Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

CERT.LV Public Performance Report 2017

2018

This report consists of publicly available information. Accounts of CERT.LV activity involving undisclosed information are excluded from this report. The report is purely informative.

Content

Summary

2017 was a year characterised by a considerable shift in the development of various ransomware, which inevitably had its effect also here in Latvia. Until recently cryptoviruses were mainly used for financial gain by extorting a ransom from victims in exchange for the retrieval of their data, however last year various large-scale ransomware campaigns (e.g. WannaCry, NotPetya) took place, which had political aims and were most likely supported at a state level.

The advancement of the Internet of Things took a swift pace and is expected to continue at this rate throughout the next five years. The variety of products that can be connected to the internet is growing steadily, however manufacturers are not always sufficiently concerned with the level of security of these products. Although the industry has set certain security standards they are not always respected, and as of now protocols for confronting such manufacturers are not accordingly defined or implemented. As a result possibilities for abusing the Internet of Things are increasing. The incompliance to security standards is a growing concern of the owners of the critical infrastructure, whose objects are connected with smart components.

Data leakage incidents occurring in global cyberspace in 2017 were partly due to ill-informed usage of cloud services and their respective security levels. Users' failure to fully understand the terms of use, the full capacity, and the security mechanisms of these services is a serious but solvable problem in the opinion of CERT.LV. Considering this, it is expected that 2018 will be a year when cloud service usage will be a topic of increasing importance on an individual, as well as the state level.

January 2017 saw one of the most positive developments of the year – regulations by the Cabinet of Ministers Nr. 442, "Procedures for ensuring the compliance of information and communication technology systems with the minimum security requirements" came into effect. Public authorities have begun to adapt the respective procedures and information systems, and implemented the requirements of these regulations in their tender specifications. This continues to contribute to raising the overall security level of the state.

Overall, in the time frame of this report, CERT.LV registered 477 252 threatened unique IP addresses, undertook 13 penetration tests on websites of various state and municipal authorities where 3 critical and 11 high hazard security vulnerabilities were detected. CERT.LV also provided the respective support to resolve incidents in the public and the private sector, as well as for law enforcement authorities. CERT.LV participated in 125 different events, and educated close to 8000 people.

1. Processing of incidents

Every month CERT.LV gathers information about threatened IP addresses in Latvia. In order to provide a more comprehensive overview of the Cyberspace of Latvia and to ensure that the gathered data can be internationally compared, since January 1st of 2017 CERT.LV has adapted internationally used incident taxonomy for registering threats and hazards (a taxonomy developed by the project eCSIRT.net). In the following statistics all the threats and hazards registered by CERT.LV will be listed together and grouped by the type of the threat or hazard (e.g. malware, intrusion, fraud), as well as the type of infection (e.g. Confiker, Zeus, Mirai) and the type of vulnerability (e.g. Opendns, Openrdp).

Every month of the report time frame CERT.LV gathered information about 90 000 - 100 000 threatened unique IP addresses.

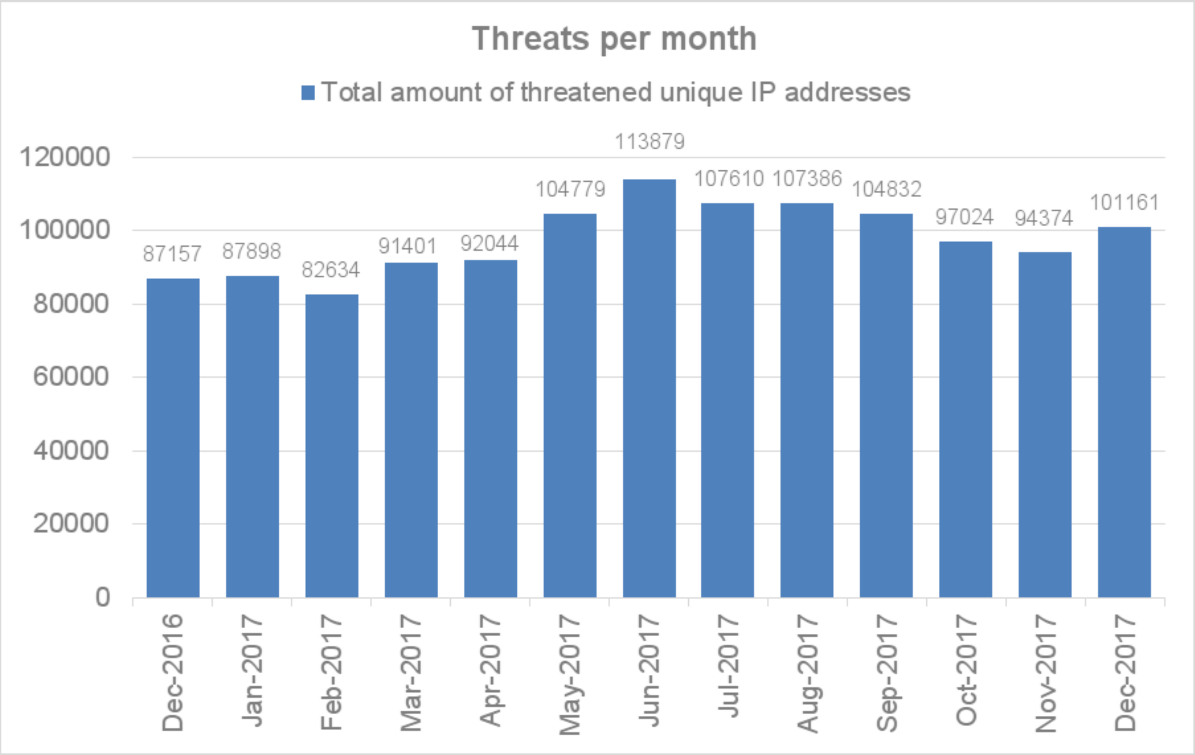

Figure 1 - threatened unique IP addresses registered every month by CERT.LV in 2017

The effect of the global campaigns WannaCry and NotPetya can also be detected in the statistics compiled by CERT.LV showing an increase in the months of May and June (Figure 1).

Up until the end of year 2016 CERT.LV compiled the information about the threatened IP addresses on a quarterly basis by adding up all the threatened IP addresses (Figure 2 – blue bars). Starting with January of 2017 CERT.LV considered only the unique IP addresses threatened every quarter, thus avoiding listing the same IP address twice (Figure 2 – red bars).

As an example, there were 192 284 threatened unique IP addresses registered in the fourth quarter of 2017 (by the previous method this number would have been as high as 292 559 IP addresses). The difference in these numbers illustrates that in the time-span of several months the same IP addresses are being repeatedly registered as threatened, due to repeated threats or failure to eliminate them.

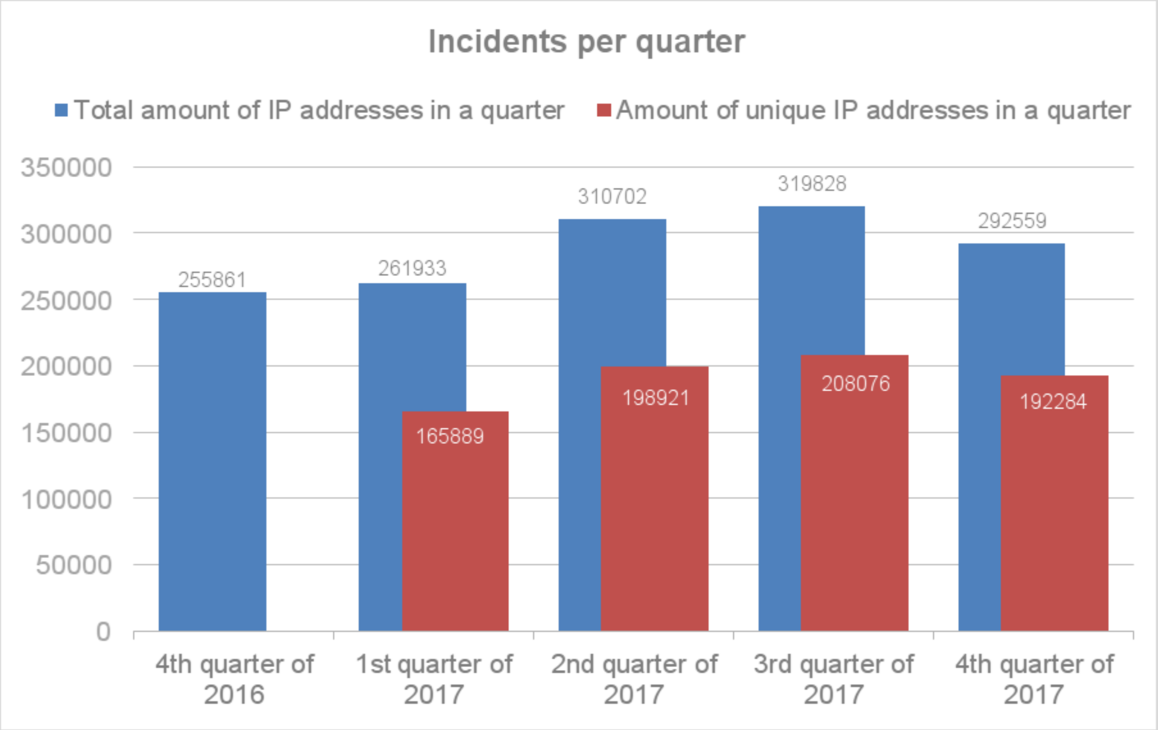

Figure 2 - threatened unique IP addresses registered by CERT.LV on a quarterly basis in 2017

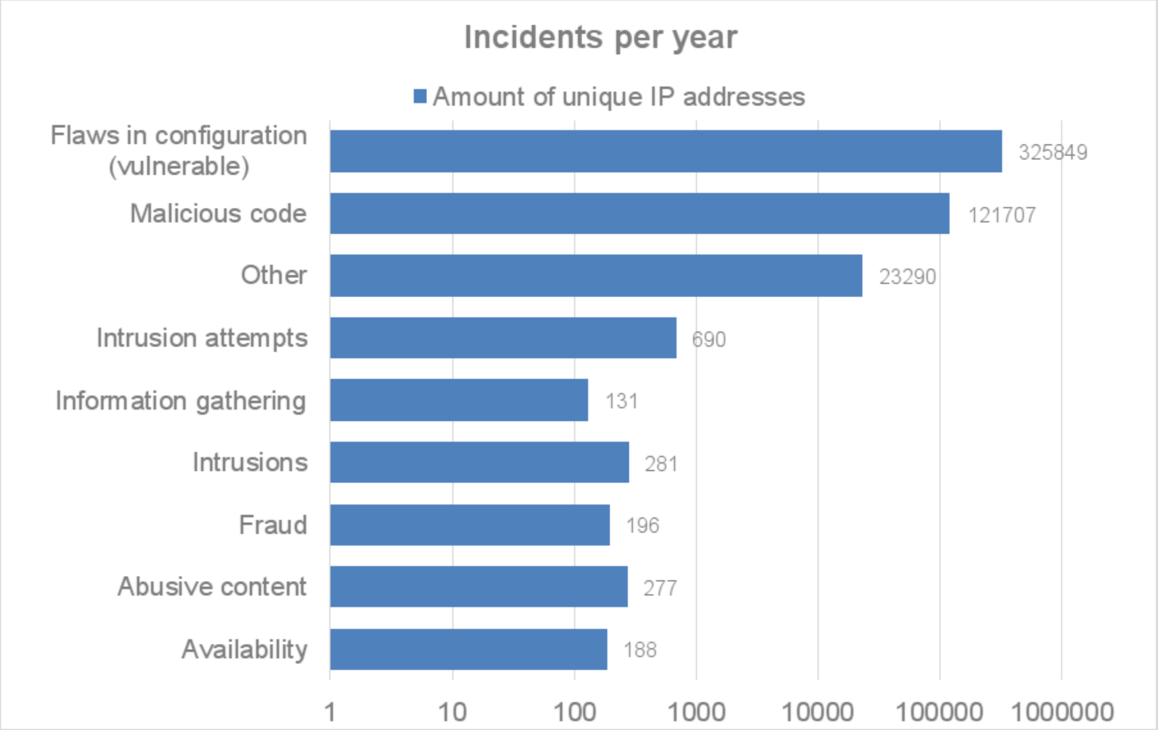

Figure 3 - threatened unique IP addresses registered by CERT.LV in 2017 by type of threat

The prevalent type of threat consistent across the time frame of the report was flawed configuration, followed by malicious code and intrusion attempts.

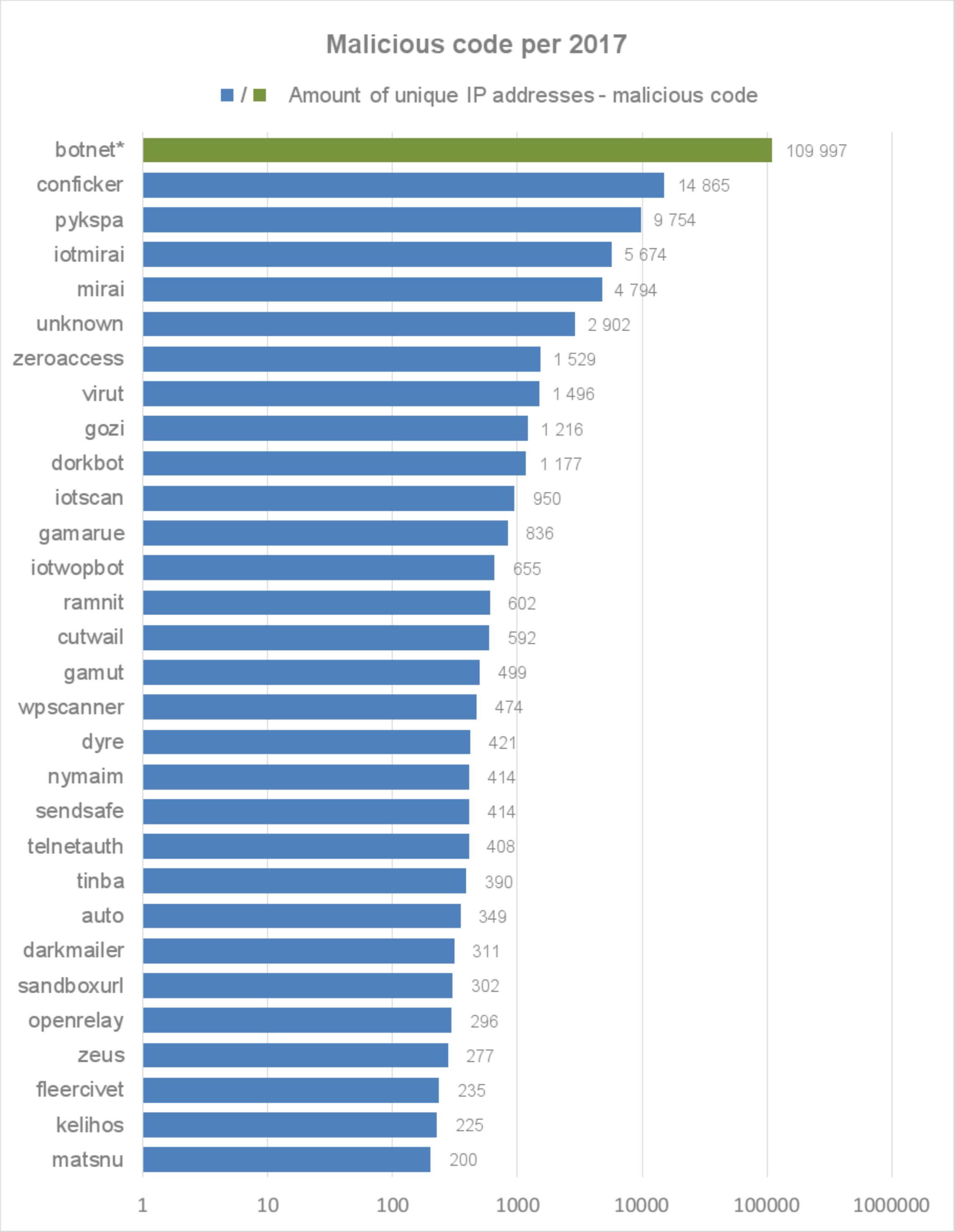

Figure 4 - threatened unique IP addresses registered by CERT.LV in 2017 due to malicious code

The most widespread malware this year was by far the botnet malware; a detailed breakdown is presented in Figure 4.1.

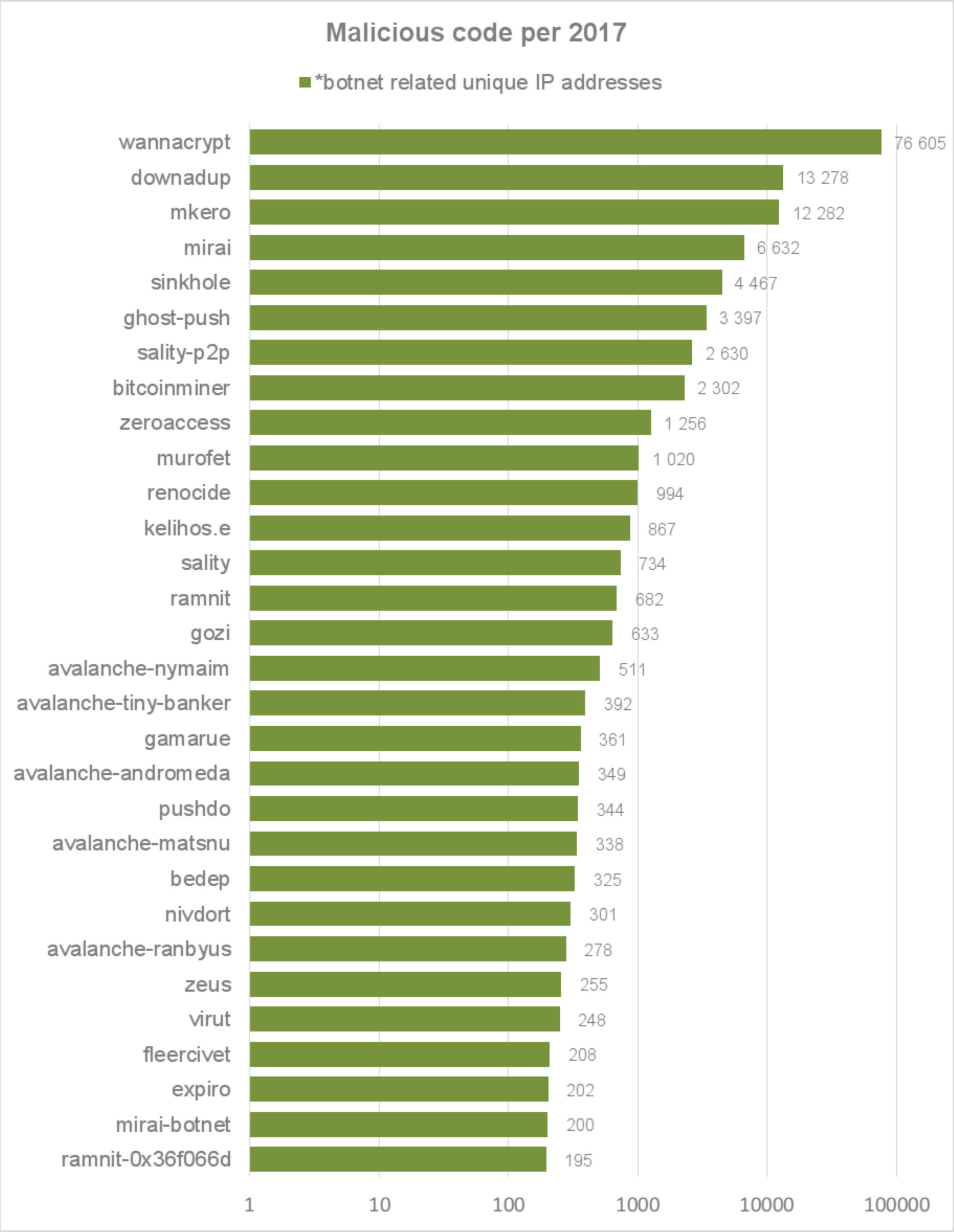

Figure 4.1 - threatened unique IP addresses registered by CERT.LV in 2017 due to malicious code

Figure 4.1 illustrates that the most widespread malware last year was WannaCry or WannaCrypt. The second most widespread malware in 2017 was Conficker or downadup, despite the fact that it already is a well-known and relatively easy to prevent malware. MKero Android Trojan is in the 3rd place, which is a malware capable of bypassing the CAPCHA authentication system, and subscribing users to various cost related services without their knowledge.

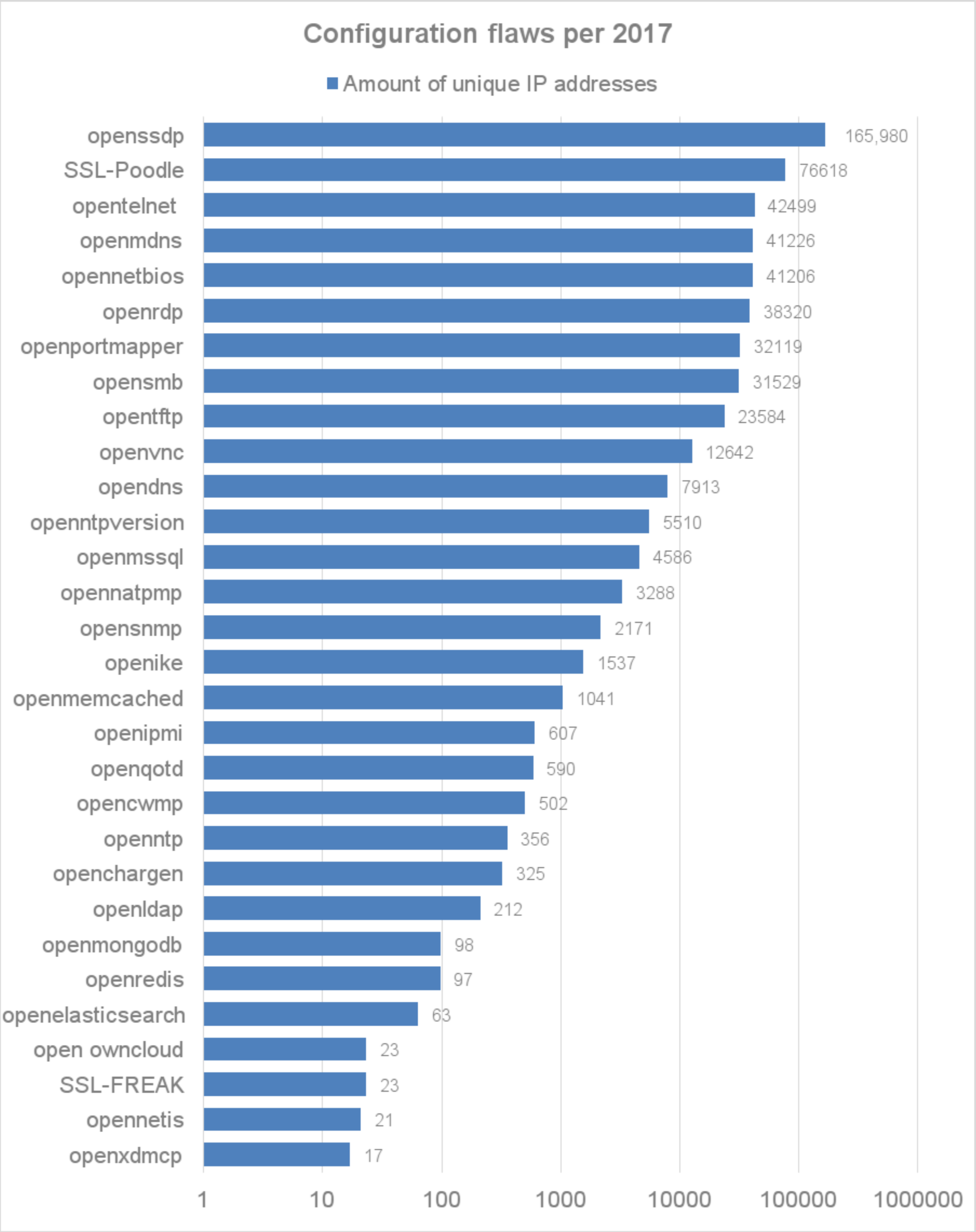

Figure 5 - threatened unique IP addresses registered by CERT.LV in 2017 due to flawed configuration

Opensmb, a newcomer among the other configuration flaws in the first half of 2017, ranked 8th in the full time frame of the report. This rather common configuration flaw was the cause for the rapid spread of such ransomwares as WannaCry and NotPetya.

Compromised websites

CERT.LV gathers and lists information about hacked or defaced websites. In 2017 there were 859 cases in total, which is a 35% increase comparing to 2016. In 29 cases the websites were hacked repeatedly.

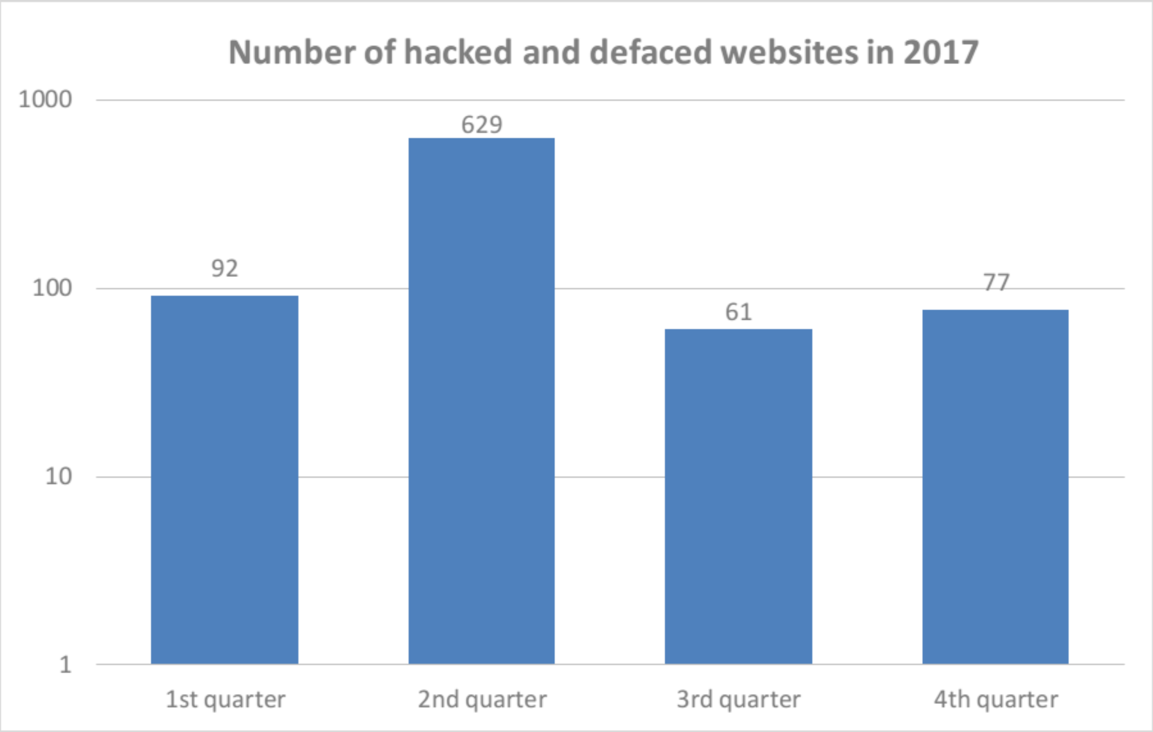

Figure 6 – number of compromised websites in 2017 on a quarterly basis

2. Significant incidents

In the time frame of the report CERT.LV cooperated with state and municipal institutions, banks, internet service providers and other organizations in handling various security incidents. The report contains a summary of the most important incidents, characterizing the predominant tendencies of the year.

2.1. Ransomware

In the time frame of the report CERT.LV regularly received reports of various ransomware, such as Cerber, WannaCry, BTCWare, NotPetya, Scarab ransomware, Locky, Kryptik and others. The reports received from individuals and small businesses were considerably more common than those received from state and municipal institutions.

This year two large ransomware campaigns were on the rise, which also attracted the attention of the media – the WannaCry and NotPetya campaigns in May and June respectively.

At the time of the WannaCry campaign more than 200 000 Windows operated devices in 150 different countries were infected. CERT.LV received information about 20 victims in Latvia.

However, in contrast to other countries where the list of victims included for example hospitals or telecommunication companies, the victims in Latvia were mainly individuals, as well as some small businesses.

On the other hand the virus NotPetya hit Ukraine the hardest, also leaving a heavy impact on the companies cooperating with the country. According to the information received by CERT.LV there were 4 victims in Latvia – 3 commercial enterprises and one individual.

In most cases the data was retrieved from backup copies or with the help of decryption tools provided by the project „No More Ransom". In rare cases the victim had to negotiate with the attacker.

CERT.LV advises never to pay the attacker, as it results in providing the attacker with resources for further attacks and the development of new ransomware, which the victim might not be aware of. There is also no guarantee that the data of the victim will be decrypted after the ransom has been paid.

2.2. Business e-mail compromise

In 2017 CERT.LV received various accounts from state and municipal institutions, as well as different companies concerning fraudulent emails, which are also known as Business email compromise.

Emails of such nature are most commonly received by either accountants or other employees responsible for the financial matters of the organization. The sender usually disguises as someone who is in a management position of the company – a board member, a CEO, a director, an acting director etc. The email usually contains instructions for transferring a specific sum of money to an account that seemingly belongs to a partner of the company, when in reality this account belongs to the fraudster. This scheme contains some elements of social engineering, through which victims' emotions are manipulated, e.g. the instructions may demand that an employee immediately must take emergency action. CERT.LV has also concluded that these fraudulent emails are increasingly harder to detect because of the grammatically correct use of the Latvian language.

The largest of these campaigns were registered in April and August. In all cases the Reply-To address of the email raised suspicion, which aided the detection of these fraudulent emails.

CERT.LV has no information concerning if any of the recipients of the registered emails suffered any financial loss.

In order to avoid attacks of this kind, CERT.LV advises to use tools that render the email addresses listed on the website of the company or institution undetectable by scanners, as well as to create SPF records that determine from which specific servers emails with specific domain names can be sent, in order to prevent the spread of fraudulent emails.

2.3. Fraud

Most of the fraud attempts registered in the time frame of the report were linked to fraudulent websites, including fake versions of original websites, some of which integrated emblems of state institutions for example. Usually the intention of such websites is to illegally extract data of a client of the respective company or institution.

At the end of 2017, before the holiday season, requests from various users were received asking for help in determining if certain websites were reliable. In all cases CERT.LV pointed out the fairly recent domain registration date and the short time of the online shop's existence. In addition to the surprisingly low prices in the pre-holiday season, this raised marked concerns about a potential fraud. A lack of contact details on a website in question is also an important indicator of the untrustworthiness of a site.

CERT.LV also received information about a fraudulent phone call. The caller pretended to be a representative of Microsoft and asked for a certificate related payment so that the user would not receive any error messages. The user was instructed that a small sum for the certificate had to be paid using a certain website. The user proceeded with entering their bank account details into the fraudulent website.

After the phone call a sum of 3000 EUR was taken from the victim's bank account. The victim was advised to file a police report.

2.4. Phishing campaigns

The aim of phishing campaigns is to extract sensitive information from internet users, e.g. credit card information, social media and email passwords, passport details etc. The most common reports of phishing campaigns were of fraudulent emails (supposedly from the email provider) requesting a renewal of the email account or the password.

A few examples of phishing campaigns are listed below:

- In April, CERT.LV obtained information that a large number of email addresses in the .LV domain zone received a message stating that the storage limit has been exceeded and that one should proceed by clicking on a given link and enter the necessary data for the renewal of the service or else the email address would no longer be accessible. CERT.LV informed the respective website provider of the given link about its fraudulent nature and requested its termination.
- In April CERT.LV also obtained information about a malicious Google Chrome browser extension designed to supposedly ease the process of authentication by offering to authorize the user with a single click, if the user allows for the extension to save the username, password and all the code card codes; all this data entered in the extension would in reality be forwarded to the fraudsters. Google was informed about the fraudulent nature of this extension.

2.5. Denial-of-service attacks (DoS and DDoS)

In the time frame of the report CERT.LV received various accounts of DoS and DDoS attacks from state and municipal institutions, as well as from one of the commercial banks of Latvia. On various occasions information was received from other European CERT units regarding Latvian IP addresses with different configuration flaws (openDNS, OpenResolver etc.), which were used in DDoS attacks. The providers of these addresses were identified and informed.

Most of the attacks were successfully repelled, however in few cases the attack resulted in a temporary disruption of the internet resource's accessibility. On all occasions advice was given by CERT.LV for improving the security of the site, for example by limiting actions of robots within the website.

An insight concerning a few DoS and DDoS attacks is provided by CERT.LV below:

- At the end of January a commercial bank informed CERT.LV about a planned SPAM attack with the aim of extorting money. Approximately 60 thousand emails were sent to the institution and a small demonstrative DDoS attack was carried out using UDP Flood. These emails came from legitimate servers, e.g. scientificamerican.com, robly.com etc. No more than 20 - 30 emails were sent from each of these servers. Mainly various news and media portals were used that offer subscriptions to notifications about certain article topics. CERT.LV gave advice on how to proceed in these kinds of situations – do not communicate with the extortionists and do not pay them. A request was made to terminate the Google email address used in the attack. An actual full scale attack did not follow.
- In May information was received about an attack on a state institution portal. Analysis of the log files revealed that a planned attack on the portal was carried out by using specialized tools for finding potential vulnerabilities. By evening the attack had reached the DoS phase and rendered the portal inaccessible. The portals operation was fully restored in less than an hour.
- In October an account was received listing 87 Latvian IP addresses that had been used in a denial-of-service attack (DDoS). An OpenResolver configuration flaw was detected in these addresses and the respective providers were warned.

2.6. Financial platforms

Various users of unlicensed stock trading platforms fell victim to fraud resulting in losses from 2000 EUR up to 100 000 EUR.

Before using financial services CERT.LV advises to make sure that the service provider has received a licence from the Financial and Capital Market Commission, otherwise the client will not be protected by the state. Information about all the licensed investment service providers can be found on the website of the Financial and Capital Market Commission.

As cryptocurrencies are gaining popularity, the attacks on cryptocurrency wallets are becoming more frequent too. To retrieve the lost cryptocurrency is even harder than actual money, because of the lack of regulation and customer protection guidelines. Users have to be careful and informed about the necessary security measures and the authenticity of the site where these activities are carried out.

2.7. Mobile malware

CERT.LV has received information about some instances of mobile malware activity, but the losses suffered by mobile device users were mostly due to careless subscription to paid services or replying to fraudulent messages with an SMS that results in extra fees. No mobile malware campaigns directed at Latvian users have been detected.

2.8. Social networks

In 2017 CERT.LV received information about various incidents regarding social networks.

- Various fake Twitter and Facebook accounts were detected that claimed to represent state institutions. Inaccurate news was posted on these accounts. The institutions were asked to request the termination of the fake accounts.
- Various users gave accounts of attempts made to extort their Facebook account details either through a notification about the termination of their account or by offering to receive information about the view count of their profile. If the users opened the attached link they were redirected to a fraudulent website with a request to enter their email address and Facebook password.
- For various users the attempt to meet new people on the social network Facebook resulted in blackmail and extortion attempts. There were cases where people claimed to be located in a war zone and asked for financial support or suggested to communicate via video call and later demanded a ransom so that the recording of the video call would not be made public. In case of a blackmail attempt CERT.LV advises not to communicate with the blackmailer and never to pay the requested amount of money, because another request will most likely be made asking for an increasingly larger sum. All blackmail attempts should be reported to the police.
- The users of the messaging service Whatsapp were also subjected to fraud attempts. An invitation to participate in a fake lottery or a threat to terminate the service were among the methods used by fraudsters to get potential victims to send a cost related message or to enter their credit card data into a fraudulent website.
- Various complaints were received about unauthorized posts on Facebook. In these cases CERT.LV advises to firstly use the site facebook.com/hacked to reveal the presence of any malicious applications that may have been granted access to post on behalf of the user, as well as to check the device for any viruses.

2.9. Intrusions/ compromised devices

- CERT.LV identified various compromised websites where an SQL injection vulnerability was detected, including a few municipal websites. This vulnerability makes unauthorized data retrieval possible. CERT.LV contacted the website providers, informed them about the detected vulnerability and gave advice on how to avoid it.
- Various cases of compromised routers were identified. On one occasion the router was sending a user’s data to a command-and-control server. In another instance a hacked router was used as a command-and-control centre for the spreading of the malware Trickbot, which is a banking Trojan used for extorting financial data. CERT.LV informed the providers and gave advice on mending the vulnerabilities.

- Various state institution websites were compromised and defaced. CERT.LV gave recommendations on how to improve website security.
- Towards the end of the year various reports were received about a malware found in banner ads on one of the websites owned by a Latvian news portal. The banners contained a malicious code that was mining cryptocurrency and burdening the users' computers. The providers of the website were informed and the banners were fixed.

2.10. Data

No large scale data leakages were detected in the time frame of the report, however information was received about various instances where sensitive website information was publicly available on the internet, which posed a data leakage threat. CERT.LV informed the website providers and advised to limit data accessibility on the public network.

2.11. Vulnerabilities

- Specialists of the Latvia State Radio and Television Center (LVRTC) implemented an e-signature and conducted the related security system audit. They also developed a software update using the cryptographic algorithm SHA256.
- Information about critical vulnerabilities in various websites was received. Various website parameters were subjected to an SQL injection attack type which would enable the attacker to take control of the website and the server. Website providers were informed and received advice on how to prevent these vulnerabilities.

3. Informative communication events

In 2017 experts at CERT.LV continued to give interviews and answer questions from the media regarding cybersecurity and other current topics on TV, radio and in media outlets. This year the media fixed its interest on such topics as mobile device security, the process of renewing bank authentication, cybersecurity in Latvia, ransomware, fraudulent online shops and others.

3.1. Informative events for the media

On May 15th CERT.LV held a press conference to inform the media about the WannaCry ransomware and its effect in Latvia.

On June 28th CERT.LV invited the representatives of the media to a press conference to answer their questions about the ransomware NotPetya and its effect in Latvia.

On October 18th a representative of CERT.LV took part in the joint press conference of the Latvian Safer Internet Centre and CERT.LV with the name "Media Breakfast" where media representatives were informed about current cybersecurity topics. This press conference was a part of Cyber Security Month.

3.2. Communication in the digital environment

The number of followers on the popular social networks Twitter and Facebook grew steadily this year:

- At the end of the time frame of the report the Twitter account twitter.com/certlv had 1853 followers.
- At the end of the time frame of the report the Facebook profile facebook.com/certlv had 762 followers**.**

CERT.LV provides the website https://www.cert.lv where information is published regarding the current threats, tips for raising the IT security level and various upcoming events. Last year the CERT.LV website had 67 855 unique visits.

CERT.LV also continued to run the portal for user education www.esidross.lv where users can receive replies to their comments and where new articles are being posted regularly.

For every month within the time frame of the report, informative cyber security newsletters “OUCH!” were issued in collaboration with the institute SANS, available to every internet user.

4. Educational events

In 2017 CERT.LV continued to organize educational events regarding security related questions for IT security specialists, employees of state and municipal institutions, students as well as others. In the time frame of the report CERT.LV took part in 125 events and educated 7957 participants.

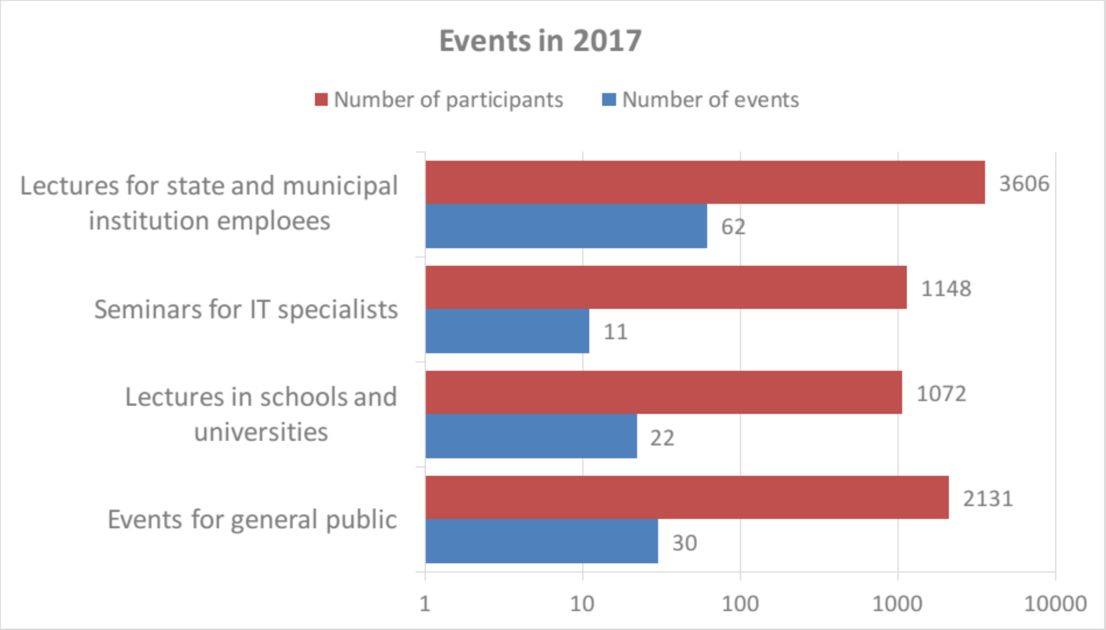

Figure 7 – number of CERT.LV organized events and participants in 2017

The largest event of the year was the annual IT security conference “Cyberchess 2017” which took place in the Radisson Blu Hotel Latvia on October 5th. More than 500 people took part in this event and the livestream of the conference had an additional 3000 unique views.

The conference was organized in collaboration with the ISACA Latvia chapter. The event was supported by LMT, SQUALIO cloud consulting and Accenture Latvia.

4.1. CERT.LV organized events for IT security specialists

On April 6th CERT.LV organized a seminar for IT security specialists "Esi drošs" ("Be safe") where participants could learn about current topics in IT security as well as mobile device security, Internet of Things security, vectors of attack on social networks and the risks of open-source information.

On October 5th CERT.LV collaborated with the ISACA Latvia chapter in organizing the IT security conference "Cyberchess 2017" as part of the Europe's Cyber Security Month (ECSM). Notable topics of the conference were Internet of Things and its security, Artificial Intelligence, DDoS, ICT supply chain risks, digital state, implementation of the NIS Directive, cybersecurity as part of state security, cyber independence and others.

On November 13th a practical seminar for IT security specialists "DNS abuse: Tools and methods for investigations" was organized by NIC in collaboration with CERT.LV and ICANN.

On December 11th CERT.LV organized a seminar for IT security specialists "Esi drošs" ("Be safe") where participants could learn about the current topics in IT security as well as the threats of ransomware, the most important vulnerabilities, the most common mistakes made by an internet user, safe and informed choices of domain names, security on social networks and others.

4.2. CERT.LV presentations on IT security for public education

From March 27th to April 2nd the eight EU e-Skills Week took place in Europe as well as in Latvia. This year the emphasis was placed not only on the development of e-skills, but also on cyber security, and consequently March 28th was named the day of Digital security. Three seminars/discussions took place on this day that were dedicated to various cyber security topics: cyber security policies in Latvia, mobile security and the Internet of Things and its security. Representatives of CERT.LV took part in all three discussions.

On March 29th, as part of the e-Skills week, another Computerologist campaign took place at CERT.LV where anyone could bring their computer, tablet or smartphone to an IT specialist for a check and receive advice about the security of their data and device free of charge.

On March 31st a representative of CERT.LV took part in the live broadcast seminar "Your e-opportunities" organized by VARAM as a part of the e-Skills week and gave a presentation "Reality in virtual environment".

On April 26th a representative of CERT.LV gave a presentation "Internet of Things – how the Internet of things is affecting our present and what to expect in the future" as a part of the event "Digital Era 2017".

On May 26th CERT.LV took part in the event "Work anywhere" organized by Microsoft and

VARAM informing participants about the IT security aspects that need to be taken into consideration when travelling or visiting public areas.

On September 12th a representative of CERT.LV took part in the Erasmus+ Strategic School Partnership project convention “The ICT road to STEM through TCC” and gave a presentation on CERT.LV materials for educating 1st to 6th grade pupils about IT security. The representative also took part in the discussion and exchanged information concerning the education of younger pupils.

On April 12th a CERT.LV representative took part in online cyber security seminar for companies organized by Bite Bizness and gave a presentation on mobile device security and the Internet of Things (IoT) security. The seminar was part of the European Cyber Security Month.

On October 19th, as part of the ECSM, the DSS organized conference “ITSEC 2017” took place where a CERT.LV representative gave a presentation „Firmware over the air: Case study of Adups FOTA”.

On October 25th as part of the ECSM, another Computerologist campaign took place at CERT.LV where anyone could bring their computer, tablet or smartphone to an IT specialist for a check-up and receive advice about the security of their data and device free of charge.

On November 1st a representative of CERT.LV participated in a Digital Freedom Festival organized discussion "Money and cybersecurity".

On November 24th a representative of CERT.LV gave a presentation “Current ICT security threats – a look at the private sector” at the conference “Commercial Law and Artificial Intelligence: qou vadis?” organized by the Ministry of Justice and the LU Faculty of Law.

On December 6th a representative of CERT.LV participated in the fake news discussion initiated by the President of Latvia “Security of Latvia in the 21st century. Fake news as a means of affecting the public opinion”.

5. Cooperation with state institutions

In the time frame of this report, CERT.LV undertook 13 penetration tests on websites of various state and municipal authorities, where 3 critical and 11 high hazard security vulnerabilities were detected.

A positive shift was seen in 2017 – the interest shown by state and municipal institutions in the penetration tests offered by CERT.LV has grown notably. This means that along with their interest, the sense of responsibility these institutions have for their internet resources and their security has increased as well.

5.1. Cooperation with the Ministry of Defence

Meetings with the Secretary of State for Defence were held regularly; there was also regular communication with the National Cybersecurity Policy Coordination Section.

CERT.LV was regularly involved with the Ministry of Defence team for the implementation of the NIS Directive.

5.2. Other cooperation partners

CERT.LV cooperated with the National Guard Cyber Defence unit by participating in technical training as well as providing a unit with a virtual training environment for developing the skills needed for security incident resolution.

CERT.LV continued to support the activity of the Security Expert Group (DEG) which provides a discussion forum for IT security specialists in the private as well as the state sector. Security Expert Group meetings were held monthly.

6. International cooperation

Within the time frame of the report CERT.LV strengthened cooperation between CERT units from other countries and other international organisations. CERT.LV specialists gave presentations in international conferences and seminars and acquired new skills through technical trainings.

6.1. Cooperation with the CERT community

In the time period of the report CERT.LV representatives participated in TF-CSIRT and FIRST technical seminars and meetings. CERT.LV representative also has been holding a chair position in TF-CSIRT.

From January 23rd to January 25th the representatives of CERT.LV participated in TF-CSIRT gathering and the FIRST regional symposium in Valencia where a CERT.LV representative presented the „Firmware over the air, case study of ADUPS Fota”.

From May 8th to May 10th CERT.LV and the Ministry of Defence welcomed CERT representatives from Montenegro, which was a part of the European Commission TAIEX program.

The guests from Montenegro learned about CERT.LV's excellent experience in resolving various incidents, various types of international cooperation, educational activities and their other branches of activity. The main goal of the visit was the exchange of experience in order to raise the capacity of CERT in Montenegro.

6.2. Cooperation with ENISA

A wide range of collaborations were carried out with the European Union Network and Information Security Agency (ENISA), e.g. preparing for conferences etc.

On March 21st a representative of CERT.LV took part in a seminar in Brussels, Belgium where ENISA's activities over the last 8 years were evaluated, and discussions about the tasks, mandate and strategy for the future of ENISA were held.

In May 9th and 10th the final report conference of ENISA European Cyber Security training “Cyber Europe 2016” took place, as well as the planning of future trainings („Cyber Europe 2018” and „EUROSOPEx 2017”).

6.3. Cooperation with NATO CCDCoE

CERT.LV representatives have collaborated with the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCoE). One of the most important events was the international cyber security training “Locked Shields 2017”, which took place from April 24th to April 29th. CERT.LV representatives were part of the organizing (white), defending (blue) as well as the attacking (red) teams. The joint team of CERT.LV and US EUCOM took the 5th place.

In August of 2017 a cooperation agreement with NATO CCDCoE was signed for a collaborative organization of the technical cyber security training “Crossed Swords”. A preparation for the training, that took place in January of 2018, began.

The report was drawn up by:
CERT.LV public relations project manager Madara Grinvalde, phone: 67085888, email madara.grinvalde@cert.lv

March 23, 2018