CERT-LT ACTIVITY REPORT FOR THE FOURTH QUARTER OF 2015

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 2015. **During the said quarter, CERT-LT investigated 10641 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.** If compared with the fourth quarter of 2014 (11822 incidents), the number of incidents decreased by 10 percent. If compared with the third quarter of 2015 (9708 incidents), the number of incidents increased by 9.6 percent.

More than 40 percent of recorded incidents are related to vulnerabilities of network devices - 4383. A quarter of all incidents is taken by malicious software (viruses, Trojan horses, etc.) - 2686 cases. Also during the period referred to 2517 system compromises were recorded. 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). The quarter differs significantly when compared to Q4 2014. And main differences if compared to Q3 2015 are:
1) number of system compromise cases increased by 49 percent;
2) number of denial of service cases decreased by 36 percent;

During Q4 2015 we investigated 116 phishing cases. Social websites (facebook.com, vk.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. By prompt actions of CERT-LT those fakes were liquidated relatively quickly.

Other received and investigated notifications:
1) on illegal use of electronic data – 0;
2) on denial of electronic service – 7;
3) on breach of integrity – 5;
4) various types – 927 (including 95 consultations).

Notable events of this quarter are:
1) Many unwanted emails with dangerous ransomware attachments were circulating on the web. Ransomware viruses encrypt user's files and request a certain payment to decrypt them. Although there are several tools designed to decrypt encrypted files (e.g. https://noransom.kaspersky.com/), a chance to succeed is very little. Plenty of IT / IT security related websites consider ransomware to be the biggest threat in 2016.
2) At the end of December of 2015 a worm called “Pykspa” has taken over hundreds of computers located in Lithuania. During a peak of its activity there were more than 600 compromised computers.

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 investigated by CERT-LT in the 4th quarter of 2015

Type of incident	Number of incidents	Percentage
Malicious software	2686	25.2
System compromise	2517	23.7
Denial of service	7	0.1
Phishing	116	1.1
Breach of integrity	5	0
Device security vulnerabilities	4383	41.2
Illegal use of electronic data	0	0
Other	927	8.7

Table 2. Comparison of the number of incidents investigated by CERT-LT in the 4th quarter of 2014, the 3rd and the 4th quarter of 2015

Type of incident	Number of incidents		Change, in percent	
	Q3 2015	Q4 2014	Q4 2015 / Q3 2015	Q4 2015 / Q4 2014
Malicious software	2612	3237	2.8	-17
System compromise	1686	1369	49.3	83.9
Denial of service	11	42	-36.4	-83.3
Phishing	103	208	12.6	-44.2
Breach of integrity	2	0	150	n/d
Device security vulnerabilities	4490	5197	-2.4	-15.7
Illegal use of electronic data	8	6	-100	-100
Other	796	1763	16.5	-47.4

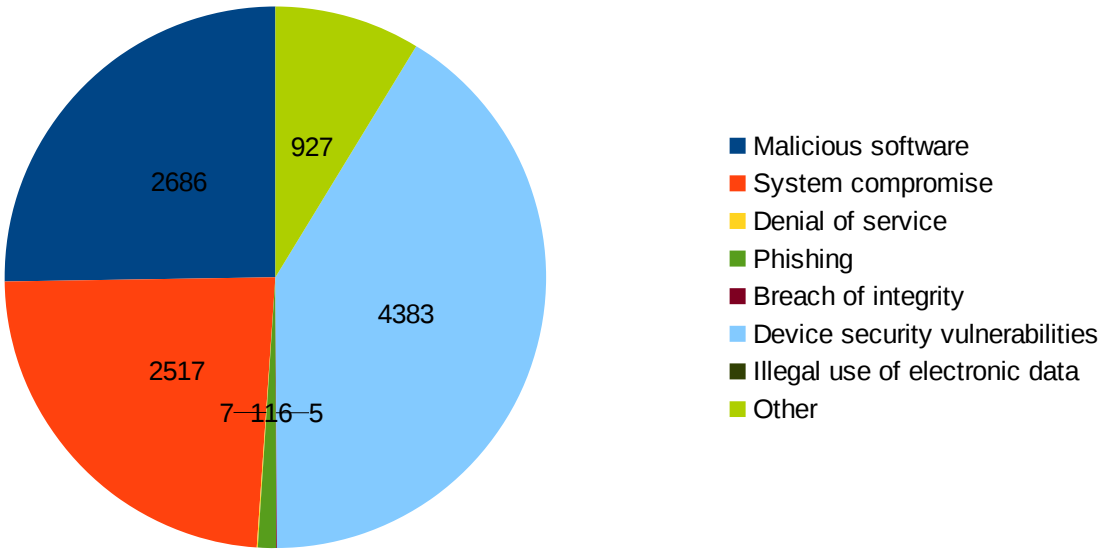

Fig. 1. Statistics of the incidents recorded by CERT-LT in the fourth quarter of 2015