CERT-LT ACTIVITY REPORT FOR THE FIRST QUARTER OF 2017

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 2017. **During the said quarter, CERT-LT handled 14,643 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.** 20 percent of incidents were handled manually. Manually processed incidents include system compromise, DoS cases and every message sent by any institution, enterprise or person. If compared with the 1st quarter of 2016 (12,035 incidents), the number of incidents increased by 21.7 percent. If compared with the 4th quarter of 2016 (13,874 incidents), the number of incidents increased by 5.5 percent.

Percentage of the 3 main incident types has only slightly changed. 40 per cent of the recorded incidents were related to vulnerabilities of network devices (including Internet of Things) – 5,848. 17.6 per cent of all incidents was taken by malicious software (ransomware, Trojan horses, etc.) – 2,580 cases. It seems that the number of system compromises has stabilized. During the period referred 2,962 compromise cases were recorded, and that is 2.1 per cent more than in Q1 2016. CERT-LT research data demonstrated that the majority of the detected computer compromise cases were carried out by automated means and were associated with vulnerable software (e.g. a web server or a content management system) or bad configuration (including weak passwords).

The number of phishing cases increased dramatically from 143 to 340. As in previous periods, social websites (facebook.com), e-mail systems (gmail.com, yahoo.com), the electronic billing website paypal.com were falsified most often. In January, there was a wave of phishing websites targeted at the clients of Lithuanian banks.

Other investigated notifications:
1) on breach of integrity – 2;
2) on denial of service – 12;
2) of various types – 2,899.

Notable events of this quarter are (Lithuanian announcements are at https://www.cert.lt/naujienos.html):
1) According to CERT-LT data, number of Lithuanian devices which were a part of Mirai botnet decreased. At the end of 2016, there were almost 150 such devices, meanwhile at the end of the said quarter there were approximately 90 devices.
2) Many enterprises using MongoDB database management system were attacked. Due to an improper configuration, these systems were accessible from the Internet and, therefore, vulnerable. Evil-minded persons used to compromise MondoDB installations and to encrypt the data. At the end of the quarter, there were almost 28,000 vulnerable MongoDB systems, including 50 in Lithuania.
3) State Tax Inspectorate phishing messages were circulating on the web. Such messages could be identified by the poor Lithuanian grammar. The messages contained a link to the forged website of the Inspectorate.
4) Cybercriminals were engaged in fraudulent campaigns. They used to pretend to be the CEO of a victim company and requested an “urgent payment”. CERT-LT encourages the accountants to stay alert and carefully analyse such “requests”.

A table and a chart 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. Comparison of the number of incidents handled by CERT-LT in the 1st and the 4th quarter of 2016 and in the 1st quarter of 2017

Type of incident	Number of incidents			Change, in percent	
	Q1 2016	Q4 2016	Q1 2017	Q1 2017 / Q1 2016	Q1 2017 / Q4 2016
Malicious software	2 887	2 989	2 580	-10.6	-13.7
System compromise	2 902	3 098	2 962	+2.1	-4.4
Denial of service	10	4	12	+20	+200
Phishing	112	143	340	+203.6	+137.8
Breach of integrity	6	1	2	-66.7	+100
Device security vulnerabilities	4 963	5 801	5 848	+17.8	+0.8
Illegal use of electronic data	1	0	0	-100	n/d
Other	1 154	1 838	2 899	+151.2	+57.7
Total	12 035	13 874	14 643	+21.7	+5.5

Fig. 1. Percentage of the incidents handled by CERT-LT in the 1st quarter of 2017