CERT-LT ACTIVITY REPORT FOR THE FOURTH 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 fourth quarter of 2016. **During the said quarter, CERT-LT handled 13,874 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.** 15 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 4th quarter of 2015 (10,641 incidents), the number of incidents increased by 30.4 percent. If compared with the 3rd quarter of 2016 (12,563 incidents), the number of incidents increased by 10.4 percent.

Percentage of the 3 main incident types has only slightly changed. 42 percent of the recorded incidents were related to vulnerabilities of network devices – 5,801. 22 percent of all incidents was taken by malicious software (viruses, Trojan horses, etc.) - 2,989 cases. For many months the number of system compromise only increases. During the period referred 3,098 compromise cases were recorded, 30 percent more than in Q3 2016. 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 Q4 2016 we investigated 143 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 breach of integrity – 1;
2) on denial of service – 7;
2) various types – 1838.

Notable events of this quarter are (Lithuanian announcements are at https://www.cert.lt/naujienos.html):
1) Critical vulnerabilities found in “PHPmailer” library, used by many popular IT systems like “Joomla”, “Drupal”, “SugarCRM”, etc.
2) Huge “Mirai” botnet was found operating. The operators of this botnet carried out several attacks against foreign ICT companies. Lithuanian Internet users also encountered the consequences of these attacks (e. g. websites were not accessible). At the end of the year, there were almost 150 Lithuanian Internet devices compromised by “Mirai” (the calculation takes into account unique IP addresses).
3) CERT-LT and Lithuanian police combined forces and joined 2 international education campaigns. The 1st campaign was related to mobile malware and the other was related to participation of youth in cyber-crimes.
4) In October, CERT-LT and several Lithuanian ICT companies participated in cyber exercises called “Cyber Europe 2016”. These exercises were the largest and the most sophisticated exercises carried out in the EU so far. IT security professionals from more than 300 EU and EFTA based organizations took part in these exercises. More information is available at https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016/.

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 2015 and the 3rd and the 4th quarter of 2016

Type of incident	Number of incidents			Change, in percent	
	Q4 2015	Q3 2016	Q4 2016	Q4 2016 / Q4 2015	Q4 2016 / Q3 2016
Malicious software	2 686	2 805	2 989	11,3	6,6
System compromise	2 517	2 383	3 098	23,1	30
Denial of service	7	11	4	-42,9	-63,6
Phishing	116	153	143	23,3	-6,5
Breach of integrity	5	3	1	-80	-66,7
Device security vulnerabilities	4 383	5 309	5 801	32,4	9,3
Illegal use of electronic data	0	0	0	n/d	n/d
Other	927	1 899	1 838	98,3	-3,2
Total	10 641	12 563	13 874	30,4	10,4

Fig. 1. Percentage of the incidents handled by CERT-LT in the 4th quarter of 2016