CERT-LT ACTIVITY REPORT FOR THE THIRD 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 third quarter of 2016. **During the said quarter, CERT-LT handled 12,563 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.** 16 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 3rd quarter of 2015 (9,708 incidents), the number of incidents increased by 29.4 percent. If compared with the 2nd quarter of 2016 (10,991 incidents), the number of incidents increased by 14.3 percent.

Percentage of the 2 main incident types has slightly increased. 42 percent of the recorded incidents were related to vulnerabilities of network devices – 5,309. Almost a quarter of all incidents was taken by malicious software (viruses, Trojan horses, etc.) - 2,805 cases. We constantly witness significant number of system compromise. During the period referred 2,383 compromise cases were recorded, 41 percent more than in Q3 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 Q3 2016 we investigated 153 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. These incidents are easy to deal with and the threats are removed rapidly.

Other investigated notifications:
1) on illegal use of electronic data – 0;
2) on breach of integrity – 3;
3) various types – 1899.

Notable events of this quarter are (Lithuanian announcements are at https://www.cert.lt/naujienos.html):
1) Many unwanted emails with dangerous attachments are still circulating on the web. ZIP containers in those e-mails contain malicious “JavaScript” files. Subjects of emails are mostly in English and are related to an invoice or a scanned document. The good thing about this threat is that it can be easily recognized because the attachments are quite small (several KB). However, if the attachment is activated, the computer may be infected with an extremely hostile malware (which is called ransomware).
2) Dangerous vulnerabilities found in popular database management systems “MySQL” and “MariaDB”.
3) Vulnerabilities found in “Cisco” devices.

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 2015 and the 2nd and the 3rd quarter of 2016

Type of incident	Number of incidents			Change, in percent	
	Q3 2015	Q2 2016	Q3 2016	Q3 2016 / Q3 2015	Q3 2016 / Q2 2016
Malicious software	2,612	2,531	2,805	7.4	10.8
System compromise	1,686	2,290	2,383	41.3	4.1
Denial of service	11	36	11	0	–69.4
Phishing	103	147	153	48.5	4,1
Breach of integrity	2	11	3	50	–72.7
Device security vulnerabilities	4,490	4,417	5,309	18.2	20.2
Illegal use of electronic data	8	0	0	–100	n/d
Other	796	1,559	1,899	138.6	21.8
Total	9,708	10,991	12,563	29.4	14.3

Fig. 1. Percentage of the incidents handled by CERT-LT in the 3rd quarter of 2016