CERT-LT ACTIVITY REPORT FOR THE SECOND 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 second quarter of 2016. **During the said quarter, CERT-LT handled 10991 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.** 17 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 2nd quarter of 2015 (9527 incidents), the number of incidents increased by 15.4 percent. If compared with the 1st quarter of 2016 (12035 incidents), the number of incidents decreased by 8.7 percent.

Percentage of the 2 main incident types hardly changed. 40 percent of the recorded incidents were related to vulnerabilities of network devices - 4417. A quarter of all incidents was taken by malicious software (viruses, Trojan horses, etc.) - 2531 cases. We constantly witness significant number of system compromise. During the period referred 2290 compromise cases were recorded, almost 80 percent more than in Q2 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 Q2 2016 we investigated 147 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.

In April and May dozens of denial of electronic service (DoS) attacks were carried out. We have recorded 36 distributed DoS attacks which targeted websites of Lithuanian institutions, banks, mass media companies, etc. Unfortunately, it is not easy to mitigate such attacks since the source IP addresses are usually spoofed. Good anti-DoS defence should include cooperation among ISPs, hosting companies and the owners of the attacked information systems. Other investigated notifications:
1) on illegal use of electronic data – 0;
2) on breach of integrity – 11;
3) various types – 1559 (including 51 consultations).

Other 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) Thousands of problematic Lithuanian websites were detected. The main problem was an improper configuration of a “pingback” function within the popular content management system “Wordpress”. Evil-minded persons, which had a large list of such websites, used this vulnerability for carrying out the DDoS attacks against a particular website.

Tables and charts 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. Summary of incidents handled by CERT-LT in the 2nd quarter of 2016

Type of incident	Number of incidents	Percentage
Malicious software	2531	23
System compromise	2290	20.8
Denial of service	36	0.3
Phishing	147	1.3
Breach of integrity	11	0.1
Device security vulnerabilities	4417	40.2
Illegal use of electronic data	0	0
Other	1559	14.2

Table 2. Comparison of the number of incidents handled by CERT-LT in the 2nd quarter of 2015 and the 1st and the 2nd quarter of 2016

Type of incident	Number of incidents		Change, in percent	
	Q1 2016	Q2 2015	Q2 2016 / Q1 2016	Q2 2016 / Q2 2015
Malicious software	2887	2579	-12.3	-1.9
System compromise	2902	1278	-21.1	79.2
Denial of service	10	14	260	157.1
Phishing	112	83	31.3	77.1
Breach of integrity	6	2	83.3	450
Device security vulnerabilities	4963	4698	-11	-6
Illegal use of electronic data	2	8	-100	-100
Other	1154	865	35.1	80.2

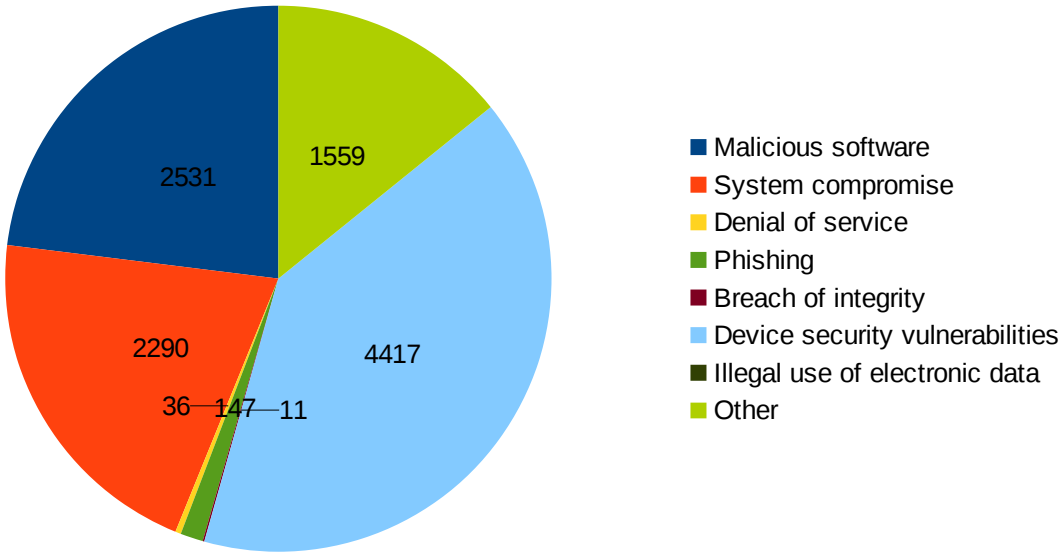

Fig. 1. Statistics of the incidents handled by CERT-LT in the 2nd quarter of 2016