CERT-LT ANNUAL ACTIVITY REPORT FOR 2015

The National Electronic Communication Networks and Information Security Computer Emergency Response Team (CERT-LT) of the Republic of Lithuania has summarized its activity results for 2015. In 2015, CERT-LT investigated 41,583 reports on incidents received from Lithuanian electronic communications service providers, foreign CERT services engaged in the investigation of international incidents, and Lithuanian Internet users. Compared to 2014 (36,136 reports), the number of cyberincidents increased by 15 per cent. The summaries of the investigated reports by type are presented in Table 1 and Figure 1.

Table 1. Reports by type investigated by CERT-LT in 2015

Type of report	2015				
	Q1	Q2	Q3	Q4	Total
Malicious software	3 051	2 579	2 612	2 686	10 928
Information system compromise	1 494	1 278	1 686	2 517	6 975
Denial-of-service	18	14	11	7	50
Phishing	257	83	103	116	559
Breaches of integrity	1	2	2	5	10
Device security vulnerabilities	4 856	4 698	4 490	4 383	18 427
Unlawful use of electronic data	5	8	8	0	21
Other	2025	865	796	927	4 613

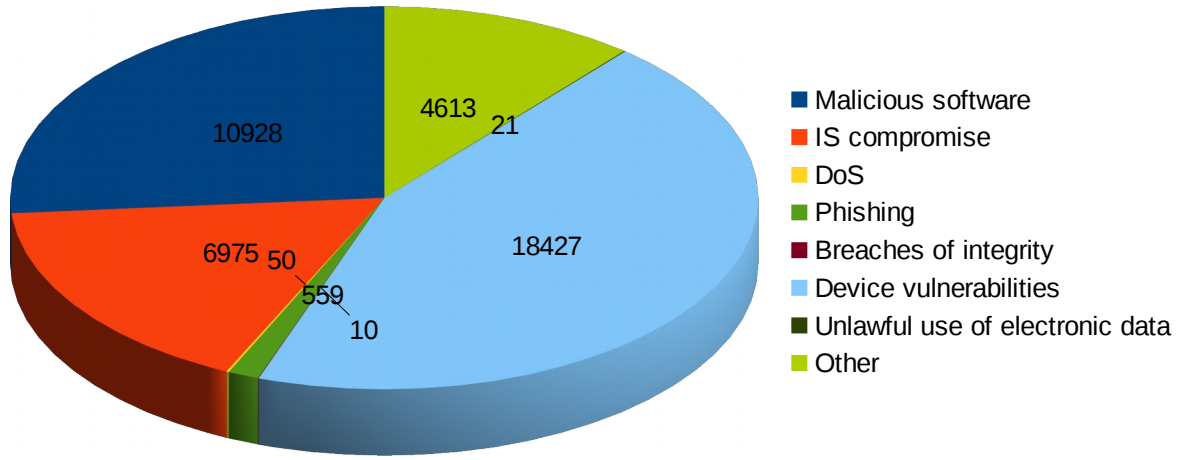

Figure 1. Types of reports received and issued by CERT-LT in 2015

Main cybersecurity issues

Major cybersecurity problem in Lithuania (18,427 reports in 2015) was privately owned devices (e.g. routers) with security vulnerabilities. It should be noted that usually such vulnerabilities do not pose a direct threat to the safety of the data of device owners; however, they facilitate malicious use of such devices in distributed reflection denial of service (DRDoS) attacks.

Many incidents related to the use of malicious software were identified in 2015. CERT-LT investigated 10,928 cases of malicious software use (11,276 in 2014). One of the goals of development and distribution of viruses is inclusion of computers into botnets. Owners of the computers may be unaware of inclusion of their machines into a botnet for a long time (a computer basically continues to operate normally with occasional slowing of Internet connection). Another common goal was money extortion by distribution of ransomware (encrypting viruses demanding for ransom). Antivirus software has the heuristic analysers which detect malicious code in the affected computer by analysing the behaviour of the code even when it is not included into the antivirus software database. However, it should be noted that it could take a certain period of time for antivirus software to recognise a new malicious code.

In 2015, a spam message spread on the Internet urging to open a PDF file which was supposedly an invoice. The link usually contained a ZIP file with the virus EXE file. CERT-LT reminds that attachments to any email should be treated with caution (e.g. they can be checked on the site www.virustotal.com before opening). Email attachments from unknown senders should not be opened.

Malicious software is closely related to the botnets which are used for cyberattacks: distribution of malicious code and spam, denial-of-service attacks, etc. According to the data of CERT-LT, about 2,500 computers, remotely used without the knowledge of their owners, were identified daily in Lithuania in 2015. The website https://www.cert.lt/en/stats_botnets.html registers and publishes information on activity level of computers detected in the botnets.

In order to reduce the probability of virus infection of a computer, users should observe basic “hygiene” when using a computer and Internet since this significantly reduces safety risks. For instance, do not click on suspicious links, do not open unknown files received by email, via “Skype”, etc. It is obligatory to install antivirus software, make back-up copies, and use complex passwords.

Threats for the websites

Malicious code “Stealrat” was active throughout 2015. Such malicious code searches for unsafe websites and security vulnerabilities in content management systems and seeks to exploit them. This is followed by creation of botnets and sending of spam from compromised servers which attempt to include other computers into the botnet, as well as to distribute malicious code from such websites. In the identified cases CERT-LT provided recommendations to the owners of the websites and hosting companies on removal of this code.

In addition to “Stealrat”, there were other cases of malicious code compromising vulnerable websites (e.g. “Angler”). The total number of server compromise incidents in 2015 was 6,975 (4,853 cases in 2014). Analysis data showed that most of the detected compromise cases had been committed by the automated means, employing botnets, inserting malicious code into poorly protected websites, usually exploiting security gaps of outdated content management systems.

In 2015, CERT-LT investigated 559 phishing reports (630 reports in 2014). Malicious developers establish fake websites either to obtain online account details or to make profit of such data. The most reports involve fake websites of electronic payment systems: usually “Paypal”, as well as “Facebook”, “Gmail”, “Yahoo”, and “VK.com”. CERT-LT provides notifications on fake websites to Lithuanian and foreign Internet service providers, international partners and administrators of servers, hosting such sites. All detected fake websites were eliminated.

In order to reduce the threat of system compromise, owners of websites should take care of security issues: they should secure website administration panel, use complex access password and change it constantly, install updates of content management systems and plug-ins. Use of plug-ins without special need is discouraged. Website developers who install popular content management systems (“Wordpress”, “Joomla” and similar) should also take care of their proper configuration.

Incidents of other types

CERT-LT investigated 50 reports on denial-of-service attacks in 2015. 165 reports were investigated in 2014. Such attacks are usually automated by using botnet resources or exploiting vulnerable devices (e.g. vulnerability in SSDP protocol). In order to stop the ongoing DoS attacks, CERT-LT gave recommendations to website owners or companies providing electronic information hosting services on how to stop such attacks and coordinated actions with Internet service providers and CERTs operating in other countries.

There were also 10 reports on breach of integrity (including 2 cases sufficiently significant to be reported to European Union Agency for Network and Information Security ENISA), 21 cases of unlawful use of electronic data and 4,613 incidents of various nature. In conclusion, we provide a summary of cyberincidents registered by CERT-LT during the period from 2009 to 2015.

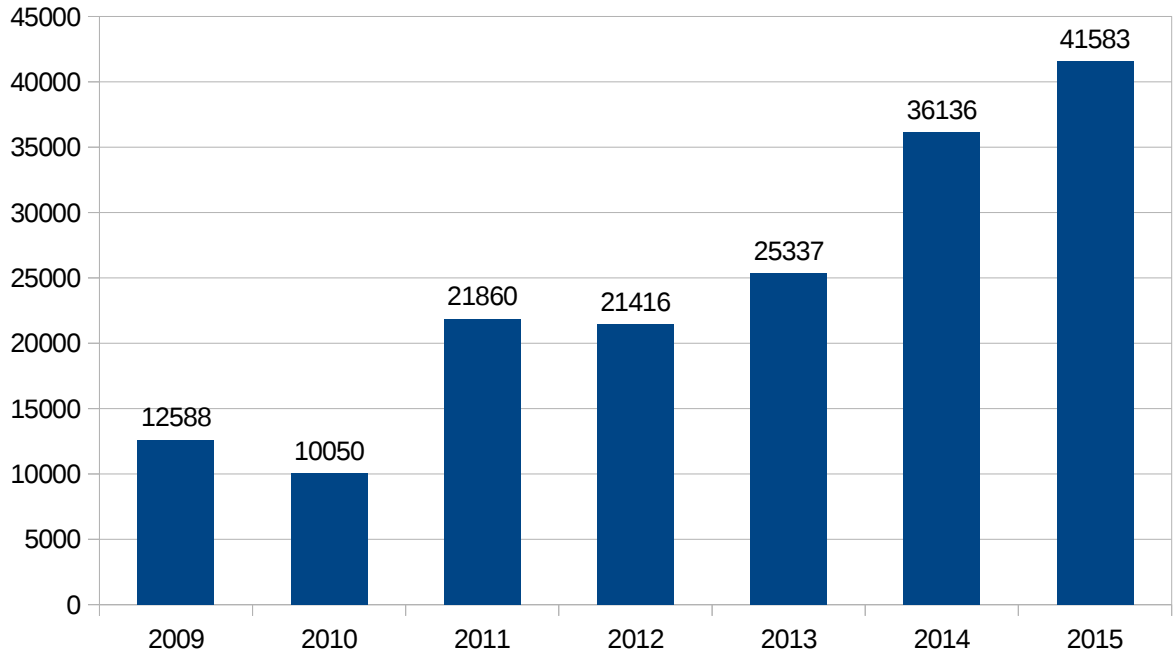

Figure 2. Summary of incidents processed by CERT-LT in 2009-2015

New requirements for Internet service and web hosting providers

In June 2015, the new edition of the Rules on the Ensurance of Security and Integrity of Public Communications Networks, Public Electronic Communications Services and Electronic Information Hosting Services was approved. The Rules establish requirements for combating the most pressing cybersecurity issues in the networks: IP address spoofing and denial-of-service attacks. The main change in the Rules is related to the implementation of provisions of the Law on Cybersecurity, according to which for the first time Lithuanian providers of electronic information hosting services are given the rights and obligations for ensuring proper security and integrity of their services. Read more at:
https://www.cert.lt/doc/Rules_on_the_Ensurance_of_the_Security_and_Integrity.pdf

Cooperation, notification

On 27 February and 4 June 2015, CERT-LT organized the meetings with Internet service providers on improving of efficiency of network security. Meetings included briefing on the present situation, discussions on obstacles to combating security vulnerabilities of devices (e.g. home routers), analysis of suggestions and experience of providers. In 2016, CERT-LT will continue cooperation with Internet service providers and encourage users to take care of security of their network equipment.

An important aspect of the activity of CERT-LT is the exchange of cybersecurity information. Increasingly efficient technical means of automated information processing and distribution are being used and developed. Figure 3 presents 5 main recipients and senders of security notifications in Lithuania.

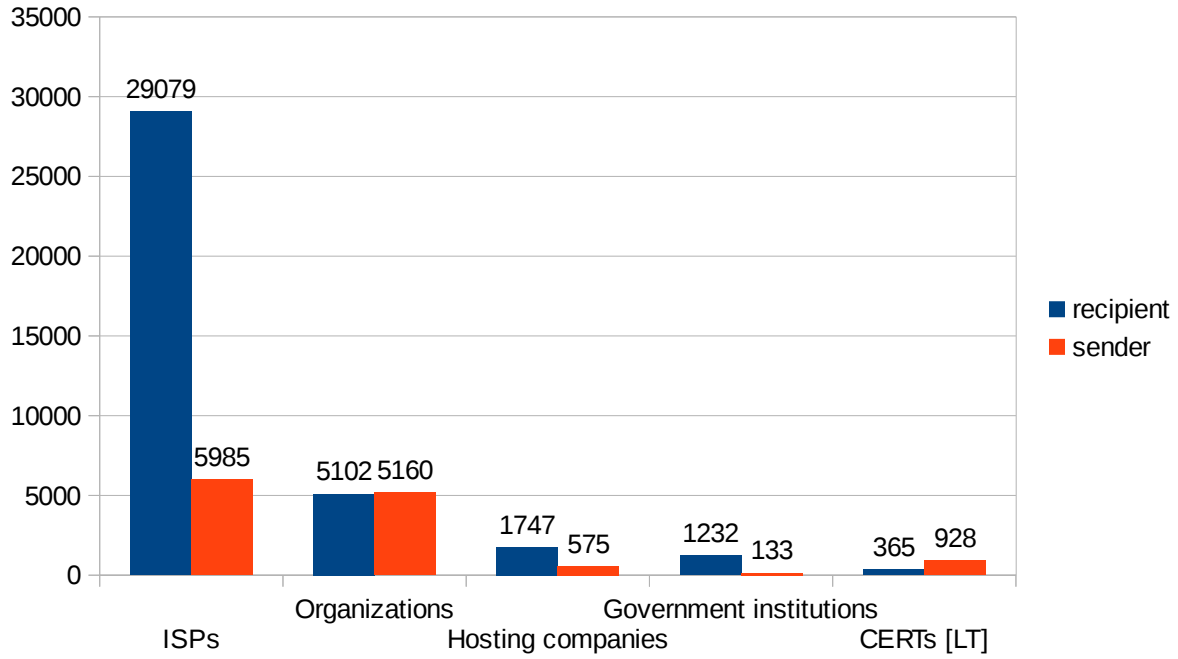

Figure 3. Main recipients and senders of security notifications of CERT-LT in 2015

Much important information is presented by CERT-LT on its website. The updated mobile-friendly website www.cert.lt/en/ which is also accessible via IPv6 protocol allows the following:

1) reading the IT security-related news;
2) review of summarized statistics (both charts and reports);
3) learning the main objectives of CERT-LT;
4) familiarizing with legislation, regulating security in public communications networks;
5) using inspection tools (e.g. for checking if a network device uses the vulnerable UPnP 1.0 protocol, a computer is not involved in activity of a botnet or the current IP address is not identified in the CERT-LT database as taking part in malicious activities, etc.).

Users who face network or data security problems are advised to contact their Internet service provider immediately, and if the provider is unable to solve the problems, users should notify CERT-LT by filling in the form at the website www.cert.lt/en/report.html. More online security-related information for internet users is available on the website www.esaugumas.lt (in Lithuanian only).

CERT-LT also provides cybersecurity-related notifications and short cybersecurity news on “Twitter”. If you wish to learn about IT security issues, follow us on twitter.com/cert_lt.