CERT.LV
Information Technologies
Security Incident
Response Institution

Institute of Mathematics and
Computer Science University of Latvia

Ministry of Defence
Republic of Latvia

2020

CERT.LV Annual Report

The report contains information accessible in the public domain which does not contain information regarding the results achieved by CERT.LV that include limited access information. The report is for informational purposes only.

Contents

Abstract

In 2020, Latvia faced several challenges — rapid adaptation process to remote work, a series of special campaigns of fraud and innovative cyberattacks. The number of cyberattacks on private household equipment, such as private computers, routers and smart TVs, has grown significantly. Compared to the pre-pandemic period, the number of these attacks has grown by 15-30%. Recurrent attacks have been carried out against remote work tools like VPN (Virtual Private Network) and RDP (Remote Desktop Protocol) — an increase of about 20%. An increase in fraudulent campaigns, unrelated to the pandemic, has also been observed. The intended audience for these campaigns was mainly end users, and the goal — the retrieval of authentication data.

The reporting period was marked by the detection of several particularly critical vulnerabilities. This was the first year when such a number of critical vulnerabilities was detected within a single year. The attackers exploited several of these vulnerabilities in their advancements until the appropriate updates were released. CERT.LV identified the potentially vulnerable systems in the public sector, informed system operators, made recommendations to address the vulnerabilities and gave support to handle incidents.

As a matter of urgency, dictated by the rapid spread of the Covid-19 pandemic, many companies and organisations made compromises in regard to safety in order to switch to fully-fledged remote work as soon as possible. Inadequately configured RDP access points were a threat even before the pandemic, and the problem only escalated during it. The attackers abused the insufficiently protected RDP services and VPN gateways, in order to compromise systems and access the internal networks of companies and organisations. The most common issue turned out to be the lack of secure passwords that enabled the attackers to easily guess or find them, as well as expired VPN devices and the lack of other security mechanisms.

The attackers kept taking advantage of the society's lack of knowledge and understanding about the way multi-factor authentication mechanisms work. During the active campaign of attacks, people received phone calls from scammers pretending to represent the employees of the bank or *Smart-ID* in order to obtain confirmation of the second factor and to scam financial resources. To increase credibility, scammers falsified bank phone numbers in their calls.

As the role of social media in the communication of people (and institutions) is increasing, scammers have tried to take over the accounts of facilities and companies with a base of users large enough to use for advertising various products or services, mainly in the Far East. The scammers used an intimidation tactic involving pretending to be the administrator of a social network and threatening to suspend the user's account due to a violation of the terms of use. Access to the accounts of several institutions was lost as users entered their login details on sites made by the scammers (none of the accounts had used two-factor authentication until then).

A new trend emerged in extortion-related attacks. Extensive (up to 180 Gb/s) distributed denial-of-service (DDoS) attacks were targeted at financial institutions and large companies. The attackers demanded a ransom to halt the attacks, and threatened to suspend the operation of companies by organising attacks of up to 2 Tb/s. The processes of intimidation did not last for longer than a few days, sometimes they lasted less than an hour. Usually, no attacks followed. If a company avoided communication with the extortionists, they usually lost interest and moved on to a new goal.

In cases of break-in, when the attackers managed to enter the system by using an insufficiently protected RDP service or VPN gateway, the attackers demanded a ransom not only for the recovery of encrypted data, but also for not leaking it (data had been copied before encryption).

In the second half of 2020, the malware *Emotet* spread rapidly both on the global and the Latvian web. The malware spread from the infected devices to their contact list, increasing the trustworthiness of the malicious emails with the help of chat fragments from the user's device, as well as carried out other malicious actions on the device. Within a small timeframe, more than 200 organisations came into contact with *Emotet*, and they lost control over email conversations and other information. It is expected that after a year or more the obtained information might pop up in recurrent attacks or be used in other malicious campaigns.

Overall, in 2020 CERT.LV registered 346,108 unique endangered IP addresses. No significant fluctuations regarding the number of endangered IP addresses have been observed in the reporting period when comparing to 2019.

In 2020, CERT.LV organised and attended 58 educational events on cybersecurity, as well as trained and educated 6758 people. Due to the pandemic, the number of events held in the second and third quarter decreased. The Covid-19 restrictions led to the discontinuation of on-site activities, and events were moved to the online environment.

From 14 September to 12 October, with co-funding from the Connecting Europe Facility, CERT.LV organised an educationally informative awareness raising campaign on cybersecurity in the workplace. The aim of the campaign was to raise the awareness of state and municipal employees about the principles of cyber hygiene, and to teach them how to identify and prevent potential cyberattacks. Different communication channels were used to reach the target audience — explanatory videos were put together, a digital user's handbook was created, posters were put up in the urban environment, informative articles were prepared for the largest news pages, and active communication was maintained on social media. Statistics show that the campaign reached almost 500,000 Latvian internet users.

On 1 and 2 October, to kick off *European Cyber Security Month*, CERT.LV organised the online technical cybersecurity conference *Cybershock 2020*.The event provided a platform for a variety of technical topics related to cybersecurity to be discussed in-depth with the help of practical examples and demonstrations. A total of 760 participants signed up and remotely attended the conference. The presentations were given by seven lecturers from five different countries. In cooperation with *Cybexer Technologies* and *Tet group*, a *Capture the Flag (CTF)* competition was held simultaneously with the conference, engaging 100 participants from 29 teams.

During the next reporting period, as the remote operation mode remains relevant, continuous attacker interest in remote access and communication tools, such as RDP, VPN and online communication tools, is predicted. The hunt for passwords, abuse of vulnerable systems and the search for uncovered vulnerabilities will persist. This will give even greater importance to

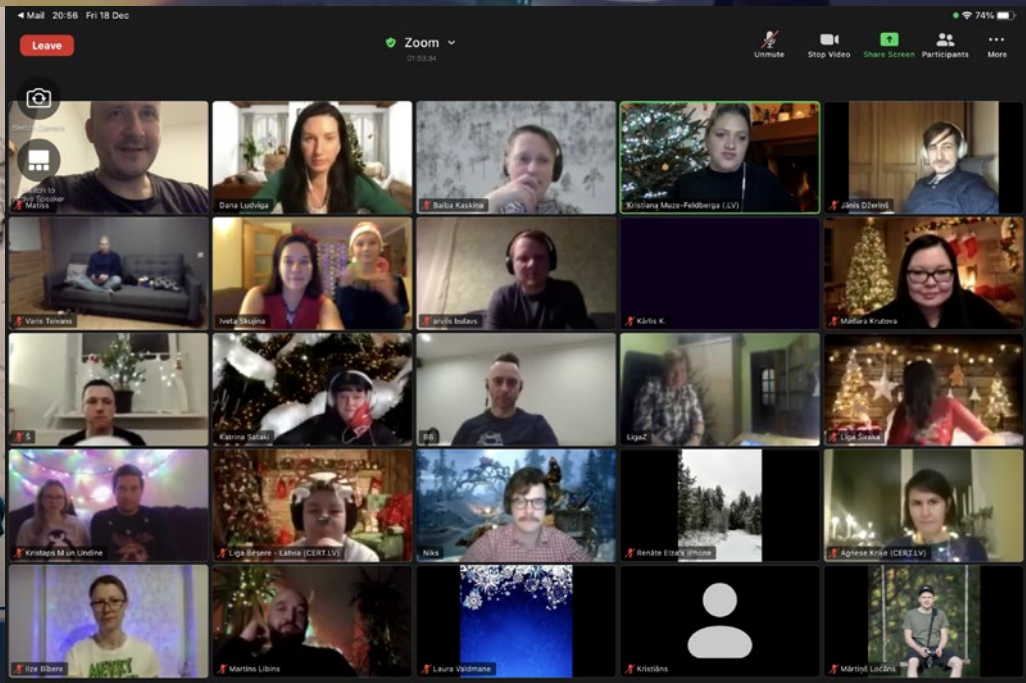
the timely installation of updates and adherence to the best cybersecurity practices. For more effective protection, CERT.LV recommends following the *Zero Trust* approach, which entails a careful inspection of all system processes and login attempts by being suspicious of everything and everyone, before concluding that the system, device or connection is safe. Not only the introduction of multifactor authentication wherever possible, but also the ability to ensure that users are knowledgeable on the way it works, will become essential.

Considering the increasing amount of operations conducted online, such as remote work, meetings, studies, shopping, and communication, as well as the data leaks that have already taken place and the potential ones, more adjusted and targeted cyberattacks can be expected.

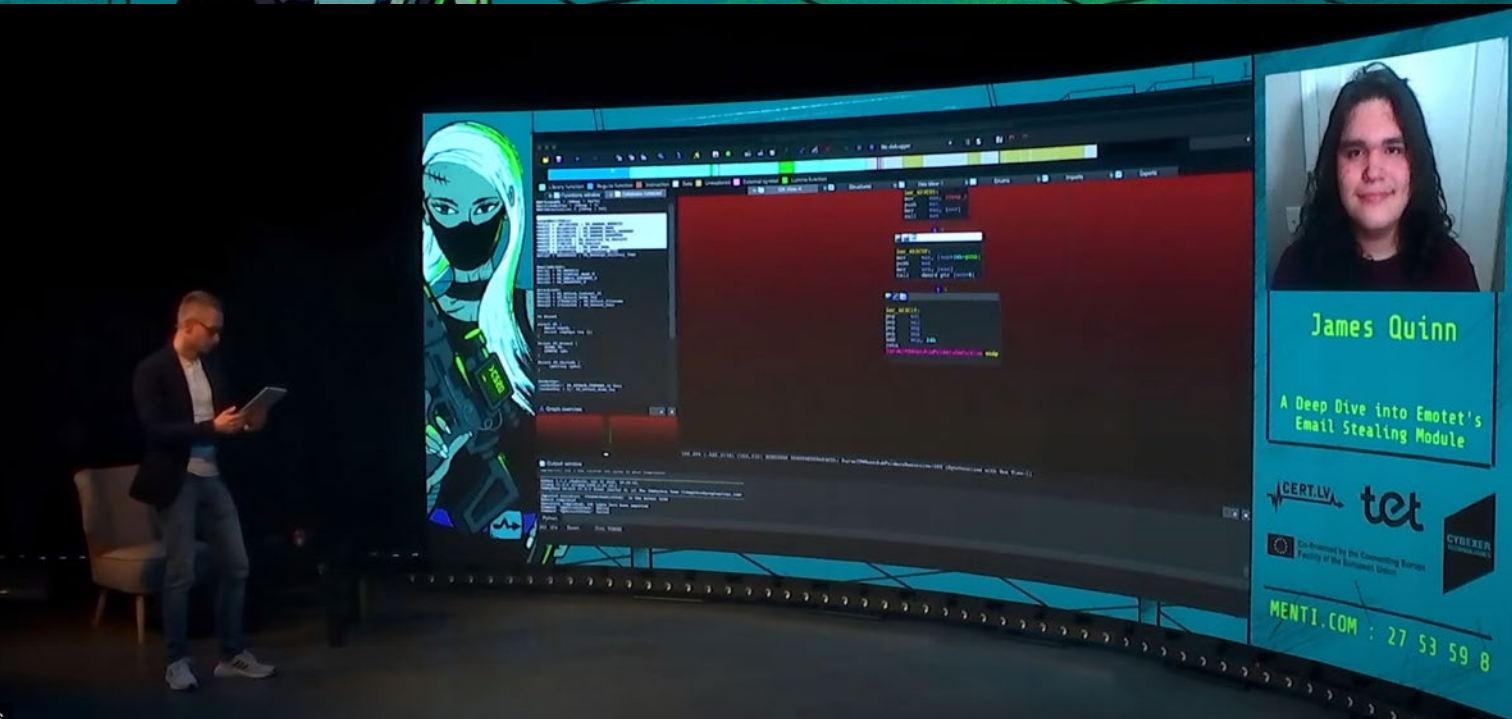
All the restrictions of 2020, including those of funding — will create additional challenges for the continuous maintenance and improvement of cybersecurity, therefore we wish everyone endurance and strength in 2021!

In the name of the CERT.LV team,
Baiba Kaškina
Head of CERT.LV


CERT.LV
CERT.LV


Leave
Zoom
Unmute
Stop Video
Share Screen
Participants
More


Cyber Shiv
2020


James Quinn
A Deep Dive into Emotet's Email Stealing Module
CERT.LV
tet
CYBEXER
MENTI.COM : 27 53 59 8

1.

Incident Processing

CERT.LV compiles information on the threatened Latvian IP addresses every month. For threat accounting CERT.LV works with an internationally used incident taxonomy (the taxonomy developed by the eCSIRT.net project). All registered threats are accounted for by CERT.LV in one place by dividing them into types of threats (e.g. malware, break-ins, fraud), infection (e.g. *Confiker*, *Zeus*, *Mirai*) and vulnerability (e.g. *Opendns*, *Openrdp*).

During the reporting period, CERT.LV compiled information on 85,000-100,000 unique vulnerable IP addresses every month.

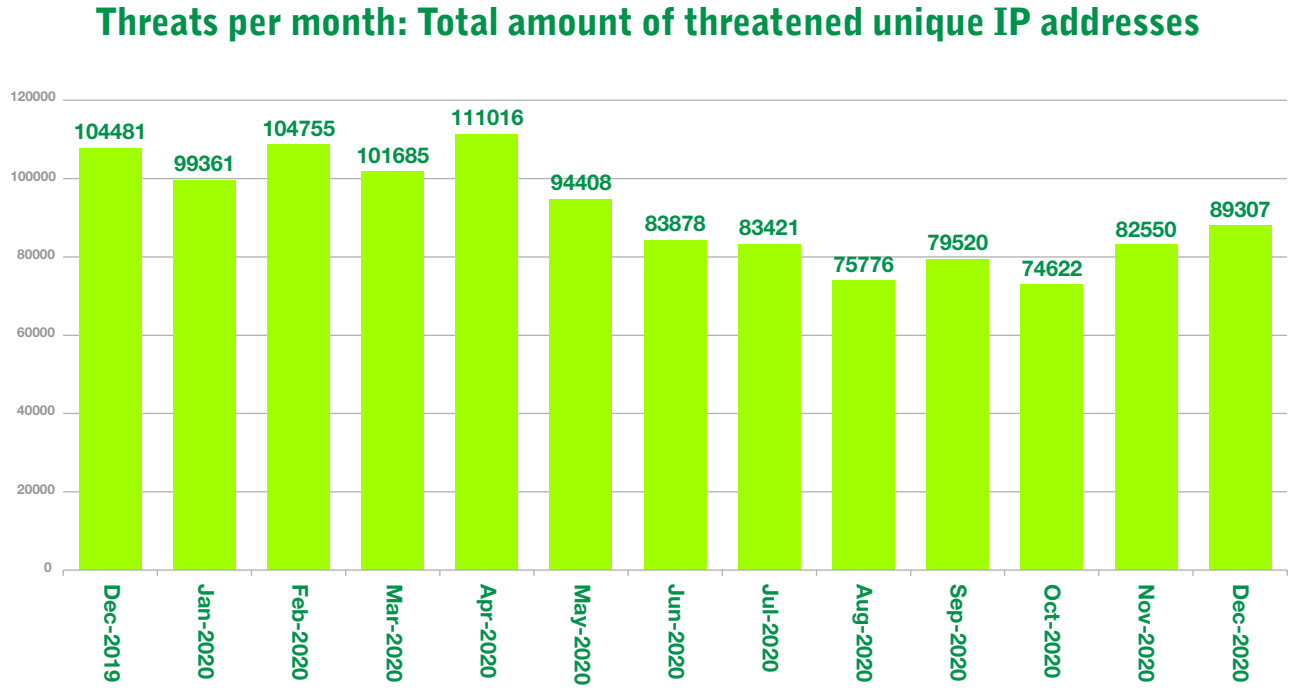


Figure 1 – Monthly registered unique IP addresses in 2020 by CERT.LV.

Threatened IP addresses per quarters in 2020

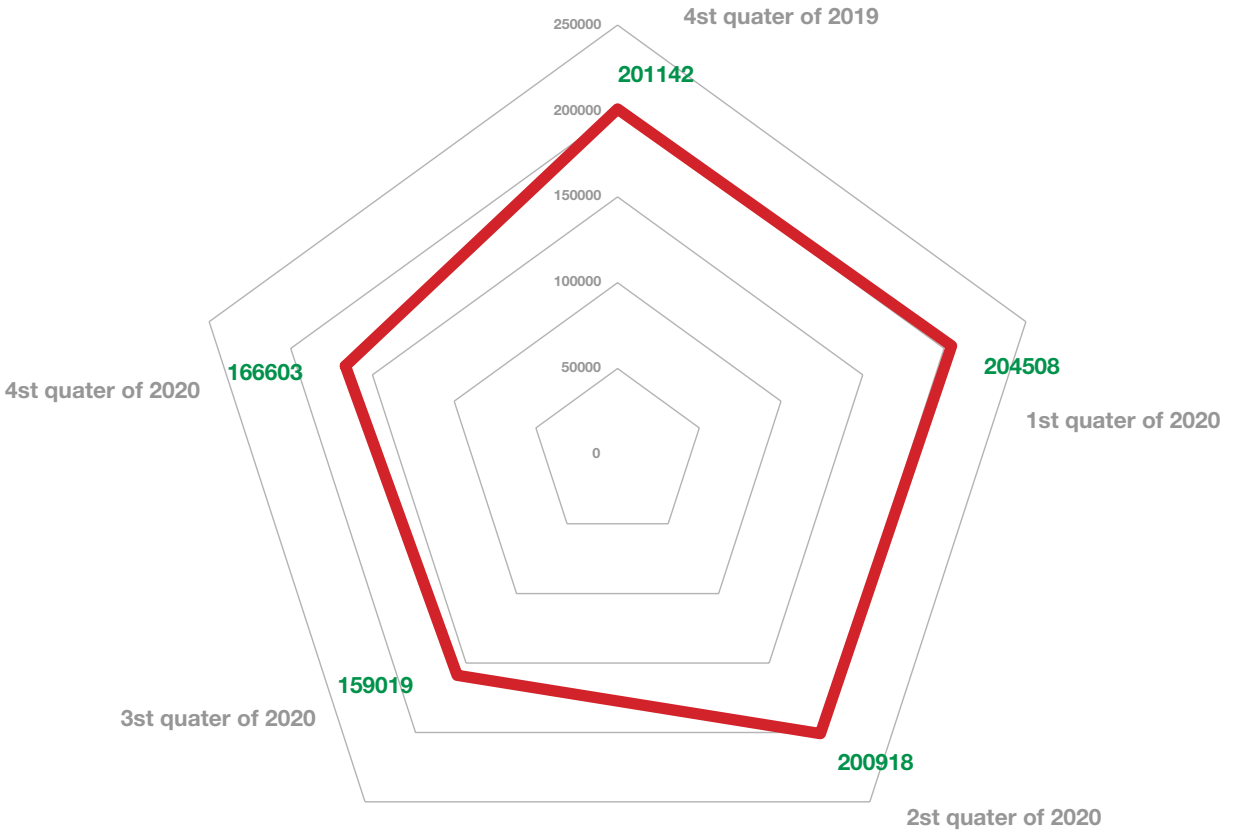


Figure 2 – Registered threatened unique IP addresses per quarter in 2020.

The most common type of threats remained vulnerabilities, the second most common type — malicious code, the third — intrusion attempts. The category Other includes the provision of advice on various issues related to cybersecurity, mainly to state and municipal institutions and the population of Latvia, as well as other cases of information processing that are not directly linked to threat prevention or incident resolution.

Registered threats — the amount of affected IPs in 2020

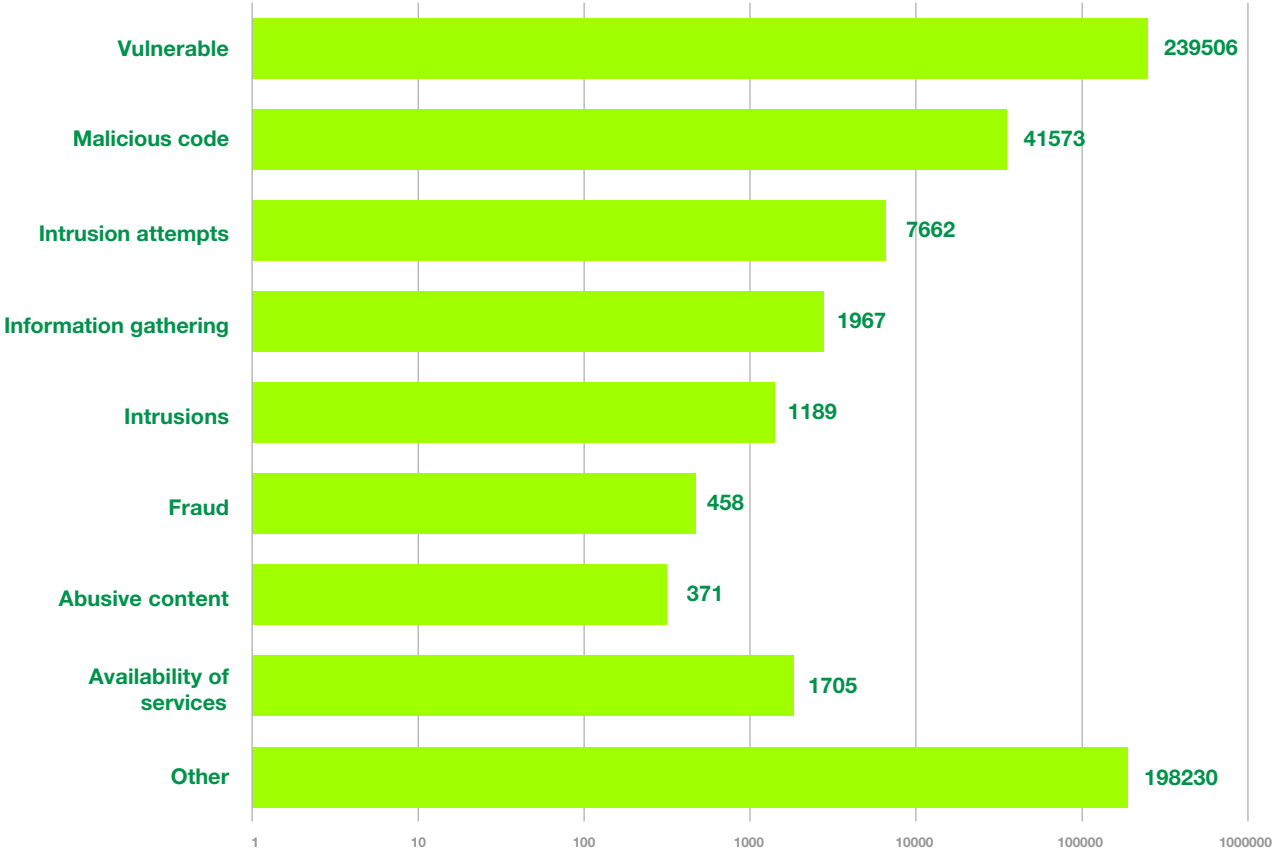


Figure 3 – Threatened unique IP addresses registered by CERT.LV by type of threats in 2020.

Top Malicious Code 2020

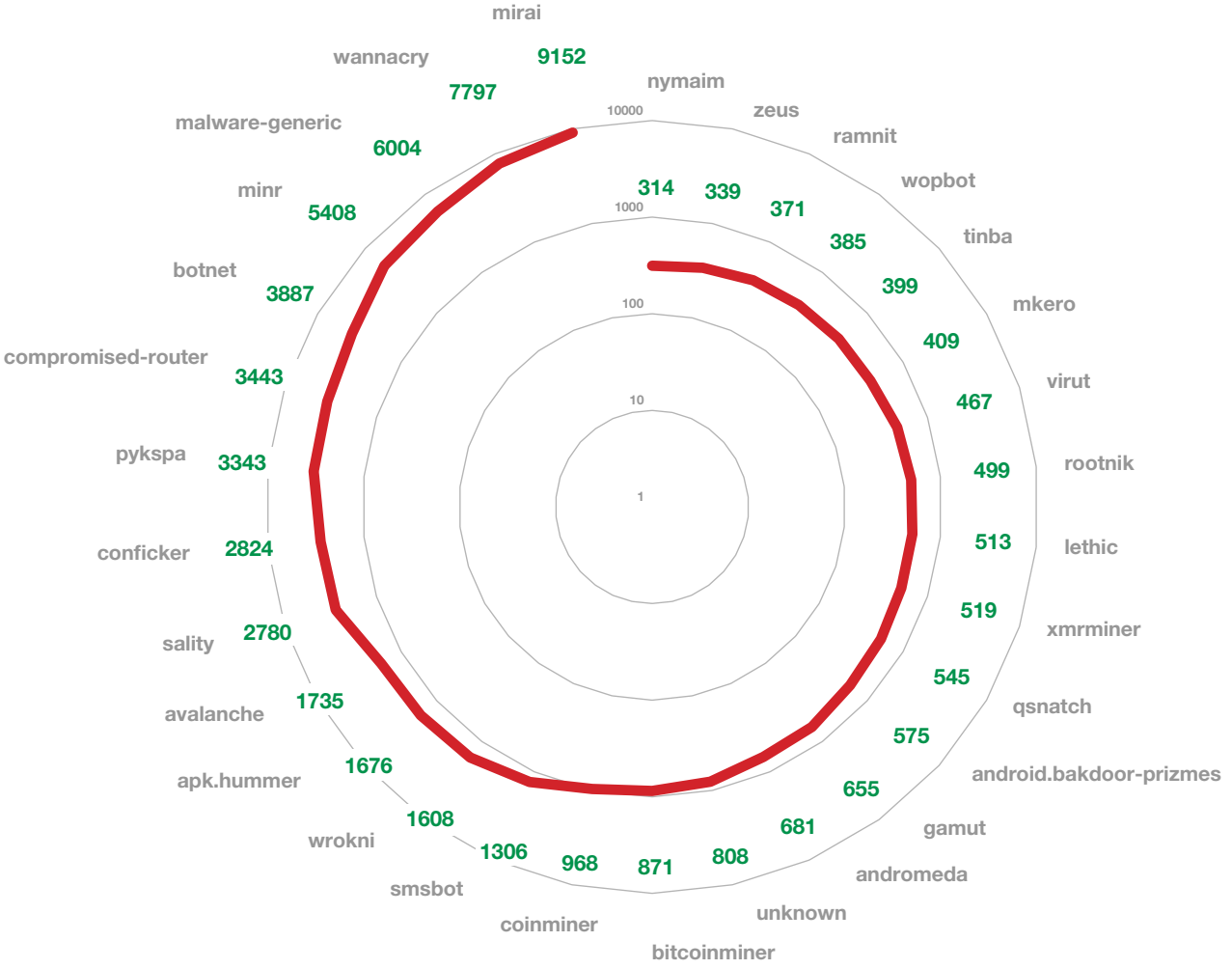


Figure 4 – Total number of CERT.LV registered threatened unique IP addresses in 2020 with type of threat – malicious code.

In 2020, the most widespread in the Latvian web was malware *Mirai,* which endangers the inadequately protected Internet of Things (IoT) devices. Smart TVs, internet routers, security cameras and similar devices which are connected to the internet using the username and password provided by the manufacturer after being set up are infected most often. These manufacturer settings, or default passwords, are widely known, and using them puts devices at the risk of attacks.

WannaCrypt or *Wannacry* encrypting ransomware takes second place in the top of the most widespread malware. It affects devices operating on *Microsoft Windows* and spreads via vulnerabilities in the *Server Message Block (SMB)* protocol, which is used in file exchange within the internal network. Virus effect and spread can be prevented by installing software updates that are available even for such neglected *Windows* versions as *Windows XP* and *Windows Server 2003.*

Minr takes third place in the top of most widespread malware — it is a malicious code that can usually be found on hacked websites in order to employ the website's visitors' computer power to mine cryptocurrency *Monero* (cryptocurrency that is orientated to privacy and has gained popularity in criminal circles) without the user's knowledge. By carelessly employing the power of the device, irreversible damage can be done to it.

Top vulnerabilities 2020

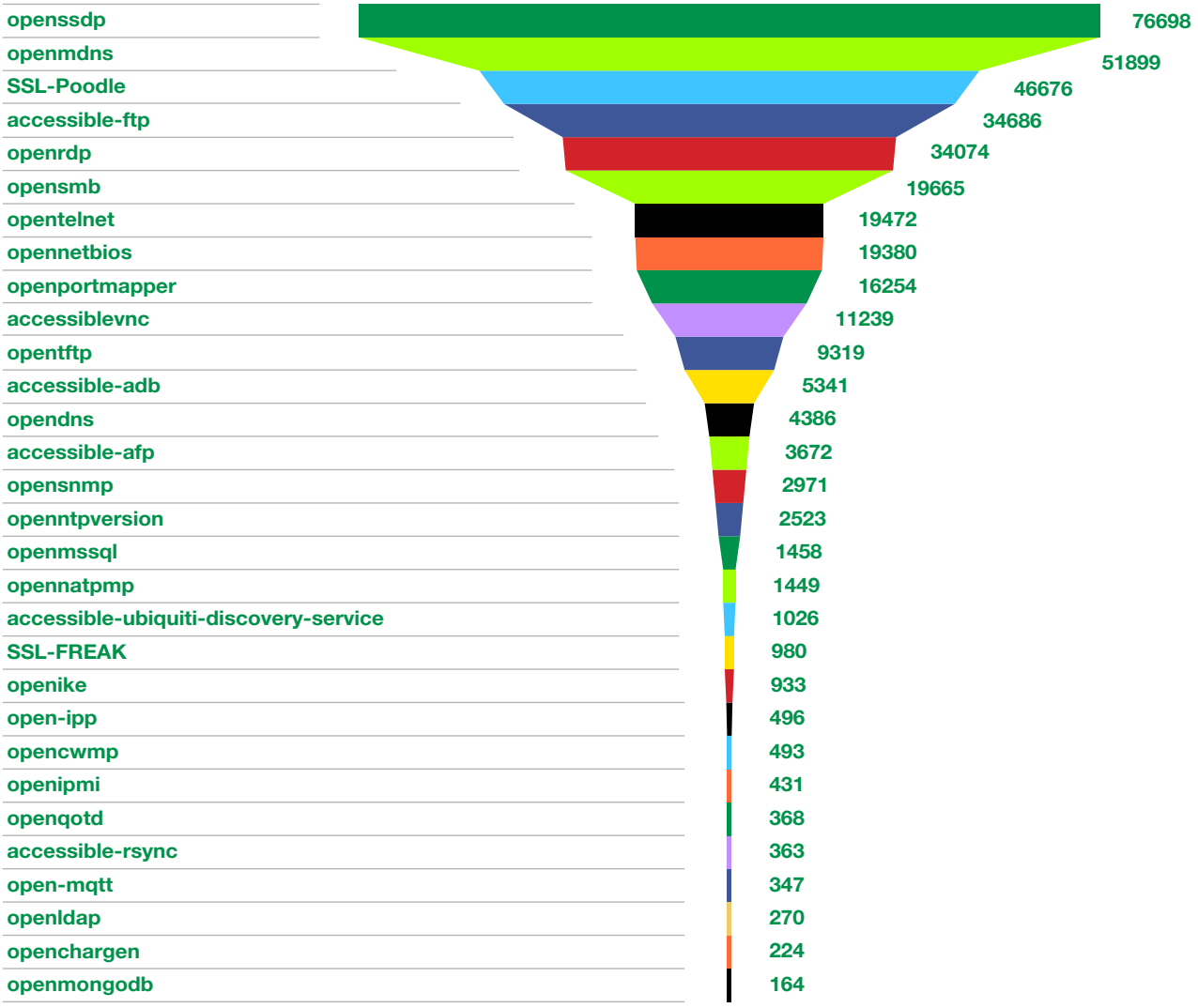


Figure 5 – Number of threatened unique IP addresses registered by CERT.LV in 2020 with the type of threat – vulnerabilities.

OpenSSDP takes first place in the top of vulnerabilities — devices with unsafe configuration that can be used in denial-of-service attacks. *Simple Service Discovery Protocol* (*SSDP*) is integrated in several network devices in order to locate one other and communicate more quickly. As a result of inadequate configuration, the functionality of *SSDP* is often unavailable to the user, and that makes the device a powerful weapon for the attacker.

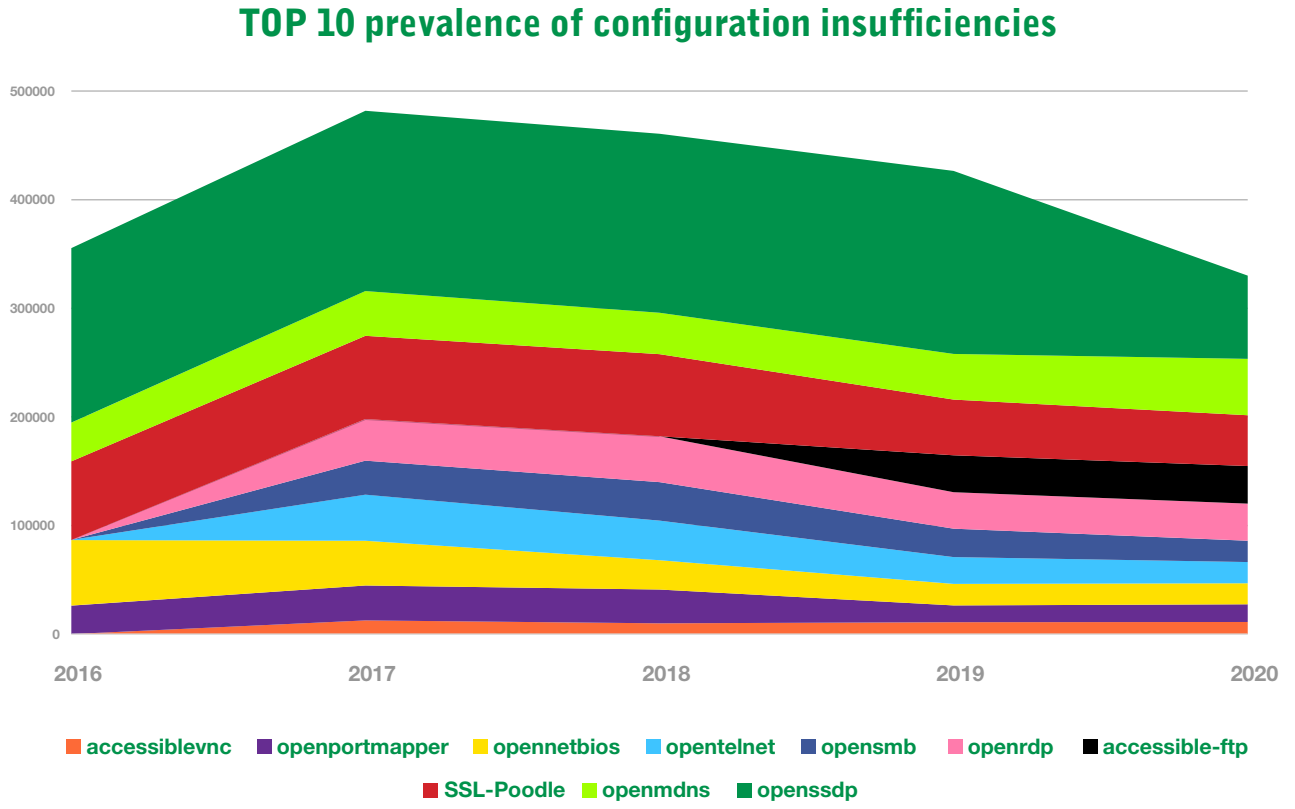


Figure 6 – Number of threatened unique IP addresses registered by CERT.LV with the most widespread configuration insufficiencies of 2020.

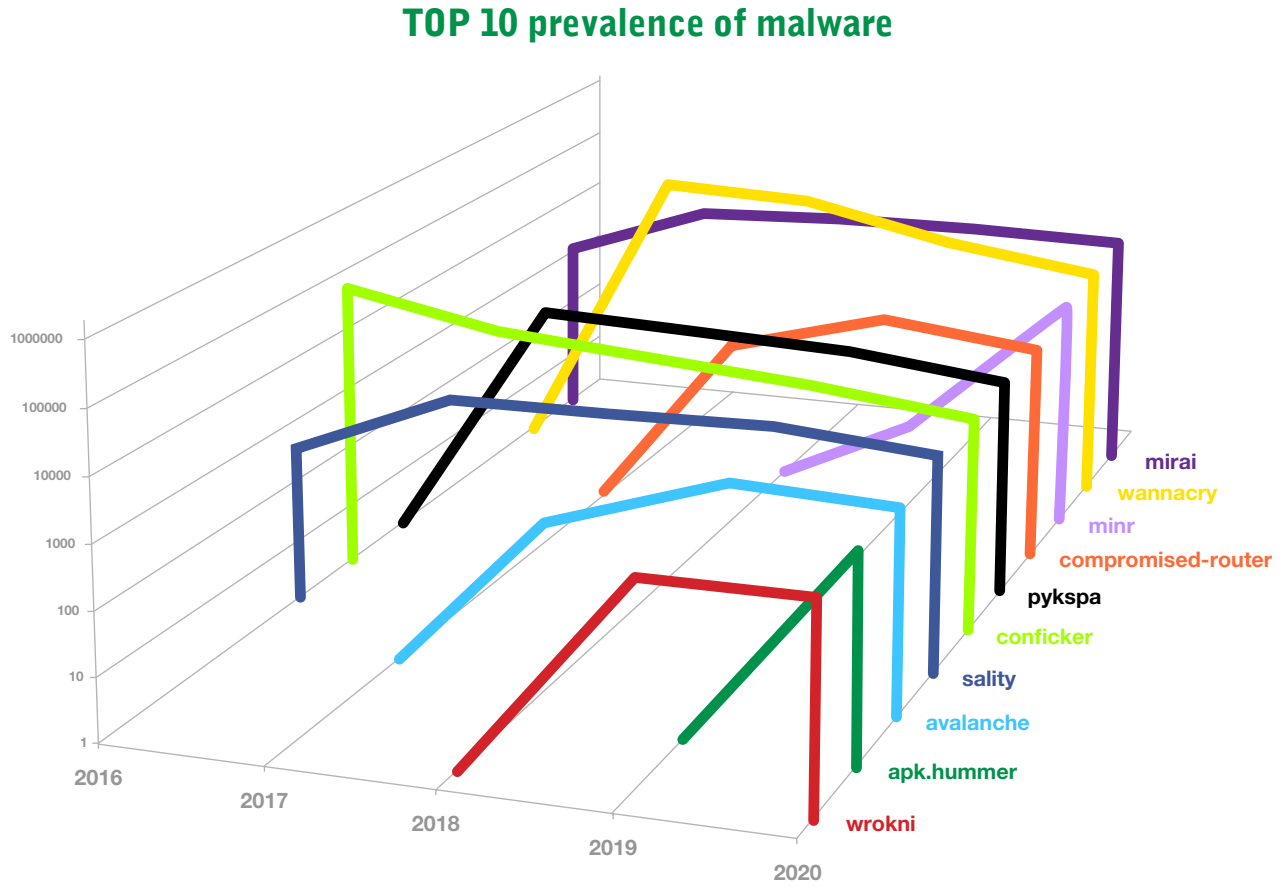


Figure 7 – Number of threatened unique IP addresses registered by CERT.LV with the most widespread malware of 2020.

Openrdp vulnerability that takes fifth place in the configuration insufficiencies or vulnerability top (Figure 5) indicates an activated *Remote Desktop Protocol* (RDP) that is accessible through a public network and presents a risk if a simple password is used and access is not limited by the use of, for example, a virtual private network (VPN). Attackers can take advantage of an inadequately protected RDP access point in order to enter the system, retrieve data or demand a ransom for the recovery of corrupted data.

When inspecting the 10 most widespread vulnerabilities and types of malware of 2020, it can be observed that the most common vulnerabilities of the reporting period have been observed and quite widespread for the last five years[1] (Figure 6), as opposed to the most widespread malware of 2020, most of which did not even exist five years ago, and three of the most widespread types of malware have entered the cyberspace of Latvia just a few years ago (Figure 7).

This leads to the conclusion that device owners do not pay enough attention to the protection of their devices, they do not take action to prevent configuration deficiencies, and this exposes their devices to the risk of attack; the attackers, in turn, work to improve their attack methods in order to create new malware to compromise as many devices as possible.

In cooperation with internet service providers, CERT.LV regularly educated the operators of vulnerable devices within the "Responsible Internet service provider" initiative by explaining the impacts of potential threats and making recommendations to prevent them, yet, unfortunately, most of the users often ignored the notice regarding device endangerment sent out by their service providers upon receiving it.

[1] There is insufficient data about the configuration deficiencies *OpenSMB*, *OpenRDP*, *Accessible-ftp* and *accessiblevnc* in 2016.

2.

The Most Notable Incidents of 2020

During the reporting period, CERT.LV cooperated with state and municipal institutions, banks, internet service providers and other organisations in order to solve cases of incidents of different importance. CERT.LV publishes an overview of the most relevant incidents every month on their website in the section called *Kiberlaikapstākļi* (Cyber Weather). By using such comprehensible weather forecast symbolism, it is easy to look back at the events of the previous month.

Here, the most notable incidents have been compiled, marking the main tendencies of the year.

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

Several popular websites have become increasingly overloaded due to the pandemic: www.spkc.gov.lv, www.e-klase.lv, www.eveseliba.gov.lv, etc., as well as the user authentication module www.latvija.lv. All anomalies were legitimate, meaning that no external influence was observed.

As of September, money extortion attempts have gained relevancy both in Latvia, and in Europe, and they have mainly been aimed at financial institutions and other private sector companies. By threatening to halt the operation of company websites and other resources by means of attacks of up to 2 Tb/s, attackers performed a series of trial attacks. Although temporary (in some cases they lasted several days, but mostly — less than an hour), the attacks were significantly extensive — of up to 180 Gb/s. As a result of the attacks, the resources/services of certain companies were available with random downtimes for several hours.

CERT.LV has published recommendations for endangerment prevention and active protection against DoS attacks. It is important not to establish communication with the extortionists and not to make payments, so as not to encourage repeated attacks in the future.

2.2. Phishing or Personal Data Scams

Phishing attacks have been relevant all year. In the majority of cases, campaigns were aimed at the scamming of email and *Office 365* data, acquisition of bank, international payment system, including *Smart-ID*, access data, and defrauding of access data to accounts on popular social media sites, such as *Facebook* and *Instagram.* The topicality of Covid-19 was often used to attract the users' attention in fraudulent emails and social media announcements.

During the pandemic, an increase in data scamming attempts via package delivery service provider brands, such as *Latvijas Pasts, DHL, Omniva, DPD, AliExpress,* etc., has been observed. These phishing attempts became increasingly persistent during the pre-holiday season, as it happens at the end of every year.

In August, information about innovative attacks in order to attain *Office 365* access rights was received. The attacks were hard to spot by technical means, since no malicious actions were taken on the victim's device and the attacks were carried out within *Office 365* using a fraudulent app created on the *Microsoft* app store *Azure.*

During the whole reporting period, upon spotting phishing campaigns, CERT.LV published informative material for the users of certain services to invite them to be more attentive and careful and, when possible, to set up and use two-factor authentication for additional security, in order to make it significantly more difficult for attackers to access user data, even if they learn the user passwords.

2.3. Fraud

In terms of fraud, 2020 has been very intense; Latvian internet users have periodically had to endure active fraud attempts, such as extortion campaigns in which attackers claimed to have hacked a user's device and obtained compromising material for which a ransom was set, and

fraudulent lotteries organised by certain companies, offering to win the latest smartphone models or other valuable prizes.

A new trend was observed — extortion emails containing threats to leak data were aimed at companies as well. In these emails, the attackers claimed to have hacked a company's website and learnt the data of its clientele, and demanded a ransom for not publishing it.

Misleading advertisements continued to circulate on social media. Using the names of famous Latvian people without their knowledge, advertisements invited internet users to invest in cryptocurrency. Scammers also made phone calls and tried to persuade people to invest. In certain cases, repeated fraudulent attempts were observed where the victims of financial fraud were offered help to get their lost resources back. CERT.LV has knowledge about a Latvian citizen who followed the advice of scammers, deposited money in an unlicensed financial platform, and lost 60,000 euros, as well as an additional 10,000 euros to a repeated scam when trying to regain his/her lost funds.

CERT.LV invites people to refrain from engaging in transactions proposed to them and end such calls as soon as possible, block the caller on their device, and inform their mobile service provider. Information on licensed Latvian financial service providers can be found on the Financial and Capital Market Commission website www.fktk.lv.

By falsifying the phone numbers of different credit institutions and impersonating bank and *Smart-ID* employees, scammers use the public's lack of knowledge on additional authentication methods and defraud financial resources from several thousands of users, causing total losses worth hundreds of thousands to Latvian credit institutions. Banks and CERT.LV would like to remind people that a bank would never call and ask for a username, password or a *Smart-ID* code.

Attackers have adjusted their methods to the necessity for companies and institutions to start working remotely and to immediately send out documents electronically, which would allow deviations from previously approved norms. A number of company accountants received emails in the name of the director or another employee to make an urgent payment or change the payroll

accounts. Cases of fraud have been documented when the scam has promptly been detected and the money has been recovered.

There were also reports from companies of interference in business correspondence. By compromising the emails of companies or their collaboration partners, attackers picked a suitable moment to send one of the parties a bill with an altered account. In most cases the fraudulent activity was detected; however, there have been at least two cases when the payment was made and the resources were lost.

The public were concerned about messages containing link shortcuts (ej.uz) sent out by state institutions to inform people about the state of emergency and the epidemiological situation in the country. Link shortcuts are often also used in scammer messages to mask the actual link destination. CERT.LV cautions institutions to immediately publish the relevant information on their website and social media profiles, and instantly warn the public about upcoming announcements and the methods of releasing them, in order to avoid misunderstandings.

Fake online stores thrive during the holiday season, and this year was no exception. Although they are around all year, the number and activity of such stores skyrockets during the holiday season by means of social media advertisements, etc. This lures in new shoppers and the profit potential of scammers increases.

2.4. Intrusion Attempts

Information about break-ins comes in all throughout the year, although, in quite low amounts. Break-in attempts coming from other countries were aimed at the state and municipal institution servers of Latvia, and some attacks coming from Latvian IP addresses were aimed at state institution servers of other countries.

As organisations switched to remote work, increased activity of bots searching for vulnerable, inadequately configured devices and/or weak passwords for devices connected to a network was

observed. Some of the targets of these bots were hastily employer-issued devices, devices with insecure configuration or personal laptops that started getting used for work, as well as poorly protected RDP services with weak passwords.

Different break-in methods were used. CERT.LV observations indicate that the most common methods used by attackers were password guessing by means of the Instant Message Access Protocol (IMAP) service, service overload attempts using Transmission Control Protocol (TCP) requests, and data retrieval attempts using *SQL* injections.

2.5. Malware

Like previously, in 2020 malware was mainly spread for two purposes — to obtain information or to make a profit. To obtain information, spying malware was released, and it forwarded the data accessed on the victim's device, such as passwords, to the attacker. To make profit, encrypting ransomware was distributed, and, as a result, the data on the user device was encrypted and a ransom was demanded for the recovery of the stolen data. The ransom was set depending on the encrypted device, the victim of the ransomware, and the volume of the encrypted data — the more important the data, the higher the ransom. Several companies, state and municipal institutions, and a healthcare service institution were among the victims of it.

CERT.LV stresses that the ransom should not be paid when possible. Making the payment does not guarantee recovery of the lost data and enforces such malicious practices, as well as works to show the attackers that victims are ready to pay, and this may lead to recurrent attacks.

A series of attempts to spread malware was carried out under the cover of Covid-19:

- E-mails were sent out, seemingly in the name of the World Health Organization, indicating that the attachment includes the latest information on Covid-19.

- By publishing sites to charts showing the spread of Covid-19, the functionality of which was to steal user data.
- Malicious emails were sent out to healthcare institutions regarding the delivery of Covid-19 protective equipment, etc.

In the second half of 2020, the malware *Emotet* spread rapidly both on the global and the Latvian web. *Emotet* usually reached the device of its next victim through the email of an already infected contact. This malware is intended to steal sensitive information. In order to mislead the recipients and increase its trustworthiness, emails containing *Emotet* included fragments from previous correspondence, which convinced people that the received email was the follow-up to the previous interaction. More than 200 Latvian companies were infected. It is expected that, after a certain period, the obtained information might pop up in recurrent attacks or be used in other malicious campaigns.

Emails containing infected attachments were the main medium used to spread malware. Attackers usually injected the encrypting ransomware into the devices of its victims by taking advantage of inadequately protected RDP services. Attackers guessed or discovered weak passwords by using databases obtained during other attacks or data leaks.

2.6. Compromised Devices and Data Leaks

Equipment compromises affected individuals, companies, as well as state and municipal institutions. Already compromised email accounts were used as a vector for the attack, and employees of the organisations infected their devices by opening email attachments or links from seemingly known contacts in their address book — colleagues and business partners. The goal of these actions was to obtain email access data and other sensitive information.

As the main protection mechanism, CERT.LV recommends to set two-factor authentication for the protection of emails, as well as *Microsoft* accounts.

In the case of compromised websites, the attacks were often carried out via an outdated plugin or outdated content management system. In most cases, compromised sites contained malicious code to redirect users to the desired malicious site, or to retrieve data, but in some cases there was also a data leak. This reaffirms the need to provide both resources and funding for the maintenance and updating of systems, as well as to follow the available updates and install them in a timely manner.

Several state institutions temporarily lost access to their social media accounts as attackers took over one of the account administrator's profiles. In none of the cases was two-factor authentication used for additional security, which would have made it difficult to take over the accounts.

Reports of *Zoom, MS Teams* and other platform meeting break-ins were received. However, after reviewing the situation, it was found that the meeting organisers did not use the available safeguards (waiting rooms, limited access from abroad, etc.) to prevent outsiders from joining the meeting.

In November, the news about the data leak from the Chinese company *Zhenhua Data*, which affected approximately 2.4 million people worldwide, received wide resonance in the Latvian media. Among the victims, information about 480 Latvian citizens could be found. The leaked data showed that the company had collected publicly available information about individuals — from the media, social networks, etc. Specially designed applications were used to collect the information.

2.7. Vulnerabilities and Configuration Insufficiencies

The reporting period was marked by an alarming amount of detected vulnerabilities (*Windows DNS: CVE-2020-1350, SMB: CVE-2020-0796, Windows Server: CVE-2020-1472, SAP: CVE-2020-6287,* etc.). The vulnerabilities either allowed an attacker to remotely execute arbitrary code on the target device, or to retrieve sensitive information from the target system. Several

of these vulnerabilities were actively used in attacks before manufacturers managed to publish updates to address them. This gave these vulnerabilities *zero day* vulnerability status. CERT.LV identified the potentially vulnerable systems in the public sector, informed system operators, made recommendations to address the vulnerabilities and gave support to handle incidents.

Reports regarding the websites of several companies and institutions were received, stating that they were subject to personal data retrieval attacks as a result of improper configuration. CERT.LV worked to inform the resource maintainers and coordinated the prevention of vulnerabilities.
At the beginning of 2020, an average of 20,000 unique IP addresses with *OpenSSDP* (*Open Simple Service Discovery Protocol*) vulnerabilities which are exposed to the risk of use in DoS attacks, were registered every month. A fraction of the inadequately configured devices were smart TVs.

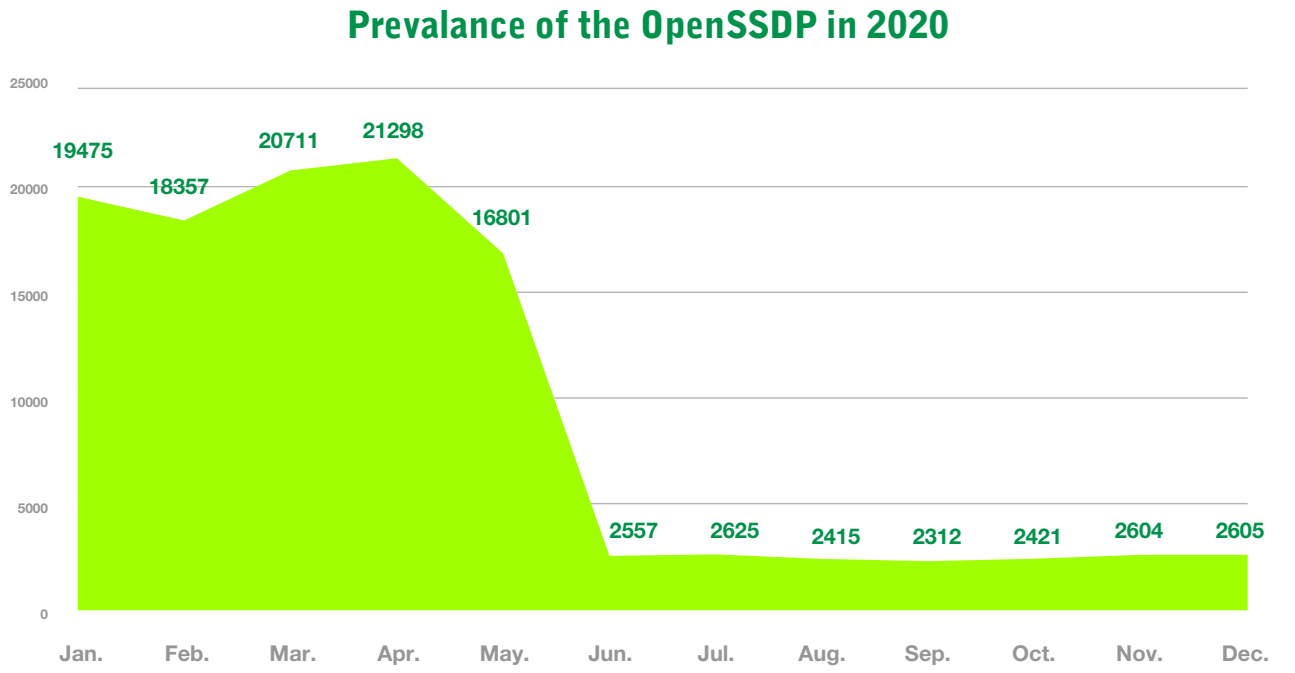


Figure 8 – Number of threatened unique IP addresses registered by CERT.LV in 2020 with the vulnerability OpenSSDP.

In May, CERT.LV called on ISPs not only to inform customers about incorrectly connected *UpnP (Universal Plug and Play)* devices, as *UPnP* technology is only intended for use in the internal network, but also recommended to restrict network-level access to the *SSDP* service used to provide *UPnP* functionality by blocking the UDP1900 port or centrally disabling *UPnP* functionality on managed client internet access devices. Starting from June, the average number of unique IP addresses registered per month with configuration deficiencies in *OpenSSDP* was 2,500 — a decrease of 87.5% (Figure 8).

CERT.LV conducted inspections of the email settings of municipal and state institutions in order to establish their compliance with Cabinet of Ministers Regulation No. 442 *Procedures for Ensuring Compliance of Information and Communication Technology Systems with Minimum Security Requirements.* The requirements demand the use of the *DMARC* (*Domain-based Message Authentication, Reporting & Conformance*) protocol. The inspections revealed that only one third of the resources tested met the requirements because they used the appropriate technology, but it should be emphasised that this type of inspection does not fully verify that the technology has been implemented correctly.

Via internet service providers, CERT.LV regularly informed internet users about all significant vulnerabilities and how to treat them. These tips can be found here: https://www.esidross.lv/informacija-par-apdraudejumiem/.


3!
Responsible
Vulnerability
Disclosure

CERT.LV supports the good practice of responsible detection of IT security vulnerabilities, and invites security researchers to report vulnerabilities to CERT.LV so that CERT.LV can actively coordinate the prevention of vulnerabilities, thus better protecting the Latvian internet space.

During the reporting period, CERT.LV received several reports about detected vulnerabilities in various resources of state and municipal institutions. As a result of these reports, a number of government websites were protected mainly from cross-site scripting (XSS) attacks, which, if successful, would allow an attacker to perform actions in a user's browser, such as manipulating site content and cookies or taking advantage of browser-appropriate exploits. In one case, it was found that developers created new vulnerabilities while trying to prevent them, and it affected the functionality and security of the resource. An additional security audit was performed on the resource to detect and address the vulnerabilities.

Security researcher Oskars Veģers cautioned about a newly discovered *zeroday* vulnerability within the *MS Teams* platform. The vulnerability allowed attackers to take over the entire infrastructure and *Office 365* accounts by remote code execution. The implementation of the attack did not require the user's involvement (*zero-click*), only the sending of a properly prepared message to the user. Such a discovery only once again confirms the high level of knowledge and training of our specialists, which is definitely worth being proud of!

In 2021 as well, CERT.LV invites to report discovered vulnerabilities by writing to cert@cert.lv; more about the responsible detection of vulnerabilities on the CERT.LV website https://www.cert.lv/lv/par-mums/atbildiga-ievainojamibu-atklasana.

4.

Penetration Tests

Penetration tests are an important step in making sure that the online resource created — system, database, website, etc. — complies with established safety requirements and good practice principles. During the year, CERT.LV specialists performed several penetration tests on various information resources of national significance, in some cases repeating it. In certain cases, significant deficiencies were identified, but in some of the trials it was found that the systems were designed in accordance with safety requirements and no safety deficiencies were identified or they were deemed insignificant, easily fixable. For information system maintainers, CERT.LV prepared a report on the performed tests and their results, as well as provided recommendations for the elimination of deficiencies.

In some cases, the system was found to use outdated, endangered technologies for which the manufacturer no longer provides technical support and updates. Long-term compliance with security requirements is hampered if resources and funding are only provided for project development, but not for further maintenance of the project and ensuring an adequate level of security throughout the life of the project or resource.

5.

Informative Communication Events


15° SALDUS
IZGLĪTOTS DARBINIEKS - LABĀKAIS PRETTRIECIENS KIBERUZBRUKUMIEM REĀLAJĀ DZĪVĒ
PANORĀMA
7:25


.LV


CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija
Gints Mālkalnietis
CERT.LV KIBERDROŠĪBAS EKSPERTS


KĀ SARGĀJAM LATVIJU?
Latvijā kiberuzbrukumi uzņēmumiem tiek konstatēti ik dienu


FINANŠU
NOZARES
ASOCIĀCIJA
mastercard
viedpircējs


Baiba Kaskina
zoom


CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija


KĀ SARGĀJAM LATVIJU?
Latvijā kiberuzbrukumi uzņēmumiem tiek konstatēti ik dienu

The opinion of CERT.LV experts in 2020 has been especially important — interviews and answers to media questions on both TV and radio on various topical topics related to cybersecurity were provided. Altogether, CERT.LV has appeared in more than 422 TV, radio, website and print media publications in both Latvian and Russian.

During the reporting period, the media was particularly interested in pandemic-related cyberattacks, data collection campaigns (phishing), fraudulent lotteries, and telephone frauds of scammers impersonating bank employees. The opinion of CERT.LV experts is most actively — 49.3% of all publications — expressed on internet websites, 30.6% — on the radio, 11.1% — on TV and 9.0% — in printed publications. The estimated portion of Latvian citizens reached exceeds 1.2 million.

CERT.LV maintains the website https://cert.lv, where information on current threats, recommendations for increasing the level of IT security, information on various events and a calendar of events can be found. In 2020, 104 news items were published on the website, 32.7% of which were news and monthly, quarterly and annual reports, while 28.8% were warnings about fraud and malware, 16.3% were informative announcements, 15.4% were recommendations for action and only 6.7% were about events. During the year, the CERT.LV website had a total of 108,007 unique visits or sessions from 70,935 users.

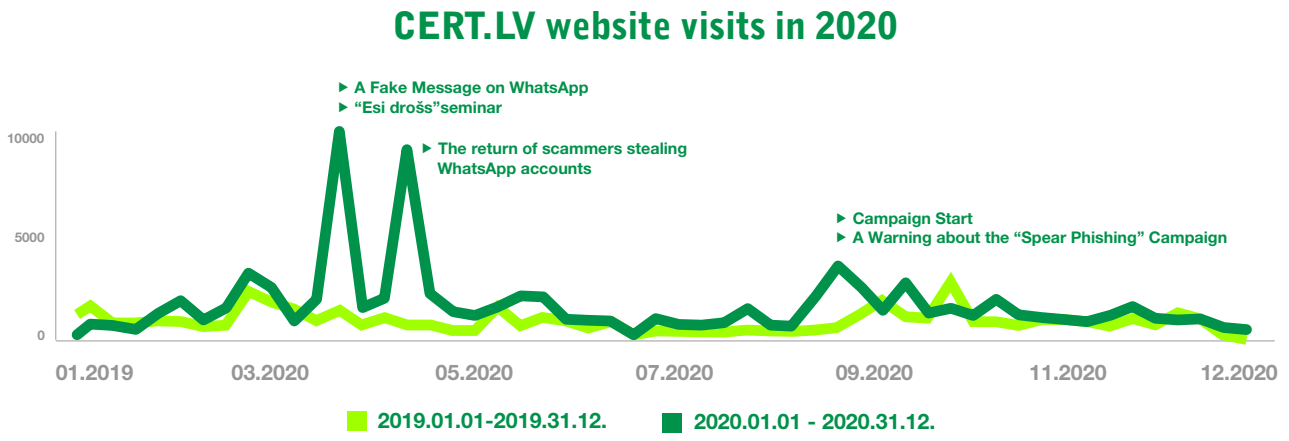


Figure 9 — CERT.LV website visits in 2020.

CERT.LV also maintains the user education portal www.esidross.lv, regularly publishing new articles with tips and suggestions for internet users on how to operate more safely in the virtual environment. During the reporting period, an important information communication event was the public educational campaign *Kiberdrošība darbavietā* (Cyber Safety in the Workplace, 14.09-11.10). As part of it, the portal www.esidross.lv underwent visual changes to make it more convenient for its users. During the campaign, the public was introduced to three new Latvian words "parolīze" (careless conduct with work passwords, emails and the internet which leads to the workplace being destroyed or paralysed), "muļķerēšana" (attempts to scam people who carelessly enter their login information on random websites), "spaidonis" (an uncontrollable urge to download and click on everything one finds on the internet) through special videos, advertising and articles. In total, more than 500 thousand Latvian internet users were reached. In the campaign materials, CERT.LV experts provided advice on how to create persistent and effective cyber security habits, how to best take care of the security of your equipment, how to create effective passwords and remember them. The total number of views of the campaign videos on *YouTube* reached 427 thousand, and almost 400 participants decided to test their newly acquired knowledge in practice, answering catchy questions in the campaign's digital guide — rokasgramata.esidross.lv. All campaign materials will continue to be available on the website www.esidross.lv.

In order to facilitate the communication of the participants of the initiative *Responsible Internet Service Provider* (Atbildīgs interneta pakalpojumu sniedzējs) with its end users about the threats identified in their equipment, as well as to provide users with information on various threats, their impact and prevention opportunities, CERT.LV published the active threat descriptions on the website esidross.lv https://www.esidross.lv/informacija-par-apdraudejumiem/.

During the reporting period, monthly cybersecurity bulletins *OUCH!* were issued and published on the website https://cert.lv and in the portal www.esidross.lv in cooperation with the *SANS* Institute. In the bulletins, internationally recognised cybersecurity specialists provide commentary on current cyber threats and practical recommendations for improving individual cybersecurity in a way that is understandable to any internet user. CERT.LV will continue to ensure the availability of these monthly bulletins for Latvian internet users in 2021 as well.

The social network platforms used by CERT.LV — *Facebook*, *Twitter* and also *YouTube* — are becoming more and more important in everyday communication.

CERT.LV cyber security experts' opinions, warnings and recommendations are followed by:

- 2852 people on *Twitter* (*twitter.com/certlv*); on average one CERT.LV message reaches 2,000 Twitter users.
- 3576 people on *Facebook* (*facebook.com/certlv*); on average one CERT.LV message reaches 11,000 *Facebook* users.
- 177 people on *YouTube*.

As a result of the pandemic, there was a significant increase in the number of followers of CERT.LV social media profiles — on Facebook by 63.5%, on Twitter by 19.3%. This significantly increased the reachable audience of CERT.LV news compared to the previous year, thus ensuring greater awareness of the Latvian public about current events in the country's cyberspace.

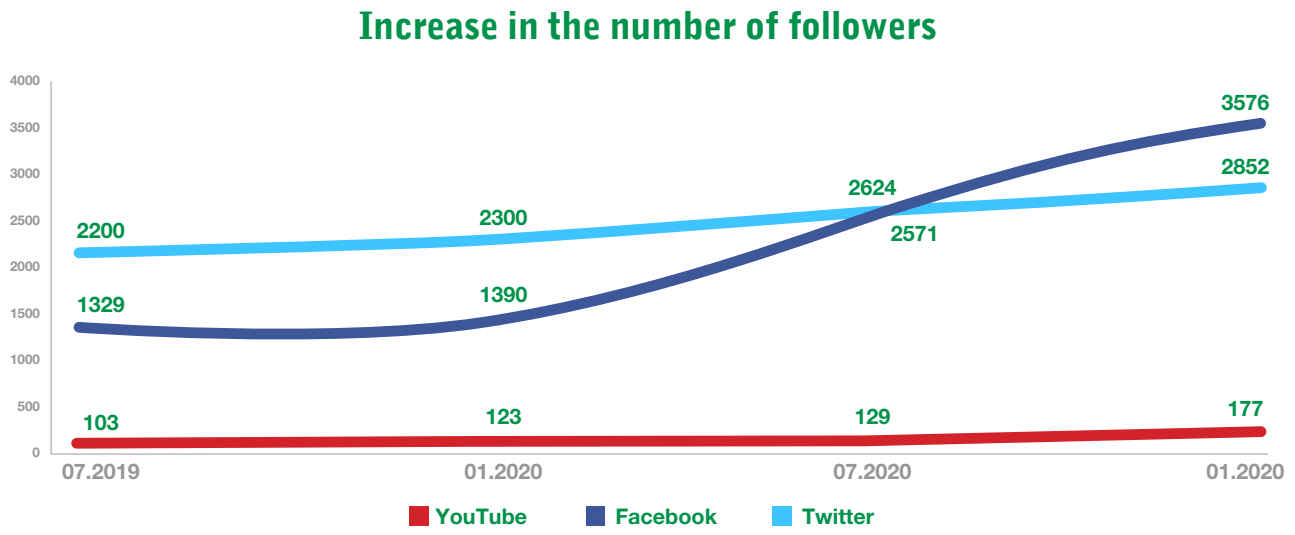


Figure 10 — the popularity of CERT.LV social media profiles in 2020.

6.

Educational Events

The number of events in 2020 was notably affected by the Covid-19 pandemic and the need to organise events remotely. The number of events in the second and third quarters is small, as only a small number of organisers and participants had managed to switch to remote work mode. CERT.LV continued to organise educational events on cybersecurity issues for IT security specialists, employees of state and municipal institutions and the general public. During the reporting period, CERT.LV participated in 58 events and educated 6758 participants.

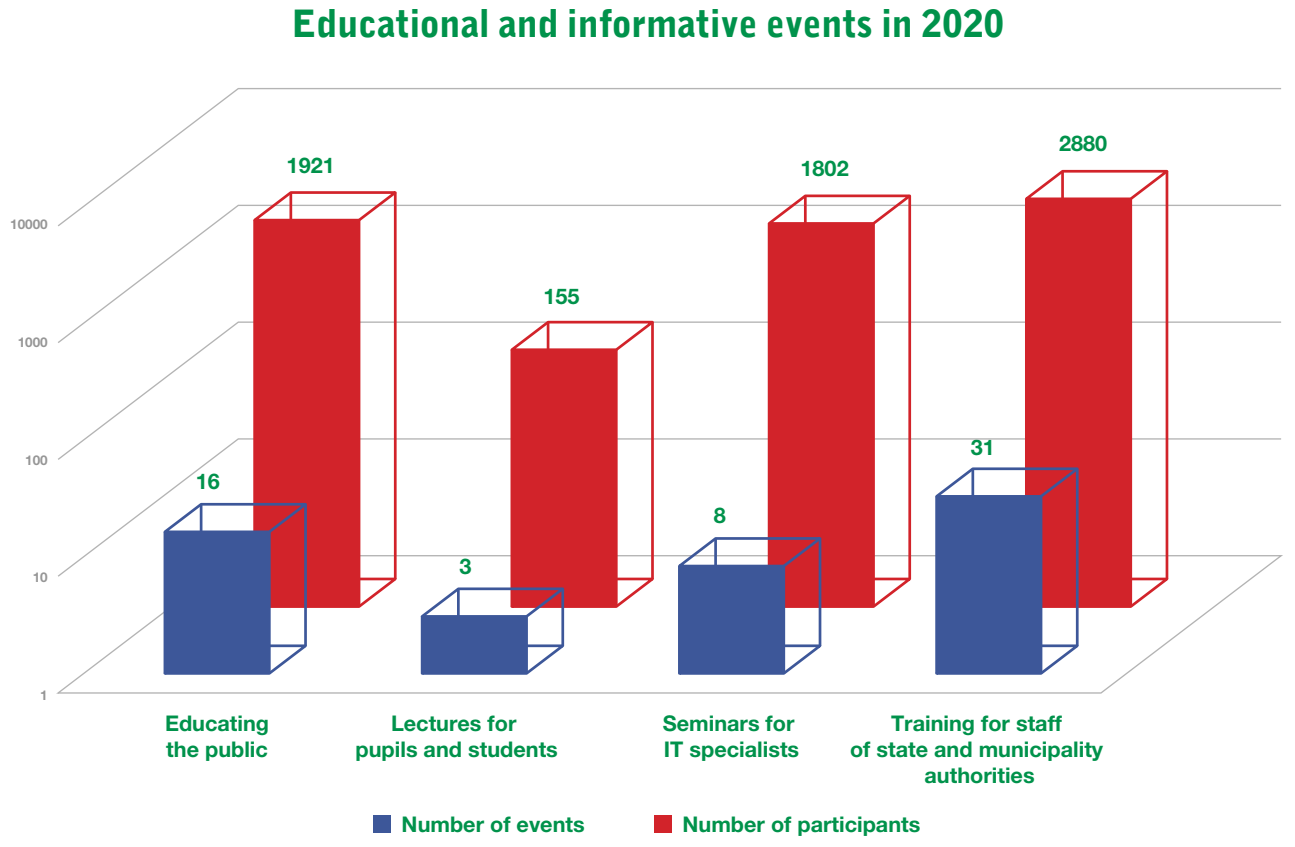


Figure 11 — Number of events and audience reached in 2020.

6.1. International Cyber Security Conference Cybershock 2020

Due to the pandemic, it was decided not to organise the annual international IT security conference *Cyberchess* (Cyberchess) during the reporting period. In accordance with the epidemiological requirements, on 1 and 2 October, at the beginning of the European Cyber Security Month, the technical cybersecurity conference *Kiberšoks 2020* (Cybershock 2020), https://cybershock.lv/), organised by CERT.LV, took place online. It covered various technical topics related to cybersecurity in-depth, with practical examples and demonstrations, such as the methods used by cryptographic anti-virus protection against detection, the use of the *Yara* tool and the analysis of digital image metadata. 760 participants signed up and remotely attended the conference; the presentations were given by seven lecturers from five different countries. In cooperation with *Cybexer Technologies* and *Tet group,* a *Capture the Flag (CTF)* competition was held simultaneously with the conference, and 100 participants from 29 teams took part in it.


Cyber Stuck
2020
YC520


VBS & VTL
• Virtualization Based Security
• Virtual Trust Levels
• Created via SLAT and Hypervisor
• Used for kernel exploits mitigation
• Partition still same
• Rings still same
• VTL1 > VTL0

Dan Demeter, Cybershock 2020

Copy link

Dan Demeter

Up your Threat Hunting Game using Yara

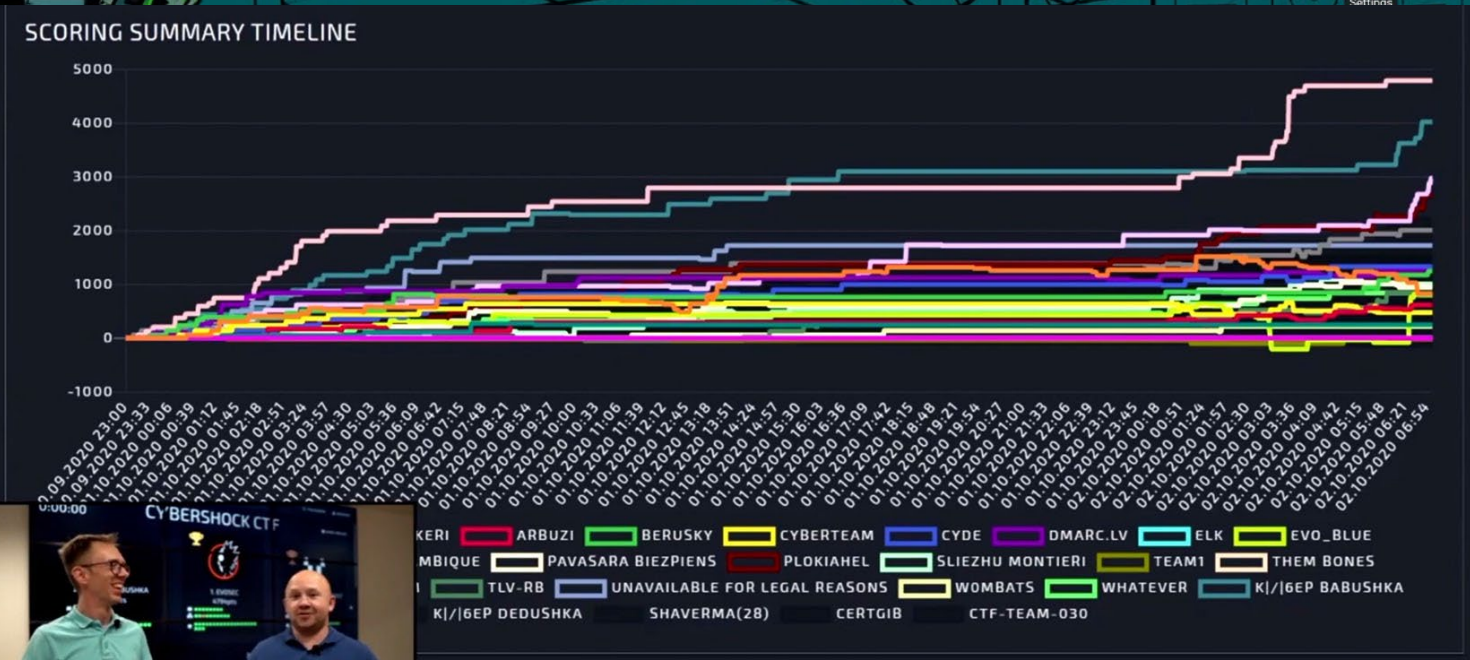
CERT.LV tet CYBEXER TECHNOLOGIES

Co-financed by the Connecting Europe Facility of the European Union

MENTI.COM : 27 53 59 8

MORE VIDEOS

Settings



Dan
@_xdanx

One of the most kick-ass virtual stages I've seen :)

> **CERT** @certlv · Oct 2, 2020
> Ready to start second day of the technical cybersecurity conference CyberShock with @_xdanx @lazyactivist192 @hanskan @bb_certlv Kārlis Apalups and Uldis Lībietis

2:03 PM · Oct 2, 2020 · Twitter for Android

Hans Lõugas @hanskan · 1h
Thanks for the cool shirt, was a great CTF 👏 @certlv @bb_certlv @CybexExchange @ctf_tech

Kelsey Hightower @kelseyhightower · Dec 6
If virtual events are going to become the norm, then I hope a bunch of local studios and sound stages pop up, as I can't be the only one tired of these talking head videos.

31 35 590

Randy Pargman
@rpargman

Replying to @kelseyhightower

Did you happen to see the CyberShock 2020 conf put on by @certlv? That was an outstanding effort with a proper stage setup and good production quality. I'd like to see more great events like that!

2:53 AM · Dec 6, 2020 · Twitter for iPhone

6.2. Events Organised by CERT.LV for IT Security Specialists

In addition to the international cyber security conference *Kiberšoks 2020* (Cybershock 2020), which was targeted towards IT security professionals, two more thematic seminars *Esi drošs* (Be safe) were organised. Every year in spring and autumn, they bring together mainly state and municipal authorities responsible for IT security and other representatives of the IT industry. During the pandemic, the *Esi drošs* (Be safe) seminars were held online. On average, 400 participants watched and applied for the seminar each time. Presentations and recordings are available on the website www.cert.lv.

In March: During the *Digital Week*, *Esi drošs* (Be Safe) addressed various issues and security aspects related to the organisation of remote work.

In December: *Esi drošs* (Be safe) seminar participants were introduced to current IT risks and cyberthreats to state and municipal authorities, trust service providers and electronic identity, a study on the European Commission's digital security law, the implementation of a single state and municipal web platform, cyber incident response action plan, and the relevant cyberattack campaigns in Latvia in 2020.

In mid-October, CERT.LV organised practical seminars for IT security specialists on the good practice of email system protection, providing practical knowledge about the *DMARC* implementation process and email system security auditing. Due to the great interest, the seminars were reorganised. A total of 113 information technology security specialists participated in the seminars.

6.3. CERT.LV Presentations on IT Security for Public Education

Every year, CERT.LV carries out active work to educate the public by organising and participating in various thematic seminars, informing them about current events in the field of cybersecurity, as well as by reminding them about good practices for protecting oneself and one's equipment.

On **September 14**, CERT.LV launched a month-long informative and educational campaign *Kiberdrošība darbavietā* (Cyber Security in the Workplace) to promote the understanding of state and municipal institution workers and other employees about cybersecurity. This was done in order to enhance the employees' ability to identify and prevent potential cyberattacks. As part of the campaign, three informative explanatory videos were developed on the use of passwords (https://www.esidross.lv/2020/09/13/apturi-parolizi) for data fraud attempts (https://www.esidross.lv/2020/09/13/nepaklaujies-mulkeresanai) and other fraudulent online activities (https://www.esidross.lv/2020/09/13/neesi-spaidonis), as well as practical tips for following good cybersecurity practices have been compiled by creating a Digital Handbook (https://rokasgramata.esidross.lv/). New words were used to make cybersecurity issues more attractive: parolīze, muļķerēšana and spaidonis (see definitions in paragraph 5). During the campaign, a number of topical articles for major news portals was produced, and interviews were held both on TV and on radio. The campaign was supported by the European Union's *CEF* project *Improving Cyber Security Capacities in Latvia* (INEA/CEF/ICT/A2017/1528784).

Other key events of 2020 include:

30 January — participation in the annual conference of the Latvian Open Technology Association, presentation on Open Data Initiatives in Latvia and Examples in the World, reviewing various open data projects and inviting to evaluate the security aspects of such projects.

11 February — taking part in the discussion *What Doesn't the Internet Tell You? Or individual and national digital security* as part of the *SkeptiCafe* project (café for the promotion of science and critical thinking — a soiree for like-minded people).

11 February — together with NIC.LV, participation in the *Safer Internet Days* event organised by the *Riga Central Library branch library Pūce*, where students were introduced to domain names, phishing and other aspects related to safe internet use.

26 March — participation in the remote informational event *Mazā Kibernakts* (Small Cybernight) organised within the framework of the *European Digital Week*, organised by Latvia State Radio and Television Centre. The event also focused on remote work and related challenges, including various risks of cyberattacks, document signing and childcare using digital technologies. The event was streamed on the social network *Facebook* and on the website lmt.straume.lv.

29 October — participation in the conversation on data security and protection organised by the Latvian Council of Science — *How to live on social networks?* The aim of the event was to give an opportunity to hear the opinions of recognised professionals or scientists on topical issues in society.

11 November — within the framework of participation in Riga Conference 2020, an interview on personal cyber security issues was given (https://www.rigaconference.lv/video/).

2 December — within the framework of the Latvian Information and Communication Technology Association annual ICT industry conference *DIGI->FIT 2020*, the most prestigious ICT industry award, *Platinum Mouse 2020*, was also awarded in the category *Best Cybersecurity Initiative*. This year it was received by *PwC cyber security escape room*, which educates employees about cybersecurity in the form of a cybersecurity escape room. The aim of the category is to increase the role of cybersecurity issues in the development of ICT solutions by raising awareness of cybersecurity, as well as to promote the creation of innovative solutions and increase their visibility. Awards were presented in four more categories, as well as one special award was given. CERT.LV participated in the evaluation commission of applications submitted for the *Platinum Mouse 2020* award.

7.

Strategic Cooperation 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.

In Latvia, the work was continued by the **National Information Technology Security Council**, the aim of which is to coordinate the planning and implementation of tasks and measures related to information technology security in Latvia. Representatives from CERT.LV are also involved in the work of the Council.

CERT.LV closely cooperated with the National Cyber Security Policy Coordination Division of the Ministry of Defence, and within its competence actively participated in the implementation of the National Cyber Security Strategy. The most important nationwide activities of 2020, in which CERT.LV took part:

- Carrying out a study on the most popular remote communication tools in order to present detailed results to the main cooperation organisations and to promote informed decision-making of other cooperation partners and an appropriate level of IT security. During the analysis of the tools, they were evaluated both from the aspect of data security and their offered functionality, country of origin, identified vulnerabilities, etc.
- Instructions for the configuration of *MS Exchange* servers were prepared, which would facilitate more efficient spam filtering and the recognition of potentially harmful emails. The recommendations were also disseminated to other state institutions through the Ministry of Defence.
- CERT.LV provided consultations to state and municipal institutions on the application of Cabinet of Ministers Regulation No. 442 *Procedures for Ensuring Compliance of Information and Communication Technology Systems with the Minimum Security Requirements*, as well as during the development and coordination of changes to ensure the minimum security framework for target audiences covered by the *Information Technology Security Law*.

- Representatives of CERT.LV participated in the opening meeting, which was dedicated to the evaluation of the implementation of *NIS (Network and Information Security Directive)* and its possible changes. Representatives of CERT.LV provided an assessment of the implementation of the NIS Directive in Latvia, as well as participated in an interview organised by EC representatives on this issue, both as a national CERT unit and as representatives of the *Digital Security Monitoring Committee.* CERT.LV expressed its opinion on the relevant issues regarding the NIS Directive, for example, the necessary clarifications in the NIS Directive for the identification of digital service providers in connection with exceptions. CERT.LV also expressed concerns about plans to create new EU-wide administrative regulations, creating an additional burden.
- CERT.LV participated in the meetings of the *Digital Security and Reliability Working Group*, providing support to the MEPRD in preparing the Digital Transformation Guidelines.
- CERT.LV provided recommendations for changes to the *Electronic Communications Law* regarding the right of CERT.LV to request the disabling of .lv domain names, so that the right to disable or change domain name records would be regulated together in the *Information Technology Security Law.*
- CERT.LV participated in the meetings and provided comments on the amendments to the *Saeima Election Law*, which envisages the use of the electronic online voter register in polling stations abroad located at the diplomatic and consular missions of the Republic of Latvia upon the voters' proposal.
- CERT.LV commented on the draft informative report prepared by the Ministry of Transport and the MEPRD and the draft protocol decision *On the Use of the Fourth and Sixth Versions of the Internet Protocol in Public Administration*, expressing their concerns about the existing security risks.
- CERT.LV participated in discussions on the inclusion of responsible vulnerability detection in regulatory enactments, providing examples of international experience and considering practical vulnerability detection situations.

- CERT.LV participated in a meeting organised by the *Financial Industry Association* on cooperation between banks, electronic communications companies and the regulator. CERT.LV provided consultations on technical aspects regarding fraudulent telephone calls, call numbering and previous incidents.
- Cooperation was initiated with the *Consumer Rights Protection Centre (CRPC)* in the study of Internet of Things (IoT) devices in order to assess the security of IoT cases.
- CERT.LV participated in a meeting with the State Audit Office on how state institutions ensure the continuity of a service, what incidents have occurred, how incident reporting is organised and controlled.

CERT.LV is an active member of the **Digital Security Monitoring Committee**, the operation of which is determined by Cabinet of Ministers Regulation No. 695 of 1 November 2016. The Committee is a collegial supervisory institution under the Minister of Defence, the purpose of which is:

- To monitor and register qualified electronic identification service providers and qualified high-security electronic identification service providers and the services provided by them in the register of qualified electronic identification service providers.
- To monitor and approve trusted certification service providers and the services they provide, and establish, maintain and publish trusted lists.

In 2020, under the supervision of LVRTC and other trust service providers, the Committee reviewed and re-approved LVRTC as a qualified electronic identification service provider and its qualified electronic identification means, certified LVRTC service *eSignature* in accordance with *eIDAS* requirements, recognising it as a qualified electronic signature after a positive audit report was received, evaluated and accepted the changes in the procedure for issuing the PIN/PUK code of *eID* cards and conducted research on the issues of certification of a qualified signature creation device.

CERT.LV closely cooperated with the **Cyber Defence Unit** of the National Guard, which in the event of an IT security crisis or threat, in cooperation with CERT.LV, could provide support to the

state and the private sector. The Cyber Defence Unit has been established in accordance with the National Guard Law, uniting experts employed in the private sector who are willing to participate voluntarily, and who are interested in establishing regular cooperation regarding IT security issues in their free time, improving expertise and knowledge at the national and international levels. In 2020, the most important cooperation took place in the cyber security training *Crossed Swords*, both in creating the learning environment and participating in the learning process. The unit was also involved in solving individual incidents, in which the Cyber Defence Unit provided support in system security assessment.

Any interested information technology expert is invited to contribute to national security by joining the Cyber Defence Unit. Additional information about the unit and application can be found on the National Guard website https://www.zs.mil.lv/lv/zemessardzes-vienibas/zemessardzes-kiberaizsardzibas-vieniba.

CERT.LV also continued to coordinate the **Information Technology and Information Systems Security Expert Group**, which informally started its activities in March 2007, but was formally implemented in 2012 by establishing the group's statutes and code of ethics. Information Technology and Information Systems Security Expert Group meetings take place on the second Thursday of each month — they discuss cybersecurity issues in a free format. Information Technology and Information Systems Security Expert Group is the place where Latvian IT experts from various institutions and organisations can exchange views, good practices and experiences. Anyone who undertakes to comply with the Information Technology and Information Systems Security Expert Group's Code of Ethics and Statutes, as well as receives recommendations from two existing members, can join the group. More information on the CERT.LV website https://cert.lv/lv/iniciativas-un-aktivitates/drosibas-ekspertu-grupa-deg.

Together with the Latvian Internet Association (LIA), **the Responsible Internet Service Provider** initiative was continued, inviting Internet Service Providers (ISPs) registered in Latvia to cooperate by applying to CERT.LV for information on endangered end-user equipment and delivering it to its clients — internet users. As part of the initiative, ISPs are invited to respond to messages received from the Latvian Internet Association's Safer Internet Centre on illegal internet content on ISP

servers, informing the appropriate content provider accordingly and calling for the violation to be taken care of and illegal content to be deleted. Currently, 13 largest ISPs in Latvia have joined the initiative. More information on the CERT.LV website https://cert.lv/lv/elektronisko-sakaru-komersantiem/atbildigs-ips.

8.

International Cooperation

During the reporting period, CERT.LV consistently strengthened cooperation with IT security incident prevention units and international organisations in other countries. CERT.LV specialists also gave presentations at international conferences and seminars. New skills were acquired, and qualifications were improved by participating in international technical training programmes.

CERT.LV regularly participated in the meetings of the *NIS CSIRT Network* (NIS Directive CERT cooperation network). The goal of them is to strengthen cooperation between IT security incident prevention teams at the European level. The meetings take place three times a year and at the moment are organised by the country holding the Presidency of the Council of the European Union in cooperation with ENISA. Joint sessions with the NIS Directive cooperation group also take place once a year.

There are several topical working groups within the *NIS CSIRT Network*. Representatives of CERT.LV are also active in two of them: The *Cyber Weather* working group regularly collects information on major cyber incidents and produces a quarterly report on cyber weather for Europe; The *Maturity* working group is working to increase the maturity of IT security incident prevention teams in EU Member States.

Following the Covid-19 pandemic, the *NIS CSIRT Network* Information Exchange Group was set up in March. The aim of the group was the rapid circulation of information on incidents related to Covid-19, as well as on cybersecurity issues in the healthcare sector. For several months, information on the situation in all European countries was collected on a weekly basis and an overview was prepared for decision-makers in the *NIS Cooperation* Group and elsewhere.

Confirming the maturity and high qualification of the team, CERT.LV regularly participates in *peer reviews* of the IT security incident prevention units of the CERT cooperation network of the *NIS* directive. In 2020, CERT.LV audited the Slovenian national CERT unit SI-CERT and the Portuguese national unit.

CERT.LV is an active member of FIRST and continued to operate in the *FIRST Membership Committee*, helping to improve the membership process in order to ensure higher quality

information submitted for admission to the FIRST organisation. Baiba Kaškina, the head of CERT.LV, was elected co-chair of the *FIRST Membership Committee.*

CERT.LV also participated in the programme committee of the FIRST conference, providing support in the development of the conference programme, as well as participated in the TF-CSIRT/FIRST symposium in Malaga, where it gave several presentations.

Cooperation with the *NATO Cooperative Cyber Defence Centre of Excellence* (NATO CCDCoE), located in Tallinn, Estonia, is very important for CERT.LV. CERT.LV regularly conducts training courses for NATO CCDCoE. CERT.LV provides support in organising stages and secures the NATO CCDCoE technical cybersecurity exercises, such as *Crossed Swords* and *Locked Shields.*

CERT.LV took part in the organisation of *Crossed Swords*, participating in the preparation stage of the study content, development of the mock design and determination of the directions of the skills to be developed. In January 2020, the cybersecurity exercise *Crossed Swords* took place in Riga. It brought together more than 120 technical experts, national Cyber Command, special forces and military police from 26 countries. *Crossed Swords* has evolved from technical red flag team training into a unique and complex offensive cyber operation training programme that combines a variety of technical skills with a kinetic force component and spans multiple geographic locations simultaneously. The main emphasis of the training in 2020 was on transnational and interdisciplinary cooperation in the implementation of a full range of offensive cyber operations. *Crossed Swords 2020/II* took place in December in Tallinn, and there, too, CERT.LV was involved in both the training planning and development process, as well as the management of the training process.

Due to the pandemic, the course of *Locked Shields 2020* cyber security training was cancelled during the reporting period. Preparations for participation in the *Locked Shields 2021* cybersecurity exercise were launched and discussions were held with potential partners. In 2021, the Latvian team will participate in the training in cooperation with the team from the Republic of Korea (South Korea). This will be the first time in the history of *Locked Shields* that such interregional collaboration will take place within a single team, providing valuable experience from the viewpoint of cultural, technological and geographical factors.

CERT.LV regularly participates in the international cybersecurity training *Cyber Europe* organised by *ENISA* (European Network and Information Security Agency). Although the training planned for 2020 was cancelled due to the Covid-19 pandemic, preparations for the next time in autumn 2021 will continue.

During the reporting period, CERT.LV also participated in several discussions and provided recommendations and feedback on the implementation of the NIS Directive, development of the EU Cyber Security Act and its impact on the CERT network, creation of a single European cyber unit, legal framework for cyber security requirements for ICT products and critical infrastructure protection.

An in-depth study of the fraudulent activity tool *Sp0m* was carried out in collaboration with the Italian CSIRT team. The tool is intended for use on social media platforms, and it provides partial automation of malicious activities for cyber attackers. The results of the study were communicated to both the CERT community and the general public. The research made it possible to find out how the compromised websites are obtained, which are used for the respective tool to host harmful content.

On 20 November, CERT.LV was admitted to the Energy Information Exchange and Cooperation Group *Energy ISAC Camelot.* This group currently consists of teams from the EEA Energy and National CERT units from Austria, Sweden, Norway, Switzerland, Finland and Latvia.

9.

Implementation of Projects Co-financed by the EU

The implementation of the project **Improving Cyber Security Capacities in Latvia** (agreement with the European Commission No. INEA/CEF/ICT/A2017/15287842018) started on 1 September 2018 and continued until 31 December 2020. The aim of the project, as its name suggests, was to strengthen Latvia's cybersecurity capacity. During the implementation of the project:

- Active involvement in the development and testing of *MeliCERTes — Cyber Security Core Service Platform* continued. The aim of the platform is to provide a unified framework for the resolution of international cyber incidents and the exchange of information on cyber incidents by summarising the requirements of IT security incident prevention units for international cooperation.
- Work continued on the *Deep Analysis System: Pastelyzer – the Paste Analyzser* development. A beta version of the *Deep Analysis System* was released and presented at the TF-CSIRT conference in Malaga to the wider CERT community, inviting CERT teams to work together to further develop the system. The purpose of the system is to ensure the automated selection and analysis of large amounts of data as part of the day-to-day work of the existing IT security incident prevention units. Several teams responded to the challenge. The system, installation instructions and the user manual is available here.
- Almost 40% of CERT.LV employees were provided with qualification improvement, allowing them to obtain internationally recognised certificates and to strengthen the overall maturity of the CERT.LV team.
- An informative and educational campaign Kiberdrošība darbavietā (Cybersecurity in the Workplace) was actively prepared and implemented. The campaign went on for one month from 14 September to 11 October. Employees of organisations and companies — internet users — were addressed in an attractive way with the new words "parolīze", "muļķerēšana" and "spaidonis". During the course of four weeks, addressing the public through special videos, advertisements and articles, more than 500 000 Latvian internet users were reached. In the campaign materials, CERT.LV experts provided advice on how to create persistent and effective cybersecurity habits,

how to best take care of the security of your equipment, as well as how to create effective passwords and remember them. The total number of views of the campaign videos on YouTube reached 427 thousand, and almost 400 participants decided to test their newly acquired knowledge in practice, answering catchy questions in the campaign's digital user's handbook — rokasgramata.esidross.lv. All campaign materials will continue to be available on the website www.esidross.lv.

The implementation of the project **Cyber Exchange** (agreement with the European Commission No. INEA/CEF/ICT/A2017/1528784) started on 1 November 2018 and will continue until 30 June 2022. The project aims to strengthen international cooperation between national and government IT security incident units (CSIRT/CERT organisations). The *Cyber Exchange* project is a response to growing cyber security threats, with a particular emphasis on the necessary international cooperation in the fight against them. Latvia is one of the 10 European countries participating in the project. Experience exchange visits are planned within the project.

As a result of the travel restrictions set to limit the spread of the Covid-19 virus, the planned exchange visits, which are the main activity of the project, were cancelled in 2020 and the project will resume when the epidemiological situation improves.

10.

Services for Strengthening Latvian Cyberspace

DNS Firewall: Work continued on further development of the DNS RPZ (Domain Name Service Response Policy Zone) or DNS firewall. This project is developed by CERT.LV and NIC.LV. The project provides an opportunity to protect users from malicious content on the internet related to incident indicators already known to cybersecurity authorities (domain names, IP addresses, etc.). 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 date more and more successful cases where active protection has saved devices from becoming infected are known proving the success of the project. More information and detailed instructions available at https://dnsmuris.lv

Early Warning System: Early Warning System or the Sensor is a passive safety device that helps to identify threats and protect the user. Early Warning System provides data network traffic anomaly analysis, malware detection and alerts for detected threats.

Early Warning System installation and configuration is provided by CERT.LV, the organisation must provide two electrical connections and two network connections (*access + mirror).* A cooperation agreement is concluded for the installation of the Early Warning System. The service is primarily available to state and municipal institutions, as well as operators of essential services and digital service providers. To learn more about the Early Warning System and decide on its installation at your organisation, please write to: cert@cert.lv.

CERT.LV mission is to promote information technology (IT) security in Latvia.

Main objectives of CERT.LV are: to update informattion about IT security threats; to provide support to state institutions regarding national IT security; to provide support regarding IT security incidents to every private end user or legal entity, if the incident involves a Latvian IP address or .LV domain; to conduct research, organize educational events and trainings in the field of information technologies security.

Contact CERT.LV:

Telephone: +371 67085888

E-mail: cert@cert.lv

Web: www.cert.lv

Follow CERT.LV:

www.twitter.com/certlv

www.facebook.com/certlv

Co-financed by the Connecting Europe Facility of the European Union