CERT.LV
Information Technologies
Security Incident
Response Institution

Institute of Mathematics and
Computer Science University of Latvia

Ministry of Defence
Republic of Latvia

2021

CERT.LV Public Performance Report

The report contains publicly accessible information and does not contain information on CERT.LV's activities which contain confidential information. The report is for informational purposes only.

Contents

Introduction

Changes in our daily routines continued to affect us all in 2021, and before we get down to the next tasks in the rapidly changing cyberspace, we invite you to take a look back at the past year altogether.

In 2021, the global cyberspace experienced some major disturbances that were felt in Latvia as well. A series of critical vulnerabilities (*MS Exchange servers*, *Print Spooler*, *Log4j*, etc.) and high-profile cyber-attacks on foreign companies (fuel supply network Colonial Pipeline, meat processing company *JBS*, *Kaseya's* remote management tool, and the Irish e-health system) caused people to hold their breath.

Even though the year was full of newly discovered vulnerabilities, in many incidents that took place in Latvian cyberspace, the attackers' success was based on insufficient system protection – outdated software and weak passwords. The pandemic influenced the fragmentation of IT infrastructure making the security of individual workstations and users' cyber hygiene habits increasingly important and thus imposing additional threats.

As an additional test of citizens' vigilance, cyber criminals' innovative approach to fraudulent phone calls was implemented by using fake caller IDs – both by pretending to be a bank and by "borrowing" people's telephone numbers.

The cyber-attacks directly on supply chain companies around the world have also raised the issue of cybersecurity in Latvia. It highlighted the challenges for both Latvian companies providing products to the global market and for Latvian companies and organisations cooperating with information and communication technologies (ICT) suppliers.

Given that society's dependence on digital solutions and technologies has increased significantly, and that protection against cyber-attacks is becoming more challenging, it is important to prepare for these challenges well in advance.

Overall, CERT.LV registered 254,392 unique endangered IP addresses in the reporting period, which is about 36% less than in 2020. No significant fluctuations regarding the number of endangered IP addresses have been observed in the reporting period.

In 2021, CERT.LV organised and participated in 123 events, reaching and informing 13,619 participants. The pandemic restrictions forced the transfer of face-to-face events online, and while an online event does not completely replace a face-to-face event, it allowed a significant increase in the size of the audience covered.

On 6–7 October, as part of the European Cyber Security Month, CERT.LV organised *CyberShock 2021*, a technical online conference for cybersecurity professionals, where internationally renowned experts provided participants with an in-depth insight into a wide range of issues related to cybersecurity, whilst presentations also included real-time demonstrations. *CyberShock 2021* attracted 923 participants from 53 countries. In parallel with the conference, the CTF (*Capture the Flag*) competition took place, in which 31 teams took on various cybersecurity challenges.

In the next reporting period, protecting the digital environment against cyber-attacks will become increasingly important and challenging. **It is important to prepare for these challenges well in advance, without leaving action to the last minute when threats with potentially significant consequences have already occurred.**

As a large part of our society continues to work remotely, organisations and businesses **should look at the creation of individual, mutually independent cybersecurity solutions for individual devices to** improve cybersecurity. The frequently mentioned *Zero Trust* model is one way to facilitate this, in addition to enabling multi-factor authentication wherever possible. However, it is important to emphasise, **that it is the strengthening of each individual's cyber hygiene awareness** that is one of the cornerstones of cybersecurity in the new working environment.

Although, for the time being, supply chain attacks have had relatively little impact in Latvia, they are rapidly gaining popularity among criminals in the global cyberspace, as they provide an opportunity to compromise a range of customers and products developed by that supplier by compromising the supplier of one component. **Latvian companies manufacturing products for the global market need to take into account the possibility of becoming a target of cyber-attackers and pay increased attention to cybersecurity issues to** prevent attacks to compromise the supply chain.

The looming geopolitical tensions will also create additional challenges in the area of cybersecurity – therefore strength and resilience for all in 2022!

On behalf of the CERT.LV team,
Baiba Kaškina
Head of CERT.LV


AIZSARDZĪBAS
MINISTRIJA
CERT.LV
10. GADADIENĀ
Paldies par
sadarbību kiberdrošības stiprināšanā!
2021. gada 1. februārī


Cyber
SHOCK
2021
CS21
CS21

1.

Incident Processing

CERT.LV compiles information on 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 threats accounted for by CERT.LV are placed in a single registry and organised by types of threats (e.g. malware, intrusions, fraud), infections (e.g. *Conficker*, *Zeus*, *Mirai*) and vulnerabilities (e.g. *OpenDNS*, *Openrdp*).

During the reporting period, CERT.LV concluded that on average, there were 64 000 unique vulnerable IP addresses every month.

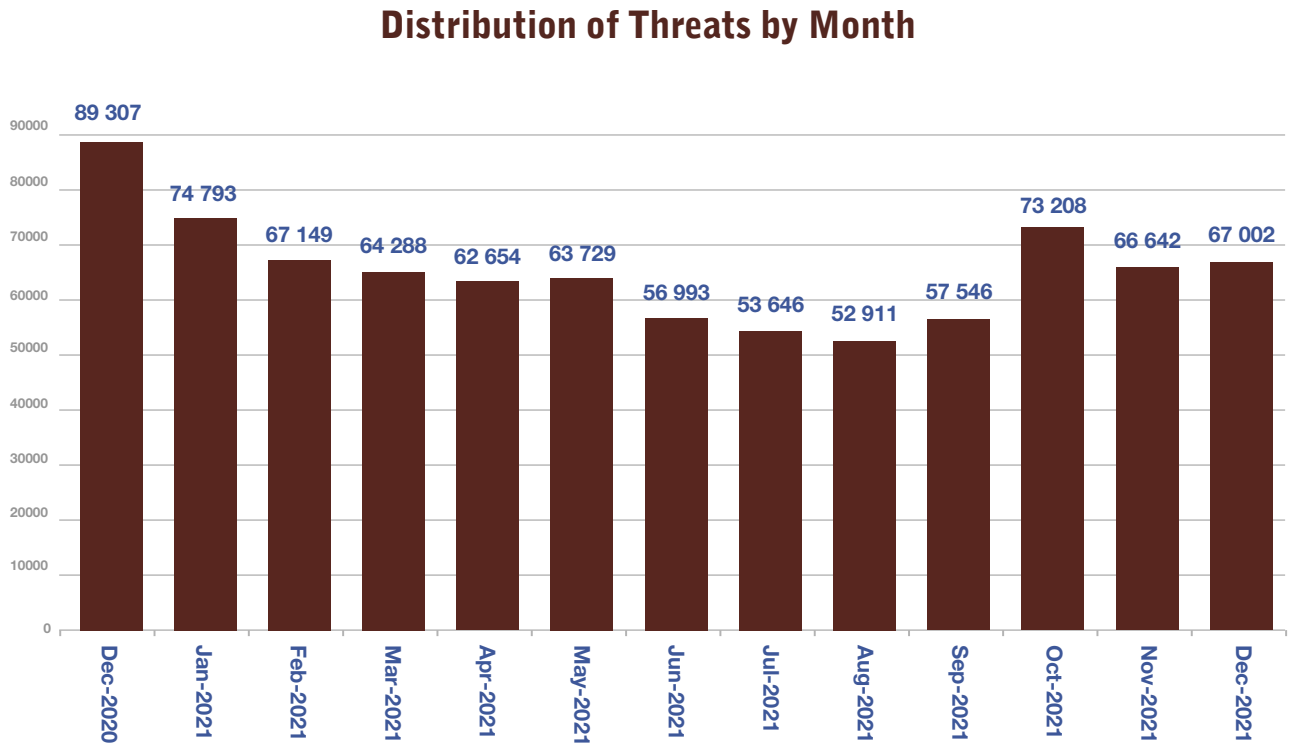


Image 1 – the unique endangered IP addresses registered by CERT.LV monthly in 2021

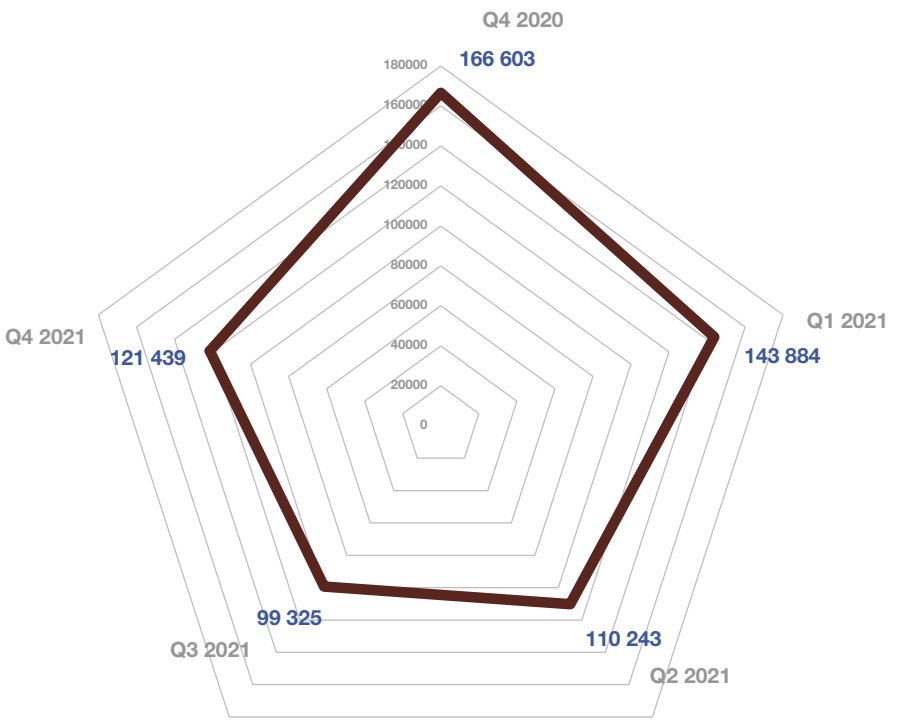


Image 2 – the unique endangered IP addresses registered by CERT.LV quarterly in 2021

Overall, CERT.LV registered 254 392 unique threatened IP addresses in the reporting period. No significant fluctuations regarding the number of threatened IP addresses were observed in the reporting period.

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

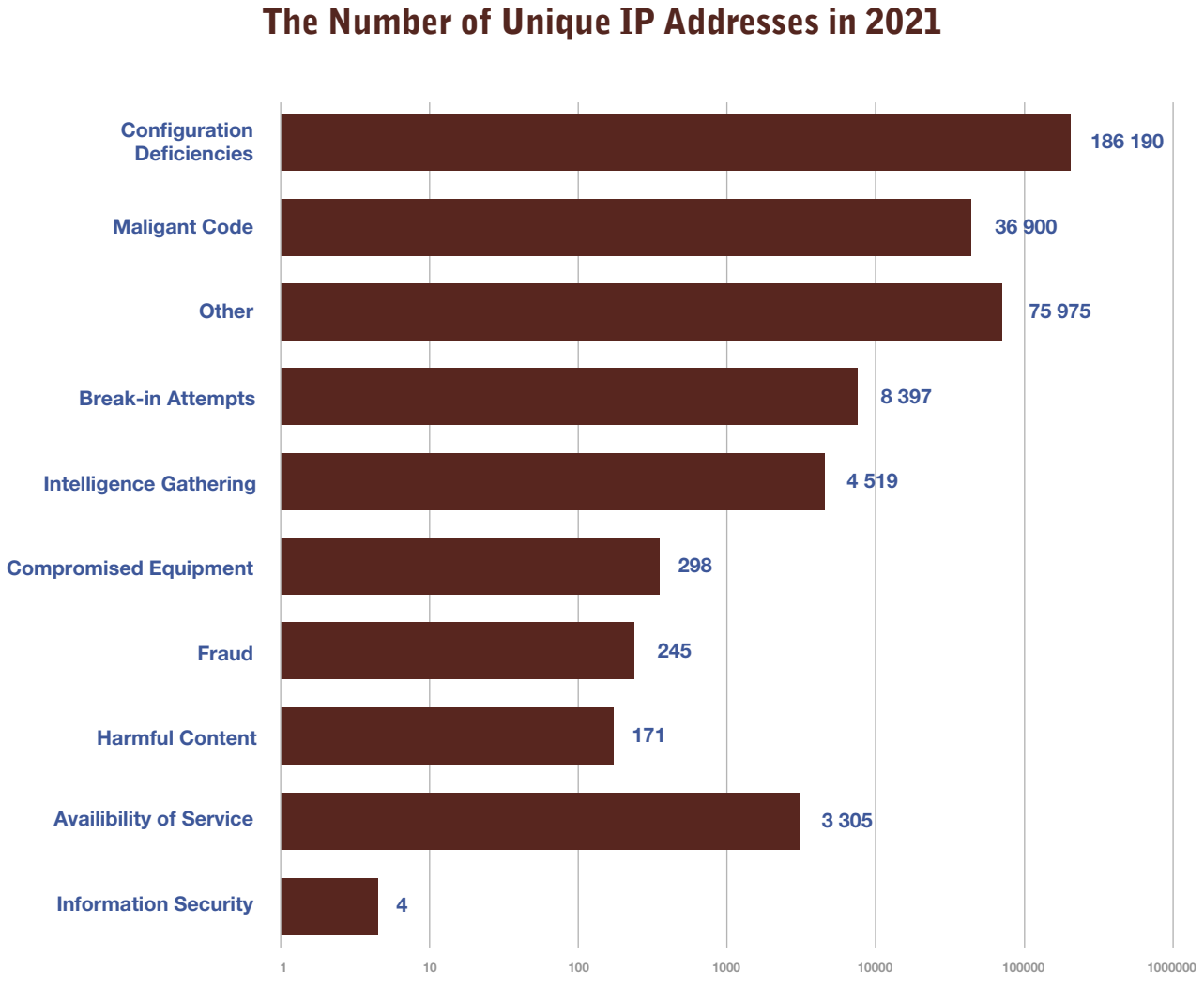


Image 3 – the unique endangered IP addresses registered by CERT.LV by type of threat in 2021

Number of Unique IP Addresses – Malignant Code in 2021

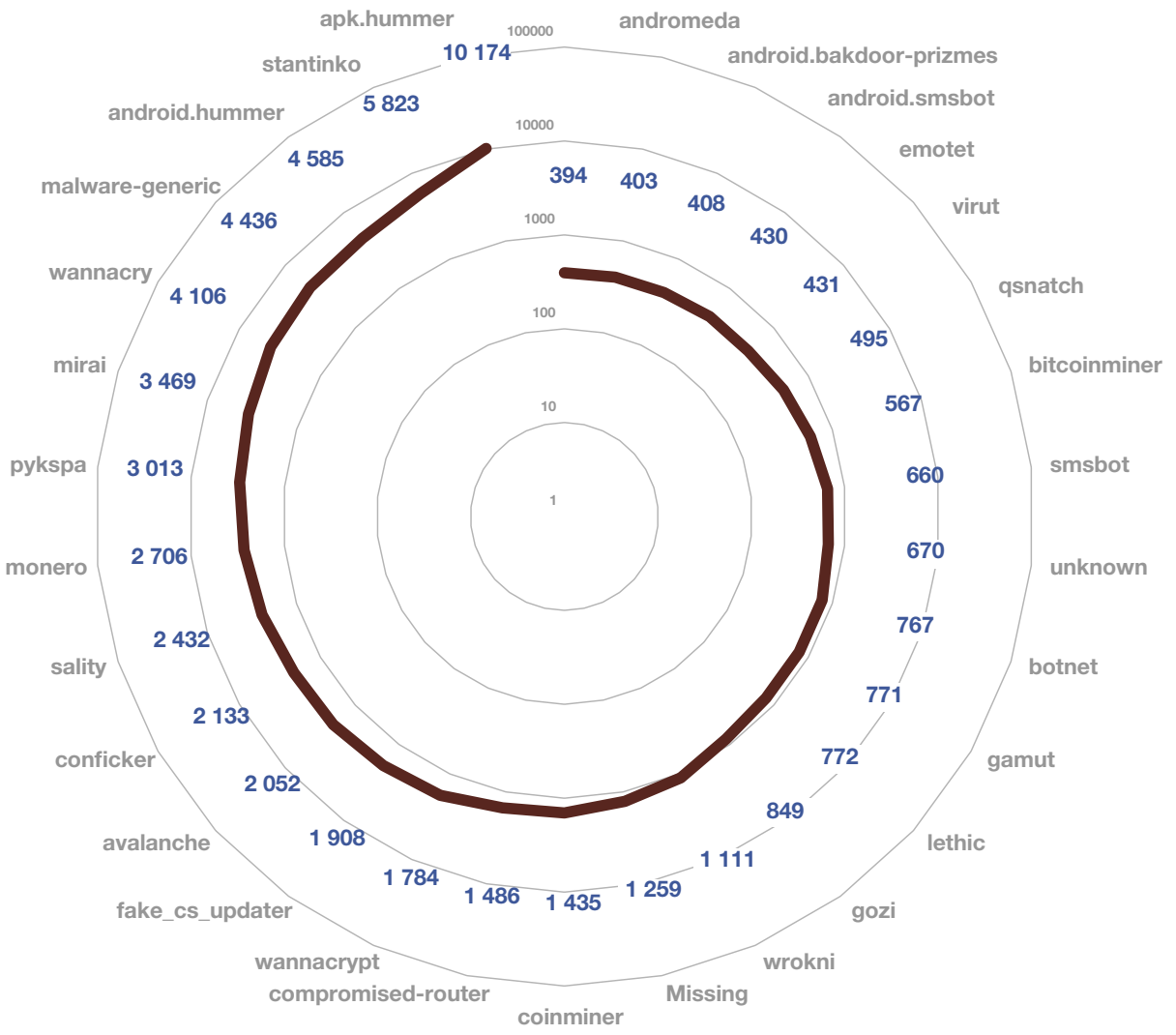


Image 4 – total number of unique threatened IP addresses registered by CERT.LV in 2021 with the type of threat: malicious code

The leading malware is *Apk.Hummer*, which displays pop-up ads on Android devices (tablets and smartphones) and downloads various apps independently.

In second place is the *Stantinko* malware, designed to mine various cryptocurrencies, using the victim's device resources in an unauthorised way, potentially overloading the device. It also displays ads to the user, thus providing a profit for the advertisers.

The third place goes to *WannaCrypt*, also known as the *Wannacry* ransomware. 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. The effect of the virus and it's spreading further can be prevented by installing software updates that are available even for unsupported *Windows* versions such as *Windows XP* and *Windows Server 2003.*

OpenmDNS (*multicast DNS*) is leading the list of vulnerabilities. In addition to being at risk of large-scale information leaks, these devices can be used in UDP amplification attacks, disrupting access to other devices and organisational resources.

In second place we find *OpenRDP*. RDP is a remote access solution that is often used in attacks. If good practices are not followed, and access to the RDP service is not restricted, for example by limiting the IP addresses allowed to connect or by defining access via VPN, an attacker can take control of inappropriately configured devices where remote access ports are freely open to the internet and a sufficiently secure access password is not set.

In third place is the *SSL-Poodle* vulnerability that exposes the device to a POODLE (*Padding Oracle On Downgraded Legacy Encryption*) attack, allowing attackers to intercept encrypted traffic such as usernames, passwords, cookies, etc., and impersonate the device's user.

By looking at the top vulnerabilities and malware, we can see that the ten most widespread configuration deficiencies in 2021 have been present in the Latvian cyberspace since 2017 (Image 6), whilst only five of the ten most widespread malware in 2021 were observed in the Latvian cyberspace in 2017 (Image 7).

Number of Unique IP Addresses – Configuration Deficiencies in 2021

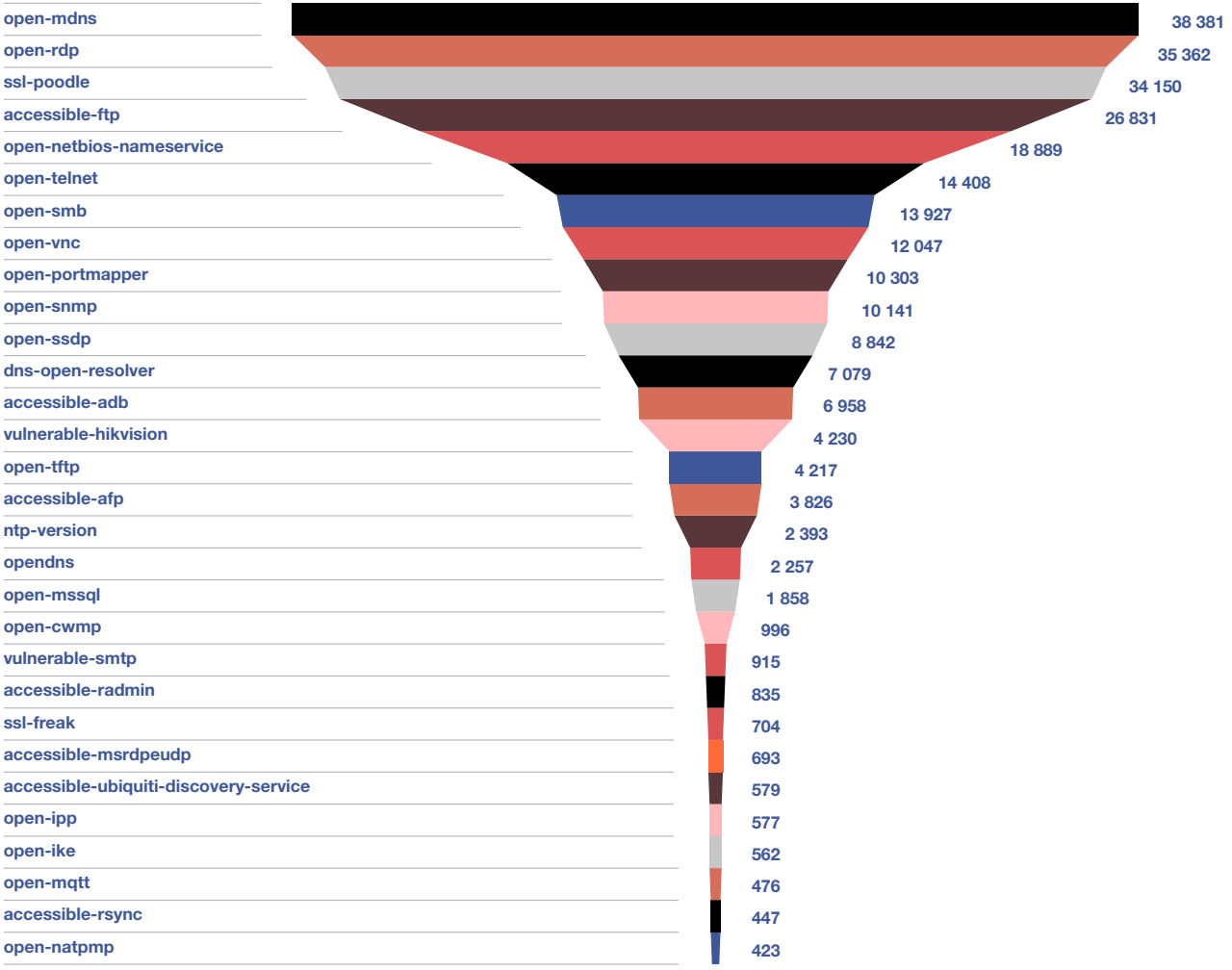


Image 5 – number of unique threatened IP addresses registered by CERT.LV in 2021 with the type of threat: vulnerabilities

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

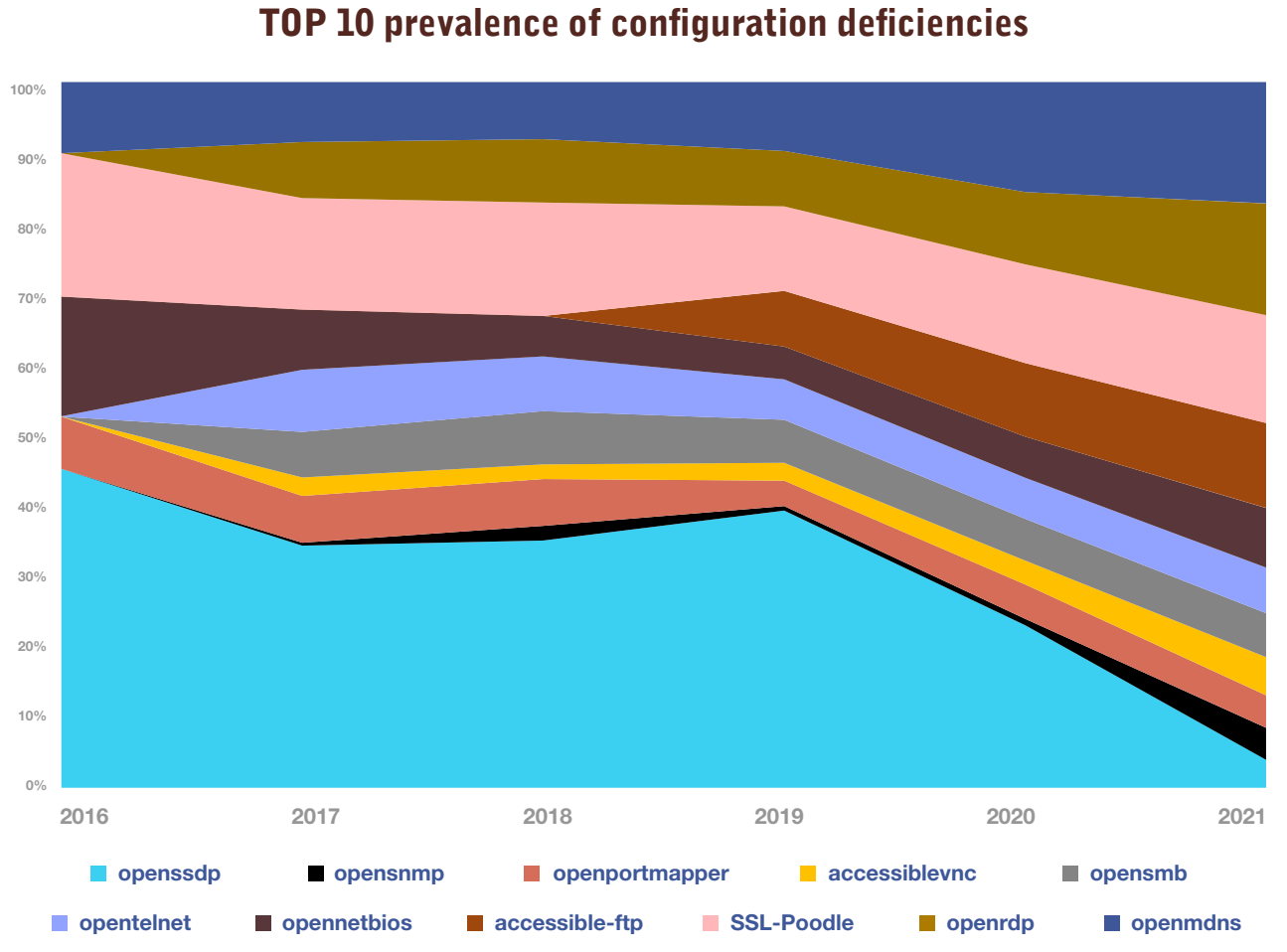


Image 6 – number of unique threatened IP addresses registered by CERT.LV in 2017–2021 with the most widespread vulnerabilities.

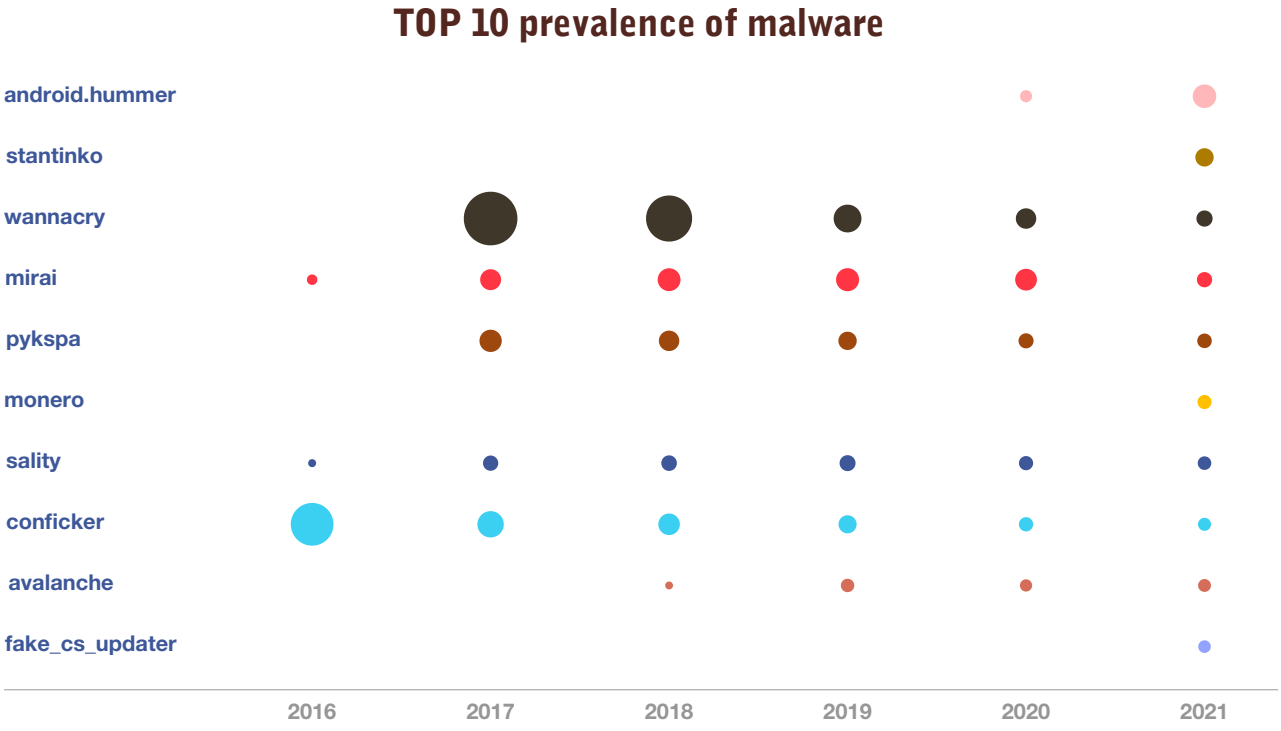


Image 7 – number of unique threatened IP addresses registered by CERT.LV in 2017–2021 with the most widespread malware.

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.

2.

The Most Notable Incidents of 2021

During the reporting period, CERT.LV cooperated with state and municipal institutions, banks, internet service providers and other organisations to solve incidents of varying 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.

The section below will outline the most notable incidents, which in turn shows the tendencies of the year.

2.1. Availability of Services

The ransom-based distributed denial-of-service *(DDoS)* attacks continued targeting financial institutions at the beginning of the year. The attackers carried out demonstration attacks exceeding 400 Gbps and demanded payment in cryptocurrency to prevent another, even larger attack. Initial attacks were successfully repelled by the institutions, and no further attacks followed. There was also an increase in the distributed denial-of-service attacks against Latvian public sector resources and some media outlets. At the end of the year, DDoS attacks were targeting mainly the telecommunications service providers.

There were several reports of disruptions to national resources. The analysis of the technical data showed that the resources were not exposed to external influences. Temporary resource malfunctions were caused by system failures or inadequate configuration of DDoS protection solutions.

At the beginning of the year, registration for the Covid-19 vaccine was launched on the www.manavakcina.lv website. Website visitors experienced a malfunction of the website, with virtual queuing times in some cases exceeding one hour. The malfunction was caused by both the high number of visitors and the inability of the *latvija.lv* authentication module to cope with the high traffic. Due to the overload, the *latvija.lv* authentication service was unavailable

for several hours for all applications – not only *manavakcina.lv*, but also *e-health*, tax return submission and other services.

Several educational institutions experienced malfunctions caused by the DDoS attacks against school infrastructure. Given that the attacks were only observed during active school hours, between 9:00 and 14:00, it is likely that the attacks were initiated by school pupils who used paid services to carry out the attacks. Similar challenges were faced by educational institutions in other European countries as well.

Both the international community and the Latvian population felt the importance of social networks in their daily lives. These networks not only serve as a platform for communication but are also widely used as a sign-up tool for other websites and online services, such as shopping sites or smart TVs. The unavailability of social networks for several hours also made it difficult for people in Latvia to access their usual services.

2.2. Fraud

As the pandemic continued, more and more people had to move various daily activities online, such as the purchasing of goods or services. Some looked online for an opportunity to improve their financial situation, driven by the availability of funds not spent on holiday trips and the growing availability of cryptocurrencies, which opened up access to various micro-investment platforms and new channels of financial speculation to the general public.

Unfortunately, in many cases, when starting a new digital journey, people lacked the experience and knowledge to protect their data and finances, and to were unable to recognise fraud. Fraudsters used a wide range of attacks to make sure they didn't miss out. Payments were scammed through fake trading sites and fraudulent investment platforms, and payment card credentials were obtained through fake delivery services or by calling from fake numbers and posing as representatives of a bank or law enforcement and threatening with financial losses or

fines for wrongdoing. Attackers often were in possession of information that allowed them to carry out a personalised attack, such as the victim's name, age and contact details. This data was most often obtained from publicly available profiles on social networks or from various data leaks, such as *Facebook* or *LinkedIn* user data leaks.

Fraudsters also improved their attack methods and started using caller ID spoofing in fraudulent phone calls. The attackers misused bank telephone numbers and impersonated bank employees, as well as misused customer numbers of various telephone operators and impersonated law enforcement agents to allegedly warn the recipient of the call about an offence committed on his or her behalf and threaten with a fine if the actions requested by the callers (fraudsters) were not carried out.

The new situation caused outrage and confusion when users of the misused telephone numbers received phone calls from strangers accusing them of calling and behaving inappropriately, and significantly burdened the work of law enforcement authorities. Although challenging, a successful resolution of this problem is essential and necessary, to avoid security risks and overloading call centres and rescue services.

Attempts to trick people to share photos of their identification documents were detected in Latvia. The images can be used to register for other services, such as cryptocurrency platforms, using the victim's identity and without their knowledge. As Latvian citizens become customers of international services, the range of threats to which they are exposed widens, for example by becoming targets of global phishing and identity theft campaigns. Campaigns no longer need to be adjusted and a different national language is no longer an obstacle.

Fraudsters were also attempting to steal social networking accounts of businesses, imitating the administration of social networks. Threatening breach notices were sent out to provoke account managers to act impulsively and make bad decisions, including entering account credentials on fictitious social networking sites set up by fraudsters.

A report of an unprecedented incident was received – a person joined a videoconference using someone else's identity. During the same period, similar cases where videoconferencing

was joined by people using fake IDs occurred in Lithuania, the Netherlands and the UK, and can be seen as part of a single campaign. The attackers are believed to have used *deepfake* technologies. Such attacks are expected to become more frequent in the future, especially given the high popularity of videoconferencing and the growing availability of video image processing solutions.

Information about fraudulent links sent by citizens and identified by CERT.LV is promptly placed in the DNS firewall https://dnsmuris.lv maintained by CERT.LV and NIC.LV. By using the DNS firewall, it is possible to successfully protect its users from attacks. The DNS firewall is available free of charge to every citizen, company, institution and organisation in Latvia.

2.3. Intrusion Attempts

Information about intrusion attempts was received throughout the year, although, in quite low amounts. In most cases, these attacks were *brute-force.* The attacks targeted various internet service providers, state and local authorities and also the private sector.

The attackers targeted mostly technologies used for remote working, such as *Remote Desktop Protocol* (*RDP*), *Virtual Private Network* (*VPN*) as well as video conferencing and chat platforms. Criminals, using various types of attacks, including newly discovered vulnerabilities, persistently sought to penetrate the internal networks of companies and organisations to gain unauthorised access to sensitive information or to encrypt devices and demand a ransom for data recovery.

Attackers also exploited long-known configuration deficiencies in widely used products, such as the unrestricted use of *Macros* in *MS Office* software. The primary solution to combat such attacks is to configure devices according to good practices, educate users and prevent system vulnerabilities by regularly updating.

2.4. Malicious Code

Like previously, in 2021 malware was mainly spread for two purposes – to obtain data or to make a profit. Emails with malicious attachments were distributed in a campaign to extract information on behalf of banks, companies, and governmental institutions. Upon opening the attachment, the device was infected with malware that collects usernames, passwords, cryptocurrency wallet and access information, etc., to send it to a server controlled by the attacker.

To make a profit, ransomware was distributed, the data on the devices were encrypted and a ransom was demanded for the recovery of the stolen data. The amount of 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. Ransomware attacks were experienced in both the private and public sectors.

It is important to note, however, that it is not the exploitation of newly discovered vulnerabilities that has most often led to encrypted systems, but the inadequate protection of resources – weak passwords and outdated software with vulnerabilities publicly known for several years that could have been fixed with a timely software update. In some cases, poor design of the IT infrastructure was an additional contributing factor to the spread of the virus.

A less traditional method was also used to spread malware. For example, attackers placed a paid *Google* ad. When searching for *AnyDesk* remote management software, this ad appeared as the first result and led to a website containing malware (Trojans). The attackers had also cryptographically signed the malware, which made it less likely that the system would warn the user of a potential threat.

2.5. Compromised Devices and Data Leaks

Cases of compromised devices affected individuals, businesses, and state and local authorities, though most of the compromised devices were routers in small businesses or individual households.

The attacks were carried out using emails with malicious attachments sent from already compromised accounts of colleagues or business partners, as well as weaknesses in the protection of various ICT resources, such as weak passwords and outdated software with vulnerabilities that have been publicly known for years.

The attacks aimed to extract data, manipulate payment information, direct payments to the attackers' bank accounts, or encrypt equipment to demand a ransom for data recovery and possibly non-leakage.

At the beginning of the year, information was received about a ransomware attack on *Civinity* with potentially 30 000 affected customers. The company acted responsibly and informed customers of a possible data leak. CERT.LV provided the company with the necessary support to help it to recover from the incident.

Several Latvian companies were victims of business email compromise (BEC). Attackers accessed a company's or business partner's email account to send out fake invoices with altered bank accounts. The total amount of losses in the reports received by CERT.LV amounted to almost €500 000. CERT.LV encouraged companies to contact their business partner whenever a request to change financial data had been received, and get a confirmation that the information received is correct by using other methods of communication e.g., a phone call.

A relatively new target of attacks was cryptocurrency wallets on compromised devices and specialised cryptocurrency storage solutions. One incident caused financial losses of 2 bitcoins or almost €100 000 (at the time).

Supply chain attacks were observed around the world, which also raised security concerns in Latvia. Latvian companies, especially those that provided products to the global market, were required to increase their attention to cybersecurity matters. These companies can become potentially interesting to attackers, to gain access to their customers' devices and infrastructure. Similar precautions should be taken by Latvian companies and organisations that use services and products of foreign ICT suppliers to reduce the possibility of supply chain attacks.

At the end of the year, a popular *JavaScript* library was compromised in a high-impact *supply chain attack.* The library is widely used in various IT solutions, e.g. to find out the type of device and software used by the user. The attack infected millions of *Linux* and *Windows* devices with malware designed to intercept passwords and make unauthorised use of device resources to mine cryptocurrencies. This *JavaScript* library is also used in products from *Facebook*, *Microsoft*, *Amazon, Instagram, Google, Slack, Mozilla, Discord, Elastic,* and many others. CERT.LV encouraged people to check whether the system has been compromised if this library is used in the project and to follow the guidelines for implementing security measures.

CERT.LV called for multi-factor authentication (2FA, MFA) to be used wherever possible as an important mechanism to protect devices and accounts. As an additional tool for threat prevention, CERT.LV and NIC.LV offer the DNS firewall https://dnsmuris.lv/, which holds up-to-date information about current threats and can be used free of charge by every citizen, company and organisation in Latvia.

2.6. Vulnerabilities

2021 was a year full of newly discovered critical zero-day vulnerabilities *(MS Exchange: CVE-2021-26855, MSHTML: CVE-2021-40444, Log4j: CVE-2021-44228, GlobalProtect: CVE-2021-3064 etc.).* Critical vulnerabilities gave attackers the ability to perform a remote code execution, gaining access to the vulnerable system. When identifying compromised devices in Latvian cyberspace, it was found that the number of compromised devices in the public sector and of local authorities was noticeably lower, probably due to relatively quick and active communication with CERT.LV about potential threats. In some incidents, it was observed that the servers of state and local authorities were updated within a week, in contrast to the private sector, where the vulnerabilities discovered remained for several weeks, even after communication with CERT.LV. It should be noted, however, that the situation is not unique to Latvia; it is also known that the private sector abroad is more reluctant than state and local authorities.

CERT.LV notified the holders of vulnerable systems in the public sector, as well as provided support in incident analysis and prevention, in some cases, also involving the National Armed Forces Cyber Defence Unit.

The security of smart devices (IoT) was brought to attention, with alerts sent out for several thousand vulnerable heating systems and video surveillance devices. The vulnerabilities gave attackers the ability to remotely take control of the devices, posing a direct (disconnected heating) or indirect (information about whether someone was present at the object) threat to the owner. As a result of the warnings, Latvian electricity supply groups and telecommunication operators started inspections of similar heating devices and the elimination of deficiencies.

CERT.LV regularly informed internet users about all significant vulnerabilities and recommendations for preventing them via internet service providers. Threat information available at: https://www.esidross.lv/informacija-par-apdraudejumiem/


3.
Responsible
Vulnerability
Disclosure

CERT.LV supports the good practice of responsible IT security vulnerability disclosure and encourages security researchers to report vulnerabilities to CERT.LV. This allows CERT.LV to actively coordinate vulnerability response, thus better protecting the internet space of Latvia.

During the reporting period, CERT.LV received several reports of vulnerabilities detected in various resources of state and local authorities. Thanks to the reports, several websites of state authorities were protected, mainly from cross-site scripting (XSS) attacks. If successful, they would allow an attacker to perform actions in the user's browser, such as manipulating website content and cookies or using browser-specific exploits.

On 29 July, a study was published on the security problems in electronically signed documents with dynamic content. The threat was not critical, but the topic received attention because the general public is very sensitive to electronic signature issues.

The problem was caused by the design of the electronic signature system, which is identical practically in all countries of the world. From the user's point of view, the electronic signature confirms the information displayed on the screen, but technically the file is signed without considering its content. The most popular file formats .docx (*Microsoft Office*), .odt (*Libre Office*) and .pdf may contain dynamic parts that may vary from one time the document is opened to another, including dynamic downloads from the internet, such as changing amounts, volumes, disclaimers, etc. Latvia State Radio and Television Centre, as the e-signature maintainer, in cooperation with CERT.LV published information about the discovered vulnerability and reached out to the international CERT community to explore options for a centralised solution.

CERT.LV invites people to report discovered vulnerabilities in 2022 by writing to cert@cert.lv. More about the responsible vulnerability disclosure read on the CERT.LV website: https://www.cert.lv/lv/par-mums/atbildiga-ievainojamibu-atklasana.

4.

Penetration Testing

Security or penetration tests are an important step in making sure that the online resource developed – 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, repeatedly.

In some of the tests, significant deficiencies were identified. For information system maintainers, CERT.LV prepared a report on the performed tests and their results, as well as provided recommendations for the mitigation of deficiencies.

5.

Informative Communication Events


digiTuvi
KIBERDROŠĪBAS AKTUALITĀTES
#digiTuvi


esi drošs
IT drošība darba vietā - 2021
CERT.LV
CERT.LV 2021.gads


Latvijas
Digitālās inovā
centrs
ARMĪNS PALMS
KIBERDROŠĪBAS EKSPERTS CERT.LV
DIGITĀLAIS CILVĒKS


IKT RESURSU CENTRALIZĀCIJA| IZDEVĪGI, DROŠI, ĒRTI
#digiTuvi


RE!

The opinion of CERT.LV experts have been widely requested in 2021 as well. With the Covid-19 pandemic losing its relevance, publicity has fallen slightly compared to the previous year, down 3.5%, but is still high compared to previous years – for example, up by 67.2% in 2021 compared to 2019.

CERT.LV experts have expressed their opinions through interviews, comments and answers to media questions on TV, radio, print and online media on various cybersecurity-related issues. In total, CERT.LV has been featured in more than 725 TV, radio, online and print media publications – in Latvian (75.1%), Russian (24.0%) and English (1.0%).

During the reporting period, the attention of the media was turned to cyber-attacks involving phishing campaigns, fraudulent lotteries and phone calls from fraudsters on behalf of banks. The opinion of CERT.LV experts are expressed most actively – 59.3% of all publications – as usual, on internet portals, 22.8% on radio, 7.8% on TV and 10.2% in printed publications.

CERT.LV moderates the website www.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 2021, 90 posts were published on the website, of which monthly, quarterly and annual reports and news accounted for 37.8%, while fraud and malware alerts accounted for 21.1%, informative notices for 22.2%, recommendations for action for 8.9% and 10% on events organised. During the year, the CERT.LV website had a total of 82,073 visits or sessions from 55,354 users.

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. The portal had 44,699 visits or sessions by 33,139 unique users.

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 devices, 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 https://cert.lv/en/about-us/responsible-disclosure-policy.

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 2022 as well.

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

- ***Twitter*** account *twitter.com/certlv* is followed by 3 264 users
- ***Facebook*** profile *facebook.com/certlv* – 4 534 users
- ***YouTube*** channel is followed by 267 users

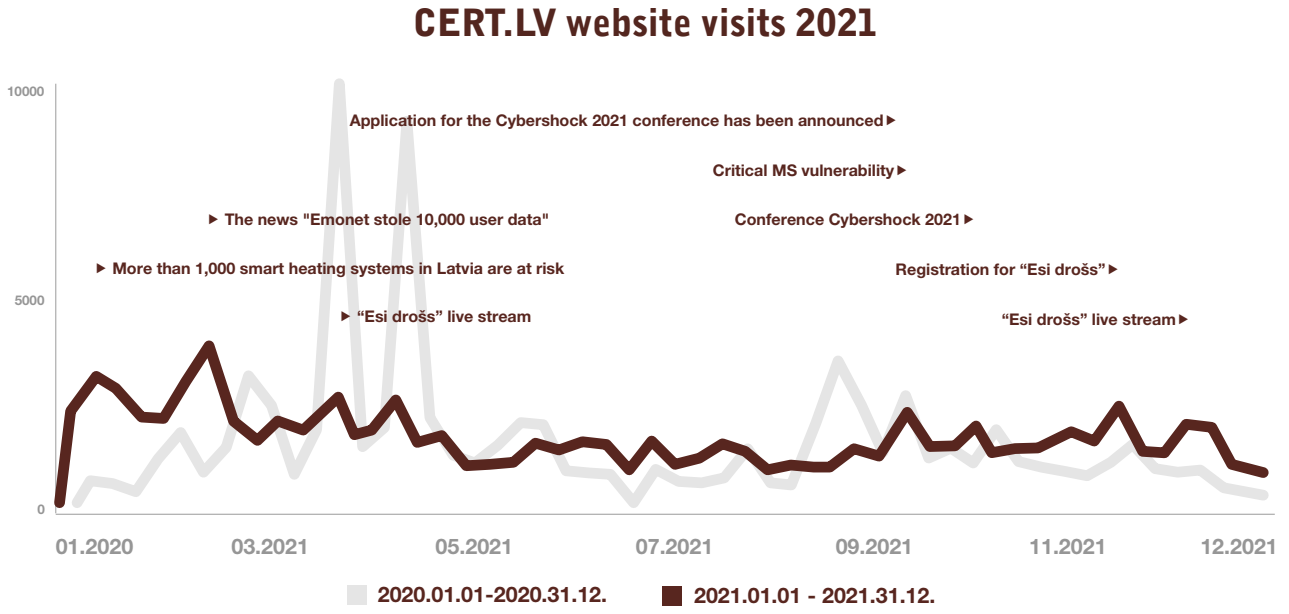


Image 8 – CERT.LV website visits in 2021

6.

Educational Events

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 123 events and educated 13 619 participants.

Educational Events in 2021

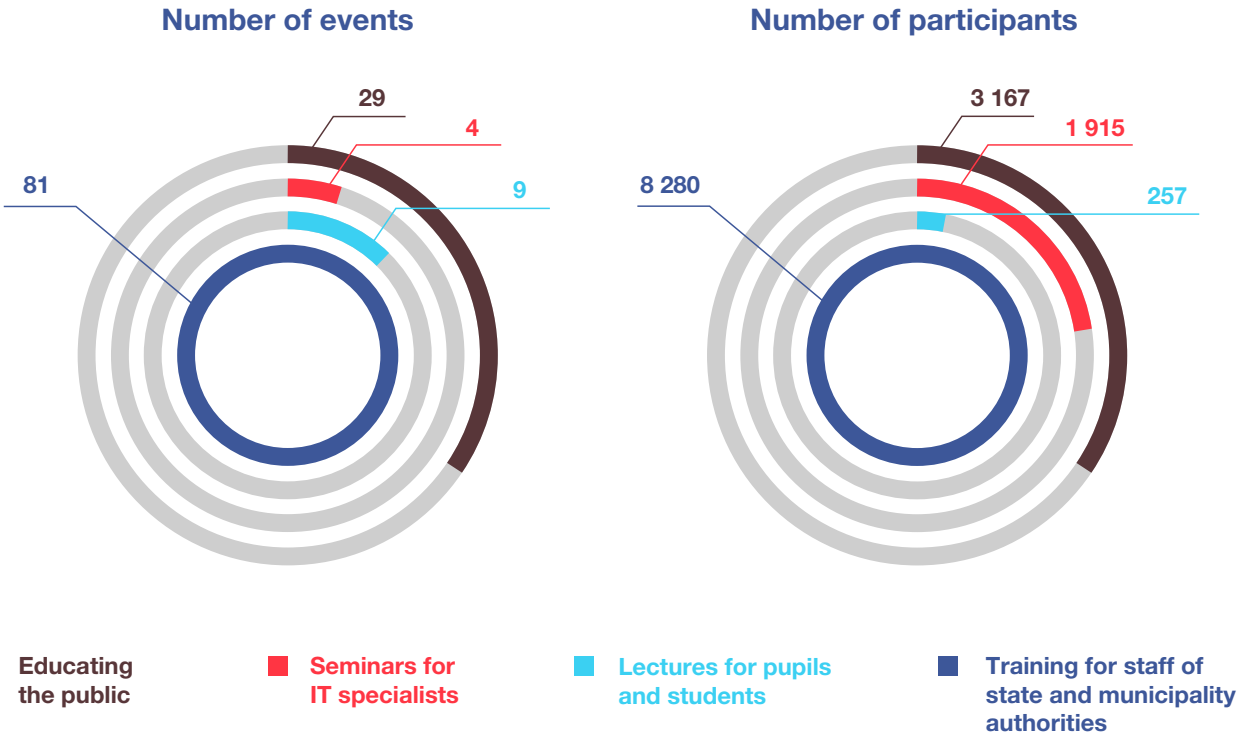


Image 9 – number of events and trained people in 2021

6.1. International Cyber Security Conference CyberShock 2021

On 6–7 October, as part of European Cyber Security Month, CERT.LV organised *CyberShock 2021*, a strictly technical online conference for cybersecurity professionals, where internationally renowned experts provided participants with an in-depth insight into a wide range of issues related to cybersecurity, while presentations also included real-time demonstrations. *CyberShock 2021* attracted 923 participants from 53 countries. In parallel with the conference, the CTF (*Capture the Flag*) competition took place, in which 31 teams took on various cybersecurity challenges. (https://cybershock.lv/)


2021
CS21


KT SERVISS


Cyber SHOCK
2021
47:18
Gil Biton
Offensive security engineer, Sygnia [IL]
Scaling up offensive pipelines
47:17
ON AIR
STOP
7.29
OK
SAMSUNG

From: Koichiro Komiyama (JPCERT/CC)
To: Baiba Kaskina
Date: Wednesday, September 15, 2021, 6:16:31 AM
Subject: [1st-news] Cybershock conference
6-7 October 2021 - invitation

===Original message text=========================
Baiba, The event page looks pretty cool! Is this
by a professional designer? Sparky

--
Koichiro Komiyama, Ph.D, CISSP / 小宮山 功一朗
Director, Global Coordination Division
Our latest activities on http://blogs.jpcert.or.jp

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

In addition to the international Cyber Security Conference *CyberShock 2021*, which was targeted toward IT security professionals, two more thematic *Esi drošs* (Be safe) seminars were organised. Every year in spring and autumn, they bring together mainly employees of 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 www.cert.lv website and video recordings are published on the CERT.LV *YouTube* channel.

In March: The *Esi drošs* (Be safe) seminar introduced participants to the implementation of secure email technologies, the EU Cybersecurity Strategy and NIS2 Directive, an overview of the *Solarwinds* incident, effective authentication mechanisms, the defeat of the second wave of *Emotet*, and a look back at current events in cyberspace in Q1 2021.

In August, CERT.LV organised a practical online seminar on evidence gathering after a cyber incident, which covered cyber incident triage, evidence and its gathering procedure, as well as practical tips and demonstrations. The event was watched online by 280 participants.

In December: The seminar covered business continuity planning for critical infrastructure, cybersecurity crisis planning and crisis simulations, proper backup creation and storage, domain names in the context of the administrative-territorial reform, the use of games in cybersecurity training and a look back at the cybersecurity events in 2021.

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 the most current events in the field of cybersecurity, as well as reminding them about good practices for protecting themselves and their devices.

Key events in 2021:

On 22–26 March, the activities of European Digital Week took place, in which CERT.LV also actively participated. On 22 March, CERT.LV in cooperation with NIC.LV, in a presentation Kā viegli nePAZAUDĒT naudu internetā (How to easily not to LOSE money on the Internet), told entrepreneurs about financial security in the digital environment, types of cyber attacks, email forgery, use of domain names in cyber-attacks and the most widespread mistakes made by users (https://www.digitalaiscentrs.lv/skaties/2021/certlv-ka-viegli-nepazaudet-naudu-interneta).

On 25 March, Digital Identity and Security Day was celebrated, during which CERT.LV participated:

- in RigaTV24's Digital Week #digiClose (Digitālā nedēļa #digiTuvi), giving an insight into cybersecurity issues (https://fb.watch/4KztHjUhgb),
- at the cybersecurity seminar organised by *LVRTC*, *KIBERNAKTS dienas vidū* (CYBERNIGHT in the middle of the day*)*, giving presentations *Kiberdrošības dzeņa vēders. Cik atšķirīga ir izpratne par drošību uzņēmumos* (Cybersecurity Woodpecker Belly. How security is perceived differently in companies*)* and *Paroļu ēras beigas, jeb kāpēc identitātei ir jābūt drošai* (The end of the password era, or why identities need to be secure) (https://fb.watch/4KzHj6xUp-) and
- in a high-level expert discussion on *CYBERNIGHT 2021 | Cyberdependence*, discussing digital skills in the new reality, threats in the digital space, the national

cyber defence strategy and its implementation, and preventive measures to improve cybersecurity (https://fb.watch/4KAdNLyYW7/).

At the end of September, CERT.LV experts took part in the CYBER.EU.VET project. It is led by the Latvian European Community Studies Association (LECSA) and aims to raise awareness and improve the knowledge of young people and educators on cybersecurity issues. As part of the project, young people had to create a game designed to help them achieve the project's objectives. CERT.LV experts presented information on current cyber threats to young people and took part in the evaluation board.

On October 21, as part of the European Cyber Security Month, SIA Tet held a cybersecurity forum CyberShield, the purpose of which was to draw public and business attention to virtual security, bringing good cyber hygiene practices to life, analysing the latest trends in cyberspace and encouraging everyone to be vigilant and invest energy in improving their digital skills. At the forum, CERT.LV representatives gave an overview of the current developments in Latvian and global cyberspace. (https://www.tet.lv/uznemumium/vairak/ forums-cybershield).

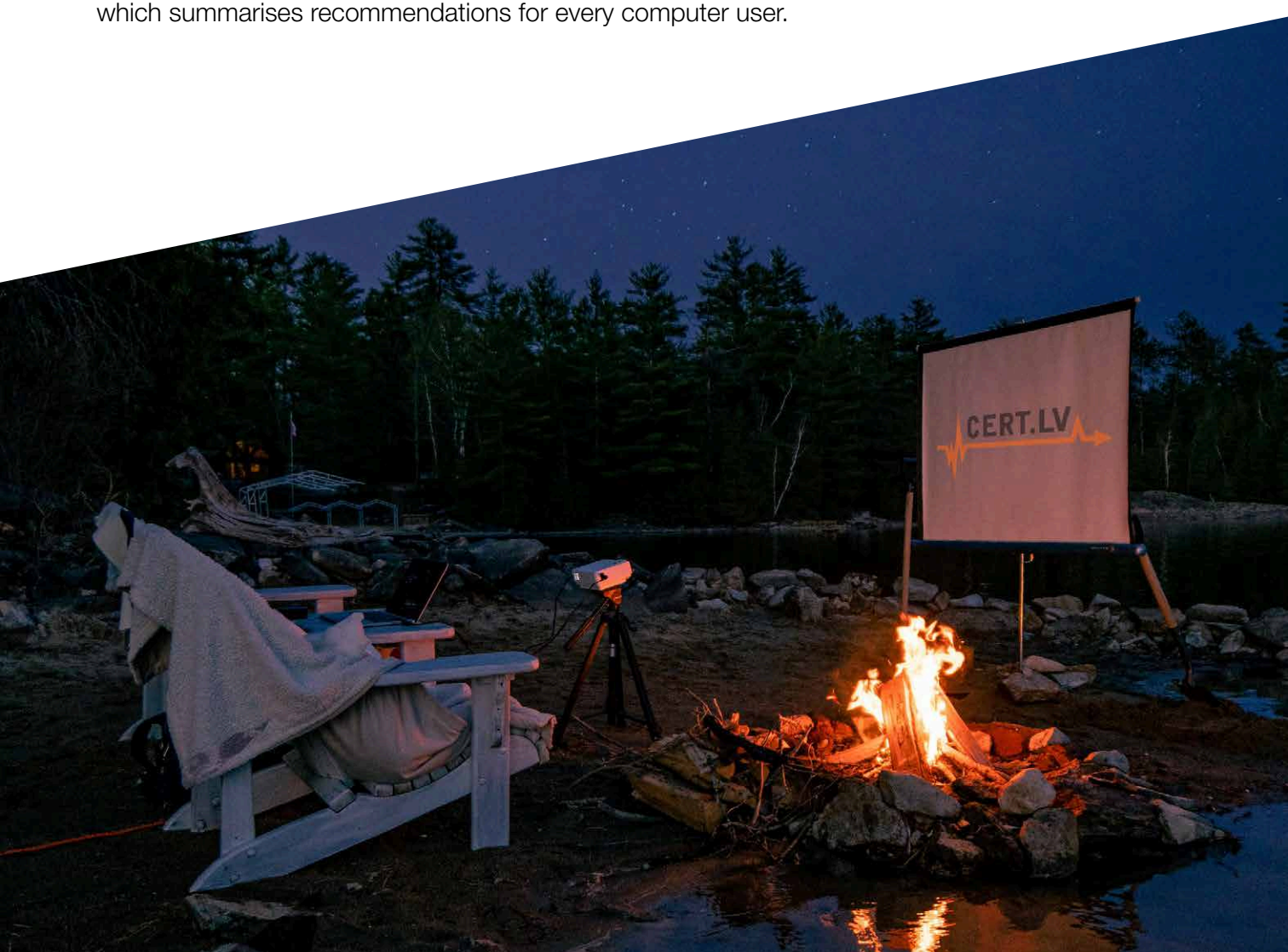
On November 5, CERT.LV in cooperation with NIC.LV participated in the seminar for entrepreneurs *IT risinājumi biznesa attīstībai* (IT solutions for business development) organised by the *Zemgales uzņēmējdarbības centrs* (Zemgale Entrepreneurship Centre), where they presented recommendations on how to recognise cyber-attacks and how to protect both your company and your domain name in the digital environment.

From November 26, on the initiative of the Ministry of Defence, CERT.LV organised five cybersecurity seminars for members of the Parliament of the Republic of Latvia and their assistants on the basic principles of information security and good practices.

CERT.LV representatives also took part in several career and professional growth related events, talking to young people about the knowledge and skills needed to work in cybersecurity and the potential challenges in the cyber environment.

To raise awareness about the types of financial fraud and what to do in such situations, CERT.LV took part in the information campaign Neuzķeries! Esi gudrāks par krāpniekiem (Don't fall for it! Be smarter than the fraudsters) organised by the Finanšu nozares asociācija (Financial Latvia Association).

CERT.LV continued to translate and publish informative and educational material on https://www.esidross.lv – the monthly security bulletin *OUCH!*, prepared by the SANS Institute, which summarises recommendations for every computer user.



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 were 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 2021, in which CERT.LV took part:

- Consulting on IT security requirements and their implementation in the development of an IT solution for the *Vaccination Project* led by the Ministry of Health and the Latvian National Health Service (NVD).
- Participation in the Critical Infrastructure Working Group organised by the Ministry of the Interior, where the new *Directive on the resilience of critical entities* (CER), which provides for the protection of critical infrastructure at the European level, and other issues was discussed.
- A new version of the Electronic Communications Law was being drafted, incorporating the requirements of the Electronic Communications Code. CERT.LV underlined the need to be able to continue to inform end-users about all threats detected in their devices, not just the critical ones. As well as the need to receive reports not only about service availability issues but also about critical incidents in a broader sense. CERT.LV also participated in the drafting of the Regulation of the Cabinet of Ministers related to the Electronic Communications Law, providing comments on the desired outcome within the scope of its competence.
- Participation in meetings and drafting of comments in the working group of the professional standard of *Information Security Manager* organised by the Ministry

of Education and Science. On 11 August, the relevant occupational standard was adopted at a meeting of the Vocational Education and Employment Tripartite Co-operation Sub-council (PINSTA).

- CERT.LV participated in the preparation of the informative report of the Ministry of Defence on Improving National Cybersecurity Management *(Par valsts kiberdrošības pārvaldības uzlabošanu).* To strengthen the national cyberspace and ensure coordination on cybersecurity issues, especially in the context of the new European Union Regulation (NIS2 Directive), the report foresees the establishment of a National Cybersecurity Centre.
- The management of a project has been launched, which will carry out research on the safety of wearable devices over three years in cooperation with the Latvian Council of Science (LZP). During the reporting period, testing of automated remote systems started and a prototype model was under development.

Provided comments, suggestions and recommendations:

- for the NIS2 Directive proposal document;
- about the Digital Services Act and the Digital Markets Act;
- on the necessary changes to the Regulation of the Cabinet of Ministers No. 442 *Procedures for Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements;*
- on Digital Transformation Guidelines for 2021–2027;
- on amendments to the Regulation of the Cabinet of Ministers No. 764 *General Technical Requirements of State Information Systems* and the Regulation of the Cabinet of Ministers No. 71 *Procedure for Supervision of State Information System Development Projects;*
- for the National Cyber Security Strategy of Latvia for 2023–2026.

CERT.LV actively participates in the **Digital Security Monitoring Committee** (DDUK), the operation of which is determined by the Regulations of Cabinet of Ministers No. 695 of 1 November 2016. CERT.LV continued its work on monitoring trust service providers and providers of qualified electronic identification services and continued to maintain the list of trusted Latvian service providers and trusted services *(trust list).*

CERT.LV closely cooperated with the National Armed Forces **Cyber Defence Unit**, 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 under 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 2021, the most important cooperation took place through participation in the *Locked Shields* cybersecurity exercise, as well as through the unit's involvement in various incidents.

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 organise the **Information Technology and Information Systems Security Expert Group** meetings, 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, and 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 devices 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, the 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.

Cooperation with the CERT network

The NIS Computer Security Incident Response Team's Network of the NIS Directive is made up of Computer Emergency Response Teams (CERT) and CERT-EU representatives of the European Union member states, while the European Commission acts as an observer in the network. The establishment of the cooperation network was determined by the NIS Directive. The Directive aims to achieve a uniformly high level of cybersecurity in the networks and information systems of EU member states, enhancing each country's cybersecurity, as well as promoting EU-level cooperation and risk management.

CERT.LV regularly participated in the meetings of the 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 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.

At the NIS Directive CERTs Network meeting on **2–3 June**, CERT.LV gave a presentation on Trust Issues in Digital Signing, looking at the aspect of dynamic content in signed documents.

On 1 October, CERT.LV participated in the *CyberSOPex 2021* European CERT Network Exercise organised by ENISA to enhance the readiness of participants to respond to a large-scale cross-border incident.

There are several topical working groups within the NIS CSIRT Network. Representatives of CERT.LV are also active in three of them:

- the *Cyber Weather* working group regularly collects information on the most relevant cyber incidents and produces a quarterly Cyber Weather Report for Europe;
- the *Maturity* working group is working to increase the maturity of Computer Emergency Response Teams in EU member states;
- the Terms of Reference Review working group is reviewing the Network's constitution and bylaws, updating them accordingly.

Cooperation within FIRST

FIRST is the global Forum of Incident Response and Security Teams. Membership in FIRST enables incident response teams more effectively respond to security incidents, as well as to take preventive measures. It is a trusted network of partners, forming a global community of incident response experts.

CERT.LV is an active member of FIRST and participated in the FIRST Framework working group to develop a common framework for the roles, competencies and skills of CERT team members. Head of CERT.LV Baiba Kaškina continued her work as co-chair of the FIRST Membership Committee, participating in the review of new member applications and contributing to the improvement of the membership process. CERT.LV also participated in the FIRST Conference Programme Committee, supporting the development of the conference programme.

Cooperation within TF-CSIRT

The *Task Force on Computer Security Incident Response Teams* (TF-CSIRT) is a Europe-wide cooperation forum of CERTs, which promotes the exchange of experience and the use of common standards and procedures in solving incidents, and coordinates various community activities, such as training or the creation of new CERT units. TF-CSIRT also maintains a register of trusted CERTs and accredits and certifies them according to the level of maturity demonstrated by the team *(Trusted Introducer Service or TI).* CERT.LV has maintained the

status of a certified team since 2016 (at the end of the reporting period, 437 teams were included in the register, of which 40 were certified), which confirms the high level of maturity and preparedness of the CERT.LV team.

CERT.LV continued its work in the *TF-CSIRT Futures* working group to develop a new management model for *TF-CSIRT and Trusted Introducer* for European CERT cooperation. The working group was closed in September 2021, having achieved its objectives: a non-profit organisation in the Netherlands was recommended as a future model for TF-CSIRT. The TF-CSIRT *Steering Committee* will continue its work to implement this recommendation.

CERT.LV led the meetings of the TF-CSIRT International *CERT PR Working Group*, during which CERT representatives talked about current challenges in the field of cybersecurity awareness, shared their experience in organising educational campaigns and provided recommendations for the organisation of more successful communication.

European Union and ENISA initiatives

CERT.LV participated in the *EU Cybersecurity Index Working Group* meetings, in which the methodology for calculating the cybersecurity index value is being developed. The working group aims to assess the level of cybersecurity in EU member states to determine the overall level of cybersecurity in the EU and the impact of existing rules and guidelines on cybersecurity and business operations.

CERT.LV joined the *EU CyberNet* project as one of the partners. The project aims to strengthen and develop cybersecurity expertise not only within the EU but also beyond its borders (www.eucybernet.eu). Participation in the project provides an opportunity for CERT.LV experts to strengthen their knowledge and capacity.

CERT.LV participated in a study conducted by ENISA (European Union Agency for Cybersecurity) on the experience of EU member states with reporting cybersecurity incidents in the medical sector, providing information on national practices, regulatory framework, measures taken to

improve cybersecurity and strengthen cooperation, as well as information exchange between sector representatives, CERT.LV and the Ministry of Defence.

CERT.LV also participated in an ENISA study on raising and strengthening awareness of cybersecurity issues among EU citizens. The study aims to gather information on the experiences of different countries in raising awareness, identify challenges and make recommendations on the most effective methods. The results of the study will be compiled in a document and distributed to representatives of all member states.

On 3 December, CERT.LV participated in the *European Cybersecurity Competence Centre* (ECCC) meeting on the further development of the *Security Operation Centres'* (SOC) idea to facilitate European-level information exchange on current threats in cyberspace under the EU Cybersecurity Strategy.

On 7 December, CERT.LV participated in a meeting organised by ENISA on the establishment of a *Joint Cyber Unit* (JCU). The national representatives took part in the discussion, sharing their experiences, tools used so far and projects launched to facilitate the creation of a unit with clearly defined tasks and operational principles. The unit aims to facilitate a coordinated European response to a large-scale cybersecurity threat.

Cooperation with NATO member states

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 workshops for NATO CCDCoE and provides support in organising the NATO CCDCoE technical cybersecurity exercises, such as *Crossed Swords.*

On 13–16 April, Locked Shields, the world's largest and most complex international real-time cyber defence exercise, was organised by NATO CCDCoE. The Latvian team implemented unprecedented inter-regional cooperation by participating in a training exercise as part of the joint team of Latvia and the Republic of Korea. In the context of the Covid-19 pandemic, the work of

the joint team was coordinated remotely, successfully overcoming the challenges presented by the significant time zone and language differences. This experience of a cross-regional joint team provided an opportunity to develop the cyber capabilities of both nations and to improve both internal and external cooperation.

CERT.LV participated in the planning of *Crossed Swords 2021*, the NATO CCDCoE annual technical red teaming cyber exercise. Work was carried out on the development of the technical elements of the training environment, the coordination of the exercise execution and the management of the industrial control systems attack scenario. The training is designed not only to improve the technical skills of penetration testers, digital forensics and situational awareness experts but also to enhance leadership skills. A CERT.LV representative also took part in the training exercises, which were held on **7–9 December,** leading one of the training teams. Almost 100 participants from 21 countries took part.

From 31 May to 4 June, CERT.LV participated in ***The Coherent Resilience 2021 Baltic*** *(CORE 2021-B)*, a tabletop cybersecurity exercise organised by the NATO Energy Security Centre of Excellence (NATO ENSEC CoE) and the Joint Research Centre of the European Commission, aimed at promoting and improving the cybersecurity of critical energy sector infrastructure in the Baltic states.

From 29 November to 3 December, CERT.LV participated in the NATO cyber defence exercise ***Cyber Coalition 2021***. The exercise aims to facilitate cooperation – activities carried out by NATO members and partners were aimed at achieving common goals to improve their ability to prevent and repel threats in the cyberspace and to contribute to the growth of NATO. 1000 participants representing 30 NATO member states, several partners and the European Union, took part in the exercise.

Other international activities

CERT.LV participated in the Energy Information Exchange and Cooperation Group *Energy ISAC Camelot* meetings to facilitate information exchange and promote cybersecurity in the energy sector. The industrial research laboratory, developed by CERT.LV was presented to the group and was highly appreciated.

CERT.LV supported Canada in selecting the most appropriate Coordinated Vulnerability Disclosure model by participating in the *Coordinated Vulnerability Disclosure* working group organised by the Government of Canada to gather information on responsible vulnerability disclosure processes and experiences from other countries. The discussions resulted in the document *See Something, Say Something. Coordinating the Disclosure of Security Vulnerabilities in Canada* to promote public sector information technology security by providing a framework for cooperation between external security researchers and the public sector.

On 8 September, CERT.LV hosted a delegation of Estonian colleagues from RIA and CERT-EE to facilitate the exchange of experience in dealing with complex incidents, more effective use of tools and solutions, preventive measures and raising public awareness.

9.

Implementation of Projects Co-financed by the EU

On 1 November 2018, CERT.LV continued the implementation of the **Cyber Exchange** project approved under the 2017 CEF Telecom-Cyber Security call (contract No. INEA/CEF/ICT/A2017/1528866 with the European Commission) (hereinafter – the Cyber Exchange project).

The project aims to strengthen international cooperation between national and government CERT organisations. The Cyber Exchange project is a response to growing cybersecurity 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. The main activity of the project is the organisation of exchange visits. Latvian CERT.LV representatives were visiting CERT teams from other project member states or welcoming colleagues from other CERT units.

Within the project, CERT.LV representatives went on an experience exchange visit to Poland, where the automation of phishing incidents was reviewed and analysed, and other incident automation tools and CERT.PL experience in handling cybersecurity incidents was presented. As a result of the visit, the relationship between the CERT.LV and CERT.PL teams were improved. It is very useful both for day-to-day cooperation and for the implementation of joint projects and activities.

Due to the Covid-19 restrictions, the project was extended until 30 June 2022.

On 1 July 2021, CERT.LV started the implementation of the project **Joint Threat Analysis Network (JTAN)** approved in the 2020 CEF Telecom Call – Cybersecurity call, contract No. INEA/CEF/ICT/A2020/2373165 with the European Commission.

The leading partner of the project is CERT.PL, the Polish Information Technology Security Incident Response Team, which operates within the *Naukowa i Akademicka Sieć Komputerowa* (NASK) institute. Partners from Austria, France, Estonia, Luxembourg, Romania and Slovakia are also participating in the JTAN project. The overall objective of the JTAN project is to create a *Joint Threat Analysis Network* (JTAN). CERT.LV's main involvement in this project is to develop the *Graphoscope* tool.

In 2021, CERT.LV worked on the design, development and improvement of *Graphoscope*. On 9 December 2021, the *Graphoscope* open source licence was published to allow other project partners to test, evaluate and suggest improvements to the tool. The tool is publicly available at https://github.com/cert-lv/graphoscope. During the reporting period, CERT.LV participated in remote JTAN project meetings.

Graphoscope is a tool designed to correlate data from different data sources and display them in a visual form. The *Pastelyzer* tool, which was developed in a previous European-funded project (Improving Cyber Security Capacities in Latvia, 2017-LV-IA-0058), can also be used as a data source. Key features of *Graphoscope*: 1) support for multiple data sources; 2) a web-based interface that does not depend on pre-installed databases; 3) easy system setup; 4) the interface provides flexible filters that facilitate the analysis of large amounts of data.

The implementation of the JTAN project is planned until 30 June 2024.

10.

Services for Strengthening Latvian Cyberspace

DNS Firewall: Work continued on the development of the DNS RPZ (*Domain Name Service Response Policy Zone*), also known as the DNS firewall project developed by CERT.LV and NIC.LV. As mentioned before, the solution provides an opportunity to protect users from malicious content on the internet related to incident identifiers already known to cybersecurity authorities (domain names, IP addresses, etc.). Any internet user in Latvia (both individuals and organisations) can use the DNS PRZ service without signing a contract or signing up. To use it, NIC.LV recursive DNS servers must be used. More information and detailed instructions are available at https://dnsmuris.lv.

More than 50 000 potential cyber incidents intercepted in 2021!

DNS ugunsmūris

CERT.LV started negotiations with several internet service providers (ISP), with whom the "Responsible ISP" memorandum of understanding has been signed, to offer DNS RPZs to their customers. A joint meeting was also held with the Public Utilities Commission to agree on the feasibility of such cooperation from a regulatory perspective.

Early Warning System (ABS): an early warning sensor is a passive safety device that allows threat identification and helps in incident investigation. The Early Warning System provides data network traffic anomaly analysis, malware detection and alerts for detected threats.

The Early Warning System installation and configuration are provided by CERT.LV, the organisation must provide two electrical connections and two network connections. An agreement must be signed for the installation of the Early Warning System. The service is primarily available to critical infrastructure organisations, state and local institutions, as well as providers of essential services and digital services. To learn more about the Early Warning System and decide on its installation at your organisation, please write to: cert@cert.lv.

A new **public Stratum 1 NTP time server** has been installed. The server receives accurate time from GPS and has a built-in oscillator with an error of no more than 1.6 s per year. With the new server, CERT.LV provides a total of three public NTP servers, two of which are Stratum 1 and one Stratum 2. All servers are connected to the Latvian NTP server pool "lv.pool.ntp.org". CERT.LV recommends using this pool as a source of the exact time.

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

CERT.LV
Information Technologies
Security Incident
Response Institution