ENISA

CURRENT THREAT + LANDSCAPE EMERGING

ETL 2013

ENISA Threat Landscape 2013

Overview of current and emerging cyber-threats

11 December 2013

enisa

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

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.

ISBN: 978-92-9204-120-5 ISSN: 2363-3050 doi:10.2824/022950

Executive summary

The year 2013 has brought big news, significant changes and remarkable successes in the cyber-threat landscape. Among the dynamic developments and changes that happened, there is one thing that has remaained stable: the race between defenders and adversaries has continued and will continue in the future.

Over 250 reports and sources have been analysed for this year's report. From a threat landscape perspective, 2013 has brought good and bad developments. Let's start with the bad:

- Threat agents have increased sophistication of their attacks and their tools.
- It has become clear that maturity in cyber activities is not a matter of a handful of nation states. Rather, multiple nation states have now developed capabilities that can be used to infiltrate all kinds of targets both governmental and private ones in order to achieve their objectives.
- Cyber-threats go mobile: attack patterns and tools that targeted PCs a few years ago, have been migrated to the mobile ecosystem.
- Two new digital battlefields have emerged: big data and the Internet of Things.

But 2013 has also brought us important good developments. Positive developments observed in 2013 in the area of cyber-threats include:

- Impressive successes by law-enforcement have been achieved. The police has arrested a gang responsible for the Police Virus. The Silk Road operator has been arrested and the platform has been shut down. The developer and operator of Blackhole, the most popular exploit kit, has been arrested.
- The number of reports and data regarding cyber-threats has increased and so has the quality of available information. This has facilitated threat analysis.
- Vendors have increased the speed in which they respond to threats and vulnerabilities via updates of their products.
- Cooperation among relevant organisations to commonly assess and defend cyber-threats has been envisaged and is going to gain speed in the near future.
- Issues related to industrial espionage and state sponsored surveillance became a major discussion topic during this reporting period. The ENISA Threat Report takes account of these issues to the extent that these activities are related to assessed cyber-threats. It should be noted however that, apart from providing guidelines on how to protect systems against the technical threats enumerated, any additional response to industrial espionage and state sponsored surveillance is not in ENISA's mandate.
- The present document targets security professionals, decision makers, media and all other interested individuals interested in obtaining information on threats and threat trends for emerging technology areas.

Hopefully, lessons learned and conclusions drawn will help streamlining activities in the stakeholder community. ENISA will capitalize on this knowledge and will inject it into the activities of forthcoming ENISA Work Programmes:

- Actively involve end-users in defence of cyber-threats;
- Increase cyber-threat intelligence by creating and disseminating appropriate knowledge and by coordinating activities of relevant organisations;
- Increase the speed of threat assessment to reduce exposure;
- Invest in research to enhance appropriateness of security policies and security controls.

In the figure below, an overview of the top 15 assessed current threats and threat trends for emerging technology areas are being presented. Much more information can be found in the report.

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Critical Infrastr.	Mobile Computing	Social Networ-king	Cloud Compu-ting	Trust Infrastr.	Big Data	Internet of Things
1. Drive-by Downloads	↑	↑	↑	↑		↑	↑	
2. Worms/ Trojans	↑	↑	↑	↑	↑	↑	↑	↑
3. Code Injection	↑	↑	↑	→	↑	↑	↑	
4. Exploit Kits	↑	→	↑	↑	↑	↑	↑	
5. Botnets	→	↑	↑	↑	↑			
6. Physical Damage/Theft /Loss	↑	↑	↑	↑	↑	↑	↑	↑
7. Identity Theft/Fraud	↑		↑	↑	↑	↑	↑	↑
8. Denial of Service	↑	↑			↑			↑
9. Phishing	↑	↑	↑	↑	↑	↑	↑	↑
10. Spam	→			↑				↑
11. Rogueware/ Ransomware/ Scareware	↑							
12. Data Breaches	↑		↑		↑	↑	↑	↑
13. Information Leakage	↑	↑	↑	↑	↑	↑	↑	↑
14. Targeted Attacks	↑	↑				→	↑	↑
15. Watering Hole	↑							

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

Table 1: Overview of Threats and Emerging Trends of the ENISA Threat Landscape 2013[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 5). Arrows that show a stability in a threat may be increasing in emerging areas. This is because current threat landscape includes all threats independently from particular areas.

Table of Contents

1 Introduction

This document is the 2013 ENISA Threat Landscape (ETL 2013). The ENISA Threat Landscape is a reporton significant cyber-threats that have been assessed in the reporting period, i.e. within 2013. Moreover, the ENISA Threat Landscape delivers predictions for threat trends regarding emerging technology areas. The work on the ENISA Threat Landscape has been performed as part of the ENISA Work Programme 2013 under the Work Stream "*Evolving risk environment & opportunities*".

The objective of this work is to provide stakeholders with information about developments in the cyber-threat landscape and to identify threat trends for the near future, ie in the coming year. For the prediction of trends, important areas of IT innovation and development were taken as a basis. The assessed top threats from 2013 are mapped to these areas and thus an emerging threat landscape is created.

ETL 2013 is based on a comprehensive information collection of publicly available open source material. Reports of various kinds (i.e. content, context, level of detail, subject areas, etc.) are collected over the entire reporting period. These reports are parsed to identify relevant content, such as threats, threat agents and trends. The collected information is collated and consolidated. In 2013, a large number of such reports have been collected (over 250). They span the period beginning end 2012 up to the publication date of this report, ca. end of November 2013. Reports appearing after this period will be considered in the next year's ETL, to be delivered around the same period in 2014.

In a similar fashion as in last year's report, ETL 2013 includes:

- A *Current Threat Landscape* consisting of contemporary developments of cyber-threats as they have been reported by national and international stakeholders such as CERTS/CSIRTs, industry, governmental organisations, networks of excellence, academia, press and individual security experts;
- An Emerging Threat Landscape consisting of threat trends identified for a number of areas/sectors with high levels of innovation and market potential and,
- Identification of *Threat Agents* being the main source of assessed cyber-threats.

Issues related to industrial espionage and state sponsored surveillance became a major discussion topic during this reporting period. The ENISA Threat Report takes account of these issues to the extent that these activities are related to assessed cyber-threats. It should be noted however that, apart from providing guidelines on how to protect systems against the technical threats enumerated, any additional response to industrial espionage and state sponsored surveillance is not in ENISA's mandate.

In this year's ETL, we have introduced the concept of "attack workflow", indicating how assessed threats are being deployed by threat agents within an attack. This information is considered as important because it delivers information on how threats, the malicious tools of adversaries, are being used in order to set up a successful attack.

Lessons learned and conclusions are indicating future actions for the cyber-security community in order to achieve good progress in the subject of threat analysis and trend identification. In forthcoming ENISA activities, these issues will be taken into account as a contribution in improving cyber-security capabilities of all involved stakeholders.

Policy Context

The Cyber Security Strategy of the EU[2] 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 regulation, in particular by contributing to the identification of emerging trends in cyber-threats and understanding the evolution of cyber-crime (see 2.4 regarding proposed role of ENISA).

Moreover, the new ENISA regulation[3] mentions the necessity 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 EU Cyber Security Strategy by streamlining and consolidating available information on cyber-threats and their evolution.

Target audience

The target groups of this document are all specialists/individuals who are concerned with the development/evolution of threats in cyber space: primarily security experts interested in assessing the "external environment" and "Internal environments"[4] in the framework of threat and risk assessments. This information might be interesting when formulating security policies or creating protection profiles. Finally, interested decision makers and users of IT components may find information in order to make informed decisions towards investment for the protection of potentially valuable assets or to define their risk appetite.

ETL 2013 will be of interest for policy makers: current threats and threat trends may be important input in policy actions in the area of cyber-security, national cyber-security preparedness and possible coordination and cooperation initiatives.

Through the large number of collected reports, ETL 2013 provides a unique collection of information regarding cyber-security threats. Hence, a further target group of this document consists of individuals who would like to obtain access to these sources in order to use them for their own purposes.

Last but not least, and as experience with ETL 2012 has shown, the threat landscape is an important piece of information for media as it provides to non-security experts information to understand dependencies and developments in the area of cyber-security. Moreover, it serves as a continuous source of information to better analyse and understand the whereabouts of incidents in the area of cyber-security.

Structure of this document

The structure of ETL 2013 is as follows:

[2] 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.
[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF, accessed 28 Nov 2013.
[4] 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.

In the chapter entitled "*Purpose Scope and Method*" we provide information about the scope of this work, methods followed in the process of information collection, the position of ETL within the risk assessment and risk management process and, finally the terminology used.

The chapter "*Overview of Threat Agents*" provides information about the cyber-adversaries. It provides information about their motives and capabilities. Moreover, it shows what kinds of threats are assumed within each threat agent group.

The chapter "*Current Threat Landscape*" provides information about the top 15 threats assessed this year. For each threat a short description is provided, together with a number of issues concerning developments within this threat. Moreover, the trends, other related threats and a graphical representation of the threat within the attack workflow/kill chain are presented.

The chapter "Emerging Threat Landscape" provides information about threat trends in emerging technology areas. For each emerging area, the top 10 threats are mentioned together with the corresponding trends. Following this, a number of emerging issues related to threats and cyber-security in general are also delivered.

Finally, ETL 2013 is concluded by the chapter "*Food for Thought: Lessons Learned and Conclusions*". In this chapter the summarized experience in performing this task for a second year is being presented, together with the conclusions showing open issues and future activities in the subject matter.

At this point it should be stressed that particular emphasis was given to keeping ETL 2013 as modular as possible. Chapters of this document have been developed in a way to comprise content modules that are as independent as possible. The objective behind this decision is to enable selective updates of the content of each module: should, for example, a midyear current threat landscape be developed, the corresponding chapter can be taken as basis for the relevant updates. This will save resources and maintain the consistency of the entire content.

Page intentionally left blank

ETL 2013: Purpose, Scope and Method

2 Purpose, Scope and Method

2.1 Purpose of ETL

The purpose and positioning of the ENISA Threat Landscape (ETL) has been documented in ENISA's 2012 deliverable "ENISA Threat Landscape: Responding to the Evolving Threat Environment"[5] (also referred to as ETL 2012 in the rest of this document).

In this year's ETL, we will give an overview of its purpose by highlighting the major objectives to be met by this document[6]. It is worth mentioning, that through the learning curve we have been through in two years of ETL, some shifts/improvements in our practices have been introduced. These developments are also reflected in the present chapter.

The purpose of ETL is to provide answers to the following key questions with regard to threats in cyberspace and the purpose of ETL:

What is a threat landscape?

A threat landscape is a collection of threats. This information contains identified threats, trends observed and threat agents involved. ETL consists of a list with top threats prioritized according to the frequency of appearance and NOT according to the impact caused. The reason for this approach is that we do not see ourselves in the position to objectively decide about impact levels. As explained below in this section, this is a task that has to be left to the discretion of the asset owner.

Why does the threat landscape change?

The threat landscape, also called threat environment[7,8,9,10,] is a dynamically changing ecosystem. Main forces contributing to these changes are: increased complexity of IT-products, various external forces such as financial crisis, new vulnerabilities, sophistication of available tools and attacks, available resources (both personnel and monetary), available skills, networks enabling knowledge transfer and growth of illegal profits in cyberspace.

How many kinds of threat landscape exist?

Various types of threat landscape exist, depending on their orientation with regard to threatened assets and with regard to the time horizon taken into account. Examples of sector oriented threat landscapes are: a financial sector threat landscape, CIIP threat landscape[11], health sector threat landscape[12]. Examples of threat landscapes taking into account time are: current threat landscape[13], emerging threat landscape[14], future threats[15]. Of particular importance are emerging threat

[5] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport, accessed 18 Oct 2013.
[6] Individuals interested in the details of ETL purpose may also refer to chapter "3 Scope and Definitions" of ETL 2012.
[7] http://www.fbi.gov/news/testimony/protecting-the-nation-in-todays-complex-threat-environment, accessed 21 Oct 2013.
[8] http://defensetech.org/2010/01/11/the-2010-cyber-threat-environment/, accessed 21 Oct 2013.
[9] http://www.symantec.com/connect/blogs/changing-threat-environment-requires-mssps-adapt-their-approach, accessed 21 Oct 2013.
[10] http://securityintelligence.com/keeping-up-with-the-changing-threat-environment/, accessed 21 Oct 2013.
[11] An ENISA deliverable on Smart Grid Threat Landscape is going to be published soon. The URL is going to be added as far as it is available.
[12] http://www.verizonenterprise.com/DBIR/2013/industries/, accessed 21 Oct 2013.
[13] http://www.trendmicro.com/us/security-intelligence/current-threat-activity/, accessed 21 Oct 2013.
[14] http://gtsecuritysummit.com/pdf/2013ThreatsReport.pdf, accessed 21 Oct 2013.
[15] https://www.europol.europa.eu/content/facing-future-cyber-threats, accessed 21 Oct 2013.

landscapes as they reflect threat exposure of deployments of new technology, often characterised by a low maturity regarding technical vulnerabilities.

What is the content of ETL?

ETL contains a summary of the current threat landscape and an emerging threat landscape. The current threat landscape contains consolidated, prioritized list of threats that have been identified by collecting publicly available threat information (see Chapter 3). The emerging threat landscape presents threat trends in various key areas of information technology. Moreover, ETL provides information on threat agents.

What has been left out from ETL?

In general, ETL is covering cyber-threats. Hence, threats resulting from the physical environment (environmental,deliberate human actions, etc.) are not considered within this document. In this year's threat landscape we have not included any geographical data on threat distribution. Also, threats that are not explicitly related to IT have been left out. Finally, attack patterns have not been included in this year's ETL. It is planned to cover these issue in prospective threat landscapes depending on stakeholder demand and resource availability.

How many reports have been analysed and how have they been collected?

ENISA has analysed over 250 sources for the present threat analysis. The sources collected were reports from private and public sector, information from blogs, discussions, prsentations, etc. They have been collected by using Open Source Intelligence (OSINT) methods (see also chapter 2.4).

2.2 Scope, Rationale and Structure of ETL

In order to identify required protection levels of valuable assets it is common to perform a risk assessment. Subsequently, security measures have to be introduced to achieve this protection by mitigating (part of) the assessed risks. Other risks might be transferred or accepted. As discussed below, threats are an important element in risk assessment.

In this chapter we present the scope of the ENISA Threat Landscape (ETL). It consists of a number of threats to which IT and IT related assets are exposed. Hence, the presented threat landscape is an important tool for those who want to assess the risks within an IT environment of any complexity. Based on these risks, appropriate security measures can be selected to achieve risk mitigation.

The role of threats in the risk assessment equations becomes evident when looking at the components of risks. According to the widely accepted ISO 27005 definition risks emerge when: "*Threats abuse vulnerabilities of assets to generate harm for the organization*". In more detailed terms, we consider risk as taking into account the following elements:

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

The elements of risks are graphically depicted in the figure below:

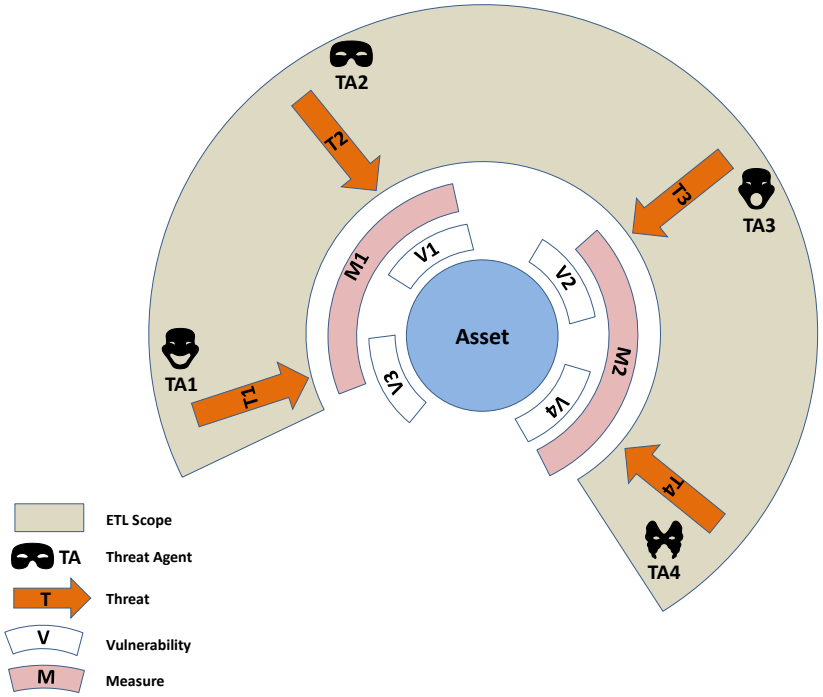


Figure 1: Threats targeting an asset by trying to exploit its vulnerabilities.

This figure has been adopted from ISO 13335-4 and shows how how threat agents (TA), deploying threats (T) , try to exploit asset vulnerabilities (V) in order to harm/take over the asset. The asset owner has implemented security measures (M) to protect the asset, that is, to eliminate negative effects from threat exposure. The impact achieved by the potential materialization of a threat is the final element to evaluate the risk of an asset (see also risk definition above).

While the definition of risks for an asset is a quite straight forward task, in complex environments it is often a challenge to assess risks. This is due to interdependencies between assets, cascading effects of vulnerabilities, dynamics in threat environment, capabilities of threat agents, attack methods, etc.

From the above becomes clear that in order to assess risks, all elements of the risk equation need to be available. ETL contributes to the understanding of the threat environment. With this information at hand, asset owners will be in the position to assess risks applying to the assets they own. We consider this as a win-win situation: ETL reflects changes in the dynamic threat environment to support the ones who own and master the complexity of assets.

In fact, ETL is asset agnostic- that is- it does not assume any particular environment and/or the processes implemented through it. The assessment of consequences of these threats to assets is left to the asset owner. To this extent, ETL is a supporting tool for the performance of risk assessments. Such a tool may be essential for the asset owner: the dynamics and main trends of the complex threat environment are key to the assessment of the inherently complex, interdependent assets.

In this document, we provide information on threats and threat exposure in a consolidated form compiled by analysing publicly available reports. In addition, we deliver information on how these threats behave within certain areas/domains. This is done in terms of a prioritization of threats and of identification of trends related to each area/domain.

2.3 Structure and focus of ETL 2013

For the the ENISA work programme of 2013, ETL consists of a general report on top threats and one-two threat landscape reports that "deepen" into specific domains/areas. The subject areas for the specialized, sector oriented threat landscapes are identified with the support of ENISA stakeholders. Finally, and in order to cover significant events in the area of cyber security, flash notes have been defined as part of this work. With flash notes[28], ENISA responds to important/high impact events with statements consolidating published information, while at the same time – when relevant - proposing mitigation/protection measures and/or establishing the context to activities at EU level.

In 2013, besides ETL (the present report), ENISA delivers two sector specific threat landscapes in the areas of Smart Grid[11] and Trust Services[16].

The structure of the ETL 2013 is presented in Figure 2 below. The process behind the creation of ETL is described in the forthcoming chapter (see chapter 2.4 below).

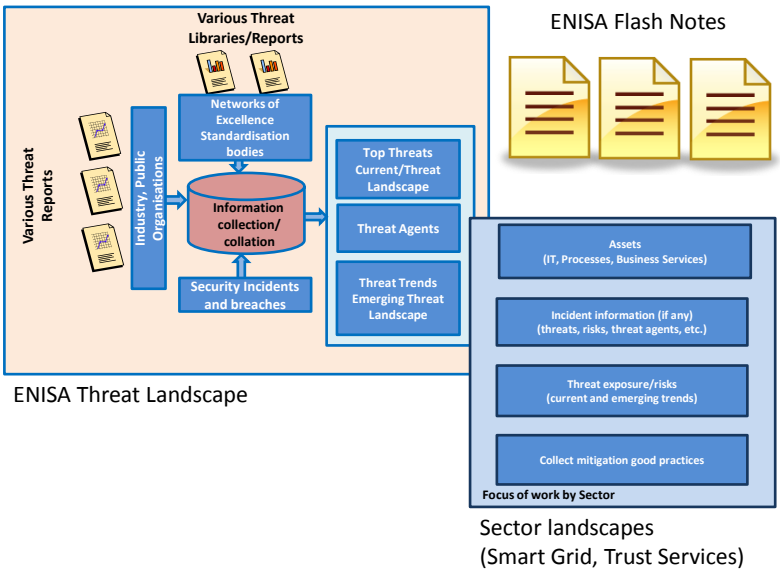


Figure 2: Structure and content of ETL stream of work within ENISA in 2013.

2.4 Methods and tools

The method followed for the creation of ETL is information collection, analysis and collation. As input to these activities solely public information is used. Hence, the method we follow goes beyond pure information research and uses the principles of Open-Source Intelligence[17] (OSINT): it serves the collection and dissemination of information to the appropriate audience in order to address threat exposure in cyber space[18] in a timely manner. Through this activity a basic level on intelligence on cyber threats can be achieved that can be used in various cyber security assessment activities.

[16] An ENISA deliverable on Tust Services is going to be published soon. The URL is going to be added as far as it is available.
[17] http://en.wikipedia.org/wiki/Open-source_intelligence, accessed 22 Oct 2013.
[18] http://www.gpo.gov/fdsys/pkg/PLAW-109publ163/html/PLAW-109publ163.htm, accessed 23 Oct 2013.

OSINT is not a new method and has been used by various groups, such as journalists, private companies and individuals. OSINT is particularly effective when collecting information about globally relevant events, such as cyber threats and comprises a good practice in this area[19,20,21]. This is because threat information can be identified timely and information from various sources can be cross-checked and combined in order to establish the desired context, that is, to understand an incident and find evidence about the whereabouts of the deployment and impact achieved. There are online tools related to OSINT[22,23,24]. In this year's ETL, available OSINT tools and their relevance/capabilities/content has not been assessed by ENISA.

The performance of open source search assumes a set of skills related with the ability to find, understand and validate required information[25]. The skills/challenges for open source searches are:

Understand who is knowledgeable: It is important to understand which sources provide what information and how to find and follow-up on these sources. Examples are knowledgeable individuals in social networking, blogs and online media. Due to the nature of threat information, it is crucial to track available information timely.

Evaluate quality and accuracy of information: In the technological area of cyber security, details matter. Hence, quality and accuracy of the collected information is an important attribute. It helps to spot ambiguity/bias and to understand the origin of a threat, weaknesses exploited and potential protection. This can be achieved via source validation[26].

Filter the identified information: Once qualitative information has been identified, it needs to be filtered in such a way to comply with the level, structure/attribution and context required for the purpose at hand. This can be achieved by parsing the identified information on the basis of structure/templates that reflect information requirements.

Find the right levels to store, associate and communicate: Once information has been filtered and properly structured, ways to store it need to be found in order to serve the usability criteria set. Moreover, both core and dynamic interconnections/relationships between stored information objects need to be maintained/identified for future use cases. Last but not least, it is important to find the right level and structure in order to present assessed information according to target group profile(s).

Just as during 2012, ETL 2013 is based on information from reports and publications issued by actors such as: Virus/Malware protection vendors; Information service of CERT-EU[27]; National security agencies; Industrial associations and standardisation bodies; Commercial companies in the area of cyber security; Networks of excellence; Academic institutions; Individual information security experts.

ETL information collection has been performed over the following channels: Online media; Web-based content and information services; Social media content; Publicly available reports and publications; Participation in relevant events; Discussions with various experts. It is remarkable that in this year's work, the channel of social media has proved to be very efficient in collecting

[19] http://resources.infosecinstitute.com/using-osint-in-your-business/, accessed 23 Oct 2013.
[20] http://www.infosecisland.com/download/index/id/109.html, accessed 23 Oct 2013.
[21] http://clusit.it/docs/Rapporto_Clusit%202013_ENG.pdf, accessed 23 Oct 2013.
[22] http://opensourcerss.net/, accessed 30 Oct 2013.
[23] http://searchsecurity.techtarget.in/photostory/2240160102/Nine-must-have-OSINT-tools/1/Nine-OSINT-tools-every-security-researcher-must-have, accessed 30 Oct 2013.
[24] http://cyber.law.harvard.edu/cybersecurity/Cybersecurity_Annotated_Bibliography, accessed 30 Oct 2013.
[25] http://www.theosintgroup.com/open_source_intelligence.html, accessed 23 Oct 2013.
[26] http://jeffreycarr.blogspot.co.uk/2013/11/in-osint-all-sources-arent-created-equal.html, accessed 2 Dec 2013.
[27] http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html, accessed 30 Oct 2013.

information. By following various individuals and organisations, we were able to become aware of issued reports and announcements very quickly.

Time matters in cyber security: the quicker an event has been spotted, reported and analysed, the less the impact and the quicker a weakness will be fixed. For this reason ENISA has introduced various ways of covering cyber security incident/threat announcements. Significant events are covered timely by means of flash notes[28]. Furthermore, as it was the case this year[29], ENISA issues midyear ETL reports in order to summarize important developments in threat landscape in the middle of the reporting year. Finally, around year's end the yearly ETL (the present document) is issued. It is worth mentioning that this dissemination strategy is still at the beginning and is currently under further development/evaluation/optimization.

2.5 Building Threat Intelligence: The Workflow of Attacks

As already mentioned in ETL 2012, building intelligence about cyber-threats is a consequent next step following threat and vulnerability analysis. This intelligence is related to the understanding of patterns that are common to attack scenarios. Hence the objective is to depart from simply listing threats and vulnerabilities and try to understand patterns that are characteristic for attacks: the workflow of attacks. In this workflow, threats, technical vulnerabilities, threat agents and user actions are being put in connection. The causal relationship between them provides an end-to-end perspective of all steps involved in an attack. Threat analysis - and in particular the identification of top threats - provides significant insights into the whereabouts of an attack, yet it does not make up the whole story. There are some additional elements making up an attack.

In various on-going activities in threat analysis and threat intelligence, approaches have been developed to allow for a coherent representation of all indicators, actions and actors involved in an attack[30,31,32]. This goes beyond the description of cyber-threats and includes information about the campaign, observations made, indicators, protection, incidents and targeted asset.

The proliferation of such approaches requires significant effort in building the context of an attack including information collection and analysis, incident data, threat agent information, exploitation strategies. Although all these issues are important for the development of threat intelligence, within the current version of ETL we consider as feasible to proceed with an initial step towards threat intelligence by adding to assessed threat some information about the *role* of a threat in the workflow of an attack. This will be performed by means of a marker (i.e. a bar spanning the relevant steps) in the attack workflow to indicate in which step of the attack a particular threat is being utilized. The use of attack workflows/kill chain is considered as a facilitator for building threat intelligence. There is a long way to go in this direction. It is proposed that relevant players elaborate further on this concept to provide more specialized information towards defending assets (see also conclusions at the end of this document).

For this purpose we adopt the work done in "Kill Chains"[33]. A kill chain is a set of generic steps characterising attacks. In particular, a kill chain consists of the following seven steps:

[28] http://www.enisa.europa.eu/publications/flash-notes, accessed 23 Oct 2013.
[29] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013, accessed 23 Oct 2013.
[30] http://stix.mitre.org/, accessed 27 Nov 2013.
[31] http://capec.mitre.org/, accessed 27 Nov 2013.
[32] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf, accessed 27 Nov 2013.
[33] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf, accessed 2 Dec 2013.

Reconnaissance: is the action of researching and analysing information about the target and the environment within which the attack will be deployed. In this phase, assumptions for the number and kind of vulnerabilities to be exploited are being made.

Weaponization: is the phase where the malicious payload to be used has been selected and "loaded", that is, made ready for use for the target environment.

Delivery: is the action of transmission of the malicious payload to the target environment.

Exploitation: is the act of letting the delivered payload make his job by exploiting vulnerabilities that are available in the target environment. Usually these are technical vulnerabilities but in some attacks these may well also be systemic or organisational vulnerabilities including humans.

Installation: is the phase where the delivered payload has successfully exploited a vulnerability and has been installed in the target environment.

Command and Control (C2): in this step the installed payload establishes outbound connection to the controller environment in order to enable interaction with the adversary who launched the attack.

Action on Objectives: this is the final phase of a successful attack where the threat agent is in the position to take over the targeted asset. Depending on the kind of target, this activity may include information retrieval, information manipulation, application misuse, etc.

The instrument of attack workflow has various use cases, depending on the available information on an attack (e.g. desktop analysis, reverse engineering based on an incident, tracking of malicious activities based on data, etc.). Within ETL, attack workflows (also referred to as kill chains) are used to indicatively determine the role of an assessed threat within the seven phases of an attack. Due to the fact that we take into account incident information but we do not perform incident analysis, the threat information delivered in this report will be merely mapped among the first 6 phases of the attack workflow. This is because ETL is based on desktop analysis and does not consider consequences of successful attacks (incidents) that took place in the reporting period. However, for some threats that inherently contain the targeted asset, step seven will be taken into account (i.e. Denial of Service, Physical Damage/Theft/Loss, Data Breaches and Targeted Attacks).

The role of a threat in the attack workflow will be presented graphically, as shown in the example of the figure below.

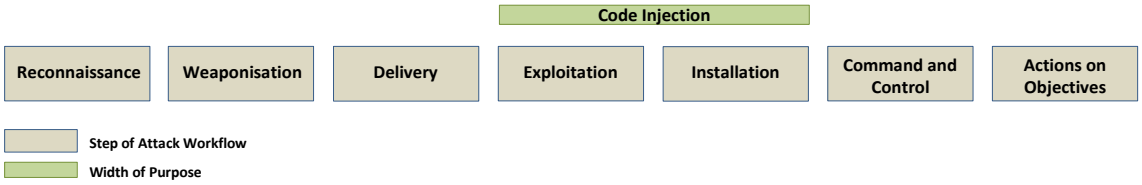


Figure 3: An example of attack workflow showing the role of Code Injection threat.

2.6 Used definitions

Just as in many complex areas, in cyber threat assessment wording matters. In the present 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 2012. In order to visualize the relationships among all elements of risks, we use a figure taken from ISO 15408:2005 (see Figure 4). 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 pattern is not displayed in this figure. Attack patterns have been left out of the scope of this report and will be subject of forthcoming work in the area of threat landscape.

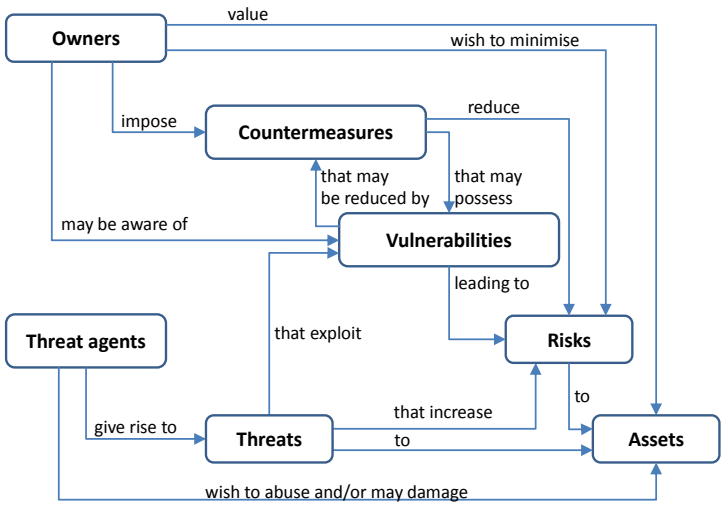
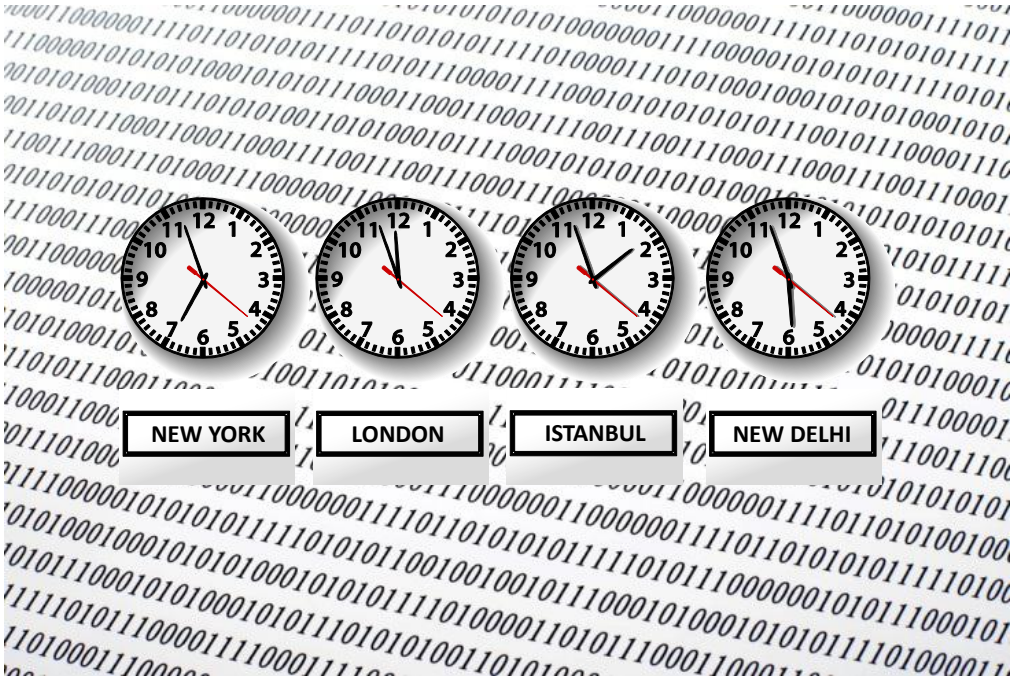


Figure 4: the elements of a risk and their relationships according to ISO 15408:2005

For risk, we use the definition given in section 2.2 above. It is worth mentioning that Figure 4 and Figure 1 have intentional redundancies: yet they serve a different view and together they complete the picture of the focus set and the terminology used in this report.

Page intentionally left blank

ETL 2013: Current Threat Landscape



3 Top Threats: The Current Threat Landscape

In this chapter we provide the top threats assessed from existing reports that have been analysed in the reporting period. The material presented is the *Current Treat Landscape 2013*. The assessment is based on reports that have been published until ca. mid of November 2013. Hence, the present report takes into account relevant publications and information that spans approximately one year (December 2012-November 2013). The remaining publications from this year will flow into the ETL 2014, eventually in form of a mid-year and an end year report.

As already stated, the assessed threats have been prioritized according to the frequency of their appearance/reference in corresponding reports. The references found are mostly based on detected incidents and infections. In some cases, they are based on estimated appearances of a threat, for example regarding spam and denial of service. In prioritizing these threats within a single list, the need to extrapolate those values arose. In the presentation of the threats below, more frequent threats are mentioned first.

Having said that, it is worth mentioning that further prioritization criteria are also feasible, such as geographical spread, classification according to categories of impacted assets, according to threat agents, according to kind of organisations affected, etc. We have chosen appearance frequency as the priority scheme to balance available resources and quality of the required analysis. During the reporting period, various stakeholders have proposed using additional schemes, in particular geographic spread (i.e. regarding European territory) and size of organisations affected (i.e. large organisations vs. SMEs). These requests are under consideration and the feasibility of their implementation will be evaluated in upcoming versions of ETL.

In the following discussion, the top 15 threats from end 2012 to end 2013 can be found. 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 to a threat and v) the position of the threat in the attack workflow.

This chapter is concluded by a comparison between the current threat landscapes of ETL 2012 and ETL 2013. This will help readers to easily understand the changes of the current threat landscape in this time period.

3.1 Drive-By Downloads

Web based attacks implementing drive-by downloads scores for one more year as the top cyber threat. This is quite natural as web browsers are the first level of user interaction with the Internet. As such, web pages, web servers and web services have become the most important attack surface: attackers target web sites with the aim to infect them with malicious code, usually exploit kits (see corresponding threat below). Infected web sites are referred to as malicious URLs and are “door openers” for other threats such as exploit kits and malicious code infections (i.e. Worms/Trojans). Visitors of these web sites are automatically scanned through the maliciously installed exploit kits for weaknesses/vulnerabilities. Once vulnerabilities have been found in the device of the visitor, exploit kits automatically install the appropriate malware on the device. The installed malware may vary significantly according to the underlying user system/configuration and the vulnerabilities found. This threat belongs to the broad category of unauthorised software installation to the victim’s device: starting from a victim web server and reaching the devices of visitors.

In the reporting period we have assessed that:

- Web based attacks remain as the number one threat. Malicious URLs are considered the main channel for malware installation. It has been observed that there is a shift from Botnets to URLs as means for malware distribution[56].
- Java remains the most exploited software[34,35] to infect a web site. In addition, attackers use code injection attacks (see threat below) to create malicious URLs[47].
- As predicted in 2012, drive-by downloads have fully embraced mobile platforms. Just as any other device, mobile platforms are targeted by vulnerability scanning capabilities of exploit kits.
- As mentioned in the code injection threat below, manipulated CMSs are another source for the creation of malicious URLs[36,37].
- Web based attacks are increasingly used within targeted attacks. Through the watering hole technique, attackers lure a specific group of victims to visit their malicious URLs. This technique has been increasingly used in 2013 with high infection rates[38,47] (see also threat below).

Observed current trend for this threat: *increasing*

Related threats: Code Injection, Exploit Kits, Worms/Trojans, Rogueware/Ransomware/Scareware, Targeted Attacks, Watering Hole.

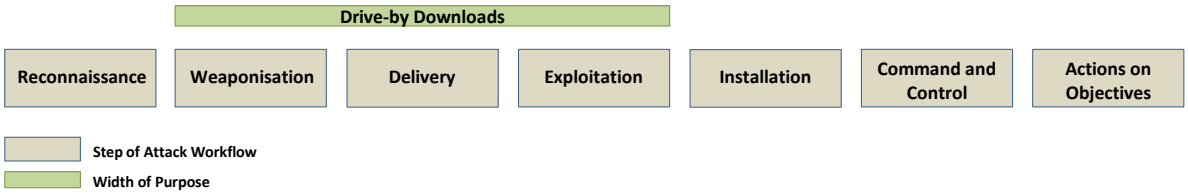


Figure 5: Position of Drive-By Downloads in attack workflow

3.2 Malicious Code: Worms/Trojans

In the reporting period, the threat of spreading malicious programs has been reported as very high in related reports. Malware and particularly trojans have been derived from previous versions in thousands of variants. This is due to the use of available toolkits allowing for the generation of user defined malware through variations of existing malware code. Due to functionality offered by toolkits, this activity can be performed by adversaries with moderate capabilities. The vast number of malware variations is deployed as an effective method to fool signature-based virus scanners: due to their large numbers, signatures of the created variants are not always available, leading thus to unnoticed infections. Mobile platforms supported the successful deployment of this threat. Mobile malware takes a significant part in malware statistics.

In the reporting period we have assessed that:

[34] http://www.kaspersky.com/about/news/virus/2012/Oracle_Java_surpasses_Adobe_Reader_as_the_most_frequently_exploited_software, accessed 8 August 2013.
[35] http://globenewswire.com/news-release/2013/07/18/561078/10041006/en/Bit9-Research-Shows-Java-is-Most-Targeted-Endpoint-Technology-for-Cyber-Attacks-Widely-Deployed-Older-Versions-Represent-Greatest-Risk.html, accessed 8 August 2013.
[36] http://www.symantec.com/connect/blogs/risk-content-management-systems, accessed 18 Nov 2013.
[37] https://www.bsi.bund.de/DE/Publikationen/Studien/CMS/Studie_CMS.html, accessed 18 Nov 2013.
[38] http://securityaffairs.co/wordpress/14725/hacking/watering-hole-attacks-exploit-kits-indian-gov-site-case.html, accessed 18 Nov 2013.

- Malware increasingly targets mobile platforms, with mobile trojans coming at the first position. This is due to the increasing use of mobile devices, the increased sophistication of attacks (see below) but also due to the weaker/immature security mechanisms implemented on these platforms.
- Available attack tools (see also exploit kits) allow for the creation of malware variants based on available malware code. This activity can be performed even from users with moderate capabilities. This phenomenon is called polymorphism of existing code and is a key trend in malware development.
- An increased sophistication in malware has been reported, especially on mobile platforms. Code obfuscation (i.e. code that bypasses vetting process of gated app stores) and use of multiple channels use are some characteristics of the complexity of malware[39].
- Coordinated activities of developers have demonstrated their true potential in generating sophisticated malware by launching malware attacks against Mac computers[40,47].
- There is a growing black/grey market for stolen user data[41]. This brings information stealing malware on the rise. Given the increased use mobile devices and the sophistication of attacks, information stealing malware is here to stay.
- Rogue certificates have been used to sign malicious code and thus distribute signed apps[42]. This has demonstrated that incidents with rogue certificates are still a serious risk that cannot be easily mitigated[109,43].

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Code Injection, Exploit Kits, Botnets, Identity Theft/, Data Breaches, Rogueware/Ransomware/Scareware, Phishing, Targeted Attacks.

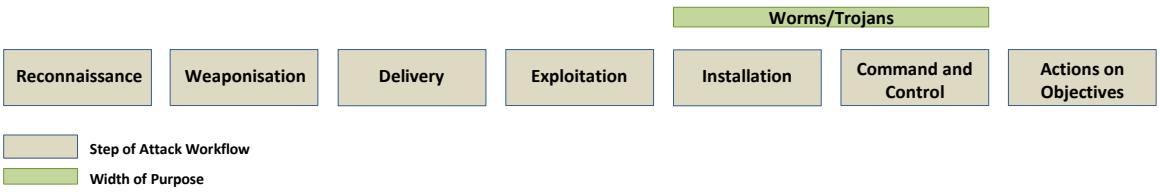


Figure 6: Position of Worms/Trojans in attack workflow

3.3 Code Injection

In 2013, the mix of tools available to perform code injection attacks remained unchanged: Cross-Site Scripting (XSS), Directory Traversal, SQL injection (SQLi) and Cross-Site Request Forgery (CSRF). Within 2013 Code injection attacks are on sharp rise. The proliferation of automated attack tools impacted the frequency of this threat in the reporting period: hackers are in the position to launch large vulnerability scans in short time.

In the reporting period we have assessed that:

[39] http://www.infosecurity-magazine.com/view/31801/mobile-malware-gets-serious-rats-can-bypass-sandboxes-and-encryption/, accessed 18 Nov 2013.
[40] http://www.f-secure.com/weblog/archives/00002558.html, accessed 18 Nov 2013.
[41] http://gigaom.com/2013/08/22/your-identity-is-probably-worth-5-on-the-black-market/, accessed 18 Nov 2013.
[42] http://threatpost.com/winnti-cyberespionage-campaign-targets-gaming-companies-041113, accessed 8 Nov 2013.
[43] https://www.csis.dk/en/csis/blog/4114/#, accessed 3 December 2013.

- A notable issue with regard to this threat is attacks against popular Content Management Systems (CMSs). Due to their wide use, popular CMSs make up a considerable attack surface that has drawn the attention of cyber-criminals[44,45].
- Large scale automated attacks are being increasingly launched from within cloud service provider networks[61].
- Code injections are combined with other threats to successfully infect victims[144]. A typical example in the reporting period is a series of incidents that have been caused by successful attacks combining SQLi together with spear-phishing and watering hole techniques[46].

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Exploit Kits, Data Breaches, Targeted Attacks.

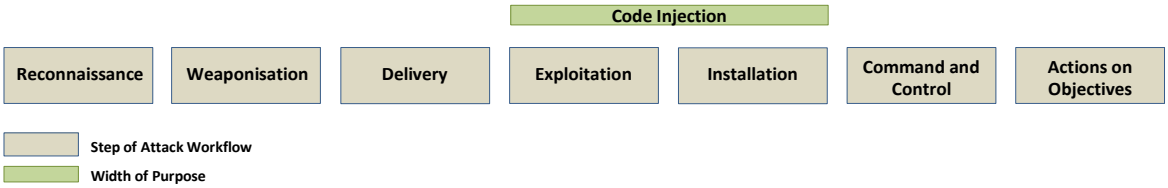


Figure 7: Position of Code Injection in attack workflow

3.4 Exploit Kits

Exploit kits are the main tools in the hands of threat agents. These are ready-to-use software tools offering a large variety of functions, configuration options and automated means to launch attacks. Exploit kits search for vulnerabilities in order to abuse them and launch any applicable attack to take over an asset (also mentioned as Exploit attacks[47]). Exploit kits have been heavily used by hackers within the reporting period. Further, it has been reported that new business models emerge around such tools: developers of exploit kits maintain interaction with customers by offering support, customized configurations, etc[48,49]. The ability for updating, customization and the degree of automation provided is considered to be one of the main parameters for increase in all kinds of threats supported, such as malware, code injections, exploitation of vulnerabilities, etc.

In the reporting period we have assessed that:

- Exploit kits are entering a new era of higher maturity towards developer/user relationship. Additional "services"[50,51] are developed and it seems that developers and users of exploit kits are two distinct types of cyber threat agents.

[44] http://www.h-online.com/open/news/item/CMSs-mostly-vulnerable-through-addons-says-German-security-agency-1894431.html, accessed 8 August 2013.
[45] http://securitywatch.pcmag.com/security/310350-wordpress-joomla-sites-under-brute-force-password-attack, accessed 8 August 2013.
[46] http://www.infosecurity-magazine.com/view/33493/water-hole-replacing-spearphishing-as-statesponsored-weapon-of-choice/, accessed 2 Dec 2103.
[47] http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf, accessed 4 Nov 2013.
[48] http://blog.trendmicro.com/trendlabs-security-intelligence/what-to-expect-from-toolkits-and-exploit-kits-this-2013/, accessed 4 Nov 2013.
[49] http://networksasia.net/article/cybercrime-exposed-cybercrime-service-1372901941, accessed 7 Nov 2013.
[50] https://blog.damballa.com/archives/1893, accessed 18 Nov 2013.
[51] http://resources.infosecinstitute.com/cybercrime-as-a-service/, accessed 18 Nov 2013.

- Users are confronted to exploit kits mostly by accessing compromised URLs (see threat drive-by downloads above).
- Due to the popularity of exploit kits and the emerging need to feed them with known vulnerabilities, there is an increasing interest in zero-day vulnerabilities. This is a significant amplification effect for the market of exploits/vulnerabilities[52]. It is important to note that both hostile and friendly actors in cyber space show interest in purchasing zero-day vulnerabilities[47].
- Efforts have been invested by exploit kit developers to encrypt their payloads, thus make them invisible from detection mechanisms[53].
- Due to the existence of a market, it is expected that a developers instead of developing new malware, will concentrate on development of exploit kits[48]. Rather, exploit kits will be able to include new malware and available vulnerabilities.
- The developer and operator of Blackhole[54], the most successful exploit kit has been arrested. It will be very interesting to observe future developments with this malicious tool. Are other threat agents going to take over development and operation of Blackhole or its derivates? Are other tools going to fill the possibly created gap? It is suggested to keep an eye on this issue, as it going to introduce significant impact to the threat landscape.

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Code Injection, Worms/Trojans, Phishing, Rogueware/Ransomware/Scareware.

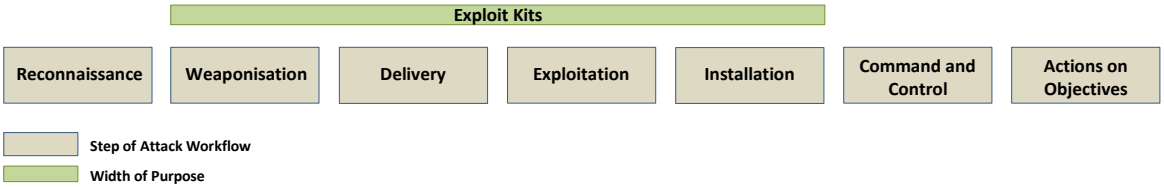


Figure 8: Position of Exploit Kits in attack workflow

3.5 Botnets

Botnets, networks of compromised, remotely controlled computers, still pose a serious cyber threat. Being one of the oldest and more "mature" malicious infrastructures in cyber space, botnets currently undergo significant changes in their adaptation, reduction of traceability, business cases, channels used and technology usage. In the reporting period we have seen some of these changes become reality. The use of peer-to-peer technologies, not only increases the resilience of single nodes, it also enhances their ability to stay undetected. Although this development has been observed since 2012, the benefits of this technology have been demonstrated in 2013, as they can run on cloud infrastructures. Noticeable changes in the business models include a shift from botnets to URLs as means to install malware. Further, the botnet business model has concentrated on Bitcoin mining[55]. In addition, click fraud payloads have been deployed.

[52] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/, accessed 4 Nov 2013.
[53] http://resources.infosecinstitute.com/battling-cyber-warriors-exploit-kits/, accessed 18 Nov 2013.
[54] http://www.zdnet.com/blackhole-malware-toolkit-creator-paunch-arrested-7000021740/, accessed 28 Nov 2013.
[55] http://www.fortinet.com/press_releases/2013/fortiguard_threat_landscape_research_team_reports.html, accessed 4 Nov 2013.

In the reporting period we have assessed that:

- Threat analysts see malicious URLs replacing botnets as the primary means for distribution malware (see also drive-by downloads above)[56]. Botnets are on decline with regard to this threat.
- Existing botnet infrastructure has been updated with P2P technology[57]. This increases resilience of botnet nodes when servers are taken down.
- Existing versions of botnet infrastructure are equipped with Bitcoin mining and click fraud functions. At the same time, they continue targeting social networks with spam.
- Botnets sometimes use the anonymizing network TOR. Lately malware families have been found using TOR as communication network[58]. It can be assumed that a considerable part of the vast increase of TOR traffic is caused by its use for malicious purposes[59],[60].
- Although botnet malware infections are on the decline[56], it seems that botnets are still one of the most important cyber threats. The reasons for can be found in changes of malware infection strategies, use of P2P technology, use of anonymizing technologies etc.
- Within the current trend of cyber-crime-as-a-service, we see various "traditional" botnet functions to be offered as a service; similarly the availability of hosting services makes the use of cloud as a high performance botnet feasible[61,62].

Observed current trend for this threat: *stable/slightly increasing*

Related threats: Drive-by Downloads, Worms/Trojans, Phishing, Spam, Denial of Service, Rogueware/Ransomware/Scareware.

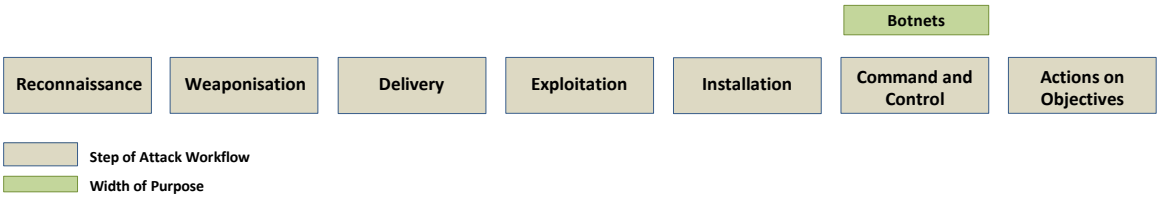


Figure 9: Position of Botnets in attack workflow

3.6 Physical Damage/Theft/Loss of media

This threat has increased in 2013 due to the increasing number of mobile devices used and consequently stolen, lost or damaged. Taking reported percentages as a basis, one can conclude that

[56] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf, accessed 4 Nov 2013.
[57] http://www.csoonline.com/article/734485/malware-increasingly-uses-p2p-communications-researchers-say?page=1, accessed 4 Nov 2013.
[58] http://www.net-security.org/malware_news.php?id=2545&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:%20Help NetSecurity%20%28Help%20Net%20Security%29, accessed 4 November 2013.
[59] http://news.softpedia.com/news/Cybercriminals-and-NSA-Spying-Cause-350-Increase-in-Tor-Traffic-395779.shtml, accessed 5 Nov 2013.
[60] http://www.solutionary.com/research/threat-reports/quarterly-threat-reports/sert-threat-intelligence-report-q3-2013, accessed 5 Nov 2013.
[61] http://www.firehost.com/company/newsroom/press-releases/firehost-report-suggests-commodity-cloud-providers-are-bolstering-botnet-agility, accessed 4 November 2013.
[62] http://www.mcafee.com/sg/resources/white-papers/wp-cybercrime-exposed.pdf, accessed 4 Nov 2013.

some 70-80 million devices have been broken, stolen or lost[63]. Meanwhile, it is considered that hacking is not the main cause of data loss: ca. 36% of data breaches are attributed to theft/loss of devices[64].

In the reporting period we have assessed that:

- Damage of devices seems to be the number one cause for losing data[63]. And although users are concerned about cyber-attacks, the awareness about the possibility of a damage/loss of device seems to be rather low. In this area there is a lot of space for improvements.
- As already assessed within the threat of data breach (see above), a significant part of data breaches is caused through physical access to the storage device. Theft/damage/loss seems to be the main cause for this[65].
- Most of the data on damage, theft or loss are based on surveys/statistics and not on incidents. This is due to the fact that related incidents on physical damage, theft and loss are not always reported and gathered. Hence concluded damages (and costs[118]) are just estimations that need to be validated.
- To reduce the impact of the damage/theft/loss threat, it is noticeable that the following factors play a significant role towards a reduction of incurred costs: "*strong security posture, incident response capabilities and appointment of a CISO*"[118].

Observed current trend for this threat: *increasing*

Related threats: none

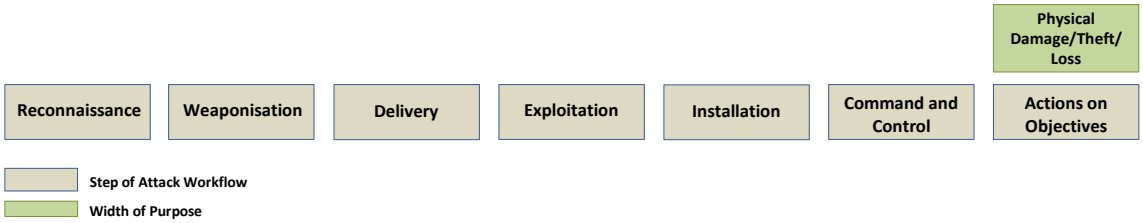


Figure 10: Position of Physical Damage/Theft/Loss in attack workflow

3.7 Identity Theft/Fraud

Identity theft and identity fraud are threats that have led to some of the most impressive successful attacks in the reporting period[63,66]. Identity theft is one of the core activities of many threat agent groups, as it gives access to a lot of data that bear potential for numerous malicious activities. Malware and trojans belong to the main tools to perform identity theft. In 2013, for example, financial trojans (e.g. Zeus, SpyEye, Citadel[67]) have been use to implement 2-factor authentication attack on mobile platforms[68]. The interest in identity theft, but also its importance in deploying multiple attacks has led to the creation of a market for this kind of data[96]. It is expected, that this threat will continue increasing, as the methods used increase in sophistication and spread.

In the reporting period we have assessed that:

[63] http://media.kaspersky.com/pdf/Kaspersky_Lab_B2C_Summary_2013_final_EN.pdf, accessed 7 Nov 2013.
[64] http://www.symantec.com/connect/blogs/symantec-intelligence-report-may-2013, accessed 7 Nov 2013.
[65] http://www.acronis.com/download/docs/glme/whitepaper2, accessed 7 November 2013.
[66] http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/, accessed 19 Nov 2013.
[67] http://www.mcafee.com/us/resources/white-papers/wp-citadel-trojan.pdf, accessed 7 Nov 2013.
[68] http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf, accessed 7 Nov 2013.

- The inclusion of mobile platforms in identity hunting malware is a matter of fact and has demonstrated the potential behind successful attack on these platforms. As expected, data on financial and payment institutions are the most prominent ones for identity theft[69,70].
- A significant source for applying this threat remains social media[71]. It is worth mentioning that an increase in malicious browser extensions has been registered, aimed at taking over social network accounts[72,73]. A market around social accounts has already been created[74]
- The use of Near Field Communication (NFC) capabilities for financial transactions, exchange of messages and interaction with other devices increases. This technology will provide an attack surface, especially with regard to eavesdropping[75].
- Man-in-the-browser attacks are similar to man-in-the-middle attacks except that the intervention on an infected device happens over a Trojan that deviates traffic over a botnet (e.g. SpyEye v1.3 botnet[76]). Through these attacks, threat agents are stealing almost any information from the browser memory[77].
- It is worth noticing how threat agents adapt to additional authentication mechanisms used for securing identity information, especially in financial transactions. SMS forwarding has been introduced to existing malware. This includes permissions linked with the SMS relay, whereas PC injection requests users to ender data that are also displayed on the handset. Hence a connection between these devices is established. Then the malware takes over SMS communication with the bank and misuses communicated credentials[78] (i.e. man-in-the-mobile).

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Exploit Kits, Code Injection, Botnets, Worms/Trojans, Phishing, Spam, Information Leakage, Data Breaches, Rogueware/Ransomware/Scareware.

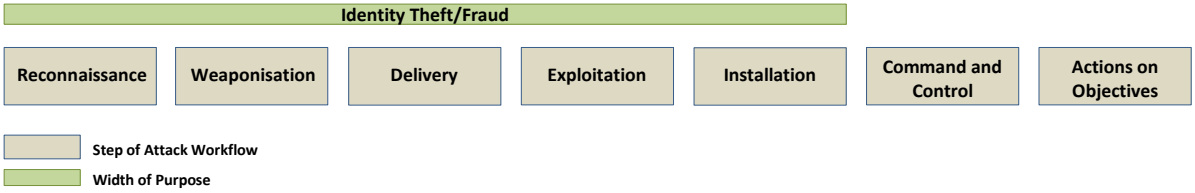


Figure 11: Position of Identity Theft/Fraud in attack workflow

[69] http://krebsonsecurity.com/2013/03/mobile-malcoders-pay-to-google-play/, accessed 8 Nov 2013.
[70] http://www.ft.com/cms/s/0/a95130fc-3b18-11e2-b3f0-00144feabdc0.html#axzz2l56MZIKd, accessed 19 Nov 2013.
[71] http://bits.blogs.nytimes.com/2013/06/03/malware-that-drains-your-bank-account-thriving-on-facebook/, accessed 8 August 2013.
[72] https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_05-2013.en-us.pdf, accessed 8 August 2013.
[73] http://news.cnet.com/8301-1009_3-57584111-83/microsoft-warns-of-new-trojan-hijacking-facebook-accounts/, accessed 8 Nov 2013.
[74] http://www.businessinsider.com/facebook-targets-76-million-fake-users-in-war-on-bogus-accounts-2013-2, accessed 8 Nov 2013.
[75] http://www.forbes.com/sites/michaelvenables/2013/08/08/wall-of-sheep-near-field-communication-hack-at-def-con/, accessed 19 Nov 2013.
[76] https://blogs.rsa.com/man-in-the-middle-standing-between-you-and-your-cash/, accessed 8 Nov 2013.
[77] http://www.trusteer.com/glossary/man-in-the-browser-mitb, accessed 8 Nov 2013.
[78] http://www.emc.com/collateral/fraud-report/rsa-fraud-report-062013.pdf, accessed 8 Nov 2012.

3.8 Denial of Service

In the reporting period, a significant jump of Denial of Service attacks has been detected[79]. After the Spamhaus[80] attack, DNS reflection attacks have gained in popularity[81,82]. DNS reflection amplification attacks target poorely configured DNS servers. Attackers seem to have adopted the DNS reflection technique to launch amplification attacks, an old technique that has made a come-back. Another reason for this increase is assumed in the availability of easy-to-use attack tools that embrace DoS capabilities[82]. Users with low skills can easily launch DoS attacks, and, when done in orchestration with other actors, significant striking power can be developed. Moreover, available high performance botnets contribute to the increased volume of DoS attacks[83]. Amplification, wide availability of tools/resources and coordination among threat agent groups seem to be the reason for the impressive DoS bandwidths achieved (2-10Gbps up to 300Gbps[85,86]). The duration of attack has grown, indicating that attackers are risking detection of their resources (botnets, tools) in order to maximize impact on the attacked sites

In the reporting period we have assessed that:

- Sophistication of DoS attacks grows (multi-vendor and multi-layer attacks) making them difficult to defend[84].
- Performance of available DoS attack infrastructure has grown. This includes both use of technology (amplification) and involved threat agents (coordination, orchestration).
- Features of attack infrastructure (see botnets above) such as resilience, clandestine communication and use of encryption lower detectability and allow for a longer duration of attacks.
- Attack bandwidths achieved have reached impressive levels: the rate of 2-10Gbps attacks has doubled[85] and the level of 300Gbps attack was reached in 2013[86].
- While DoS targets mainly enterprise and commerce it seems that US and Asia Pacific are more targeted through DoS. Europe has lower attack rates[87].
- A series of DDoS attacks to banks has drawn the attention of security professional in the reporting period[88].

Observed current trend for this threat: *increasing*

Related threats: Botnets, Worms/Trojans.

[79] http://www.arbornetworks.com/corporate/blog/5025-q3-findings-from-atlas, accessed 5 Nov 2013.
[80] http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability/at_download/fullReport, accessed 8 August 2013.
[81] http://www.akamai.com/stateoftheinternet/, accessed 8 August 2013.
[82] https://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q2/pr.html, accessed 5 Nov 2013.
[83] http://arstechnica.com/security/2013/04/fueled-by-super-botnets-ddos-attacks-grow-meaner-and-ever-more-powerful/, accessed 5 Nov 2013.
[84] https://www.securityweek.com/multi-vector-ddos-attacks-grow, accessed 5 Nov 2013.
[85] http://www.arbornetworks.com/corporate/blog/4922-q2-key-findings-from-atlas, accessed 8 August 2013.
[86] http://www.arbornetworks.com/corporate/blog/4813-putting-the-spamhouse-ddos-attack-in-perspective, accessed 8 August 2013.
[87] http://www.akamai.com/dl/akamai/akamai_soti_q213_exec_summary.pdf, accessed 5 Nov 2013.
[88] http://www.bankinfosecurity.com/ddos-what-to-expect-from-next-attacks-a-5653, accessed 18 Nov 2013.

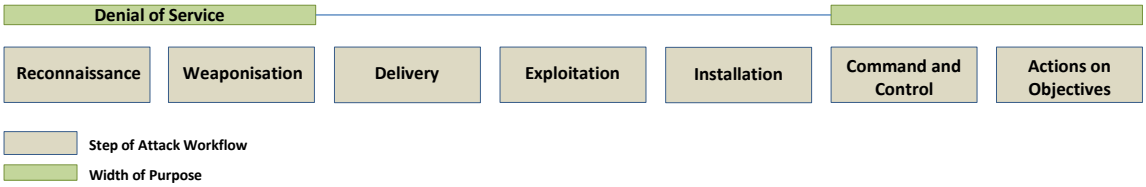


Figure 12: Position of Denial of Service in attack workflow

3.9 Phishing

The hunting of user credentials through phishing continues in 2013. Tools are e-mails, manipulated web pages, mobile apps and social media/social gaming. Through the proliferation of mobile devices, they constitute main targets/channels to obtain user credentials. In this context social engineering approaches target users over various channels supported in mobile devices such as voice, instant and short messages and rogue apps. These channels come to complement e-mail as common phishing delivery method[89].

The complexity/sophistication of phishing methods varies as well. Fake websites is the simplest tool going up to infected web sites, malware and Pharming/DNS manipulations[90]. The range of complexity allows all threat agent groups, from novice to experts, to launch phishing attacks[47]. All in all, there has been an increase in phishing in 2013, with phishing sites targeting mainly Social Networking, Financial, Online Services, E-Commerce and Gaming[90,91](sequence according to number of phishing sites). Nevertheless, phishing targets vary from country to country[90].

In the reporting period we have assessed that:

- Sophistication of phishing increases: in the reporting period we have seen phishing strategies to include methods that are difficult to spot[90] by end users. Moreover, phishing strategies seem to seek for tactics to fool users of multilevel security procedures introduced by targeted organisations.
- Phishing has a geographic component[90,91]. Phishing strategies are adapted to cultural, social and technological development of particular geographic areas. Therefore, phishing mitigation strategies have to take this dimension into account.
- As in other threats assessed, phishing can also be facilitated by easy-to-use tools[90]. This enables threat agents with low capabilities to launch phishing attacks.
- Phishing is heavily based on web site vulnerabilities[92]. This fact underlines the importance of in-depth web site/web application protection strategies.
- Powerful hosting environments (i.e. cloud computing), are an important target of phishing attacks. This is due to the multiplication effect of a successfully mounted attack. This strategy follows the same pattern as for botnets and DoS attacks, all using the power of virtual environments and the vast accumulation of data[92].

[89] http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf, accessed 5 Nov 2013.
[90] http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf, accessed 5 November 2013.
[91] http://www.microsoft.com/security/sir/default.aspx, accessed 5 Nov 2013.
[92] http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf, accessed 5 Nov 2013.

- Threat agents will target end users of financial systems directly in order to obtain important information to perform fraud[90] and achieve profits. Hence, end user awareness, sensibilization and training are the key to protect against this threat.

Observed current trend for this threat: *increasing*

Related threats: Exploit Kits, Code Injection, Botnets, Worms/Trojans.

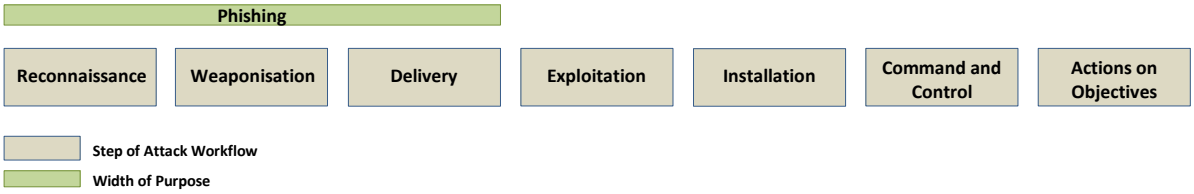


Figure 13: Position of Phishing in attack workflow

3.10 Spam

With ca. 75% of the entire e-mail traffic, spam continues to constitute the major part of messages sent to bother security experts and end users[91]. Not only is filtering spam a resource consuming task; spam is one important channel to spread malware, attract user to malicious URLs, commit fraud, etc. Hence, defending against this threat is not all about filtering spam but also how to avoid the impact on end users with regard to fraud and malicious e-mail content. As originating mainly from botnets, spam has demonstrated an activity that is in analogy to the botnet activity: in the 1st quarter on 2013 we have experienced a dramatic increase[56,93], whereas the volume of spam dropped till the 1st half of the year[91,94]. Finally, just like almost all other threats, spam has gone mobile: spam with Android malware has been on the rise[95].

In the reporting period we have assessed that:

- Spam has a strong geographic component, with spam origin being on the focus[91,96]: while in some areas spam traffic in on decline, there are countries with high/very high spam traffic.
- Spam content is related mainly (i.e. over 85%) to pharmacy, images, the so called "Nigerian scam"[97], malware and non-pharmacy product ads[91]. Moreover, spam messages chose contemporary hot topics from the press to attract potential victims[98] (e.g. Boston Marathon bombings, Pope Francis election, etc.). This might be an important piece of information for end users.
- Tricks used in spam/scam are identity theft targeting social accounts. This is being attempted either by means of luring potential victims through prizes/gifts, or by using fake websites to convince them to enter credential information[99].

[93] http://www.commtouch.com/uploads/2013/04/Commtouch-Internet-Threats-Trend-Report-2013-April.pdf, accessed 6 Nov 2013.
[94] http://www.commtouch.com/uploads/pdf/Commtouch-Internet-Threats-Trend-Report-Q3-2013.pdf, accessed 7 Nov 2013.
[95] http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2013.pdf, accessed 6 Nov 2013.
[96] https://www.ibm.com/services/forms/signup.do?source=swg-WW_Security_Organic&S_PKG=ov16986&S_TACT=102PW63W, accessed 6 Nov 2013.
[97] http://en.wikipedia.org/wiki/Nigerian_scam, accessed 6 Nov 2013.
[98] http://www.commtouch.com/uploads/2013/04/Commtouch-Internet-Threats-Trend-Report-2013-April.pdf, accessed 6 Nov 2013.
[99] http://www.symantec.com/security_response/publications/threatreport.jsp, accessed 6 Nov 2013.

- It seems that spammers are checking regularly the capability/performance of existing spam filters. In the reporting period we have seen spams that have obviously no malicious background, have strange content and/or structure[98,100].
- The techniques of spammers evolve. For end users it is important to understand tricks[101] and have basic sensitivity/awareness on this matter.

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

Related threats: Drive-by Downloads, Exploit Kits, Code Injection, Botnets, Worms/Trojans.

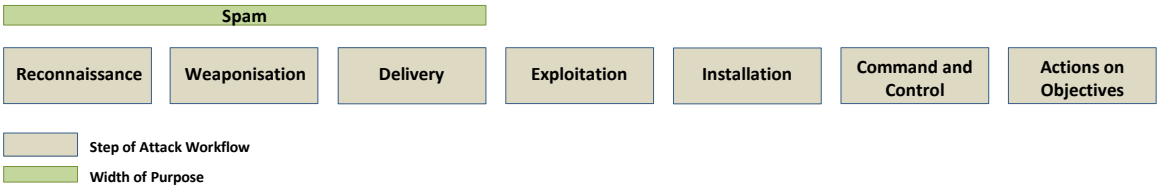


Figure 14: Position of Spam in attack workflow

3.11 Rogueware/Ransomware/Scareware

This threat is used to obtain profits from terrified end users. Rogue security software, ransomware and scareware are malicious pieces of software - distributed by threat agents - to terrify/blackmail users, thus demanding ransom payments. Although a decline has been reported regarding the number of fake Anti-Virus (AV) products in comparison to 2012, the overall numbers of rogueware/ransomeare/Scareware remain high[56,102,103]. In particular, ransomware has reached high levels of infection[104]. Despite recent law enforcement advances[105], the reports analysed provide strong evidence that there is an increase in ransomware threat[104]. One reason for the growth is the expansion of ransomware and fake Antivirus distribution to mobile platforms, such as Android[106]. Again, one significant component of the increase registered related to mobile platforms: ransomware (i.e. FakeAV) has hit this year Android[104,107,108].

In the reporting period we have assessed that:

- The availability of anonymous payment services to channel illegal profits obtained from this threat is a key enabler for this kind of fraud[109].
- Rogueware, ransomware and scareware are distributed via exploit kits, while exploiting Java and Adobe vulnerabilities. The use of exploit kits (see also description of exploit kits threat above), is

[100] http://www.spiegel.de/netzwelt/web/e-mail-provider-gmx-und-co-der-raetselhafte-buchstaben-spam-a-931933.html, accessed 6 Nov 2013.
[101] http://www.appriver.com/downloads/global-threatscape-reports/2013/GlobalThreatScapeReport_6MonthEdition.pdf, accessed 6 Nov 2013.
[102] http://www.kindsight.net/sites/default/files/Kindsight-Q2-2013-Malware-Report.pdf, accessed 6 Nov 2013.
[103] http://www.itproportal.com/2013/04/10/ransomware-the-cybercrime-money-machine-of-2013/, accessed 19 Nov 2013.
[104] https://www.us-cert.gov/ncas/alerts/TA13-309A, accessed 18 Nov 2013.
[105] https://www.europol.europa.eu/content/police-dismantle-prolific-ransomware-cybercriminal-network, accessed 8 August 2013.
[106] https://www.infoworld.com/t/mobile-security/ransomware-android-it-was-only-matter-of-time-221285, accessed 8 August 2013.
[107] http://www.symantec.com/connect/blogs/fakeav-holds-android-phones-ransom, accessed 6 Nov 2013.
[108] http://blog.fortinet.com/Ransomware/, accessed 6 Nov 2013.
[109] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf, accessed 8 August 2013.

concluded from the wide spread and the existence of variations/derivates of this malware, that is, alternations to some initial code performed by individual threat agents[110].

- Just as it is the case with the rest of malware, the sophistication of ransomware increases[111],[112].
- In the reporting period a significant success of law enforcement led to arrest of members of cyber-criminal gang responsible for the "Police Virus" (statement of the Spanish Ministry of Interior[113]). This success demonstrates the importance of cooperation at international level[114,115].

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Exploit Kits, Code Injection, Botnets, Worms/Trojans, Phishing, Spam.

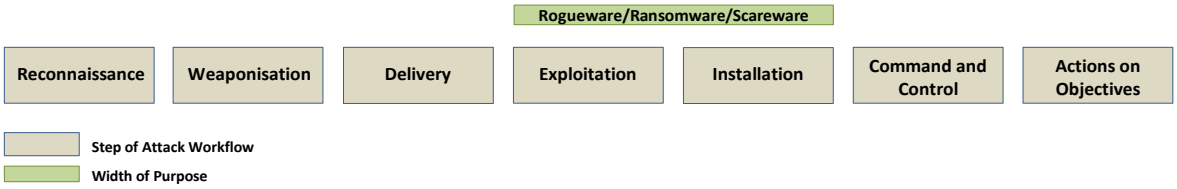


Figure 15: Position of Rogueware/Ransomware/Scareware in attack workflow

3.12 Data Breaches (Compromising Confidential Information)

In cyber security, a lot of attention is being paid to data breaches. With this threat, we refer to loss of data occurring via intentional or unintentional information disclosure (i.e. through mistakes in managing information assets). This threat might originate from internal threat agents or external ones. In both cases there might have both hostile[116] and non-hostile intentions (i.e. lack of knowledge or negligence). As regards intentional causes, this threat is rather a cumulative implication of other threats mentioned in this report on data. The unintentional part of it, however, is a threat that can materialize due to errors and mistakes of personnel. In all cases, data breaches are systematically reported in related publications. Data breaches are related to incidents from materialized threats, whereby information has been compromised. As such, data breach reporting is considered to be an important indicator of the protection level for company data, but also the effectiveness of malicious actions[117]. This information is useful for decision and policy makers, especially from the economic point of view[118].

In the reporting period we have assessed that:

[110] http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Quaterly-Report.pdf, accessed 6 Nov 2013.
[111] http://news.techworld.com/security/3470388/ransomware-criminals-attack-smes-using-strong-file-encryption-eset-warns/, accessed 19 Nov 2013.
[112] http://en.wikipedia.org/wiki/CryptoLocker, accessed 2 Dec 2013.
[113] http://www.lamoncloa.gob.es/ServiciosdePrensa/NotasPrensa/MIR/2013/130213policiainformatica.htm, accessed 6 Nov 2013.
[114] http://pandalabs.pandasecurity.com/operation-ransom-police-virus-authors-arrested/ , accessed 6 Nov 2013.
[115] http://www.youtube.com/watch?feature=player_embedded&v=wBMyaOa4Xnw, accessed 6 Nov 2013.
[116] For internal threat agent see also Employee in Figure 20.
[117] http://www.reuters.com/article/2013/10/29/us-adobe-cyberattack-idUSBRE99S1DJ20131029, accessed 5 Nov 2013.
[118] https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf, accessed 6 Nov 2013.

- Small organisations are more targeted by malware aiming at financial fraud. Larger organisations are targeted merely with the intention of espionage[119]. This might be indicative for the quality/quantity of protection measures. Eventually, larger organisations are better off in protecting themselves against more simple kinds of attacks, while they often become victims of highly skilled organised crime.
- As regards data breaches, internal actors are at the minority. The vast amount of data breaches are attributed to external threat agents[119]. This is reflected in a study on the costs of data breaches: malicious attacks are at the first position, while system failure and human factor score second and third respectively[118].
- Data breach reporting is an important tool for the evaluation of effectiveness/maturity of existing controls. Data breach notification mechanisms are envisaged from policy makers as an instrument towards better cyber security governance[120].
- Through the deployment of simple/low cost security controls organisations may drastically reduce data breaches: over 70% of incidents are based on simple/low difficulty attacks.
- Most of misuse actions are caused by physical access, either directly or indirectly to the asset targeted. LAN and remote access are following[119].

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Exploit Kits, Code Injection, Botnets, Worms/Trojans, Identity Theft/Fraud, Information Leakage, Physical Damage/Theft/Loss, Phishing, Spam, Rogueware/Ransomware/Scareware, Targeted Attacks, Watering Hole.

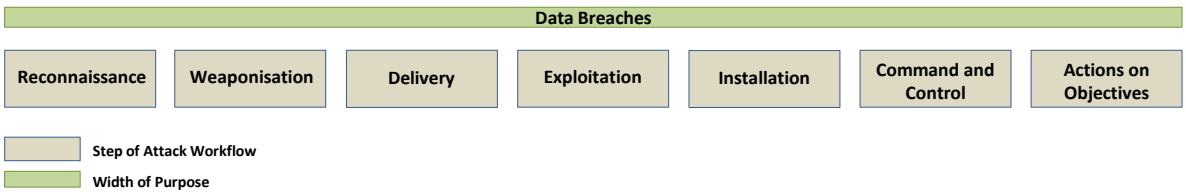


Figure 16: Position of Data Breaches in attack workflow

3.13 Information leakage

With information leakage we cover a set of threats related to the unintentional or maliciously triggered revelation of information of security related information to an unauthorised party. This threat is differentiated from data breaches, as it merely concerns technical or organisational information that might be interesting for threat agents in order to perform reconnaissance and delivery of their attacks; as opposed to data breach which is result of a successful attack targeting customers' data. In the reporting period aggressive adware collecting information has been encountered[121,122]. Moreover, unsecured file transfers might lead to severe information leakage[65], as well as poor encryption practices for mobile devices.

[119] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf, accessed 5 Nov 2013.
[120] http://www.computerweekly.com/news/2240203760/EU-data-breach-disclosures-to-be-enforced-soon, accessed 5 Nov 2013.
[121] http://www.trendmicro.co.uk/cloud-content/us/pdfs/security-intelligence/reports/rpt-zero-days-hit-users-hard-at-the-start-of-the-year.pdf, accessed 8 Nov 2013.
[122] https://blog.lookout.com/blog/2013/06/05/world-current-of-mobile-threats/, accessed 8 Nov 2013.

In the reporting period we have assessed that:

- Broken authentication and session management has the consequence that attackers may hijack user sessions, gain user credentials and obtain access to business transactions. This is based on leakage from bad session management[123].
- Directory traversal is a threat that has been already mentioned in code injection (see above). Path manipulation[124] and resource injection[125] are attacks based on directory information leakage.
- Network reconnaissance[126],[127] is a known, yet very important information gaining method/attack to obtain system, network and other resources. Network reconnaissance is based on leakage of network structure and is an important part of targeted attacks. Besides networks, availability of information on other resources may facilitate all kinds of attacks[128].
- Due to user negligence but also maturity level of available apps, big parts of mobile communication take place unsecured, often over unsecured channels. This can lead to significant information leakage including personal and business information[65].
- Research with support of social media can be a very effective way to obtain information on human resources. Widely available services on the web[129] allow for identification of further personal details which, when combined with additional information may result in significant knowledge about targeted individuals.
- Although not explicitly a leakage issue, it is worth mentioning cloud services (e.g. cross VM side channels) as a potential to abuse computing power, data concentration and extract sensitive data[130,131].

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Exploit Kits, Code Injection, Botnets, Worms/Trojans, Identity Theft/Fraud, Information Leakage, Physical Damage/Theft/Loss, Phishing, Spam, Rogueware/Ransomware/Scareware, Targeted Attacks, Watering Hole.

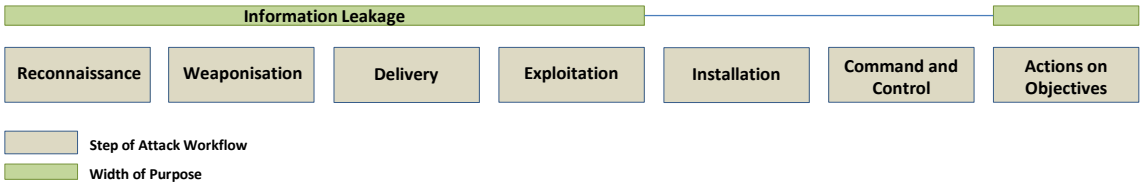


Figure 17: Position of Information Leakage in attack workflow

[123] https://www.owasp.org/index.php/Top_10_2013-Top_10, accessed 8 Nov 2013.
[124] https://www.owasp.org/index.php/Path_Manipulation, accessed 8 Nov 2013.
[125] https://www.owasp.org/index.php/Resource_Injection, accessed 8 November 2013.
[126] http://www.thesecurityblogger.com/?tag=network-reconnaissance, accessed 8 Nov 2013.
[127] http://www.thesecurityblogger.com/?p=2241, accessed 2 Dec 2013.
[128] http://www.shodanhq.com/, accessed 19 Nov 2013.
[129] https://datafinder.com/, accessed 8 Nov 2013.
[130] http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf, accessed 8 Nov 2013.
[131] https://cloudsecurityalliance.org/research/top-threats/, accessed 8 Nov 2013.

3.14 Targeted Attacks

Targeted attacks are characterized by their long endurance and specificity of the victim. Targeted attacks are further characterised by the capability level and dedication of the threat agent deploying the attack: all of the (successful) attacks reported in 2013 have been performed by threat agents with assumedly large resources[132]. Another important observation in the reporting period is a shift of APT targets from financial institutions to politically motivated targets such as NGOs, governmental organisations, politically active groups, etc[133,134].

In the reporting period we have assessed that:

- 2013 has been characterised by numerous APT attakcs, whereas it has become clear that one should not assume only a few rogue states as main originators of targeted attacks. There are quite some nation states that have developed sufficient capabilities and infrastructure to successfully launch targeted attacks that can be used to infiltrate all kinds of targets.
- In 2013, targeted attacks demonstrated their true potential. In particular, cyber espionage attacks using targeted attack campaigns reached dimensions that went far beyond expectations[135,136].
- With recent advances in mobile threats such as malware, code injection, scam/spam, etc., mobile platforms have become an important attack surface for targeted attacks[95,137]. It is worth mentioning that mobile spyware applications might become strong tools for APTs targeting Bring Your Own Device environments[138].
- Targeted attacks are applied as a pressure instrument at multiple levels. Concrete examples in the reporting period of successful attacks to notable social media accounts[96,139] have shown the potential towards the materialisation of risks similar to "Digital Wild Fires in a Hyper-connected World"[140].
- Sophistication, complexity and stealthiness of targeted attacks are state-of-the-art in cyber-attack techniques[141]. Prevention from such attacks is a complex task that has to embrace all levels of organisational assets, from technology to processes to people. The defence has to be prepared and implemented as orchestrated as the attack itself.

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Exploit Kits, Code Injection, Botnets, Worms/Trojans, Identity Theft/Fraud, Information Leakage, Physical Damage/Theft/Loss, Phishing, Spam, Rogueware/Ransomware/Scareware, Targeted Attacks, Watering Hole.

[132] http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, accessed 7 Nov 2013.
[133] http://www.eset.com/us/resources/threat-trends/Global_Threat_Trends_June_2013.pdf, accessed 7 Nov 2013.
[134] http://www.networkworld.com/news/2013/022813-targeted-attack-against-tibetan-activists-267224.html, accessed 7 Nov 2013.
[135] https://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons/at_download/fullReport, accessed 7 Nov 2013.
[136] http://www.globalresearch.ca/nsa-spies-on-world-bank-imf-un-pope-world-leaders-and-american-politicians-and-military-officers/5356455, accessed 7 Nov 2013.
[137] https://www.securelist.com/en/blog/208194186/, accessed 7 Nov 2013.
[138] http://www.kindsight.net/sites/default/files/Kindsight-Q2-2013-Malware-Report.pdf, accessed 7 Nov 2013.
[139] http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall, accessed 7 Nov 2013.
[140] http://www.weforum.org/reports/global-risks-2013-eighth-edition, accessed 7 Nov 2013.
[141] http://www.securelist.com/en/analysis/204792292/IT_Threat_Evolution_Q1_2013, accessed 7 Nov 2013.

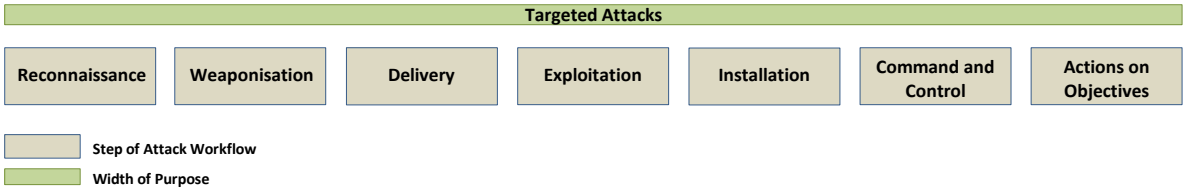


Figure 18: Position Targeted Attacks in attack workflow

3.15 Watering hole attacks

Watering hole attacks consist of the attempt to attack a certain target group by manipulating web sites visited and trusted by members of this target group. When visiting a manipulated web site, devices of members of the target group get eventually infected[142].

Although already mentioned in 2012, in the reporting period this threat has significantly increased and led to several successful attacks targeting high tech companies[143,144], but also governmental organisations [145]. Though relatively low in number, these attacks have demonstrated the effectiveness of this threat as it has hit companies who are at the leading edge of technology. Hence, it is alarming that when targeting lower tech users, such attacks will be at least equally successful! This has created a lot of awareness in the threat analysts' community[47], especially due to the fact that such attacks are usually launched within more extensive targeted attacks.

In the reporting period we have assessed that:

- Information about surfing habits are tracked via tracking services as the ones used by marketing companies to collect data. By tracking users of a specific company, it is possible to find web sites that are frequently used by groups of people. Obviously, these web sites are the best candidates to infect[146].
- Watering hole attacks have some commonalities with search engine poisoning (SEP): attracting potential victims to visit an infected web site based on their interests. However, watering hole attacks are more effective especially when attackers want to focus to a specific user group.
- It is worth mentioning that watering hole attacks are more a method to downsize the effort of threat agents while being more successful: fewer web site infections do more effectively reach target victim group. Otherwise, the methods used for victim infection are the ones mentioned above (drive-by downloads, exploit kits, malware).
- It is expected that deployments of this type of threat will increase in the future[147]. It might be meaningful if owners of infected web sites inform their visitors. At the end, every web site is a "water hole" of some user group.

Observed current trend for this threat: *increasing*

Related threats: Drive-by Downloads, Exploit Kits, Code Injection, Worms/Trojans.

[142] http://en.wikipedia.org/wiki/Watering_Hole, accessed 3 Dec 2013.
[143] http://threatpost.com/why-watering-hole-attacks-work-032013/77647, accessed 8 Nov 2013.
[144] http://ics-cert.us-cert.gov/monitors/ICS-MM201306, accessed 8 Nov 2013.
[145] http://www.darkreading.com/attacks-breaches/us-department-of-labor-website-discovere/240153967, accessed 8 Nov 2013.
[146] https://blog.cloudsecurityalliance.org/2013/09/23/watering-hole-attacks-protecting-yourself-from-the-latest-craze-in-cyber-attacks/, accessed 8 Nov 2013.
[147] http://blog.fortinet.com/Security-101--Watering-Hole-Attacks/, accessed 19 Nov 2013.

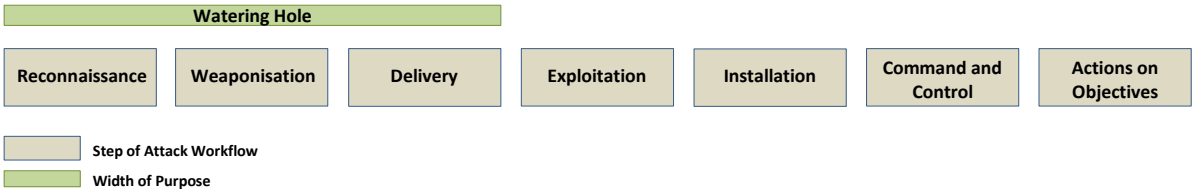


Figure 19: Position of Watering Hole in attack workflow

3.16 Visualising changes in the current threat landscape

As expected, in comparison with 2012 there have been changes in the current threat landscape. To facilitate comparability with the results of 2012, this section visualises changes between current threat landscape 2012 and 2013. In addition, changes in threat rankings of are also indicated in the table below.

Top Threats 2012	Assessed Trends 2012	Top Threats 2013	Assessed Trends 2013	Change in ranking
1. Drive-by exploits (this threat has been renamed)	↑	1. Drive-by downloads	↑	→
2. Worms/Trojans	↑	2. Worms/Trojans	↑	→
3. Code Injection	↑	3. Code Injection	↑	→
4. Exploit Kits	↑	4. Exploit Kits	↑	→
5. Botnets	↑	5. Botnets	→	→
6. Denial of Service	→	6. Physical Damage/Theft/Loss	↑	↑
7. Phishing	→	7. Identify Theft/Fraud	↑	↑
8. Compromising Confidential Information (this threat has been renamed to Data Breaches)	↑	8. Denial of Service	↑	↓
9. Rogueware/ Ransomware/Scareware	→	9. Phishing	↑	↓
10. Spam	↓	10. Spam	→	→
11. Targeted Attacks	↑	11. Rogueware/Ransomware/ Scareware	↑	↓
12. Physical Theft/Loss/Damage	↑	12. Data Breaches	↑	↓
13. Identity Theft	↑	13. Information Leakage	↑	↑
14. Information Leakage	↑	14. Targeted Attacks	↑	↓
15. Search Engine Poisoning (Threat dropped from list because no evidence	→	15. Watering Hole	↑	↑

Top Threats 2012	Assessed Trends 2012	Top Threats 2013	Assessed Trends 2013	Change in ranking
about this threat has been found in analyzed material)				
16. Rogue Certificates (Integrated with worms/trojans)	↑			

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

Table 2: Overview of Current Threat Landscapes 2013 and 2012 comparison

ETL 2013: Threat Agents

4 Threat Agents

4.1 Overview of Threat Agents

In this chapter we provide an overview of the threat agents that have been identified in this year's analysis. Firstly, it should be mentioned that in 2013 more elaborated/qualitative descriptions have been found on this topic[148,149]. Moreover, through relevant publications[150,151,152,153,154] details about incidents and potential attacks caused by each particular threat agent group have been published. All in all, in comparison to 2013 a better and more concise coverage of threat agents in the causal chain of attacks has been assessed. This is definitely an advancement compared to 2012.

The above developments support a better description of threat agents, including profiles, motives capabilities, etc. While the threat agents from ETL 2012 still remain relevant, the details assessed this year provide the basis for a more elaborated description. In addition, two new threat agents groups have been added, script kiddies and cyber fighters.

In particular, the major threat agents identified are as follows:

Corporations: The objective of corporations is mainly the creation of competitive advantages. Hence, corporations may act as hostile threat agents when involved in activities to: collect business intelligence, to breach intellectual property rights, to gather confidential information on competitors, to be engaged in intelligence gathering connected to bids, etc. Generally speaking, corporations may be involved in reconnaissance activities, intrusion and data breach. Corporations may engage salaried threat agents from other groups to achieve their objectives. Depending on their size, sector and level of engagement in high-tech areas and secrecy levels corporations may possess significant cyber capabilities to perform malicious activities towards achieving their objectives. In such cases, corporations may use sophisticated targeted attacks to infiltrate their victims.

Nation States: 2013 has clearly unveiled the true dimension behind the potential of this threat agent group. In the reporting period it has become clear, that cyber activities are not a matter of one-two nation states. Rather, multiple nation states have developed capabilities that can be used to infiltrate all kinds of targets both governmental and private in order to achieve their objectives. Main targets of this threat agent group are state secrets, military secrets, data on intelligence, as well as threatening the availability of critical infrastructures. Acting with a high level of capabilities, the methods/vectors of launched attacks vary significantly. Yet, high effort and high sophistication targeted attacks belong to the main attack methods used. The degree of successfulness of performed attacks can be considered as rather high.

Hacktivists: Hacktivists is a threat agent group that has enjoyed great media attention, particularly in 2011[155] and to some extend 2012. Hacktivists are ideologically motivated individuals that can dynamically form groups/subgroups, usually lacking a central organisation structure. Their main

[148] https://www.ncsc.nl/english/current-topics/news/cyber-security-assesment-netherlands.html, accessed 30 Oct 2013.
[149] http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf, accessed 16 Oct 2013.
[150] http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=302:hackers-profiling-who-are-the-attackers&catid=50:issue-7&Itemid=187, accessed 16 Oct 2013.
[151] http://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background, accessed 16 Oct 2013.
[152] http://www.verizonenterprise.com/DBIR/2013/, accessed 16 Oct 2013.
[153] http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf, accessed 16 Oct 2013.
[154] http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/global-profiles-of-the-fraudster/Documents/global-profiles-of-the-fraudster-v2.pdf, accessed 2 Dec 2013.
[155] http://www.wired.com/threatlevel/2011/12/2011-hactivist-verizon/, accessed 30 Oct 2013.

motivation is usually the defence of ideas that are sometime manifested[148]. Due to the dynamics behind this group, it is difficult to shape a sharp profile for this group: 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.). Targets of hacktivists are selected in such a way, that media attention to successful cyber-attacks create high visibility (e.g. government sites, big companies, media, public and private infrastructure components, etc.). It is common that breached data are published to embarrass victims and achieve desired public attention. Although not considered to possess average capabilities, due to group dynamics and media visibility, hacktivists may achieve severe impact.

Cyber Terrorists: yet controversially discussed, this group is mainly used to attribute potential threats to cyber-targets that will harm national security and society[156]. As a matter of fact, only minor incidents have been documented. Officials speak about some attacks that are being kept confidential[157]. 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. Activities of this threat group are mostly impact oriented and may affect or harm large parts of society, just to generate necessary pressure. Cyber terrorists may use technology both as the means and target of their attacks, while critical infrastructures comprise one of the main targets[158]. Further targets of this group may be traffic control, military infrastructures[159], government systems, etc. Information collection, reconnaissance and social engineering are methods that may belong to the key capabilities of this group, while access to high tech tools and methods are also considered within their capabilities, especially due to blurring lines between this and other threat agent groups[160].

Cybercriminals: This threat agent group is the most widely known as its objective is to obtain profit from illegal/criminal activities in the cyberspace. Cybercriminals act mainly in the cyberspace and so do their victims. Hence, cybercriminals are involved in fraud regarding all kinds of e-finance, e-commerce, e-payment, ransomware, cybercrime-as-a-service, delivery and development of malicious tools and infrastructures. It should be noted, that in this group we do not consider individuals involved in a "traditional" crime using IT to facilitate their criminal activity.

Cybercriminals have high capabilities in performing their tasks, can be globally interconnected[161] and may easily obtain access to the means needed for their hostile activities. 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[162].

Although essentially belonging to the group of cybercriminals group, we discriminate between users and **providers/developers/operators** of malware, botnets and other kinds of malicious cyber-tools. It is considered that those who develop, deliver and operate malicious infrastructures are the most skilled among all cyber threat agents and as such they have the highest cyber striking power from all other threat agent groups considered. Nevertheless, one can assume that they mainly provide the means for attacks (i.e. services/tools) to other cybercriminals and they may not be actively involved in fraudulent activities.

[156] http://en.wikipedia.org/wiki/Cyberterrorism, accessed 3 Dec 2013.
[157] http://www.psmag.com/politics/nsa-really-stopping-terrorist-plots-70159/, accessed 3 Dec 2013.
[158] http://www.timesofisrael.com/internet-cable-cutters-caught-by-egypt-signal-new-terror-threat/, accessed 16 Oct 2013
[159] http://www.japantimes.co.jp/news/2013/09/04/world/al-qaida-hopes-to-sabotage-destroy-drones/, accessed 16 Oct 2013
[160] http://cryptome.org/2013/04/terrorist-hackers.htm, accessed 16 Oct 2013
[161] http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf, accessed 16 Oct 2013.
[162] http://www.smh.com.au/technology/technology-news/silk-road-mastermind-ross-william-ulbricht-tripped-up-by-careless-online-mistake-20131003-2utky.html, accessed 16 Oct 2013.

Cyber Fighters: Cyber fighters are groups of nationally motivated citizens. This is an emerging phenomenon where patriotic motivated groups of citizens bear the potential to launch cyber-attacks in a coordinated manner[163]. 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[164]. One can argue that such groups are special cases of Hacktivism (i.e. an evolution or yet another instance). 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[165]. Their activities may include conflicts with other groups (i.e. other hacktivists). Depending on their number and capabilities, such groups may form a considerable striking power. They can be considered as underground cyber fighters in support of the interests of a nation state[166].

Script Kiddies: "As more young people learn to code, more will learn to hack"[167]. This statement indicates the birth site of hackers. This is when young individuals get thrilled about achievements and skills of tech savvy individuals who assumedly gave a lesson to persons, organisations or brands considered outrageous. Despite being in a self-discovery phase and technically novice, due to their large number, script kiddies are susceptive to external influences from other threat agent groups, in particular cyber criminals and hacktivists. On the other hand, due to reduced knowledge about both the use of hacking tools and the consequences of their activities, script kiddies may achieve great impact. Typically this threat agent group is engaged in DDoS and code injection attacks[149]. Script kiddies may also form ad-hoc groups with common targets and develop to a considerable striking power[168].

Online Social Hackers: there is an increasing significance of social engineering as element of cyber-attack pattern[169]. Therefore this threat agent group plays a key role when deploying cyber threats. These online social hackers are skilled with social engineering knowledge, are in the position to analyse and understand behaviour and psychology of social targets and to generate false trust relationships. Even if not necessarily using high-tech methodologies and tools, activities of this threat agent group may cause significant impact especially in areas of identity theft, collection of confidential personal data, user credentials, cyber bullying, etc[170]. The capabilities of this group can be characterised as low to medium as regards the use of technology. However their social engineering skills might be quite high. With increasing use of social networking, it is expected that the importance of this group in cyber-attacks will grow in the future.

Employees: this group is the one behind the insider threat that often scores within the top 10 cyber threats[171,172]. This threat agent group (or also widely referred to as "internal actors"[148]), can be staff, contractors, operational staff, former employees, etc. The reasons for acting within threat agent group may vary significantly, i.e. lax handling of security procedures, user error or even malicious intent. This threat group is usually equipped with low to medium-tech methods and tools. However, due to graded access rights to all kinds of assets of an organisation, they might cause significant

[163] http://krebsonsecurity.com/2013/06/iranian-elections-bring-lull-in-bank-attacks/, accessed 29 Nov 2013.
[164] http://www.dailymail.co.uk/news/article-2313652/AP-Twitter-hackers-break-news-White-House-explosions-injured-Obama.html, accessed 16 Oct 2013.
[165] http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf, accessed 16 Oct 2013.
[166] http://mashable.com/2012/08/10/syrian-electronic-army/, accessed 16 Oct 2013.
[167] http://www.fastcolabs.com/3013102/why-the-script-kiddie-next-door-is-just-as-dangerous-as-a-chinese-government-hacker, accessed 16 Oct 2013.
[168] http://www.cnhinews.com/wpbloom/x862178305/Teens-hone-hacking-skills-in-contests, accessed 16 Oct 2013
[169] http://public.tableausoftware.com/views/VERISCommunity/SummaryofActions#1, accessed 16 Oct 2013.
[170] http://resources.infosecinstitute.com/social-engineering-a-hacking-story/, accessed 16 Oct 2013.
[171] https://cloudsecurityalliance.org/research/top-threats/, accessed 16 Oct 2013.
[172] http://www.red-book.eu/, accessed 16 Oct 2013.

damage, especially when having malicious intent. Dissatisfaction, frustration, dissent or corruption are common causes behind malicious behaviour of this threat agent group.

The above mentioned threat agents are a consolidated form of the significant ones mentioned in relevant publications. Yet the list is not exhaustive: depending on particular incidents, viewpoints and scope, additional groups are being considered. Besides this fact, and given the often blurry lines between legitimate cyber agents and hostile ones, cases where "camp changes" take place have been reported. In other words, bad guys might be engaged within state or company sponsored efforts[173] and good guys may serve hostile tasks[174].

In order to give an overview of existing agents/actors acting in cyber space - both hostile and friendly - a taxonomy of cyber agents has been developed (see Figure 20). 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.

The purpose of this figure is to deliver information on agents/actors acting in cyber space such as motive, capability or areas of engagement. Furthermore, 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. Drawing these kinds of possible interdependencies on demand, may facilitate the work of security experts willing to understand possible interactions among these groups and thus better assess the capabilities behind asserted threat agents.

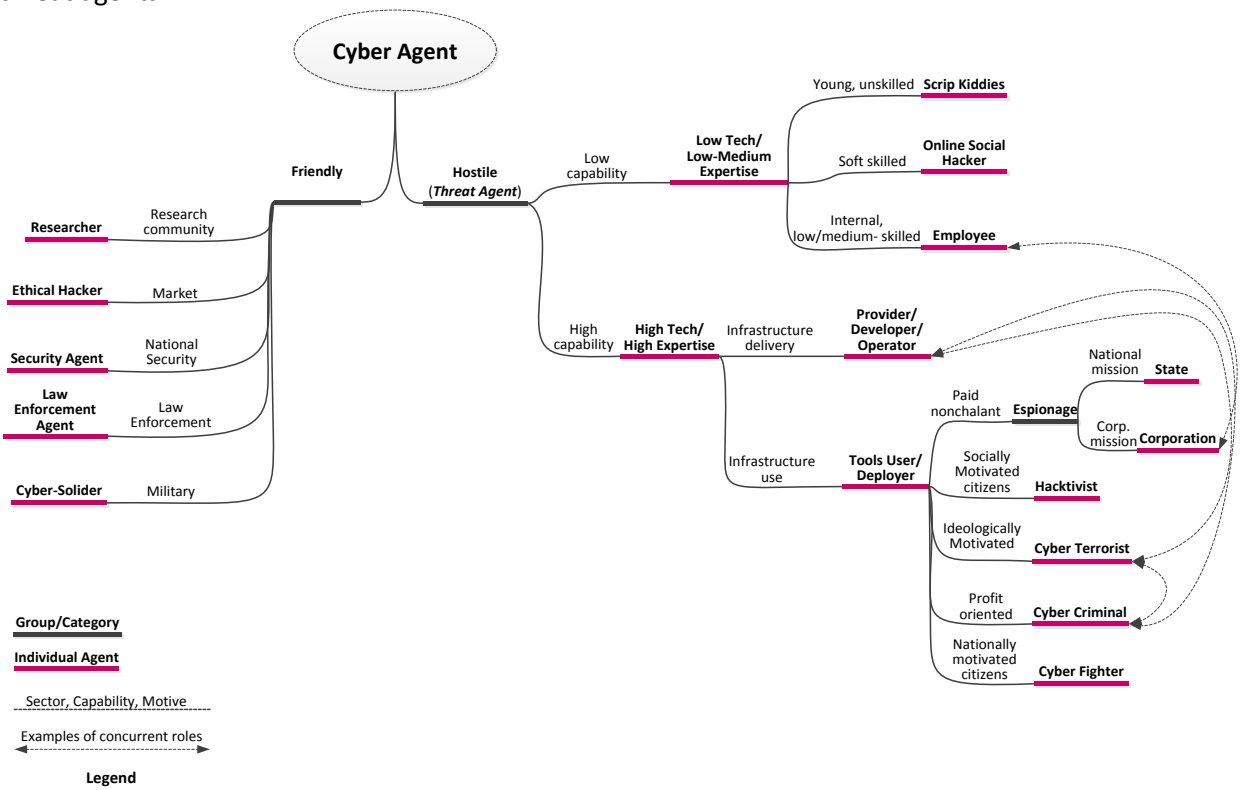


Figure 20: Overview of Agents in Cyber Space

[173] http://www.telegraph.co.uk/technology/news/10317634/Cyber-hackers-hired-to-attack-governments-and-banks.html, accessed 16 Oct 2013.
[174] http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/, accessed 16 Oct 2013.

4.2 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 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.

As already stated, overlaps among the threat agent groups do exist. This is reflected in the table by eventual similarities in the way of threat deployment.

	Threat Agents								
	Corporations	Nation States	Hacktivists	Cyber Terrorists	Cyber Criminals	Cyber Fighters	Script Kiddies	Online Social Hackers	Employees
Drive-by exploits		✓			✓				
Worms/Trojans		✓		✓	✓	✓		✓	✓
Code Injection	✓	✓	✓	✓	✓	✓	✓		
Exploit kits			✓	✓	✓	✓	✓		
Botnets	✓	✓	✓	✓	✓	✓			
Physical Damage/ Theft/ Loss	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity Theft/. Fraud	✓	✓	✓	✓	✓	✓	✓	✓	✓
Denial of service		✓	✓	✓	✓	✓	✓		✓
Phishing	✓	✓			✓			✓	
Spam	✓				✓			✓	
Rogueware/ Ransomware/ Scareware					✓				
Data Breaches	✓	✓	✓	✓	✓	✓	✓		✓
Information Leakage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Targeted Attacks	✓	✓	✓	✓	✓	✓		✓	
Watering Hole	✓[175]	✓			✓	✓			

Table 3: Involvement of threat agents in the top threats

[175] http://www.zdnet.com/symantec-industrial-espionage-on-the-rise-smbs-a-target-7000014061/, accessed 2 Dec 2013.

ETL 2013: Emerging Threat Landscape

5 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. Both threat trends and emerging technology areas have been either directly mentioned or have been implicitly assessed from the analysed material.

Threat trend identification by means of emerging technology areas is an approach that has also been followed in ETL 2012. It aims at establishing the context between threats and various technology areas that will undergo significant development in the near future (i.e. coming year). By mapping threats to emerging developments, future/emerging trends within the threat landscape are being captured.

Within ETL 2013, all of the areas addressed in 2012 have been maintained, as they still represent the state-of-the-art in IT technology development. As such they are of paramount importance for a large group of stakeholders from both public and private sectors. Last year's list has been expanded with one "newcomer", the *Internet of Things*. Whilst it is not a new area in cyber-security, this area is considered by analysts as an innovative field that has reached a maturity enabling its entrance to the market.

It is worth mentioning, that in the reporting period ENISA has performed specific/detailed assessments in the areas of Critical Infrastructures and Trust Infrastructures; assessments regarding threat and risk exposure of smart grids and the use of e-ID in financial sector have been performed and are going to be available as autonomous ENISA deliverables. The presented information regarding these two areas is a summary of the work conducted in these ENISA projects.

In particular, the emerging technology areas considered are:

- *Critical Infrastructures*: Critical infrastructures are a vital part of society and national sovereignty. The security of critical infrastructure will remain high priority for governments and big operators.
- *Mobile Computing*: Besides cloud computing and Internet of Things, mobile computing is another major trend that has changed traditional IT architecture. Mobile computing has made digital convergence to reality and has caused a revolution in application development. This area it is going to continue being a platform for innovations.
- *Social Networking*: The paradigm of interconnected individuals, professionals and knowledge is one of the major social phenomena of recent years. Social media have already penetrated the lives of a significant part of online users. This development is going to continue for the years to come.
- *Cloud Computing*: Cloud computing is an integral counterpart of the current internet architecture. Besides storage, it increasingly accommodates application services by thus innovating commercial IT operations. Cloud computing also embraces the promise of a more effective implementation of security mechanisms by leveraging on economies of scale.
- *Trust Infrastructure*: Trust infrastructures and authentication infrastructure in particular is the spine of cyber-security. Attacks, but also technology and implementation issues hereof are important elements of every cyber-security assessment. It is expected that this area will retain its central role for the future.
- *Big Data*: The role of big data for security has worried security professionals for quite some time now. In the reporting period, big data has been the subject of vivid discussions after revelations on industrial espionage and state sponsored surveillance activities. Through the proliferation of mobile and smart devices, big data is going to be for quite some time in the future on the focus of cyber-security professionals and cyber-criminals alike.
- *Interconnected Devices – Internet of Things*: Inter- and hyper-connected devices form the future of internet: the Internet of Things. Low cost devices form an interconnected community to

provide smart consumer services in many areas, such as smart houses, e-health, industrial control systems, energy, cars, transportation, etc. Alike the other areas, the Internet of Things will be the main source of technological innovations and challenges in the years to come.

It is obvious that these areas are not completely independent or overlap free. Developments in one area may include aspects of others (i.e. technology, components, functions). However, splitting threat trends according to those areas allows for a better establishment of the context of each threat and helps assessing and understanding trends.

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. Just as in the current threat landscape, the sequence of presentation of the emerging threats is a prediction of the overall frequency of the threat materialization (i.e. more frequent threats appear first). For each area, the top 10 threats have been assessed, expect in the area of Internet of Things, where only 9 emerging threats were identified. When applicable, references to resources indicate the sources used for the assessment. These sources can be used by interested readers in order to find more extensive information about the corresponding topic. In the following discussions, trends issued in the reporting period have been accommodated[176,177].

5.1 Threat Trends in Critical Infrastructures

This area is key for society and national security. Critical Infrastructure and their main components Industrial Control Systems (ICS) have and are still considered as main potential targets of highly capable threat agent groups, namely terrorists and nation states. Due to their complexity, critical infrastructures are complex systems and so is their protection. One can take as given that availability of critical infrastructure is the most important property to maintain. This sheds the right light to the exposure but also the difficulty of protection of such infrastructures. Finally, critical infrastructures and ICSs are considered within strategic priorities for cyber-security by various actors[178,179,180].

In the reporting period, ENISA has delivered a dedicated threat landscape in the area of smart grids. As a matter of fact, smart grids are an ideal representative in the area of critical infrastructures: being a very complex system combining both legacy and innovative systems; and playing a key role for energy distribution in the years to come. As in many complex systems, smart grids consist of a variety of components ranging from high end monitoring and control systems up to low cost end-user devices. These systems grow gradually by using a variety of communication protocols, applications and devices all being at a different maturity level both from the technology and security utilization point of view. Hence, the main cause of threat exposure in this area emerges from the technological diversity, component integration, coordination level and cyber security preparedness

[176] For a comprehensive summary of issues trends please visit: http://www.zdnet.com/cybersecurity-in-2014-a-roundup-of-predictions-7000023729/, accessed 3 December 2013.
[177] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Fokus_IT-Sicherheit_2013_nbf.pdf;jsessionid=9CFAC1176CDDA96ACA5DB0EF7AA77882.2_cid359?__blob=publicationFile, accessed 3 December 2013.
[178] http://www.red-book.eu/, accessed 20 Nov 2013.
[179] http://www.gtsecuritysummit.com/2014Report.pdf, accessed 20 Nov 2013.
[180] https://www.ncsc.nl/binaries/en/current-topics/news/cyber-security-assesment-netherlands/1/Cyber%2BSecurity%2BAssessment%2BNetherlands.pdf, accessed 20 Nov 2013.

of the actors involved in the supply chain. Known incidents in the reporting period show that the energy grid is one of the main targets of cyber-criminals[181].

Top emerging threats to Critical Infrastructure and to smart grids in particular are:

	Emerging Threat	Threat Trend
1.	Worms/Trojans (affecting important parts of the grid infrastructure such as ICS).	↑
2.	Code Injection	↑
3.	Drive-by Downloads	↑
4.	Exploit Kits	→
5.	Physical Theft/Loss/Damage	↑
6.	Denial of Service	↑
7.	Botnets	↑
8.	Phishing	↑
9.	Information Leakage	→
10.	Targeted Attacks	→

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 4: Emerging threats and their trends in the area of Critical Infrastructures – Smart Grid

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

- Through the utilisation of wireless communication, interconnected components will be vulnerable to relevant threats. Besides this kind of vulnerabilities, it seems that there is a lack of available information vulnerabilities related to CII infrastructures, scenarios and components. It is expected that in the near future capabilities for building up and testing of such scenarios will be developed[182].
- Words matter: it is important to develop and maintain terms and definitions. Besides serving as a basis for experts, such a vocabulary would be necessary in the area of crisis management regarding smart gird, but also other areas of CIIP: it emerges from the necessity to bridge engineering and cyber security terms[183,184].
- It seems to be very important to elaborate on overlapping issues of safety, physical security vs. cyber security. CIIP is a traditional engineering area in which safety standards and physical security requirements are mandatorily implemented. Cyber security overlaps with safety and

[181] http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage, accessed 20 Nov 2013.
[182] http://www.tecnalia.com/, accessed 21 Nov 2013.
[183] http://cip.gmu.edu/wp-content/uploads/2013/06/October-2013_Financial-Services.pdf, accessed 21 Nov 2013.
[184] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids/at_download/fullReport, accessed 21 Nov 2013.

physical security as it concerns the operational parts of CIIs. These overlaps need to be identified and interfaces need to be established[185].

- Like any complex infrastructure used for large amounts of users/customers, the energy grid will generate large amounts of data. This data will reflect, among other things, customer behaviour regarding energy consumption. This massive information is a valuable asset for many organisations and actors. It is expected that this information might be subject of data breaches, manipulation, and fraud[186].
- Due to the inherent openness of the grid infrastructure, security measures based on detection of intrusion/misuse will be necessary. Such measures will be developed around data exchanged information. In particular, anomaly detection seems to be a very promising method to data manipulation, fraud and targeted attacks[187].
- Due to the need of intensive investments in smart grid infrastructures, it is likely that security will be developed on the basis of scenarios[188;189]. This is the next logical step from current practices based on requirements[190] and will be part of activities regarding the definition of security architectures for smart grids in the coming year.

5.2 Threat Trends in Mobile Computing

As it can be easily foreseen, mobile computing will remain the prevailing platform for end-user interaction and online activities. Being the perfect media convergence platform, mobile devices will continue to be first choice for all kinds of users. But mobile computing goes beyond end-user devices: mobile sensors, wirelessly interconnected components of intelligent environments, mobile security devices, etc. are taking an important position within the mobile ecosystem that is currently under significant development. Together with various infrastructure components and development capabilities, this ecosystem becomes an inherent part of the internet architecture and services.

The current trend of "migration" of all kinds of malicious methods and tools into this ecosystem will be continued in future[179]. But besides moving their attention to mobile computing, adversaries will invest a lot of energy in identifying vulnerabilities in the mobile ecosystem: this is a new challenge, as due to changes in user interaction and architecture models, new kinds of vulnerabilities will be discovered and exploited.

Top emerging threats to mobile computing are:

Emerging Threat	Threat Trend
1. Worms/Trojans (in particular performing man-in-the-mobile[239] attacks).	↑
2. Physical Theft/Loss/Damage	↑

[185] http://www.researchgate.net/publication/256918306_A_cyber-physical_experimentation_environment_for_the_security_analysis_of_networked_industrial_control_systems, accessed 21 Nov 2013.
[186] http://www.forbes.com/sites/jeffmcmahon/2013/09/26/big-data-from-smart-grid-tells-utilities-more-than-they-want-to-know/, accessed 21 Nov 1023.
[187] http://www.ida.liu.se/labs/rtslab/publications/2012/RacitiNadjmTehrani-critis12.pdf, accessed 21 Nov 2013.
[188] http://www.smartgridnews.com/artman/publish/Technologies_Security/Electric-Sector-Failure-Scenarios-and-Impact-Analyses-6106.html, accessed 21 Nov 2013.
[189] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_security.pdf, accessed 21 Nov 2013.
[190] http://www.nist.gov/el/smartgrid/cybersg.cfm, accessed 21 Nov 2013.

	Emerging Threat	Threat Trend
3.	Drive-by Downloads	↑
4.	Exploit Kits	↑
5.	Code Injection[191]	↑
6.	Phishing	↑
7.	Identity Theft	↑
8.	Information Leakage	↑
9.	Botnets[192]	↑
10.	Data Breaches	↑

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:

- In the reporting period we have seen significant defences of mobile security at risk: vulnerabilities can be introduced into apps by overcoming vetting process of app store operator[179,193]; and sandboxes have been bypassed[194]. These shortcomings provide an attack surface that will be exploited by adversaries.
- The mobile ecosystem has introduced a change in existing protection strategies of organisations. The fact that insecure devices enter into the company network makes them attractive to threat agents as a steppingstone to the corporate environment.
- New attack patterns presented recently have given an impression of possible malicious activities involving mobile devices[195]. If seen in combination with the availability of low cost miniaturized hardware[196,197], one can expect that in short to middle term more and more attack vectors attacking mobile devices will emerge.
- The mobile ecosystem is one of the most significant "contributors" to big data. Apart from the risk that this data is available to developers, operators and wireless providers without user consent, it can also be easily manipulated[198]. Yet, it is a fact that the implications of this exposure to end-users are not yet fully understood[179].

[191] http://threatpost.com/remote-code-injection-vulnerabilities-discovered-in-ios-apps, accessed 22 Nov 2013.
[192] http://www.theregister.co.uk/2013/09/06/android_malware_spotting_hitching_a_ride_on_mobile_botnet/, accessed 22 Nov 2013.
[193] http://www.tgdaily.com/mobility-brief/73765-apple-stores-malware-problem-exposed-by-researchers, accessed 22 Nov 2013.
[194] http://threatpost.com/using-kernel-exploits-bypass-sandboxes-fun-and-profit-031813, accessed 27 Nov 2013.
[195] http://hackaday.com/2013/08/01/blackhat-ios-device-charger-exploit-installs-and-activates-malware/, accessed 22 Nov 2013.
[196] http://www.raspberrypi.org/, accessed 22 Nov 2013.
[197] http://www.bbc.co.uk/news/world-europe-24539417, accessed 22 Nov 2013.
[198] https://mocana.com/blog/2013/03/26/manipulating-real-time-android-based-traffic-data-at-black-hat-europe/, accessed 22 Nov 2013.

- Last but not least, mobile devices are a main source for information leakage threats. Seen in combination with the vast amount of data that are available through the utilization of mobile devices (e.g. geo-location, media behaviour, etc.), the potential of this information becomes evident. Currently, mobile operators investigate business opportunities based on this data[199]. All this indicates that the attractiveness of mobile will grow further, also for adversaries.

5.3 Threat Trends in Social Networks

In the reporting period social online activities have continued to increase and go mobile[200]. In addition to this trend, more and more activities regarding leisure, education and professional life are performed over social media. As result, this technology becomes the main channel for communication, collection of knowledge[201], dissemination of information, marketing.

During 2013 it has also become clear, that information from social media is just a part of the information available online about behaviour and habits of users. Other sources are blogs, mails, web activities, phone calls, etc. When all this data is combined via mining tools, large amount of details about people's lives can be assessed[202], with young generation being the main group that is digitally omnipresent[178]. It is evident that available social networking data are extremely interesting for both good and bad. In the reporting period we have seen representative examples of misuse of social media, such as misinformation, fake news, identity theft, fake social accounts etc[203]. These cases are the evidence that social media have become a regular fixture in hacking business.

Top emerging threats to social networks are:

Emerging Threat	Threat Trend
1. Worms/Trojans[204,205]	↑
2. Information Leakage (by abusing information found social media, attackers can achieve advances in all attack patterns and threats)	↑
3. Phishing[206]	↑
4. Spam[207]	↑
5. Identity Theft	↑

[199] http://www.technologyreview.com/news/513016/how-wireless-carriers-are-monetizing-your-movements/, accessed 22 Nov 2013.
[200] http://www.businessinsider.com/facebook-is-almost-mobile-first-2013-10, accessed 25 Nov 2013.
[201] Within ENISA Threat Landscape, for example, we have experienced impressive dissemination speeds of information related to cyber-threats and cyber-security, sometimes exceeding the speed of professional services.
[202] http://www.theguardian.com/world/2013/feb/10/software-tracks-social-media-defence?CMP=twt_gu, accessed 25 Nov 2013.
[203] http://socialmediatoday.com/mrisher/1227536/asocial-network-how-hackers-use-social-networks-destroy-your-online-life, accessed 25 Nov 2013.
[204] http://www.techspot.com/news/53679-zeus-trojan-modified-for-social-media-purposes.html, accessed 25 Nov 2013.
[205] http://www.computing.co.uk/ctg/news/2272203/social-media-malware-rising-significantly-says-mcafee-report, accessed Nov 2013.
[206] http://www.symantec.com/connect/blogs/phishing-easy-way-compromise-twitter-accounts, accessed 25 Nov 2013.
[207] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf, accessed 25 Nov 2013.

	Emerging Threat	Threat Trend
6.	Exploit Kits[208] (Exploit kit spam campaigns target social networks)	↑
7.	Physical Theft/Loss/Damage (lost devices contain credentials for social accounts)	↑
8.	Drive-by Downloads[209] (installation of browser add-ons to hijack social media accounts)	↑
9.	Code Injection[210] (leaked or breached big data will provide adversaries with information to effectively perform their attacks)	→
10.	Botnets[211]	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 6: Emerging threats and their trends in the area of Social Networks

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

- The speed of information propagation over social media is higher than any other journalistically crafted publication. As a consequence, misinformation propagation speed exceeds that of serious journalism. Social media spread context free content. The relevance and authenticity of spread information cannot be easily checked. This is a risk for society[212], as misinformation can be used with political, cultural, censorship or propaganda objectives in mind.
- An important question for users for social networking systems will be how to balance their privacy and security with benefits gained by using applications processing their location data, personal preferences and habits. While some will look for anonymity based solutions, others might scrutinise their digital presence. It is expected that anonymity technologies will be developed and that the discussion about digital rights and "right to be forgotten"[213,214] will be refuelled.
- Information found in big data can lead to a virtual growth of knowledge about social networking: it includes information about visited sites, performed searches, collaboration, phone calls, blogs, calendars, contact lists, etc[178]. This network of interconnections can be easily modelled and constructed. It encompasses much more than friends and likes: it is a reflection of human live in the digital space. Besides using this data for good, adversaries will keep trying to misuse this information.
- Human engineering attacks through online social hackers will continue keeping the cyber security community busy. Social hacking will remain an important channel for malware, phishing,

[208] http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-exploit-kit-spam-campaign-hits-pinterest/, accessed 25 Nov 2013.
[209] http://blog.trendmicro.com/trendlabs-security-intelligence/malware-hijacks-social-media-accounts-via-browser-add-ons/, accessed 25 Nov 2013.
[210] http://arstechnica.com/security/2013/02/facebook-computers-compromised-by-zero-day-java-exploit/, accessed 25 Nov 2013.
[211] http://www.computerworlduk.com/news/security/3443498/botnets-target-social-networks-with-spam/?olo=rss, accessed 25 Nov 2013.
[212] http://www.weforum.org/reports/global-risks-2013-eighth-edition, accessed 25 Nov 2013.
[213] http://www.nationalsecuritylawbrief.com/the-right-to-be-forgotten-in-a-digital-age/, accessed 25 Nov 2013.
[214] http://www.mondaq.com/x/274428/data+protection/Court+Ruling+Reinforces+The+Right+To+Be+Forgotten+On+Social+Media+Sites, accessed 25 Nov 2013.

spamming and identity theft attacks[215]. Despite awareness, well-crafted social media attacks will show high success rates, especially when additional information (see section on big data and Internet of Things) is being used to round up the attack.

- Social forensics is an interesting area that analyses user behaviour from various information sources providing evidence about interactions, trust level of connections, exchanged messages, etc. Beyond using this tools/technology for law enforcement reasons, such tools might be used to unveil social "robots", that is, social profiles that have been created with nefarious objectives in mind[178,216].

5.4 Threat Trends in Cloud Computing

Cloud computing is becoming an integral part of the business IT ecosystem: company services and data may be hosted in cloud servers, while at the same time end-users maintain theirown cloud (storage) services to increase effectiveness and convenience. Mostly, business data in the cloud are protected only via security mechanisms provided by the cloud environment. Taking as given that business data are stored in multiple cloud environments (e.g. through business users using could storage on their mobile devices), the enforcement of a comprehensive security policy for cloud services is a challenging task. This is an opportunity for attackers: potential weaknesses in cloud security are abused to gain access to company data. And these weaknesses are not at the cloud side but rather at the user side. For example (cloud) identity theft: the easiest targets for attackers will be weakly secured mobile devices accessing a cloud service.

Gradually, cloud services go beyond storage and cover hosting of applications and databases. Through the proliferation of web services - accessed via browsers and apps - the cloud is exposed to software vulnerabilities and web-specific attacks. In the reporting period we have seen many attack patterns affecting cloud services based on threats like code injection[217], malware and botnets[218,219]. We will keep seeing these threats affecting cloud services, while cloud providers will further enhance protection of their services via additional security mechanisms[220]. Moreover, the continuous concentration of data in the cloud will raise issues of resilience, as these services are going to reach a high degree of criticality. Nevertheless, in the reporting period significant efforts have been invested by cloud providers in performing threat and risk assessments for cloud services[221],[222]. Also other stakeholders have issued protection practices for cloud services[223]. This contributes to a better assurance of cloud services; in many cases protection offered in a cloud environment may be higher than in legacy IT-environments. Yet due to complexity, the implementation of these measures remains a challenge[224].

[215] http://www.pcworld.com/article/2059940/fake-social-media-id-duped-securityaware-it-guys.html, accessed 25 Nov 2013.
[216] http://online.wsj.com/news/articles/SB10001424052702304607104579212122084821400?mod=WSJ_hp_LEFTWhatsNewsCollection, accessed 25 Nov 2014.
[217] https://www.digitalocean.com/community/articles/how-to-secure-a-cloud-server-against-sql-injection, accessed 3 Dec 2013.
[218] http://www.alertlogic.com/resources/cloud-security-report/, accessed 2 Dec 2013.
[219] http://www.darkreading.com/cloud, accessed 4 Dec 2013.
[220] http://www.cs.ucsb.edu/~koc/ns/projects/12Reports/PucherDimopoulos.pdf, accessed 3 Dec 2013.
[221] https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf, accessed 26 Nov 2013.
[222] http://security.force.com/security/tools/forcecom/scannerhelp, accessed 2 Dec 2013.
[223] https://docs.google.com/document/d/1KBpPRBY9E0_v_H2JvFO-_XUXy-KSfBTRXOphjqoNS_4/edit?pli=1, accessed 3 Dec 2013.
[224] http://www.darkreading.com/cloud/cloud-security-measures-too-opaque-for-c/240148526, accessed 3 Dec 2013.

Top emerging threats to cloud computing are[225]:

	Emerging Threat	Threat Trend
1.	Information Leakage	↑
2.	Code Injection (web servers and web applications on the cloud will be subject of code injection)	↑
3.	Identity Theft	↑
4.	Data Breaches	↑
5.	Worms/Trojans	↑
6.	Phishing (cloud customers may be victims of phishing in order to obtain credentials)	↑
7.	Denial of Service	↑
8.	Exploit Kits (exploit kits may include attack patterns to steal credentials of cloud services and they might be installed in the cloud (Malware-as-a-service)).	↑
9.	Physical Damage/Loss/Theft (lost end-user devices may contain credentials to access cloud services used)	↑
10.	Botnets	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 7: Emerging threats and their trends in the area of Cloud Computing

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

- The concentration of large amounts of data within small number of huge computing centres has continued in the reporting period. Undoubtedly these concentrations of user data are THE target for threat agents. Attackers will keep trying to take over control of these data[226,227] and services in order to achieve numerous of malicious objectives, the main being to breach large amounts of data.
- Following recent nation state sponsored espionage activities, one can expect customers to pay more attention to the location of data centers and the impact of foreign legislation on cloud services[228]. Such issues might be show-stopper for existing cloud services and foster the creation of appropriately equipped clouds. These issue will be relevant for a significant number of

[225] It should be noted that the threats mentioned below result from the exposures of both customer and provider and include all kinds of services offered/used (i.e. IaaS, PasS, SaaS).
[226] http://www.websense.com/content/websense-2014-security-predictions-report.aspx, accessed 25 Nov 2013.
[227] http://www.infosecurity-magazine.com/view/35234/sql-injection-and-crosssite-scripting-attacks-surge-in-q3/, accessed 25 Nov 2013.
[228] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds, accessed 25 Nov 2013.

potential users coming from the governmental and agency sector, especially within Europe[229,230,231].

- In general, the proliferation of web services accessed via browsers opens doors for all kinds of web-specific threats in the entire chain of components involved in the interaction, that is, from the client to the back end system. Hence, when cloud services are used (i.e. SaaS, IaaS) these are exposed to threats abusing software vulnerabilities such as code injection, exploit kits, rogueware/ransomware/scareware. Nevertheless, it is expected that cloud computing will positively contribute to reduce exposure[232]. This is because of security measures that can be put in place and enforcement of software and infrastructure architectures/frameworks.
- The computing capabilities of cloud environments are an attractive use-case for cyber-criminals. Instead of maintaining expensive and easy to locate own computing capabilities, powerful cloud computers would be beneficial for their purposes for nefarious activities[233,234]. The race between threat agents and cloud providers is going to be continued in 2014. Cloud providers will have to find ways to detect malicious use of their resources.
- Through the use of mobile computing, business users consume various cloud storage services for the purposes of convenience. Often, these services are operated on private basis and circumvent corporate security policies. Lax cloud security policies introduce a serious risk for corporate data. Information thefts, elevation of privilege and data breaches are the results. It is expected that the challenge of scrutinizing security of business data will continue bothering security professionals.
- Customers will look for encryption mechanisms/technology to mitigate certain risks, but encryption can only mitigate some risks. In many cloud computing scenarios, customers are actually processing data on the cloud platform, and this processing cannot, for example, be encrypted to prevent eavesdropping by the provider. Further, current encryption mechanisms/technology does not provide the desired efficiency for use within a cloud environment[179,235]. It is expected that new mechanisms will be introduced in order to avoid existing shortcomings[236] of available approaches[237].

5.5 Threat Trends in Trust Infrastructures

Trust infrastructures considered to be systems, components and functions that provide strong authentication. As such, trust infrastructures are building the backbone for a variety of security mechanisms, as they establish authenticity, and thus trust, between an object and a subject. Subjects may be humans or other trustworthy components participating in a trusted interaction. Such functions are increasingly utilized by service providers, while it is clear that authentication methods without trusted devices (i.e. hardware/non-replicable tokens) are less secure and thus

[229] http://europa.eu/rapid/press-release_MEMO-13-898_en.htm, accessed 25 Nov 2013.
[230] http://www.pcworld.idg.com.au/article/464906/european_us_cloud_providers_go_head-to-head_after_nsa_revelations/, accessed 25 Nov 2013.
[231] http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing, accessed 25 Nov 2013.
[232] http://www.infosecurity-magazine.com/view/32698/microsoft-unveils-cloudbased-realtime-botnet-infosharing-initiative/, accessed 25 Nov 2014.
[233] http://securitywatch.pcmag.com/software/299448-malware-as-a-service-simplifies-launching-cyber-attacks, accessed 25 Nov 2013.
[234] http://www.computerworld.com/s/article/9241629/Cybercriminals_use_Google_Cloud_Messaging_service_to_control_malware_on_Android_devices accessed 25 Nov 2013.
[235] http://www.enisa.europa.eu/publications/flash-notes/securing-data-in-cyber-space/at_download/file, accessed 25 Nov 2013.
[236] http://www.networkworld.com/news/tech/2013/040913-cloud-encryption-268542.html, accessed 25 Nov 2013.
[237] http://eprint.iacr.org/2013/409.pdf, accessed 25 Nov 2013.

vulnerable[238]. Trust infrastructures are one of the main targets of cyber criminals: successful attacks against them unveil a wide variety of fraud options, especially in the area of banking, finance and payment.

In the reporting period, ENISA has conducted work regarding trusted authentication in the area of e-Finance and e-Payment services. Various methods of widely used authentication services are considered, including passwords (OTP, TAN), signatures (based on chip or mobile), tokens (OTP generators, mobile phones, etc.), etc. Particular attention is being paid to multi-channel authentication methods, i.e. two-factor authentication. This work examines the threat exposure of electronic Identity and Authentication Systems (eIDAS) and assesses related risks. Though sector specific, this work is considered representative for trust infrastructure. Conclusions made and open issues can be applied to other related areas by analogy. Authentication has been addressed in other related reports, by identifying risks, issues and gaps[178].

Top emerging threats to trust infrastructure are:

Emerging Threat	Threat Trend
1. Phishing	↑
2. Identity Theft	↑
3. Drive-by Downloads	↑
4. Worms/Trojans (in particular performing identity theft and man-in-the-browser[239],[240] attacks).	↑
5. Code Injection (affecting web baking servers)	↑
6. Exploit Kits	↑
7. Physical Theft/Loss/Damage	↑
8. Information Leakage (esp. session hijacking in order to launch replay and man-in-the-middle attacks).	↑
9. Data Breaches	↑
10. Targeted Attacks	→

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 8: Emerging threats and their trends in the area of Trust Infrastructure

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

- Chains of authentication and discontinuity of used media (all kind of devices, applications to perform authentication) have proven to be weak points of currently used mechanisms. In the

[238] http://www.computerweekly.com/news/2240207697/Google-to-release-two-factor-security-token, accessed 21 Nov 2013.
[239] http://en.wikipedia.org/wiki/Man-in-the-browser, accessed 21 Nov 2013.
[240] http://viewer.media.bitpipe.com/1039183786_34/1295277188_16/MITB_WP_0510-RSA.pdf, accessed 2 Dec 2013.

short to medium term the need emerges to impose end-to-end authentication with as few authentication steps as possible, with strong mechanisms and less devices involved (i.e. service decoupling[241]).

- Chains of authentications to elevate access rights to more sensitive actions and data access need to be checked upon logical and technical impermeability. Unification of authentication methods among various application areas should be an objective for operators of e-commerce, e-payment and e-baking applications.
- Broken authentication [242] is a significant risk. Especially in web applications, broken authentication has achieved second of top 10[243]. In the middle term, a more intensive testing of weaknesses/potential attack patterns for used authentication mechanisms seems to be necessary[244].
- Successful attacks on authentication target the human interface. It is important to raise awareness among operations and users of authentication systems through continuous training[245,246].
- Authentication mechanisms implemented through application and kernel functions are susceptive to attacks bypassing sandboxes[247]. This fact underlines the importance of information security in application development. It also demonstrates potential weaknesses of software authentication solutions, especially for high risk operations/transactions.
- Authentication over NFC-enabled devices is coming[248]. While this technology is considered as very effective in implementing authentication/identification functions, the security functions of NFC itself are not part of the NFC tag specification. Due to contactless nature of this protocol, interception of communication is quite easy. As NFC becomes popular, attack methods on NFC devices will be an issue to take care of in the middle term[249].

5.6 Threat Trends in Big Data

Big data are large collections of data that emerge from the operation and usage of large infrastructure, applications, devices/appliances, web services, user interaction, etc. In the reporting period, big data has enjoyed significant popularity[250251]. Also the potential behind this "asset" has been more extensively manifested and discussed[199,252]. As a matter of fact, big data seems to be main source of monetization from commercial organisations that are in the possession of this good[253]. This is gradually understood by end users as they suffered information losses or the negative consequences to their privacy resulting from their online activities[254]. Generally speaking, big data has started to become an issue because various actors in society have been aware about

[241] http://hdknr.github.io/docs/identity/signed_nonce.html, accessed 22 Nov 2013.
[242] https://www.owasp.org/index.php/Broken_Authentication_and_Session_Management, accessed 22 Nov 2013.
[243] https://www.owasp.org/index.php/Top_10_2013-Top_10, accessed 22 Nov 2013.
[244] http://link.springer.com/chapter/10.1007/978-3-642-37949-9_63#page-1, accessed 22 Nov 2013.
[245] http://www.inforisktoday.com/whitepapers/when-criminals-defeat-authentication-lessons-learned-from-w-874, accessed 22 Nov 2013.
[246] http://queue.acm.org/detail.cfm?id=2422416, accessed 22 Nov 2013.
[247] http://threatpost.com/using-kernel-exploits-bypass-sandboxes-fun-and-profit-031813, accessed 22 Nov 2013.
[248] http://www.nfcworld.com/technology/authentication/, accessed 22 Nov 2013.
[249] http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/, accessed 22 Nov 2013.
[250] http://www.computerworld.com/s/article/9215033/Big_data_to_drive_a_surveillance_society, accessed 26 Nov 2013.
[251] http://www.computer.org/portal/web/computingnow/content?g=53319&type=article&urlTitle=big-data%2C-big-brother%2C-big-money, accessed 26 Nov 2013.
[252] http://reports.weforum.org/outlook-14/the-future-of-surveillance/, accessed 26 Nov 2013.
[253] http://www.com/watch?v=85mu9PLWCuI, accessed 23 Nov 2013.
[254] http://www.youtube.com/watch?v=Rn4Rupla11M, accessed 27 Nov 2013.

the value and potential of this asset, albeit it has been actually generated as side-product on online activities.

In the short to medium term, big data is considered as an important asset that can be used as a source for monetization through commercial organisations. Moreover, recent worldwide discussions on surveillance based on big data have given rise to concerns about use vs. abuse of this information with regard to the privacy of users.

But also the influence big data will have on the market are of big interest and importance: is big data going to create monopolies that will build their influence on knowledge of user's life and on profiles? How are states going to regulate the collection and use of this information in order to find the best balance between security and privacy, while maintaining the opportunities for new business models to be developed and established?

Top emerging threats emerging from the misuse of big data by adversaries are[255]:

	Emerging Threat	Threat Trend
1.	Information Leakage (big data leaks will provide information to adversaries to facilitate the launch of attacks)	↑
2.	Data Breaches (information gained from big data will provide insights in order to breach user and company data. Breaches of big data will be a priority for attackers too)	↑
3.	Worms/Trojans (leaked or breached big data will provide adversaries with information to effectively perform their attacks)	↑
4.	Exploit Kits (leaked or breached big data will provide adversaries with information to effectively perform their attacks)	↑
5.	Code Injection (leaked or breached big data will provide adversaries with information to effectively perform their attacks)	↑
6.	Drive-by Downloads (leaked or breached big data will provide adversaries with information to effectively perform their attacks)	↑
7.	Phishing (leaked or breached big data will provide adversaries with information to effectively perform their attacks)	↑
8.	Identity Theft (leaked or breached big data will provide adversaries with information to effectively perform their attacks)	↑
9.	Physical Theft/Loss/Damage (leaked or breached data from stolen/lost devices will provide adversaries with information to effectively perform their attacks)	↑
10.	Targeted Attacks (this threat will be used in order to breach collected big data from collecting organizations)	↑

Legend: ↓ Declining, ➲ Stable, ↑ Increasing

Table 9: Emerging threats and their trends in the area of Big Data

[255] The threats considered are primarily related to the abuse of big data by adversaries to launch attacks. They do not cover threat exposure of big data itself (i.e. manipulation, fraud, theft, etc.).

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

- As the amount of data created by user activities grows and users realize that this data is used for business, profiling, marketing and analysis purposes[256], the desire to keep information private will grow[257]. This desire emerges from the feeling of complete and constant observability of their lives through a virtually omnipresent, yet blurry defined "big brother".
- Given that big data will be the main source for collecting intelligence at all levels of society (commercial, state), it inevitably moves in the focus of adversaries. And it does so in a dual way: firstly it comprises main source of intelligence for malicious purposes, and as such becomes a desirable good; and at the same time is a target for manipulations in order to hide own activities (for the later see next point).
- As big data will be increasingly used for analysis, anomaly detection, intelligence gathering by governments and agencies, mission creep, etc., adversaries will look for ways to hide their activities. In a similar manner, they will try to manipulate big data to seamlessly affect results of analysis, metrics and fool established response mechanisms[179].
- Despite existing public/media confidence that big data is collected, controlled and analysed by government agencies, the fact is that it mainly emerges through systems and technologies that are owned and operated by private sector[252]. Hence, activities of governmental agencies take place at a second level[251] with regard to primary creation and collection. As far as this interaction is not transparent, the fears of public regarding influence to democracy and self-determination of private data usage will grow. Intransparent data collection and analysis regimes are a risk for all involved actors and the pressure to mitigate this risk will constantly grow.
- Uncontrolled collection, usage and dissemination of user and systems data are the perfect playground for malicious activities. Over the existing cyber-physical relationship, fraud regarding cyber-reputation and a person's digital footmark is likely to happen. And is may have devastating impact to people's lives[254]. Such fraudulent activities targeting individual persons or group of individuals will be based on access and manipulation of big data.
- An important part of big data is data related to security. According to experiences gained in the reporting period, it seems that harnessing the potential of big security data is still at an immature state. Though commercially explored by security companies, security data has still enormous potential with regard to coordination of activities, response and knowledge gathering. Areas like threat analysis, attack pattern recognition and quick adaptation of existing defence may be significantly advanced when using big security data. In short to medium term, the security community will leverage on these potential advantages, forced by the number, variety, sophistication and impact of cyber-attacks.
- Security big data are quite easily available/accessible from non-commercial sources[258],[259]. It should be assessed if some controls might be necessary to identify potential recipients of this information.

5.7 Threat Trends in the Interconnected Devices: The Internet of Things

Although not new[260], the issue of security of interconnected devices and Internet of Things (IoT) has bothered threat analysts in the reporting period[179,180,257,264,266]. This is obviously because of the

[256] http://www.spiegel.de/netzwelt/web/lg-smart-tvs-senden-heimlich-nutzerdaten-in-die-konzernzentrale-a-934614.html, accessed 26 Nov 2013.
[257] http://www.symantec.com/connect/blogs/2014-predictions-symantec-0, accessed 26 Nov 2013.
[258] http://datalossdb.org/, accessed 27 Nov 2013.
[259] http://www.shodanhq.com/, accessed 27 Nov 2013.
[260] https://www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel, accessed 26 Nov 2013.

estimated number of interconnected devices in one-two years' time (ca. 15 to 25 billion[179]). Main concern is the low level of security provided: small devices are interconnected, usually over insecure channels and protocols, generate a great deal of data, are designed to perform primitive tasks and do not implement any security measures.

Because of poor security, eventually poor maintenance but also due to the nature of data and functions performed, smart environments are considered as the ultimate target for cyber criminals. Potential impact of attacks based on, for example, home appliances will be very difficult to prevent. One needs to imagine a phishing attack whereas the adversary possesses knowledge about the whereabouts of the smart home of the victim. Or the impact of information leaked from a user's media centre in the creation of profiles. Not to talk about potential impact from the manipulation of smart devices used within e-Health applications, monitoring of minors[261] and elderly people. Even critical infrastructure services based on smart devices are at risk[262].

Given these developments, it is obvious that in the near future the Internet of Things is going to attract the attention of cyber-security professionals, government and consumers. Although potentially new threats are going to be emerge in this area, in the table below we try to demonstrate how available threats may be applied to this ecosystem.

Top emerging threats to Interconnected Devices are:

Emerging Threat	Threat Trend
1. Worms[263]/Trojans	↑
2. Information Leakage	↑
3. Data Breaches	↑
4. Identity Theft	↑
5. Phishing	↑
6. Spam	↑
7. Physical Damage/Loss/Theft	↑
8. Denial of Service	↑
9. Targeted Attacks	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 10: Emerging threats and their trends in the area of Interconnected Devices

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

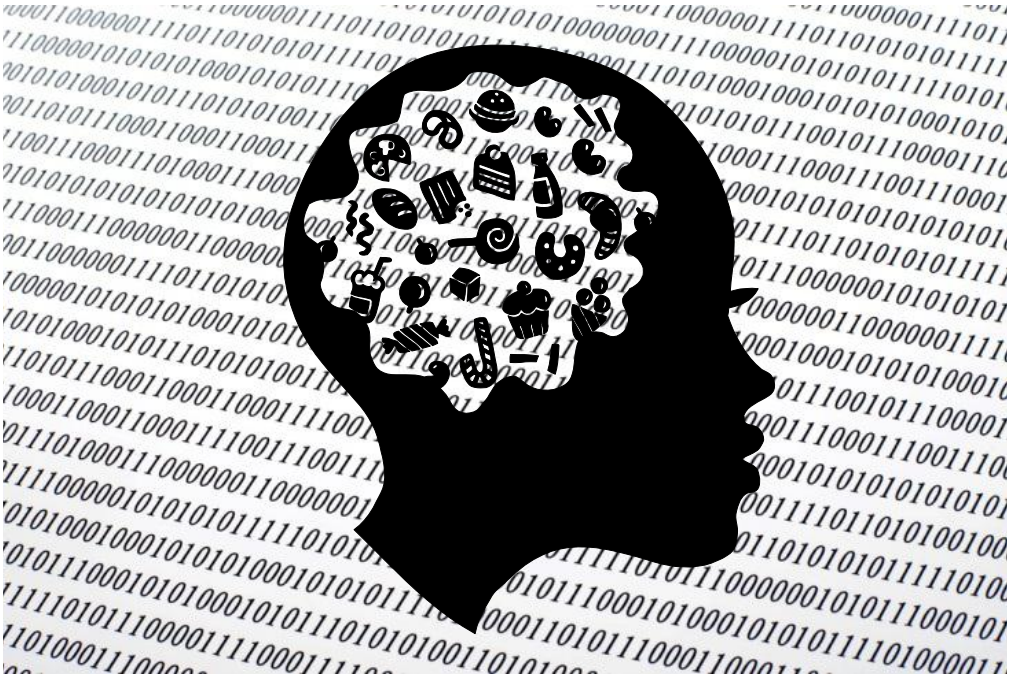
[261] http://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/, accessed 26 Nov 2013.
[262] http://www.spokesman.com/stories/2013/oct/28/israeli-road-control-hacked-shutting-down-haifa/, accessed 26 Nov 2013.
[263] http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices, accessed 2 Dec 2013.

- Greater device interaction leads to larger amount of data creation and data concentration within a home network with lax security measures. Moreover, given the fact that interconnected devices permanently send data, they pose performance requirements to network infrastructures, also outside their locations (based on the external interconnections available)[180.]
- Dynamicity in connection of appliances leads to dynamic context and content of transmitted data[264]. This leads to potentially large amount of vulnerabilities and security issues, as data may reveal details about the functions, operating patterns and behaviour of the owner. This poses significant privacy challenges/concerns[180].
- Devices have built in functionality, often as embedded systems. These functions are not accessible to users, may include unknown functions[265] and are difficult to update, maintain, i.e. patching[257] to accommodate updates fixing identified vulnerabilities[266].
- Due to none or low level security, smart environments per se do not generate information to inform users about their operational status, nor can they be easily connected to existing security back-end systems such as incident and emergency response.
- Interconnected devices and smart environments provide an ideal environment for all threat agent groups to perform malicious activities[257] ranging from data collection and data manipulation up to fooling home appliances of their victims, thus creating harm even to their lives.

[264] https://www.europol.europa.eu/content/project-2020-scenarios-future-cybercrime, accessed 26 Nov 2013.
[265] http://doctorbeet.blogspot.gr/2013/11/lg-smart-tvs-logging-usb-filenames-and.html, accessed 26 Nov 2013.
[266] http://www.theatlantic.com/technology/archive/2013/08/coming-soon-the-cybercrime-of-things/278409/, accessed 26 Nov 2013.

Page intentionally left blank

ETL 2013: Food for Thought
Lessons Learned and Conclusions



6 Food for Thought: Lessons Learned and Conclusions

6.1 Lessons learned

Being in the second year of its existence ETL 2013 was a step forward in the learning curve of information collection and threat analysis. In this section we would like to share some experience gathered during this work. This experience concerns two sides of the activities performed: a) the "process" followed in ENISA's work, that is, experience with information collection and analysis, and b) some highlights from the analysed content. In particular:

Lessons from the ETL process:

- From the reception of this work, we believe that threat landscapes are very interesting for multiple stakeholders in the area of cyber security and beyond. Although threat information is available, analysis and assessment are at a low level of maturity.
- It is necessary to include more information sources into the threat landscape, such as incident data, perform better analysis of breaches and coordinate and enhance threat knowledge.
- Social media are a very fast dissemination channel. Besides risks (see section 5.3) this brings some advantages, especially when time matters as it is the case in threat analysis. By following various individuals, organisations and groups in social media, we were in the position to increase the speed of threat information acquisition.
- By tracking the uptake of previous ENISA deliverables in the area of threat landscape (i.e. ETL 2012 and 2013 midyear report), we have found out that the appetite of the security and media community with regards to information on threats and threat trends is quite big. One can argue that this strong trend will be continued in the coming year.
- Although usually outside of the scope of assessments, the threat landscape is significantly affected by low frequency large impact events[267,268,269,270] (black swans[271]). Black swans have an impact on the threat landscape, as they represent high impact unexpected events. After a black swan event, it is clear that a new kind of threat does exist (independently from the likelihood of occurrence). It is then left to threat analysis if this kind of threat should be considered in threat analysis. However, in the cyber security community, black swans are often meant to be seldom events that are not being managed and/or their mitigation is expensive. This is a deviation from the definition of black swan. This can create confusions within experts and bears risks.
- In the reporting period we have found out that quite a few European organisations work on areas touching the threat landscape. It is imperative that these organisations are coming together and adapt their work in a way that all potential synergies are mobilized. ENISA will take up this coordination task in the coming years.

Lessons from the analysed content:

- Although fairly simple security measures significantly minimize threat exposure, it is remarkable that still over half of the organisations fail to apply/implement them.

[267] http://arstechnica.com/security/2013/03/spamhaus-ddos-grows-to-internet-threatening-size/, accessed 22 Oct 2013.
[268] http://blog.crysys.hu/2013/02/miniduke/, accessed 22 Oct 2013.
[269] http://intelreport.mandiant.com/, accessed 22 Oct 2013.
[270] http://news.yahoo.com/e-u-pushes-stricter-data-protection-snowden-nsa-233347589.html, accessed 22 Oct 2013.
[271] http://en.wikipedia.org/wiki/Black_swan_theory, accessed 22 Oct 2013.

- Identification of regional trends is not always possible for all threats at a moderate level of effort. This is because the geographic dimension for all kind of threats and incidents is not always reported.
- Relevance of threats for various organisation profiles is not always possible at a moderate level of effort. This is because it is difficult to draw conclusions about types of assets found within company profiles. Yet, ENISA work in 2013 in the area of smart grids and eID for financial services has demonstrated that this is possible when sufficient resources and expertise are available.
- With the current level of cooperation, data availability and trust levels, it is not possible to validate current threats and threat trends based on real data in a near-time manner. Although significant amount of data exists, it is not optimally used for the validation of threat assessments.Within ENISA it is planned to combine information collection (i.e. including Art 13a activities[272]) with exchange of information with other stakeholders, both public and private ones. This will be enforced witin the work on the ETL 2014.
- Current practices in cyber security measures are based on the assumption that a cyber-security strategy should minimize exposure of as many threats as possible. By transferring this approach to the automotive sector, it is as if one tries to build a car that survives all accidents unscathed.
- In the reporting period, we have seen a far better coverage of threat agents within the collected material. A deficit in this area has been mentioned in the conclusions of ETL 2012. It seems that the community has achieved good progress on this matter.
- The awareness for cyber threats has increased, especially within security professionals. Albeit being a result of a more efficient collection practices from ENISA's side, there is evidence that in the reporting period number, width and quality of threat information collected has significantly increased. This is a significant and important improvement in comparison to 2012.
- In the reporting period we were in the position to "test" own and other predictions made in 2012. The comparison has been made within 2013 mid-year report[29]. We have found out that the majority of predictions for 2013 have been realized.
- The arrest of the developer and operator of the exploit kit Blackhole[54] is considered as a major event in the reporting period. It remains to be seen what impact this event will have in the fast developing area of exploit kits: is this going to create an unfilled gap, are other adversaries going to take over further development of the tool or are other exploit kits going to fill the gap? Evaluation of this situation is decisive for understanding the interconnections and levels of cooperation among threat agents. This may be a strong indicator for the entire cyber-threat landscape.

6.2 Conclusions

The above mentioned learned lessons bring us seamlessly to the conclusions of ETL 2013 by means of open issue and need for further work. The sequence of open issues below is according to assumed importance:

- The **end-user perspective** needs to be seriously taken into account by the cyber-security community. End-users have to get more actively involved in protection against cyber-

[272] https://resilience.enisa.europa.eu/article-13, accessed 3 Dec 2013.

threats. Analysis shows that knowledge about implementation of simple security measures is not available in the wide basis of end-users. Adoption of simple security measures by end-users would *half* the number of cyber incidents worldwide!

- It has become clear that a greater **coordination** of information collection, analysis, assessment and validation among involved organisations is necessary. Numerous public and private organisations work on overlapping issues of threat information collection and threat analysis. Increased coordination, for example, among the ones working on open source information and ones working with operational data could increase quality and speed of assessed threats.. Moreover, activities of Member States and stakeholders from private sector will be also considered. Objective is to assess the feasibility of such coordination/cooperation and establish proper areas and steps to obtain it.
- Threats need to be expanded with additional information regarding **attack workflow/kill chains and attack patterns**. This information needs to be extracted from incident analysis, establishing thus the necessary feedback to improve quality of assessed threats. This will be real added-value for all stakeholders using a threat landscape, as every threat description would contain information on attack scenarios derived from real incidents.
- **Building threat intelligence** remains one of the main challenges in the cyber-security community: ways to facilitate information collection, develop tools to support threat analysis, sharing of information, etc. In 2013 ENISA has delivered important information in approaches and tools for creating and sharing threat intelligence[273]. It is important to capitalize on these recommendations and establish a community working towards their achievement.
- In the analysed material, security experts have underlined the importance of *increasing* **speed in threat assessment** and dissemination by reducing detection and assessment cycles. In order to achieve this, stakeholders need to synergise (see above point) and tune up their activities.
- Increasing sophistication of attacks, increasing complexity of IT-architectures, increasing volume of data and blurred limits of security perimeter pose significant challenges to cyber-security defences. The research community need to **examine the elasticity of security** measures: besides active measures (e.g. firewalls, IDSs), passive security mechanisms need to be developed (e.g. automated policy generation, validation and enforcement[274]). IT-infrastructures need to be resilient and robust to successful attacks without suffering severe impact regarding their availability, integrity and confidentiality.

[273] http://www.enisa.europa.eu/activities/cert/support/data-sharing, accessed 28 Nov 2013.
[274] http://www.ptidej.net/seminar/130418%20-%20Makan%20Pourzandi%20-%20ESF%20--%20An%20Elastic%20Security%20Framework%20For%20Cloud%20Infrastructures/130418%20-%20Makan%20Pourzandi%20-%20ESF%20--%20An%20Elastic%20Security%20Framework%20For%20Cloud%20Infrastructures.pdf, accessed 3 Dec 2013.

TP-AE-13-001-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: 978-92-9204-120-5
ISSN: 2363-3050
DOI: 10.2824/022950

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