CERT-LT ACTIVITY REPORT FOR THE THIRD 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 3rd quarter of 2017. **During the said quarter, CERT-LT handled 13,281 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.**

9.5 percent of incidents (1,255) 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 3rd quarter of 2016 (12,563 incidents), the number of incidents increased by 5.7 percent. If compared with the 2nd quarter of 2017 (13,530 incidents), the number of incidents decreased by 1.8 percent.

22 percent of all incidents was taken by malicious software (ransomware, Trojan horses, etc.) – 2,898 incidents cases. During the period referred 2,704 compromise cases were recorded. Usually a compromised system is a hacked website which spreads a malicious code or just contains the hacker's signature. However hackers follow trends and we had 2 extraordinary cases: websites containing cryptocurrency mining script. When a visitor opens such a website the browser utilizes the CPU with intense calculations. Obviously this happens without visitor's consent.

There were 6 464 cases related to network devices having various vulnerabilities. The mentioned number includes devices called *Internet of Things*. Vulnerable devices may eventually become a part of a certain botnet (for example, Mirai).

The number of phishing cases increased by 68 percent (compared to 3rd quarter of 2016) to 257. 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 the beginning of July and in the middle of August we encountered the fake copies of the billing systems of Lithuanian banks. It is worth mentioning that phishing links spreaded via email and SMS. Persons carrying out other kind of social engineering attacks – *C-level fraud* – were constantly active during the mentioned quarter.

Other investigated notifications: on breach of integrity – 4, on denial of service – 11, of various types – 943.

Lithuanian cybersecurity announcements are located at https://www.cert.lt/naujienos.html.

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 3rd quarter of 2016 and in the two quarters of 2017

Type of incident	Number of incidents			Change, in percent	
	Q3 2016	Q2 2017	Q3 2017	Q3 2017 / Q3 2016	Q3 2017 / Q2 2017
Malicious software	2 805	2 755	2 898	+3.3	+5.2
System compromise	2 383	2 775	2 704	+13.5	–2.6
Denial of service	11	7	11	0	+57.1
Phishing	153	376	257	+68	–31.6
Breach of integrity	3	7	4	+33.3	–42.9
Device security vulnerabilities	5 309	5 905	6 464	+21.8	+9.5
Other	1 899	1 672	943	–50.3	–43.6
Total	12 563	13 530	13 281	+5.7	–1.8

Fig. 1. Percentage of the main incidents handled by CERT-LT in the 3rd quarter of 2017