CERT-LT ACTIVITY REPORT FOR THE FIRST QUARTER OF 2015

National Electronic Communications Networks and Information Security Incident Response Team of the Communications Regulatory Authority of the Republic of Lithuania (CERT-LT) summarizes activity results of the first quarter of 2015. **During the said quarter, CERT-LT investigated 11707 incidents pursuant to the notifications received from the Lithuanian electronic communications service providers, foreign CERT services engaged in the investigation of international incidents, and the Lithuanian Internet users.** If compared with the first quarter of 2014 (7375 incidents), the number of incidents increased by 59 percent. If compared with the fourth quarter of 2014 (11822 incidents), the number of incidents decreased by 1 percent.

According to the number of prevailing incidents this quarter is similar to the last quarter of 2014. The largest number of recorded incidents are related to vulnerabilities of network devices – 4856. In terms of the number of incidents, malicious software is in the 2nd place - 3051 cases. The increasing trend of these two types of incidents has changed and now the number of recorded insidents is slightly smaler (respectively 6.5 percent and 5.7 percent less than in the previous quarter). Also during the period referred to 1494 system compromises were recorded. CERT-LT studies have demonstrated that the majority of the detected computer compromise cases were carried out by automated means and associated with vulnerable Internet software.

There were 257 cases of phishing. Social websites (facebook.com, vk.com), e-mail systems (gmail.com, yahoo.com), the electronic billing website paypal.com were imitaded the most. Also websites of banks operating in Lithuania were faked. Using spam or other fraudulent means the evil-minded individuals were inviting to visit fake websites in order to obtain passwords or other confidential data. By prompt actions of CERT-LT those fakes were liquidated relatively quickly.

Other received and investigated notifications:
1) on illegal use of electronic data – 5;
2) on denial of services – 18;
3) on breach of integrity – 1;
4) various types – 2025.

CERT-LT regularly informs Internet users about cybernetic threats and provides recommendations on the website: www.cert.lt. The following events of the first quarter of 2015 should be noted:
1) Spread of the malicious software code "CTB Locker". It belongs to *the ransomware* (demanding a ransom) code family. Activated on a PC with Windows OS version, code encrypts files and displays a message proposing to pay a ransom (usually in bitcoins). CERT-LT advises to make backups constantly (at least one of which must be stored elsewhere).
2) A malicious Chrome browser add-on was spreading in the social website Facebook. Installed on a computer as an add-on, the program was sending to Facebook friends a link purportedly to a video clip. By clicking on a link, the other person could also infect his computer. Having completed the analysis, CERT-LT appealed to foreign service providers with a request to remove the components of the said harmful activity.
3) On 17 March, large part of the Lithuanian Internet, including websites of state institutions, was affected due to the state enterprise "Infostruktūra" equipment failure. Personnel of CERT-LT monitored occurance of the failure and its consequences using Lithuanian Internet Monitoring System LITIS. The European Network and Information Security Agency *(ENISA)* was notified about the failure. The consequences of failure were eliminated in about 3 hours.
4) The persistent activity of the malware code "Stealrat" generating botnets. Every day, CERT-LT records both new and already known infected websites. In all cases, the companies providing information hosting services and web hosts are encouraged to take measures for the elimination of malicious code and protection of the website.

Tables and charts provide summaries of incidents. All CERT-LT statistical incident reports can be found at: https://www.cert.lt/statistika.htm.

Table 1. Summary of incidents investigated by CERT-LT in the first quarter of 2015

Type of incident	Number of incidents	Percentage
Malicious software	3051	26
System compromise	1494	12.8
Denial of services	18	0.2
Phishing	257	2.2
Breach of integrity	1	0
Device security vulnerabilities	4856	41.5
Illegal use of electronic data	5	0
Other	2025	17.3

Table 2. Comparisson of the number of incidents investigated by CERT-LT in the fourth quarter of 2014 and the first quarter of 2015

Type of incident	Number of incidents Q4 2014	Number of incidents Q1 2015	Change, in percent
Malicious software	3237	3051	-5.7
System compromise	1369	1494	9.1
Denial of services	42	18	-57.1
Phishing	208	257	23,5
Breach of integrity	0	1	n/d
Device security vulnerabilities	5197	4856	-6.5
Illegal use of electronic data	6	5	-16.6
Other	1763	2025	14.8

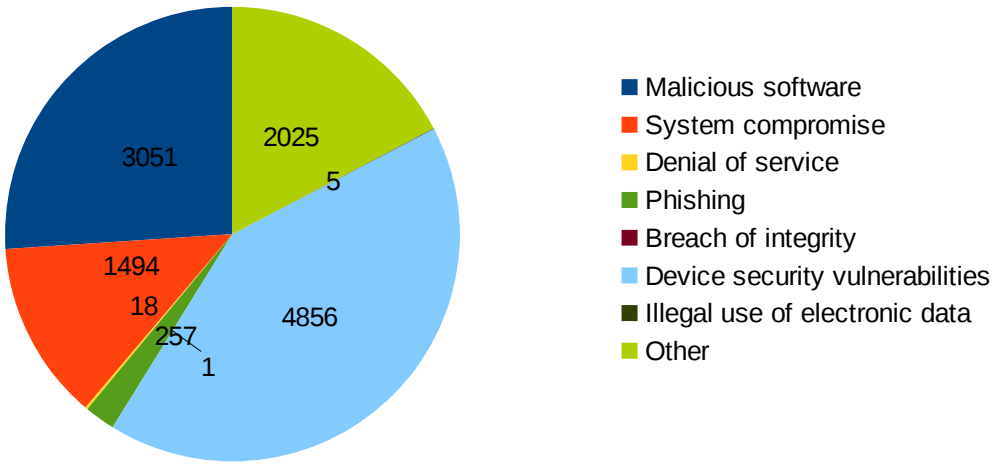

Fig. 1. Statistics of the incidents recorded by CERT-LT in the first quarter of 2015