COMPUTER EMERGENCY RESPONSE TEAM (CERT-LT) OF
THE NETWORK AND INFORMATION SECURITY DEPARTMENT OF
THE COMMUNICATIONS REGULATORY AUTHORITY OF
THE REPUBLIC OF LITHUANIA

COMPUTER EMERGENCY RESPONSE TEAM (CERT-LT)
ANNUAL ACTIVITY REPORT FOR 2014

Feb 2015 No. LD
Vilnius

The National Electronic Communication Networks and Information Security Computer Emergency Response Team (CERT-LT) of the Republic of Lithuania summarizes its activity results for 2014. In 2014 CERT-LT investigated 36,136 incidents on reports received from Lithuanian electronic communications service providers, foreign CERT services engaged in the investigation of international incidents, and Lithuanian internet users. Compared to 2013 (25,337 reports), the number of reports received increased by 43 per cent. Summaries of investigated reports are presented in Table 1 and Figure 1.

Table 1. Reports by type investigated by CERT-LT in 2014

Type of incident	Quarters of 2014				
	Q1	Q2	Q3	Q4	Total
Malicious software	2 820	2 412	2 807	3 237	11 276
System compromise	1836	526	1 122	1 369	4 853
Denial of service	43	35	45	42	165
Phishing	121	81	220	208	630
Breach of integrity	19	11	5	0	35
Device security vulnerabilities	1 673	3 310	3 647	5 197	13 827
Illegal use of electronic data	13	5	8	6	32
Other	850	993	1 712	1 763	5 318

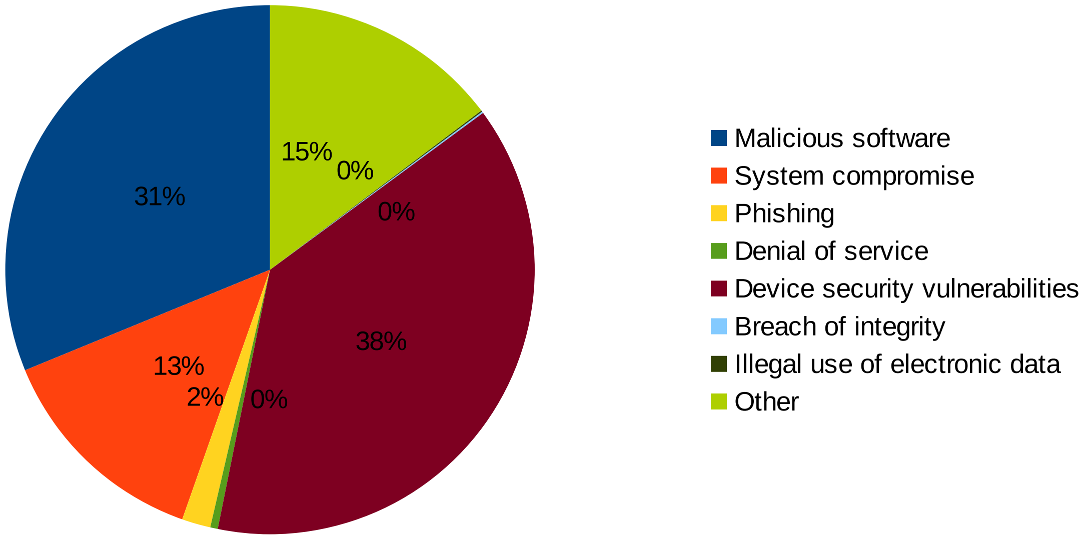

Figure 1. Types of reports received and issued by CERT-LT in 2014

A major cybersecurity problem for Lithuania (13,827 reports in 2014) was and is still presented by mostly privately owned devices with security vulnerabilities. It should be noted that usually such vulnerabilities do not present a direct threat to the safety of the data of device owners; however, they facilitate malicious use of such devices as distributed denial-of-service (DDoS) attack amplifiers.

In 2014 CERT-LT organized meetings with internet service providers to present the current status on security vulnerabilities in network devices, discuss barriers in fighting security vulnerabilities, analyse suggestions and experience of the providers. In 2015 CERT-LT aims to step up the fight against device vulnerabilities: there are plans for more active cooperation with internet service providers, expansion of educational activities by encouraging user to take care of security of their network devices.

As in 2013, many malicious software related incidents were identified in 2014. CERT-LT investigated 11,276 cases of use of malicious software (11,125 in 2013). The usual use of malicious software was for including user computers into botnets. Computer owners can remain long unaware of inclusion of their machine into a botnet (the computer basically continues to operate normally with occasional slowing of internet connection). Antivirus software has the so-called heuristic engines (aimed at detecting malicious code even when it is absent from the antivirus software database by analysing the behaviours of the code if it were to be executed). However, CERT-LT notes that it is usual for antivirus software to recognise malicious code only after a few days (e.g. as in the case with “Geodo” and “Feodo” viruses). Virus developers are expected to be even more active in creating malicious code for smartphones and tablet computers in 2015.

In 2014 CERT-LT investigated 165 reports of denial-of-service (DoS) attacks. Compared to 2013 (130 reports), the number of reports increased by 27 per cent. Such attacks are usually automated by using botnet resources. 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, it coordinated actions with Internet service providers and CERTs operating in other countries.

A major threat is presented by botnets used for criminal activities: distribution of malicious code and spam, denial-of-service attacks, etc. According to data of CERT-LT, an average of 2,000 computers, remotely used without the knowledge of their owners, were identified daily in Lithuania in 2014. In December 2014 a number of such computers identified daily decreased to approximately 1,500. The reduction of this number was due to new incident management measures implemented by CERT-LT.

It is expected that in 2015 the number of devices included in botnets in Lithuania will fluctuate significantly due to:

1) detection of software vulnerabilities (it is easier to address the detected and publically known vulnerabilities);

2) activity of people developing malicious software;

3) behaviour and awareness of internet users (caution, installation of software updates, etc.).

In 2014 high activity of the “GameOver ZeuS” botnet was witnessed. In early summer CERT-LT and partners identified more than 2,000 Lithuanian IP addresses involved in activity of this botnet. At the end of 2014 a number of “members” of this botnet was reduced to approximately 80 by effort of CERT-LT. CERT-LT registers and publishes information on activity level of computers detected in botnets on its internet site https://www.cert.lt/botnet.

Dozens of internet sites operating on Lithuanian servers in 2014 were infected by malicious code “Stealrat” due to possible vulnerabilities of content management systems. This code creates botnets and uses the controlled computers to send spam which aims to include other computers into the botnet. In the identified cases CERT-LT provided recommendations to the owners of the sites and hosting companies on removal of this code, which reduced the number of such sites to single digits.

Since mid-2014 a spam messages spread on the internet urging to open a file, which was supposedly an invoice, sent by a mobile carrier or other company. The link to a PDF file usually contained a ZIP file with the virus EXE file, which on the initial days was recognised by just a few antivirus programmes. The emails were sent by computers involved in “Geodo” botnet. “Geodo” uses the same infrastructure of infected computers and method of spreading as its predecessor “Feodo”. CERT-LT wishes to remind that even when the email is received from a reliable source, attachments should be treated with caution (e.g. they can be checked on sites www.cert.lt/antivirus/ or www.virustotal.com). Opening email attachments from unknown senders is not recommended.

In 2014 CERT-LT investigated 630 phishing reports (558 reports in 2013). Malicious developers are establishing fake websites either to obtain online account details or to make profit of such data. Every week there are reports on fake online payment service sites (usually “Paypal”). Reports on fake “Facebook”, “Gmail”, “Yahoo” and “VK.com” internet sites are also frequent. In late 2014 increased appearances of fake websites of police and Interpol were observed. The later fake website is dangerous in that it operates in a way to make it difficult for the user to close the browser window, thus, it appears that the computer has been “blocked”. CERT-LT provides notifications on fake websites to Lithuanian and foreign internet service providers, international partners and administrators of servers, hosting such sites. It should be noted that such fakes were eliminated rather quickly due to swift actions on part of CERT-LT.

Cases of compromised information systems have more than halved. There were 10,924 of such incidents in 2013. As a result of active steps taken by CERT-LT, the number of cases of system compromisation was reduced to 4,853 in 2014. Investigation data show that most of the identified cases of compromisation were carried out by automated means via botnets by inserting a malicious code into poorly secured websites.

A significant achievement was the international cyber training “X14” organised by CERT-LT in September 2014. That was the second CERT-LT organised training in Lithuania which was joined by four EU member states. The training was aimed at checking the effectiveness of inter-institutional cooperation, ability to find contacts of responsible representatives of relevant institutions in critical situations and respond to cyber incidents. The training included testing of skills to quickly exchange information during possible cyber incidents, readiness to use easily available encryption means for data transmission via public networks, competence of institutional IT administrators to perform simple tasks, for example, conduct a quick automated event log analysis. The training involved 25 state institutions of Lithuania, 8 banks, 5 national security incident investigation CERT groups (of Lithuania, Latvia, Ukraine, Bulgaria and Romania) and 5 CERT groups of Lithuania (LITNET, SVDPT, Ministry of National Defence, TEO LT and NRD CERT).

An important factor of operation of CERT-LT is exchange of cyber security related information via communication technologies. It should be noted that in 2014 CERT-LT provided 241 consultations to residents and public bodies of Lithuania. Figure 2 includes 5 major recipients and senders of messages.

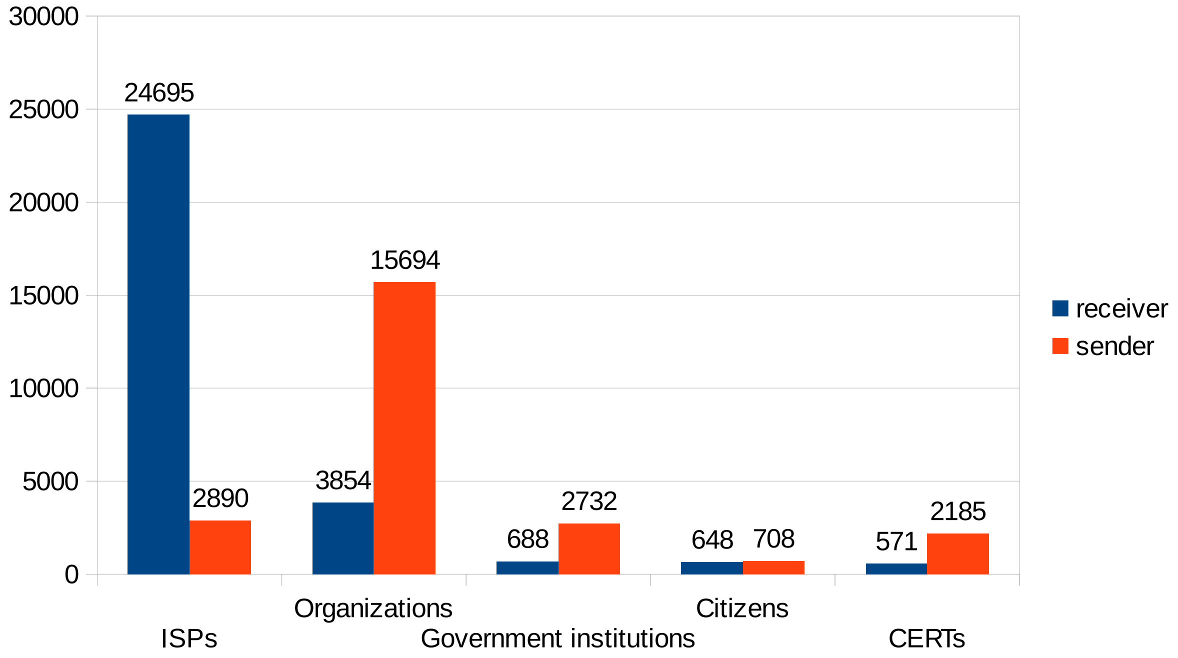

Figure 2. Major recipients and senders of messages of CERT-LT in 2014

The website www.cert.lt which is also accessible via IPv6 protocol, allows the following:

1) reading IT security related news
2) viewing statistics for a long period of time (both charts and reports)
3) learning the main objectives of CERT-LT
4) familiarizing with legislation, regulating security in public communications networks
5) using one of 6 tools (e.g. for checking if a network device does not use the vulnerable UPnP 1.0 protocol or whether a computer is not involved in activity of a botnet, or if the current IP address is not identified in the CERT-LT database as taking part in malicious activities, etc.).

Users who have faced network or data security problems are advised to contact their internet service provider immediately and if the provider is unable to solve such problems, it is necessary to notify CERT-LT by filling in the form at the website www.cert.lt/pranesti. More online security related information for Lithuanian internet users is available at www.esaugumas.lt.

To conclude, here is the summary of reports processed by CERT-LT from 2009 to 2014.

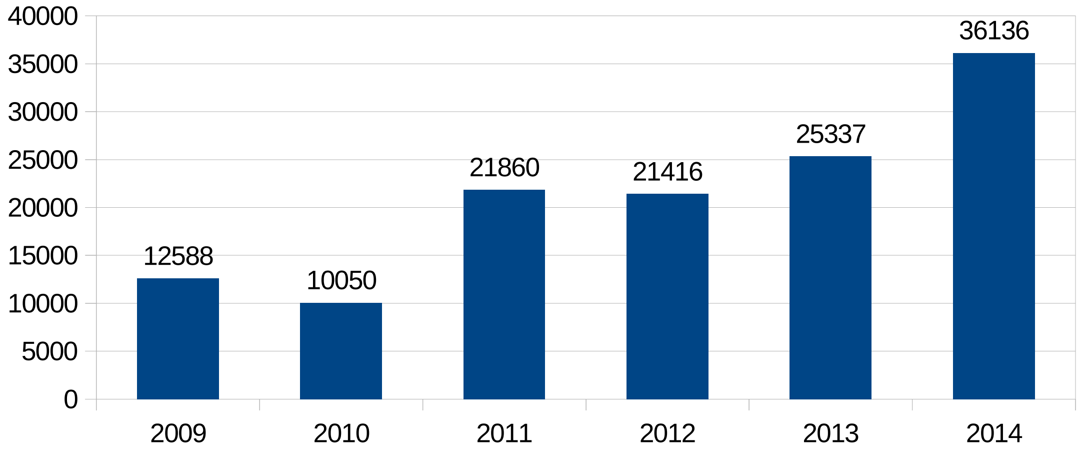

Figure 3. Summary of reports processed by CERT-LT from 2009 to 2014

Head of Computer Emergency Response Team (CERT-LT) Mindaugas Razbadauskas

Prepared by Arnoldas Judinas

Feb 2015