CERT-LT ACTIVITY REPORT FOR THE FIRST QUARTER OF 2016

National Electronic Communications Networks and Information Security Incident Response Team of the Communications Regulatory Authority of the Republic of Lithuania (CERT-LT) summarizes its activity results of the first quarter of 2016. **During the said quarter, CERT-LT investigated 12035 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 1st quarter of 2015 (11707 incidents), the number of incidents increased by 2.8 percent. If compared with the 4th quarter of 2015 (10641 incidents), the number of incidents increased by 13.1 percent.

Percentage of the 2 main incident types hardly changed. 41 percent of the recorded incidents were related to vulnerabilities of network devices - 4963. A quarter of all incidents was taken by malicious software (viruses, Trojan horses, etc.) - 2887 cases. We witness growing number of system compromise. During the period referred 2902 compromise cases were recorded, almost twice as much as in Q1 2015. CERT-LT research data demonstrated that the majority of the detected computer compromise cases were carried out by automated means and associated with vulnerable software (e.g. a web server or a content management system).

During Q1 2016 we investigated 112 phishing cases. Social websites (e.g. facebook.com), e-mail systems (gmail.com, yahoo.com), the electronic billing website paypal.com were imitated the most. Also websites of banks operating in Lithuania and in foreign countries were faked (mostly the latter). 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 – 1;
2) on denial of electronic service – 10;
3) on breach of integrity – 6;
4) various types – 1154 (including 60 consultations).

Notable events of this quarter are:
1) Many unwanted emails with dangerous attachments were circulating on the web. The main difference compared to the previous quarters – type of attachment. Instead of EXE attachments (which are usually put into ZIP containers) we encountered “JavaScript” files. Subjects of emails were mostly English and were related to an invoice or a scanned document.
2) Security specialists found 2 critical vulnerabilities in widely used software. One of vulnerabilities existed since May of 2008 (Lithuanian announcements are at https://www.cert.lt/naujienos.html). It is worth noting that IT-Sec firm “Risk Based Security” had 14185 records in vulnerabilities catalogue of 2015.

Tables and charts provide summaries of incidents. All CERT-LT statistical incident reports can be found at: https://www.cert.lt/en/statistics.html. CERT-LT publishes warnings on incidents and short cybersecurity news in “Twitter” (mostly in Lithuanian). You are welcome to join us at https://twitter.com/cert_lt.

Table 1. Summary of incidents investigated by CERT-LT in the 1st quarter of 2016

Type of incident	Number of incidents	Percentage
Malicious software	2887	24
System compromise	2902	23.1
Denial of service	10	0.1
Phishing	112	0.9
Breach of integrity	6	0
Device security vulnerabilities	4963	41.2
Illegal use of electronic data	1	0
Other	1154	9.6

Table 2. Comparison of the number of incidents investigated by CERT-LT in the 1st and the 4th quarter of 2015 and the 1st quarter of 2016

Type of incident	Number of incidents		Change, in percent	
	Q4 2015	Q1 2015	Q1 2016 / Q4 2015	Q1 2016 / Q1 2015
Malicious software	2686	3051	7.5	-5.4
System compromise	2517	1494	15.3	94.2
Denial of service	7	18	42.9	-44.4
Phishing	116	257	-3.4	-56.4
Breach of integrity	5	1	20	500
Device security vulnerabilities	4383	4856	13.2	2.2
Illegal use of electronic data	0	5	n/d	-80
Other	927	2025	24.5	-43

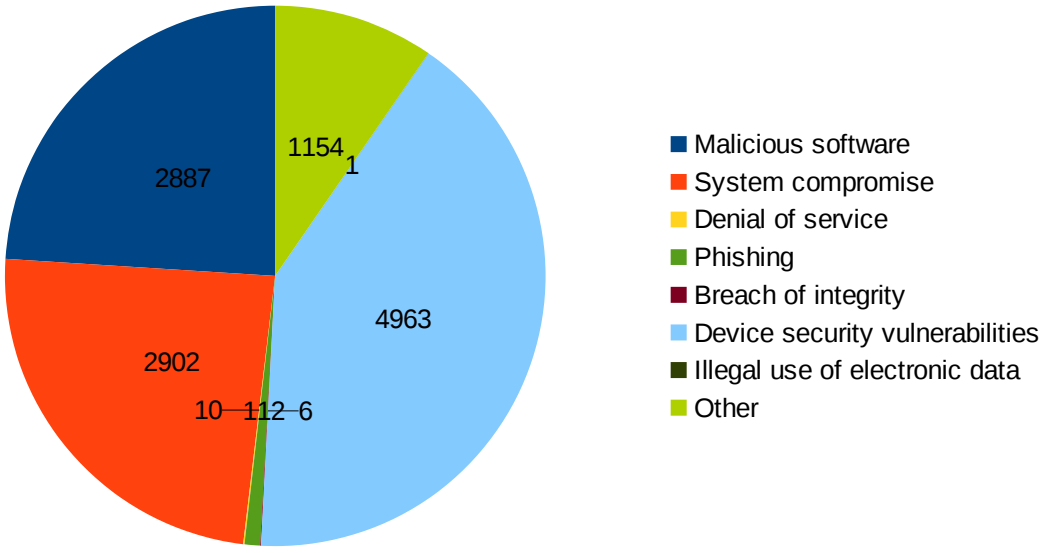

Fig. 1. Statistics of the incidents recorded by CERT-LT in the 1st quarter of 2016