INSPECTING CURRENT CYBERSECURITY STATUS AND NEW TRENDS IN HUNGARY

Kálmán Hadarics[1]

DOI: 10.24989/ocg.v335.11

Abstract
In the 21st century online services became standard way to handle our affairs every day. The digital revolution and usage of smart devices made possible the existence of new type of cybersecurity threats. The malware distribution and their impact are constantly changing. The primary goal of cybersecurity attacks is catching sensitive data and business benefit. Instead of hobby hacking well organized cybercrime groups carry out the most offense. Computer Security Incident Response Teams (CSIRTs) must handle security incidents for e-Government information systems appropriately. This is extremely important if we want to mitigate the impact of a cybersecurity threat.

In this paper, I will examine the available statistical data and reports of Government Incident Response Team of Hungary. Analyzing this information will point out what are the new trends of threats and malware. This paper also presents the findings gained from processed data.

Keywords: *malware, threat, cybersecurity, incident*

1. Introduction

In the 21st century digital online services are available in almost every field of life. The proper operation of digital services can make our lives much easier and their use is self-evident. Our personal and other specific data are accessible from different devices like computers, tablets, smartphones, and IoT devices or through different cloud services. However if our data are available online they are exposed to theft, destruction or unwanted manipulation. The problem was identified several years ago in European Union level, and Regulation (EU) No 526/2013 of European parliament defined the tasks of European Union Agency for Network and Information Security (ENISA).

"The threat landscape is continuously changing and security incidents can undermine the trust that users have in technology, networks and services, thereby affecting their ability to exploit the full potential of the internal market and widespread use of information and communication technologies (ICT)." [1]

This regulation also defines some important generic findings: "Network and information security problems are global issues. There is a need for closer international cooperation to improve security standards, including the definition of common norms of behaviour and codes of conduct, and information sharing, promoting swifter international collaboration in response to, as well as a global approach to, network and information security issues." [1]

[1] University of Dunaújváros, H-2400 Dunaújváros, Táncsics M. u. 1/A., hadarics@uniduna.hu

The ENISA should provide also operational cooperation with EU Member States CSIRTs (Computer Security Incident Response Teams). According to the EU cybersecurity aims:

“At the same time, today’s ICT systems can be seriously affected by security incidents, such as technical failures and viruses. These kinds of incidents, often called network and information systems (NIS) incidents, are becoming more frequent and difficult to deal with.

Moreover, cyber-attack are estimated to cost the global economy €400 billion every year.

Many businesses and government across the EU rely on digital networks and infrastructure to provide their essential services. This means that when NIS incidents occur, they can have a huge impact by compromising services and stopping businesses from working properly.” [2]

2. Background and research input

ENISA publish annual reports as Threat Landscapes. From year 2012 these reports are available and contains information about threat agents and attack vectors. These threat landscapes are provide information about:

- Top threats (current threat landscape)
- Threat agents and
- Threat trends.

The main purpose of these reports are to identify a cyber-security threat landscape based on aggregated data collected from various ENISA stakeholders and also from global perspective from international sources.

In ENISA Threat Landscapes the used data source can be grouped in the following categories;

- Reports from Virus/Malware protection vendors, that covers operating specific data;
- Reports from CERTS, that covers incidents data;
- Reports from security agencies, that incidents, attacks and threat agents with a geographical focus;
- Reports from commercial security companies, that focus on particular areas of threats;
- Reports from industrial associations and committees, that focus on threats that is related to members infrastructure;
- Reports from Network of Excellence, that provide to predict future threats based on upcoming application areas, assets and types of infrastructure.

3. Analyzing of the threat landscape reports

ENISA Threat Landscape reports [3] and related web application [4] contains information about cyber threats. Currently 49 different threat type are identified. If we want to classify them into group, at least three different group can be created:

- Generic (common) threats;
- Hardware (HDW) related threats;
- 5G/Virtualization/SDN (Software Defined Network) related threats;

Generic threats

Malware: Malware is malicious code that can be installed in a device and cause harm to components (hardware, software, data) if this device.

Web-based attacks: Web based attacks are those that use web components as an attack surface.

Web application attacks: Web application attacks are related to attacks against available web applications and web services.

Denial of Service: A cyber-attack that aims to exhaust system or network resources to render them unavailable to its users.

Botnets: A network of infected machines typically from all over the world used for malicious activities.

Phishing: An attack that aims to lure users to malicious sites in order to covertly steal usernames, passwords and financial credentials.

Spam: Spam or unsolicited e-mail is the main means for the transport of malware and malicious URLs.

Ransomware: Ransomware is a type of malware that imprisons user data by making them unavailable or by encrypting them and requesting a ransom to release them.

Insider Threat: An insider threat is a malicious actor acting from within an organization/company for his own or a third party's agenda.

Exploit kits: Exploit kits are - next to botnets - major tools for the installation of malware.

Data breaches: Data breaches refer to incidents involving the illegal disclosure and dissemination of user data.

Identity theft: Identity theft is a special case of data breach and is related to compromise of identity information of humans or machines.

Information leakage: Information leakage is a category of cyber-threats abusing weaknesses of run-time systems, of components configuration, programming mistakes and user behavior in order to leak important information.

Cyber espionage: The act of espionage in cyber terms.

Physical manipulation/damage/theft/loss: Though not always a technical/cyber threat, physical manipulation/damage/theft/loss continues to have severe impact on all kinds of digital assets. Physical loss and theft used to be the most important causes of data breaches.

Unauthorized activities: This threat is implemented by performing unauthorized activities (e.g. through abuse of access rights, escalation of privileges, vulnerabilities, etc.). Some forms for unauthorized activities may be:

- Unauthorized access to resources/information
- Unauthorized installation of software
- Unauthorized use of software
- Unauthorized administration of devices and systems

Hardware related threats

HDW specific threats:
Such threats may relate to different hardware-related assets, exploit vulnerabilities which are specific to the hardware assets in scope of this document, or require different handling when compared to traditional IT security approaches. The described threats can cause/affect or be related to other threats in various ways. This way of specifying threats would not be suitable to determine the most relevant hardware-related risks due to its ambiguity (i.e. the successful manifestation of one threat can cause more threats to successfully manifest). However, listing threats in a more detailed (yet unfortunately ambiguous to a certain degree) manner ensures that this document provides guidance for readers with different backgrounds and expectations who do have to put less effort into understanding which further events could be caused by few accurate threats. In addition, it supports the design of good practices on multiple levels and taking potential security measures for multiple assets into account.

HDW modifications:
The modification of hardware can be performed in various ways; this threat focuses on non-intrusive ways which (ab-) use available interfaces (such as Firewire, PCI Express, or USB) to modify hardware to carry out/support unintended functions. The threat table below will contain various examples of potential hardware modifications.

HDW Attack Persistence:
Traditional security controls focus on the prevention and detection of logical threats on the application or operating system level. Attacks that are carried out in a way that bypasses those levels (e.g. by attacking firmware which may not even be accessible by the operating system/application or modifying the functioning of hardware in a transparent way) cannot be detected by traditional controls or mechanisms to verify the integrity of the computing environment.

This results in a very high level of attack persistence that can be achieved by attackers and cannot even be countered with a complete system re-install.

HDW Remote Firmware Attacks:
Attacks which can compromise the firmware of a device in a remote way (e.g. software vulnerabilities are exploited in the firmware of an Ethernet network interface card) result in the same impact as described in Firmware Modification above, however, no logical or physical access to the device is required. If the attack is carried out in a sophisticated way (e.g. by immediately modifying essential functions), there is also no way for traditional security controls to detect the attack.

HDW Traffic Sniffing:
The access to network traffic is a common threat in typical IT environments. However, in the context of hardware-related attacks, traffic sniffing is not limited to network connections but can also be carried out on internal buses and connections, such as the memory or hard drive bus. Those bus systems traditionally do not assume threats from within those system/devices which are physically connected so that no compensating controls are implemented.

HDW Firmware Modification:
The modification of firmware is less intrusive than the physical modification of hardware and can have very similar effects. The function of the hardware can be modified, processed data intercepted, and security functionality be bypassed by modifying (i.e. exploiting weakness of) the logic which manages the hardware. Firmware modifications can be implanted in different ways, e.g. by:

- Using existing firmware update mechanisms,
- exploiting a vulnerability in the firmware already loaded onto the device and
- using binary firmware loading mechanisms, or exploiting the lack of access control/write protection of firmware storage (e.g. unlocked NVRAM during boot).

HDW Surveillance:
Surveillance is a specific type of access to information that combines the basic information access with a focus on personal/private data and the use of hardware to gather information from the physical world, for example by (ab-) using microphones, cameras, or location data. Typical personal mobile computing environment comprise various sensors that can be abused to form strong surveillance capabilities.

HDW Data Tampering/Spoofing:
Comparable to surveillance threats, the tampering or spoofing of data on mobile computing devices can have wider impact than typical data tampering: Spoofed location, audio, or visual data can lead to a variety of abuse scenarios.

HDW Information Access:
Hardware devices and mobile computing devices in particular, store all types of information which often form/represent significant parts of the identity and belongings of users. Hardware-related attacks can lead to a completeness of information access that extends the capabilities of typical logical IT threats and thus need to be covered in a dedicated manner.

HDW Malfunction:
In a connected world that is supported by computing devices in all areas of life, the malfunction of devices can result in a variety of harm and negative impact. Several specific threat scenarios are for example the malfunctioning of medical devices (performing critical tasks on a patient), access control systems (preventing unauthorized access to people's homes), or monitoring systems (e.g. for hazards such as fire).

HDW Denial-of-Service:
Comparable to malfunction, (successful) denial-of-service attacks are comparable to maliciously induced malfunction. This threat represents the denial-of-service of mobile/personal/embedded devices, e.g. the crash of a smartphone, the outage of a monitoring solution, or the error state of an alarm system.
Denial-of-service attacks originating from mobile/personal/embedded devices (e.g. as happened recently in the case of the Mirai Botnet [5]) can be a threat for the same classes of devices, however, it would be a generic threat. In addition, it is also a potential effect/impact of a successful materialization of a threat like Remote Firmware Attacks.

HDW Modification-of-Service:
Mobile computing devices provide a variety of services, tampering with the way the service is delivered or changing the result/outcome of the service delivery, various specific threat scenarios can be realized. While the malfunctioning of a device can impact various assets, the modification-of-service can in addition pave the way for further threats/attacks. This kind of attacks will bother us in the future, in particular in complex autonomous systems found often in vehicles and complex industrial systems.

HDW Loss of Compliance:
Mobile computing devices are used in various areas, some of those requiring strict certification (e.g. FDA approval or the CE marking) for any computing device to be used. Modification of those devices in any way can result in a loss of certification and thus compliance violations. Tampered devices can also violate regular security violations when it comes to access control requirements.

HDW waste of resources:
Attacks on certain types of mobile computing devices can result in a waste of resources. While energy can also be wasted as a result of logical attacks, even bigger amounts and different types of resources (e.g. water) can be wasted when control systems are attacked.

5G/Virtualization/SDN related threats

5G technology suffers from several threats:

- 5G Spectrum sensing data falsification (signal fading, harmful interference)
- 5G MAC layer attack (MAC spoofing, congestion attack, jamming attack)
- 5G User emulation (exclusive use of bandwidth, mimic incumbent signals)

Threats to servers of virtualized network functions:
Virtualization of functions and their operation on virtual machines (e.g., a server that can be used as a network switch) is a common practice in SDN. Therefore traditional security threats for servers

running virtualized network operations such as network monitoring, access control, network management etc. should be considered.

Threats related to virtualization mechanism (Network Virtualization bypassing):
The use of the network between different tenants need to assure that only legitimated traffic enters or leaves a network slice, but also that any switching element checks and enforces the traffic isolation by installing legitimate flow rules preventing slice trespassing.

Software/Firmware exploits in SDN:
This threat involves exploiting vulnerabilities of the software/firmware in order to cause some malfunction, reduction or disruption of service, eavesdrop data or destroy/compromise data. Software/firmware exploits may occur in all layers of the SDN reference architecture, and depending on the layer that they relate to they have been distinguished into network element software/firmware exploits, controller software/firmware exploits, and SDN applications software/firmware exploits. Software/firmware exploits of network elements and controllers cause the malfunction or even their termination of operation. In the case of switches, for example, the exploited switches can drop, slow down, clone or deviate network traffic. Exploited switches software/firmware can also create forged traffic in order to exhaust other switches and/or the controllers the switches are connected to.

Beyond that SDN components and SDN communication can suffer from different threats (e.g. SDN API exploitation, identity spoofing, .side channel attack …)

Table 1 summarize the top 15 threats occur in ENISA Threat Landscape.

From these report we can identify the following statements:

- Malware, Web-based attacks, Web application attack are the most frequent threats in all examined year.
- From positon 4 to 9 the threats hardly change their positions. Two new threats occurred in that list (Ransomware, Insider threat) and two went down (Exploit kits, Physical damage/theft/loss).
- Ransomware increased in period 2014 – 2017
- A new threat introduced in the 2018 year report, the cryptojacking.

Cryptojacking (also called malicious cryptomining) is an emerging online threat that hides on a computer or mobile device and uses the machine's resources to *mine* forms of online money known as cryptocurrencies. It's a burgeoning menace that can take over web browsers, as well as compromise all kinds of devices, from desktops and laptops, to smart phones and even network servers.

	2014	2015	2016	2017	2018
1.	Malicious code (Worms/Trojans)	Malware	Malware	Malware	Malware
2.	Web-based attacks	Web-based attacks	Web-based attacks	Web-based attacks	Web-based attacks
3.	Web application attacks	Web application attacks	Web application attacks	Web application attacks	Web application attacks
4.	Botnets	Botnets	Denial of Service	Phishing	Phishing
5.	Denial of Service	Denial of Service	Botnets	Spam	Denial of Service
6.	Spam	Physical damage/theft/loss	Phishing	Denial of Service	Spam
7.	Phishing	Insider threat	Spam	Ransomware	Botnets
8.	Exploit kits	Phishing	Ransomware	Botnets	Data breaches
9.	Data breaches	Spam	Insider threat	Insider threat	Insider threat
10.	Physical damage/theft/loss	Exploit kits	Physical damage/theft/loss	Physical damage/theft/loss	Physical damage/theft/loss
11.	Insider threat	Data breaches	Exploit kits	Data breaches	Information leakage
12.	Information leakage	Identity theft	Data breaches	Identity theft	Identity theft
13.	Identity theft	Information leakage	Identity theft	Information leakage	***Cryptojacking***
14.	Cyber espionage	Ransomware	Information leakage	Exploit kits	Ransomware
15.	Ransomware	Cyber espionage	Cyber espionage	Cyber espionage	Cyber espionage

Table 1. Top 15 threats from annual ENISA Threat Landscapes 2014 - 2018

4. Hungarian CSIRT incident results

Hungarian National Cyber Security Center (GovCERT-Hungary – Government Incident Response Team) regularly publish awareness material. Such publication Hungarian name is “Nemzetközi IT Biztonsági Sajtószemle”. It contains news from IT security different fields like a press review and also a report from announced security incidents in Hungary. [6]

I have summarized the available weekly reports for year 2018, and tried to identify trends and rules. It can also be interesting, how follows the Hungarian incidents the international expectations submitted by ENISA.

We can’t compare the results directly, because ENISA reports are Threat Landscapes, and GovCERT-Hungary results contain completed and reported incidents. Each uses different taxonomies, the mapping between them not necessarily evident.

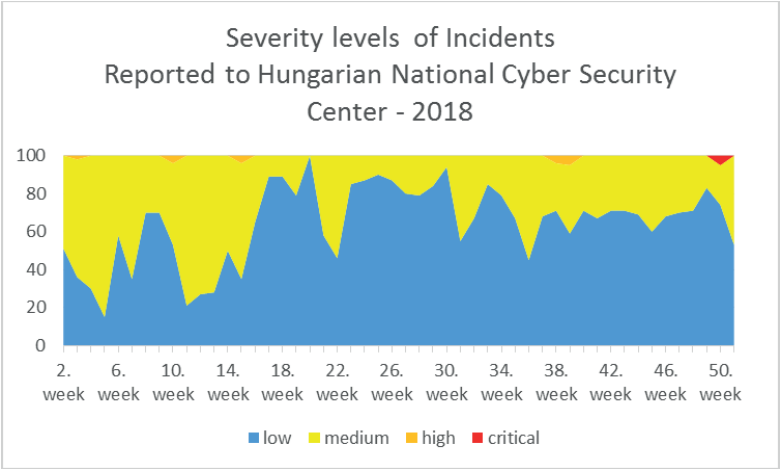

Figure 1. Severity levels of reported incidents in Hungary - 2018

Analyzing the severity levels of reported incidents (Figure 1) we can identify that high and critical incidents are relatively rare. Totally five incidents got that severity during 2018. The ratio of the low and medium level incidents are continuously alter. Usually the ration of the low level incidents are higher than medium incidents.

Inspecting the weekly statistics of GovCERT Hungary (Figure 2), the top five incidents are:

1. Malware
2. Phishing
3. Unauthorized access
4. SPAM
5. Web based attack/defacement.

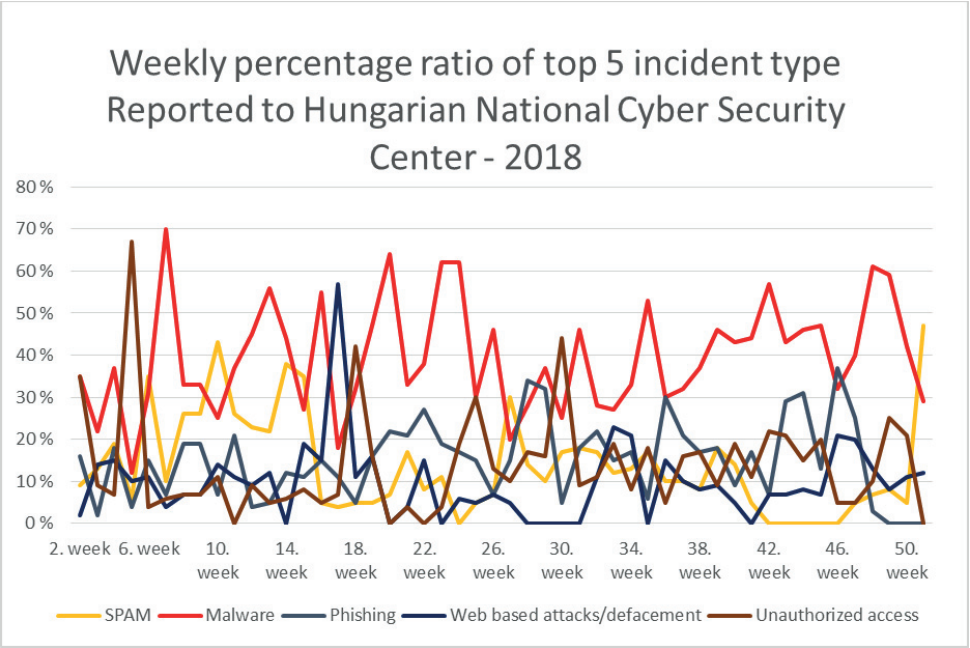

Figure 2. Top 5 reported incidents in Hungary - 2018

In summary we can say that, the incidents in Hungary fundamentally follow the international trends.

5. Identified trends and new threats

Ransomware attacks will continue. A new form of malware can be spread about, the ransomworm. It exhibits the behaviors of both ransomware, which encrypts data and demands payment for a decryption key, and a worm, which self-replicates by exploiting security vulnerabilities and can automatically propagate throughout a network without user interaction.

Malicious spam also will be the primary vector of malware. Many malware infections start with an email message, which may or may not have either a link, an attachment, or both. At the very least, be aware that malware may leverage files you might not consider dangerous, like Office documents, to start the infection process.

The Android platform has long been a more popular target for malicious app-makers. The open nature of the platform and low barriers to entry for developers has long been a double-edged sword, making it easier to get apps built and functional. The growing and persistent threat of mobile malware is also expected. While malware that runs on the Windows operating system vastly outnumbers malware for any other platform, users of mobile devices are increasingly subject to malicious activity pushing malware apps to their phones, tablets, or other devices running Android and iOS.

Cryptominer code in mobile games or utilities will also be increased. The code would run whether or not the app itself was running, and functioned as a constant drain on the phone's (or other device's) battery.

As our homes and businesses adopt more internet-connected devices, especially those not traditionally connected to the internet, criminals have been devising new ways to hijack those devices to use as nodes in huge botnets. Criminals can then leverage these botnets to engage in distributed denial-of-service attacks, mine cryptocurrency, and infiltrate networks for the purposes of espionage or data theft.

A new threat also can become popular called phishing-in-the-app. One way that criminals can bypass the Play Market's source code checks was by not including anything malicious in the app itself, but rather by making an app that, in essence, is a browser window to a phishing site. The apps, in this case, were designed in tandem with the phishing site so the user had a seamless experience.

6. Conclusion

The world of cyber security threats is sophisticated. The threat landscape is huge, offensive and defensive technologies change continuously. According to Symantech predictions [7], attacker will exploit artificial intelligence (AI) and use AI to aid their assaults. The growing 5G deployment will increase attack surface area. The botnet-powered distributed denial of service attacks will massively use IoT devices. Attacks will increase that target is supply chain, the attacker try to implant malware into legitimate software packages at its usual distribution location. Beyond that file less malware attacks increase. Proper data protection and incident response will be challenge for all organization.

7. References

[1] Regulation EU No 526/2013 (the 'ENISA Regulation') https://eur-lex.europa.eu/legal-content /EN/TXT/?uri=CELEX%3A32013R0526

[2] Reform of cybersecurity in Europe https://www.consilium.europa.eu/en/policies/cyber-security/

[3] ENISA Threat Landscape https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

[4] ETL (ENISA Threat Landscape) web application https://etl.enisa.europa.eu/

[5] ANTONAKAKIS, Manos, et al. Understanding the Mirai botnet. In: USENIX Security Symposium. 2017. p. 1092-1110.

[6] International IT Security press review (Nemzetközi IT biztonsági sajtószemle) https://itbiztonsag.govcert.hu/dokumentumok/sajtoszemle

[7] Cyber Security Predictions: 2019 and Beyond https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond