enisa
European Network and Information Security Agency

ENISA Threat Landscape

Responding to the Evolving Threat Environment

[Deliverable – 2012-09-28]

Contributors to this report

This report was produced by ENISA using publicly available information on incidents and threats.

Authors of this report in alphabetical order are:

- *Louis Marinos*, European Network and Information Security Agency and
- *Andreas Sfakianakis*, European Network and Information Security Agency

The authors would like to thank all ENISA colleagues and external experts who provided information on existing threat resources and have contributed through discussions on the subject matter.

About ENISA

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

Contact details

For contacting ENISA for general enquiries on this report, please use the following details:

- E-mail: opsec@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

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

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

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2012

Contents

List of Tables

1 Executive Summary

The ability to respond to the evolving cyber-threat environment is not a destination but rather a journey. There is and always will be a permanent race in cyber space between attackers and defenders. Unfortunately, at the moment attackers are one step ahead. In this race it is impossible to know and, finally, to beat the opponents without understanding their attack methods. Hence, understanding threats is a vital element towards protecting cyber assets that needs to be in the focus of information security professionals.

The ENISA Threat Landscape provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. Over 120 recent reports from security industry, networks of excellence, standardisation bodies and other independent institutes have been analysed.

The current top cyber threats have been identified. Current threat trends have been derived from the comparison of current threat information with that of the last years. Finally, a number of threat trends for emerging areas of Information Technology have been formulated. We call them emerging threats and they have been identified for the following areas: mobile computing, social technology, critical infrastructures, trust infrastructures, cloud computing and big data. The summary of the achieved results has been consolidated into a single table that has been attached to this executive summary (see Table 1).

The target group of this report are: decision makers, security professionals, risk managers but also interested individuals who would like to obtain information about threats and find references to current available material on this topic.

"Know yourself, know the enemy. A thousand battles, a thousand victories"[1].

The ENISA Threat Landscape document is a contribution towards understanding the "cyber enemy". Many steps need to follow to leverage on Sun Tzu's wisdom. Some of those are proposed in the conclusions of this report. In summary, proposed steps are:

- Collect and develop better evidence about attack vectors;
- Collect and develop better evidence about impact achieved by adversaries;
- Collect and maintain more qualitative information about threat agents;
- Use a common terminology within threat reports;
- Include the user perspective;
- Develop use cases for threat landscapes;
- Collect security intelligence that cover incidents in an end-to-end manner;
- Perform a shift in security controls to accommodate emerging threat trends.

[1] *Sun Tzu, http://www.brainyquote.com/quotes/authors/s/sun_tzu.html, accessed 16 November 2012.*

Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 1: Overview of Threats and Trends of the ENISA Landscape[2]

[2] *Please note that the ranking of threats in the emerging landscape is different than the one in the current landscape. The rankings of emerging threats can be found in the corresponding section (see section 6).*

2 Introduction

This report provides a security threat landscape based on aggregated data collected from ENISA stakeholders. The report is a deliverable that has been defined within the ENISA work programme 2012 in the area of Identifying & Responding to the Evolving Threat Environment. ENISA's objective with this work is to provide stakeholders with information on how threats are evolving. More specifically, the aim is to identify particular trends thereby helping relevant stakeholder communities to recognise and respond to changes in the threat landscape that are particularly relevant to their activities.

The approach followed in the production of this deliverable is to collect and aggregate existing, publicly available information and compile it into single report on the threat landscape. Over 120 individual reports have been taken into account for this work, most of those issued in 2012. Elements of the ENISA threat landscape included in this deliverable are:

- A *Current Threat Landscape* consisting of development of threats as they have been reported by international stakeholders such as CERTs, industry, professional associations and academia and
- An *Emerging Threat Landscape* consisting of threat trends identified.

The target group of this document are security professionals who are interested in considering a threat landscape for their work, e.g. within risk assessments and definition of mitigation strategies. Another target group of this deliverable are decision makers who would like to understand emerging threat trends in order to consider them in their decision making process. The present material will be of interest for policy development, as threat trends will guide policy actions in the area of cyber-security, national cyber-security preparedness and possible cooperation initiatives to encounter cyber-attacks. Finally, the processes material and the presented findings will be a basis for experts to deepen into the subject matter of threat reporting and find detailed information on particular threats, technology areas, attack vectors and threat agents.

The present document is structured as follows: section 3 provides the scope of this work by setting the scene for the developed threat landscapes, referring to their components, highlighting the method of work and the kind of information being consolidated.

Section 4 refers to the current threat landscape. It presents the top threats identified and gives information about various key findings and the trends of each threat as they have been observed till today.

Section 5 delivers information on threat agents, in particular their capabilities and involvement within the identified current threat landscape.

Section 6 presents the assessed emerging threat landscape. In doing so, we have identified six emerging technology areas and we have delivered information about the relevant threats, together with trends that have been identified pro area.

Section 7 concludes this report by summarizing the findings.

Finally, interested individuals can find in the Annex detailed finding of the performed analysis, together with the references to the relevant information resources.

3 Scope and Definitions

3.1 Scope

3.1.1 What is threat landscape?

The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses/vulnerabilities, threats may lead to a loss or takeover of assets. The assets at stake are usually important elements within a value chain and may be related to sectors/scenarios/user groups. Hence, a threat landscape can be a prioritized list with threats grouped according to their asset relevance. Examples are: top 10 security threats[3], threats for smart phones[4], threats for App-Stores[5], etc.

There are numerous other examples of threat landscapes[6][7]: some contain just threats, others combination of threat information with various attack methods (vectors), others containing information about threat agents, exploits, vulnerabilities and so on. In some cases, threat landscapes contain an amount of information that makes them come very close to a *risk landscape* (see section 3.1.4).

3.1.2 What are the factors leading to a change of threat landscape?

There are quite a few "forces" that might lead to changes to the threat landscape. Taking a look at the elements of a risk and their interrelationship (see Figure 2) it becomes apparent that threats are related to vulnerabilities and thus to assets. In other words, the more valuable an asset, the more attacks it will be possibly exposed to. And existing vulnerabilities/weaknesses of the asset will lead to higher success rates of attacks. Thus threats depend heavily on vulnerabilities that can be exploited and the value of the assets at stake. Methods to identify and abuse vulnerabilities of assets are often mentioned as "Exploits".

Another reason leading to the evolution of a threat landscape is changes in the capabilities of threat agents. Given that parameters such as available skills, available tools, available resources, information on exploits and motivation make up the profile of a threat agent, any change that can affect these parameters will potentially lead to a change to the threat

---

[3] http://www.net-security.org/secworld.php?id=10154, accessed 12 November 2012.

[4] https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport, accessed 12 November 2012.

[5] http://www.enisa.europa.eu/media/press-releases/app-store-security2013-the-five-lines-of-defence-new-report-by-eu-cyber-security-agency-enisa, accessed 12 November 2012.

[6] https://www-950.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/ThreatLandscape2012/$file/ThreatLandscape2012.pdf, accessed 12 November 2012.

[7] http://www.bitdefender.com/media/materials/e-threats/en/H1_2012_E_Threat_Landscape_Report_Aug_6.pdf, accessed 12 November 2012.

landscape. Enhanced capabilities of threat agents will lead to a better identification and exploitation of weaknesses.

Finally, changes might be observed by means of new attack methods and new threats, emerging from new types of assets and new weaknesses/vulnerabilities. Often, the introduction of new technology results in weaknesses that are related to low technological maturity, improper use, improper integration with existing systems, low user awareness, etc. This builds the ground for new threats targeting such assets.

3.1.3 How many kinds of threat landscapes exist?

There might be various kinds of threat landscapes, depending on sector, kind/group of assets and time horizon assumed. Hence, when reported threats to assets are aggregated, one can talk about a current or contemporary threat landscape[8]. When threats to a certain type of infrastructure are encountered, e.g. to the Financial Sector, one can speak about a sector threat landscape. When conclusions from current threat landscape are projected to the future, we can talk of an emerging threat landscape[9] (also referred to as future threat landscape[10]).

Usually, a threat landscape can be derived from or is part of a risk assessment. Contemporary threats can be found in risk assessments of existing systems, whereas emerging threats can be found in assessments regarding emerging applications, technologies and assets in general[11][12].

In the case of current threats, reported incidents play a significant role: successful attacks to various systems/assets are collected by various entities, are aggregated and announced to the public (references). Ideally, this information should flow into risks assessments and lead to adaptations of identified risks and their mitigation strategies.

3.1.4 Threat landscape vs. risk landscape

As mentioned above, a threat landscape may contain significant information that goes towards the description of risks, such as vulnerabilities, assets and countermeasures (see also Figure 2). An example of such an approach is CAPEC[13]. CAPEC provides attack pattern enumeration and classification including mitigation controls, weaknesses, security requirements, etc.

---

[8] http://www.net-security.org/secworld.php?id=11034, *accessed 12 September 2012.*

[9] http://www.us-cert.gov/GFIRST/presentations/2012/threat_landscape_2012boerio_mccracken.pdf, *accessed 12 September 2012.*

[10] http://www.continuityforum.org/content/news/press_release/139844/isf-announces-10-future-threat-scenarios-threat-horizon-2012-repor, *accessed 12 September 2012.*

[11] http://www.oecd.org/sti/futures/globalprospects/19134071.pdf, *accessed 16 November 2012.*

[12] http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk, *accessed 12 September 2012.*

[13] http://capec.mitre.org/documents/Attack_Patterns-Knowing_Your_Enemies_in_Order_to_Defeat_Them-Slides.pdf, *accessed 12 November 2012.*

A risk landscape on the other hand, i.e. an assessment of risks exposure of assets[14], will be based on a threat landscape (i.e. assume some threats), while taking into account impact and providing mitigation controls for the assumed threats. Just as risk embraces more information than only threats, a risk landscape is more comprehensive than a threat landscape. An excellent example of a risk landscape is the Global Risks 2012 report from World Economic Forum[15].

It becomes apparent that there is a certain overlap between a risk landscape and a threat landscape. Ideally, a threat landscape should be part of a risk landscape or –in other words- a risk landscape should be based on an assessment that takes into account a threat landscape.

All in all, both risk and threat landscapes address global challenges in the area of concern being network and information security.

Within this work, we consider risk and threat landscapes as two distinct types of content and we concentrate mainly on the threat landscape.

3.1.5 Objectives of this work

The aim of this report is to identify a cyber-security threat landscape based on aggregated data collected from various ENISA stakeholders. The aggregated data covers the European and global perspective and is based on publicly available material. This material has been collected from various national and international sources.

Information compiled in this report is mainly related to threats and their components. Hence, any information regarding vulnerabilities and risks is out of the scope of this report.

The collected data has been aggregated and consolidated (collated) into a compound and independent view based on threats, on threat agents and trends observed. Care has been taken in consolidating existing reports with information on threats produced by networks of excellence, standardisation bodies and other independent institutes. From this information collection, we provide lists of top threats, threat agents and threat trends. In particular, the collected threat reports have been compiled into a current threat landscape (see section 4). Based on this information, threat trends have been identified by means of an emerging threat landscape. This has been achieved by identifying a number of emerging technologies and by projecting current threat to those areas, building thus an emerging threat landscape (see section 6).

In summary, the work performed is depicted in Figure 1:

[14] http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf, accessed 12 November 2012.

[15] http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf, accessed 13 November 2012.

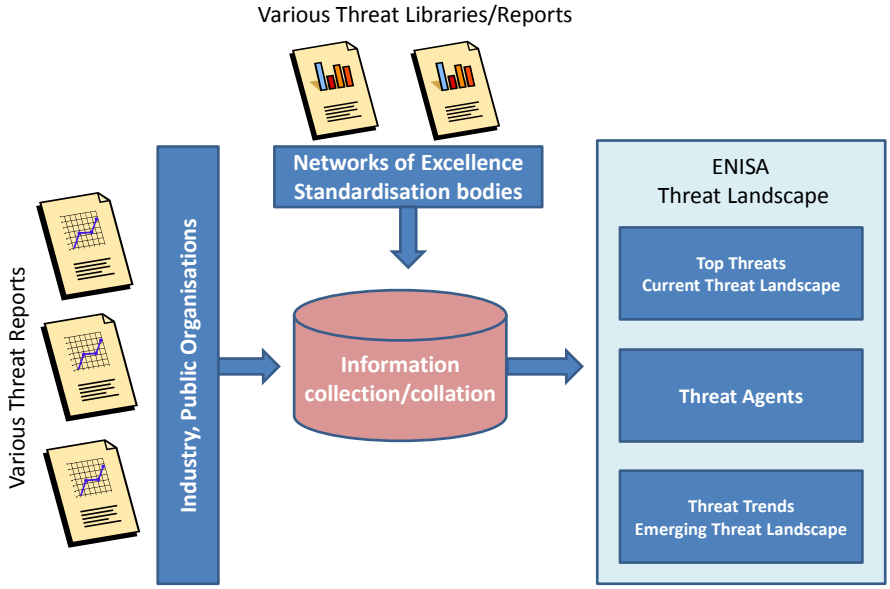

Figure 1: Information collection and collation leading to the ENISA Threat Landscape

Summarised, the ENISA threat landscape provides information about:

- Current threat landscape (Top Threats)
- Overview of threat agents (Threat Agents) and
- Emerging threat landscape (Threat Trends).

Both current and emerging threat landscapes are important data for risk assessments, but also for mitigation strategies and decision making in the area of threat management. Furthermore, non-technical threat landscapes may be used in impact assessments of policy activities at the level of governmental bodies or regulators.

3.1.6 What is beyond the scope of this report?

Some issues have been intentionally left out of the scope of this report:

- Geographical distribution of information on threats: Geographical distribution of threats has not been taken into account. Despite the fact that some of the processed reports provide geographical distribution of threats, we are not currently in the position to satisfactory deduce geographic spread for all kinds of threats collected.
- Threats that are not in the immediate scope of Information Security: Threats that do not directly exploit vulnerabilities of IT assets have been left out of this threat landscape. Examples of such threats are natural disasters, sabotage acts, failures in the area of facility management, etc.

3.1.7 Processed material

Numerous reports have been collected and aggregated within this work. The collected information can be grouped in the following categories;

- *Reports from Virus/Malware protection vendors*: reports of this category include statistics from infections detected in protected platforms (Microsoft, MAC) and categories of components (clients, servers) and a variety of infection vectors (online, offline/local).
- *Reports from CERTS*: reports of this category provide evidence from a wider range of components, as they cover incidents reported from various networks and proprietary systems.
- *Reports from security agencies*: such reports provide a consolidated picture of assessed/reported incidents, attacks and threat agents with a geographical focus. Such reports capture the impact of (global) threats to the infrastructure and/or types of businesses within a particular country.
- *Reports from commercial companies in the area of security*: such reports stem from labs/companies performing analysis and response capabilities for customers. Such reports usually focus on particular areas of threats, depending on the expertise of the company.
- *Reports from industrial associations and committees*: reports of this category provide overviews related to particular types of threats and particular types of components, according to members business and infrastructure types.
- *Reports from Networks of Excellence*: such reports provide forecasts for future threats based on accurate contemporary data collected by various stakeholders (see categories above). Such reports provide a projection to upcoming application areas, assets and types of infrastructure.

Over 120 reports have been taken into account. Most of those including information generated in 2012 but also summarising 2011. In addition, trends mentioned in the collected material have also being consolidated by means of the trends described in section 6.

3.2 Definitions

In this section we provide definitions as used within this report with particular focus on threats. Examining the role of threats helps to clarify the context of all terms used in this report and – in turn - to specify what is considered to be a *threat landscape*.

According to the widely accepted ISO 27005 definition, risks emerge from the "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization". Concretely, it is consider that risk embraces the following components:

Risk =Asset, Threat, Impact

Hence, risk depends on:

- The **Asset** covering its business importance, existing vulnerabilities or weaknesses and level of protection implemented through controls;
- The **Threat** consisting of a threat agent who – depending on their capabilities - utilizes an attack vector to compromise an asset or set of assets. The effectiveness of an attack (expressed via likelihood of success) depends on the capability of the threat agent and the sophistication of the attack;
- The **Impact** that takes into account the value that the asset represents for the business and the consequences when the confidentiality, integrity, availability or privacy of that asset is compromised though the threat.

As defined above, risk is heavily based on threats. The above definition of risk and its components (i.e. asset, threat and impact) complies with most existing definitions, good practices and standards found in the literature (OWASP[16], CAPEC[17], ISO 15408[18], ISO 31000[19], WEF[20]).

In order to visualize the relationships among the elements of risks, we will use a figure from ISO 15408:2005 (see Figure 2). This figure has a level of granularity that is sufficient to illustrate most of the elements of risk mentioned in this section. It should be noted that "owner" refers to the owner of the asset; moreover, the issue of attack vector is not directly displayed in this figure. We assume that an attack vector is part of a threat.

Existing threat catalogues, vulnerabilities/weaknesses, assets and impact statements are often reused in individual risk assessments. It is worth mentioning, however, that often a different context is assigned to these terms. Therefore, when reusing these elements for own assessments, it is important to understand the context assigned to an element and treat it accordingly within the assessment framework. Otherwise, misunderstandings or misinterpretations of the assessed information may occur.

---

[16] https://www.owasp.org/index.php/Threat_Risk_Modeling, *accessed 12 November 2012.*

[17] http://capec.mitre.org/, *accessed 12 November 2012.*

[18] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341, *accessed 12 November 2012.*

[19] http://www.iso.org/iso/catalogue_detail?csnumber=43170, *accessed 12 November 2012.*

[20] http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf, *accessed 12 November 2012.*

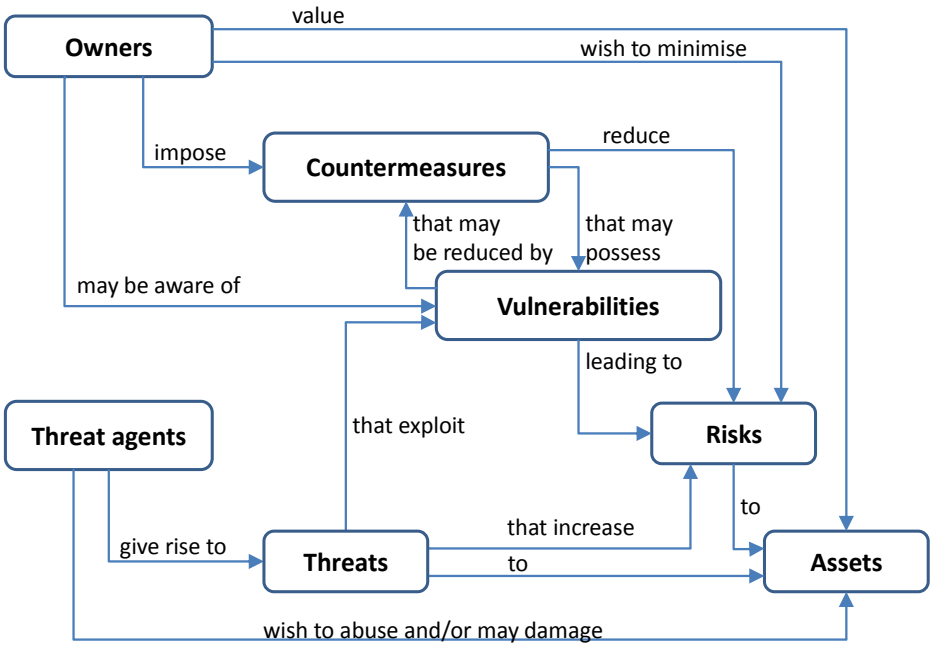

Figure 2: the elements of a risk and their relationships according to ISO 15408:2005

4 Top Threats: The Current Threat Landscape

In this chapter we provide the results of our study of existing material on threats, covering thus the *Current Threat Landscape*. Following an initial collection of relevant information, we have identified top threats, as they have been assessed in the compiled reports. The working assumption for the information collection was: the more recent a threat report the better. Information on threats from 2012 (consolidation of 2011 findings) and from the first three quarters of 2012 have been aggregated, together with trends for 2012 predicted during 2011-2012. Such threat reports have been assigned a higher priority than older reports. However, some – to our opinion important – older reports have been also considered.

The sequence of the presentation below reflects the overall frequency of the threat materialization mentioned in the processed reports, that is, more frequent threats are mentioned first.

It is worth mentioning that this sequence might change, should additional aspects being taken into account, such as impact of the threats, relevance to a specific type of infrastructure, assets and sectors. To this extend, the sequence of the threats below is rather a consequence of statistics of incidents, rather than of impact.

The information per threat consists of a short, non-technical description of the threat; and of a number of so called "key findings" providing information about the whereabouts of the particular threat, such as methods and tools used, threat agent activities, etc. The detailed, technical material collected for each of the presented threats has been annexed to this report (see Annex).

4.1.1 Drive-by Exploits

This threat refers to the injection of malicious code in HTML code of websites that exploits vulnerabilities in user web browsers. Also known as drive-by download attacks, these attacks target software residing in Internet user computers (web browser, browser plug-ins and operating system) and infects them automatically when visiting a drive-by download website, without any user interaction.

Key findings:

- Drive-by downloads attacks against web browsers have become the top web threat. More specifically, attackers are moving into targeting browser plugins such as Java (Java exploits are the major cross-platform threat[21]), Adobe Reader and Adobe Flash.
- The drive-by download attacks are almost exclusively launched through compromised legitimate websites which are used by attackers to host malicious links and actual malicious code.

[21] https://www.websense.com/assets/white-papers/Websense_2013_Security_Predictions_2013.pdf, *accessed 16 November 2012.*

- In May 2012, the first drive-by download for Android was spotted. This means that, apart from PCs, drive-by download attacks are a mobile threat as well.
- Most of drive-by download attacks detected originate from cybercriminals who have adopted this exploitation technique and use it widely via exploit kits e.g. Blackhole[22].

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.2 Worms/Trojans

Worms are malicious programs that have the ability to replicate and re-distribute themselves by exploiting vulnerabilities of their target systems. On the other hand, trojans are malicious programs that are stealthily injected in users systems and can have backdoor capabilities (Remote Access Trojans - RATs) or steal user data and credentials. Both worms and trojans are two classic types of malware being widespread in cyberspace.

Key findings:

- Data theft trojans are widely used by cyber criminals for money making.
- Trojans are the most reported type of malicious code. Although a relatively small amount of computer systems were infected by worms, massive worm epidemics observed in the past have been replaced by an increasing number of targeted trojans.
- Trojan Autorun and Conficker worm are still two of the top threats worldwide. These two pieces of malware are more than four years old and, even though the vulnerabilities that allow them to infect systems have been addressed, they still claim victims.
- Social networks are an appealing distribution channel for malware authors, e.g. the Koobface[23] worm that targeted and infected users of major social networking sites.
- Trojans is the major malware threat in mobile platforms. These trojans vary in nature from simple SMS-Trojans to multifunctional and more sophisticated trojans (e.g. data stealing trojans).

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.3 Code Injection Attacks

This threat category includes well-known attack techniques against web applications such as SQL injection (SQLi)[24], cross-site scripting (XSS)[21], cross-site request forgery (CSRF)[21], Remote File Inclusion (RFI)[21] etc. The adversaries placing such attacks try to extract data, steal

[22] https://sophosnews.files.wordpress.com/2012/03/blackhole_paper_mar2012.pdf, *accessed 22 November 2012.*

[23] http://www.infowar-monitor.net/reports/iwm-koobface.pdf, *accessed 22 November 2012.*

[24] https://files.pbworks.com/download/u0CHSqBuXL/webappsec/13247059/WASC-TC-v2_0.pdf, *accessed 15 November 2012.*

credentials, take control of the targeted webserver or promote their malicious activities by exploiting vulnerabilities of web applications.

Key findings:

- In the last years, the most common attack vector against web applications is SQL injection. Moreover, SQL injection attacks are popular among hacktivist groups (e.g. Anonymous), hacker groups (e.g. LulzSec) and cyber criminals (e.g. as mass SQL Injection campaigns like LizaMoon[25]).
- A significant increase in reported cross-site scripting attack cases has been observed during the last years. Moreover, cross-site scripting attacks work on any browsing technology including mobile web browsers.
- The most critical vulnerability for traditional and Web 2.0 applications is cross-site scripting. However, the resulting risk is lower than SQL injection since attackers do not appear to leverage them as much in money making scenarios.
- SQL Injection is the top attack method for entertainment, retail, technology, media and education websites. CSRF is the top Attack Method for Web 2.0 and Hosting Providers websites.

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.4 Exploit Kits

Exploit kits are ready-to-use software packages that "automate" cybercrime. They use mostly drive-by download attacks whose malicious code is injected in compromised websites. These attacks exploit multiple vulnerabilities in browsers and browser plug-ins[26]. Moreover, exploit kits use a plethora of channels to deliver malware and infect unsuspected web users. An important characteristic of exploit kits is their ease of use (usually through a web interface) allowing people without technical knowledge to purchase and easily use them.

Key findings:

- Malware-as-a-Service (MaaS) is a new and emerging criminal business model. Thus, there is an on-going professionalization and commercialization of cybercrime-ware through this kind of threat.
- Exploit kits evolve and use sophisticated techniques (e.g. encoding/polymorphism and heavy obfuscation) in order to evade classic detection mechanisms.
- The Blackhole exploit kit is the most advanced and the most commonly detected exploit family in the first half of 2012[27].

---

[25] http://money.cnn.com/2011/04/01/technology/lizamoon/index.htm, *accessed 9 November 2012.*

[26] http://contagiodump.blogspot.gr/2010/06/overview-of-exploit-packs-update.html, *accessed 9 November 2012.*

[27] http://download.microsoft.com/download/C/1/F/C1F6A2B2-F45F-45F7-B788-32D2CCA48D29/Microsoft_Security_Intelligence_Report_Volume_13_English.pdf, *accessed 21 November 2012.*

- Blackhole integrates a lot of distribution channels for its malware: a) malicious advertising through compromised ad servers in social networks, b) malicious code hosted in compromised legitimate websites, c) search engine optimization poisoning and d) email spam. Moreover, Blackhole exploits vulnerable browser plug-ins such as Java, Adobe Reader and Adobe Flash Player.
- Just like any other software developers, authors of exploit kits support and develop their products. During September 2012, Blackhole's authors released the Blackhole Exploit Toolkit 2.0 that provides new capabilities to its users.

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.5 Botnets

A Botnet[28] is a set of compromised computers which are under control of an attacker. These compromised systems are called bots (or 'zombies') and they communicate with the bot master that can maliciously direct them. Botnets are multiple usage tools that can be used for spamming, identity theft as well as for infecting other systems and distribute malware.

Key findings:

- In order to increase their stability and avoid single points of failure, botnet command and control infrastructure is becoming decentralized by peer-to-peer technologies (e.g. ZeroAccess[29] botnet).
- Botnets have evolved from single-purpose (spamming, DDoS etc.) to multi-purpose botnets.
- Nowadays, botnets are used as a commodity. Interested parties can rent botnet in order to achieve their purposes.
- Sophisticated operations refrain from massive botnet that attract a lot of attention from law enforcement and the security industry (especially after major botnet takedowns in the last few years). The new trend is smaller botnets that are difficult to be tracked and taken down.
- Botnets support infection capabilities for multiple OSs. In April 2012, a botnet called Flashback was reported that contained more than 600,000 infected Apple Mac computers.
- Malware authors appear interested in turning Android mobile phones into 'zombies.'
- Cloud Computing platforms are already being used to set up botnets.

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

---

[28] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence, *accessed 22 November 2012.*

[29] http://www.kindsight.net/sites/default/files/Kindsight_Malware_Analysis-ZeroAcess-Botnet-final.pdf, *accessed 22 November 2012.*

4.1.6 Denial of service

A denial-of-service attack (DoS) is an attempt to make a resource unavailable to its users. A distributed denial-of-service attack (DDoS) occurs when multiple attackers launch simultaneous DoS attacks against a single target. In DDoS attacks, attackers use as much firepower as possible (usually through compromised computer systems/botnets) in order to make the attack difficult to defend. The perpetrators of DoS attacks usually either target high profile websites/services or use these attacks as part of bigger ones in order achieve their malicious goals. As stated, despite the fact that these kinds of attacks do not target directly the confidentiality or integrity of the information resources of a target, they can result in significant financial and reputation loss.

Key findings:

- DoS attacks appear to abandon their simple flood-based approach (UDP, ICMP, and SYN floods). They increase in sophistication and the number of applications they target (HTTP, DNS and SMTP are the most frequently targeted ones).
- Modern DoS attack tools mostly work at the application layer and are publicly available.
- DDoS bitrates of 20 Gbps are the new norm, while the barrier of 100 Gbps has been broken during 2011.
- Hacktivism, vandalism and extortion are the major DDoS attack motivations.
- In 2012 IPv6 DDoS attacks were reported for the first time[30].

Observed current trend for this threat: *Stable*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.7 Phishing

Phishing states the combined use of fraudulent e-mails and legitimate looking websites by cybercriminals in order to deceitfully gain user credentials. Phishers use various social engineering techniques to lure their victims into providing information such as passwords and credit card numbers.

Key findings:

- Typically, sites that target financial institutions account for most active phishing sites at any given time. However, payment services, social networking, ISP, non-profit organizations, Parcel services and government sectors websites were as well some of the most spoofed organizations in phishing e-mail attacks.
- The uptimes of phishing sites dropped to a record low in the first half of 2012.
- A new trend in phishing is phishing sites that target PCs as well as mobile platforms with the ability to attack some two-factor authentication schemes. Furthermore, phishing sites reach smartphone via SMS messages.

[30] http://www.arbornetworks.com/research/infrastructure-security-report, *accessed 15 November 2012.*

- Phishers host their sites in compromised legitimate servers using shared web hosting environments. This is a consequence of changes in security policies and website registration process as well as due to the prevalence of hacking tools that automate hacking.
- VoIP systems are targeted by "vishing" scams (telephone-based phishing) since criminals try to collect sensitive information from users.

Observed current trend for this threat: *Stable*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.8 Compromising confidential information

Compromising of confidential information refers to data breaches that occurred via intentional, unintentional information disclosure performed by internal or external threat agents. This threat targets sensitive information from various sectors such as public health sector, governmental organizations, small-medium businesses (SMBs), large organizations etc. Data breaches are usually realised through some form of hacking, incorporated malware, physical attacks, social engineering attacks and misuse of privileges.

Key findings:

- 2011 was characterized as the year of the Security Breach.
- In the last years, the number of data breaches detected at healthcare organizations has increased. The adoption of electronic health record systems that store personally identifiable information seems to attract the attention of cybercriminals.
- Data breaches today have become more targeted.
- Negligent insiders and external malicious attacks are the main causes of data breaches. Moreover, cybercriminals and hacktivists are the major external threat agents for data breaches.
- More than 9 out of 10 breaches would have been prevented if organizations had followed data protection and information security best practices.
- Key to many data breaches are web application vulnerabilities.
- Enterprises that suffer data breaches do not only lose money but also reputation and customers.

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.9 Rogueware/Scareware

The Rogueware threat consists of any kind of fake software that cybercriminals distribute (e.g. via social engineering techniques) in order to lure users to their malicious intentions. A more specific kind of rogueware is scareware, rogue security software, which tries to infect computers by providing fake security alerts.

Key findings:

- While fake security software is still being a big problem, the recent fall off of this threat is a result of better users' awareness as well as of more effective international cooperation (i.e. in the areas of law and law enforcement).
- Rogueware products have undergone little technical evolution in the last years. However, their distribution methods have changed as they now can be distributed via search engine optimization (SEO) poisoning, spam emails and drive-by downloads (being the more classical malware distribution method).
- During 2011, fake antivirus products appeared targeting Mac users.
- One of the most prevalent threats of the last months is the 'Police Virus'[31], a scareware that evolved to ransomware, indicating an increasing adoption of ransomware techniques[32] through cybercriminals.

Observed current trend for this threat: *Stable*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.10 Spam

Spam is the abusive use of e-mail technology to flood user mailboxes with unsolicited messages. Adversaries using this threat force the e-mail messages to be received by mail recipients. Spam activity costs very little to the sender; on the other hand it is time consuming for recipients of spam messages and costly in terms of resources (network and storage) for the service providers.

Key findings:

- Due to coordinated activities at national and international level, email spam activity was significantly lower in 2011. This trend continued in 2012 remaining below levels of previous years.
- There have been increased pressures on spammers in the last 2 years (e.g. Rustock[33], Bredolab[34] and Waledac[35] botnets takedown). This has resulted in a shift of focus on social networks and more targeted approaches.
- Throughout first half of 2012, regionally specialized spam (i.e. custom spam messages translated in the victim's native language) was on the rise.

---

[31] http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf, accessed 21 November 2012.

[32] http://www.symantec.com/connect/blogs/top-5-security-predictions-2013-symantec, accessed 15 November 2012.

[33] https://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx?Redirected=true, accessed 15 November 2012.

[34] http://blogs.technet.com/b/mmpc/archive/2010/10/26/bredolab-takedown-another-win-for-collaboration.aspx?Redirected=true, accessed 9 November 2012.

[35] http://blogs.technet.com/b/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx?Redirected=true, accessed 9 November 2012.

- The content of criminal spam is becoming ever more convincing. Spam content mostly include fake medication (e.g. pharmacy spam), sex/dating, compulsive gambling and (unintentional) participation in criminal activities and malware.
- The education, automotive, public and pharmaceutical sectors are the most spammed ones.

Observed current trend for this threat: *Decreasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.11 Targeted Attacks

A targeted attack occurs when attackers target a specific entity/organization over a long time span. Often the objective of targeted attacks is either data exfiltration or gaining persistent access and control of the target system. This kind of attack consists of an information gathering phase and the use of advanced techniques to fulfil the attacker's goals. The first phase can possibly involve specially crafted e-mails (spearphishing), infected media and social engineering techniques, whereas the second phase involves advanced and sophisticated exploitation techniques.

Key findings:

- A trend reported during the first half of 2012 is the increase of targeted attacks. These attacks need time (in some cases a few years) to be detected and are rather hard to avoid.
- Spearphishing and social engineering techniques are on the rise. Spearphishing is increasing, mainly due to the increased use of social networking for private and business purposes. The phishing message can include a link or attachment (e.g. executable file, ZIP, PDF, Text Documents, etc.) leading to infection of the target system, often with custom malware (i.e. bypassing anti-virus detection mechanisms).
- More and more targeted attacks against small companies have been registered. This trend could be based on the perception that small companies, with eventually less security measures, are an easier target.
- The most common infection vector for Industrial Control Systems networks was spear-phishing. The energy sector was the one that reported most of the intrusion incidents. The rapid rise in existing vulnerabilities in SCADA systems[36] is an indication for success perspectives of this kind of threat.
- One of the major events during 2012 was the detection of the Flamer malware, a powerful cyber weapon similar to Stuxnet and Duqu. Flamer was designed for perpetrating targeted attacks and it is estimated that its development could have taken more than 10 years of work.

[36] http://www.ptsecurity.com/download/SCADA_analytics_english.pdf, *accessed 12 November 2012.*

- The exploitation technique called "watering hole attack" was used by the Elderwood[37] gang. Moreover, Elderwood gang used eight zero-day vulnerabilities over the last three years.

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.12 Physical Theft/Loss/Damage

This category describes threats relevant to device theft, device loss, hardware theft as well as loss and damage of data storage media.

Key findings:

- Due to the wide adoption of mobile computing, the probability of data loss (potentially sensitive data) and device theft is increasing.
- BYOD (Bring Your Own Device) has an impact on corporations since in case of theft or loss of mobile devices maintained by businesses potentially sensitive corporation data will be disclosed.
- Loss or theft of mobile devices and other equipment by staff is a major internal threat for organisations.
- Loss or theft of mobile devices and hardware are a major external threat for corporations.
- Corporations having experienced a data breach reported that one of top 3 causes is physical theft of devices containing sensitive data.
- Lack of encryption on mobile company devices is an issue that should be addressed[38].

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.13 Identity Theft

In a networked world, the identity of a user is the unique piece of information that makes this specific user distinguishable. This information is usually a pair of credentials (username/password) or other confidential information such as Social Security Number (SSN) or credit card number. Identity theft is an attack that occurs when an adversary steals user credentials and uses them order to serve malicious goals, mostly related with financial fraud.

Key findings:

- Cybercriminals have a very professional approach towards exploiting home banking. As a result an increase of advanced trojan malware designed for identity theft and identity fraud can be observed.

---

[37] http://www.symantec.com/connect/blogs/elderwood-project, *accessed 9 November 2012.*

[38] http://www.bbc.co.uk/news/technology-20343745, *accessed 21 November 2012.*

- Zeus[39] and SpyEye[40] are the two major families of banking trojans that are specialized in stealing online banking credentials. These trojans have evolved by introducing advanced modularity characteristics that allow flexible customization.
- Mobile users increasingly use their devices for online banking and financial transactions. As a result, they have become target of cybercriminals; this is reflected in the observed increase of mobile versions of well-known PC-based trojan malware (e.g. Zeus-in-the-Mobile).
- There are publicly available hack tools that enable their users to intercept Wi-Fi traffic, spot users and passwords for popular services and hijack personal accounts (e.g. Faceniff[41], DroidSheep[42]).
- Identity theft and identity fraud have high frequency and high level of risk in social networks. The identity of social media users may prove more valuable to cybercriminals than their credit card numbers.

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.14 Abuse of Information Leakage

Information leakage refers to the unintentional or deliberate revealing of information, making it thus available to an unauthorized party. This information can be further processed and abused, e.g. to start an attack or gain access to additional information sources.

Key findings:

- User data tracking as well as geo-location data can be leaked and misused in order to breach privacy in mobile platforms.
- In a similar manner as traditional applications, user information leakage through poorly written 3rd party mobile application is a privacy threat.
- Aggressive advertising networks in mobile applications have access to mobile user data without notifying the user.
- Web applications suffer from information leakage vulnerabilities exposing system specific information that could be useful for malicious users in order to place further attacks (e.g. injections).
- In cloud environments, researchers have found ways to access data without prior authorization.

---

39 https://www4.symantec.com/mktginfo/whitepaper/user_authentication/21195180_WP_GA_BankingTrojansImpactandDefendAgainstTrojanFraud_062611.pdf, accessed 22 November 2012.

40 https://blog.damballa.com/archives/tag/spyeye, accessed 22 November 2012.

41 http://faceniff.ponury.net, accessed 15 November 2012.

42 http://droidsheep.de, accessed 15 November 2012.

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.15 Search Engine Poisoning

Search Engine Poisoning (SEP) attacks exploit the trust between Internet users and search engines. Attackers deliver bait content for searches to various topics. In this way, users searching for such items are being diverted to malicious content.

Key findings:

- Search engines are one of the major methods used by the cybercriminals in order to make users visit malicious sites.
- The attackers are very successful in poisoning image search results which shows a new trend in black hat search engine optimization (SEO) campaigns.
- Apart from major events, perpetrators of SEP attack feed search engines with bait content for minor events and topics that may target special interest groups.
- Search engine poisoning attacks can be performed by manipulating user search history and online profile[43].

Observed current trend for this threat: *Stable*

Detailed findings and references to the analysed material can be found in the Annex.

4.1.16 Rogue certificates

Digital certificates are a means of defining trust in Internet. Attackers steal, produce and circulate rogue certificates which break the aforementioned chain of trust, giving them the capability of engaging in attacks that are undetectable for end users. By using rogue certificates, attackers can successfully run large scale man-in-the-middle attacks. Moreover, rogue certificates can be used to sign malware that will appear as legitimate and can evade detection mechanisms.

Key findings:

- Stuxnet, Duqu and Flamer malware used rogue certificates to evade detection mechanisms.
- Certification Authorities need to enforce, permanently review and adapt basic security best practices in order to prevent attacks against them.
- Large-scale man-in-the-middle attacks have been conducted due to stolen certificates.
- Rogue certificates are used in cyber warfare, espionage and cybercrime operations.

Observed current trend for this threat: *Increasing*

Detailed findings and references to the analysed material can be found in the Annex.

[43] http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf, accessed 21 November 2012.

5 Overview of Threat Agents

In this chapter we provide an overview concerning the threat agents that have been identified within the performed analysis. The definition of threat agent has been adopted from IT Law Wiki[44], namely: *"A threat agent is any person or thing that acts (or has the power to act) to cause, carry, transmit, or support a threat"*. Within the performed analysis, a plethora of threat agent libraries have been identified (e.g. Intel Threat Library[45], VERIS Threat Agent Categories[46] [47], FAIR Threat Communities[48], OWASP Threat Agent Groups[49], NIST Threat Sources[50] and Vidalis et al Threat Agent Classification[51]). At the same time, threat agents have been mentioned in the analysed threat reports. In the present section we present all relevant threat agents by providing information about their main characteristics. Moreover, we provide an overview of their activities with regard to the assessed top threats.

Threat agents have some characteristics and attributes such as hostility/intent, access, objective, skills/capability, resources, preferred targets, motivation etc. However, due to the fact that threat agents and their characteristics evolve or change, the adoption of a continuous threat agent identification process is needed.

Below we present some of the major threat agents in cyberspace, providing a short description for each one of them:

- **Corporations**. This kind of threat refers to corporations/organizations/enterprises that adopt and/or are engaged in offensive tactics. Corporations can be considered as hostile threat agents their motivation is to build competitive advantage over competitors, who also make up their main target. Depending on their size and sector, corporations usually possess significant capabilities, ranging from technology up to human engineering intelligence, especially in their area of expertise.
- **Cybercriminals**. Cybercriminals are hostile by nature. Moreover, their motivation is financial gain and their skill level is, nowadays, quite high. Cybercriminals can be organised on a local, national or even international level. It should be taken as given, that a certain degree of networking between cybercriminals is being maintained.
- **Employees**. This category refers to the staff, contractors, operational staff or security guards of a company. They can have insider access to company's resources and they are

[44] http://itlaw.wikia.com/wiki/Threat_agent, accessed 12 November 2012.

[45] http://www.intel.com/it/pdf/threat-agent-library.pdf, accessed 12 November 2012.

[46] http://veriscommunity.net/doku.php?id=agents, accessed 12 November 2012.

[47] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, accessed 12 November 2012.

[48] http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf, accessed 12 November 2012.

[49] https://www.owasp.org/index.php/Category:Threat_Agent, accessed 12 November 2012.

[50] http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf, accessed 12 November 2012.

[51] Analysing Threat Agents & Their. Attributes. Dr. Stilianos Vidalis, Dr. Andrew Jones.

considered as both non-hostile threat agents (i.e. distracted employees) as well as hostile ones (i.e. disgruntled employees). This kind of threat agents possesses a significant amount of knowledge that allows them to place effective attacks against assets of their organisation.

- **Hacktivists**. Hacktivism is a new trend in threat agents. Hacktivists are politically and socially motivated individuals that use computer systems in order to protest and promote their cause. Moreover, they are usually targeting high profile websites, corporations, intelligence agencies and military institutions.
- **Nation States**. Nation states can have offensive cyber capabilities and could potentially use them against an adversary. By their very nature and due to the importance of the means at their disposal, Nation States may present a threat in the area of cyber warfare.
- **Terrorists**. Terrorists have expanded their activities and engage also in cyber-attacks. Their motivation can be political or religious and their capability varies from low to high. Preferred targets of cyber terrorists are mostly critical infrastructures (e.g. public health, energy production, telecommunication etc.), as their failures causes severe impact in society and government. It has to be noted, that in the public material analysed, the profile of cyber terrorists still seems to be blurry.

It is worth mentioning that various further groups and sub-groups of threat agents can be found in the literature. The threat agents presented in this section match the findings from the performed analysis. All in all, we have found that publicly existing intelligence about threat agents is at a low level of maturity and we think that the issue of threat agent identification requires further elaboration.

The involvement of the above threat agents in the identified top threats is presented in the table (see Figure 3).

As it can be seen in the table below, Cybercriminals and Terrorists are involved in similar activities. There are opinions in the literature, that these groups are not clearly distinguishable based on existing evidence; therefore, they are considered as overlapping with the difference being solely in their intent.[52]

[52] https://www.fas.org/sgp/crs/terror/RL32114.pdf, *accessed 12 November 2012.*

	Threat Agents					
	Corporations	Cybercriminals	Employees	Hacktivists	Nation states	Terrorists
Drive-by exploits		✓				✓
Worms/Trojans		✓			✓	✓
Code Injection		✓		✓		✓
Exploit kits		✓				
Botnets	✓	✓		✓		✓
Denial of service		✓		✓	✓	✓
Phishing attacks		✓				
Compromising confidential information	✓	✓	✓	✓	✓	✓
Rogueware / Scareware		✓			✓	
Spam	✓	✓				
Targeted attacks	✓	✓			✓	✓
Physical Theft / Loss / Damage	✓	✓	✓		✓	✓
Identity theft	✓	✓	✓		✓	
Abuse of Information Leakage	✓	✓	✓	✓	✓	✓
Search Engine Poisoning	✓	✓				
Rogue certificates		✓			✓	

Figure 3: Involvement of threat agents in the top threats

6 Threat Trends: The Emerging Threat Landscape

In this chapter we provide information on *threat trends* that have been assessed by our study of existing material. This part of the report covers thus the *Emerging Threat Landscape*. In order to better comment on upcoming threat trends, we have mapped the identified current threat landscape to emerging areas we consider as important for the future.

By mapping current threats to emerging areas, we aim at providing more qualified predictions of trends about possible targets that are going to be on the radar of threat agents within the coming time (half to one year). The emerging areas we assume are:

- *Mobile Computing*: Covering several aspects of Consumerization of IT, BYOD (Bring Your Own Device) and mobile services, such as social networking, business applications and data, use of cloud services, interpersonal communication, voice, video, etc.
- *Social Technology*: Use of social media is one of the main activities performed by private users. Moreover social networking plays an increasingly significant role in businesses.
- *Critical Infrastructures*: This is an area that is definitely going to attract threat agents, as the impact of such an attack is big at all levels (society, government, national security, etc.).
- *Trust Infrastructure*: Attacks on the trust infrastructure break the chains of trust and generate very serious impact at many levels and application areas. Success of such attacks allows attackers to greatly enlarge their attack surfaces and targets.
- *Cloud Computing*: The proliferation of cloud computing and the sheer concentration of users and data on rather few logical locations are definitely an attractive target for future attacks.
- *Big Data*: Use of big data within businesses but also for the enhancement of security is already in discussion. On the other hand it is also expected that attackers are going to abuse big data in order to enhance their capabilities, collect intelligence, but also to better hide their attacks.

These areas are not overlap free. There are clear interrelationships among them within most usage scenarios (e.g. between mobile and cloud computing, social technology and mobile computing, big data and cloud, and so on). Nevertheless, these areas are going to be the basis for most of the innovation expected in the area of IT and as such will lead to changes in the threat landscape.

In the following section we give a brief description of the situation in each of these emerging areas and we provide a prediction of the relevant threats. It has to be noted, that the threats mapped to the emerging areas are the threats associated with the Current Threat Landscape, whereas the sequence has been changed in order to show their relevance to the particular emerging area. Just as in Current Landscape, the sequence of the presentation below reflects the overall frequency of the threat materialization, that is, more frequent threats are mentioned first. Should any of the 16 current threats not seem to have any relevance to an

emerging area, it has been left out. Finally, we have restricted the relevant emerging threats up to 10 top threats per area.

6.1 Threat Trends in Mobile Computing

In almost all of the compiled material mobile computing (also referred to as *mobile systems*), an exponential increase in threats is being predicted. This trend follows the relevant market trends of mobile devices, consumerization of IT, BYOD and mobile user empowerment. Along with increases in the bandwidth of mobile communication protocols (3G, HSDPA, LTE, etc.) and processing power, mobile devices will take over the role PCs previously hold.

The increase in threats is due to the nature of mobile systems and devices: all communication takes place over poorly secured (GSM) or unsecured channels (Wi-Fi). Moreover, the software used in such systems, both operating system and applications are of a rather moderate maturity level. Finally, the mobility of devices – one of their main advantages – makes them vulnerable to theft and loss. Given the increasing trends resulting Consumerization of IT (and BYOD), business and personal data on the move will be an attractive target for threat agents. In addition, due to increasing processing power and bandwidth, mobile devices will be targets for attacks that were considered to be "traditional" for PCs, such as botnets and phishing.

Finally, the fact that such devices will be owned by a vast variety of users of all ages with varying security knowledge (youngsters, adults with almost none technical and security knowledge, etc.), will lead to an increased attack activity.

The top emerging threats to mobile devices are as follows:

Emerging Threat	Threat Trend
1. Drive-by exploits (affecting mobile OS and mobile apps[53])	
2. Worms/Trojans (trojans affecting mobile OS, SMS-Trojans[54])	
3. Exploit Kits (mobile OS vulnerabilities are already incorporated into exploit kits)	
4. Physical Theft/Loss/Damage (mobile devices will be main targets of this threat)	
5. Compromising confidential information (data breaches of sensitive data stored on the devices or being on the move over communication channels)	
6. Code Injection (availability of code injection for mobile devices	

[53] http://arstechnica.com/gadgets/2012/05/android-users-targeted-for-the-first-time-in-drive-by-download-attacks/, *accessed 14 November 2012.*

[54] http://www.h-online.com/security/news/item/The-alleged-flood-of-Android-trojans-1668760.html, *accessed 14 November 2012.*

Emerging Threat	Threat Trend
such as cross-zone scripting[55], SQL Injection flaws in mobile applications[56])	
7. Phishing (phishing will target increasingly mobile device users)	↑
8. Abuse of information leakage (data relevant to privacy, leakages from poorly written applications, user errors)	→
9. Identity Theft (through credential stealing trojans targeting identity information stored on device)	↑
10. Botnets (through infections of mobile platforms)	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 2: Emerging Threat and their trends in the area of Mobile Computing

Besides the above mentioned emerging threat landscape, we have identified the following *emerging issues*:

- The development of cross-platform threats will have similar code and run on several platforms including all mobile OSs, implementing thus "device agnostic" malware.
- Due to mobility, an increase in proximity based hacking (based on NFC and other wireless communication) will be an important attack vector.
- Due to the usage of mobile platforms for financial transactions (payments, banking, etc.), these platforms will gain the attention of attackers.
- Weaknesses from weak introduction of BYOD policies will be exploited to successfully attack mobile devices and services.
- Advancements in app store security need be introduced to improve security[4], such as lower malware infections of mobile devices[57], check security characteristics of apps, etc. The maturity of these measures needs to be increased[58].

6.2 Threat Trends in Social Technology

With social technology we refer to social networks, private and professional applications and services on mobile devices, but also the infrastructure of providers of social networking applications. Given the number of users of such platforms, the level of interconnections and

[55] http://blog.watchfire.com/wfblog/2012/10/old-habits-die-hard.html, *accessed 14 November 2012.*

[56] http://www.information-age.com/channels/security-and-continuity/perspectives-and-trends/2110463/mobile-developers-repeating-security-mistakes-of-the-web.thtml, *accessed 14 November 2012.*

[57] http://www.zdnet.com/blog/hardware/googles-android-market-bouncer-does-it-offer-enough-protection/17981, *accessed 14 November 2012.*

[58] http://www.computerworlduk.com/in-depth/security/3372385/google-bouncer-beaten-at-black-hat-2012/, *accessed 14 November 2012.*

the penetration levels of social networking in other applications, social technology is one of the main targets of malicious attacks.

As a matter of fact the main "entry points" to social networks is via mobile devices. This underlines the dependence relationship between mobile computing and social networking and makes clear, that this overlap will mutually reinforce the success of attacks to either platform.

At the same time, social networks themselves have low to medium maturity of security controls. Combined with possible security gaps at the "entry points" and the low security awareness of end-users, social networks offer a relatively large surface for any type of attacks to privacy, data theft, identity theft and misuse. Let alone the possibilities to launch social engineering and data profiling attacks.

Successful attacks on social network participants, together with the large user base would have significant impact to privacy but would also impact interconnected functions, applications and businesses.

The top emerging threats to social technology are as follows:

Emerging Threat	Threat Trend
1. Worms/Trojans (by abusing fake trust in social networking, malware infection vectors are being implemented)	
2. Abuse of information leakage (including data mining from available information)	
3. Physical Theft/Loss/Damage (of mobile device including credentials to access user data)	
4. Phishing attacks (using social engineering techniques based on social networking content)	
5. Spam (although declining, spam will concentrate on exploitation of social media)	
6. Exploit kits (by means of malicious advertising from compromised ad servers that appears in social networking)	
7. Identity theft (especially by taking over mobile end-user devices containing identity information and credentials for access to	

	Emerging Threat	Threat Trend
	social networks)	
8.	Drive-by exploits (applications from parties that have generated fake trust over social networking[59])	↑
9.	Rogueware/Scareware (using fake trust built over malicious advertising within social media sites)	→
10.	Targeted attacks (spearphishing using social engineering techniques)	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 3: Emerging Threat and their trends in the area of Social Technology

Besides the above mentioned emerging threat landscape, we have identified the following *emerging issues*:

- Attackers will continue with development of techniques to generate fake trust within social media.
- The increasing popularity and penetration of social media will lead to *ubiquitous social technology*[60]. Due to increasing interconnections of social technology with other areas/applications, new possibilities of abuse will be exploited (e.g. interconnection of social media and automotive electronics, Internet of Thinks, healthcare, education, etc.).
- Exploitation of social networks as basis for social engineering attacks will be continued. It is expected that a better adaptation to various social groups will be observed (e.g. minors, social minorities, etc.).
- The emergence of social bots will be an issue to bother cyber security experts[61].
- Existing functions of social media can be misused to achieve misinformation and eventually control political expression[62].
- The proliferation of BYOD will lead to a better level of knowledge regarding the secure use of social technology, as businesses will embrace it and will develop professional security policies to cope with social media. Users participating in BYOD programmes will be thus forced to apply these policies. This will lead to a better awareness of existing threats and their mitigation.
- Network and information security training and education programmes for minors will have a positive effect towards the awareness required when using social media.

[59] https://www.computerworld.com/s/article/9220557/Drive_by_download_attack_on_Facebook_used_malicious_ads, accessed 14 November 2012.

[60] http://www.wired.co.uk/news/archive/2012-10/17/the-ubiquitous-social-network, accessed 14 November 2012.

[61] https://www.usenix.org/system/files/conference/leet12/leet12-final10.pdf, accessed 20 November 2012.

[62] https://www.usenix.org/system/files/conference/leet12/leet12-final13_0.pdf, accessed 20 November 2012.

6.3 Threat Trends in Critical Infrastructures

Critical infrastructures are complex "systems of systems" that play a critical role for the wellbeing of citizens and, at the same time, are important to national security both in piece and crisis. Critical Infrastructure poses high requirements in availability, resilience and security: real-time situation awareness, for example, is often a requirement for many sectors belonging to Critical Infrastructures. The balance between availability, resilience and security requirements needs to be maintained. This is a difficult task due to the fragmented security policies of various sub-systems and the often missing "big picture" of existing dependencies.

As failure of Critical Infrastructures is considered to be a significant risk for society globally[63], the security of such systems and their sub-systems needs to be strengthened. Cyber-attacks will continue targeting Critical Infrastructures by mainly abusing security gaps in the interconnected systems.

Further, the notion of critical infrastructure/critical system will undergo permanent changes. Just as the Internet plays an increasing role in communication and interconnection of "traditional" Critical Infrastructures, other systems will undertake important roles too. Examples are infrastructures of cloud providers, providers of mobile software (both OS and Apps), ISPs, IXPs, etc. The changing dependencies among various systems can cause cascaded failures in Critical Infrastructures in case of individual (sub-) system failures resulting cyber-attacks.

The top emerging threats to critical Infrastructures are as follows:

Emerging Threat	Threat Trend
1. Drive-by exploits (injections and drive-by downloads will be a serious threat to components of Critical Infrastructures)	
2. Worms/Trojans (the increasing trend in creation of trojans will affect components of Critical Infrastructures)	
3. Code Injection (cross site scripting will play a significant role, especially in web applications involved in Critical Infrastructures)	
4. Exploit kits (tools to identify and abuse exploits found in most common infrastructure elements, both web and client systems)	
5. Denial of service (is considered as an effective technique to attack critical systems and achieve impact with relatively low capabilities, e.g. through Hacktivists)	
6. Phishing attacks (phishing attacks using social engineering techniques)	

[63] http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf, *accessed 9 November 2012.*

Emerging Threat	Threat Trend
7. Botnets (botnets will continue to pose a threat for Critical Infrastructures, especially through the advancements in mobile computing)	➲
8. Compromising confidential information (data breaches will have an impact in Critical Infrastructures, e.g. by providing valuable information to launch an attack, e.g. in the periphery of the infrastructure such as smart meters)	↑
9. Targeted attacks (spearphishing and APTs will remain a significant concern in this area generating high impact for Critical Infrastructures)	↑
10. Physical Theft/Loss/Damage (loss of devices and of information, either intentional or unintentional, eventually through the proliferation of mobile computing)	↑

Legend: ↓ Declining, ➲ Stable, ↑ Increasing

Table 4: Emerging Threat and their trends in the area of Critical Infrastructure

Besides the above mentioned emerging threat landscape, we have identified the following *emerging issues*:

- Going along with advances in performance and bandwidth, attack methods and tools have reached a maturity that could be used for cyber warfare[64] (i.e. "*weaponized software*"). Increased availability of such tools will have an impact on the capabilities of relevant threat agents, leading thus to an advancement in striking power.
- Critical Infrastructures consist of many sub-systems (including technology and operators). It is important to establish and maintain interfaces at both technical and organisational level in order to identify gaps and arrange and coordinate common response to incidents affecting multiple parties.
- The proliferation of consumerization of IT (including BYOD) will lead to additional weak points in the supply chain of Critical Infrastructure services.
- Political instability might cause failures in parts of national critical services and lead to domino effects in other critical areas or even other countries.
- Current financial crisis but also cost pressure in manufacturing might lead to use of cheap devices/sensors in critical systems that are difficult to manage or control.

6.4 Threat Trends in Trust Infrastructure

With trust infrastructure we mean any information system that provides strong authentication and aims at establishing a trusted, secure connection between two end points.

[64] http://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf, *accessed 9 November 2012.*

Trust infrastructure components may be used at all levels of information systems, i.e. from application level to network protocols. Trust infrastructures are usually based on strong encryption technology and key management. Examples of trust infrastructures are authentication infrastructures, secure communication protocols, public key infrastructure components, etc.

Trust infrastructures are extremely important for information security as they build the basis for securing information at many levels; and help authenticating partners or systems by establishing trusted interactions (i.e. trusted connections, trusted transactions, electronic signatures, etc.).

With the introduction of electronic identity systems for the identification of citizens, trust infrastructures play a significant role in the security at level of states. As most of electronic identity infrastructures are based on trust infrastructures, it is clear that any successful attack to the trust infrastructure would have high to very high impact on information security but also on national security worldwide.

The top emerging threats to trust infrastructures are as follows:

Emerging Threat	Threat Trend
1. Denial of service (an effective technique to attack trust infrastructure components and achieve impact by blocking access to relevant components, e.g. handshaking with SSL servers[65])	
2. Rogue certificates (compromising trust relationships will be key in generating fake trust within components of trust infrastructure but also other systems using them)	
3. Compromising confidential information (data breaches will have an impact in trust infrastructures, e.g. by providing valuable information to launch an attack)	
4. Targeted attacks (spearphishing and APTs will remain a significant concern in this area[66])	
5. Physical Theft/Loss/Damage (loss of devices and of information, either intentional or unintentional)	
6. Wrong implementations (of existing cryptography standards, including key management[67, 68])	

[65] http://www.eweek.com/c/a/Security/Hackers-Release-DoS-Attack-Tool-Targeting-SSL-Servers-868830/, *accessed 10 November 2012.*

[66] http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf, *accessed 10 November 2012.*

[67] https://threatpost.com/en_us/blogs/research-shows-serious-problems-android-app-ssl-implementations-101912, *accessed 10 November 2012.*

Emerging Threat	Threat Trend
7. Identity theft (credentials stealing trojan with the objective to obtain credentials for system access)	➲
8. Abuse of information leakage (leading to intelligence that will facilitate successful attacks)	➲

Legend: Declining, Stable, Increasing

Table 5: Emerging Threat and their trends in the area of Trust Infrastructure

Besides the above mentioned emerging threat landscape, we have identified the following *emerging issues*:

- The security of trust infrastructures will need to be taken more seriously. Not only paper-based security policies but also their flawless enforcement are necessary and need to be continuously checked. A holistic security approach including proactive security measures need to be in place and permanent security monitoring needs to be implemented.
- Implementations of trust functions will need to be better checked. Providers of App stores will need to pay special attention to implementation of trust and security functions in order to avoid serious impact on the user trust. In the emerging area of cloud computing, cryptographic functions and corresponding key material will need to be better protected[68].
- The role of the trust infrastructure needs to be better known to its end users. Through more pervasive education/training users need to understand what the function of trusted services is and that abnormal behaviour need to be reported immediately.
- Compliance and quality requirements for implementations of trust functions will need to be better enforced and checked. Although all necessary information on how to check and certify correctness of cryptographic functions do exist, a better use of this information needs to be enforced when it comes to applications that process confidential information.
- Operators of trust infrastructures need to undergo much more extensive, intensive and frequent security testing than any other infrastructure. The establishment of intelligence knowledge bases to be used commonly by relevant organisations will reduce the effects of successful attacks.

6.5 Threat Trends in Cloud Computing

Cloud Computing is the commissioned delivery of various infrastructure services based on a virtualized environment that is accessible over a web browser, usually over the Internet. Cloud Computing has received a lot of attention. Although many IT experts consider it primarily as a marketing innovation rather than a technical one, the adoption of cloud

[68] http://www.scmagazine.com.au/News/322042,co-lo-vms-busted-by-crypto-attack.aspx, accessed 10 November 2012.

products proceeds rapidly or is in the plans of most businesses. The degree of adoption varies in depth and width.

Over the trend of consumerization of IT, cloud services have also been adopted by private users, either by means of embedded services in purchased mobile devices or as useful tool to store and share information among various devices and platforms.

The concentration of vast amounts of data in few logical locations makes cloud computing an attractive target for attackers. At the same time, the capabilities offered attract cybercriminals to use the cloud for their purposes. Security issues regarding the cloud have been extensively addressed[69] in industry and academia.

The threats to the cloud can be mitigated effectively by the adoption of security controls by cloud providers. The adoption of security measures can outbalance the increased exposure of cloud services, caused by the increased number of expected attacks.

Nevertheless, the assumption made is that "*a large public cloud is an attractive target for threat attacks due to the large quantity of information attackers can access after successful attacks. The size of this information justifies even a large investment in time and resources to implement an attack.*"[70]. The integration of cloud services in mobile devices will let the attack surface of cloud further grow in the near future. Attackers will exploit vulnerabilities of mobile devices to gain access to cloud services.

By considering all service provision models available - that is IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) - threats applying to other computing resources are also considered relevant for cloud computing (see also section 4). The potential impact of an attack in the cloud, however, might be bigger due to the concentration of data.

The top emerging threats to cloud computing are as follows:

Emerging Threat	Threat Trend
1. Code Injection (code injections such as SQLi and Directory Traversal can affect cloud sources[71])	
2. Worms/Trojans (Just like any computer, worms and trojans target cloud computers[72][73][74]. They can lead to data loss/leakage)	

[69] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport, accessed 10 November 2012.

[70] http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport, accessed 16 November 2012.

[71] http://www.cloudtweaks.com/2012/07/press-release-q2-2012-firehost-web-application-attack-report-shows-sharp-rise-in-sql-injections/, accessed 16 November 2012.

[72] http://www.simplysecurity.com/2012/08/07/new-zeus-trojan-sets-sights-on-cloud-payroll-services/, accessed 16 November 2012.

Emerging Threat	Threat Trend
3. Drive-by exploits (web sites hosted on could computers are subject to injections (HTML, Javascript). Injections of web sites of cloud customers may lead to data loss and affect data of multiple customers)	↑
4. Abuse of Information leakage (based on the quality of implemented controls, information leakage will be one of the trends to be observed in cloud environments, especially with increased use of mobile devices)	↑
5. Compromising confidential information (data breaches performed by internal or external threat agents is one of the threats that will create significant impact in a cloud environment and might affect multiple users)	↑
6. Botnets (cloud functionality, esp. SaaS can be abused to implement botnet functions[75])	→
7. Denial of service (just as any IP address, cloud services can be subject of denial of service attacks)	→
8. Identity theft (credentials stealing trojan will remain a threat in could environments, especially in connection with the increased use of mobile devices)	↑
9. Physical Theft/Loss/Damage (given the concentration of data in cloud services, data loss due to malicious physical attacks might be an emerging issue, especially from malicious insiders)	→
10. Targeted attacks (there is an increased trend of observing targeted attacks on cloud services[76]. Yet of low frequency, the impact will be high)	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 6: Emerging Threat and their trends in the area of Cloud Computing[77]

[73] http://thenextweb.com/insider/2012/12/03/a-worm-is-hijacking-tumblr-blogs-and-posting-spam-said-to-affect-thousands-of-accounts/, accessed 3 December 2012.

[74] http://thenextweb.com/google/2012/11/17/new-malware-variant-recognizes-windows-8-uses-google-docs-as-a-proxy-to-phone-home/, accessed 3 December 2012.

[75] http://www.infoworld.com/d/security/study-lack-of-abuse-detection-allows-cloud-computing-instances-be-used-botnets-206008, accessed 11 November 2012.

[76] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trends-in-targeted-attacks.pdf, accessed 10 November 2012.

Besides the above mentioned emerging threat landscape, we have identified the following *emerging issues*:

- Attacks on (architectural) low levels of the cloud infrastructure will grow. Commonly used APIs of the virtual machines will be subject to attacks, especially those performing security tasks, such as encryption[78].
- Risks to cloud environments emanating from the increased use of mobile devices will grow. When exploited by attackers, vulnerabilities found in mobile platforms will have impact on the security of could services (e.g. loss of credentials to access cloud services and unsecured communication).
- Due to risks of co-hosting of sensitive information with other cloud customers, it is expected that a separation of sensitive workloads to dedicated hosts will be necessary in order to mitigate risks of data breaches[79].
- The use of cloud services as a cyber-tool will become an issue: attackers will leverage on the capabilities offered by cloud services to store malware, launch attacks, and gain proximity to potential victims (i.e. other could users) and thus maximise their impact. The issue of *Cybercrime-As-A-Service* is currently coming up within expert discussions[80].

6.6 Threat Trends in Big Data

As a consequence of the proliferation of social technologies, cloud computing, mobile computing and the internet use in general, huge collections/aggregations of data have been created. This concentration is called big data and is "*.. defined as large volumes of a wide variety of data collected from various sources across the enterprise*"[81]. The challenge with big data is it is difficult to process, analyse, capture, store, validate, etc. At the same time, even if still at early stages of adoption, big data is one of the highest priorities for businesses[55] and as such an emerging issue.

---

[77] *For this estimation we have also considered the report of CSA on threats to cloud computing and in particular: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf and https://downloads.cloudsecurityalliance.org/initiatives/top_threats/Top_Threats_Cloud_Computing_Survey_2012.pdf, both accessed 16 November 2012.*

[78] *http://www.scmagazine.com.au/News/322042,co-lo-vms-busted-by-crypto-attack.aspx, accessed 10 November 2012.*

[79] *http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf, accessed 14 November 2012.*

[80] *http://www.crn.com/news/security/240062607/fortinet-examines-cybercrime-as-a-service-industry.htm, accessed 10 November 2012.*

[81] *http://www.idgenterprise.com/press/big-data-initiatives-high-priority-for-enterprises-but-majority-will-face-implementation-challenges, accessed 11 November 2012.*

Exploitation of big data will affect data privacy. At the same time, exploitation of big data through adversaries might open doors to new type of attack vectors. A number of challenges have been identified for big data security[82]. Indicatively, these challenges address data protection, data access control and data filtering issues for huge data amount that are beyond the processing power of contemporary Security Information and Event Management (SIEM) products[83].

The top emerging threats to big data are as follows:

Emerging Threat	Threat Trend
1. Drive-by exploits (big data will provide attackers with information to place more successful malware attacks)	↑
2. Worms/Trojans (big data will provide attackers with information to place more successful malware attacks)	↑
3. Exploit kits (information gained by big data will provide attackers with additional intelligence about exploits and methods to better utilize exploit kits)	↑
4. Phishing attacks (big data, and in particular privacy information will allow attackers to run more targeted phishing attacks)	→
5. Compromising confidential information (big data will provide with insights towards data breaches)	↑
6. Spam (data gained from big data will allow for more targeted spamming attacks)	→
7. Targeted attacks (big data will provide information for targeted attacks)	→
8. Identity theft (discovery of information within big data will facilitate identity theft)	↑
9. Abuse of information leakage (analysis of big data will facilitate discovery of leaked information)	↑

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 7: Emerging Threat and their trends in the area of Big Data

Besides the above mentioned emerging threat landscape, we have identified the following *emerging issues*:

[82] https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Top_Ten_v1.pdf, *accessed 11 November 2012.*

[83] http://searchsecurity.techtarget.com/news/2240157901/Gartner-Big-data-security-will-be-a-struggle-but-necessary, *accessed 11 November 2012.*

- Based on big data, new methods regarding the collection of intelligence to launch attacks will be developed by attackers in order to improve their success rates.
- Businesses, and especially security industry, will devote efforts in the development of intelligence in order to better analyse big data towards management of security incidents. Security intelligence will be combined with existing security techniques/controls (i.e. SIEM) in order to have a more holistic approach in the management of cyber-security. The gathering and sharing of security intelligence will be one of the main trends in security sector for the years to come[84].
- Risk management will converge with Corporate Governance (GRC - Governance Risk and Compliance) and will be better interfaced with business objectives, detection of possible attack targets and operational security data. Big data will play a significant role in the decision support for better risk mitigation.
- The challenges faced within big data will lead to a change in security controls. Data centred security controls will be developed that, despite contemporary security policies, will focus of various aspects of data protection, data access, secure storage and secure data transactions[56].

[84] http://searchsecurity.techtarget.com/magazineContent/Information-security-threats-Building-risk-resilience, *accessed 11 November 2012.*

7 Concluding remarks

Concluding this work, it is worth referring to a number of issues that would need further elaboration within the information security community with regard to threat landscapes and their role in information security management.

After the collection, compilation and analysis of the available resources, it is considered as important to:

- *Collect and develop better evidence about attack vectors*: Delivery and hacking vectors might be different within a certain attack. It is important to develop a better understanding about the "workflow" of an attack, from its entry point down to the final asset targeted. This information is very rare in existing threat reports, an approach that goes this direction has been identified[85].
- *Collect and develop better evidence about impact achieved by adversaries*: In the information material analysed, we were not in the position to find some evidence on the impact achieved by successful threats. This information would be very interesting in order to understand the final targets of attackers and prioritise protection measures.
- *Collect and maintain more qualitative information about threat agents*: Despite the fact that literature on threat agents does exist, we were not able to find evidence of a co-relation between incidents and threat agents. An approach going towards this direction has been identified[59].
- *Use a common terminology*: It is considered as an important activity to develop a common vocabulary in threat management, e.g. to be used by standardisation bodies, international organisations, governments and NGOs. Approaches towards this objective are available[12], however a wider adoption seems to be necessary.
- *Include the user perspective*: The perspective of end-user is still absent from available information. Eventually, the end-user perspective could contain the impact of threats to end-users, but also provide guidance for development of threat awareness.
- *Develop use cases for threat landscapes*: It seems to be important that the information security community elaborates on use cases of threat landscapes and generate good practices for their inclusion in information security management activities/lifecycle.
- *Collect security intelligence*: With growing threat activity and increasing sophistication of attacks it seems inevitable to generate better conditions for the collection of intelligence on threats, risks and mitigation techniques by means of knowledge bases that can be commonly developed and shared among organisations.
- *Perform a shift in security controls*: It is important that a shift is performed from perimeter based, fragmented security controls towards data cantered, holistic and coherent end-to-end security policies and protection mechanisms.

[85] http://public.tableausoftware.com/views/VERISCommunity/SummaryofActions, *accessed 14 November 2012.*

Annex

NOTE: All points mentioned below are citations from the corresponding reports analysed.

Drive-by Exploits

- Today, drive-by downloads have become the top web threat.
  (Sophos - Security Threat Report 2012)[86]
- In May 2012, the first Android malware to use the drive-by download method was spotted in the wild.
  (McAfee - Threats Report: Second Quarter 2012)[87]
- Attackers regularly compromise marketing service providers' server applications to get them to deliver a malicious payload that leads to drive-by exploits.
  (BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]
- Today, malware distribution via drive-by exploits almost exclusively happens using compromised legitimate websites.
  (BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]
- Drive-by downloads have long been a standard infection vector for PC-based threats, but until now we had not seen it used by mobile threats. This changed in the middle of May, when we reported that the first drive-by download malware for Android had been spotted in the wild.
  (F-Secure - Threat Report H1 2012)[89]
- Continuing growth of Android malware. Android malware to use the drive-by download.
  (F-Secure - Mobile Threat Report Q2 2012)[90]
- Attackers can use exploit kits, compromise other websites, and redirect visitors of those sites to the exploit kit. Popular methods include embedded invisible iframes.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]

---

[86] http://www.sophos.com/en-us/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf, *accessed 14 November 2012.*

[87] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf, *accessed 14 November 2012.*

[88] https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html, *accessed 14 November 2012.*

[89] http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2012.pdf , *accessed 14 November 2012.*

[90] http://www.f-secure.com/weblog/archives/MobileThreatReport_Q2_2012.pdf, *accessed 14 November 2012.*

[91] http://www.secureworks.com/resources/articles/featured_articles/20120626-gen/index.html, *accessed 14 November 2012.*

- Detections of exploits that involve malicious HTML inline frames (IFrames) decreased slightly throughout the period, continuing a trend of moderate declines since 3Q11. These exploits are typically generic detections of inline frames that are embedded in webpages and link to other pages that host malicious web content. These malicious pages use a variety of techniques to exploit vulnerabilities in browsers and plug-ins; the only commonality is that the attacker uses an inline frame to deliver the exploits to users. The exact exploit delivered and detected by one of these signatures may be changed frequently.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Detections of the generic family JS/IframeRef more than doubled between 1Q12 and 2Q12 after several quarters of small declines. IframeRef is a generic detection for specially formed HTML inline frame (IFrame) tags that point to remote websites containing malicious content.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- iFrame injections that take users blindly down a path to web services, content, and often to offers that they do not desire.
  (Websense - Threat Report 2012)[93]
- First in the rating are various malicious URLs (we previously detected them as Blocked) that are already on our blacklist. Compared with the previous quarter these were down 2 percentage points to 84% of all detected problems. This list is principally filled with the websites that users are redirected to. Typically users get to these sites from hacked legitimate resources with embedded malicious scripts.
  (Kaspersky Lab - IT Threat Evolution: Q1 2012)[94]
- The use of malicious JavaScript code designed to exploit one or more web-enabled technologies accounted for nearly three-fourths of HTML and JavaScript exploits detected in the first half of 2012, primarily because of the Blackhole exploit kit.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Encrypted pieces of JavaScript code that appends itself to HTML pages or to other JavaScript snippets. It is then used to redirect the user to a page that hosts other e-threats, particularly web exploits against the browser and the Java Runtime

[92] http://download.microsoft.com/download/C/1/F/C1F6A2B2-F45F-45F7-B788-32D2CCA48D29/Microsoft_Security_Intelligence_Report_Volume_13_English.pdf, *accessed 14 November 2012.*

[93] https://www.websense.com/content/websense-2012-threat-report-download.aspx, *accessed 14 November 2012.*

[94] https://www.securelist.com/en/analysis/204792231/IT_Threat_Evolution_Q1_2012, *accessed 14 November 2012.*

Environment.
(Bitdefender - H1 2012 E-Threat Landscape Report)[95]

- Return of web browser exploitation - Recently, we identified a spike in browser exploitation though increased reports of the JavaScript_Shellcode Detected signature. A dramatic increase in this signature being triggered is probably due to a rise in web browser exploit toolkits. In turn, this may be due to an increase in web application attack campaigns looking for vulnerable servers to serve malicious links and, in some cases, to serve the actual malicious code.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- The second popular and much more dangerous attack category is drive-by download (an attack, in which the process of infecting a computer is done by exploiting a vulnerability in the browser or its plug-in is done automatically, unnoticed by the user). In 2011 attacks exploiting Java vulnerability in browsers were a significant element.
  (CERT Polska - An Analysis of Network Security Incidents in 2011)[97]
- High and critical browser vulnerabilities continue to rise and we have also observed an increase in drive-by-download attacks that have moved into targeting third-party browser plug-ins rather than the browser itself.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- For years, web browsers were the primary target of drive-by-download attacks. Although the number of high and critical browser vulnerabilities was up year over year, the number of exploits released for browser vulnerabilities is lower than any year since 2006. Drive-by-download attacks have moved into targeting third-party browser plug-ins more often than the browser itself.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Document readers are one such third-party component that has been a favourite of attackers as malicious document files can be used in drive-by download scenarios.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Infections from hacked legitimate websites and drive-by downloads, brought about by a failure to patch vulnerabilities in applications or the browser, remained common and costly to businesses.
  (Sophos - Security Threat Report 2012) [86]

---

[95] http://www.bitdefender.com/media/materials/e-threats/en/H1_2012_E_Threat_Landscape_Report_Aug_6.pdf, *accessed 14 November 2012.*

[96] http://www-03.ibm.com/security/xforce/downloads.html, *accessed 14 November 2012.*

[97] https://www.cert.pl/PDF/Report_CP_2011.pdf, *accessed 14 November 2012.*

[98] http://www-03.ibm.com/security/xforce/downloads.html, *accessed 14 November 2012.*

- Malware authors use drive-by downloads or phishing runs that typically depend only on social engineering tricks to infect a machine.
  (F-Secure - Threat Report H1 2012)[89]

Worms/Trojans

- By the end of 2011, Conficker was still the largest network threat in the world.
  (Sophos - Security Threat Report 2012)[86]
- Win32/Autorun 2nd position in Microsoft SIR V13 top 7 threat families.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- While Trojans account for most infections (80%), it is worth noting the relatively small number of PCs infected by worms. This demonstrates that massive worm epidemics have become a thing of the past, and have been replaced by a silent Trojan invasion.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- The highlight of the first quarter is the new record set in the creation of Trojan samples (four of every five new malware strains were Trojans).
  (PandaLabs – Quarterly Report January - March 2012, PandaLabs – Quarterly Report April - June 2012)[99],[100]
- For Q2 2012, Trojan was the most reported new malicious code, representing 41% of the top reported new malicious codes, followed by script (7.1%) and worm (7%).
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- In the first quarter of 2012, Trojan was the most frequently reported malicious code, representing 42.4% of the top reported malicious codes, followed by script (13.2%) and worm (6.8%).
  (ASEC - AhnLab Monthly Security Report – Vol.27)[102]
- 84% of mobile threats are Trojans. Most mobile threats are profit motivated.
  (F-Secure - Mobile Threat Report Q1 2012)[103]

---

[99] http://press.pandasecurity.com/wp-content/uploads/2012/05/Quarterly-Report-PandaLabs-January-March-2012.pdf, *accessed 14 November 2012.*

[100] http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf, *accessed 14 November 2012.*

[101] http://image.ahnlab.com/global/upload/download/asecreport/ASEC_Report_Vol.30_Eng.pdf, *accessed 14 November 2012.*

[102] http://image.ahnlab.com/global/upload/download/asecreport/ASEC_Report_Vol.27_Eng.pdf, *accessed 14 November 2012.*

[103] http://www.f-secure.com/weblog/archives/MobileThreatReport_Q1_2012.pdf, *accessed 14 November 2012.*

- Most of the infections were caused by Trojans (80% of all new malware samples), setting a new record high.
  (Anti-Phishing Working Group - Phishing Activity Trends Report, 1st Quarter 2012)[104]
- Password stealers showed a strong surge this quarter.
  (McAfee - Threats Report: First Quarter 2012, McAfee - Threats Report: Second Quarter 2012)[105,87]
- With the regionalization of malware, the world statistic of malicious codes is no longer significant. According to the malware statistics released by top security providers, Conficker worm, Autorun worm, Virut virus, Sality virus and rogue antivirus were reported in multiple countries.
  (ASEC - AhnLab Monthly Security Report – Vol.24)[106]
- Compared to the previous month, the number of Trojan and worm increased, whereas the number of script, adware, dropper, virus, downloader and spyware decreased.
  (ASEC - AhnLab Monthly Security Report – Vol.27)[102]
- In the first six months of 2012, the malware landscape remained relatively constant, with Trojan.AutorunInf, Win32.Worm.Downadup and Exploit.CplLnk as the top three e-threats worldwide. The first two pieces of malware are more than four years old and, even though the vulnerabilities that allow them to infect systems have been addressed, they still claim victims.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- Trojan.AutorunINF.Gen–Trojan.AutorunInf needs no introduction - it has been one of the world's top three e-threats for about four years. This detection addresses rogue Autorun files created by a variety of malware families to facilitate spreading via removable media.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- Win32.Worm.Downadup – The Downadup worm emerged in early 2008 and caused one of the largest epidemics of all times, as it managed to infect more than 12 million computers in less than 24 hours.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]

[104] http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf, *accessed 14 November 2012.*

[105] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf, *accessed 14 November 2012.*

[106] http://image.ahnlab.com/global/upload/download/asecreport/ASEC_Report_Vol.24_Eng.pdf, *accessed 14 November 2012.*

- The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system
  (ESET - Global Threat Reports)[107]
- Social networks represent a vehicle for malware authors to distribute their programs in ways that are not easily blocked. The Koobface Worm which infiltrated Facebook, Myspace and other social networking sites.
  (IBM - IBM X-Force 2012 Cyber Security Threat Landscape)[108]
- Social networks threats and risks: malware (worms, Trojans, rootkis) : frequency very high, likelihood very high.
  (CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]
- The biggest recent spyware event was the detection of the Flame worm.
  (Kaspersky Lab - IT Threat Evolution: Q2 2012)[110]
- Win32/Autorun is a generic detection for worms that attempt to spread between mounted computer volumes by misusing the AutoRun feature in Windows.
  (Microsoft – The evolution of malware and the threat landscape – a 10-year review)[111]
- Win32/Dorkbot is a worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Autorun is a generic detection for worms that spread between mounted volumes using the Autorun feature of Windows. Recent changes to the feature in Windows XP and Windows Vista have made this technique less effective, but attackers continue to distribute malware that attempts to target it.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Families that were significantly more prevalent on domain-joined computers during at least one quarter include the worm family Win32/Conficker.
  (Microsoft - Security Intelligence Report Volume 13)[92]

---

[107] http://www.eset.com/us/resource/papers/reports/, *accessed 14 November 2012.*

[108] https://www-950.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/ThreatLandscape2012/$file/ThreatLandscape2012.pdf, *accessed 14 November 2012.*

[109] http://www.clusit.it/docs/rt67d_o23xfrsh9IIE.pdf, *accessed 14 November 2012.*

[110] https://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012, *accessed 14 November 2012.*

[111] http://www.microsoft.com/security/sir/story/default.aspx#!10year, *accessed 14 November 2012.*

- Targeted attacks are generally carried out using Trojans, but in this case we are talking about a worm, which introduces a new factor: Worms can replicate themselves automatically, so virus authors could eventually lose control of who or whose computers their creations are infecting.
  (PandaLabs – Quarterly Report April - June 2012)[100]
- Massive worm epidemics have become a thing of the past and have been replaced by an increasing avalanche of Trojans, more specifically, banking Trojans and the infamous 'Police Virus".
  (PandaLabs – Quarterly Report April - June 2012)[100]
- Facebook continues its reign as the number one social networking site but it also is a favourite target of cyber-crooks. In January, a worm was discovered that had stolen over 45,000 Facebook login credentials. Researchers fear that the criminals used these 'infected' accounts to send links to people's Facebook friends, spreading the computer worm further.
  (PandaLabs – Quarterly Report January - March 2012)[99]
- More than three years after its initial release, the Conficker worm is still the most commonly encountered piece of malicious software.
  (Sophos - Security Threat Report 2012) [86]
- In terms of the most prevalent threats (i.e. the ones that are mostly responsible for the rise in the statistics), simple SMS mobile trojans.
  (ESET - Global Threat Report August 2012)[112]
- Espionage has gone digital. And while we've seen several cases of nation-state espionage done with backdoors and Trojans.
  (F-Secure - Threat Report H1 2012)[89]
- Nearly half (49%) of all Kaspersky Lab threat detections in the second quarter of 2012 were multifunctional mobile Trojans that steal data from telephones (contact names, email addresses, telephone numbers, etc.), and are also capable of downloading additional modules from servers run by malicious users.
  (Kaspersky Lab - IT Threat Evolution: Q2 2012)[110]
- Using the official Android marketplace is no security guarantee either, as it has also been targeted by cyber-crooks luring users into installing Trojans disguised as legitimate apps. Something which, by the way, has also happened to Apple's App Store, but to a lesser extent than to Google's Play Store.
  (PandaLabs – Quarterly Report April - June 2012)[100]

[112] http://go.eset.com/us/resources/threat-trends/Global_Threat_Trends_August_2012.pdf, *accessed 14 November 2012.*

- The idea that this computing platform would be targeted en mass is something Internet security experts have warned about for years. That day has finally arrived. A trojan by the name of Flashback, which first appeared last year, had a breakout performance in April, successfully infecting approximately 600,000 Macs.
  (Symantec - Intelligence Report: May 2012)[135]
- Rise of Mac Malware.
  (Sophos - Security Threat Report 2012) [86]
- Flashback Mac Malware. first massive malware outbreak on the Mac OS X platform (F-Secure 1H2012) Another major development in Mac malware in the first half of the year is the discovery of targeted malware (Mac APT). This targeted malware's purpose is to steal user data.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Mac OSX APT : A successful attack saw Mac OS X systems infected with Backdoor.OSX.Lasyr. This backdoor allows cybercriminals to gain control of an infected machine and get access to all the information on the computer. It was detected in mid-March 2012. This was not the only case of targeted attacks using Mac malware in the first quarter of 2012. The second case involved only a backdoor for Mac OS X - Backdoor.OSX.MaControl.
  (Kaspersky Lab - IT Threat Evolution: Q1 2012)[94]

Code Injection Attacks

- We have seen steady growth in SQL injection, which is keeping pace with the increased usage of cross-site scripting and directory traversal commands, such as HTTP "DotDot" commands.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- The most common vector has been SQL injection attacks that, when successful, not only significantly impact the availability of targeted sites but also create a significant risk of data leakage by their nature.
  (Akamai - The state of the Internet, 1st Quarter, 2012 Report)[113]
- Cross-site scripting (XSS) and SQL injection (SQLi), which remain the most popular attack vectors, have been holding steady at roughly 30% of the total vulnerabilities in 1Q2012.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- Mass SQL injection e.g. LizaMoon (2011).
  (ASEC Report Vol.24)[106]

[113] http://www.akamai.com/stateoftheinternet/, *accessed 14 November 2012.*

- The latest version of these SQL mass injection attacks began to emerge in April 2012. The recent SQL injection attack is most probably related to LizaMoon but has evolved through social engineering so that it spreads through pages that pretend to offer 'never-before-seen' sexual content or fake antivirus products.
  (AVG - AVG Community Powered Threat Report Q2 2012)[114]
- Significant increase in reported XSS cases within the past two years.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Vulnerabilities and corrections related to flaws that allow SQL injection attacks continue to be a widespread problem.
  (Cisco - 2011 Annual Security Report)[115]
- SQL Injection has been in the news frequently over the last year and the data collected shows a significant rise in attacks, as well. As 2011 progressed, SQL Injection became one of the attack techniques of choice causing the rise in attacks.
  (HP - 2011 top cyber security risks report)[116]
- While XSS and RFI have remained relatively flat over the year, SQL Injection saw a steady rise throughout much of 2011 and also showed a wide variance in attack technique. The rise in SQL Injection attacks is likely due to its popularity from the Anonymous and LulzSec attacks, as well as mass SQL Injection campaigns like Liza Moon and Lilupophilupop.
  (HP - 2011 top cyber security risks report)[116]
- A sharp decrease in XSS attacks is observed from 2010 to 2011, while a sharp increase in SQL Injection from 2010 to 2011 is seen after seeing a decrease from 2009 to 2010. RFI attacks remained steady from 2010 to 2011.
  (HP - 2011 top cyber security risks report)[116]
- While SQL injection was observed in the traditional applications, it was not represented in the Web 2.0 sample size. The top critical vulnerability across both traditional Web applications and Web 2.0 applications remains cross-site scripting.
  (HP - 2011 top cyber security risks report)[116]
- SQL Injection to be a favourite attack vector amongst malicious groups. Attackers are analysing Web applications (written in .ASP, PHP, etc.) running on the Web server in order to find SQL injection vulnerabilities they can exploit.
  (IBM - IBM X-Force 2012 Cyber Security Threat Landscape)[108]

---

[114] http://www.avg.com.au/files/media/avg_threat_report_2012-q2.pdf, *accessed 14 November 2012.*

[115] http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf, *accessed 14 November 2012.*

[116] http://www.hpenterprisesecurity.com/collateral/report/2011FullYearCyberSecurityRisksReport.pdf, *accessed 14 November 2012.*

- Through the disclosure of breaches in 2012, we continue to see SQL injection reigning as the top attack technique. In addition, attackers seem to be taking advantage of cross-site scripting vulnerabilities for web applications. Over 51% of all web application vulnerabilities reported so far in 2012 are now categorized as cross-site scripting.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- The decline of reported SQL injection vulnerabilities continued in 2012 but cross-site scripting vulnerabilities increased again to a projected all-time high.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- The hacktivist groups, Anonymous and Lulzsec, had a major presence in SQL injection tactics early in 2011 and continued to hone their skills with new injection attack vectors. However, their activity levels had entered a brief lull that was recognizable.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- In 2012, we are seeing even higher levels of SQL injection attempts and the expansion rate of this type of attack appears to be higher than at the end of 2011. The net result of all this activity has kept SQL injection in the highest position for the first half of 2012.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Attackers continue to combine different technologies together, creating a layered attack from which they may have a greater chance of success and can be difficult to defend against. SQL injection is one of the most common exploits found in these tool kits, especially when combined with other commonplace exploits, such as shell command injection, or cross-site scripting.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Hackers like DoS. In our hacker forum study from October 2011, we observed that 22% of discussions focused on DoS, slightly higher than SQL injection at 19% of all discussions.
  (Imperva - Hacker Intelligence Initiative, Monthly Trend Report #12)[117]
- Attacks against websites using SQL injections rose by 69% between April and June 2012.
  (MELANI - Semi-annual report 2012/I, January – June)[118]
- Analysis of malicious or criminal attacks experienced by 18 companies: SQL injection 4th place 28%.
  (Ponemon Institute - 2011 Cost of Data Breach Study)[119]

---

[117] http://www.imperva.com/docs/HII_Denial_of_Service_Attacks-Trends_Techniques_and_Technologies.pdf, *accessed 14 November 2012.*

[118] http://www.news.admin.ch/NSBSubscriber/message/attachments/28312.pdf, *accessed 14 November 2012.*

- Basic vulnerabilities such as SQL injection and cross-site scripting still account for a majority of security flaws in web applications. By exploiting these types of flaws, hacktivists operating under the Anonymous banner compromised several high-profile sites in 2011.
  (Secunia - Yearly Report 2011)[120]
- For Web-based attacks, SQL injection remains the number one attack method for the fourth year in a row.
  (Trustwave - 2012 Global Security Report)[121]
- SQL Injection is the top Attack Method for Entertainment, Retail, Technology, Media and Education websites.
  (Trustwave - 2012 Global Security Report)[121]
- CSRF is the top Attack Method for Web 2.0 and Hosting Providers websites.
  (Trustwave - 2012 Global Security Report)[121]
- SQL Injection is the No1 Web Application Risk.
  (Trustwave - 2012 Global Security Report)[121]
- The most common attack methods : SQL Injection, PHP Code Injection/Execution, Remote File Inclusion.
  (T-Mobile - Security on the Internet-Report on information and Internet security)[122]
- The favourite vulnerability class of malicious hackers, SQL Injection, remained the 8th most prevalent website vulnerability, even though it dropped 3 by points to 11% of websites.
  (WhiteHat SECURITY - Statistics Report 2012)[123]
- If XSS is the most prevalent website vulnerability, SQL Injection is likely the most exploited. Still, SQL Injection remains fixed in 8th place on the WhiteHat Top Ten and has even dropped 3 points down to 11% of websites- several times less prevalent than XSS. This should be a reminder that vulnerability prevalence does not automatically correlate to vulnerability exploitation.
  (WhiteHat SECURITY - Statistics Report 2012)[123]

---

[119] https://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-cost-of-a-data-breach-2011, *accessed 14 November 2012.*

[120] https://secunia.com/?action=fetch&filename=Secunia_Yearly_Report_2011.pdf, *accessed 14 November 2012.*

[121] https://www.trustwave.com/global-security-report, *accessed 14 November 2012.*

[122] http://www.telekom.com/static/-/151706/2/pdf-report-security-in-the-internet-12-si, *accessed 14 November 2012.*

[123] https://www.whitehatsec.com/assets/WPstats_summer12_12th.pdf, *accessed 14 November 2012.*

- One of the most devastating scourges on the Web is the formidable mass SQL Injection worm, with the most recognizable being LizaMoon.
  (WhiteHat SECURITY - Statistics Report 2012)[123]
- In 2011 XSS vulnerabilities half as likely to exist in customer's as compared to 4 years ago However, XSS vulnerabilities still appear in about 40% of the applications IBM scans - High for something well understood and easily addressed.
  (IBM - IBM X-Force 2012 Cyber Security Threat Landscape)[108]
- Cross-site scripting has been one of the most persistent exploits of the Internet. This attack works on any web browsing technology, including mobile devices. The attack is extremely popular and can pose a significant security risk.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Cross-site scripting (XSS) attacks have become the most prevalent and dangerous security issue affecting web applications. The MSRC has observed a significant increase in reported XSS cases within the past two years, to the point where XSS vulnerabilities have started to displace other types of reported vulnerabilities by percentage.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- While XSS flaws are the prevalent finding within Web applications, the resulting risk level is lower than SQL injection as attackers are not leveraging them as much in profit-driven attack scenarios.
  (Trustwave - 2012 Global Security Report)[121]
- In 2010, 64% of websites had at least one Information Leakage vulnerability, which overtook the notorious Cross-Site Scripting (XSS) as the most prevalent issue by just a few tenths of a percent. During 2011, Information Leakage and XSS switched top spots again and both vulnerability classes saw a notable reduction. In 2011, XSS regained its title as the most prevalent website vulnerability being found in 55% of websites.
  (WhiteHat SECURITY - Statistics Report 2012)[123]
- SQL injection, cross-site scripting, cross-site request forgery, and remote file include are the most common vulnerabilities in OSVDB (2000-2011) that can be exclusively exploited via the Web.
  (HP - 2011 top cyber security risks report)[116]
- Mobile applications are different, but the same. They use different frameworks and Web services than their desktop counterparts, but mobile applications are susceptible to the same types of vulnerabilities as normal, non-mobile applications. We found multiple instances of cross-site scripting, easily broken authentication, and information leakage across the sample set.
  (HP - 2011 top cyber security risks report)[116]

- SQL injection and cross-site scripting are growing rapidly as favoured attack methods, and that our trending information matches the assertion.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]

Exploit Kits

- Cyber criminals are adopting an increasingly professional attitude through the marketing of 'commercial' crimeware kits, the most advanced crimeware, the Blackhole exploit kit.
  (AVG - AVG Community Powered Threat Report Q1 2012)[124]
- Blackhole is a sophisticated and powerful exploit kit, mainly due to its polymorphic nature, and it is heavily obfuscated to evade detection by anti-malware solutions.
  (AVG - AVG Community Powered Threat Report Q1 2012)[124]
- More exploit kits to distribute malware.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- Blackhole continues to rule the malware market with a 63 percent malware market share. Blackhole exploits include: a) Social networks overwhelmed by malicious advertising from compromised ad servers, b) Seemingly normal graphics images containing malicious script, c) Tricks to trap experienced website owners and administrators.
  (AVG - AVG Community Powered Threat Report Q3 2012)[125]
- With the 'release' of Blackhole Exploit Toolkit 2.0 in September we can expect in future months to see an upsurge in large-scale attacks.
  (AVG - AVG Community Powered Threat Report Q3 2012)[125]
- Commercial' toolkit, Blackhole, continues to rule the malware market with 63 percent market share. With the 'release' of Blackhole Exploit Toolkit 2.0 in September, we can expect in future months to see an upsurge in large-scale attacks. These will likely be more aggressive as a result of the new evasion techniques introduced in this latest version.
  (AVG - AVG Community Powered Threat Report Q3 2012)[125]
- BlackHole can be used to make money themselves through credit card and banking frauds and by installing rogue security products or through ransomware and other payloads.
  (AVG - AVG Community Powered Threat Report Q1 2012)[124]

---

[124] http://www.avg.com.au/files/media/avg_threat_report_2012-q1.pdf, *accessed 14 November 2012.*

[125] http://www.avg.com.au/files/media/avg_threat_report_2012-q3.pdf, *accessed 14 November 2012.*

- The most common methods users are encountering Blackhole exploit kits so far are i) through compromised websites, ii) Search Engine Optimization (SEO) poisoning and iii) email spam. Blackhole exploits vulnerable browser plug-ins such as Java, Adobe Reader and Adobe Flash Player.
  (F-Secure - Threat Report H1 2012)[89]
- Exploit kits, which criminals can purchase, are software packages that attempt to install malware on a victim's computer by exploiting vulnerabilities in web browsers and third-party add-ons such as Adobe Acrobat Reader and Java. Attackers can use these kits, compromise other websites, and redirect visitors of those sites to the exploit kit. Popular methods include embedded invisible iframes.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- Attacks are increasingly aimed at application vulnerabilities that are discovered by exploit kits (and less on operating systems, thanks to automated patch cycles).
  (Websense - Threat Report 2012)[93]
- One of the more powerful and effective stages of an advanced threat is the exploit kit, with Blackhole being one of the leading exploit kits for the year in review.
  (Websense - Threat Report 2012)[93]
- Cybercrime has developed exploit kits and advanced methods to attack Windows systems and the software that resides on this platform as the target installed base is very large.
  (Websense - Threat Report 2012)[93]
- Blackhole was the most commonly detected exploit family in the first half of 2012 by a large margin.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- The Blackhole exploit kit targets a large number of exploits in web browsers and browser plug-ins in an effort to infect vulnerable computers through drive-by download attacks.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- The Exploit category, which had been increasing gradually for several quarters, fell slightly in 2Q12. This trend corresponds to the increase and apparent peaking of the Blackhole exploit kit. (Microsoft - Security Intelligence Report Volume 13)[92]
- New Criminal Business Model Emerges: Malware-as-a-Service (MaaS)
  (Verisign - 2012 iDefense Cyber Threats and Trends)[126]

[126] https://www.verisigninc.com/assets/whitepaper-idefense-2012-trends.pdf, *accessed 14 November 2012.*

- Like software developers in any other field, the authors of these exploit kits have been steadily improving their products and product support.
  (F-Secure - Threat Report H1 2012)[89]
- The use of Web attack toolkits has been on the rise since the end of 2011.
  (Symantec - Intelligence Report: July 2012)[127]
- Blackhole Exploit Kit The most active threat on the web, 63.2% of detected malware.
  (AVG - AVG Community Powered Threat Report Q3 2012)[125]
- Blackhole's market share in the global malware market is on average 35 per cent, and its market share among the crimeware toolkits is on average 70 per cent.
  (AVG - AVG Community Powered Threat Report Q1 2012)[124]
- The popularity of the Blackhole exploit kit increased significantly in 2011, and the kit now appears to be the exploit kit of choice for the majority of cyber criminals.
  (HP - 2011 top cyber security risks report)[116]
- Rise in exploit kit popularity and obfuscation in exploit kits.
  (HP - 2011 top cyber security risks report)[116]
- In August, AVG Threat Labs identified an explosion of attacks using the notorious Blackhole Exploit kit that targeted key social networks including Facebook.
  (AVG - AVG Community Powered Threat Report Q3 2012)[125]
- Exploit kits are a keystone in the attack ecosystem, and more and more, they use encoding and obfuscation to make detection more difficult.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- Malicious code injected by attackers into compromised websites usually does not target only one single vulnerability. Instead, it leads to a so-called exploit kit. An exploit kit (or exploit pack) is a software package that automates the exploitation of vulnerabilities on users' PCs using drive-by exploits subsequently infecting them with malware.
  (BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]

Botnets

- Cybercriminals have created the first Android bootkit which turns phones with the Android operating system into 'zombies'.
  (AVG - AVG Community Powered Threat Report Q2 2012)[114]

[127] http://www.symanteccloud.com/en/gb/mlireport/SYMCINT_2012_07_July.pdf, accessed 14 November 2012.

- ZeroAccess(Win32/Sirefef) rootkit, one of the most prevalent threats of its kind in Q2, P2P botnet.
  (F-Secure - Threat Report H1 2012)[89]
- Zeusbot/Spyeye P2P Updated.
  (Symantec - Intelligence Report: February 2012)[128]
- Infections related to botnets have reached a 12-month high.
  (McAfee - Threats Report: Second Quarter 2012)[87]
- ZeroAccess uses a P2P network protocol for communicating with the C&C. Implements a number of malicious techniques:1)BlackHat SEO, 2) Clickjacking, 3) Substitution of its own choice of URLs for the legitimate results that a search engine would generate for an uncompromised system: in this case, to implement click fraud.
  (ESET - Global Threat Report June 2012)[129]
- Botnet command and control architecture is becoming decentralized.
  (Georgia Tech Cyber Security Summit 2011 - Emerging Cyber Threats Report 2012)[130]
- Economies of scale drove the very logical evolution from the single-purpose botnet, perhaps deployed for either spamming or denial of service attacks, to the multi-purpose botnet, the modular design of which allowed different tasks to be pushed to the same collection of compromised machines without having to repeat the infection process.
  (ESET - Global Threat Report August 2012)[112]
- Malware coders appear interested in setting up botnets via malicious mobile apps
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- In 2011, Zeus was far and away the largest botnet.
  (Blue Coat - Blue Coat Systems 2012 Web Security Report)[131]
- It is clear from the data that though botnets may be taken down, infected computers remain. Conficker provides a prime example.
  (Blue Coat - Blue Coat Systems 2012 Web Security Report)[131]
- Botnets are now also being rented out professionally, and their “customers” use them to take revenge, gain competitive advantages and for criminal purposes like extortion. Attacks may also be politically or religiously motivated. Another trend began to emerge in 2010: “hacktivism”.

---

[128] http://www.symanteccloud.com/en/gb/mlireport/SYMCINT_2012_02_February_FINAL.PDF, *accessed 14 November 2012.*

[129] http://go.eset.com/us/resources/threat-trends/Global_Threat_Trends_June_2012.pdf, *accessed 14 November 2012.*

[130] http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf, *accessed 14 November 2012.*

[131] https://www.bluecoat.com/sites/default/files/documents/files/BC_2012_Security_Report-v1i-optimized.pdf, *accessed 14 November 2012.*

(BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]

- Cloud Computing platforms are already being used to set up botnets.
  (BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]
- ZeuS – P2P+DGA variant – mapping out and understanding the threat.
  (CERT Polska - An Analysis of Network Security Incidents in 2011)[97]
- Instead of just a few very large botnets, usually managed by established criminal enterprises, there are now dozens of smaller botnets engaging in criminal activity. Moreover, the availability of botnet toolkits has greatly increased the number of botnets, allowed more variations, and complicates the task of analysing their behaviour patterns and providing protection from them. The number and variety of these smaller botnets make it challenging for security professionals to track their movements.
  (Cisco - 2011 Annual Security Report)[115]
- Sophisticated criminal operations are moving away from the massive botnets commonplace in years past because law enforcement and the security industry are keeping a close watch on this activity. However, many smaller botnets have been developed—with each one capable of inflicting more damage per bot.
  (Cisco - 2011 Annual Security Report)[115]
- Private organizations partnering with law enforcement disrupted several large botnet operations and worked to eliminate associated malware from infected systems.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- The CTU research team is currently tracking more than 225 botnets specifically dedicated to DDoS. Some of these botnets are dedicated to a particular actor or group, while other botnets are contract-based and will attack any host as long as the botnet operators are paid.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- Lots of small botnets have been detected and are being used for information theft such as personal data and home banking credentials from compromised computers.
  (ESET - Global Threat Report September 2012)[132]
- Flashback integrated infected Macs into a botnet. In April, it was reported that more than 600,000 Mac computers – mostly those with the Snow Leopard operating system – were infected. For the first time ever, Apple published a special tool for removing the

[132] http://go.eset.com/us/resources/threat-trends/Global_Threat_Trends_September_2012.pdf, *accessed 14 November 2012.*

malware. Hence, malware has definitely arrived in the Mac universe.
(G Data - Malware Half-yearly report January – June 2012)[133]

- Communicating through peer-to-peer networks instead of ordinary structures with individual central servers. Since central servers present a single point of failure in the infrastructure of botnets because they can be shut down by investigating authorities or providers, this innovation greatly increased the stability of the botnet (Gameover botnet).
  (G Data - Malware Half-yearly report January – June 2012)[133]
- Large botnets of infected mobile devices have started to appear on the scene and this is only the beginning.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Spam continues to decline in the past months and even years. We believe this is due to several botnet takedowns.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- On July 18th, 2012, we witnessed the take down of the Grum botnet. This resulted in an annual low of spam volume.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Mobile systems will constitute and escalating portion of botnets as they have valuable processing power and bandwidth, and most of them are not provided with effective anti-malware protections, users often tamper them to unlock some advanced functions, which often make them even more vulnerable.
  (CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]
- Botnets currently control millions of personal computers around the world, which can be summoned as a kind of malicious software as a service (SaaS).
  (Juniper Networks - The Evolving Threat Landscape)[134]
- Botnet technologies have been developing for several years, giving rise to decentralized botnets and botnets managed via social networks, with drive-by downloads becoming the principal method of infection.
  (Kaspersky Lab - IT Threat Evolution: Q1 2012)[94]
- In Q1 2012, cybercriminals created a botnet using a 'fileless' bot for the first time. Security researchers discovered a mobile botnet that was comparable in size with typical Windows botnets, as well as a botnet of more than half a million Apple

[133] http://www.gdata.nl/uploads/media/GData_MWR_1_2012_EN.pdf, *accessed 14 November 2012.*

[134] https://www.juniper.net/us/en/local/pdf/whitepapers/2000371-en.pdf, *accessed 14 November 2012.*

computers running Mac OSX.
(Kaspersky Lab - IT Threat Evolution: Q1 2012)[94]

- The beginning of 2012 was marked by a qualitative change in the botnet ecosystem. Botmasters, who had begun to feel overcrowded in the Windows world actively targeted the mobile and Mac OS segments. Unfortunately, few users realize that their smartphones are fully-functional computers which contain valuable data that may be of interest to cybercriminals. Mobile devices and Macs are very attractive to cybercriminals.
  (Kaspersky Lab - IT Threat Evolution: Q1 2012)[94]
- The use of Twitter for control of mobile botnets.
  (McAfee - Threats Report: Second Quarter 2012)[87]
- Deactivation of a Zeus botnet.
  (MELANI - Semi-annual report 2012/I, January – June)[118]
- Flashback Trojan infected up to 600,000 Mac computers around the world, creating the largest botnet ever to target Apple computers.
  (PandaLabs – Quarterly Report April - June 2012)[100]
- Botnet takedowns momentarily knock out spam.
  (Sophos - Security Threat Report 2012) [86]
- Flashback—The day of the Mac threat has arrived.
  (Symantec - Intelligence Report: May 2012)[135]
- Grum botnet takedown - Security Researchers successfully disrupted one of the largest spam-sending botnets in the threat landscape in July.
  (Symantec - Intelligence Report: July 2012)[127]
- Cybercriminals are cherry-picking their targets to launch more successful campaigns. Based on Trend Micro observations this quarter, cybercriminals are poised to become more aggressive, using more sophisticated tools like automatic transfer systems (ATSs) and the Blackhole Exploit Kit to enhance the power of their respective ZeuS, SpyEye, and other botnets.
  (Trend Micro - TrendLabs 2Q 2012 Security Roundup)[136]
- Even though botnets will become smaller, they will grow in number, making effective law enforcement takedowns more difficult to realize.
  (Trend Micro - TrendLabs 2Q 2012 Security Roundup)[136]

---

[135] http://www.symanteccloud.com/en/gb/mlireport/SYMCINT_2012_05_May_FINAL-en_us.pdf, *accessed 14 November 2012.*

[136] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-its-big-business-and-its-getting-personal.pdf, *accessed 14 November 2012.*

- Mobile malware programs can build up botnets for smartphones, for example. Possible targets of attack are reachable from the Internet using infrastructure components.
  (T-Mobile - Security on the Internet-Report on information and Internet security)[122]
- The threat presented by botnets has continued to rise dramatically over the past two years, partly as a result of the risk of infection by drive-by exploits.
  (BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]
- Botnet technologies have been developing for several years, giving rise to decentralized botnets and botnets managed via social networks, with drive-by downloads becoming the principal method of infection.
  (Kaspersky Lab - IT Threat Evolution: Q1 2012)[94]

Denial of service

- Continuing a trend that has grown over time, many of Akamai's customers experienced denial-of-service (DoS) attacks during the first half of 2012. Tools that require lower traffic volumes, such as hashdos and slowloris, have become more widely used.
  (Akamai - The state of the Internet, 2nd Quarter, 2012 Report)[137]
- Application-layer (Layer 7) DDoS attacks continue to grow in both prevalence and sophistication.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]
- Both flood-based and application-layer attack components are rapidly gaining in popularity with attackers.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]
- DDoS attacks and multi-vector DDoS attacks are becoming more common.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]
- Nearly 47 percent of respondents indicated that they are able to successfully mitigate DDoS attacks within 20 minutes, a slight decrease from last year. Nearly 33 percent indicated mitigation times in excess of 30 minutes, more than double the number of operators reporting longer mitigation times than last year. This may be a result of the increasing popularity of complex application attacks that are often more difficult to detect and mitigate.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]

---

[137] http://www.akamai.com/stateoftheinternet/, *accessed 14 November 2012.*

[138] http://www.techdata.com/arbornetworks/files/Arbor%20Security%20Report%202012.pdf, *accessed 14 November 2012.*

- HTTP, DNS and SMTP most frequently targeted protocols used by applications.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]
- First-Ever Reports of IPv6 DDoS Attacks 'in the Wild' on Production Networks.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]
- Ideologically-Motivated 'Hactivism' and Vandalism Are the Most Readily-Identified DDoS Attack Motivations. 35% reported political or ideological attack motivation. 31% reported nihilism or vandalism as attack motivation. Significant increase in the prevalence of flood-based DDoS attacks in the 10 Gbps range.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]
- Q3 2012 was defined by extremely large DDoS attacks. It is clear that bitrates of 20 Gbps are the new norm.
  (Prolexic - Quarterly Global DDoS Attack Report Q3 2012)[139]
- 10 Gbps and larger flood-based DDoS attacks are the 'New Normal'.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]
- Stateful firewalls, IPS and load-balancer devices continue to fall short on DDoS protection capabilities.
  (Arbor Networks - Worldwide Infrastructure Security Report 2011 Volume VII)[138]
- The first half of 2012 went smoothly without the witnessing of huge security incidents such as large-scale DDoS attacks or disclosure of internal information reported during the same period last year.
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- The first trend is the gradual rise in backscatter activity. Backscatter is actually a side effect of spoofed denial-of-service (DoS) attacks. So, there has been a steady increase in spoofed DoS attacks since 2006.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- DoS attacks are technically broadly available: Many attack tools are freely available, Some parties offer DoS attack as a service.
  (Imperva - Hacker Intelligence Initiative, Monthly Trend Report #12)[117]
- DoS is moving up the stack and into the application layer. Over the last years, attackers move their DoS attacks up the stack and into the Web application layer in order to decrease costs, as Web app DoS is more efficient and avoids detection as many anti-DoS solutions are traditionally focused on lower layers.
  (Imperva - Hacker Intelligence Initiative, Monthly Trend Report #12)[117]

[139] https://www.prolexic.com/knowledge-center-ddos-attack-report-2012-q2.html, *accessed 14 November 2012.*

- The heavy computational burden incurred by the SSL-handshake process leaves SSL-protected resources prime candidates for effective Denial of Service (DoS) attacks. Together with an increased consumption of computer resources per session, a multitude of simple attacks can be devised very efficiently.
  (Imperva - Security Trends 2012)[140]
- DDoS attacks are now seen as a major threat by governments as well as large corporations.
  (Arbor Networks – a decade of DDoS)
- Hackers like DoS. In our hacker forum study from October 2011, we observed that 22% of discussions focused on DoS, slightly higher than SQL injection at 19% of all discussions (Imperva - Hacker Intelligence Initiative, Monthly Trend Report #12)[117]
- DoS is the top Attack Method for governmental/politics services.
  (Trustwave - 2012 Global Security Report)[121]

Phishing

- From 2010 to 2012, the email scam/phishing volume nearly quadrupled, reaching more than 83% of the 2008 levels in spring 2012.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- During the first six months of 2012, phishers were more active than in the last half of 2011. Financial institutions were once again the most targeted businesses in phishing e-mail.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- Emergence of Phishing Sites Targeting both PC and Mobile - Another trend that stood out during the last half is the prevalence of phishing websites. What made the new phishing sites distinguishable were their sophisticated designs customized for different terminals from smartphone to personal computer.
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- Targeting financial, payment services, social networking, ISP, and government sectors websites.
  (Anti-Phishing Working Group - Phishing Activity Trends Report, 1st Quarter 2012)[104]
- Public Sector remained the most targeted by phishing activity in January. Then Finance, Education, Retail, IT Services and chemical & pharmaceutical. SMBs more targeted than large enterprises. Organizations spoofed in phishing attacks : Banking, E-

[140] http://www.imperva.com/docs/HI_Security_Trends_2012.pdf, *accessed 14 November 2012.*

Commerce and information services.
(Symantec - Intelligence Report: January 2012)[141]

- Either the email contains the malicious attachment in a file, or the attachment contains a URL that leads to the malware. SMBs more targeted than large enterprises. Public Sector remained the most targeted by phishing activity in February. Organizations spoofed in phishing attacks: E-Commerce and information services.
(Symantec - Intelligence Report: February 2012)[128]
- Phishers Offer Fake Storage Upgrades, Phishing for Fake Discount Cards, The Public Sector remained the most targeted by phishing activity in May. SMBs more targeted than large enterprises. Organizations spoofed in phishing attacks: Banking, E-Commerce and information services.
(Symantec - Intelligence Report: May 2012)[135]
- The Public Sector remained the most targeted by phishing activity in June. Organizations spoofed in phishing attacks: Banking, E-Commerce and information services.
(Symantec - Intelligence Report: June 2012)[142]
- The Public Sector remained the most targeted by phishing activity in July. Phishing attacks targeting small to medium-sized businesses (1-250) accounted for one in 363.8 emails, compared with one in 418.3 for large enterprises. Phishing attacks related to well-known social networking Web sites and social networking apps accounted for 15.9 percent of phishing attacks.
(Symantec - Intelligence Report: July 2012)[127]
- Many of the phishing pages contained in the phishing emails are no longer placed on a newly registered domain. The advantage of these domains is that phishers are able to choose a domain name that is similar to the phishing victim.
(IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- The average and median uptimes of phishing attacks dropped to a record low in 1H2012, by far the lowest since we began measuring in January 2008.
(Anti-Phishing Working Group - Global Phishing Survey: Trends and Domain Name Use in 1H2012)[143]

[141] http://www.symanteccloud.com/en/gb/mlireport/SYMCINT_2012_01_January_FINAL-en.pdf, *accessed 14 November 2012.*

[142] http://www.symanteccloud.com/en/gb/mlireport/SYMCINT_2012_06_June.pdf, *accessed 14 November 2012.*

[143] http://apwg.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf, *accessed 14 November 2012.*

- The number of phishing attacks rose.
  (Anti-Phishing Working Group - Global Phishing Survey: Trends and Domain Name Use in 1H2012)[143]
- Phishers registered more subdomains than regular domain names (page 16), while the number of domain names registered by phishers has dropped by almost half since early 2011.
  (Anti-Phishing Working Group - Global Phishing Survey: Trends and Domain Name Use in 1H2012)[143]
- The number of targeted institutions has dropped; phishers continue to target larger or more popular targets. Phishers concentrated on a smaller number of targets, perhaps because it was not economical to reach users of smaller institutions, or because user credentials at certain targets command a better price.
  (Anti-Phishing Working Group - Global Phishing Survey: Trends and Domain Name Use in 1H2012)[143]
- Phishers continue to shift toward the more economical options in their quest for profits. A wide variety of factors, from changes in top-level-domain registration and security policies to the availability of automated hacking tools, have tended to shift phishing toward compromised sites and vulnerable services. In the first half of 2012, we saw phishers continue to pursue these economically driven techniques, with more hacking of legitimate servers and especially shared web hosting environments (Rise of Shared Virtual Server Hacking).
  (Anti-Phishing Working Group - Global Phishing Survey: Trends and Domain Name Use in 1H2012)[143]
- Phishers continue to use "URL shortening" services to obfuscate phishing URLs.
  (Anti-Phishing Working Group - Global Phishing Survey: Trends and Domain Name Use in 1H2012)[143]
- One of the most widely used attacks was to forward website addresses via SMS messages on a smartphone. Phishing websites that fit the mobile web browser were also made.
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- Conventional phishing, on the other hand – luring unsuspecting users to fraudulent bank websites and asking them to enter their credentials, for example – is now relatively rare.
  (BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]

- Over half of incidents handled manually by CERT Polska represented phishing from Polish networks. We have recorded growth by one-third versus 2010. It should be emphasised that most of the cases affected foreign financial entities and did not pose any threat to Polish users.
  (CERT Polska - An Analysis of Network Security Incidents in 2011)[97]
- Some criminals use VoIP systems for more sophisticated "vishing" scams (telephone-based phishing), designed to collect sensitive information from users, such as Social Security numbers.
  (Cisco - 2011 Annual Security Report)[115]
- In February, the number of unique phishing sites recorded by APWG reached an all-time high of 56,859. This criminal activity is not decreasing.
  (Anti-Phishing Working Group - Phishing Activity Trends Report, 1st Quarter 2012)[104]
- The average number of infected PCs (that means compromised by some form of malware, not just – or even primarily – viruses, of course) has declined by three points since 2011. It's still a scary 35.51 percent, though.
  (Anti-Phishing Working Group - Phishing Activity Trends Report, 1st Quarter 2012)[104]
- While a generally defined phishing attack has a success rate of less than 0.001%, success rates exponentially increase as attackers are able to obtain more sensitive information about their target.
  (IT-ISAC - The Emerging Cyber Threat Landscape: 2012 and Beyond)[144]
- At the end of 2011, we began seeing the emergence of phishing-like emails that link to websites that do not necessarily perform a phishing attack. In 2012 this activity continued where parcel services were widely used to dupe users reaching more than 27% of the scam and phishing volume. Phishers also turned attention to non-profit organizations, accounting for 66% and then dropping to 7% in the first two quarters of 2012.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- The volume of spam and the volume of scam and phishing behave contrarily.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Social networks have been the dominant targets of email phishing for more than two years. (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Phishing sites continue to pose a significant risk to web surfers; more sites host phishing attempts than solely malicious downloads or spam.
  (McAfee - Threats Report: First Quarter 2012)[105]

[144] https://www.it-isac.org/files_n/GFIRST_WhitePaper.pdf, *accessed 14 November 2012.*

- Figures for both phishing sites and impression have been mostly stable throughout 1H12. Phishers sometimes engage in temporary campaigns that drive more traffic to each phishing page for a month or two, without necessarily increasing the total number of active phishing pages they maintain at the same time. Phishing messages, which accounted for between 3.1 and 3.9 percent of messages each month for most of 1H12, rose to 5.4 percent in June.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Most phishing sites only last a few days, and attackers create new ones to replace older ones as they are taken offline, so the list of known phishing sites is prone to constant change without significantly affecting overall volume. This phenomenon can cause significant fluctuations in the number of active phishing sites being tracked, like the one seen between April and June.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Typically, sites that target financial institutions account for most active phishing sites at any given time, often by a wide margin. In 1H12, a significant short-term campaign or campaigns that began in February resulted in sites that targeted social networks outnumbering sites that targeted financial institutions in March and April before returning to a more typical level in May.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Impressions for phishing sites that target social networks peaked in April, commensurate with the elevated numbers of active social networking phishing sites observed around the same time.
  (Microsoft - Security Intelligence Report Volume 13)[92]

Compromising confidential information

- Between January 2012 and June 2012, the number of events detected at healthcare organizations has almost doubled. As healthcare organizations move toward the adoption of electronic health record systems and digitally store and manage personally identifiable information (PII), these sensitive assets seem to be coming under increasing attack by cybercriminals.
  (FireEye - Advanced Threat Report 1H 2012)[145]
- Due to current geopolitical dynamics, data surrounding the sources of fossil fuel-based energy in particular are some of the most targeted assets (energy industries).
  (FireEye - Advanced Threat Report 1H 2012)[145]

[145] http://www2.fireeye.com/advanced-threat-report-1h2012.html, *accessed 14 November 2012.*

- The CTU research team does not expect breaches to lessen, but expects that both detection and remediation will improve due to increased awareness of the costs of lax security.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- Hackers are still responsible for the highest number of data breaches at 40%, but other methods resulted in a majority of breaches overall. In fact, roughly 1 out of every 5 breaches was caused by the accidental exposure of data. The same can be said for theft or loss of hardware. The average number of breaches per month was 16.5 in our 2011 data set, while in 2012 this number dropped to 14. The average number of identities stolen is down during the same period. It is possible data breaches today have simply become more targeted. While the numbers in 2012 are down compared to 2011 they do appear to be on an upward trajectory.
  (Symantec - Intelligence Report: August 2012)[146]
- In the last eight months of 2011 the average number of identities stolen was 1,311,629 per data breach. So far in 2012, this number is down to 640,169 identities per breach—that's a drop of more than half.
  (Symantec - Intelligence Report: August 2012)[146]
- H1 2012 was also rich in data breaches and data disclosure. Extremely popular web services such as Last.FM, LinkedIn and Yahoo Voice, as well as high-traffic forums (such as Phandroid's Android Forums) were compromised, had their user database stolen and shared online. In some instances, the database leaks were followed by phishing attempts sent to victims.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- The 'golden age' of cyber-crime continues, as organizations around the world continue to suffer data breach and identity theft attacks.
  (PandaLabs – Quarterly Report April - June 2012)[100]
- The cost of just one data breach can be staggering for an enterprise. Ponemon Institute estimates range anywhere from US$1 million to US$58 million. The cost is not just financial, either: Damage to corporate reputation and loss of customers and market share are potential side effects of a high-profile data loss incident.
  (Cisco - 2011 Annual Security Report, Ponemon Institute - 2011 Cost of Data Breach Study)[115, 119]
- Data Breach Investigation Report which analysed 855 security incidents that occurred 2011, exposing 174 million records: 63 percent could have been prevented with measures categorized as "simple and cheap." Another 31 percent could have been

[146] http://www.symanteccloud.com/en/gb/mlireport/SYMCINT_2012_08_August.pdf, *accessed 14 November 2012.*

prevented with measures deemed "intermediate." In other words, more than 9 out of 10 breaches would have been thwarted if organizations had followed best practices.
(Verizon - 2012 Data Breach Investigations Report)[147]

- Cyber criminals represent 83% of data breaches world-wide. 58% of data stolen world-wide was the result of hacktivist activity even though they were only responsible for 3% of the incidents.
(Verizon - 2012 Data Breach Investigations Report)[147]
- According to Verizon's 2012 Data Breach Investigative Report (DBIR), hacktivism surpassed organized crime in the amount of data of stolen.
(Verizon - 2012 Data Breach Investigations Report)[147]
- The 2011 Cost of Data Breach Study conducted by the Ponemon Institute and sponsored by Symantec reports that, for the first time in seven years, both the organizational cost of data breach and the cost per lost or stolen record have declined. The organizational cost has declined from $7.2 million to $5.5 million and the cost per record has declined from $214 to $194. We define a record as information that identifies an individual whose information has been compromised in a data breach.
(Ponemon Institute - 2011 Cost of Data Breach Study)[119]
- Web application vulnerabilities remain key to many data breaches, and data breaches continued to rise in the first half of 2011. So much so that X-Force declared 2011 to be the "Year of the Security Breach.
(IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- More customers remain loyal following the data breach. For the first time, fewer customers are abandoning companies that have a data breach. However, certain industries are more susceptible to customer churn, which causes their data breach costs to be higher than the average.
(Ponemon Institute - 2011 Cost of Data Breach Study)[119]
- Negligent insiders and malicious attacks are the main causes of data breach.
(Ponemon Institute - 2011 Cost of Data Breach Study)[119]
- 96% of all healthcare organizations surveyed had experienced at least one data breach in the past two years.
(Ponemon Institute - 2011 Cost of Data Breach Study)[119]
- We may not see the sheer numbers of attacks per month like we did in our 2011 data set, but that doesn't mean that the threat has passed. Rather, its possible data

[147] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, *accessed 14 November 2012.*

breaches today have simply become more targeted.
(Symantec - Intelligence Report: August 2012)[146]

- The majority of our analysis of data breach investigations revealed that the third party responsible for system support, development and/or maintenance introduced the security deficiencies exploited by attackers.
(Trustwave - 2012 Global Security Report)[121]
- How do data breaches occur? 81% utilized some form of hacking, 69% incorporated malware, 10% involved physical attacks, 7% employed social tactics, 5% resulted from privilege misuse.
(Verizon - 2012 Data Breach Investigations Report)[147]
- Commonalities between reported data breaches: 79% of victims were targets of opportunity, 96% of attacks were not highly difficult, 94% of all data compromised involved servers, 85% of breaches took weeks or more to discover, 92% of incidents were discovered by a third party, 97% of breaches were avoidable through simple or intermediate controls.
(Verizon - 2012 Data Breach Investigations Report)[147]

Rogueware/Scareware

- Despite the recent fall-off, fake antivirus is still a big problem, responsible for 5.5% of infections in the last six months of 2011.
(Sophos - Security Threat Report 2012) [86]
- Fake AV actually showed a small amount of growth but the overall trend is still down. This quarter we saw ransomware at its busiest eve.
(McAfee - Threats Report: Second Quarter 2012)[87]
- Fake antivirus (Win32/FakeAV) holds the 7th position of top threat families.
(Microsoft - Security Intelligence Report Volume 13)[92]
- No2 Top Web Threat for AVG for 1H 2012.
(AVG - AVG Community Powered Threat Report Q2 2012)[114]
- Fake antivirus and rogue security software are now well-known as users have begun to educate themselves and have stopped falling for the scam.
(AVG - AVG Community Powered Threat Report Q2 2012)[114]
- These products have seen little technical change in the past few years; what has been changing recently has been their distribution methods, as we now see rogueware being spread via Search Engine Optimization (SEO) poisoning, spam emails and drive-by downloads - routes that were once more associated with malware distribution than with rogueware.
(F-Secure - Threat Report H1 2012)[89]

- Rogueware deliberately imitates the graphical user interface and branding of established, legitimate antivirus or antispyware programs, in some cases even out rightly copying the actual logos or designs with only a few minor modifications.
  (F-Secure - Threat Report H1 2012)[89]
- The most typical scenario for a rogueware infection starts with the user being shown a fake system scan warning.
  (F-Secure - Threat Report H1 2012)[89]
- International law enforcement cooperation is having an effect on the fall of fake antivirus.
  (Sophos - Security Threat Report 2012) [86]
- Fake Mac antivirus schemes came to light during 2011, and scammers use techniques such as fake antivirus to infect Macs.
  (Sophos - Security Threat Report 2012) [86]
- In 2011, fake anti-virus software and fake video codecs continued to be the most popular vehicles for distributing malware.
  (Blue Coat - Blue Coat Systems 2012 Web Security Report)[131]
- One of the most prevalent malware threats over the last few months, the so called 'Police Virus'. Over this quarter, the Police Virus has continued to evolve, from scareware to ransomware.
  (PandaLabs – Quarterly Report April - June 2012)[100]
- An increase in 'ransonware' attacks has been detected over the past few months, effectively making this technique one of the most 'popular' attack methods ahead of fake antivirus software or rogueware.
  (PandaLabs – Quarterly Report January - March 2012)[99]

Spam

- Spammers find the effectiveness of social engineering lures differs depending on countries, cultures, religions, and other factors.
  (McAfee - Threats Report: Second Quarter 2012)[87]
- Drop of roughly 5 percent in volume. Regional spam was on the rise throughout the first half of 2012.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- The result of the Rustock shutdown was an immediate drop of about 30% in global spam volumes, which decreased even further in the summer of 2011.
  (Sophos - Security Threat Report 2012) [86]
- There have been a number of pressures on spammers throughout 2011 and as a result they are now using more targeted approaches and continue to exploit social media as

alternatives to email.
(Symantec - Intelligence Report: January 2012)[148]

- By relating their mails to widely-celebrated holidays and current events with global interest, spammers and malware authors can (at first glance at least) make their messages more interesting, and increase the chance of recipients visiting spam Web sites or becoming infected.
  (Symantec - Intelligence Report: January 2012)[148]
- Pharma Spam has fallen out of favour due to law enforcement activities and botnet shutdowns.
  (Cisco - 2011 Annual Security Report)[115]
- In the spring and summer of last year we observed the same spam levels as at the beginning of 2009. After a short increase in September 2011, the volume decreased to the spring 2011 levels. In the first half of 2012 there were no major changes, and the spam volume stabilized at this low level.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Spam Almost record lows.
  (McAfee - Threats Report: First Quarter 2012)[105]
- Spam levels are still on the decline.
  (McAfee - Threats Report: Second Quarter 2012)[87]
- The most common category of spam in February related to the Adult, Sex, and Dating category, overtaking pharmaceutical related spam for the first time.
  (Symantec - Intelligence Report: February 2012)[128]
- Blocked mail volumes in 1H12 were consistent with those of 2H11, and remain well below levels seen prior to the end of 2010.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- The most common category of spam in August is related to the Sex/Dating category. Pharmaceutical is the second one.
  (Symantec - Intelligence Report: August 2012)[146]
- Pharmacy spams hold a considerable part of spam.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- Dramatic Decline in Spam Volume. Cybercriminals' growing preference toward the use of low-volume, targeted attacks, such as spearphishing campaigns.
  (Cisco - 2011 Annual Security Report)[115]

[148] http://www.symanteccloud.com/en/gb/mlireport/SYMCINT_2012_01_January_FINAL-en.pdf, *accessed 14 November 2012.*

- The spam waves identified through 1H 2012 are highly targeted and often translated in the victim's native language.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- The volume of spam e-mail may have reduced, but it is becoming increasingly targeted, so the risk potential remains just as high.
  (BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]
- Mobile operators are increasingly used for spamming. Almost every fifth report is related to mobile networks. It seems that mobile operators will have to tackle the issue of spam from their networks in the immediate future.
  (CERT Polska - An Analysis of Network Security Incidents in 2011)[97]
- Email spam activity was significantly lower in 2011 and continuing into 2012. CTU analysts concur that the focus on malware activity is gradually migrating to the mobile domain and social networks to reap dividends on poorly protected sites and devices.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- Economies of scale drove the very logical evolution from the single-purpose botnet, perhaps deployed for either spamming or denial of service attacks, to the multi-purpose botnet, the modular design of which allowed different tasks to be pushed to the same collection of compromised machines without having to repeat the infection process.
  (ESET - Global Threat Report August 2012)[112]
- Old methods of attack such as traditional phishing and spam are being replaced with new methods of deploying malware. Social media attacks are increasing and a prime target area for attackers who are successfully encroaching on their target's circle of trust by infiltrating their friends and followers.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Spam volumes continued to decline into the end of the year where a shift to spam delivering malware with zip attachments became a method of choice.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Spam continues to decline in the past months and even years due to several botnet take downs.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Plain text spam continues trending upward into 2012.
  (IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- We continue to see spam leveraging classic topics like replica watches, medical products, and software. This appears to be a well proven approach to earning

illegitimate money.
(IBM - IBM X-Force 2011 Trend and Risk Report)[98]

- Spam that takes advantage of topical news or other hot topics by promising more details when you click the link—and then infects the user's machine money.
(IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Masses of spam containing no text and only one link.
(IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Increase in speed. Spammers quickly adjust their approaches to try to stay ahead of every best effort to block it.
(IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Spam continued its decline in the first six months of 2012, reaching an all-time low of around 70% of total amount of spam sent worldwide.
(Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- Today, we are seeing very large-sized messages, with the bulk of the size coming from large sections of irrelevant Cascading Style Sheets (CSS). A current theory is the extra data is being used as a way of evading detection as it does not seem to affect the message data or formatting.
(IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Spammers continued to use image spam.
(IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- By mid-June of 2012, the size of spams exceeded 10 kilobytes. Spammers added legitimate content from randomly chosen websites to its spams, in order to confuse and pass spam filters.
(IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- On July 18th, 2012, we witnessed the take down of the Grum botnet. This resulted in an annual low of spam volume.
(IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- From 2010 to 2012, the spam volume decreased to about one third of the 2010 levels.
(IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- The shift to blended threats using email as a lure and web links remains strong as 92% of email spam contains a URL.
(Websense - Threat Report 2012)[93]
- The risk is diminishing as recipient e-mail infrastructures become overloaded. But the content of criminal spam is becoming ever more convincing. This increases the risks to the recipient, which include fake medication, compulsive gambling, (unintentional) participation in criminal activities, disclosing sensitive data, or malware. This trend is set to continue going forward.

(BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]

- The Education sector was the most spammed industry sector in July. Then Automotive, Public sector and Pharmaceutical sector. The spam rate for small to medium-sized businesses equal to large enterprises. The most common category of spam in July is related to the Newsletters category, with 62.20 percent. This is a significant shift from June, when it made up only 0.08 percent of all spam.
  (Symantec - Intelligence Report: July 2012)[127]

Targeted Attacks

- Spear phishing emails may use malicious URLs, malicious attachments, or both to exploit OS and application vulnerabilities.
  (FireEye - Advanced Threat Report 1H 2012)[145]
- Targeted phishing and the use of malicious document attachments continue to be the favoured tradecraft in APT operations because they are successful.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- APT attacks against internal systems were mostly made by using files with vulnerabilities attached to emails.
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- Low-volume, targeted attacks, such as spearphishing campaigns are heightening the potential for data to be stolen or compromised.
  (Cisco - 2011 Annual Security Report)[115]
- Increased prevalence of limited-use domains in spear phishing attacks, increased dynamism of email attachments.
  (FireEye - Advanced Threat Report 1H 2012)[145]
- With spearphishing, the average theft per victim can be 40 times that of a mass attack, according to Cisco.
  (Sophos - Security Threat Report 2012, Cisco - 2011 Annual Security Report) [86,115]
- In APTs, attackers take advantage of vulnerabilities in the digital documents written in MS Word, Adobe Reader or Hangul to corrupt the system.
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- The most common infection vector for network intrusion was spear-phishing emails with malicious links or attachments. Spear-phishing accounted for 7 out of 17

incidents.
(ICS-CERT - Incident Response Summary Report 2009–2011)[149]

- Growth of targeted attacks during 1H2012. More than 36% of all targeted attacks are aimed at small companies, compared to 18% at the end of 2011. This shift could be based on a perception that smaller business may be an easier point of entry.
(Symantec - Intelligence Report: June 2012)[142]
- Compared to 2008, these numbers declined until mid-2011. On the other hand, there are many reports about an increase of phishing. This is not a conflict because this represents the number of attacks. There might be many more attacks but each attack consists of fewer emails. In the case of spear phishing, (see sidebar) there might be only a single email.
(IBM - IBM X-Force 2011 Trend and Risk Report)[98]
- Spear Phishing and Social Engineering on the Rise.
(IBM - IBM X-Force 2012 Cyber Security Threat Landscape)[108]
- Patient and committed attackers perform extensive reconnaissance of spear-phishing targets and then contact them with highly believable communications (email, IM, or social networking message) which may reflect knowledge of the individuals' work activities, colleagues, friends, and family. The phishing message can include a link or attachment leading to infection of the target's system, often with custom malware.
(IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Multiple spear-phishing incidents were also reported. Reports came from several sectors, but the Energy Sector accounted for two-thirds of these incidents. All the spear-phishing incidents reported to ICS-CERT involved sophisticated or advanced persistent threat actors.
(ICS-CERT - Incident Response Summary Report 2009–2011)[149]
- Sophisticated threat actors were present in 11 of the 17 incidents, including the actors utilizing spear-phishing tactics to compromise networks. These threat actors were responsible for data exfiltration in several cases, which seems to have been the primary motive for intrusion.
(ICS-CERT - Incident Response Summary Report 2009–2011)[149]
- These *stealthy* attacks (targeted attacks/spearphishing) need time (sometimes years) to be discovered; they are particularly insidious and hard to avoid. No organisation can be safe from them.

[149] https://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf, *accessed 14 November 2012.*

(CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]

- Despite global levels dropping, spearphishing and spam are as dangerous as ever; consumers and businesses must remain vigilant. The sophistication of today's threats remains high (McAfee - Threats Report: First Quarter 2012)[105]
- Don't be fooled: Spam is still dangerous and targeted spearphishing attacks are even more so.
  (McAfee - Threats Report: Second Quarter 2012)[87]
- Spearphishing attacks are also on the rise. Over the past year, SophosLabs has noticed an increase in the number of targeted attacks attempting to phish users for credentials, as well as to push malware.
  (Sophos - Security Threat Report 2012) [86]
- Most of the APT (Advanced Persistent Threat) launched recently attempted to insert a backdoor into the corporate network via email, instant messaging or SNS.
  (ASEC Report Vol.24)[106]
- An outstanding trend in the security threats reported during the first half of 2012 is the increase of APT attacks designed to steal internal information. Such APT attacks against internal systems were mostly made by using files with vulnerabilities attached to emails. Such emails regularly contain a social issue or an interesting topic in the message, attracting the user to open the attachment. Attackers take advantage of vulnerabilities in the digital documents written in MS Word, Adobe Reader or Hangul to corrupt the system.
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- While a generally defined phishing attack has a success rate of less than 0.001%, success rates exponentially increase as attackers are able to obtain more sensitive information about their target.
  (IT-ISAC - The Emerging Cyber Threat Landscape: 2012 and Beyond)[144]
- Information gathering and espionage in Middle East countries. The Flame computer virus has been the highlight of the quarter without any doubts. Flame is a complex piece of malware used for information gathering and espionage in Middle East countries. This malicious code is most likely created by a government or intelligence agency, and is clearly tied to the infamous Stuxnet malware. One of the most striking features of Flame is that it can steal all kinds of data in multiple ways, even by turning on victims' microphones to record conversations.
  (PandaLabs – Quarterly Report April - June 2012)[100]
- Explosion in advanced malware bypassing traditional signature-based defences.
  (FireEye - Advanced Threat Report 1H 2012)[145]

- Flame malware.
  (F-Secure - Threat Report H1 2012)[89]
- SCADA discovery with SHODAN.
  (Dell SecureWorks - Threatscape Update for 1Q2012)[91]
- An outstanding trend in the security threats reported during the first half of 2012 is the increase of APT attacks designed to steal internal information.
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- Elderwood Project most targeted attacks is its heavy reliance on zero-day vulnerabilities.
  (Symantec - Intelligence Report: August 2012)[146]
- Elderwood has used eight zero-day vulnerabilities over the last three years. The attackers also make use of an exploitation technique called a "watering hole attack".
  (Symantec - Intelligence Report: August 2012)[146]
- Flamer case: Flamer has appeared in the Middle East, in particular in Iran, just as Stuxnet and Duqu did. It also appears to be politically motivated, as were Stuxnet and Duqu. However, while Stuxnet and Duqu shared similar code bases, at this point we have yet to find an overlap with Flamer. It seems as though Flamer could have been written by an entirely different team of programmers.
  (Symantec - Intelligence Report: May 2012)[135]
- Anti-virus detected less than 12% of the targeted malware samples collected during 2011 investigations. While anti-virus products detected at least 60% of all malware samples in our database, when we focused only on samples found during our compromise investigations, anti-virus detected less than 12% as malicious.
  (Trustwave - 2012 Global Security Report)[121]
- Common VS Targeted Malware. Common, mass-distributed malware usually seeks to self-replicate through security vulnerabilities. Targeted malware doesn't self-replicate and may not exploit common vulnerabilities.
  (Trustwave - 2012 Global Security Report)[121]
- Targeted malware is becoming more advanced; approximately 13% of our database samples used inside knowledge or an in-depth understanding of how the target business application worked to directly hook into the target applications.
  (Trustwave - 2012 Global Security Report)[121]
- Data exfiltration is on the rise, and so are Advanced Persistent Threats. A new threat called Duqu that appears to have evolved from the Stuxnet worm was discovered this year.
  (ASEC Report Vol.24)[106]

- Born in 2010, Stuxnet immediately appeared as something new and disruptive. For the first time, newspapers1 and TV news talked about this APT (Advanced Persistent Threat), a malware "specially designed and developed" by targeting a certain type, a certain brand and a certain model of the control system.
  (CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]
- Duqu is back.
  (Kaspersky Lab - IT Threat Evolution: Q1 2012)[94]
- Flamer. Growth of targeted attacks during 1H2012.
  (Symantec - Intelligence Report: June 2012)[142]
- Flame and Stuxnet: the end of antivirus? The level of sophistication within Stuxnet was nonetheless impressively high. Flame as code, on the other hand, is not very special. Flame or Stuxnet; however, it is increasingly becoming clear that the intended victims for both types of attack are not the average consumer.
  (AVG - AVG Community Powered Threat Report Q2 2012)[114]
- The first half of this year brought new surprises in terms of cyber-warfare with the discovery of Flamer - one of the most potent and complex e-threats to date. Designed to run stealthily and collect data through an astounding range of approaches, Flamer managed to evade AV detection for some five years.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- F-Secure Labs estimates that it took more than 10 man years of work to develop Stuxnet. Related attacks like Duqu and Flame might have taken even more.
  (F-Secure - Threat Report H1 2012)[89]
- In May 2012, the complex Flame malware code caused a stir and, after Stuxnet and Duqu, attracted a lot of attention in targeted cyber-spy malware circles.
  (G Data - Malware Half-yearly report January – June 2012)[133]
- Flame - the spyware saga continues: The biggest recent spyware event was the detection of the Flame worm. The main topic in the news in Q2 2012 was the detection of the Flame cyber-espionage program.
  (Kaspersky Lab - IT Threat Evolution: Q1 2012)[94]
- The malware, called "Flame", was active especially in the Middle East. Nearly half of the proven infections were in Iran. Flame was spread via USB sticks and local networks. For the infection via USB sticks, the same vulnerability was used as for Stuxnet.
  (MELANI - Semi-annual report 2012/I, January – June)[118]
- State-motivated cyber weapons were first brought into broader debate through the programs Stuxnet and Duqu. The malware code "Flame", discovered in the first half of

2012 is now considered on the same level as Stuxnet and Duqu.
(T-Mobile - Security on the Internet-Report on information and Internet security)[122]

Physical Theft/Loss/Damage

- Data loss from lost, stolen or decommissioned devices No1 Top Mobile Threat.
  (Cloud Security Alliance - Top Threats to Mobile Computing)[150]
- 10% of respondents said they had experienced critical information leaks due to the loss or theft of a mobile device.
  (Kaspersky Lab- Global IT Security Risks: 2012)[151]
- 5th in top 10 of external threats Kaspersky.
  (Kaspersky Lab- Global IT Security Risks: 2012)[151]
- 3rd in top 10 internal threats Kaspersky.
  (Kaspersky Lab- Global IT Security Risks: 2012)[151]
- Theft of hardware: 7th in top 10 external threats Kaspersky, 4th in top 10 internal threats Kaspersky.
  (Kaspersky Lab- Global IT Security Risks: 2012)[151]
- Increasing trend of device theft by an external.
  (Kaspersky Lab- Global IT Security Risks: 2012)[151]
- No2 Top cause of data breach.
  (Symantec - Intelligence Report: August 2012)[146]
- 10% of Data breaches involved physical attacks.
  (Verizon - 2012 Data Breach Investigations Report)[147]
- Corporations will have to deal with the security risks posed by the Bring-Your-Own-Device (BYOD) trend gaining increased popularity with managers all around the world. However, since many times these devices storing sensitive corporate data are not managed by IT personnel, the probability of data loss due device theft or loss is increasing.
  (Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- Corporations having experienced a data breach reported that one of top 3 causes is physical theft of devices containing sensitive data.
  (Ponemon Institute - 2011 Cost of Data Breach Study)[119]
- Influences of initial bring your own device (BYOD) in most enterprises.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]

---

[150] https://downloads.cloudsecurityalliance.org/initiatives/mobile/top_threats_mobile_CSA.pdf, *accessed 14 November 2012.*

[151] http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf, *accessed 14 November 2012.*

- One option an enterprise may require in their BYOD policy is data encryption.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]

Identity theft

- Zeus Banking Trojan Becomes an Open-Source Crime Kit.
  (Verisign - 2012 iDefense Cyber Threats and Trends)[126]
- Banking Trojan is the top Attack Method for finance services.
  (Trustwave - 2012 Global Security Report)[121]
- Identity theft and identity fraud have become established as a criminal field operated with highly professional structures. The increasing use of powerful Trojan horses has meant that the number of cases – and therefore the levels of losses – are once again on the rise compared with previous years.
  (BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]
- Zeus and Spyeye, two families of banking trojans that specialize in stealing online banking credentials.
  (F-Secure - Threat Report H1 2012)[89]
- Seldom do we see a new banking trojan with the size and complexity of Win32/SpyEye appearing. This happened last year with the discovery of Win32/Gataka: a banking trojan that is able to inject content in HTML pages and which exhibits a modular architecture that is easily extensible with plug-ins. Once installed on a computer, Win32/Gataka can be used by botnet operators to steal personal information.
  (ESET - Global Threat Report September 2012)[152]
- Mobile banking targeted for attack. Zitmo: a "Man-in-the-Mobile" Attack.
  (AVG - AVG Community Powered Threat Report Q3 2012)[153]
- In recent years, these Trojans (Spyeye & Zeus) have metamorphosed into 'malware frameworks', with modular components that can be added on for customized functionality.
  (F-Secure - Threat Report H1 2012)[89]
- Android.Hacktool.Faceniff.A - Mostly used to intercept Wi-Fi traffic, this Android tool enables attackers to spot users and passwords for popular services such as Twitter, Facebook or other social networking platforms. This hack tool can be particularly useful to those who practice identity theft through social networking websites. The

[152] http://go.eset.com/us/resources/threat-trends/Global_Threat_Trends_September_2012.pdf, *accessed 14 November 2012.*

[153] http://www.avg.com.au/files/media/avg_threat_report_2012-q3.pdf, *accessed 14 November 2012.*

3.46% infection rate places the malware fifth in our ranking system.
(Bitdefender - H1 2012 E-Threat Landscape Report)[95]

- Android.Hacktool.DroidSheep.A - Tenth in our globally-recorded infections chart, this hack tool is mostly used to hijack personal accounts by spoofing public Wi-Fi networks and collecting usernames and passwords from those connected. With a 1.76% infection rate, it proves that identity theft and account hijacking is still prevalent on Android-running devices.
(Bitdefender - H1 2012 E-Threat Landscape Report)[95]
- "Conventional" phishing is much less common these days. But that does not mean that identity theft no longer poses a threat: in fact, quite the opposite. A criminal field of activity has developed in this area which has all the hallmarks of highly professionalized structures.
(BSI-Federal Office for Information Security - The IT Security Situation in Germany in 2011)[88]
- Personal data theft, and identity theft in general, is now the most important crime on the net for its numbers and for the sign it gives if compared to the other information crimes. An identity theft is defined as any time personal data useful to commit more crimes is gathered in an illegal manner. The data collection itself entails crimes such as unauthorised access to information systems, information fraud, spread of programs aiming at damaging or interrupting an information system.
(CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]
- The appeal of digital data as a replacement of coins and banknotes is a fact that can be confirmed by the statistics of the activity to fight cybercrime, which is moving towards the deceitful exploitation of home banking. The size of the phenomenon and the international nature of online banking criminality display a systemic dimension of the attacks and, considering the importance of online transactions, it can slow the economic development of a country or even undermine it.
(CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]
- Identities are often stolen through social engineering, which are techniques used to manipulate people until they give confidential information. Phishing is one of these techniques of obtaining personal information that automatizes these processes.
(CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]
- Identity theft and identity substitution have high frequency and high level of risk in social networks.

(CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]

- WiFi Hacking - Attackers can steal passwords, leading to financial consequences and, in many cases, identity theft.
  (Juniper Networks - 2011 Mobile Threats Report)[154]
- Big Data and Privacy - As these online communities, such as Facebook, MySpace, Orkut, Twitter, LinkedIn, and others, have been adopted by Internet users, miscreants have started abusing them for a variety of purposes, including stalking, identity theft, spamming, direct advertising, spreading of malware, etc.
  (SysSec - Second Report on Threats on the Future Internet and Research Roadmap)[155]
- Consistent Reports of Malware to Steal Personal Information. The first half of 2012 saw the emergence of malicious codes designed to steal personal financial information used for online banking. By redirecting users to fraudulent phishing websites of financial institutions, such malwares tried to steal banking information such as passwords for security cards and public certificates.
  (ASEC - AhnLab Monthly Security Report – Vol.30)[101]
- Your social media identity may prove more valuable to cybercriminals than your credit cards. Harvesting social networking credentials opens the door for cybercrime to leverage a trusted relationship to introduce lures.
  (Websense - Threat Report 2012)[93]
- Typically, sites that target financial institutions account for most active phishing sites at any given time, often by a wide margin.
  (Microsoft - Security Intelligence Report Volume 13)[92]
- With the Zeus source code freely available and nearly complete, it is a safe bet that many more variants will appear. As 2011 has demonstrated, with the de facto banking Trojan's source code in an open-source format, many new malicious actors will capitalize on such a robust system to elicit financial gains (either through the use of the modified Trojans or the sale of the modified Trojans)
  (Verisign - 2012 iDefense Cyber Threats and Trends)[126]
- As Ramnit and Spyeye demonstrate, there will be more minor Trojans that include the functionality of Zeus into their arsenals. This trend will be even more pronounced when new malware families emerge that not only augment themselves with

[154] https://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf, *accessed 14 November 2012.*

[155] http://www.syssec-project.eu/media/page-media/3/syssec-d4.2-future-threats-roadmap-2012.pdf, *accessed 14 November 2012.*

components of Zeus but also augment Zeus with new functionality specific to each new variant family. The release of the Zeus source code is going to have a dramatic impact on the production of new, dangerous banking Trojans in 2012.
(Verisign - 2012 iDefense Cyber Threats and Trends)[126]

- Financial Services continued to be the most targeted industry sector in the second quarter of 2012. Similar to last quarter, during this three month period, Payment Services remained the second highest industry sector for targeted attacks.
(Anti-Phishing Working Group - Phishing Activity Trends Report, 2nd Quarter 2012)[156]
- Unlike most generic key loggers, phishing based key loggers have tracking components, which attempt to monitor specific actions (and specific organizations, such as financial institutions, retailers, and e-commerce merchants) in order to target specific information. The most common types of information are access to financial-based websites, ecommerce sites, and web-based mail sites.
(Anti-Phishing Working Group - Phishing Activity Trends Report, 2nd Quarter 2012)[156]
- In 2011, the Juniper MTC found that spyware was the dominant type of malware affecting Android, accounting for 63 percent of the samples identified.
(Juniper Networks - 2011 Mobile Threats Report)[154]
- ZeuS Trojan (aka ZeuS-in-the-Mobile, or ZitMo) with which criminals obtained user credentials to initiate online banking sessions, giving the attacker access to the victim's financial accounts.
(Juniper Networks - 2011 Mobile Threats Report)[154]
- Identity theft, and consequently credit card theft, has major financial and reputation consequences for both the individual whose identity is stolen and the company from which the data was obtained. Organizations need to be vigilant about the way they handle, use and safeguard personal information to minimize their risks.
(Sophos - Security Threat Report 2012) [86]
- The cybercrime ecosystem will get more articulated, becoming a parallel economy where various players exchange services (until proper forms of "crime as a service" emerge) and learn by trading exploits, malware, access to compromised systems, personal and financial data and so on in a global illegal market, with international organised crime managers running the show, not black hat hackers anymore.
(CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]

[156] http://www.antiphishing.org/reports/apwg_trends_report_q2_2012.pdf, *accessed 14 November 2012.*

- Financial institutions and systems are readily accessible worldwide. Today's financial fraud and cybercriminals have adapted to this new means of global trade and seek to exploit this dependence on information technology. Cybercriminals consequently have become experts at stealing stored data, data in transit, and encrypted data. They operate based on trust, long standing criminal relationships, high levels of operational security, and reliability. The culture also has evolved over the last decade and is now described as non-state sponsored, transnational, and is almost impossible to infiltrate due to its dynamic nature and operational security.
  (Verizon - 2012 Data Breach Investigations Report)[147]
- The activities of the spyware group include the recording of keystrokes, searching the system for passwords, access data for games, email portals and financial services providers as well as the manipulation of financial transactions. In the first half of 2012, its share has grown once again, and is now 17.4%.
  (G Data - Malware Half-yearly report January – June 2012)[133]
- The majority of computer crime is broadly targeted, financially motivated malware activity. Various bot networks based on Zeus were responsible for millions of dollars in losses over the last few years.
  (IBM - IBM X-Force 2012 Cyber Security Threat Landscape)[108]
- Several engagements in 2011 found that criminals explicitly targeted business financial account numbers (e.g., account routing codes, merchant identification numbers) to perpetrate payment card fraud.
  (Trustwave - 2012 Global Security Report)[121]
- Nowadays, our phones hold a treasure of sensitive information: phone numbers of our family, friends and colleagues, personal photos, financial data, passwords, virtual cash, location information, etc. In some respect, our phones may be a more valuable target to attackers than our personal computers or servers.
  (SysSec - Second Report on Threats on the Future Internet and Research Roadmap)[155]
- The increasing use of mobile devices for online banking and other financial transactions that makes users high-value targets for cybercriminals.
  (Blue Coat - Blue Coat Systems 2012 Web Security Report)[131]
- Some banking Trojans exhibit new attack schemes but Sinowal is still top-ranked. The number of banking Trojans in the spyware category has risen by almost 14%. Online banking has established itself as a market in the underground economy. Spyware thus takes second place, after the group of Trojan horses, which covers many different malware functions.
  (G Data - Malware Half-yearly report January – June 2012)[133]

- The infection numbers of Sinowal were at the usual high levels. In the second quarter, however, Bankpatch managed to climb to the top of banking Trojans for the first time. This was made possible by unusually high levels of activity in the implementation of new mechanisms for deactivating anti-virus products.
  (G Data - Malware Half-yearly report January – June 2012)[133]
- What was also remarkable in the first half of 2012 was the professionalization of the attack schemes themselves. For example, a new SpyEye variant was identified, which activates the victim's web cam and uses the video stream for its purposes.
  (G Data - Malware Half-yearly report January – June 2012)[133]
- Criminals who run malware operations continued to evolve and better serve their customers. Zeus, a popular banking Trojan horse, became stealthier with its "Gameover" version, which includes peer-to-peer command and control (C2) communications. The Zeus "Citadel" version introduced a customer ticketing system for better service. Malware authors also introduced "crimevertising," where the criminals sell ads that display in the malware platform.
  (G Data - Malware Half-yearly report January – June 2012)[133]
- Mobile Integration of Banking Trojans - 2011 saw an increase in mobile versions of the largely PC-based banking Trojan malware market. The release of Zeus source code, and its eventual merge with SpyEye malware, included Android and iPhone components used to capture Mobile Transaction Authentication Numbers (mTAN) and mobile onetime passwords.
  (Trustwave - 2012 Global Security Report)[121]
- ZeuS is a popular banking trojan. ZITMO, or "Zeus In The MObile", is a new threat. This is a new variant of Zeus, targeting smartphones as well as PCs.
  (CERT Polska - An Analysis of Network Security Incidents in 2011)[97]

Abuse of information leakage

- Mobile privacy is a growing issue. Based on Lookout's analysis, more than 5% of free applications on Google Play contain ad networks that have aggressive practices.
  (Lookout - State of Mobile Security 2012)[157]
- Data Leakage through poorly written 3rd party apps - No3 Top Mobile Threat.
  (Cloud Security Alliance - Top Threats to Mobile Computing)[150]
- In the second place on the WhiteHat Top Ten, Information Leakage, identified in 53% of websites.
  (WhiteHat SECURITY - Statistics Report 2012)[123]

[157] https://www.lookout.com/_downloads/lookout-state-of-mobile-security-2012.pdf, *accessed 14 November 2012.*

- Basic security mistakes such as information leakage and insecure communications are still being made at all organization size levels.
  (HP - 2011 top cyber security risks report)[116]
- Mobile applications are different, but the same, In addition to the broader information leakage problems presented by changing use cases and platforms, mobile applications are designed to leak data.
  (HP - 2011 top cyber security risks report)[116]
- Given the realities of the modern IT landscape, the information leakage problem is especially widespread and pernicious.
  (HP - 2011 top cyber security risks report)[116]
- Leaks from the cloud. Researchers discovered at least three different ways to hack into Dropbox and access data without authorization.
  (Sophos - Security Threat Report 2012) [86]
- Cloud-based file sharing services are heightening the potential for data to be stolen or compromised. Cloud Infrastructure Hacking.
  (Cisco - 2011 Annual Security Report)[115]
- Aggressive ad behaviour includes pushing out-of-app ads, changing browser and desktop settings and accessing personally identifiable information without suitable notification or transparency to the user.
  (Lookout - State of Mobile Security 2012)[157]
- The two main platforms Android and Apple iPhone/iPad, have been in the eye of the storm more than once for tracking user data and for the possible geo-location that modern devices offer thanks to 3G, Wi-Fi and GPS technologies.
  (CLUSIT - Italian Information Security Association 2012 Report on ICT Security in Italy)[109]

Search Engine Poisoning

- Poisoned Google Image Searches: Google image searches show new trends in black hat search engine optimization (SEO) campaigns.
  (Websense - Threat Report 2012)[93]
- Blue Coat argues that search engine poisoning constitutes ca. 40% of malware deployment.
  (Blue Coat - Blue Coat Systems 2012 Web Security Report)[131]
- Search engine, web catalogue, and portal site malware decreased to 5.1%.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Year over year there was a significant drop in Blackhat SEO poisoning leading to malware, thus resulting in safer search results. This reduction comes at the expense of

strong evidence of cybercrime activities increasing within social networking, Twitter, and blogging.
(Websense - Threat Report 2012)[93]

- Any major global event, whether it is an election or a catastrophe, will lead to Search Engine Optimizations (SEOs) created by many different people for a variety of goals, both genuine and malicious.
  (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)[96]
- Malnet operators make constant adjustments to the bait content they feed to search engines but don't necessarily focus on big news events.
  (Blue Coat - Blue Coat Systems 2012 Web Security Report)[131]
- With Search Engines/Portals representing the most requested category of content, it is not surprising that this category is also the leading entry point into malnets.
  (Blue Coat - Blue Coat Systems 2012 Web Security Report)[131]
- After social networks, search engines are the primary means used by the attackers to lure users to malicious sites.
  (ESET - Global Threat Report February 2012)[158]
- Beyond Vanilla Search-Engine Poisoning. If you compromise a user's search history and hence his online profile, the victim gets the malicious search results no matter where he logs in from.
  (Georgia Institute of Technology – Emerging Cyber Threats Report 2013)[159]

Rogue certificates

- SSL Gets Hit in the Crossfire (Attacks against PKI, theft of issued certificates, DoS).
  (Imperva - Security Trends 2012)[140]
- Combination attacks affecting DNS service providers and certificate authorities are especially dangerous.
  (Georgia Tech Cyber Security Summit 2011 - Emerging Cyber Threats Report 2012)[130]
- Additional security standards are needed for companies issuing digital certificates to secure the internet trust model against possible future attacks.
  (Symantec Security Threat Report Vol.17)[160]
- Attackers sign malware in an attempt to trick users and admins into trusting the file, but also in an effort to evade detection by security software and circumvent system

---

[158] http://go.eset.com/us/resources/threat-trends/Global_Threat_Trends_February_2012.pdf, accessed 14 November 2012.

[159] http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf, accessed 21 November 2012.

[160] https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf, accessed 14 November 2012.

policies. Much of this malware is signed with stolen certificates, while other binaries are self-signed or "test signed." Test signing is sometimes used as part of a social engineering attack.
(McAfee - Threats Report: Second Quarter 2012)[87]

- Stuxnet – stealing two certificates to sabotage a nuclear plant.
(Attacks on CAs: at risk the trust on the Internet)[161]
- Comodo – compromising a registration authority in order to try and read someone else's mails.
(Attacks on CAs: at risk the trust on the Internet)[161]
- Diginotar - Surgically hitting a CA and bringing down to its knees an entire country in order to intercept the e-mails of three hundred thousand citizens.
(Attacks on CAs: at risk the trust on the Internet)[161]
- Flame - How to fulfil the wildest dream of every malware: automatically install itself via Windows Update service.
(Attacks on CAs: at risk the trust on the Internet)[161]
- CAs should adhere to best practices since they play such a critical role in today's digital society. The attacks against CAs highlight the importance of enforcing basic security best practices.
(Operation Black Tulip: Certificate authorities lose authority)[162]

[161] http://w3.uniroma1.it/mastersicurezza/images/materiali/convegni/18_06_2012/giustozzi.pdf, *accessed 14 November 2012.*

[162] http://www.enisa.europa.eu/media/news-items/operation-black-tulip, *accessed 14 November 2012.*

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu