CERT.LV
Information Technologies
Security Incident
Response Institution

Institute of Mathematics and
Computer Science University of Latvia

Ministry of Defence
Republic of Latvia

2018

CERT.LV Public Performance Report

The report includes generally available information; it does not contain information about CERT.LV performance results that contain restricted access information. The report is for informational purposes only.

Content

Summary

The overall level of cyber security in Latvia's cyberspace can be assessed as moderate. The volume of commercially motivated attacks was consistently high, with a slowly growing trend. The main victims were small and medium-sized entrepreneurs. In the public sector, municipalities suffered mostly in the regions of Latvia. The financial sector was stable, and no major incidents were observed. Latvia continued to be a target for attackers having an opposite political ideology to that of NATO and the EU.

Last year, increased attention was given to the transparency and cyber security of the Saeima electoral process. CERT.LV classified cyber-space activity during elections as moderate, not threatening the state security and elections, and without severe occurrences. Several attacks on email systems, websites and network infrastructure, including public sector targets, were observed with varying intensity. However, they failed to cause any damage, or tangible effect, to the population, as they were successfully repelled. The most noticeable incident during the election was the defacing of the social network Draugiem.lv front page.

Reflecting on specific incidents, the reporting period was marked by a series of DDoS attacks which also received extensive media coverage (e-health, LETA, Song and Dance Celebration ticket distributor bilesuparadize.lv, Delfi.lv). Finally implementing the BCP-38 best practice standard, at least at the European level, it should be possible to find a solution to the DDoS attack problem by eliminating the possibility of sending out network packets with fake packet source (IP spoofing), which is the cause of most DDoS attacks. This would also reduce the maintenance costs of resources at the expense of DDoS protection solutions.

Frequently over a lengthy period of time, CERT.LV continued receiving messages abaut encrypted devices that have been accessed by hackers through a weakly protected Remote Desktop Protocol (RDP) by guessing overly simple passwords. Problem prevailed both in the private and in the public sector.

Innovative techniques have been observed in user-centric fraud campaigns using a more personalized approach to the preparation of fraudulent emails. In order to increase the credibility of the threats mentioned in the letter, the email contained user's personal information, such as a password or a part of the telephone number obtained from some data leak but used as "evidence" for intrusion into the device.

A positive trend for 2018 was the growing alertness and sense of responsibility of the internet users, as evidenced by the informative reports received by CERT.LV on various fraudulent campaigns, as well as the growing public interest in the origin of various software and devices and the associated risks, as was the case with Yandex Taxi, Kaspersky and Huawei.

For the first time ever in Latvia during the reporting period, CERT.LV in cooperation with NATO CCDCoE, organized technical cyber security training "Crossed Swords 2018". This was the most technically complex and challenging training so far, covering a number of geographic locations, involving both IT critical infrastructure maintainers and military units. More than eighty cyber security experts from fifteen NATO CCD CoE member states participated in the training.

On October 9th, within the framework of European Cyber Security month and support from the project "Improving Cyber Security Capacities in Latvia", CERT.LV in cooperation with ISACA Latvia chapter organized a cyber security conference "Cyber Chess 2018". This was attended by 500 participants and remotely watched by more than 2,000.

In 2018, CERT.LV launched the project "Improving Cyber Security Capacities in Latvia" approved by the European Commission in 2017 "Connecting Europe Facility, Telecom-Cyber Security" call (contract with the European Commission No.INEA / CEF / ICT / A2017 / 1528784)) and cooperation project "CyberExchange" (contract with the European Commission No INEA / CEF / ICT / A2017 / 1528784) to strengthen CERT.LV's response capabilities to information technology security incidents, increase knowledge and capacity and readiness to meet the requirements of the NIS Directive.

Overall, during the reporting period, CERT.LV registered 491,974 threatened unique IP addresses, provided the necessary support to both the public, private sector and law enforcement authorities in dealing with incidents, participated in 127 different events and educated nearly 8,000 people.

1.

Processing of incidents

Every month CERT.LV collects information about threatened Latvian IP addresses. CERT.LV uses internationally used taxonomy of incidents (taxonomy created by the eCSIRT.net project) to account for threats. In statistics, all threats registered by CERT.LV are listed together, by dividing by type of threat (for example, malware, intrusions, fraud), as well as by types of infections (such as *Confiker, Zeus, Mirai*) and vulnerabilities (such as *Opendns, Openrdp*).

During the reporting period, CERT.LV compiled monthly information on an average of 95,000 to 105,000 vulnerable unique IP addresses.

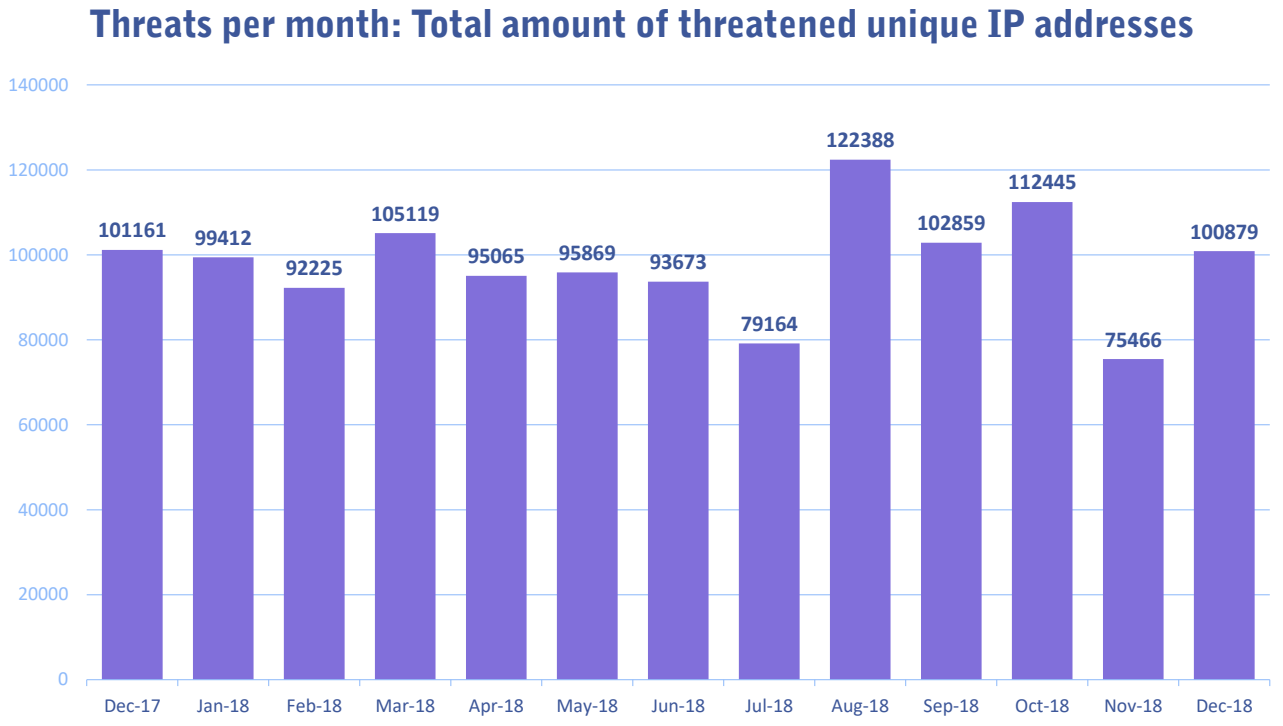

Figure 1 - CERT.LV registered unique IP addresses per month in 2018

The uneven flow of incoming data resulted in a fall in July and rise in August, while the October growth was due to the introduction of a new threat category in several data sources (Figure 1). The November fall was also caused by an uneven flow of incoming data.

Clauses 15 and 24 of the Cabinet of Ministers Regulation No. 422 “Procedure for Ensuring Compliance of Information and Communication Technology Systems to Minimum Safety Requirements” dated 2015 are applied to increased security IS from January 1, 2018 and continue to increase the level of security of state information systems. Regular employee education activities also play an important role.

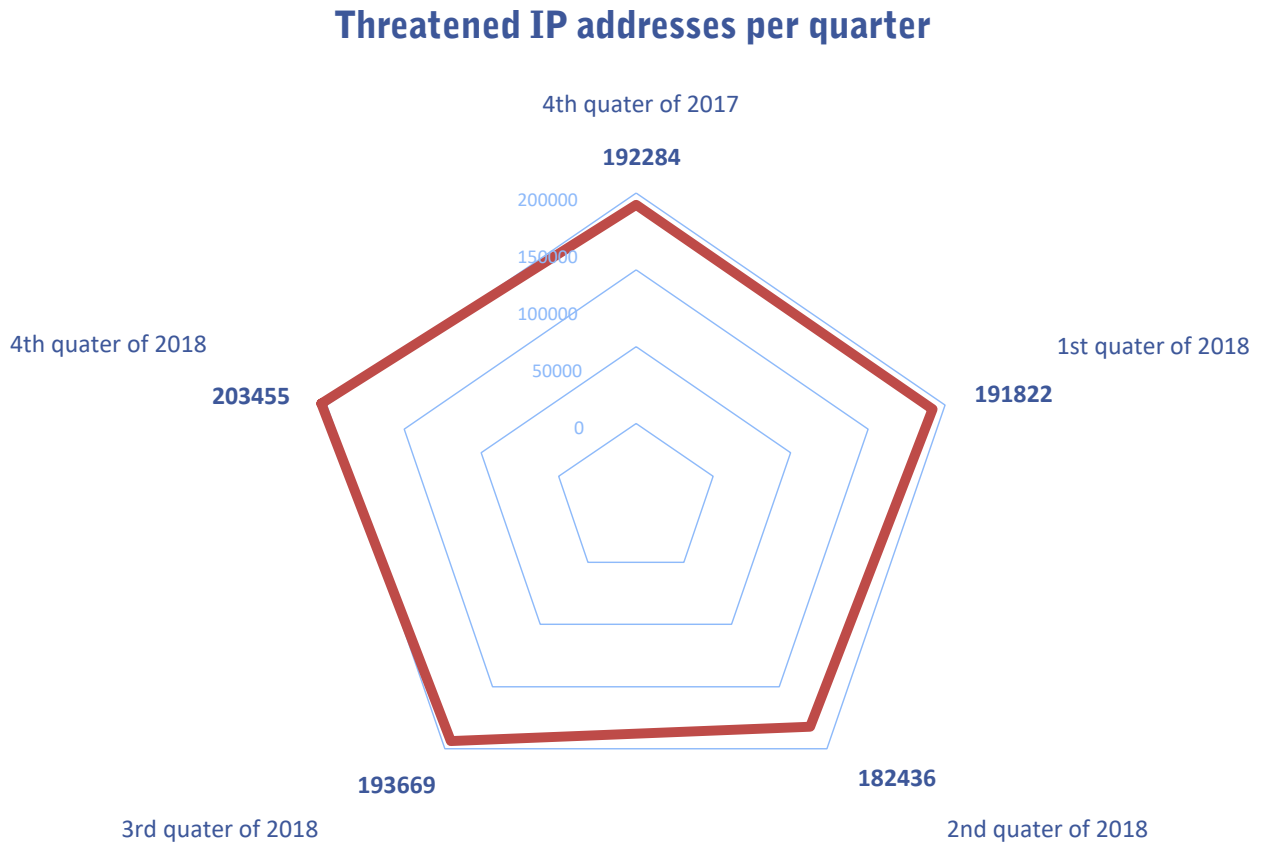

Figure 2 - CERT.LV registered threatened unique IP addresses per quarter in 2018

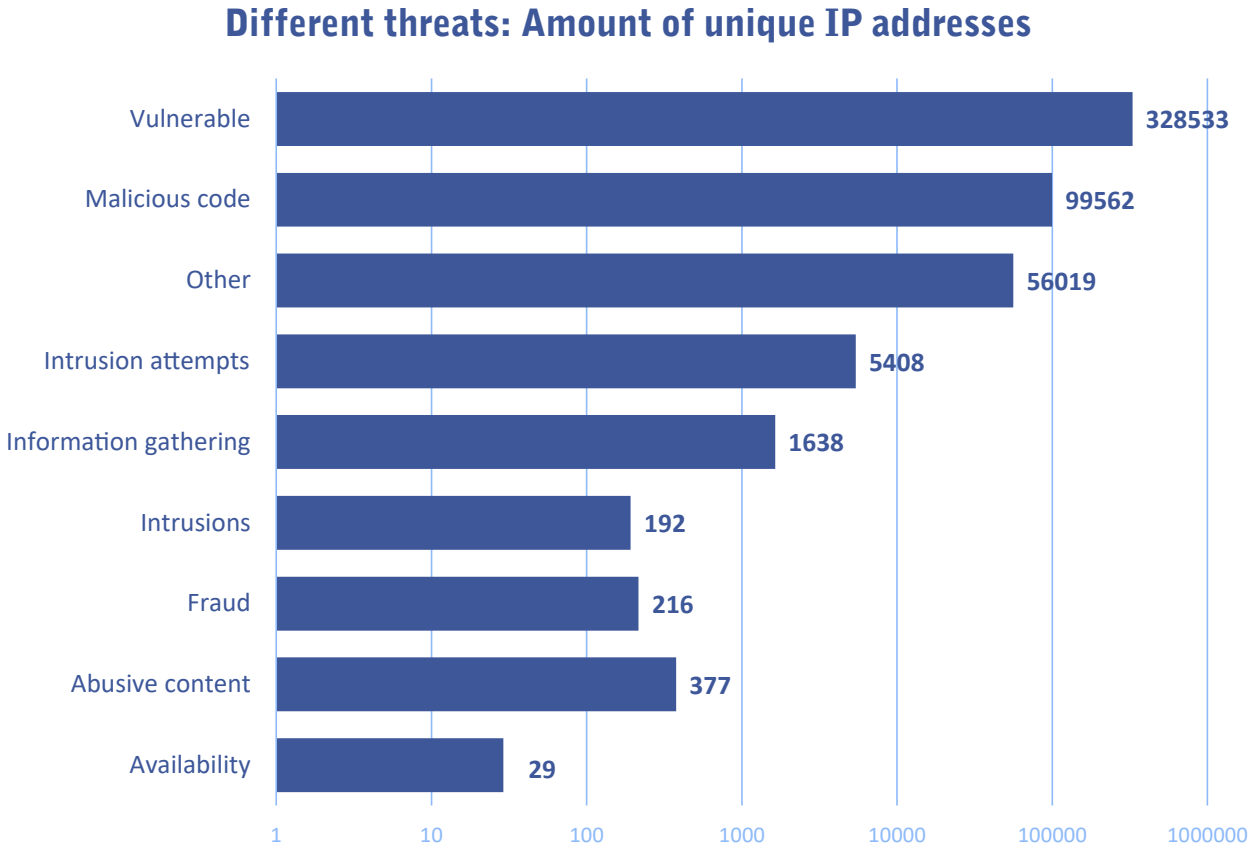

Figure 3 - Threatened unique IP addresses registered by CERT.LV by type of threat in 2018.

The most common type of threat during the reporting period related to the vulnerabilities, the second most common was malicious code, and the third was intrusion attempts.

Malicious code per 2018

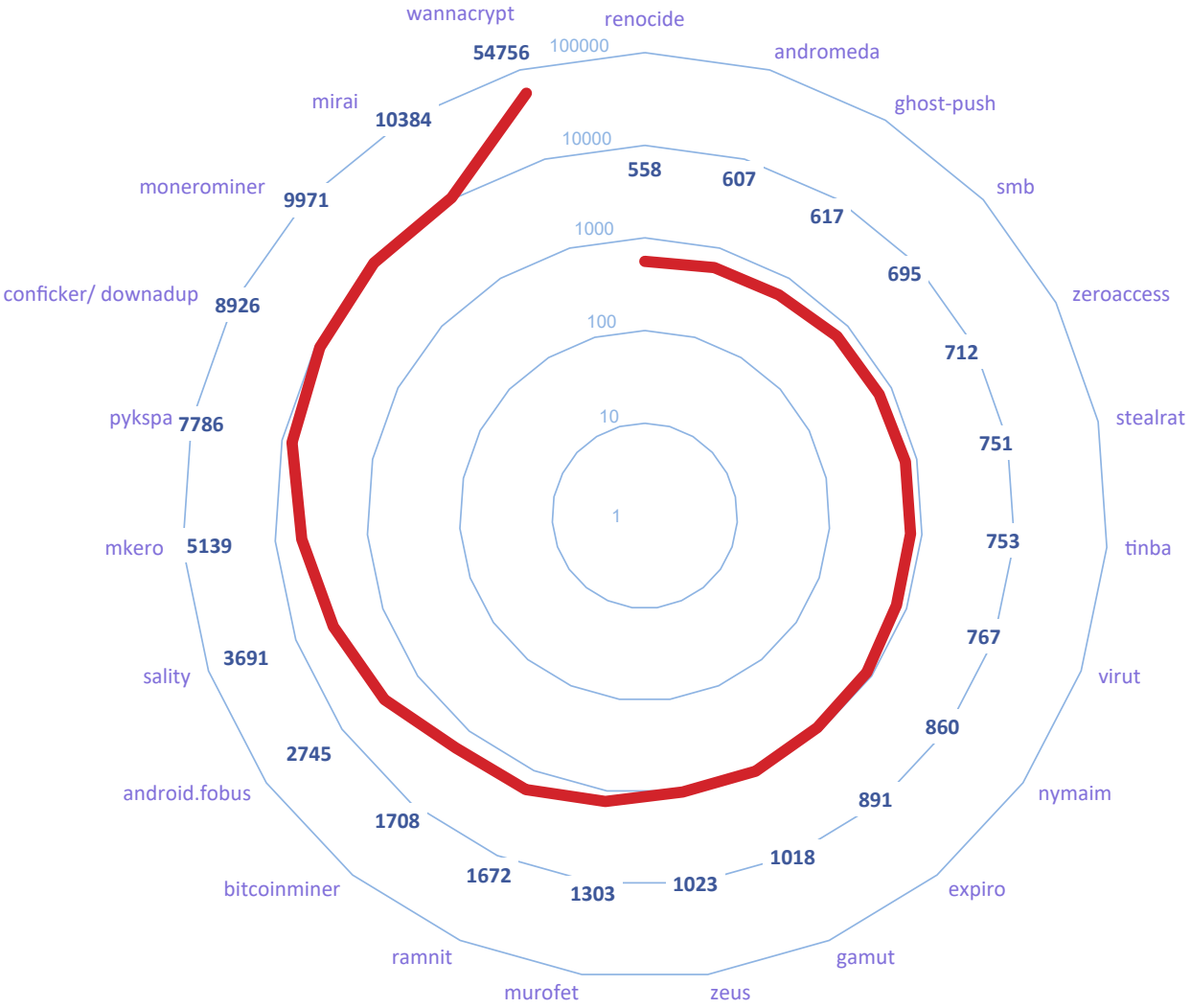

Figure 4 - Total number of CERT.LV registered threatened unique IP addresses in 2018 with the type of threat - malicious code.

WannaCrypt or *Wannacry*, which is a ransomware virus, ranked first as malware this year. It affects devices with the Microsoft Windows operating system and spreads through a vulnerability in the SMB protocol. Effects and distribution of the Virus can be prevented by installing Microsoft-made software updates that are available even for such Windows versions such as Windows XP and Windows Server 2003. It has to be admitted that the extremely high number of unique IP addresses affected by this malware significantly outperform all others, It could indicate that devices with assigned dynamic addresses using DHCP (Dynamic Host Configuration Protocol) have been infected and the actual amount of infected devices is smaller. However, this does not mean that the threat is not significant and noteworthy, especially because it refers to infected devices with the most likely outdated operating system, such as Windows XP, which no longer receives automatic updates, and puts the device at increased risk.

In second place was *Mirai*, a malware that threatens inadequately protected devices of Internet of Things (IoT). Most commonly infected are smart TVs, Internet routers or other similar devices that are connected to the Internet after purchase without changing the user name and password set by the manufacturer. These default passwords are widely known, and their use puts the device at risk of attack.

In third place was *Moneromíner*, a malware that performs the acquisition of crypto currency *Monero* (a privacy-oriented crypto currency that has gained popularity in criminal circles) using the resources of the device without the user's knowledge. Ruthlessly using the device's capacity, the device can be dangerously loaded or even permanently damaged. Crypto currency acquisition malware became popular after an unexpectedly rapid increase in the price of crypto currencies at the end of 2017 but then dropped due to rapid decrease of crypto currency prices. *Moneromíner* activity during the reporting period was the most active in June and July.

Unchanged towards the top of main issues remains *Conficker*, even though it is a long-known and relatively simply "curable" malware.

Mkero and *Android Fobus*, which are mobile malware, have also reached the upper end of the top. *Mkero* is able to bypass *captcha* checks and, without the knowledge of the user, subscribes to receiving increased fee SMS. And *Android.Fobus* presents itself as an ad-blocker, but actually makes increased fee calls and collects personal information from users.

One way for such mobile malware to enter the device is by the user installing it, in cases when this malware presents itself as a useful application, such as a mobile antivirus or ad blocker, but actually hides harmful functionality.

The other way is by downloading the software from an unofficial site, which, unlike *Google Play* or the *App Store*, does not perform any application security checks. Users who buy a mobile phone or tablet on the Internet by making the choice for the lowest possible price are also exposed to this risk. As a result, you can get a device with an unofficial Android operating system that already contains malicious components. Additionally, such a device does not provide the ability to connect to *Google Play* to download the necessary applications, instead downloading takes place from a site in China that is unlikely to run a software check or, at worst, deliberately supports the distribution of malicious software.

Openrdp vulnerability, which takes the third place in vulnerability top (Figure 5), indicates an activated remote access or RDP (*Remote Desktop Protocol*) that is available from a public network and poses a threat if a too simple password is used and access is not restricted, for example, using a private connection or VPN. In 2018, CERT.LV regularly received reports from victims of cases of successful intrusion into the internal network by guessing the weak RDP password and causing disruptions or even financial loss by encrypting the contents of one or more devices (workstations, servers) for whose recovery ransom has been demanded.

CERT.LV also lists cases of hacked and defaced websites. In 2018, 179 websites were hacked and defaced. In eight cases, the website was hacked repeatedly during the year.

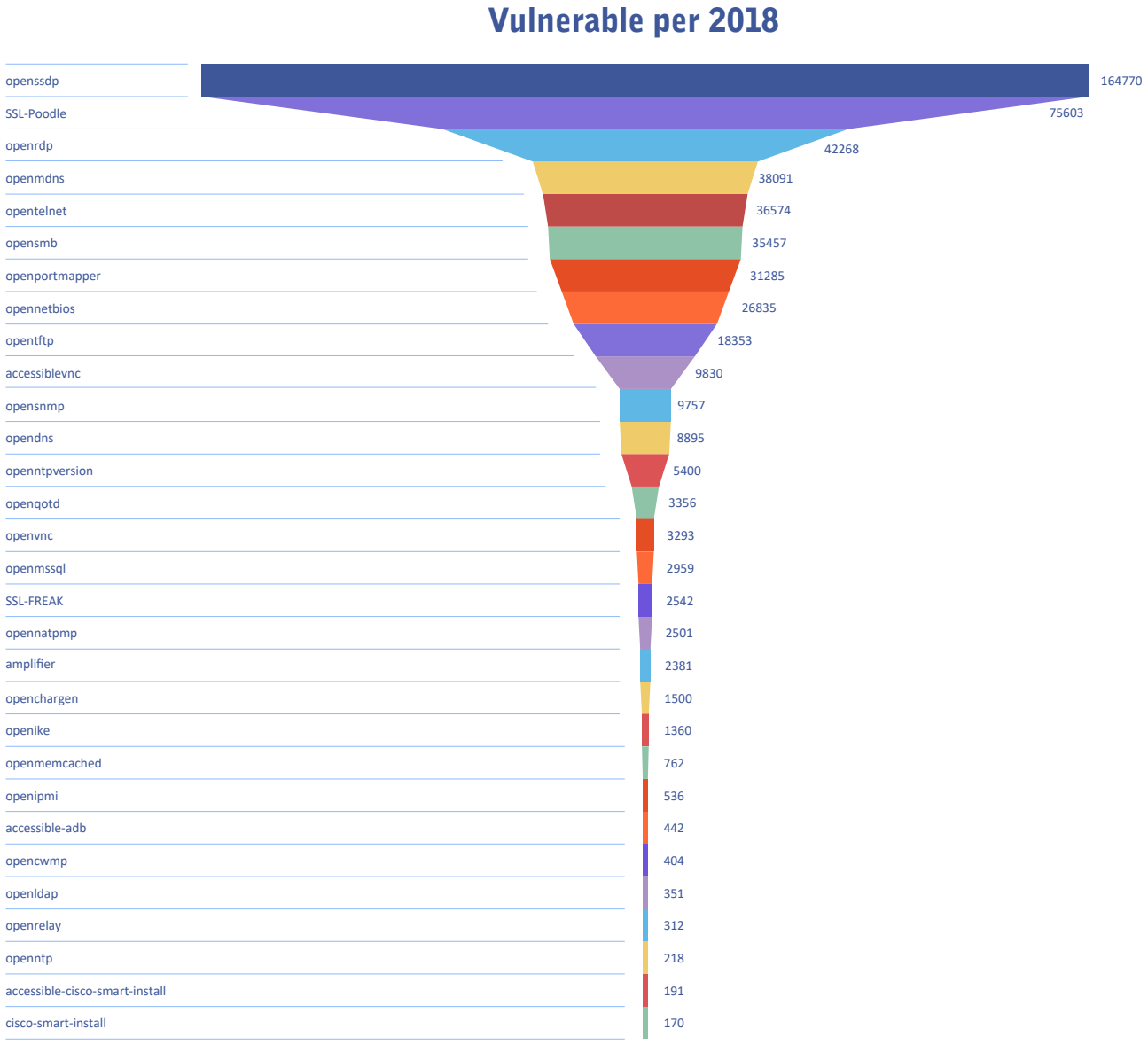

Figure 5 - Number of threatened unique IP addresses registered by CERT.LV in 2018 with type of threat - vulnerabilities.

2.

Most significant incidents in 2018

During the reporting period, CERT.LV cooperated with state and municipal institutions, banks, Internet service providers and other organizations dealing with incidents of various threat levels. The report summarizes the most significant incidents that mark annual trends.

2.1. Denial-of-Service Attacks (DoS and DDoS)

In January, the Distributed Denial-of-Service (DDoS) attack was experienced by health care quality and efficiency improvement program e-Health. The system was temporarily made unavailable, but no data leak occurred. The attack was stopped by disabling access to the system from abroad. The analyses concluded that the system was not adequately protected from DDoS and various configuration improvements were implemented.

In parallel to the e-Health system, DDoS attacks were also conducted against the news portal LETA, which was temporarily disrupted, and against several public authorities' websites. During analysis of all above mentioned attacks, several similarities in the resources involved in these attacks were observed.

The DDoS attack was also directed against the bilesuparadize.lv website. The attack overwhelmed the system, which was already experiencing an increased load in connection with the launch of the XXVI Latvian Song and XVI Dance Celebration ticket sales. CERT.LV made recommendations for improving DDoS protection.

At the beginning of the year, CERT.LV conducted analysis of series of overload attacks against a media portal. It was found that the source of the attacks was outside Latvia. CERT.LV made suggestions for improving protection against DDoS attacks.

At the beginning of September, a report was received on the DDoS attack on news portal Delfi.lv. This attack is linked to the pre-election period, as it happened on the day the portal broadcasted the debates of the prime minister's candidates. The attack intensity reached 20 Gbps, but the attack was successfully stopped, and users did not notice the impact of the attack on the service.

In the second half of the reporting period, several reports were received from tour operators about DDoS attacks on company websites to harm business operations. Several attacks have caused financial losses to the companies. In some cases, companies were threatened with telephone threats before the attack.

2.2. Phishing or Personal Data Scams

Throughout the reporting period, attempts were made to get users' email access data through phishing emails. The most common techniques used in emails:

- an invitation to follow the link in the email to make updates or prevent a certain problem;
- an invitation to follow the link to go to the latest version of email or update account security;
- an invitation to make mandatory security updates and receive personalized recommendations;
- an invitation to follow a link to prevent account deactivation due to excess quota or terms of use violation;
- an invitation on behalf of the administrator to follow the link to check the status of the account.
- If the user opened the link specified in the email and entered the email user name and password in the form provided, the data was sent to the fraudsters. Campaigns were targeted at both businesses and governmental institutions.

With reference to PayPal and apple platforms there have been several reports to steel access data. Fraudulent emails are sent out with an invitation to authenticate on the relevant sites by following the link in an e-mail to resolve problems of access, or use, of the service or to activate an account that was blocked after suspicious activity was detected.

During the reporting period, personal data phishing was also widespread by sending the victim an email with a request to send personal information (name, last name, address, birth data, copy of the passport) to receive an inheritance, compensation or simply money transfer.

At the beginning of the reporting period, one of the fraudulent email campaigns was designed to act as a final warning of debt repayment before the case was handed over to debt collectors.

2.3. Fraud

A report has been received of attempted fraud by sending several emails on behalf of PayPal and then requesting payment via Western Union to settle unpaid transport services. If this is not undertaken a final threat is made to close the account with follow up by the police.

During the reporting period, fraudulent campaigns were registered in which citizens received calls in Russian, as if they were an investment company offering to engage in dubious financial transactions and promising large profits. The initial telephone conversation was redirected to *Skype* and the callers asked the victim to share their device screen. This was followed by a proposition to buy bitcoin crypto currency by entering payment card details, and to invest in the fraudster's financial platform. The fraudsters were persistent, and threats were also used if the victim refused to follow the callers' instructions.

Throughout the year, regular reports were received from users about fraudulent emails in English, or Latvian, claiming that the attacker had set up a virus on the user's computer, aftrer user had visited adult vebsite and that a record has been created. If the cryptocurrency ransom was not payed then the victim's contacts would receive the record. In order to increase the credibility of the statement, the attacker in the e-mail indicated the user's password, which had become known as a result of this attack, but actually has come from one of the data leaks published on the Internet.

Meanwhile, e-mails were actively sent to companies on behalf of the company manager with the question of account balance and the possibility to make an urgent transfer abroad. For the sake of credibility, the amounts were not rounded, for example € 52,826.81. Some emails were written in good Latvian. To prevent this type of attack, CERT.LV recommends using tools that hide email addresses placed in the company's, or institution's, web site from scanners and create SPF records to determine which servers are allowed to send emails with certain domain names, in order to prevent the spreading of fraudulent emails.

In October, several reports of a fraudulent lottery were distributed in the WhatsApp app that promised two free tickets to the Ed Sheeran concert in Lucavsala if answers to four simple questions and a phone number were given to get the code. However, by giving the telephone number, the user made a subscription to receive priced text messages (the information was written at the bottom of the page).

2.4. Intrusion attempts

During the reporting period, a large amount of automated intrusion attempts were made by infected devices such as routers included in the robot network and attacking other similar devices, with the aim of expanding the network to carry out other malicious acts, such as Denial-of-Service or DDoS attacks.

2.5. Malware

Reports were mostly received for spreading malicious code via email, adding an ISO disk image, ZIP or RAR archive with executable .EXE files, or a .DOC document file. In some cases, emails included a link that triggered the virus loading from the Internet.

In most cases, the malicious code sent to users was designed to steal users' private information (user-names, passwords) to send it to the host server. There have also been several reports received of the ransomware viruses gaining entry to the system. The victims of these attacks were mainly companies. There were also several reports about control and command centers (C&C) maintained at Latvian IP addresses:

- ***Dorkbot worm*** (provides backdoor to victim device) controllers;
- ***Hancitor*** (malware that is delivered with infected MS Office documents and is used for downloading of other malware such as bank trojans or ransomware viruses) controllers;
- ***JBifrost*** (Remote Access Trojan RAT Modification) controllers;
- ***Neutrino*** (exploit kit) controllers;
- ***Necurs*** (a zombie network or *botnet* that distributes various types of malware, of which the Locky Encryption Virus is the most known) controllers;
- ***Pony*** (a malware specializing in personal data theft, but is also capable of performing crypto currency, e.g. bitcoin theft) controllers;

- ***NanoCore*** (Trojan that allows the attacker to remotely control the victim's device and collect information about, for example, the passwords that have been entered) controllers;
- ***NetWire*** (Trojan that performs the theft of payment card data) controllers;
- ***Loki*** (malware designed for theft of passwords and other sensitive information) controllers;
- ***Remcos RAT*** (Remote Administration Tool) controllers;
- ***AgentTesla*** (software for keyboard key pressing fixation or *keylogger*) controllers;
- ***Citadel*** (trojan for stealing victim's financial information and emptying bank accounts) controllers;
- ***Gozi*** (spying malware that intercepts network traffic, reads user access data stored in browsers and email clients, and captures keystrokes (keylogger) and information on the screen (screen capture)) controllers;
- ***AZORult*** (trojan for information – stored passwords in browsers, automatically filled in information in various forms of surveys, chat correspondence, programs installed on a device, usernames, files – theft that is intercepted by the malware and forwarded to command center) controllers;
- ***RevCodeRAT*** (trojan for remote access and management of victim device) controllers;
- ***Zbot/Zeus*** (spying malware primarily focused on victim information, online access data, and financial information, but can be adapted to acquisition of any other information or modified to interfere with device's performance or destroy device).

In all cases, holders of devices containing C&C were identified, devices were repaired, and the threat was eliminated.

In December, several reports were received on the email distributed on behalf of the Ministry of Finance with the subject "delayed tax payment" which contained a .ZIP archive acting as the PDF document. By opening this file, the computer was infected with a virus that collects passwords stored on the computer and might encrypt the files on the device to request a ransom for file recovery.

2.6. Compromised devices

Latvia continued to be a target for attackers holding an ideology opposed to that of both NATO and the EU. This was also evidenced by CERT.LV's previously identified malicious software in the IT systems of the Ministry of the Interior of the Republic of Latvia. The malware's technical parameters pointed to possible unauthorized interference by the security services of the Russian Federation. Significant work took place also in 2018 on the analysis of consequences and improvement of instructions.

During the reporting period, CERT.LV also received reports of harmful content on the websites of several public authorities. Websites were experiencing outdated versions of the content management system, which in some cases contained critical vulnerabilities. The webmasters were informed and asked to update the site to the latest version of the content management system. In all cases, the malicious code was deleted from the site, but not all sites were updated, thus exposing them to the risk of re-infection.

On the Saeima Election Day, a report on the attack on the Draugiem.lv portal was received. The portal featured images related to the Russian Federation, and the Russian anthem sounded in the background. The site was temporarily unavailable to users. Upon inspection, it did not reveal any malicious content posted on the site that would be harmful to the user's device – the attack is seen as compromising and defacing the site. The State Police were involved in the resolution of the incident.

During the reporting period, CERT.LV has regularly received reports from companies that have suffered from a ransomware virus attack that has resulted in the encryption of servers and workstations. Typically, attackers have accessed data using the RDP service, by guessing an overly simple access password. Data backup copies are also often destroyed.

2.7. Responsible vulnerability detection

Within the framework of responsible vulnerability detection, 19 reports of cross-site scripting (XSS) vulnerability were received on public authorities' websites.

Vulnerabilities would allow the execution of an attack on the visitor's browser, allowing the attacker, for example, to manipulate the content of the site and cookies, or to use exploits suitable for the browser. CERT.LV coordinated vulnerability prevention.

At the end of September, reports of critical SQL injection vulnerabilities were also received on two public authorities' websites that would allow the attacker to retrieve data freely from the system database. An incorrectly configured PHP installation was found on one of these sites – the source code contained information that would allow the malicious user to take control of the system's email account. CERT.LV coordinated vulnerability elimination.

A letter of gratitude was sent to seven discoverers of the vulnerabilities.

3.

Informative communication events

CERT.LV experts also in 2018 continued to give interviews and answer media questions regarding cyber security and other current topics on TV, radio and press. The main media interest during the reporting period was related to the following topics:

- DDoS attack on the e-health system and e-health data security;
- DDoS attack Latvian on Song and Dance Festival ticket distributor bilesuparadize.lv;
- Security of Latvian Facebook users' data – regarding several worldwide data leakages;
- Security of Yandex.Taxi app and services of Kasspersky;
- Security of the Saeima elections that took place on October 6th.

3.1. Informative events for the media

On March 6 CERT.LV participated in a press conference where the media was informed about the system overload attack of the Latvian Song and Dance Festival ticket distributor bilesuparadize.lv.

3.2. Communication in the digital environment

In 2018, the number of followers on popular social networking platforms *Twitter* and *Facebook* grew steadily:

- At the end of the reporting period the *Twitter* account twitter.com/certlv had **2086** followers.
- At the end of the reporting period the *Facebook* profile facebook.com/certlv **1075** followers.

CERT.LV maintains a website https://www.cert.lv, which publishes information on current threats, recommendations for raising the level of IT security, information on various events and calendar of events. During the year, CERT.LV had 69,589 unique visits or sessions from 42,249 users.

CERT.LV also continued to run the portal for user education www.esidross.lv regularly posting new articles and answering users' comments.

Every month of the reporting period informative cyber security newsletters "OUCH!" were issued in collaboration with the institute SANS, available to every internet user.

4.

Educational events

In 2018 CERT.LV continued to organize educational events regarding cyber security related topics for IT security specialists, employees of state and municipal institutions, students, pupils as well as other interested parties. During the reporting period CERT.LV took part in 127 events and educated 8003 participants.

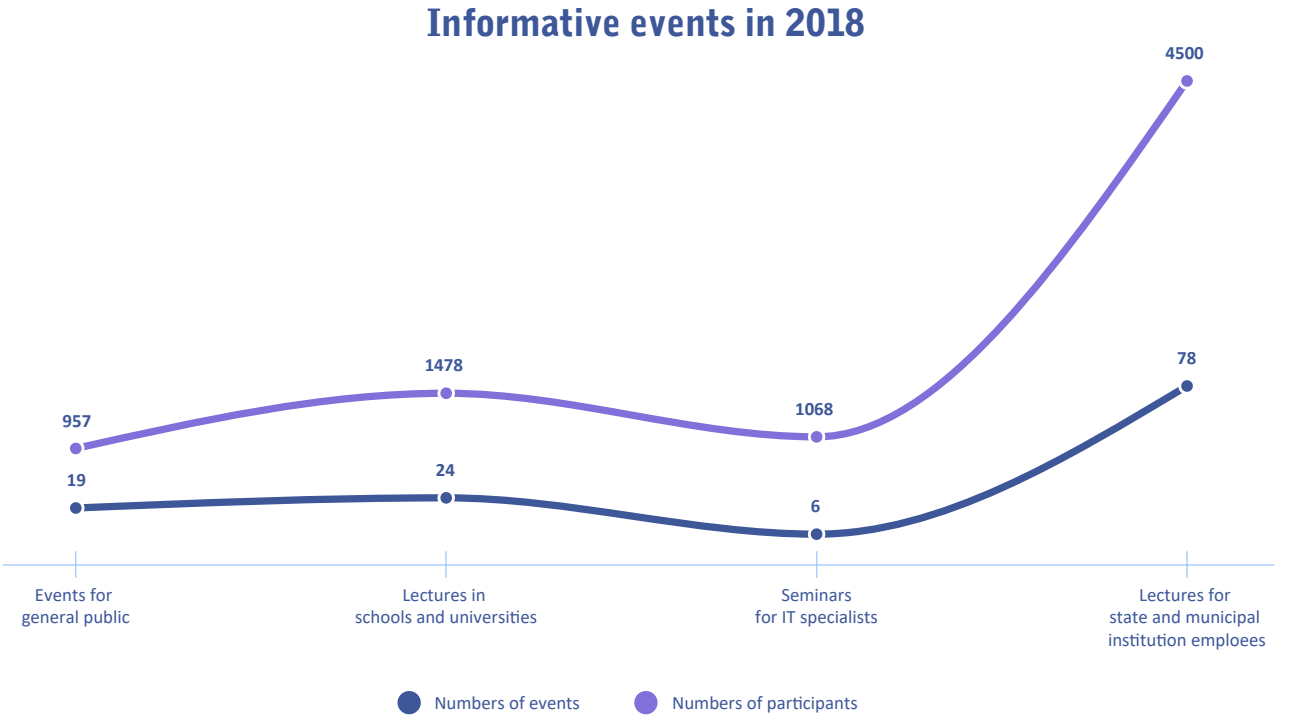

Figure 6 – Number of events CERT.LV took part in and amount of people educated in 2018

The largest event of the year was the annual IT security conference "Cyberchess 2018" which was held in the Radisson Blu Hotel Latvia on October 9th. More than 500 people participated in the event and the livestream of the conference had an additional 2000 unique views.

The conference was organized in collaboration with the *ISACA Latvia chapter*, but *LMT* and *dots*. also this year supported the event. The conference was partly co-financed by the European Union CEF project "Improving Cyber Security Capacities in Latvia" (INEA/CEF/ICT/A2017/1528784).

4.1. CERT.LV organized events for IT security specialists

On March 21st CERT.LV organized a seminar for IT security specialists “Be safe” presenting current issues of IT security that also covered such topics as: effects of vulnerabilities Meltdown and Specter, cloud computing capabilities and risks, implementation of the NIS Directive in Latvia, General Data Protection Regulation and safety requirements, as well as getting acquainted with CERT.LV and NIC.lv DNA firewall project.

On October 9th CERT.LV in cooperation with ISACA Latvia chapter organized IT security conference „Cyberchess 2018”. This year, the conference focused on global cyberspace, threat trends, various tools to mitigate the impact of these threats, and overcoming various levels of technological challenges.

On December 6th CERT.LV organized a seminar for IT security specialists “Be safe” presenting current events at CERT.LV and covered such topics such as changes in IT law, NIS directive, conditions for the implementation of modern e-mail standards in state and municipal institutions, key findings in the e-address implementation phase, consequences of not extending the domain name and how to improve security when employees are working remotely.

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

From March 19th till March 23rd the ninth Digital (formerly known as E-Skills) Week took place in Latvia and throughout Europe. On March 20th, the Digital Security Day was celebrated, and a number of live discussions were organized. CERT.LV representatives participated in the discussion “Security and confidence in the digital environment” and in the event “Cyber Security Night”, which was a high-level expert discussion on national cyber security issues.

On April 5th CERT.LV representative participated in panel discussion „Development of Global Supply Chains and Ensuring Adequate Risk Management of Disruptions" that took place within the framework of conference „Global Transport Security and Safety for a Century".

On April 19th CERT.LV representative hosted the panel discussion „Domains and cybercrime: is there a light at the end of the tunnel?" in the event dedicated to the domain industry of the Baltics „Baltic Domain Days".

On April 25th CERT.LV representative participated in the panel discussion "Justice in Cyberspace", which took place within the framework of the conference "Legal Problems in the Centenary of Latvia: Retrospective and Perspective".

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 at public areas.

In August, CERT.LV representatives participated in the Samsung School for Future project, preparing several video lectures for young people with tips on password building, the use of smart devices and social networks, and privacy protection.

On October 16th CERT.LV representative participated in a practical conference "Cyber security Competence in Latvia: Opportunities and Challenges in the context of Cyber security Strategy of the European Union", discussing the current situation in cyber security competences in Latvia, outlining the problems and opportunities to develop such model of cyber security competence provision that could create preconditions for the technological and management quality of cyber security both in the public and private sectors.

On October 25th CERT.LV representative gave a presentation "Information Security Culture" in the conference DSS ITSEC2018.

On October 29th CERT.LV representative participated in the *Digital Freedom Festival* and EC organized debate "What will ensure the cyber security of the digital future?".

On October 31st CERT.LV representative participated in the conference organized by the *State Chil-*

dren's Rights Protection Inspection - on internet security issues "Opportunities, Growth and Security on the Internet and in Life!", giving a presentation "Digital Environment - How to Protect Yourself".

On November 16th CERT.LV representative participated in the LMT Technology Day, giving a presentation on "Cyber security Challenges in Mobile Networks".

On November 22nd CERT.LV representative presented a presentation on topical issues in the field of cyber security at the international training conference "Combating and Preventing of Cybercrime" organized by the State Police.

4.3. CERT.LV participation in other events and activities

On February 16th CERT.LV representative attended the *Garage48* hackathon as a mentor. The task of the mentors was to help the teams who worked out and developed various cyber security ideas, by giving advice and suggestions for developing the chosen idea.

On June 1st Accenture in collaboration with CERT.LV organized NightHack 2018, where 40 IT security experts applied, but 25 specialists competed for the main prize throughout the night, proving their knowledge, skills and ingenuity.

In cooperation with the State Police and the Safer Internet Center, a mobile app for teenagers "My Safety" was developed. It provides the opportunity to test one's knowledge on Internet safety by completing an interactive test and playing an improvised chat, it also allows reporting harmful and illegal content or problem situations in the app.

During the reporting period CERT.LV provided support to the European Commission in Latvia for the development of digital game #DigiSafe, where young people can test their knowledge on safety and rights on the Internet in an attractive way.

5.

Cooperation with state institutions

5.1. Cooperation with the Ministry of Defense

Regular meetings were held with the State Secretary of the Ministry and regular communications with the National Cyber security Policy Coordination Department.

CERT.LV regularly participated in the Ministry of Defense working group on the implementation of the NIS Directive. As part of this process, CERT.LV, together with the Ministry of Defense, participated in the preparation of amendments to the Information Technology Security Law and Regulation No. 422 of the Cabinet of Ministers (Procedures for Ensuring Compliance of Information and Communication Technology Systems with the Minimum Security Requirements) so that they could be applied to the providers of core services, providers of digital services and critical infrastructure. Proposals for improvement of draft legislative acts were submitted (for example, by clarifying the content of system log files according to security requirements of electronic mail systems).

During the reporting period, on behalf of the Ministry of Defense, research on mobile application Yandex.Taxi was carried out and an informative report prepared with recommended actions for employees of state and municipal institutions. Attention was drawn to the Yandex taxi app after the statement from the Lithuanian Ministry of Defense that it was a threat to national security.

As a result of their contribution to the protection and security of the Latvia, CERT.LV employees Varis Teivāns and Baiba Kaškina were awarded with the honorary diploma of the Ministry of Defense.

5.2. Other cooperation partners

CERT.LV collaborated with the *National Guard Cyber Defense Unit* by participating in various technical training sessions, as well as providing the unit with a virtual training environment for improvement of solving of security incidents.

CERT.LV continued to support the work of the *Security Expert Groups* (SEG), which provides a discussion forum for IT security professionals from both the private and public sector. *SEG* meetings were held once a month.

During the reporting period, CERT.LV was actively involved in the Saeima election security coordination group. It performed activities including the strengthening of the electoral infrastructure during the pre-election period, and ensuring infrastructure monitoring during the elections. The activity observed by CERT.LV in cyberspace during the elections was rated as moderate, not threatening the security of the country or the elections themselves. Several attacks with varying intensity were observed on e-mail systems, websites and network infrastructure, including public sector targets. However, they failed to cause damage or have a tangible effect on the population; they were successfully repelled.

CERT.LV participated in discussions on the creation of a working group also in the preparation to the European Parliament elections in order to take advantage of the experience gained in the Saeima elections to reduce cyber threats.

On December 5, 2018, the State Police of the Republic of Latvia commemorated its 100th anniversary, in the framework of which the anniversary badges "Latvia State Police 100" were presented. Varis Teivāns, Deputy Head of CERT.LV, also received such award for the support provided to the State Police.

6.

International cooperation

During the reporting period, CERT.LV strengthened its cooperation with other CSIRT (Computer Security Incident Response Team) and international organizations in other countries. CERT.LV specialists gave presentations at international conferences, seminars and acquired new skills in technical trainings.

From April 16th – 24th RSA conference was taking place in San Francisco, where CERT.LV representative Karlis Podins together with a researcher Dr. Kenneth Geers gave a presentation on „Cyberwar on a Shoestring: How Kim Jong Un Stole My Malware".

CERT.LV expert discovered four critical vulnerabilities of ICS / SCADA industrial management systems (CVE-2018-10603, CVE-2018-10607, CVE-2018-10609, CVE-2018-10605) and coordinated and supported the developer of vulnerable devices for several months in order to eliminate these vulnerabilities.

The use of these vulnerabilities could lead to unauthorized execution of commands in industrial process management systems, service failure, or code execution on client's equipment. Open vulnerabilities affected the energy sector across Europe and worldwide, where the

IEC-60870-5-104 protocol is used, as well as MartemTELEM-GW6 / GWM equipment, which is mainly used in the Baltic States and Finland.

From November 8th – 10th there was the AIEEEE2018 conference in Vilnius, where CERT.LV representative Karlis Podins with the co-author Arturs Lavrenovs (University of Latvia) presented „Security Implications of Using Third-Party Resources in the World Wide Web".

6.1. Cooperation with the CERT community

During the reporting period, CERT.LV manager Baiba Kaskina continued to perform the duties of the Chair of the TF-CSIRT Steering Committee, attending both face-to-face and remote meetings and organizing the TF-CSIRT work. CERT.LV representatives participated in *TF-CSIRT* and *FIRST* technical workshops and meetings.

In the framework of the CERTs network of the NIS (Network and Information Security) Directive, rep-

resentatives of CERT.LV participates in the “CSIRT Maturity” working group. Within this working group, CERT.LV participated in a peer-review audit in Portugal, Lisbon, where the CERT.PT team (Portuguese Government and National CERT) was audited using the SIM3 (Security Incident Management Maturity Model) and working group guidelines of “CSIRT Maturity”.

CERT.LV representatives participated in the accreditation process of the Cyber security Center of Moldova, which ensured the inclusion of the Center in FIRST (Forum of Incident Response and Security Teams) organization.

From March 14th -16th in FIRST Technical Colloquium in Osaka, Japan, CERT.LV representatives gave two presentations: “Die Hard 104: Attacking and Controlling IEC-60870-5-104 Protocol-Based ICS/SCADA IoT Network Devices.” and “Beyond paste monitoring: deep information leak analysis”.
CERT.LV visited several international meetings within the framework of the CERTs network of the NIS Directive, as well as participated in two working groups - one that improved the CERTs “Terms of Reference” document and the second, which forms the European “Cyber Weather”.

From May 23rd - 25th during the „54th TF-CSIRT meeting” in Warsaw CERT.LV representative gave a presentation „Technical Incident Analysis”.

From May 27th - 30th CERT-EE Symposium in Tallinn CERT.LV representative gave a presentation „Responsible disclosure and ICS/SCADA security”.

From September 26th – 29th in the TF-CSIRT meeting in Vilnius CERT.LV representatives both managed the meeting and gave presentation „How can “know-how” exchange between CERT communication specialists improve our daily lives?”, presenting the role and specifics of public relations in CERT’s activities and inviting to form a separate cooperation group only for CERT’s public relations specialists.
On September 28th CERT.LV representatives in Vilnius met with representatives of CERT institutions in Lithuania CERT.LT and NRDCS to discuss opportunities for development cooperation.

6.2. Cooperation with ENISA

A wide range of collaborations were carried out with the European Network and Information Security Agency (ENISA).

CERT.LV representatives participated in "Cyber SOPEx" training organized by ENISA, aimed at strengthening cooperation between the European CERT units. More than 70 specialists from national cyber security incident response teams and CERT-EU participated in the training.

From June 4th – 9th, CERT.LV representatives participated in the formation, organization, management and execution of cyber security training "Cyber Europe 2018", organized by ENISA. More than 900 cyber security experts from 30 European Union Member States participated in the training this year to tackle the European aviation crisis. In an intensive two-day training scenario, which was the most comprehensive European Union cyber security training so far, staged events took place in a simulated learning environment where participants of the training had to be able to identify and prevent large-scale threats, respond to them, and better understand the cross-border effects of incidents. The total number of scenario management reports sent out within simulated training reached 23,222 emails.

6.3. Cooperation with NATO CCDCoE

CERT.LV in cooperation with the *NATO Cooperative Cyber Defense Center of Excellence* in Latvia organized technical cyber security training "Crossed Swords 2018". Compared to other years, this year's learning scale was much broader, more technically complex and challenging. The training covered a number of geographic locations, involving both IT critical infrastructure operators and military units. More than eighty cyber security experts from fifteen NATO CCDCoE member states participated in the training.

From April 23rd – 27th Cyber security training "Locked Shields 2018" organized by NATO CCDCoE took place, in which CERT.LV was involved both in organizing the exercise, developing an exercise scenario, creating a technical environment, and managing the activities of red flag (attackers) team and also par-

ticipated in exercise. This year, more than 4000 virtualized IT systems and over 2500 different attacks were integrated into the learning environment. Realistic technologies, networks and attack methods were used during the exercise.

CERT.LV, in cooperation with the Cyber Defense Unit, US EUCOM and representatives of the Canadian Armed Forces, formed a national-level blue-flag (defensive) team, and participated in a national-level strategic game, solving complex legal and political issues and communicating it with the media.

CERT.LV for the invested work acquired the status of "Locked Shields 2018" partners and together with the Ministry of Defense and the Cyber Defense Unit received the NATO CCDCoE gratitude on contributions to the organization and conduct of the exercise.

CERT.LV representative Bernhards Blumbergs received a title of NATO CCDCoE Ambassador for high achievements and a significant contribution to the strengthening of cyber security and raising the prestige of the Center and the Alliance. This status is granted for two years and the number of ambassadors is very limited - it does not exceed seven ambassadors.

On April 16th CERT.LV representative in NATO CCDCoE held a „Cyber Executive Seminar" In Tallinn, Estonia.

From May 30th – June 2nd in NATO CCDCoE conference „CyCon" in Tallinn CERT.LV representative Karlis Podins in collaboration with the researcher Dr. Kenneth Geers gave a presentation „Aladdin's Lamp: The Theft and Re-weaponization of Malicious Code".

From September 2nd – 8th CERT.LV representatives taught a NATO CCDCoE course "Malware and Exploitation Essentials" in Tallinn, Estonia.

From November 26th – 28th CERT.LV representatives held a NATO CCDCoE „Cyber Executive Seminar" in Tallinn, Estonia.

From November 23rd – 30th CERT.LV representatives participated in NATO's CCDCoE Cyber Security training "Cyber Coalition 2018", involving around 700 representatives from allied forces, partners, industry and academia to improve collaboration and procedures for information exchange, cyberspace assessment and decision-making.

7.

Implementation of EU projects

7.1. Implementation of the project "Cyber Exchange"

On November 1st, CERT.LV has launched the implementation of the project "Cyber Exchange" (contract with the European Commission No. INEA / CEF / ICT / A2017 / 1528784) (hereinafter - Cooperation Project) approved in 2017 CEF Telecom-Cyber Security call.

In November, CERT.LV representatives attended a Cooperation Project opening meeting organized by the project coordinator - CZ.NIC, z. s. p. o., which took place on November 5th in Vienna, Austria. The meeting launched the development of a cyber security experts' exchange plan and other project activities.

7.2. Implementation of the project "Improving Cyber Security Capacities in Latvia"

On September 1st, CERT.LV has started implementation of the project "Improving Cyber Security Capacities in Latvia" (contract with the European Commission No.INEA / CEF / ICT / A2017 / 1528784) (hereinafter - the Project) approved in 2017 CEF Telecom-Cyber Security call.

The project provided funding for the necessary international co-operation - CERT.LV staff's business trips to conferences and participation in various courses were co-financed by the project. The development and customization of the "Deep Analysis System" was also launched.

On September 20th, CERT.LV participated in an online meeting on the development and use of the co-operation platform MeliCERTes within the framework of the project "Improving Cyber Security Capacities in Latvia".

From September 23rd – 26th, CERT.LV representatives participated in SIM3 auditor training in Vilnius

within the framework of the project “Improving Cyber Security Capacities in Latvia” to obtain the SIM3 auditor certification.

On October 9th, the cyber security conference “Cyber Chess 2018” was held, which was co-funded by the project.

Other tasks

Work on the implementation of the CERT.LV and NIC.lv DNS RPZ (Domain Name Service Response Policy Zone) or DNS Firewall project was launched. The project provides an opportunity to protect users from malicious content on the Internet, which is linked to incident identifiers (domain names, IP addresses, etc.) already known to the cyber security authorities. Project implementation has started in 4 institutions. There have been already several cases within the project, where active protection has prevented equipment from becoming infected.

The report was prepared by:

CERT.LV public relations group manager Liga Besere
phone: +371 67085888
e-mail: liga.besere@cert.lv
web: https://cert.lv/en

Published on May 30, 2019