CERT-LT ACTIVITY REPORT FOR THE SECOND 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 2nd quarter of 2017. **During the said quarter, CERT-LT handled 13,530 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.** 14 percent of incidents (1,840) 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 2nd quarter of 2016 (10,991 incidents), the number of incidents increased by 23.1 percent. If compared with the 1st quarter of 2017 (14,643 incidents), the number of incidents decreased by 7.6 percent.

44 per cent of the recorded incidents were related to vulnerabilities of network devices (including Internet of Things) – 5,905. 20 per cent of all incidents was taken by malicious software (ransomware, Trojan horses, etc.) – 2,755 cases. It seems that the number of system is slowly going down. During the period referred 2,775 compromise cases were recorded, and that is 6.3 per cent less than in Q1 2017. 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 to 376 from 147 in 2nd quarter of 2016. 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 June, there was a wave of phishing websites targeted at the clients of Lithuanian banks.

Other investigated notifications:
1) on breach of integrity – 7;
2) on denial of service – 7;
2) of various types – 1,672.

Notable events of this quarter are (Lithuanian announcements are at https://www.cert.lt/naujienos.html):
1) Huge outbreak of ransomware called “WannaCry”. The malware was exploiting “SMB/Samba” vulnerability. Many enterprises were attacked all over the globe.
2) At the end of June cybercriminals launched another data encrypting virus called “Petya/NotPetya”. It exploited “Samba” vulnerability too.
3) A new way to carry out a phishing campaign was presented to public. The security analysts made a website very similar to the website of the famous “Apple” corporation. The domain of a fake website utilized Unicode.
4) CERT-LT introduced a new incident type – threat. A threat is a vulnerability of a high importance. Ignoring a threat may result in a serious incident.
5) Cybercriminals were engaged in spear phishing 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 2nd quarter of 2017 and in the two quarters of 2017

Type of incident	Number of incidents			Change, in percent	
	Q2 2016	Q1 2017	Q2 2017	Q2 2017 / Q2 2016	Q2 2017 / Q1 2017
Threat (a new type)	n/d	n/d	33	n/d	n/d
Malicious software	2 531	2 580	2 755	+8.9	+6.8
System compromise	2 290	2 962	2 775	+21.2	-6.3
Denial of service	36	12	7	-80.6	-41.7
Phishing	147	340	376	+155.8	+10.6
Breach of integrity	11	2	7	-36.4	+133.3
Device security vulnerabilities	4 417	5 848	5 905	+33.7	+1
Other	1 559	2 899	1 672	+7.2	-42.3
Total	10 991	14 643	13 530	+23.1	-7.6

Fig. 1. Percentage of the main incidents handled by CERT-LT in the 2nd quarter of 2017