

2019

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.

Contents

<i>Summary</i>	<i>4</i>
<i>1. Processing of Incidents</i>	<i>9</i>
<i>2. Most Significant Incidents in 2019</i>	<i>17</i>
<i>2.1. Denial of Service (DoS un DDoS)</i>	<i>18</i>
<i>2.2. Phishing and Personal Data Scams</i>	<i>18</i>
<i>2.3. Fraud</i>	<i>19</i>
<i>2.4. Intrusion Attempts</i>	<i>20</i>
<i>2.5. Malware</i>	<i>20</i>
<i>2.6. Compromised Devices</i>	<i>21</i>
<i>2.7. Vulnerabilities and Configuration Insufficiencies</i>	<i>21</i>
<i>3. Responsible Vulnerability Disclosure</i>	<i>23</i>

4. Penetration Tests	25
5. Informative Communication Events	27
6. Educational Events	31
6.1. International Cybersecurity Conference Cyberchess	33
6.2. Organised Events for IT Security Experts	37
6.3. Presentations and Events on IT Security for Public Education	37
7. Strategic Collaboration in Latvia	40
8. International Collaboration	44
9. Implementation of EU co-funded projects	48
8. Services to strengthen Cyberspace in Latvia	51

Summary

It was relatively calm in Latvian cyberspace during 2019. Major and destructive events, with significant impact, were not detected. However, medium and small-scale incidents kept Latvian internet users on their toes, regularly testing their awareness and vigilance. Fraud campaigns, with and without media attention, took place weekly. For example, targeted campaigns for *Smart-ID* users, campaigns for victims of fake crypto-currency stock markets, campaigns to lure into fake online stores offering goods with incredible discounts, and others.

All these actions showed that the growing purchasing power of the average Latvian internet user in Latvian cyberspace is becoming more interesting for attackers and fraudsters, and we see that more resource and time is being invested in attracting would-be victims. An example of this is the preparation of grammatically correct and plausible messages in the Latvian language.

The last two years have shown more targeted campaigns aimed at small and medium enterprises (SME). Compromised business e-mails, E.g. E-mails to finance departments from fake managers requesting immediate payments is the most common type of attack. To inform SMEs and make them more aware that they can also be a target of cyber attackers was the goal of several educational events explicitly organised and focused on this target group. Organised together with NIC.LV and the Latvian Chamber of Commerce and Industry, these will continue in 2020 as well.

While continuously working on educating and informing society on cybersecurity, CERT.LV organised or took part in 122 events reaching out to 7645 people. The highlight of the year was the international cybersecurity conference *Cyberchess*, which brought together 630 participants from 30 countries. More than 4,000 users viewed the live stream from the conference. *Cyberchess* took place with support from the Connecting Europe Facility funding of the European Union in collaboration with *ISACA Latvian Chapter* as well as from *LMT* and *.dots*.

In May 2019, CERT.LV successfully concluded the TF-CSIRT/ Trusted Introducer recertification process. It once again confirmed the high-level technical, organisational maturity and preparedness of the CERT.LV team. CERT.LV is one of the 32 certified teams of TF –CSIRT/ Trusted Introducer and will continue to be certified for the coming three years until the next recertification.

Several CERT.LV Team Members were highly praised by State-level awards in 2019:

- ▶ For special merit to the benefit of the Republic of Latvia, Baiba Kaškina, the General manager of CERT.LV was awarded the Order of the Three Stars.
- ▶ The Ministry of Defence awarded CERT.LV Project Manager Egils Stūrmanis, PR Team Leader Līga Besere and IT Security Specialist Kristiāns Tetters Certificates of Gratitude for their contribution and support in strengthening the security capacities of Latvia.
- ▶ In December, the Latvian State Security Service issued a Certificate of Gratitude to the Deputy Manager of CERT.LV Varis Teivāns for successful collaboration in strengthening security.
- ▶ CERT.LV representatives Uldis Koškins and Jānis Narbutis received an award for their investment and dedication to strengthening cybersecurity in Latvia.

The overall capacity of the CERT.LV Team was reinforced after the leading researcher, Bernhards Blumberds, attained a PHD Degree from the Tallinn Technical University with his dissertation titled, Specialized Cyber Red Team Responsive Computer Network Operations.

CERT.LV sees the values of responsible and safer cyberspace for the future; therefore, on 12 October 2019, CERT.LV joined the [Paris call](#). The Paris call of trust and security in cyberspace has nine core principles, which all strive to increase trust and security online while stressing the importance of the protection of human rights and highlighting the responsibility of countries in respecting international norms online.


When forecasting a prognosis for 2020, CERT.LV foresees that even more elaborate and active attempts of attacks using social engineering methods can be expected. One should never underestimate the value of basic knowledge in how to protect oneself, and your devices, as well as compliance with good practice. As IT technologies become more secure, strictly technical cyberattacks without any elements of social engineering -are too becoming less common because of their cost and low level of effectiveness.

It can be expected that attackers will continue to target IoT (Internet of Things) devices that have either been recklessly exposed online or whose security standards do not meet the potential, modern-day cyber threats.









1.

*Cyberspace
Overview*

Each month CERT.LV gathers and summarises cyberspace information on threatened IP addresses in Latvian cyberspace. The cyber incident taxonomy developed within the eCSIRT.net project is used in statistical form. All threats registered by CERT.LV are listed together, dividing by the type of threat (e.g. malware, intrusions, fraud), as well as by the type of infection (e.g. *Confiker*, *Zeus*, *Mirai*) and vulnerability (e.g. *Opendns*, *Openrdp*).

During the reporting period, CERT.LV registered on average 100 000 – 105 000 unique, vulnerable IP addresses monthly.

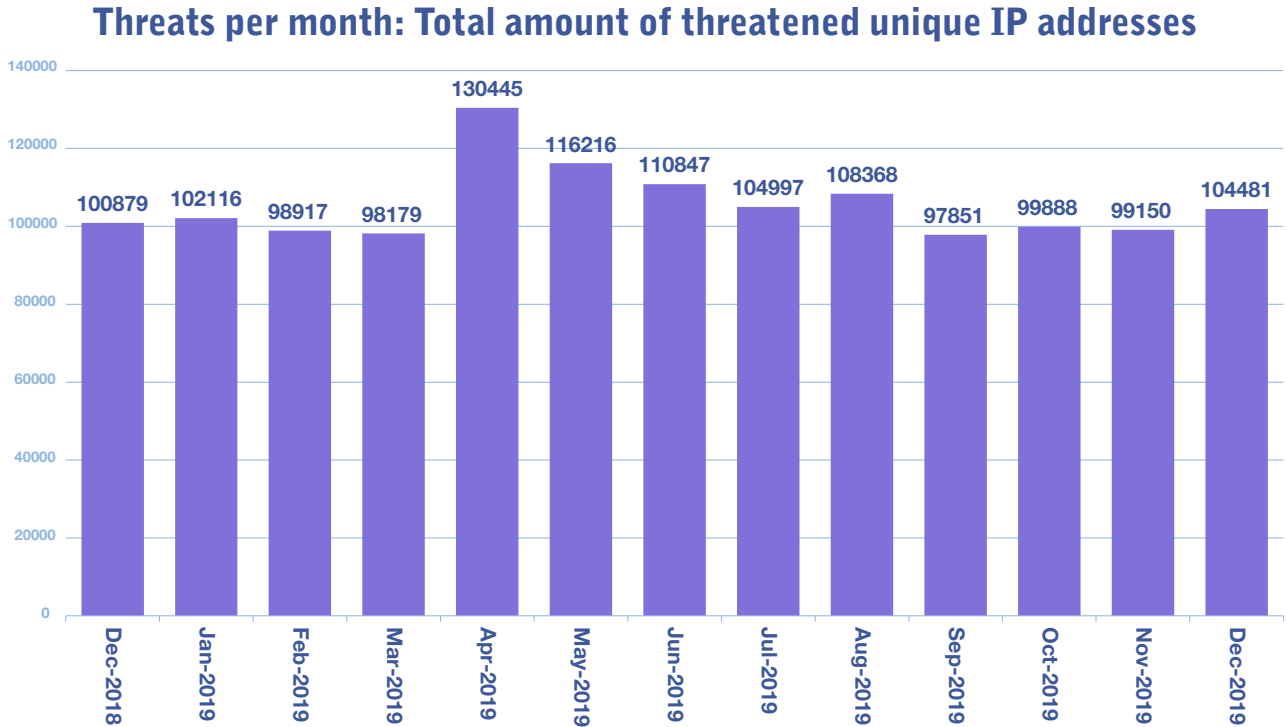


Figure 1 – Monthly registered unique IP addresses in 2019 by CERT.LV

Threatened IP addresses per quarters in 2019

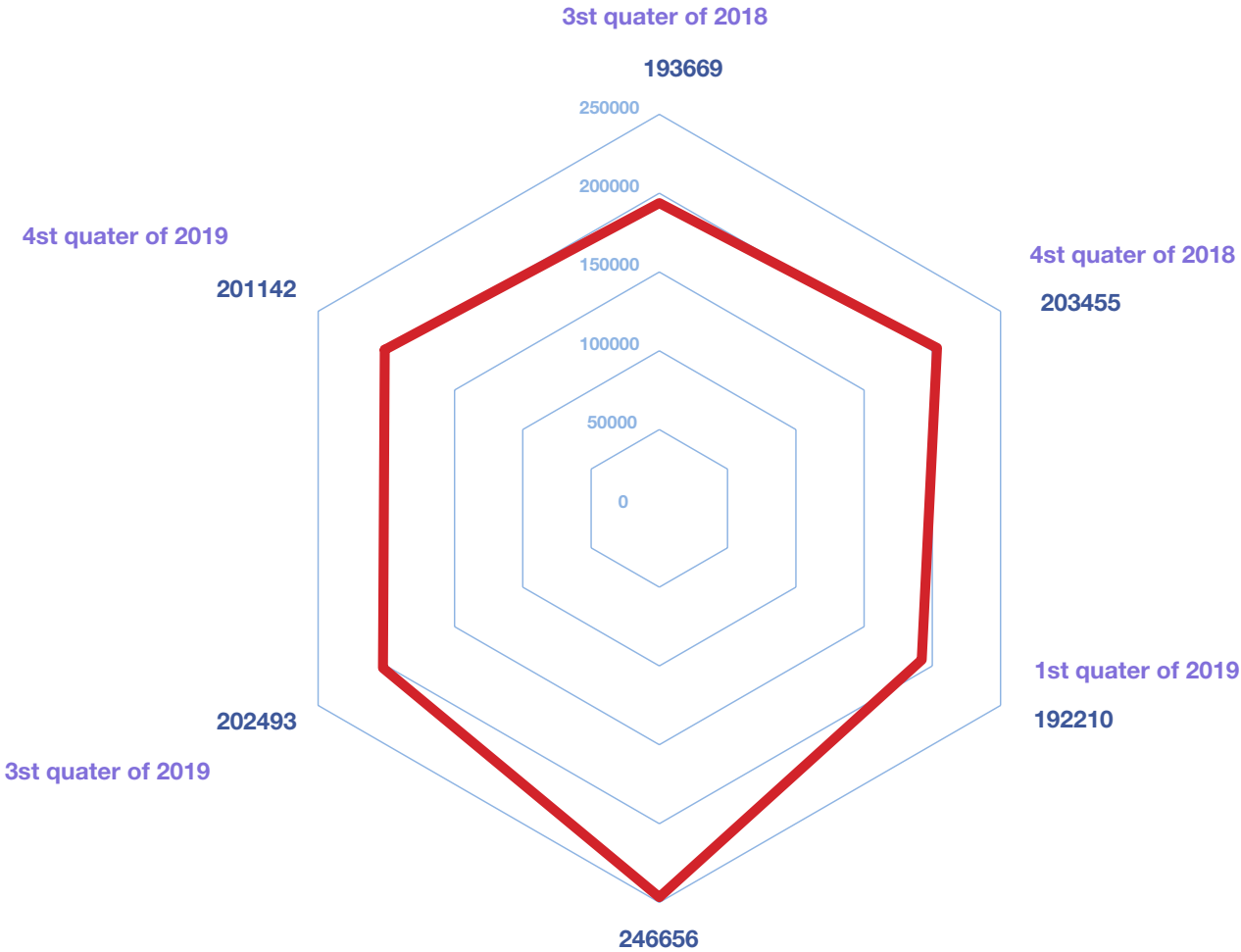


Figure 2 – Registered threatened unique IP addresses per quarter in 2019

Same as last year – the top three types of threats were – vulnerabilities, malicious code, and intrusion attempts.

Category *Other* includes consultations on cybersecurity to both – public institutions and individual users as well as the processing of information, which is not related to any of the other categories.

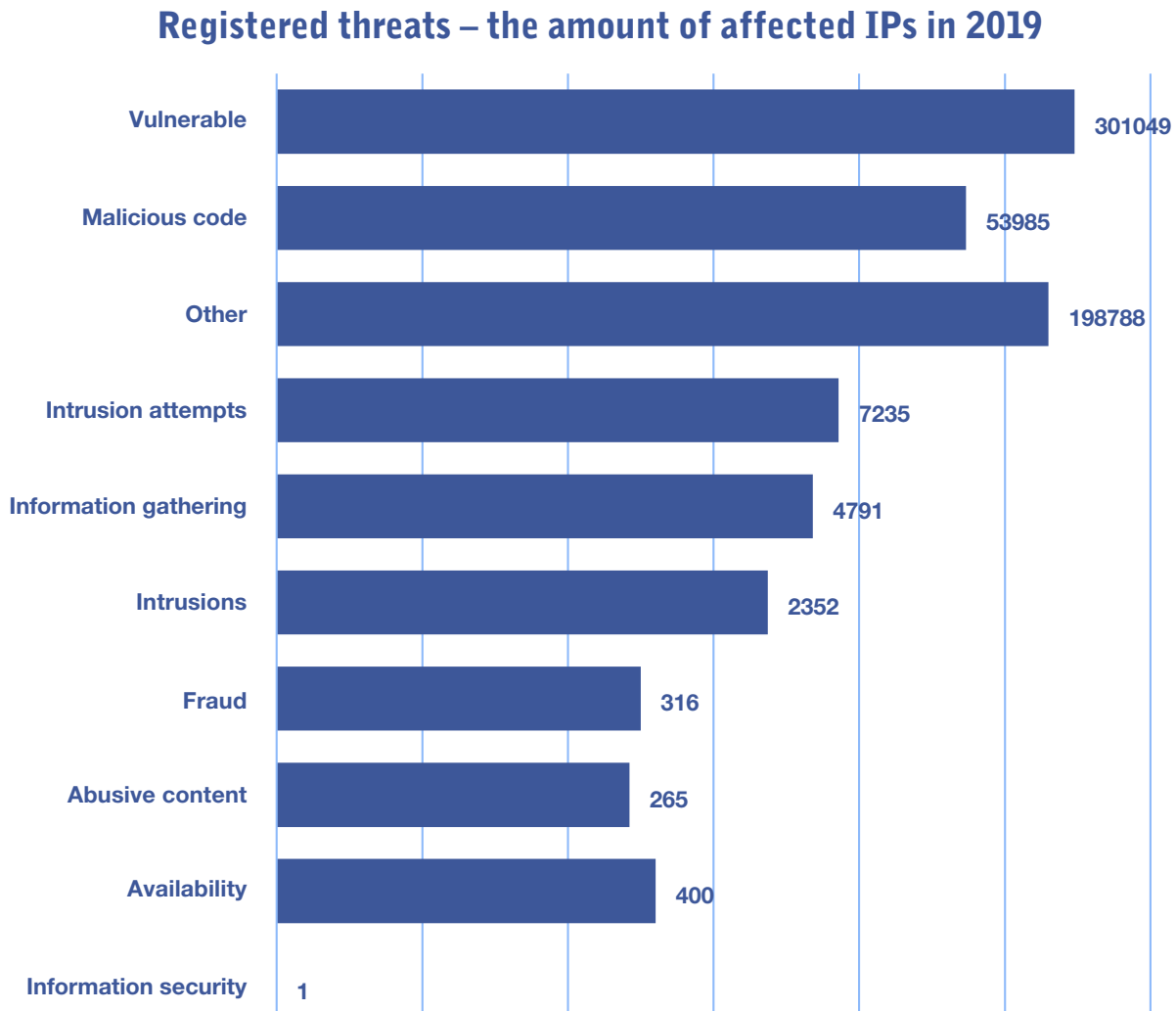


Figure 3 – Threatened unique IP addresses registered by CERT.LV by type of threat in 2019

Top Malicious Code 2019

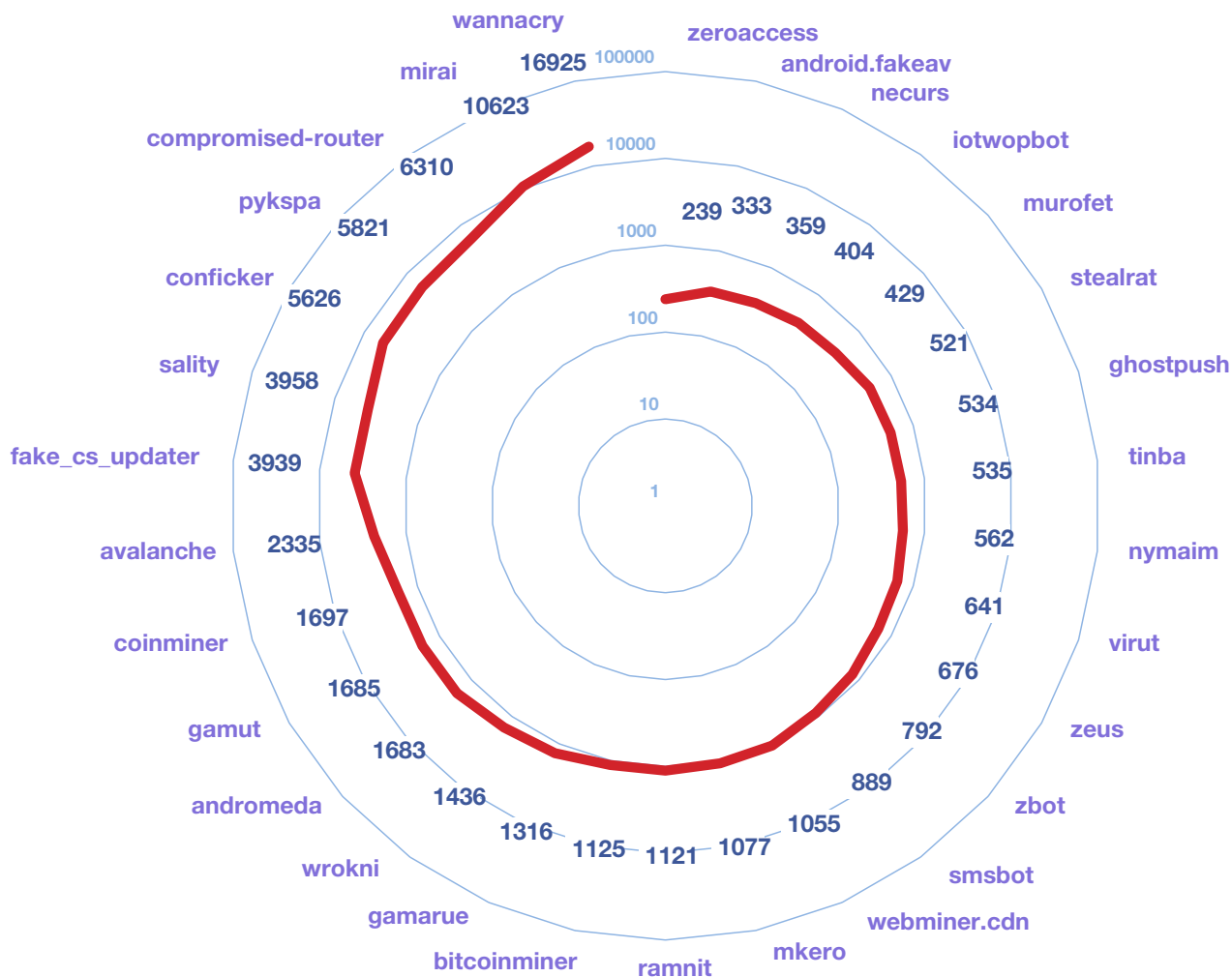


Figure 4 – Total number of CERT.LV registered threatened unique IP addresses in 2019 with the type of threat – malicious code

WannaCrypt or *Wannacry*, which is ransomware, ranked first in the malware chart, keeping its position from last year. It affects devices with the *Microsoft Windows* operating system and spreads through a vulnerability in the SMB protocol. The effects and distribution of the malware can be prevented by installing *Microsoft*-made software updates that are available even for Windows versions that are no longer supported, such as *Windows XP* and *Windows Server 2003*. It has yet to be confirmed whether 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 the infected devices is smaller. However, this does not mean that the threat is insignificant or noteworthy, primarily as 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.

Second place has been taken by *Mirai*, a malware that threatens inadequately protected devices of the Internet of Things (IoT). The most commonly infected devices are smart TVs, internet routers, or other similar devices that are connected to the internet without changing the default user-name and password set by the manufacturer. These default passwords are widely known, and their use puts the device at risk of attack.

Conficker has kept its position in the top of most widely spread malware, even though it is a long-known and relatively simple “curable” one – all that is needed is regular updating. This most likely indicates that there are old, outdated devices connected to the internet, subject to high risk of attack, as well as a lack of understanding on the importance of cybersecurity measures being in place amongst internet users.

Top vulnerabilities 2019

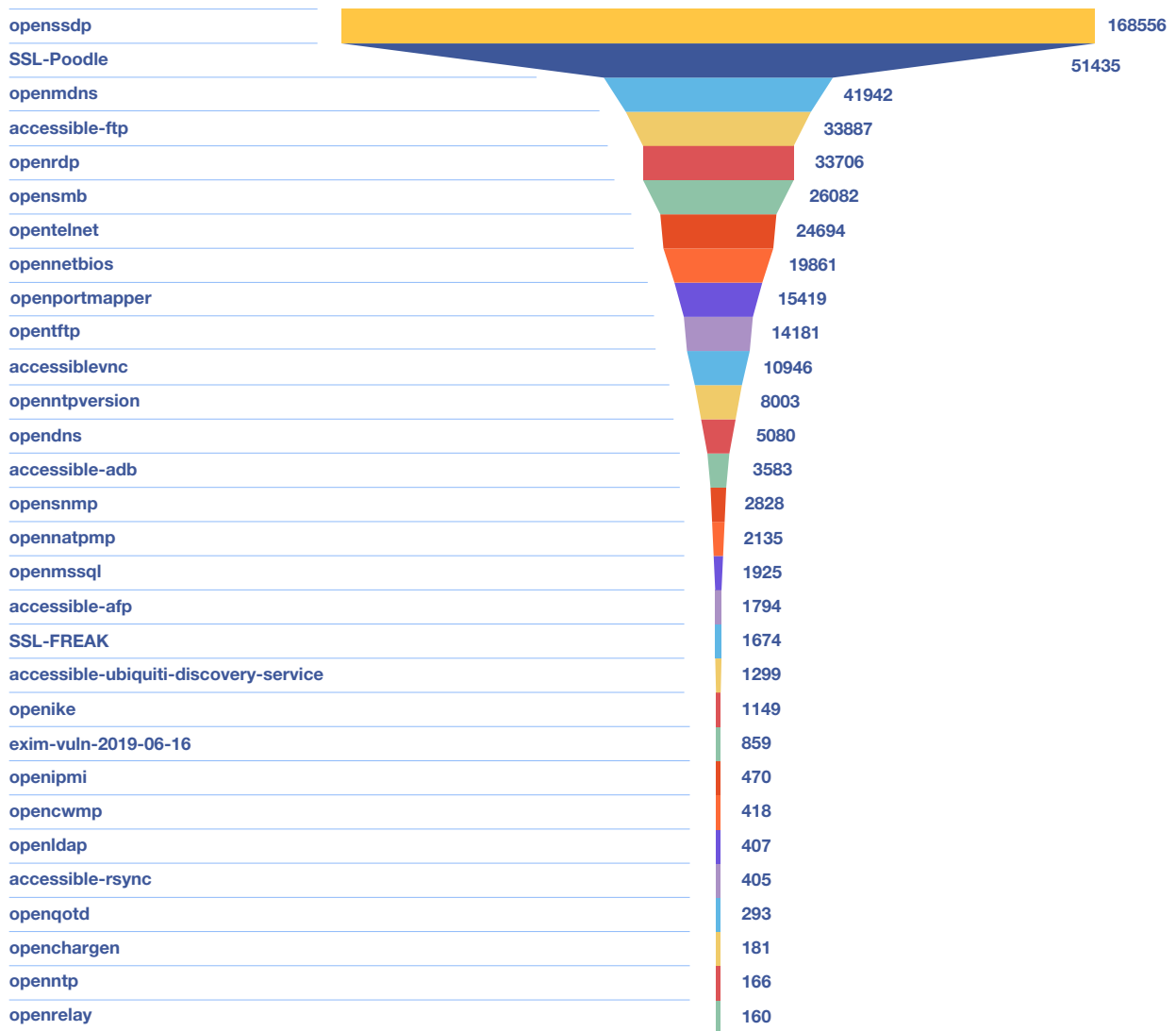


Figure 5 – Number of threatened unique IP addresses registered by CERT.LV in 2019 with the type of threat – vulnerabilities.

Open SSDP ranked first in vulnerabilities – devices, with insecure configuration potentially open to becoming part of large-scale *Denial of Service (DoS)* type of attack. *Simple Service Discovery Protocol (SSDP)* is built into many network devices, allowing these to easily “find each other”. Often, due to incorrect configuration of *SSDP*, this functionality is not even accessible by the user, while allowing the device - without the knowledge of the owner/user to become a powerful weapon in the hands of the attackers.

Openrdp vulnerability, which has lost its position by two places since last year, takes fifth place at the top of vulnerability. (see Figure 5). It indicates activated remote access or *RDP (Remote Desktop Protocol)* that is available from a public network and poses a threat if a simple password is used and access is not restricted. For example, by 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, and even financial loss, by encrypting the contents of one or more devices (workstations, servers), after which a recovery ransom has been demanded. Within the scope of the initiative, *Responsible ISP* CERT.LV continually informed end-users about the potential threats and provided recommendations on how to prevent them.

CERT.LV also lists cases of hacked and defaced websites. In 2019, 132 websites were hacked and defaced. In five cases, the website was hacked repeatedly during the year. Out of the compromised websites 120 used *Linux*, 10 used *Windows*, and in two instances *FreeBSD* operating systems were used.



2.

***Most Significant
Incidents in
2019***

During the reporting period, CERT.LV cooperated with governmental organisations, local municipalities, banks, internet service providers and other organisations handling incidents at various threat levels. The report summarises the most significant incidents that mark annual trends.

2.1. Denial of Service (DoS and DDoS)

Significant *Distributed Denial-of-Service (DDoS)* attacks were not observed in 2019. There were many cases of DDoS attacks; however, they did not affect the accessibility of services, as the infrastructure was protected by either the *anti-DDoS* solutions set up by different service providers or Latvia State Radio and Television Center (LVRTC). It is important to note that there were several cases of Denial-of-Service that were not caused by external actors, but rather by legitimate requests from users.

2.2. Phishing and Personal Data Scams

In general, phishing was active throughout the year. Most of the campaigns were aimed at defrauding e-mail access data, banking and international payment system as well as *Smart ID* access data, not forgetting the most popular social networking sites and user information as well—e.g. on *Facebook* or *Instagram*.

In 2019, tailored attacks on public administration employees were observed; in one of the cases, the e-mail sent contained a script that allowed gathering of the user information once the e-mail was opened.

CERT.LV remained active in informing internet users to be aware and vigilant as soon as new phishing campaigns were reported to CERT.LV.

2.3. Fraud

In terms of fraud, 2019 was a very active year. Active campaigns targeting Latvian internet users were seen on a regular basis.

Starting with several waves of sextortion campaigns – where the attackers claimed that they have hacked the user's device and attained sensitive user information requesting a redemption fee for them not to share these materials online – leading to fraudulent lotteries – where well known Latvian brand names and prizes in the form of latest smartphones or significant amounts of money were used as bait – 2019 did not go without fraudulent websites and fake online stores. It also saw *money lenders* who, before granting the loan, called on the borrower to make various payments for alleged loan transfer commissions, and so on.

The most highlighted incidents, which also gained media attention, were the fake announcements of Latvian celebrities investing in cryptocurrencies. Such websites claimed that celebrities had made significant profits from participating in these investment schemes. It is known that similar campaigns took place in other countries and victims varied from international superstars, actors, singers to politicians.

The calls from *Finance Specialists* continued in 2019 too. It is known that, in one case, the amount of loss exceeded 80 000 EUR. During these calls, *the Specialists* encouraged people to invest in un-licenced platforms, giving the impression, initially, that a profit is being made, then later promising the opportunity to recoup the initial *investment*.

Enterprises, especially SMEs, were not forgotten either and in 2019, more and more innovative approaches were seen in compromised business e-mails and e-mail spoofing. CERT.LV has information on one enterprise that suffered twice from this type of fraud, and only after the second time of losing a significant amount of money did it implement the suggestions provided by CERT.LV to avoid e-mail spoofing.

2.4. *Intrusion Attempts*

Information on intrusion attempts was on the radar of CERT.LV throughout the year; however, the intensity was low. There were identified intrusion attempts from outside of Latvia targeting servers of governmental organisations and local municipalities. CERT.LV received information from international colleagues regarding automated attacks on servers of a governmental organisation in another country from the Latvian IP addresses.

Methods for implementing intrusion attempts varied significantly. CERT.LV witnessed a wide range of methods, starting from automated password guessing using *IMAP* service, denial of service attempts by using *TCP* requests and data extraction attempts using *SQL* injections.

2.5. *Malware*

In 2019 Malware was distributed to achieve two objectives – to either obtain information or to make a profit. To get the information malware, spread by attackers, was designed to steal users' private information, e.g. passwords. To gain from this, the malware encrypted the data, server or the device and requested a ransom for its decryption. The amounts differed based on the encrypted data and the chosen victim – private person, enterprise or state organisation, but none were spared. In the case of backups, in most cases, access to the data was possible without paying the ransom, but there were a few cases, where no backups existed and paying a ransom was the only way to regain the data.

The best practice also endorsed by CERT.LV is never to pay a ransom. It does not guarantee that the data will indeed be retrieved and also gives an indication to the attacker that this victim is willing and able to pay. This may well result in repeated attacks and provide financial support for such malpractice to be continued.

Methods of spreading malware were different, but mostly via e-mails, often using grammatically correct Latvian and containing an attachment where the actual extension of the filename was very well disguised (e.g., *PO#august_pdf.img* where .IMG file is masked as .PDF). The subject of the e-mail was also deliberately chosen, so as to make it look as normal as possible, e.g. outstanding invoice, purchase order, etc.

Towards the end of the year, there was malware detected on an online store that was stealing customer credit card data. The enterprise was informed by CERT.LV and by close collaboration, the issue was resolved swiftly. The enterprise took all the necessary measures, informing the affected users.

2.6. Compromised Devices

Cases of compromised devices affected everyone – starting with individual users, onto enterprises and finally to governmental organisations and local municipalities. In several cases, of *Atlassian Confluence* vulnerability was abused, in the same way as the incorrect configuration of devices connected to the internet, allowing attackers to get access to sensitive information. There were cases whereby becoming a super-user, the attacker used the compromised device to modify the server to send out SPAM. There was a case reported by one Latvian online media portal, where their website was hacked, and some content on the website was changed – the site swiftly deleted the fake content and informed users about the compromise.

2.7. Vulnerabilities and Configuration Insufficiencies

The Latvian cyberspace was not spared from vulnerabilities and configuration insufficiencies in 2019. CERT.LV kept it high on the list of priorities to inform internet users about all known vulnerabilities, including providing recipes on how these can be cured.

The most significant vulnerabilities, affecting large numbers of users in Latvia, included the critical vulnerability *Confluence CVE-2019-3396*, as well as the Oracle server operating system vulnerability *CVE-2019-2729*. During the reporting period, CERT.LV consulted several website owners regarding identified configuration insufficiencies, allowing the repeatable use of authentication markers or by avoiding the set authentication mechanisms altogether. At the end of the year, an organisation was consulted on how to implement *DMARC – Domain-based Message Authentication, Reporting & Conformance (including SPF and DKIM)* technology to improve the protection of their e-mail systems and avoid receiving e-mails from their own e-mail addresses as well as other types of SPAM.

3.

***Responsible
Vulnerability
Disclosure***

CERT.LV is advocating for responsible vulnerability disclosure and is encouraging any IT security specialists and researchers to inform CERT.LV about detected vulnerabilities. These allow us, as the Information Technology Security Incident Response Institution of the Republic of Latvia, to coordinate the actions taken to mitigate potential risks and, thereby, improve the protection of Latvian cyberspace.

In 2019 CERT.LV received several reports on vulnerabilities detected in the resources of governmental organisations or local municipalities. With the help of these reports, several websites of public authorities were protected from *cross-site scripting (XSS)*. These vulnerabilities would allow for the execution of an attack from 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. Another report allowed the identification of a website hosted on an insecure *Nginx* server version creating excessive *CPU* processor load and excessive usage of memory.

CERT.LV encourages responsible vulnerability disclosure also in 2020. To do so, please e-mail us at cert@cert.lv or read more at [web site](#).



4.

***Penetration
Tests***

A Penetration Test is an important step in making sure that a developed online resource, e.g. website, database or online system meets the security requirements. During the course of 2019, CERT.LV conducted many penetration tests for national-level information resources. Most of the tests discovered significant vulnerabilities and shortcomings. In all cases, the holder of the tested resource received a detailed report that contained information on the results of the test as well as how to prevent discovered vulnerabilities and shortcomings.

Most commonly discovered vulnerabilities included:

- ▶ *Cross-site scripting (XSS)* vulnerabilities, which expose resources to the risk of retrieving information;
- ▶ Usage of an outdated content management system (*CMS*), exposing the website to critical vulnerabilities and automated cyberattacks;
- ▶ Lack of correct resource configuration, allowing attackers to attain information on the technological solutions used or causes disproportionate traffic and data load on the system.



5.

*Informative
Communication
Events*

CERT.LV had active communication with media, TV, radio, newspapers and online news portals throughout the year.

Key topics of focus for media included security of smart devices and applications, current fraud lotteries and phishing campaigns. CERT.LV also provided commentaries on how the transposition of the [NIS Directive](#) in Latvia has affected CERT.LV operations as well as on the security of the EU Parliament elections and the conference *Cyberchess 2019*.

The central source of communication for CERT.LV is its website www.cert.lv. Information on current threats, recommendations for raising the level of IT security, information on various events and calendar of events are all published there. **In 2019 there were a total of 66,518 unique visits or sessions by 39,335 users.**

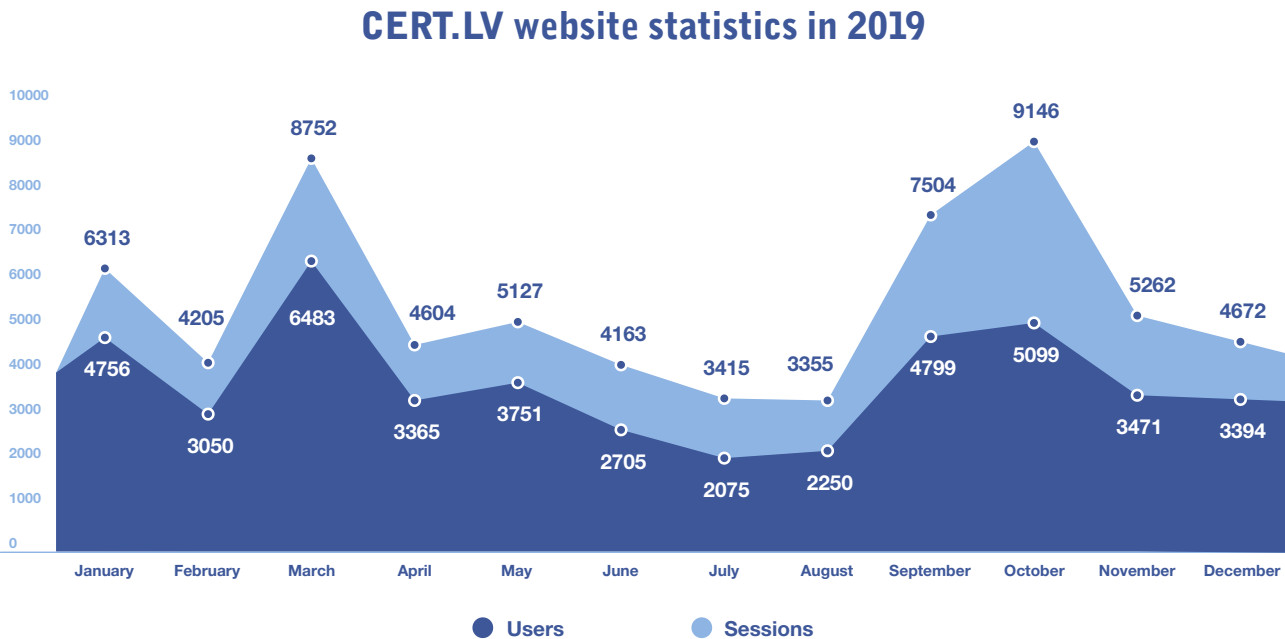


Figure 6 – website statistics of CERT.LV in 2019

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

In every month of the reporting period informative cybersecurity newsletters *OUCH!* were issued in collaboration with the SANS Institute. Every month, *OUCH!*, in a language easily understandable to any internet user, hosts an internationally recognised cybersecurity expert who comments on current trends in cyberspace as well as provides practical tips and advice that can help any user to improve their security online.

2019 was also a year of stable growth for followers on social media platforms *Twitter* and *Facebook*:

- ▶ *Twitter* account: twitter.com/certlv number of followers at the end of the reporting period was 2301.
- ▶ *Facebook* account: facebook.com/certlv number of followers at the end of the reporting period was 1306.

CERT.LV social media in 2019

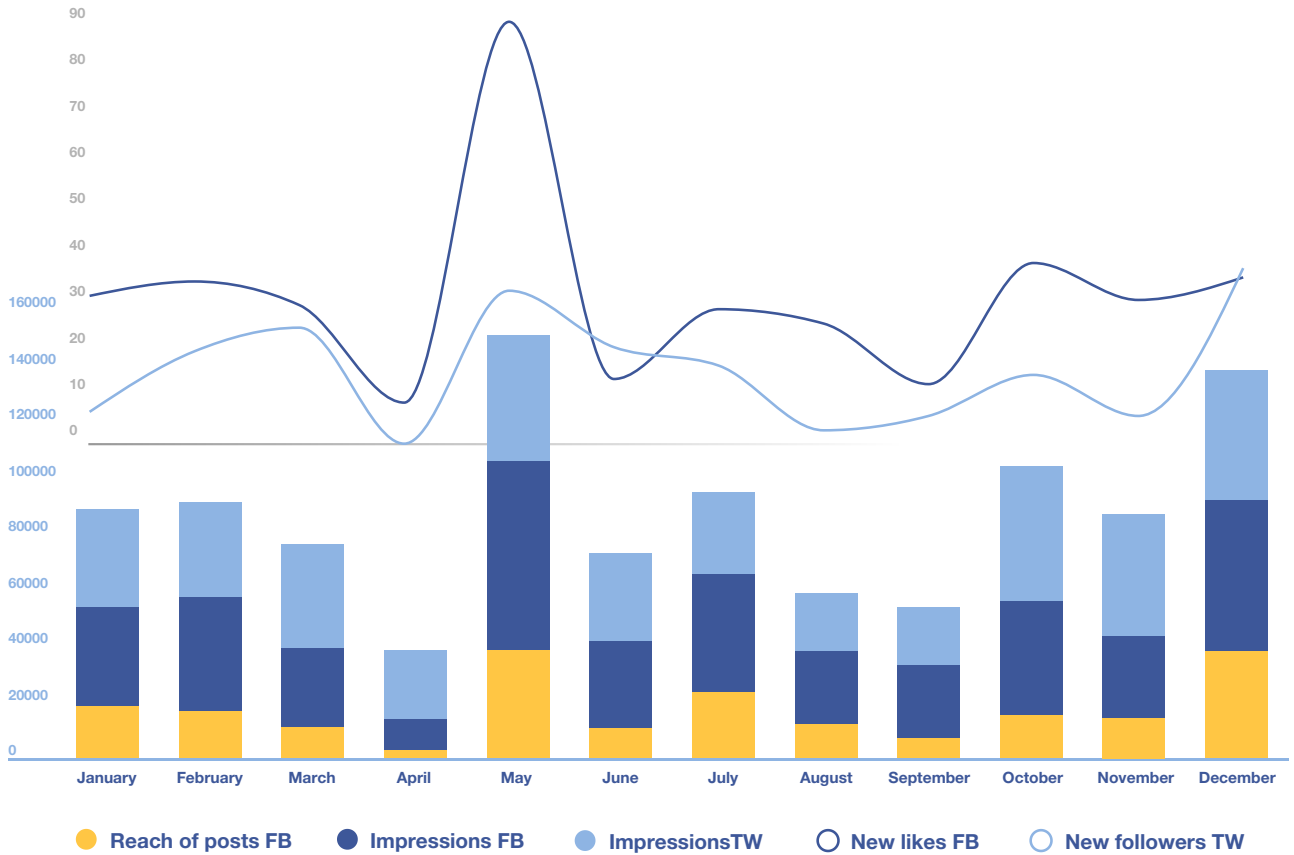


Figure 7 – CERT.LV social media profile statistics in 2019



6.

*Educational
Events*

In 2019 CERT.LV continued actively organising and taking part in educational and informative events on cybersecurity. Target audiences included IT security experts, employees of governmental organisations and local municipalities, students, pupils and other members of the general public. There were a total of 122 events reaching and informing 7 645 participants in 2019. CERT.LV is also an active supporter of events such as the *Safer Internet Day* (February), *Digital Skills Week* (March) and *Digital Security Month* (October).

Educational and informative events in 2019

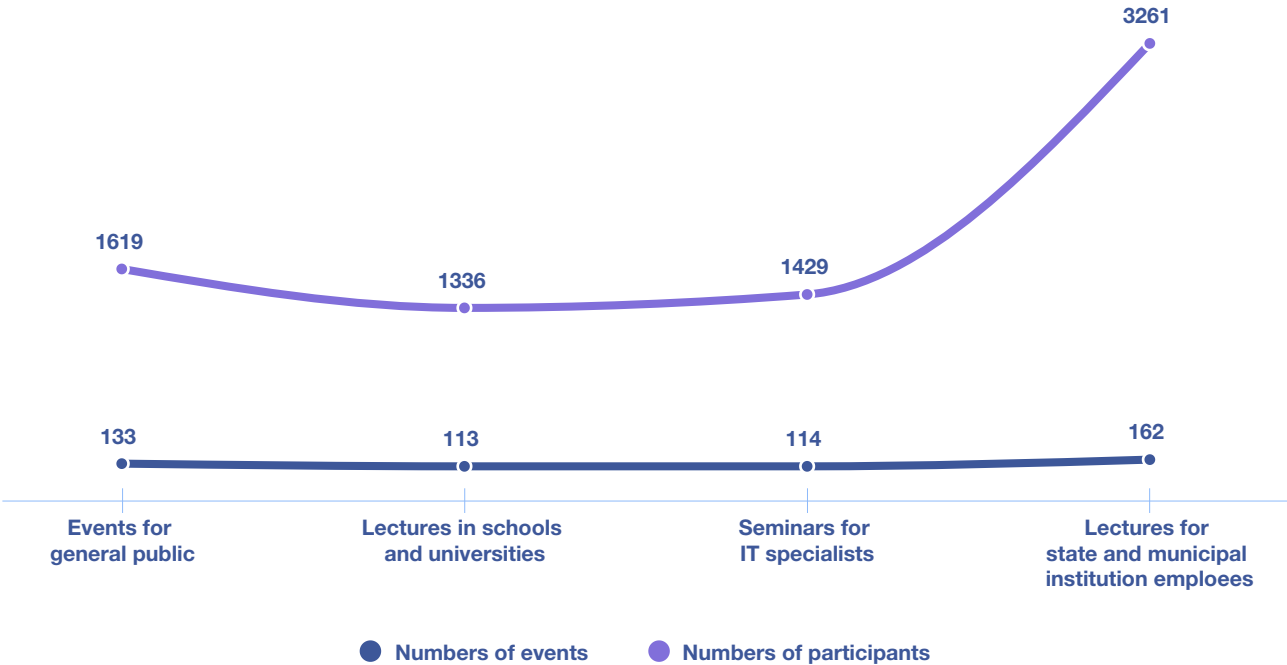


Figure 8 – Number of events and audience reached in 2019

6.1. International Cybersecurity Conference Cyberchess

The Year's largest event organised by CERT.LV was the international cybersecurity conference *Cyberchess 2019*. It was opened by the President of Latvia, Egils Levits, and Minister of Defence, Artis Pabriks, and took place in the *Radisson Blu Hotel Latvija* between 2nd and 3rd October 2019. It brought together 630 participants from more than 30 countries, and more than 4000 users viewed the live stream of the conference. This year's topics for included the evaluation of cyber-risks, monitoring of cyberspace, technological challenges and innovative methods to protect data, devices and infrastructure online. The conference is the place where latest trends in cybersecurity are discussed in terms of technological, political and technical security aspects in cyber-operations as well as the ever-growing usage of social-engineering methods in cyber-attacks.

Presentations and recordings from the conference can be still viewed online both on the website www.cert.lv as well as at straume.lmt.lv. A short video summary is [accessible here](#).

During the conference, an open *CTF (Capture the Flag)* competition took place. *CTF* is a special cybersecurity competition where the participants face different cybersecurity challenges – cryptography, binary code, network analysis, etc. There were more than 90 registered teams. From these, 46 teams were active and got a minimum of 100 points (maximum possible points: 9100). CERT.LV was delighted to see also a team of students from *Saldus Tehnikums*, who bravely competed with IT security professionals from Latvia and abroad.

The conference was organised in collaboration with the *ISACA Latvian Chapter*. *LMT* and *dots.* companies were amongst the key supporters also this year. The conference was co-financed by the Connecting Europe Facility of the European Union under the Project: *Improving Cyber Security Capacity in Latvia*.

Cyberchess 2019

Cybersecurity Conference
2 - 3 October



dots.

CYBECIRCLE



Cybersecurity Conference
2 - 3 October



Cyberchess CTF award ceremony

Cyberchess

2019

#kiberšahs 2019



6.2. Organised Events for IT Security Experts

In addition to the annual cybersecurity conference, *Cyberchess*, for which the target audience was IT Security Experts, there were several other events organised by CERT.LV for the same audience throughout the year. Seminars *Be Safe* – (In Latvian *Esi Drošs*) was one of those – organised twice a year in spring and autumn – *Esi Drošs* brings together on average 100 to 150 participants – IT Security Experts primarily from governmental organisations and local municipalities. *Esi drošs* is streamed online, and presentations and videos are available from the website www.cert.lv.

In March: Organised as part of the *Digital Skills Week*. Topics for the seminar included *DNS over HTTPS*, the safety of websites and safer usage of mobile cyberspace in governmental organisations and local municipalities. Additionally, a panel discussion on the challenges and implementation of the *Digital E-Address* was held.

In November: Participants were reminded of the current trends and threats happening in cyberspace, issues with infected IT systems, best practice of e-mail system maintenance as well as the involvement of Operators of Essential Services and Digital Service Providers in the Latvian Cyberspace.

6.3. Presentations and Events on IT Security for Public Education

Each year, CERT.LV takes an active role in educating society at large on IT and cybersecurity, both by organising and taking an active part in seminars and delivering lectures. It is always worth reminding users to take good care of their digital devices and to protect themselves and devices online. Some of the key educational events in 2019 included:

12 February: Start-up accelerator *Startup Wise Guys* organised the event *CyberNorth Warm Up*, where CERT.LV spoke on a panel of experts on cyberattacks as well as taking an active role as part of the jury to evaluate the presentations prepared by the start-ups.

13 February: CERT.LV took part in the *Shadows Day* – Latvian: *Ēnu dienas* project and hosted several students and pupils to allow seeing what a day at CERT.LV and a potential career in cybersecurity could look like to help to make the right choice in future studies and career.

27 March: CERT.LV met with the Vidzeme University of Applied Science to discuss collaboration and support in the development of a master-level study programme on cybersecurity.

28 March: CERT.LV took an active part in the LVRTC organised event *Kibernakts 2019*, which was part of the *European Digital Week*.

11 April: Participation in a conference organised by newspaper *Dienas Bizness* on *Digital Safety of Cyberspaces*.

16 April: Participation in the *Riga GDPR Forum 2019*.

29 May: Participation in *Data Security Solutions (DSS)* organised forum *Digitālā ēra*.

5 June and 24 September: In collaboration with NIC.LV and The Latvian Chamber of Commerce and Industry organised seminars on *How not to lose money in cyberspace*.

28 June: Participation in the Conversation Festival *LAMPA* discussions: *Protect Your Password as Your Underwear and Deception Online – Is Every Day the April Fools'?*

15 October: CERT.LV and NIC.LV participated in the career days for the pupils of the 9th to 12th grade to talk about the potential career opportunities in cybersecurity.

17 October: Participation in the IT Security Conference *DSS ITSEC*.

29 October: Participation in a discussion on *Safer Purchases Online* of the Association of Finance and partners as part of the national campaign “*Piik un gatavs*” (“*Beep and ready*”).

1 November: Participation in the public discussion *How Safe Do You Feel Living in Europe?* organised by the Institute of Foreign Policy in Latvia and European Commission representation in Latvia.

8 November: Participation in the Annual Conference for children *Internet and You – Who Wins?* organised by the State Inspectorate for Protection of Children's Rights

CERT.LV is a long-standing supporter of the Annual Award *Platinum Mouse* (“*Platīna Pele*” in Latvian) coordinated by the Latvian Information and Communications Technology Association (LIKTA). CERT.LV assisted the evaluation process of the award and helped to select the winner in the category *Best Cyber Security Initiative*. It was awarded to the Vidzeme University of Applied Science on their Master-level study programme Cybersecurity Engineering. The award ceremony was part of the LIKTA Annual Conference *The Arena of Knowledge*.

7.

*Strategic
Collaboration
in Latvia*

CERT.LV operates within the framework of the Information Technology Security Law, which is the main law regulating the field of cybersecurity in Latvia.

The work of **National Security Council on Information Technologies** continued its operation in 2019 as well. The aim of this Council is to plan, oversee and coordinate the appropriate, relevant national-level IT security-related tasks and events. The Council is chaired by the State Secretary of the Ministry of Defence, and the Deputy Chair is the Deputy State Secretary for Information and Communication Technologies of Ministry of Environmental Protection and Regional Development. The Council brings together high-level representatives from CERT.LV, the Ministry of Foreign Affairs, the Ministry of Economics, the Ministry of Finance, the Ministry of Internal Affairs, the Ministry of Education, the Latvian Bank, the National Armed Forces, the Ministry of Justice, the Ministry of Transport, and more besides. The Council meets at least once every four months, and the function of the Secretariat of the Council is entrusted with the National Cyber Security Policy Coordination Department of Ministry of Defence.

CERT.LV works closely together with the National Cyber Security Policy Coordination Department of the Ministry of Defence and takes an active role in implementing the National Cyber Security Strategy. Some of the key national-level activities undertaken by CERT.LV in 2019 included:

- ▶ Participation in the working group on elections for the European Parliament. During the elections CERT.LV ensured continuous monitoring of the systems.
- ▶ Participation in the National Security Committee meetings of Saeima on 5G issues. CERT.LV provided technical analysis and risk assessment on the technical implementation of 5G.
- ▶ Participation in a working group of Ministry of Defence to identify the requirements for an organisation to qualify as an Operator of Essential Services as required by the *NIS Directive*.
- ▶ Participation in a working group of the Central Election Commission on the planned Riga City Council Elections where the tasks and involvement of different organisations were defined.

- ▶ Preparations for the changes in the Cabinet Rules Nr.442, which in addition to the requirements already in place, sets out the requirements during the procurement and IT system development phase as well as requirements for service delivery by external service providers.
- ▶ Participation in a seminar organised by mobile operator *LMT* to express the concerns regarding the planned implementation of the Law Project *Procedures by which the Central Statistical Bureau requests and an electronic communications merchant provides information for the provision of official statistics*. CERT.LV noted that the chosen data anonymisation model is insufficient, and by using simple algorithms, it would be possible to identify an actual physical person.

CERT.LV is an active member of the **Digital Security Monitoring Committee**, set up initially in 2016 with the Cabinet Rules. It is a collegial monitoring committee operating under the Ministry of Defence. It aims:

- ▶ To monitor and register qualified, and qualified increased security electronic identification service operators, ensuring they have registered accordingly in the register for qualified service operators;
- ▶ To oversee and qualify trust service operators and trust services delivered according to *eIDAS* regulation by them. To ensure that information is gathered, updated and published on the list of trust.

The Committee, while implementing the oversight of the Latvia State Radio and Television Center (LVRTC), confirmed the recertification of LVRTC as a trust service operator of certified trust services (trusted electronic signature, timestamp and electronic seal) after receipt of a positive audit report.

The Committee also worked on informing the European Commission on the Latvian electronic identification scheme, consisting of four methods of identification – e-ID card, e-signature mobile,

e-signature card and e-signature card + (in Latvian - eID karte, ePraksts mobile, eParaksts karte un eParaksts karte+). The scheme has been previously attested as having a high level of trust. The Committee also reviewed the changes concerning the issue of a new type e-ID card. It also coordinated the cross-border collaboration, including information on risks and vulnerabilities.

CERT.LV closely collaborates with the **National Guards Cyber Defence Unit**. This Unit, in case of a major IT crisis or cyber threat together with CERT.LV would play a key role in supporting governmental or private sectors. The Cyber Defence Unit operates under the law for National Guards and brings together experts from the private sector, which in their spare time would be willing to collaborate, increase their knowledge and expertise both at the national level and internationally. In 2019, close collaboration took place within the scope of the cyber exercises – *Crossed Swords* and *Locked Shields*.

Anyone who is an IT expert is invited to join the Cyber Defence Unit to contribute to strengthening and protecting the national cybersecurity. To learn more and apply, please e-mail: kibersargs@mil.lv.

CERT.LV continued to coordinate the work of the **Security Expert Groups (SEG)**. Originally set up in 2012, it provides a discussion forum for IT security professionals from both the private and public sector to discuss current events and happenings in cybersecurity. It is a place where the best practice, lessons learnt and trending topics are shared. SEG meetings take place once a month and IT security experts, who agree with the Articles and Code of Practice of SEG and are recommended by two existing members, can join.

Initiative: Responsible ISP, started together with the Latvian Internet Association is ongoing. This initiative is inviting ISPs to collaborate with CERT.LV, by informing end-users on vulnerable devices and potential cyber threats and with the Latvian Safer Internet Centre by removing reported illegal content hosted on their services. In October, an informative seminar to further encourage collaboration with ISPs was organised. It brought together 45 representatives from different ISPs. Now there are 13 supporters – major ISPs in Latvia of the initiative.



8.

*International
Collaboration*

CERT.LV continuously strengthened collaboration with incident response teams internationally. During the reporting period, specialists of CERT.LV were frequent participants of international conferences – both academic and non-academic. The year went by, also working on improving knowledge and learning – a key element of this is participation in international technical training and cyber exercises.

CERT.LV took part in the [NIS CSIRT Network](#) meetings. These meetings serve as an opportunity to build further trust across incident response teams from the EU Member States. Taking place up to three times a year, meetings take place in the countries hosting the Presidency of the Council of the European Union. Topics discussed align with the specific cybersecurity priorities defined by the Presidency. Once a year, a joint session with the Cooperation Group of the *NIS Directive* takes place.

As part of the *NIS CSIRT Network*, several topical working groups take place. CERT.LV is an active participant and contributor for two of these: *Cyber Weather* working group, which regularly gathers information from the CSIRT Network on significant cyber incidents and prepares a quarterly Cyber Weather report; *Maturity* working group is working towards consistent and continuous improvement of maturity of incident response teams in the EU Member States.

Baiba Kaškina, the General manager of CERT.LV continued to serve as the Chair of TF-CSIRT *Steering Committee* – overall organisation of the work of TF-CSIRT, participation in both face-to-face and online meetings as part of her duties. Baiba Kaškina held this significant position for five years ending on the 58th TF-CSIRT Meeting in Cyprus in September 2019.

CERT.LV is an active member of [FIRST](#). CERT.LV took part in the 31st FIRST conference in Edinburg, UK. This was the largest FIRST conference ever and brought together more than 1000 participants from incident response teams and other cybersecurity organisations from more than 80 countries. CERT.LV took part in the programme-committee as part of preparations of the conference. During the conference CERT.LV was leading several technical sessions, ensured representation of Latvia in the Annual General Meeting and last, but not least took part in the capture the flag technical challenge competition.

During the course of 2019, CERT.LV participated, presented and delivered speeches at several academic and non-academic conferences. Key events to be highlighted include – *ICISSP2019 – Information Systems Security and Privacy, 5th International Conference* and [*Future Forces Forum: SCADA Security Conference*](#) both in the Czech Republic. [*ECCWS2019 – 18th European Conference on Cyber Warfare and Security*](#) in Portugal, [*Regional Cyber Resilience Forum*](#) in Moldova and [*Chaos Communication Congress*](#) in Germany.

CERT.LV regularly takes part in all international cybersecurity exercises organised by [*ENISA*](#) (European Union Agency for Cybersecurity).

In 2019 CERT.LV successfully took part in the crisis management cyber exercise *EU ELEx19* together with the European Parliament, European Commission and other EU member states. This took place in Brussels and was aimed at improving overall preparedness in case of cyber incidents during the elections of the European Parliament. CERT.LV also took part in the cybersecurity exercise *CyberSOPEx* aimed at improving cross-border collaboration in case of a major cross-country cyber incidents.

In September CERT.LV took part in the international cybersecurity exercise/ competition *CyberEx 2019* organised by *Organization of American States, INCIBE (Spanish National Cybersecurity Institute)* and *CNPIC (Spanish National Centre for Infrastructure and Cybersecurity)*. CERT.LV performed excellently and took the 16th place in the completion of 87 teams.

CERT.LV is a regular conductor of peer-reviews for other incident handling teams in Europe. During the peer-review, the quality and qualification of the incident response team are evaluated. During 2019 CERT.LV conducted peer-reviews for the following teams: Lithuanian CERT-LT, Croatian CERT.HR and Estonian CERT-EE.

As mentioned previously in May 2019 CERT.LV successfully completed the [*TF-CSIRT/ Trusted Introducer*](#) recertification process. This once again confirmed the high-level technical and organisational maturity and preparedness of the CERT.LV team. CERT.LV is one of the 32 accredited European *TF-CSIRT/Trusted Introducer* certified teams and will continue to be for the coming three years until the next recertification.

Collaboration with the Tallinn, Estonia based [NATO Cooperative Cyber Defence Centre of Excellence \(NATO CCDCoE\)](#) is of particular importance to CERT.LV. CERT.LV regularly conducts cybersecurity learning courses at *NATO CCDCoE*. CERT.LV together with *NATO CCDCoE* are core organisers of technical cybersecurity exercises *Crossed Swords* and *Locked Shields*.

The focus of the *Locked Shields 2019* was on the need for better collaboration and improving dialogue between the technical experts and decision-makers. To allow this to happen elements of both technical and strategical collaboration within a team were integrated different testing parts of communication, including consideration of potential civil and military reactions. *Locked Shields 2019* was based on real-life cyber-threats with the core task – the protection of critical infrastructure. There were more than 1200 participants from almost 30 countries. Latvian team consisted of experts from CERT.LV, National Guard Cyber Defence Unit as well as experts from Canada and the USA.

The focus of *Crossed Swords 2019* technical cybersecurity exercise was on the development of the offensive skills of the red team when planning and executing cyber operations and reacting to a cyber-threat. There were more than 100 participants from 21 countries.



9.

***Implementation
of EU co-funded
projects***

Improving Cyber Security Capacities in Latvia (Agreement number with European Commission: INEA/CEF/ICT/A2017/15287842018) started in September 2018 and will continue until December 2020. As the name of the project indicates, it is aiming to improve and strengthen cybersecurity capacities in Latvia. During the reporting period:

- ▶ Active participation in further development, testing of *MeliCERTes – Cybersecurity Core Service Platform* took place. *MeliCERTes* aims to serve as the core platform for solving and sharing knowledge regarding international cyber incidents by incorporating the needs defined by the CERT/CSIRT teams in Europe.
- ▶ Further development of *Deep Analysis System: Pastelyzer – the Paste Analyser* went on. The aim of the tool is, by being fully integrated within the existing workflow of the incident response team, allow automatic selection and analysis of defined information.
- ▶ Continuous informative and educational events throughout Latvia took place.
- ▶ The organisation of the International Cybersecurity Conference *Cyberchess 2019* was supported.
- ▶ Procurement of informative campaign *Security of Information Technologies at a Workplace* was started. The planned timeframe of the campaign is the 3rd Quarter of 2020.

Cyber Exchange (Agreement number with European Commission. INEA/CEF/ICT/A2017/1528784) started in November 2018 and will continue until November 2020. The project aims to strengthen and support international collaboration between incident response teams (CERT/CSIRT Organisations) in Europe. *Cyber Exchange* is a type of project response to ever-increasing threats in cybersecurity, stressing the need for cross-border collaboration in handling these. Latvia is one of 10 European countries taking part in the Project, and the core activity is gaining experience, sharing its own best practice and learning through *Cyber Exchange* visits.

In 2019, CERT.LV hosted *Cyber Exchange* visits from Croatian CERT.HR and Romanian CERT-RO Teams. Over several days, valuable information exchange on best practices, tools and processes

of cyber incident handling took place. Valuable discussions on incident prevention methods, educational activities and other current activities were on the agenda helping the organisations to identify and share best practice as well as increase trust among organisations.

CERT.LV was hosted by CIRCL, in Luxembourg. The core focus of the *Cyber Exchange* visit was *MISP* (*Malware Information Sharing Platform*), since CIRCL is the developer of this widely used platform. It was possible to share how CERT.LV is using *MISP* in daily operations. CIRCL shared information on how to integrate *MISP* in daily operations better. Active contribution to further developments of *MISP* took place. Sharing of daily operational practices in incident handling also took place.

```
1 (defun nbytes (stream n &optional colon-p at-sign-p)
2
3 (defun nbytes (stream n &optional colon-p at-sign-p)
4 "Formats amount of N bytes in a human-readable form,
5 of 1024, or powers of 1000 if COLON-P is true."
6 (declare (ignore at-sign-p))
7 (type unsigned-byte n))
8 (cond ((zerop n)
9 (write-string "0B" stream))
10 (t
11 (multiple-value-bind (base units)
12 (if colon-p
13 (values 1000.0d0 "BkMGTPeZY")
14 (values 1024.0d0 "BKMGTPeZY"))
15 (loop for i fixnum from 0 below (1- (length units))
16 for f double-float = (coerce n 'double-float) then (/ f base)
17 until (< f base)
18 finally (let ((unit (schar units i)))
19 (if (and (< f 10) (plusp i))
20 (format stream "~,1F~A" f unit)
21 (format stream "~D~A" (round f) unit))))))))
22
23 (defun bytes (stream bytes &optional colon-p at-sign-p)
24 "Formats a sequence of BYTES as hex-digit pairs."
25 (declare (ignore colon-p at-sign-p))
26 (etypecase bytes
27 (vector
28 (loop for byte of-type (unsigned-byte 8) across bytes
29 do (when (< byte #x10)
30 (write-char #\0 stream))
31 (write byte :stream stream
32 :base 16
33 :radix nil
34 :readably nil
35 :escape nil)))
36 (list
37 (format stream "~{~2,'0x~}" bytes))))
```


10.

***Services
to strengthen
Cyberspace in Latvia***

DNS Firewall: Tika Started in 2018, the work on further implementation and improvements of CERT.LV and NIC.LV *DNS RPZ (Domain Name Service Response Policy Zone)* or *DNS Firewall* project continued.

The project provides an opportunity to protect users from malicious content on the internet, which is linked to incident indicators (domain names, IP addresses, etc.) already known to the cybersecurity authorities. During the project, there are more and more successful cases where active protection has saved devices from becoming infected. This service can be used by any internet user in Latvia, and there is no need to sign a contract. All that is needed is the use of NIC.LV recursive *DNS* servers.

To find out more, please visit: <https://dnsmuris.lv>.

DNS
ugunsmūris



