THE COMMUNICATIONS REGULATORY AUTHORITY OF THE REPUBLIC OF LITHUANIA

NETWORK AND INFORMATION SECURITY DEPARTMENT

SECURITY INCIDENT HANDLING DIVISION (CERT-LT)

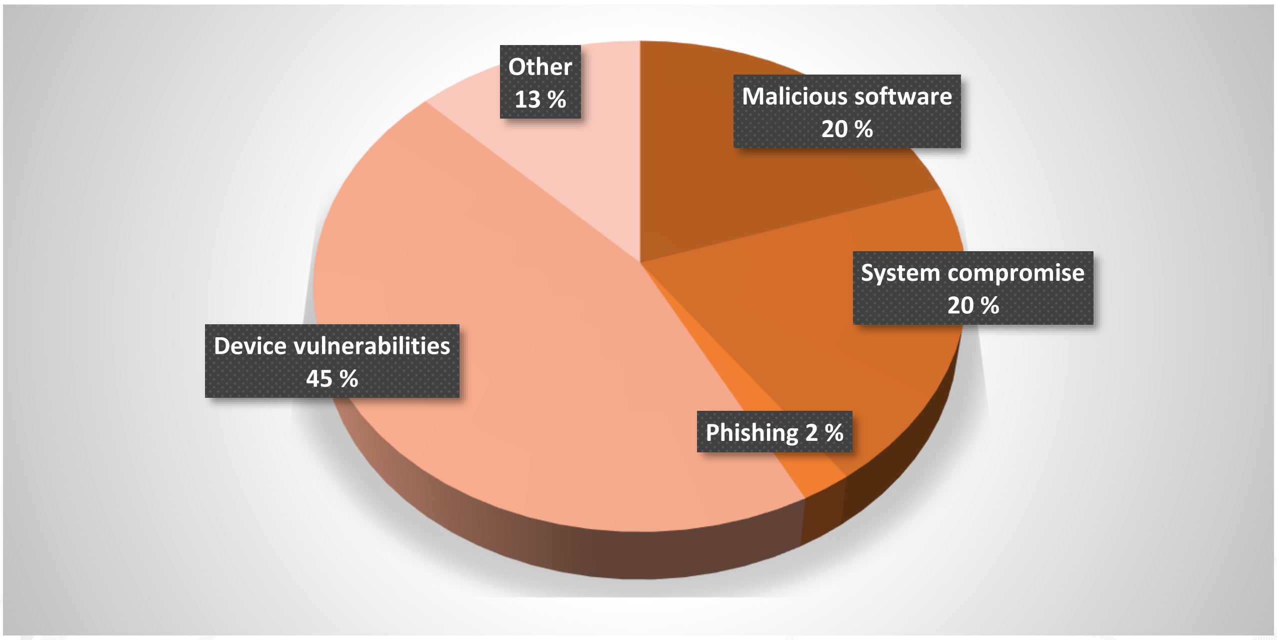
ANNUAL REPORT 2017

The National Electronic Communication Networks and Information Security Computer Emergency Response Team (CERT-LT) of the Republic of Lithuania has summarized its activity results for 2017. In 2017, CERT-LT processed 54,414 incidents on reports received from Lithuanian electronic communications service providers, hosting service providers, foreign CERT services engaged in the investigation of international incidents, and Lithuanian internet users. Compared to 2016 (49,463 reports), the number of cyber incidents increased by 10%. Summaries of the processed reports by type are presented in Table 1 and Figure 1. The following sections describe every type of incidents and special trends in 2017.

Table 1. Reports on incidents by type processed by CERT-LT in 2017

Types of processed reports	2017 period				
	Q1	Q2	Q3	Q4	Total
Malicious software	2,580	2,755	2,898	2,606	10,839
System compromise	2,962	2,775	2,704	2,510	10,951
Denial of service	12	7	11	20	50
Phishing	340	376	257	264	1,237
Breach of integrity	2	7	4	2	15
Device vulnerabilities	5,848	5,938	6,464	6,362	24,612
Other	2,899	1,672	943	1,196	6,710

Figure 1. Reports on incidents by type processed by CERT-LT in 2017, percentage



Main Cyber Security Issues in 2017

Based on incident statistics, the two biggest cyber security problems in Lithuania are malicious software (malicious codes) and vulnerable information systems, including websites. The abovementioned security problems supplement each other and increase the potential risk to internet users. On one hand, vulnerable websites are compromised (content management systems) and malicious code is uploaded herein for distribution of malicious software. On the other hand, a special shell is uploaded to the compromised website which enables the malevolent party to execute more various malicious activities; besides the abovementioned distribution of malicious software it is also possible to scan and attack the networks and information systems, collect information, control other compromised devices, etc.

Malicious Software

As the cryptocurrencies become more popular, the developers of ransomware are very active. For the second consecutive year the recorded number of internet users affected by this type of malicious software is increasing. This virus affects both individual users and companies. Ransomware differs from other viruses in their “aggressiveness” – it does not try to mask the activity in the compromised system, the main purpose of these viruses is to encrypt files important to the system owner (e.g. DOC, DOCX, XLS, XLSX) or even the entire file system expecting that the owner will be willing to pay a ransom to get them back. For this purpose complex encryption algorithms are used, thus to restore the affected files without the encryption key is impossible. In certain cases (e.g. the company accounting database is encrypted and back-up is not available) the losses can be substantially large. Free file decryption tools (e.g. “The No More Ransom Project” project) have been created for some viruses, but the dynamics of viruses is so large and the encryption algorithms are so complex that the possibility of decrypting the files using these tools is very low. .

Very fast spread of one ransomware, called “WannaCry”, was recorded on 12 May 2017 (on Friday – like majority of large-scale attacks). This was one of the largest attacks of this nature throughout the digital age history. This malicious software had worm functionality which allowed spread in the network by using a vulnerability in the Windows operating system SMB protocol. The patch for this vulnerability was released two months before the attack; therefore, a large number of infected computer systems once again showed users' indifferent attitude to their device security and that they do not understand the risk when using outdated software. During one day the number of affected computers exceeded 230 thousand and affected more than 150 countries in the world. Among the affected ones in the European Union were academic institutions, hospitals, telecommunication infrastructures, transport companies, and other important information infrastructures. About 180 IP addresses affected by this virus were detected in Lithuania. CERT-LT has not received any information about the confirmed cases (i.e., about encrypted computer systems in Lithuania). For details on "WannaCry" see CERT-LT website.

Another fast proliferating malicious code "NotPetya" was developed on the basis of ransomware "Petya" in 2016 and was massively proliferated in Europe at the end of June 2017. This virus mostly affected computer systems in Eastern Europe countries. 5 breaches of information systems were confirmed in Lithuania (in some cases – up to several hundred computers), which caused interruption of companies' activities and losses. It shall be noted that the data was not encrypted, but simply obliterated without possibility to restore it. Several methods were used for virus proliferation and one of them, as in case of "WannaCry" virus, by using "Samba" (SMB) protocol vulnerabilities.

Usually during virus activation UAC (User Account Control) window pops up. If the user presses "No", the virus is denied additional rights and it cannot do harm.

Proliferation of the abovementioned viruses was attributed to software security vulnerabilities, including "Samba". It shows how important it is to update the existing software on regular basis.

Usually the malicious software is distributed together with spam. By using social engineering there are attempts to persuade the users to open the file attached in the email which at first glance does not pose any threat to the victim's computer. In 2017, usually there were Microsoft Office or PDF documents and ZIP archives containing malicious code developed in Visual Basic or JavaScript programming language. After opening these files, the abovementioned malicious code is activated, uploads and starts another malicious code (i.e., it operates as the initiator of malicious activity), usually a ransomware.

CERT-LT reminds that upon receiving a suspicious email with attachments, it must be handed with caution. Please make sure that the sender really sent you this email, check the attachments with available antivirus software or free online tool www.virustotal.com. Do not open email attachments if you do not know the sender.

Information System Compromise

10,951 cases of information system compromise incidents were registered in 2017 (10,673 cases in 2016). This type of incidents includes the compromised devices used to execute the malicious activity and the affected, compromised websites.

Every day CERT-LT records 10 cases on average of newly compromised websites.

Since autumn 2017 we have been observing the increasing use of compromised websites for generation of cryptocurrencies. Instead of infecting the visitor devices with malicious code, as it was done previously, now website visitors' computers (or smart devices) more often are used for intense calculations.

It is a new trend of malicious activity that appeared only this year. When a person visits the website (e.g. www.example.com) with a link to a software code for generation of cryptocurrency located in the same or other website (e.g. www.example.com/script.js or www.example2.com/script.js), the website starts intense calculations. The code for generation of cryptocurrency in the website can appear in the following cases:

- cyber criminals compromise a vulnerable website (e.g. using the outdated content management system) and insert the abovementioned script.
- The software code into the website is inserted by the website developer (programmer) or administrator and this is done without knowledge of the website owner.

- The script is inserted into the website intentionally by the website owner to get financial gain.

The cases when the website owner inserts the cryptocurrency generation script intentionally and does not inform hereof the website visitors CERT-LT treats as unethical activity since the process takes place without knowledge of the visitor whose computer resources are exploited.

Websites using outdated and thus vulnerable content management system (CMS), website plugins and/or extensions, more often show the signs of website compromise – the inscriptions of malevolent parties, like "Hacked by ...", etc. Such inscriptions are usually hidden and do not execute any malicious activity, but this is the sign that the website is compromised and can contain malicious code.

According to the data of analysis performed by CERT-LT in Q4 2017, about 70 % of website contents management systems (CMS) were outdated (calculating only .LT zone domain websites and only those CMSes the versions of which were successfully identified).

To reduce the threat of compromise, the website owners must take care of the website security: protect website admin panel, use a complex login password and change it on a regular basis, install content management system and extension updates. In general the use of extensions without special need is discouraged. Website designers that install popular content management systems (Wordpress, Joomla, etc.) must also ensure their proper configuration. Read more in our recommendation.

Botnets

Networks of compromised computers (botnets) are the result of main security problems - vulnerable information systems and malicious software. They are used to conduct various cyber-attacks: distribution of malicious software and spam, denial-of-service attacks, etc. This problem is especially relevant as there is a continuous growth of "IoT" (Internet of Things) devices – any devices connected to internet: home electronics, sensors, video cameras, etc. These devices usually cause security problems (e.g. default manufacturer passwords are used, software is not updated, having vulnerabilities, etc.) and can form huge botnets. Based on "Gartner" data, there were more "IoT" devices in the world than the global population, about 8-8.4 billion items.

The owner of the device can be unaware of inclusion into the botnet for a long time. According to data of CERT-LT, an average of 3,000–3,200 computers, remotely used without the knowledge of their owners, were identified in Lithuania every month in 2017. The information on activity level of computers detected in botnets is published on our website.

In 2017, the following two "IoT" botnets were active in Lithuania: "Mirai" and "Reaper" ("Reaper IoT", "IoTroop"). "Reaper" used the part of "Mirai" software code and the other part was unique. According to CERT-LT data, in Q4 447 devices controlled by "Mirai" and "Reaper" (unique IP addresses) were detected in Lithuania. There were 626, 464, and 369 compromised devices respectively in QI, QII, and QIII.

It is very important to change manufacturer set passwords and default configuration in the used "IoT" devices and ensure their software updating.

Phishing

The number of phishing of popular websites continued growing in 2017. CERT-LT investigated 1,237 reports on website phishing. In 2016, there were 555 cases. Malevolent parties establish fake websites to make profit. The most frequent phishing development methods:

- a random vulnerable website is compromised and fake content is inserted (e.g. www.vulnerableweb.lt/fake-content).
- A new fake website is developed with the similar domain name of the original website (e.g. the original website – www.thename.lt and the fake one – www.tehname.lt).

The majority of cases of fake websites investigated by CERT-LT were the reports about the fake electronic payment system website “Paypal”, also “Facebook”, “Gmail” and similar services hosted in Lithuania. It must be noted that these fake websites were not directly targeted at the Lithuanian internet users.

Much less often (about 20 cases per year) the fake websites of e-banking platforms of banks operating in Lithuania emerge. Most often 2 compromised websites are used; one of them has only redirection, and the other one – landing page. Both websites almost always are placed in different foreign servers; therefore, the removal usually takes a little bit longer due to difference in time zones.

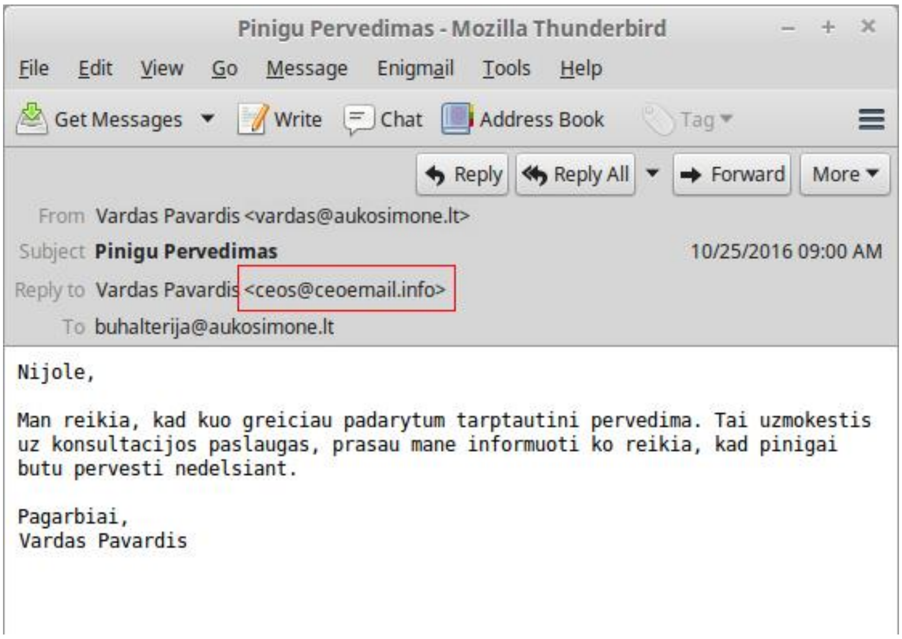
In 2017, malevolent parties distributed messages seeking to obtain login details to e-banking not only by emails, but also by SMS. The senders of SMS used to inform about the received or settled new payment and about the necessity to perform some action by clicking the internet link in the message.

Prior to entering your personal data on the website, make sure that it is authentic. Please pay attention to the domain name and the links contained on the website. E-banking systems always use secure TLS protocol, the address always begins with “https” (or green bar) and the website certificate may be checked. The banks never ask you to provide or change e-banking or payment card passwords that are known only to you via email or by phone. If there is a suspicion that the website is a fake, it is advised to enter the address of the original website into browser location bar manually.

Cyber Fraud

The scope of cyber fraud and resulting losses did not decrease in 2017. Phishers quickly master new technologies, as well as successfully apply the old ones. Though the number of people defrauded in the digital space is relatively small, but the consequences for residents and companies are painful.

“C-level fraud” phishing campaign, where “C” stands for CEO (Chief Executive Officer) started in 2016 and further successfully continued its activities in 2017. This phishing model is aimed at the company accountants or decision makers. Criminals pretend to be company managers and prompt the accountants to make urgent international transactions. A fake email looks as follows:


Pinigu Pervedimas - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More

From Vardas Pavardis <vardas@aukosimone.lt>
Subject **Pinigu Pervedimas** 10/25/2016 09:00 AM
Reply to Vardas Pavardis <ceos@ceoemail.info>
To buhalterija@aukosimone.lt

```
Nijole,

Man reikia, kad kuo greiciau padarytum tarptautini pervedima. Tai uzmokestis
uz konsultacijos paslaugas, prasau mane informuoti ko reikia, kad pinigai
butu pervesti nedelsiant.

Pagarbiai,
Vardas Pavardis
```

Fig. 1. Example of social engineering – fake email address

Another frequent phishing case is money hustling by pretending to be the company business partner. This is a more sophisticated attack where the criminals have to be well prepared by collecting the information about the company to-be-attacked, its business transactions, etc. Furthermore, during the attack sometimes the information systems of one party participating in the transaction are compromised, their internal correspondence is tracked; therefore, at the proper moment the money transactions can be directed to the accounts of the criminals.

The companies' managers must establish particular procedures to be followed during financial operations. Employees shall be informed about phishing of this type. Alertness level can be increased by regular testing of employees regarding their resistance to threats which can be performed by the company or specialists hired namely for this purpose.

One more popular phishing method is pretending to be the purchaser of movable property. A cyber criminal contacts the seller by email and asks if the latter agrees to receive a transaction for the sold property (e.g. a car) using the online payment platform "PayPal". If the seller agrees, then the alleged purchaser indicates that the car will be collected not by him, but courier, the purchaser will add 500 euros for the courier services and additional 50 euros "for additional trouble". When the counterparties finally agree and the purchaser allegedly "makes a transaction", the seller receives a fake email allegedly from "PayPal" where it is indicated that the funds have reached the seller's account, but "We've placed a temporary hold on the funds of this transaction". In order to control the abovementioned funds, the person (i.e., the seller of the car) has to get to the closest "Western Union" office and transfer 500 euros "for courier services". After the person makes such a transfer, his/her funds are usually lost.

Incidents of Other Types

A large part of "IoT" devices (for more details see Section "Botnets") have various vulnerabilities. Usually such vulnerabilities do not present a direct threat to the safety of device owners' data; however, they allow malevolent parties to use such devices for Distributed Denial of Service (DDoS) attacks as attack boosters. In 2017, there were 24,612 devices registered with security holes (in 2016 – 20,490).

In 2017, CERT-LT investigated 50 reports on Denial of Service (DoS) attacks (61 reports were investigated in 2016). Such attacks are usually automated by using botnet resources or exploiting vulnerable network devices. In order to terminate the attacks, CERT-LT provided recommendations to the owners of compromised and vulnerable devices. Also, the recommendations were provided to electronic information hosting service providers on how to stop such attacks; the actions were coordinated with the internet service providers and CERTs operating in other countries.

During 2017, 15 violations were registered of communication network integrity (in 2016 – 21). There were 6,710 various incidents (including the ones described in Section "Cyber Fraud").

To conclude, the summary of cyber incidents processed by CERT-LT during the period between 2010 and 2017 is provided.

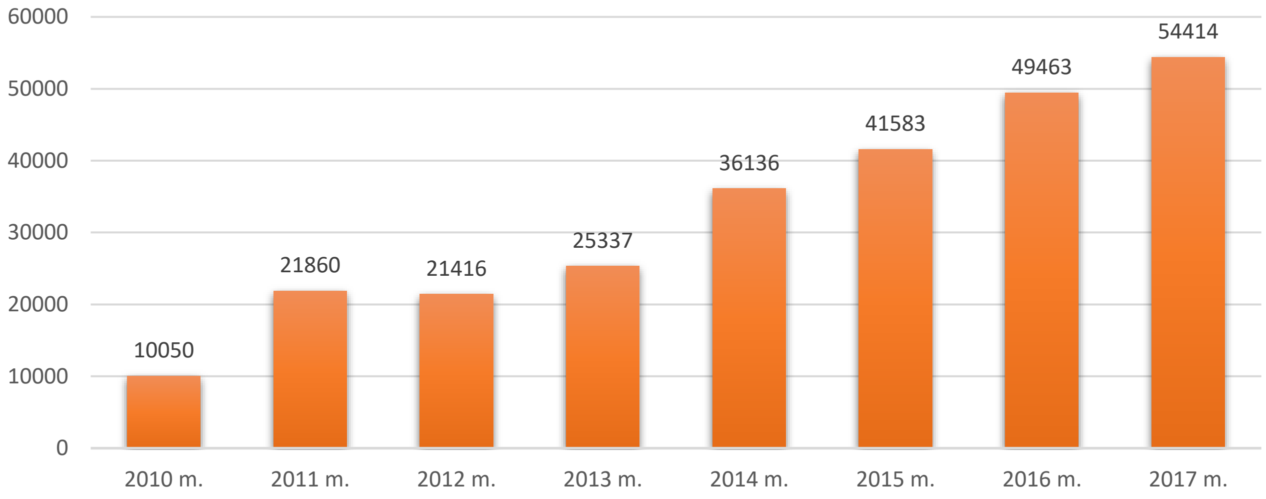


Figure 2. Summary of incidents processed by CERT-LT in 2010-2017

Amendment to the Law on Cyber Security

On 19 December 2017 the Seimas of the Republic of Lithuania adopted the amendments to the Law on Cyber Security which consolidated the security of information resources and the functions of the national electronic communications networks and information security incident investigation performed by the Communications Regulatory Authority of the Republic of Lithuania were transferred to the newly established National Cyber Security Centre under the Ministry of National Defence since 1 January 2018. The Law on Electronic Communications was also amended accordingly.

Before the abovementioned amendments came into effect, the security of information resources was ensured by the Cyber Security and Telecommunications Service at the Ministry of National Defence performing functions of the National Cyber Security Centre and Communications Regulatory Authority. The National Cyber Security Centre ensured the security of the State information resources and critical information infrastructures and the Communications Regulatory Authority – the security and integrity of public communications networks, public electronic communications services, and electronic information hosting services.

Changes made on the basis of adopted amendments will help to ensure coherent and coordinated implementation of information security policies, a clear and consistent regulation of cyber security.

Informing of the Public

CERT-LT publishes important and relevant information on its website www.cert.lt. Here you can:

- read IT security-related news;
- review summarized statistics (both charts and reports);
- learn the main objectives of CERT-LT;
- familiarize with legislation regulating cyber security;
- check your hardware for security holes and unauthorised activity;
- find security recommendations, descriptions of malicious software, and their removal manuals;
- report the criminal cyber activities;
- seek help in the event of a cyber incident.

Users encountering network and data security problems are advised to contact their internet service provider immediately and should the provider be unable to solve the problem, users should notify CERT-LT thereof by filling in the form on the website www.cert.lt/pranesti. More online security-related information for internet users is available on the website www.esaugumas.lt.

CERT-LT also provides cyber security-related notifications and short cyber-security news on social network Twitter at https://twitter.com/cert_lt.