CERT-LT ACTIVITY REPORT FOR THE FOURTH 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 4th quarter of 2017. **During the said quarter, CERT-LT handled 12,960 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.** 14.4 percent of incidents (1,866) 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 4th quarter of 2016 (13,874 incidents), the number of incidents decreased by 6.6 percent. If compared with the 3rd quarter of 2017 (13,281 incidents), the number of incidents decreased by 2.4 percent.

20 per cent of all incidents was taken by malicious software (ransomware, Trojan horses, etc.) – 2,606 incidents cases. During the period referred 2,510 compromise cases were recorded. These two incident types are slowly going down. The number of websites which spread malicious code (inserted in a corresponding content management system) is also decreasing.

The number of phishing cases increased to 264 from 143 in 4th 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. Several times we encountered the fake copies of the billing systems of Lithuanian banks. There were no web pages imitating popular Lithuanian websites.

Other investigated notifications: on breach of integrity – 2, on denial of service – 20, of various types – 1,196.

Notable events of this quarter are (Lithuanian announcements are located at https://www.cert.lt/naujienos.html):

- We observe a plenty of websites with a specific script written in JavaScript language. When a visitor opens such a website in his/her browser visitor’s CPU starts intense calculations related to cryptocurrency mining.
- Evil-minded persons targeted citizens selling their stuff (e.g. a camera, a notebook) on the Internet. The fraud scheme includes forged email from Paypal and a request to transfer a certain amount of money via Western Union.
- It is usual that during a winter time cybercriminals launch more fake e-shops. A tricked person orders some stuff, pays with his/her credit card however receives nothing.
- C-level fraud is a truly malicious phenomenon in Lithuania. There is at least a dozen of Lithuanian firms where employees were tricked to conduct a wire transfer to an account controlled by criminals.

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 4th quarter of 2016 and in the two quarters of 2017

Type of incident	Number of incidents			Change, in percent	
	Q4 2016	Q3 2017	Q4 2017	Q4 2017 / Q4 2016	Q4 2017 / Q3 2017
Malicious software	2 989	2 898	2 606	-12.8	-10.1
System compromise	3 098	2 704	2 510	-19	-7.2
Denial of service	4	11	20	+400	+81.8
Phishing	143	257	264	+84.6	+2.7
Breach of integrity	1	4	2	+100	-50
Device security vulnerabilities	5 801	6 392	6 362	+9.7	-1.6
Other	1 838	943	1 196	-35	+26.8
Total	13 874	13 281	12 960	-6.6	-2.4

Fig. 1. Percentage of the main incidents handled by CERT-LT in the 4th quarter of 2017