detection and mitigation;

[434] http://www.nil.com/2014/watch-the-presentation-security-and-sdn-a-perfect-fit-or-oil-and-water/, accessed November 2014.
[435] http://www.informationclearinghouse.info/article38485.htm, accessed November 2014.
[436] http://h17007.www1.hp.com/docs/advisories/HPNetworkingSecurityAdvisory-OpenSSL-HeartbleedVulnerability.pdf, accessed November 2014.
[437] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-nat, accessed November 2014.

https://t.me/learningnets

IDS and IPS can be configured and operated in a more efficient way. Just as cloud computing security, NV and SDN security will be part of the services and hence more affordable and transparent to customers.

- Page intentionally left blank

https://t.me/learningnets

ETL 2014: Food for Thought: Lessons Learned and Conclusions

https://t.me/learningnets

7 Food for Thought: Lessons Learned and Conclusions

7.1 Lessons learned

Lessons learned from another year of ENISA threat landscape are a collection of points regarding both advances observed and deficiencies assessed. These points constitute highlights and are thought of as potentially interesting points for individuals/organisations that are engaged in threat analysis/threat intelligence. These points are divided in two categories:

- *Lessons from the performance of ETL process within ENISA*: These are points regarding our internal information collection and analysis exercise. This list might contain interesting points for stakeholders performing threat analysis or consuming threat information; and
- *Lessons learned from the analysed content*: These are points regarding conclusions drawn from collected and analysed content. This information might be interesting for any stakeholder from the target group of this report.

Lessons from the ETL process:

- The "publicity" of threat information in related media is quite high. Threat landscape reports are important elements in the cyber-security community. Information on cyber-threats are quickly taken up by media. The number of publications has significantly increased in the reporting period. In the future it will be necessary to establish cooperation (consolidate efforts) among various players in the field to avoid duplication of work and increase quality of assessments[438].
- Tools and methods to support the collection and analysis process depend on the level of detail/quality of the threat assessment. Tool landscapes for strategic, tactical and operational information differ. Currently available tools are oriented towards collection of operational information. It is important to understand level and structure of threat information and set up environment, processes and tools accordingly.
- As the amount of threat information grows, it is important for the collection process to:
  - Find a simple classification scheme for identified resources. This may contain information on focus/scope, role of information assessor, kind of input and output data, etc.
  - Maintain some tools to locate and store this kind of information in an (semi-) automated manner (i.e. scanning information, storing relevant information in a structured way).
- Given the fact that an increasing number of projects/activities cope with cyber threats, the creation of a taxonomy for cyber-threats would facilitate at least internal communication and would establish a common denominator throughout all relevant efforts. Such a taxonomy would be an important point of consolidation of acquired knowledge.
- It is very important to understand what the counterparts of threat information are, what user needs it can serve, and how this information can be disseminated to the various stakeholder groups. A proper dissemination strategy needs to be developed.
- The state of maturity of various concepts and approaches followed can be characterized as initial. Triggering the dialogue among threat collection organisations is very important as it

[438] http://www.societalsecurity.eu/uploads/Articles/2014_Boin%20Ekengren%20Rhinard_Sensemaking_FHS%20Book.pdf, accessed November 2014.

https://t.me/learningnets

would lead to cross-fertilisation of ideas and will lead to a common understanding with regard to emerging issues for threat analysis.

- It would be important to elaborate on methods to classify importance of threats based on some prioritisation criteria. These should be based on impact, sector, detections, reported incidents, etc. Information collection could then be facilitated according to the importance criteria at scope. Similar exercises for the identification of threat trends might also be of use in building threat intelligence.

Lessons from the analysed content:

- Sloppiness with cyber-security continues to be number one reason for breaches (over 50%). This is a finding for the third year in sequence and should be an alarming signal for all stakeholders involved in cyber-security.
- Threat analyses and assessments performed by various vendors/organisation should state more clearly the scope of the assessment. This would facilitate the understanding of the assessed information and would facilitate usage of the material.
- Threat analysis and achieved results are rather complex. Ways to transfer this complex knowledge to less skilled stakeholders is key to a better uptake of produced results. In other words, cyber-security community could mitigate "sloppiness" by playing their role in the education knowledge transfer chain.
- Information collection from the dark net could be interesting. Knowing that some stakeholders are performing this kind of information collection, it would be useful for the entire stakeholder community to communicate information found more directly.
- It is difficult to compile collected information to cover the entire causal chain of: Threat Agent->Attack vector->Cyber threat->Asset->Vulnerability->Damage. This information is very useful for end-users of threat information/threat intelligence.
- Good practices on agile SIEM methods will be very important for "consumers" of threat intelligence (i.e. use of big data). Moreover, it is important to understand the role cyber-threat and the resulting cyber-risks within a security management process[439]. It might be interesting to elaborate on such issues both at the level of vendors and standardisation bodies.
- Both quality and quantity of collected information has significantly increased in the reporting period. This is a very positive development that has as a result better threat assessment and the availability of more detailed material to be used by end-users. The increase in quantity, however, has to be effectively surfaces during information collection, e.g. by the adoption of more systematic information collection practices (see also related point in process lessons above).
- ETL self-test: In the reporting period we were in the position to "test" own and other predictions made in 2013. The comparison has been made within ETL 2013[7]. We have found out that the majority of predictions – both by means of emerging trends and collusions - for 2013 were realistic.

[439] http://cryptome.org/2014/10/csan-4.pdf, accessed November 2014.

https://t.me/learningnets

7.2 Conclusions

The threat landscape in 2014 has undergone significant, partially impressive developments. Conclusions drawn in this year's ETL are based on these developments and, towards a more clear classification of their context, are divided into two categories, namely technical and policy/business related (sequence of the points below is not prioritised).

Policy/business related conclusions:

- Europe, in its role as a world leader in data privacy, should continue with setting up the standards in this area. Besides contributing to increasing the currently diminishing trust in digital life, this is a strong opportunity: it can turn it to a competitive advantage for many industry sectors related to the provision of digital services. And can have a worldwide impact on the cyber-threat landscape.
- Cyber-security and resilience of Cyber Physical Systems is another opportunity for Europe. Bridging engineered systems and cyber-space will be a significant field of growth. Europe should take advantage of strong engineering capabilities to gain a foothold in this area. Combining advances in data protection, resilience and cyber-security, this area can be a significant source of innovation and competitiveness.
- Current revelations regarding the activities of national security agencies and their role in affecting the cyber-threat landscape have increased fragmentation risks for the internet (i.e. Balkanisation of the internet[440]). A potential materialisation of this risk could threw current state of internet and cyber-security many years back. Further, such a risk would greatly impact cyber-threat landscape.
- Surveillance is affecting cyber-threat landscape, at least from end-user perspective and has a negative impact to the trust in the internet[441]. Governments are challenged to follow up on technological developments with regulations establishing a balance between the technically possible and legally transparent. In the middle term, governments will need to come up with improvements of transparency rules for their surveillance measures[405,442].
- The unknown number of breaches and security incidents is a major concern of security experts and in particular of law enforcement. Breach notification needs to be put on a wider basis via corresponding regulations in various areas/sectors, eventually covering end-user impact. This will help assessing the currently large grey numbers assumed.
- New, sophisticated attacks make the development of new defences necessary. Development of new detection methods and new security controls is an area of innovation. Examples of such innovative controls are proactive detection of websites before they turn malicious[443], or identification of anonymous writers from their writing style[444]. Advanced attack methods is

[440] http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet, accessed November 2014.
[441] http://www.bbc.com/news/technology-30115679, accessed November 2014.
[442] http://www.nytimes.com/2014/11/26/world/un-urges-protection-of-privacy-in-digital-era.html?_r=3, accessed December 2014.
[443] https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-soska.pdf, accessed November 2014.
[444] https://www.eecs.berkeley.edu/~sa499/papers/oakland2014-underground.pdf, accessed November 2014.

https://t.me/learningnets

another area of innovation[445]. Academia and businesses should invest in such attack methods and controls to increase innovation and competitiveness in the relevant market.

Technical conclusions:

- Sophistication of cyber threats continues increasing. We see currently defence practices from the past losing efficiency (i.e. classical signature based Anti-Virus). It is an undoubtable fact that advanced attack methods currently used within cyber-espionage attacks are the best "food" for cyber-criminal's learning curve. Methods used by high capability threat actors today are adopted by cyber-criminals tomorrow. This increases challenges in development of defence practices.
- Partial take down of malicious infrastructure (i.e. botnets) has created a discussion about their purposefulness. Do we have a similar case here as in medicine, where increased use of antibiotics might create more resistant viral strains whose protection is not yet possible with available means?
- Trust infrastructures are under massive stress. Both open and "closed" source implementations of basic security functions have been challenged. Shortly before finishing this report, even TOR has allegedly been "de-anonymised". What comes next? For sure that the entire cyber-community and in particular cyber-security experts should worry about the robustness of the trust infrastructure.
- A definition of purpose of data usage seems to be the solution for data breaches not only for the cloud, but throughout all processing/storage platforms. This would set the basis for a proper data protection and management, while facilitating resolution of security issues of big data.
- Threat modelling, threat intelligence over big data and setting up a novel, yet flexible security architecture are emerging practices in coping with the dynamics of the threat landscape. It remains to be seen how these novel approaches are going to reach smaller organisations with reduced knowledge and resources. Are standardisation bodies going to follow these trends? And if yes, when?
- Big data, social media, mobile computing and interconnected devices, when not properly used/protected will constitute the perfect knowledge-base for cyber-criminals, allowing for perfectly crafted, difficult to detect phishing and other targeted attacks.

[445] http://www.wired.com/2014/11/airhopper-hack/, accessed November 2014.

https://t.me/learningnets

TP-AE-14-001-EN-N

ENISA Headquarters
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

ISBN: 978-92-9204-112-0
ISSN: 2363-3050
DOI: 10.2824/061861

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

https://t.me/learningnets