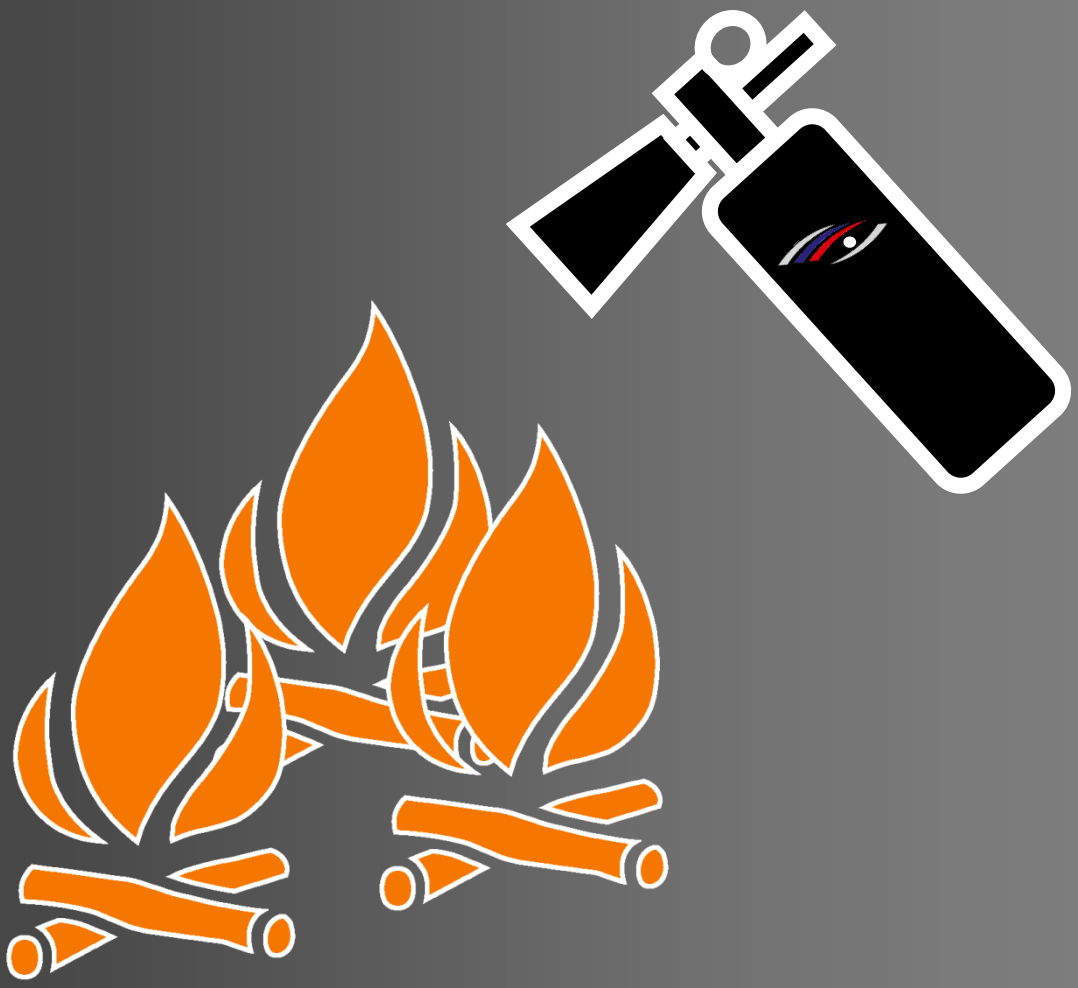
CSIRT.SK

CSIRT.SK
SECURITY ANNUAL REPORT
2014

Table of Contents



CSIRT.SK PERFORMS TASKS RELATED TO ITS FUNCTION AS THE NATIONAL POINT OF CONTACT FOR REPORTING COMPUTER SECURITY INCIDENTS

1. INTRODUCTION

This document presents selected statistics of computer security incidents that were dealt with by the CSIRT.SK specialised unit in the year 2014. The document maps attacks and security incidents that were observed in IP address space of the Slovak Republic and had an impact on its security. It contains information obtained by CSIRT.SK and also data from different sources, particularly from foreign partners. Purpose of this document is to provide readers with a picture of Slovak address space in terms of threats that have been observed, as well as to inform about events during the year 2014.

2. CSIRT.SK – SPECIALISED UNIT

Specialised unit CSIRT.SK (Computer Security Incident Response Team Slovakia) was established by the Ministry of Finance of the Slovak Republic to promote protection of national information and communication infrastructure ("NICI") and of critical information infrastructure ("CII").

CSIRT.SK performs tasks associated with responding to computer security incidents within public administration information systems as well as tasks related to its function as a single point of contact for receiving reports from abroad and coordinating incident handling process on national level.

In the Slovak Republic, CSIRT.SK performs tasks defined by Government Resolution No. 479/2009 and provides its constituency - public administration institutions with:

a) Active services – response to ongoing computer security incidents, their analysis, design of countermeasures, and cooperation with foreign entities during remediation of their impacts.
b) Proactive services – prevention of computer security incidents (publishing warnings about threats, penetration testing, consulting, providing audits, educational and training activities, exercises on critical information infrastructure protection, security monitoring, etc.).

3. RESPONDING TO SECURITY INCIDENTS

Within its active services, CSIRT.SK received notifications of security incidents and provided incident response to them or coordinated their handling on national level where necessary. Incident reports mostly originated from:

- Attacked institutions from the Slovak Republic and abroad (governmental organisations, financial institutions, Internet service providers, etc.);
- CSIRT/CERT teams;
- Security forces and law enforcement agencies in Slovakia and abroad;
- Monitoring systems for security incident detection in infrastructure, commercial, governmental and academic entities in Slovakia and abroad (detection of botnets, websites with deliberate alteration of the contents – so-called "defacement", websites involving unauthorised acquisition of information (so-called "phishing"), malicious code, etc.).

Incident reports can be filed by e-mail or telephone. All information on how to report a computer security incident is available on following websites:

- https://www.csirt.gov.sk/contact-821.html,
- https://www.csirt.gov.sk/incident-report-86c.html.

Reports received are divided into two categories according to their severity:

1. **Significant security incidents**, including:
   - Threatened functionality/availability of a public administration information system or critical infrastructure;
   - Possible leakage of sensitive information;
   - Possible occurrence of financial loss; or
   - Possible damage to reputation of the Slovak Republic.
2. **Bulk-processed security incidents**, such as:
   - Suspicion of malicious activity from the IP address space of the Slovak Republic;
   - Suspicion of website content modification;
   - Vulnerabilities in information systems.

THANKS TO CLOSE COOPERATION WITH LOCAL AND FOREIGN PARTNERS, CSIRT.SK HELPS TO INCREASE SECURITY IN SLOVAK REGION

CSIRT.SK responds to significant incidents directly in cooperation with the operator of an affected asset. A presentation of different types of serious malicious activity is shown in Chart 1.

In addition to information about the incident alone, CSIRT.SK always provides suggestions of countermeasures to prevent the occurrence of such an incident and also proposes countermeasures to mitigate the impact of already occurred incident.

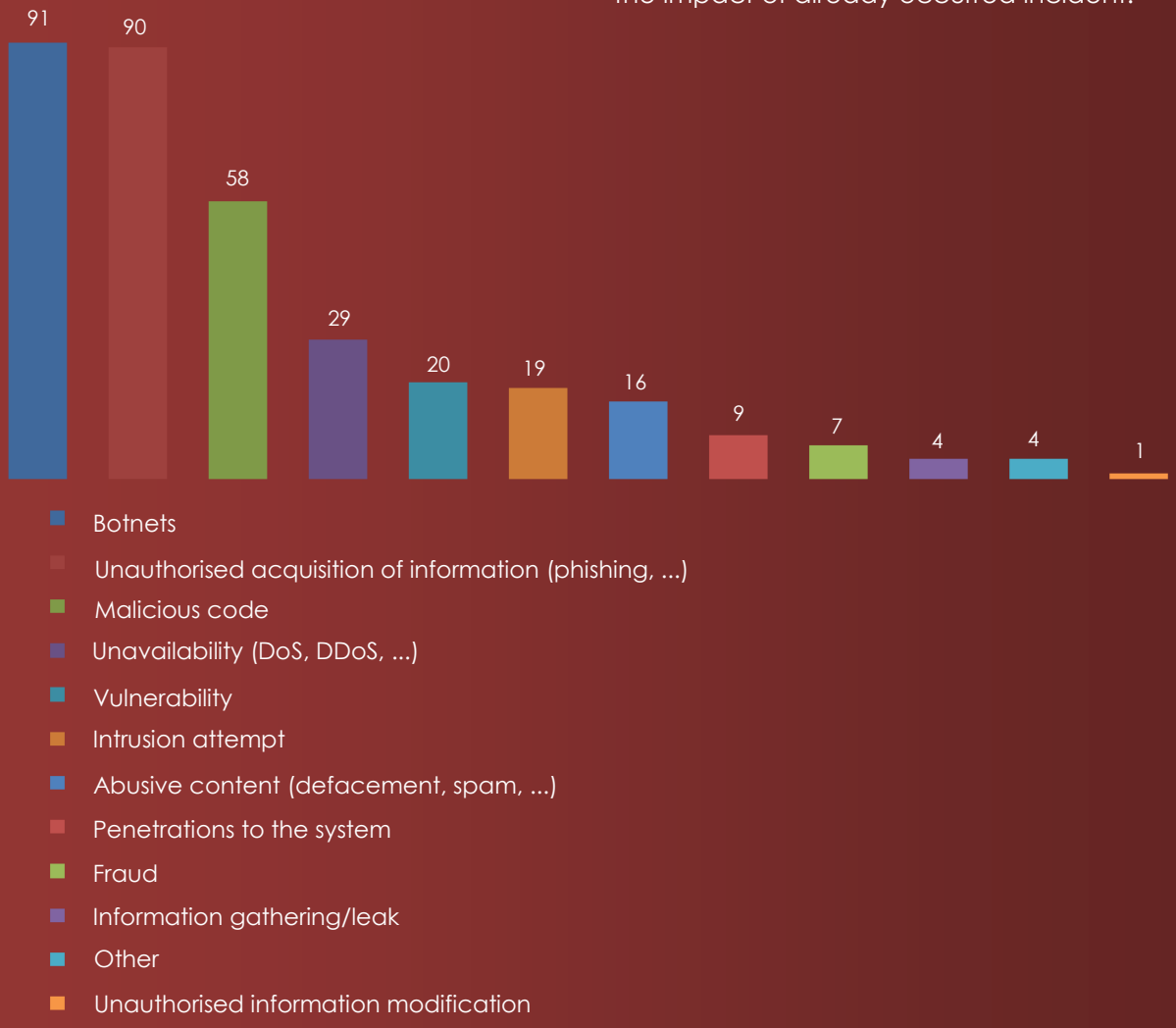


Chart 1 Types and amount of significant security incidents reported in the IP address space of the Slovak Republic for the year 2014

In the period from 1st January and to 30th June 2014, CSIRT.SK received more than two million reports of possible malicious activities occurrence in IP address range of the Slovak Republic. At the end of the year 2014 it was more than six million reports. The "open resolver" vulnerability causing unavailability of DNS servers or deploying vulnerable servers in DDoS attacks was the most frequent of all reported incidents. In addition to this vulnerability, the most common type of reported malicious activity was bot, which means the occurrence of malware on different types of devices.

In the first half of the year, 230,296 unique IP addresses were identified with suspected presence of harmful activity. In the second half of the year, 235,969 unique IP addresses were identified. The number of IP addresses does not correspond to the number of attacked devices, as one public IP address may be used by a larger number of devices. Also, the addresses use to be allocated dynamically and one client can communicate sequentially from different public IP addresses.

BOT, SCANNER, AND SPAM SENDER – NOWADAYS A "MANDATORY" FUNCTIONALITY OF ANY INFECTED SERVER

According to the incident type, the following occurred most commonly at IP addresses identified by CSIRT.SK:

- "Open resolver" vulnerability (over 173,000 IP addresses)
- Bot-type infection (over 111,000 IP addresses)
- Zeus and Citadel banking Trojan horses (more than 4,300 IP addresses)

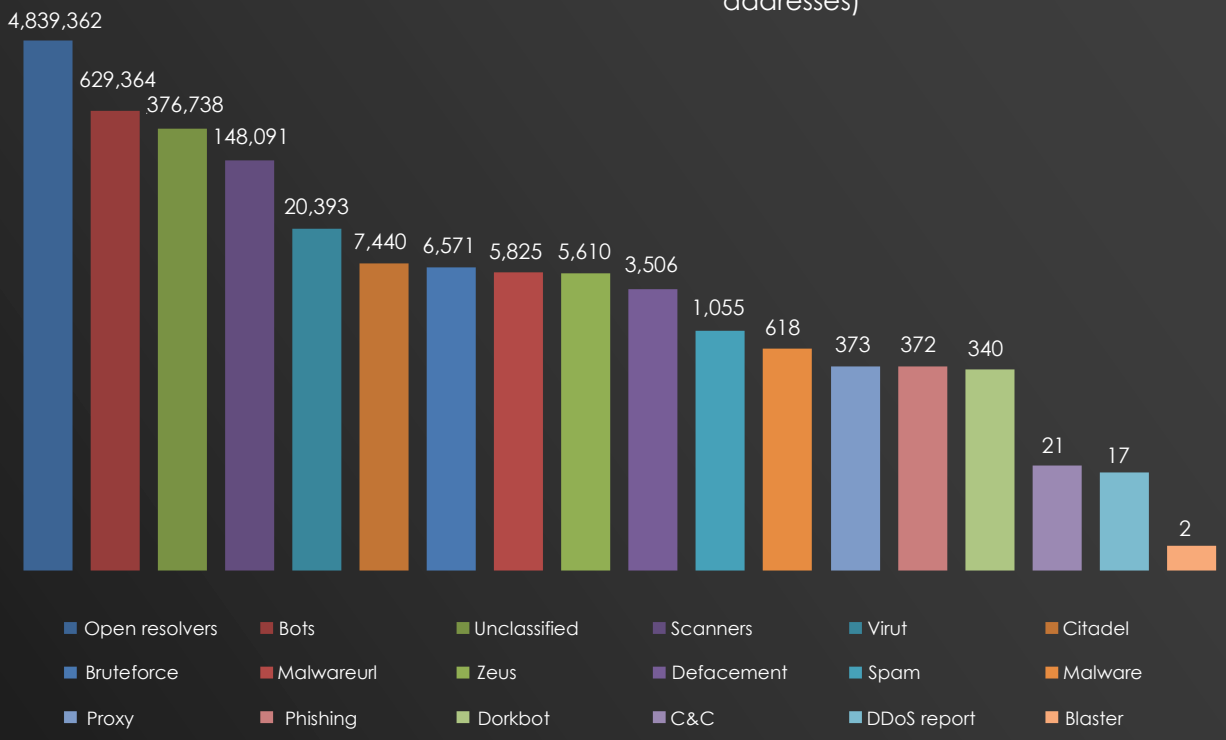


Chart 2 Types and amount of bulk-processed incidents reported in the IP address space of the Slovak Republic in the year 2014

4. TRENDS

Global trends in information security are also reflected in the Slovak Republic. In recent years, namely from 2011 to 2014, we can observe a growing number of occurrences and also instances of actual detection of serious security incidents that have been addressed by the specialised unit CSIRT.SK. During the monitoring period, we observed an increased number of attempts to break into information systems as well as an increase of phishing attacks.

The aim of the attacker is to gain control over the victim's devices and, through them, carry out various harmful activities. Servers are not being infected with just one, but with entire sets of malicious code.

An example of a device infected in this manner is a server that is part of an extensive botnet network and is also infected with malicious code scanning attacker-selected IP range of potential victims, and dispatching spam from the victim's server. Therefore CSIRT.SK always requests a thorough verification of malicious code occurrence on affected devices. In this area, CSIRT.SK also conducts activities to raise awareness of this issue.

Graphical representation of the amount of significant incidents in years 2013 and 2014 is shown in Chart 3.

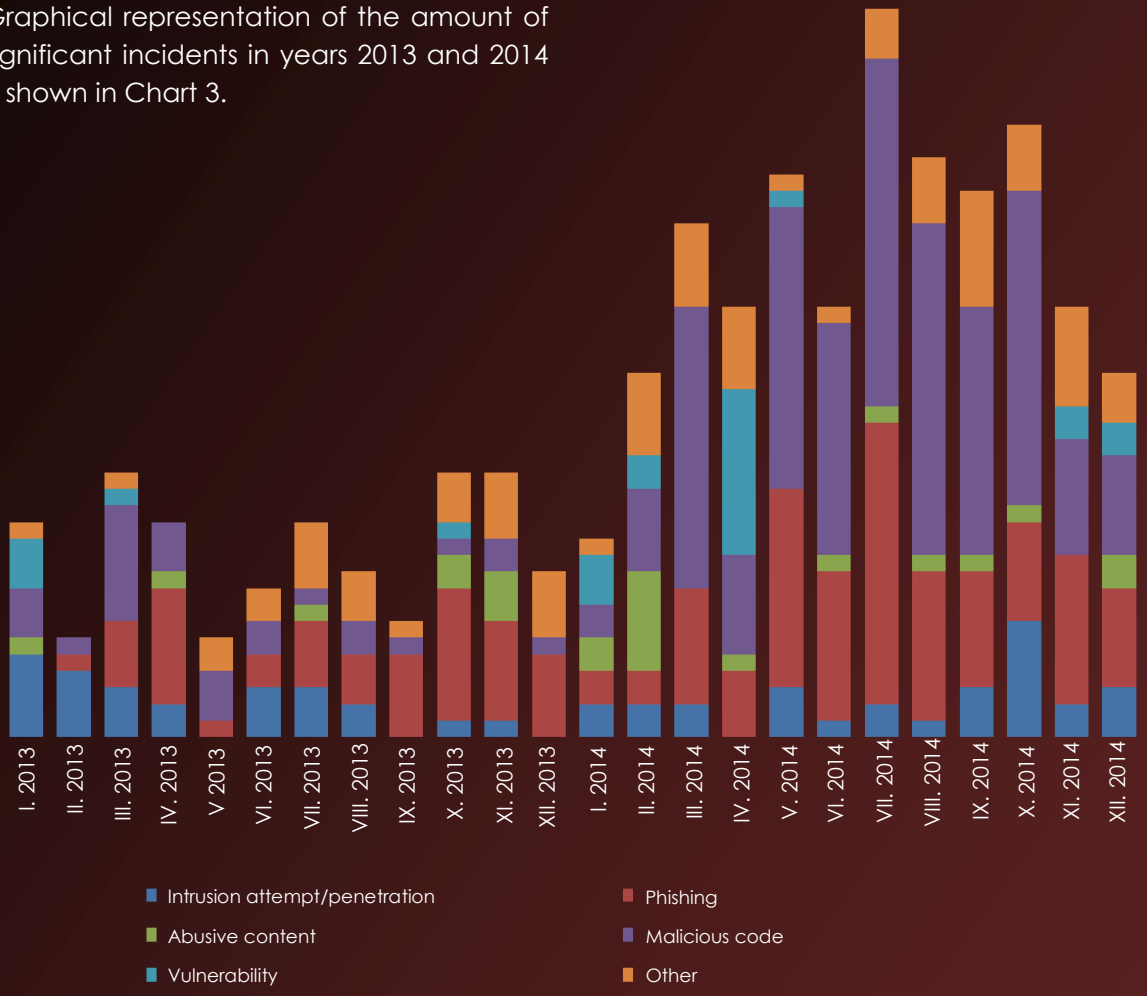


Chart 3 Amount of serious incidents by type from 1 January 2013 to 31 December 2014

The occurrence of various types of malicious activities in the Internet is shown in Chart 4. This chart summarises the operation of security devices in a small network at the point of connection to the Internet for a time interval of 72 hours.

Based on the evaluated data, it can be seen that each publicly accessible IP address (or network) is scanned by automated tools for open ports, i.e. services that are accessible from the Internet. These scans are often performed by infected devices without the knowledge of their owner, i.e. by devices that may be part of botnet networks.

By request of foreign partners in cooperation with affected server operators in Slovakia, CSIRT.SK successfully mediated the disconnection of several command and control (C&C) servers.

The blocks of IP addresses reserved for the Slovak Republic contain a total of 2,447,616 unique public IP addresses (http://www.nirsoft.net/countryip/sk.html).

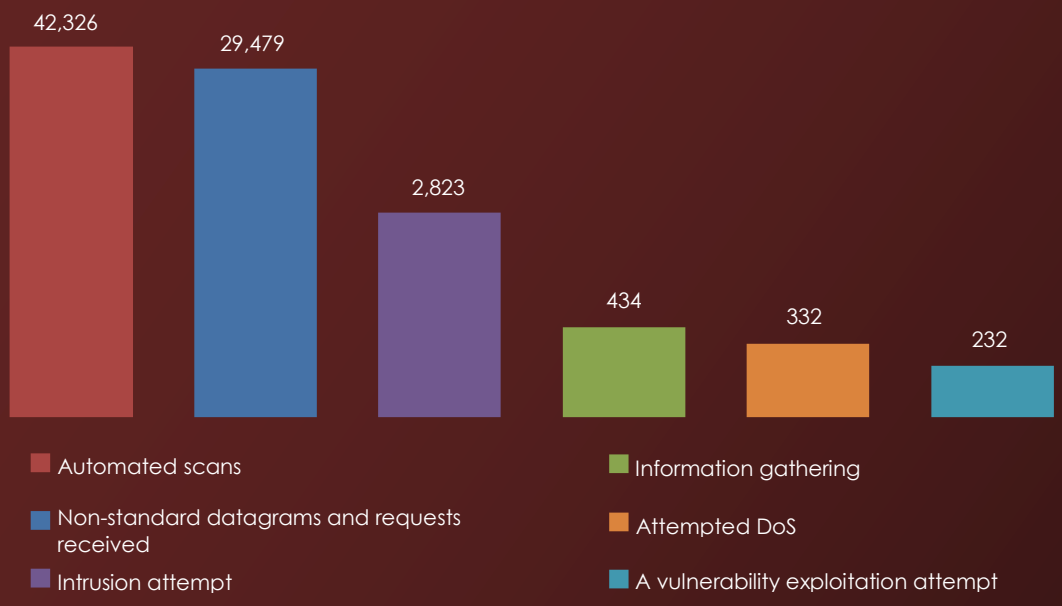


Chart 4 Sample of malicious activity observed during 72 hours

IN OUR ESTIMATION, AT LEAST 6% OF WORKSTATIONS IN THE SLOVAK REPUBLIC IS INFECTED WITH MALICIOUS CODE

Based on reports of possible occurrence of malicious activities in Slovak IP address range (Chart 2) it can be assumed that at least 100,000 to 150,000 devices in the Slovak Republic are infected with malicious code, representing at least 6 percent of all workstations in the Slovakia[1].

These devices represent a security risk to users, especially when used to perform internet banking operations, online shopping, eGovernment services, etc.

[1] If we consider that one IP address is equivalent to one workstation, i.e. disregarding network address translation (NAT), as statistics on the use of NAT are not available. The number is probably higher because not all addresses are occupied.

TENS OF THOUSANDS OF DEVICES IN SLOVAKIA ASSIST ATTACKERS IN DDOS ATTACKS WITHOUT KNOWLEDGE OF THEIR OWNERS

CSIRT.SK also observed an increased number of phishing e-mail messages in public administration environment, some of which are part of targeted attacks on these institutions. Such e-mails are often attached with or linked to a malicious code to obtain login credentials. Usually, the main objective of malicious code is to create a backdoor into a network or a system for an attacker, causing data leakage or gaining control over a device and involving it in a botnet network.

Attackers use methods of social engineering, phishing messages, and malicious e-mail messages to infect target device. The infection is then initiated by execution of malicious code contained in an attachment or by accessing compromised website (drive-by download) using a fraudulent link. Unless a zero-day exploit is used, an outdated software (operating system, antivirus software, web browsers, office suites, etc.) that is installed on a workstation with weak security (accounts without passwords, default accounts, eventually all users with administrator privileges) is an important factor.

THE AMOUNT AND QUALITY OF PHISHING SITES TARGETED ON SPECIFIC COUNTRIES IS INCREASING

Phishing sites that demand login information into various information systems did not focus on the employees of the public administration only. Often it was a phishing site designed to trick the user to enter login information into web and banking services such as Internet banking, PayPal, Facebook, or various services from Google which are used by many Slovak citizens. Majority of this kind of reported sites were operated in the region of Slovak Republic. In cooperation with operators of affected web servers, such fraudulent phishing sites were continuously removed.

THE VAST MAJORITY OF OBSERVED INCIDENTS WAS CAUSED BY IGNORING BASIC SECURITY RULES

It is a fact that the number of targeted phishing sites is constantly increasing. This involves sites that appear normal even after routine inspection by the operator or owner of the server. These sites display malicious phishing content instead of standard content only after connecting from the target country of interest (e.g. Brazil, France, or Spain).

An increasingly common type of attack on the organisation's infrastructure is DDoS attack. Attackers try to limit the availability of electronic services of the target device through resource consumption, line overload, or by disabling the device or service. The most common type of DDoS attack was the TCP-SYN flood and DDoS UDP flood over NTP DDoS attacks, involving also IP addresses belong to the address space of the Slovak Republic.

Other interesting attacks that took place in the first half of March 2014 targeted e-mail accounts to exfiltrate login credentials through the POP3 protocol.

ATTACKERS REDIRECT MORE THAN 300,000 INFECTED ROUTERS IN CENTRAL EUROPE TO FRAUDELANT DNS SERVERS

It is estimated that in Central Europe, there are approximately 300,000 infected routers with their DNS communication being redirected to attacker-designated DNS servers. In this context, CSIRT.SK developed a methodology to verify the presence of the respective vulnerability of a device, along with instructions for implementing security measures.

As a conclusion, we list the most common types of malicious code detected in the first half of 2014. These were the Zeus malicious code – a banking trojan that steals login information to Internet banking through the "Man in the Browser" attack, its peer-to-peer variant GameOver Zeus and Ebury - rootkit/backdoor trojan for Linux/Unix operating systems, which collects SSH credentials (username/password) from SSH connections.

Our predictions in the field of computer security for year 2014 has been confirmed by our data. In general, for the year 2015 it can be expected, similarly like for year 2014, that the number of serious security incidents and the resulting threats to eGoverment services, electronic banking services, e-commerce, and other electronic services through infected devices will increase.

5. PROACTIVE SERVICES

Following actions were conducted as part of proactive services in the year 2014: publication of warnings on recent threats, penetration testing and vulnerability evaluation of public administration information systems, security consulting, audits, educational and training activities for the protection of critical information infrastructure, security monitoring, and others.

1st half of 2014

Penetration testing

Free of charge penetration tests of information systems and web portal vulnerability evaluation for public administration institutions are important part of proactive services provided by CSIRT.SK. These tests identify critical vulnerabilities that can be exploited by attackers to threaten the functionality and security of systems. Countermeasures to eliminate such vulnerabilities are drafted as part of the procedure. Tests conducted by the specialised unit CSIRT.SK significantly reduce costs that would have to be covered by the state budget to carry out such tests by external entities.

Consulting

For institutions that do not have sufficient professional capacity, the unit provides professional consultation services related to securing organisation's infrastructure. The unit also provides information security audits to verify compliance with security standards defined by Decree of the Ministry of Finance No. 55/2014 on Standards for Public Administration Information Systems (PAIS) or the International Standard ISO/IEC 27001:2013.

Education

To improve security, CSIRT.SK identified the need to raise security awareness of end users. For this reason, CSIRT.SK developed a basic guide to secure a Windows workstation (the vast majority of infected devices currently uses a Windows based operating system). The guide also contains a section on parental control to protect children on the Internet. The manual, available in Slovak language, can be downloaded from CSIRT.SK website: http://www.csirt.gov.sk/informacna-bezpecnost/navody-a-odporucania/ochrana-koncovych-stanic-811.html

Warnings

Proactive services included monitoring of current security situation in digital space of the Slovak Republic and issuing warnings that were distributed either directly to potentially affected institutions or published on our website http://www.csirt.gov.sk/oznamenia-a-varovania-803.html.

CSIRT.SK created a unique contact list of governmental institutions and entities involved in information security issues, including academia, providers of electronic services, and entities in the area of critical infrastructure. These are institutions and entities that CSIRT.SK cooperates with while dealing with specific incidents and threats.

International exercises

In order to increase professional competence in the Slovak Republic, in the first half of 2014, CSIRT.SK actively participated in the first phase of the international exercise CYBER EUROPE 2014[2] - TLEx, which was aimed at verifying the technical level of individual countries and setting processes for crisis management in large-scale security incidents organised within the European Union. Slovak team composed of representatives of CSIRT.SK specialised unit and Slovak Information Service analysts finished 4th in the competition of 214 government, private, and academic teams from all over Europe.

[2] More information is available at http://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today

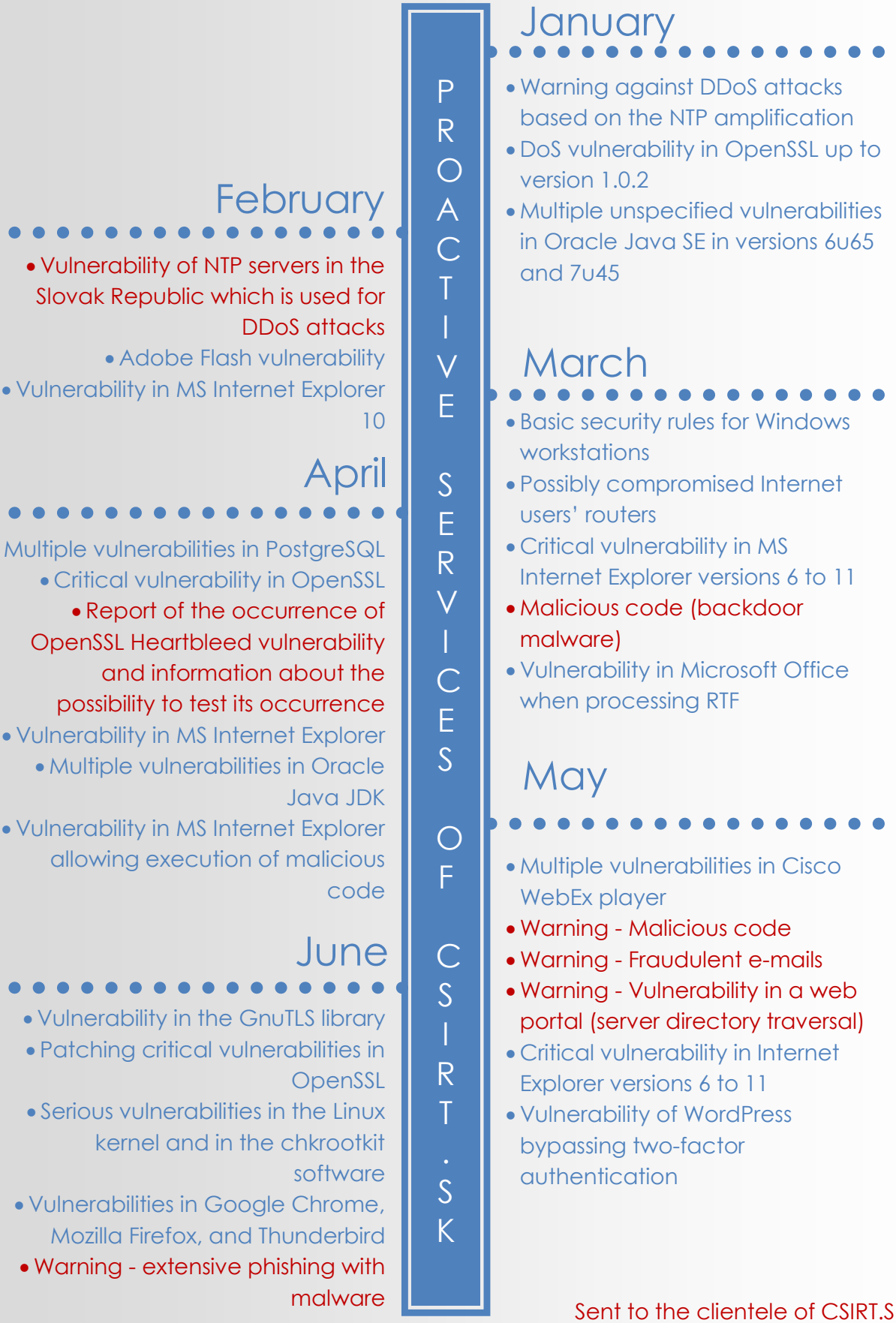


Figure 2 Warnings published by CSIRT.SK

PROACTIVE SERVICES OF CSIRT.SK

July

- Warning – Fraudulent e-mail
- Vulnerability in Linux Kernel
- Vulnerabilities of CISCO IP telephony
- Apache web server vulnerabilities fix
- Malware BlackEnergy - information
- Mozilla Firefox security patches
- 0-day vulnerability of Apple QuickTime

August

- Symantec Endpoint Protection vulnerability fix
- OpenSSL library vulnerabilities fix
- Security updates of Microsoft products
- Cisco NX-OS vulnerability
- Rom-0 vulnerability for ISPs

September

- rsync vulnerability of F5 products allowing full access to the system
- Security patches of Mozilla Firefox and Thunderbird
- Security updates of Microsoft products
- 0-day vulnerability in MS Internet Explorer 11
- Security updates of Adobe Reader and Acrobat
- Warning - Backoff Point -of-Sale malware
- Severe vulnerability Bourne-Again Shell (Bash)

October

- Warning - new wave of malware spread(CosmicDuke)
- Security patches of Google Chrome
- Malware BlackEnergy - update
- Security updates of Microsoft products
- Vulnerability of SSL protocol – Poodle attack
- Indicators of malware campaign Sofacy and BlackEnergy

November

- Warning – vulnerabilities of UPnP devices
- Indicators of malware campaign Vixen Panda/Ke3Chang
- Critical vulnerabilities of Microsoft Windows and Internet Explorer
- Proactive testing of Slovak IPv4 address space to identify the device type vulnerabilities rom-0 and open resolver

December

- Warning - SSL/TLS vulnerabilities on the public administration portals
- Increase in occurrence of fraudulent and malicious e-mails
- Summary of critical vulnerabilities per December 2014

Sent to the clientele of CSIRT.SK
Published on www.csirt.gov.sk

Figure 2 Warnings published by CSIRT.SK (continued)

2nd half of 2014

Penetration testing

Nowadays, the penetration testing is very popular, therefore we were very occupied during the year 2014 as we performed numerous penetration tests for our constituency. In the second half of the year 2014 we have expanded our penetration testing team. Each penetration test gives us a better knowledge about vulnerabilities and threats that may affect our constituency in the future so we are strengthening our preparedness for these risks.

Education & Warnings

To improve security knowledge, CSIRT.SK took part in education programme to improve the preparedness of Police Force staff and investigators in the field of cybercrime. We provided information about latest technology and modern approach based on our experience in the field of computer security.

The threat of malicious activity was present in the Slovak cyberspace in the second half of the year 2014, too. We observed a lot of campaigns that were threatening our constituency, e.g. CosmicDuke, Black- Energy, and Backoff Point-of-Sale malware.

European Cyber Security Month

CSIRT.SK participated in European Cyber Security Month in October. This project is a European Union advocacy campaign which aims to promote cyber security among citizens, to change their perception of cyber-threats and provide up to date security information, through education and sharing good practices.

CSIRT.SK in cooperation with Ministry of Finance of the SR organized following events: cyber security education, publishing a guide to secure a workstation with MS Windows, proactive vulnerability testing for selected vulnerabilities in the IP address space of SR, and malware analysis competition.

International exercises

In the second half of 2014, CSIRT.SK actively participated in the second phase of the international exercise CYBER EUROPE 2014 - OLEx, which was aimed at verifying the operational level of individual countries and setting the processes for crisis management in large-scale security incidents organised within the European Union. More than 200 organisations and 400 cyber-security professionals from 29 European countries were testing their readiness to counter cyber-attacks in a day-long simulation, organised by the European Union Agency for Network and Information Security (ENISA).

CSIRT.SK also participated in another large-scale exercise Cyber Coalition 2014 organised by NATO. NATO[3] launched its largest ever multinational cyber defence exercise on 18 November 2014. The three-day training event tested the Alliance's ability to defend its networks from the various challenges that exist when operating in the contested cyber domain.

The exercise involved over 600 technical, government, and cyber experts from 28 countries. They were operating from dozens of locations from across the Alliance and partner nations. For the first time, representatives from academia and industry have been invited as observers.

This exercise had tested our systems to make sure that skills and expertise of our cyber specialists are fully up to the task.

[3] More information is available at http://www.nato.int/cps/en/natohq/news_114902.htm

Position	Affiliation	Country	Total points	Number of incidents
1	[illegible]	PL	[illegible]	16
2	[illegible]	CZ	[illegible]	16
3	[illegible]	FR	[illegible]	11
4	CSIRT.SK	SK	[illegible]	10
5	[illegible]	HR	[illegible]	10
6	[illegible]	GR	[illegible]	8
7	[illegible]	CZ	[illegible]	9
8	[illegible]	GR	[illegible]	8
9	[illegible]	CZ	[illegible]	9
10	[illegible]	LT	[illegible]	8
11	[illegible]	NO	[illegible]	7
12	[illegible]	FI	[illegible]	9
13	[illegible]	FI	[illegible]	7
14	[illegible]	CH	[illegible]	6

Table 1 Scoreboard ranking the teams in the Cyber Europe 2014 exercise - TLP AMBER

In the first half of 2014, CSIRT.SK actively participated in the regional exercise "Central European Cyber Security Platform 2014[4]", whose aim was to verify the process of joint identification and elimination of computer incidents in V4 countries and Austria.

A TEAM COMPOSED OF REPRESENTATIVES OF CSIRT.SK AND SIS RANKED 4TH IN THE CYBER EUROPE 2014 EXERCISE IN COMPETITION OF 214 TEAMS FROM 29 COUNTRIES OF EU AND EFTA

[4] More information is available at http://www.enisa.europa.eu/media/news-items/central-european-cyber-security-platform-2014

Proactive actions in greater detail

As part of proactive actions, CSIRT.SK sends alerts on the occurrence of vulnerabilities and suspicions of presence of malicious code on devices located in the address space of the Slovak Republic and provides technical support to operators and owners of the affected information systems.

TYPE	DESCRIPTION	MEASURES OF CSIRT.SK
"Open resolver" vulnerability	Open resolver is a vulnerability of DNS servers which allows recursive query from any IP address on the Internet. An attacker can thus cause the server to participate in a DDoS attack on a selected IP address by sending a specific request which causes the server to reply to the selected IP address. The response is significantly larger than the request, which increases traffic to the victim's IP address.	Proactive vulnerability testing of DNS resolvers that belong to institutions of public sector and resolving this vulnerability (depending on the cooperation with the institutions concerned). CSIRT.SK occasionally verifies the presence of this vulnerability on servers in the IP address space of the Slovak Republic and sends notifications to owners of affected devices.
Vulnerability of NTP servers in the Slovak Republic, which is used for DDoS attacks	Through the vulnerability, an attacker can engage servers with active NTP service in a DDoS attack. The attacker sends a special request with fake IP address to the NTP server and the server sends a reply to the fake IP address. The idea of increased traffic is the same as in the case of the "open resolver" vulnerability, but the amplification is even more significant.	According to received report of vulnerabilities identified in Slovak IP address space, 64 warnings to entities managing the vulnerable NTP services were sent. A positive response eliminated later attempts to exploit this vulnerability by attackers.
Vulnerabilities of SOHO routers	Many devices in the SOHO and Small Business router categories (devices in small companies and households) are vulnerable to several types of attacks, for example, default password set by the manufacturer, easy-to-guess passwords, setting up routers in such a way that they are accessible from the external network without authentication, vulnerability in the firmware, or the possibility of modifying DNS server addresses.	CSIRT.SK has notified institutions of public sector and cooperating ISPs about this issue. CSIRT.SK has also created best practices addressing these vulnerabilities, including recommendations for their verification, resolving and mitigation. CSIRT.SK occasionally verifies the presence of rom-0 vulnerability on SOHO routers in the IP address space of SR and notifies owners of affected devices.
Possible presence of bots	Infected devices may perform malicious activities such as stealing of login information, monitoring of user, information leakage, etc. On the Internet it may provide malicious files and phishing sites, to be a proxy server for malicious activities, as well as taking part in DDoS attacks, etc.	CSIRT.SK sends notifications of possible malicious bot-type activity to various institutions in the Slovak Republic (central and local government) and provides technical support to the affected institutions.

Table 2 Proactive activity of the CSIRT.SK unit

OpenSSL Heartbleed vulnerability	Heartbleed is a security bug in OpenSSL library which is used for secure internet communication (https). It allows to read up a small part of the memory of the vulnerable systems and communication that should be encrypted. In some cases, it may lead to leakage of user names, passwords and encryption keys.	Proactive testing of public administration institutions' web sites for the presence of the OpenSSL Heartbleed vulnerability. In case of positive finding, the institution has been informed of the existence of this vulnerability and the technical support has been provided. Based on requests from affected entities, CSIRT.SK performed retesting of the websites to confirm successful vulnerability remediation.
The occurrence of critical vulnerabilities of web servers	The directory traversal-type attack exploits a vulnerability allowing to access the restricted files and directories which may contain sensitive information such as user names, server settings and logs, etc.	After identifying this vulnerability, warnings to affected institutions were sent and the security issue was subsequently removed in cooperation with server administrators.
Infected devices with the GameOver Zeus	GameOver Zeus is a peer-to-peer variant of the Zeus banking malware that spreads as a Trojan horse, and its task is to detect logins to electronic banking systems. The infected device becomes part of a network of bots and thus it can perform other malicious activity as well (leakage of information, participation in DoS attacks, etc.).	According to report received from foreign partner about communication of devices from the IP space of the Slovak Republic with the GameOver Zeus command and control server, CSIRT.SK cooperated with holders of infected IP addresses to remove the malware.
Bourne Again Shell Vulnerability - Shellshock	Shellshock is a group of critical vulnerabilities that enables the attacker to execute arbitrary command using environment variables. Bash is used by many applications and these vulnerabilities can be exploited for remote code execution.	Warning with a recommendation for resolving and mitigating these vulnerabilities was publish. CSIRT.SK performed analysis of detected attempts of exploitation and cooperated with foreign partners on elimination of these attacks.
SSL/TLS POODLE Vulnerability	POODLE vulnerability affects SSL version 3.0 and some implementations of TLS v1.2 protocols. By exploiting the vulnerability attacker is able to decipher parts of the communication, obtain cookies, and perform session hijacking attack. It is possible to force the usage of SSL v3.0 with Man-in-the-Middle (MITM) attack when TLS protocols used are not vulnerable.	Proactive testing of web sites of public sector institutions and banks to identify POODLE vulnerability. If the websites were found to be affected by the vulnerability, institutions were notified and technical support was provided when needed. CSIRT.SK checked for both variants of the vulnerability (SSL v3.0 a TLS v1.2).

Table 2 Proactive activity of the CSIRT.SK unit (continued)

6. COOPERATION

Cooperation at the national level

The most intensive cooperation within public administration sector is held with security experts from Slovak Information Service (SIS). Frequent information exchange aids to successful response to imminent and ongoing attacks against information systems of public administration. Cooperation with the Cyber Crime Department of the Police Force of the Slovak Republic in field of digital forensics is also quite intense. Other cooperating entities from public sector are the National Security Authority, the Ministry of Defence of the Slovak Republic, and other entities, where we cooperate at the level of information exchange. Within the private sector, CSIRT.SK cooperates with the banking sector and operators of critical information infrastructure. The scope of cooperation is the exchange of information about the currently ongoing security incidents. Next, CSIRT.SK cooperates with internet service providers during the elimination of attacks originating from or aimed at the information systems belonging to their IP address range. CSIRT.SK also cooperates with antivirus companies and other security companies in exchanging information on current threats and trends.

An important partner of CSIRT.SK is the academia where we cooperate within the scope of expert consultation and project solutions.

Cooperation at the international level

At the international level, CSIRT.SK is fully integrated into a network of foreign CSIRT/CERT teams in the TF-CSIRT (Task Force of Computer Security Incident Response Teams), an European professional association which forms a secure platform for their cooperation. CSIRT.SK actively cooperates with foreign teams within an informal association of teams with "national responsibility" under the auspicies of the CERT Coordination Center and FIRST (Forum of Incident Response and Security Teams).

CSIRT.SK IS ACCREDITED BY TF-CSIRT AND COOPERATING WITH FOREIGN SECURITY TEAMS ON DAILY BASIS

CSIRT.SK actively cooperates with other accredited teams distributed around the world, especially in terms of:

- Effective response to security incidents reported by partner CSIRT/CERT teams, ensuring the required level of protection for the received information;
- Cooperation in addressing large-scale security incidents;
- Exchange of information about the currently ongoing attacks;
- Participation in projects enhancing the level of security of information systems (detection and mitigation of malicious activities in the network);
- Sharing of developed tools for monitoring, recording, and resolving security incidents.

CSIRT.SK continues to be actively involved in process of creation and development of regional Central European platform for cooperation of the V4 countries and Austria in field of cyber security - Central European Cyber Security Platform (CECSP). CSIRT.SK actively represents the interests of the Slovak Republic in expert working groups focused on the issue of information security at the European Cybercrime Centre (EC3), the European Commission, the Council of Europe, the European Union Agency for Network and Information Security (ENISA) and the Organisation for Security and Cooperation in Europe (OSCE).

Figure 2 Map of national and governmental teams in Europe[5]

[5] ENISA; CERT inventory in Europe; 2014 http://www.enisa.europa.eu/activities/cert/background/inv/inventory

TERMS AND ABBREVIATIONS

ASSET - anything of value to the organisation
AVAILABILITY – an ability to be accessible and usable upon request of an authorised entity
BOT – a web robot, bot for short, is a computer program that repeatedly performs malicious activity for its owner
BOTNET – network of compromised devices controlled by an attacker without the knowledge of their owners with the objective of using their computing capacity to perform harmful activity (e.g. sending spam or conducting phishing and DDoS-type attacks)
C&C (command-and-control) server – a server used to manage a botnet remotely
CII – Critical Information Infrastructure
CITADEL – malicious code designed for unauthorised collection of personal data, including bank and financial information, or running malicious code on an infected device
CONFIDENTIALITY – a characteristic of information that is not made available and disclosed to unauthorised persons, entities, or processes
CSIRT.SK – a specialised unit for responding to computer security incidents in the Slovak Republic; it is defined by Government Resolution No. 479 of 1 July 2009
CSIRT/CERT (Computer Security Incident Response Team/Computer Emergency Response Team) – semantically identical designation of teams dealing with addressing computer security incidents for a defined clientele
COMPUTER SECURITY INCIDENT – a violation or imminent threat of violation of security policies, security principles, or standard security rules of operation of information and communication technologies
DEFACEMENT – an attack on a website that aims to change its appearance, often by displaying their own web page promoting political, religious, or other views
DIRECTORY TRAVERSAL ATTACK – exploitation of insufficient security validation of user--supplied file names, so that characters representing "traverse to parent directory" are passed through to the application interface. The goal of this attack is to order an application to access a computer file that is not intended to be accessible.
DNS (domain name system) - translates domain names into numerical IP addresses and vice versa. It stores this information in a distributed database in computer networks such as the Internet.
DOS/DDOS (denial-of-service/distributed denial-of-service attack) – is a technique of attack on Internet services or sites. It results in flooding of the service with requests that can cause a crash or malfunction and unavailability to other users. In the case of a DDoS attack, they use more than one machine or a botnet.
DRIVE-BY DOWNLOAD – a download of a malicious file without the user's knowledge
FIRST (Forum of Incident Response and Security Teams) – a forum of teams to address computer incidents
GNUTLS – a free implementation of the SSL, TLS and DTLS (Datagram Transport Layer Security) protocols
INTEGRITY – a feature providing accuracy and completeness of assets.
ISO/IEC – International Organization for Standardization/ International Electrotechnical Commission
MALWARE – malicious software – a general term for malicious programs including, e.g. computer viruses, Trojan horses, worms, spy software, etc.

NAT – network address translation
NICI – National Information and Communication Infrastructure
NTP (Network Time Protocol) – a protocol used for time synchronisation in the network
OLEX (Operational Level Exercise) – the second phase of the Cyber Europe 2014 exercise
OPEN RESOLVER – a vulnerability that allows an attacker to cause a shutdown of the DNS server or the deployment of the vulnerable server in a DDoS attack.
OPENSSL – is an open source implementation of the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols
PHISHING – an activity in which an impostor is trying to elicit users' digital identity, e.g. login names, passwords, information on a bank account, etc.
POP3 (Post Office Protocol) – an email protocol
RTF (Rich Text Format) – a standardised format of text files
SCANNER – a malicious code that scans an attacker-selected range of IP addresses of a potential victim and looks for network devices, open ports, or searches for shared folders.
SECURITY EVENT - an identified occurrence of a system, service, or network state that indicates a violation of security policy or a failure of a security measure or a previously unknown situation that may be significant in terms of security
SIS – Slovak Information Service
SPAM – an unsolicited mail
SPAM SENDER – a sender of spam
SSH (Secure Shell) – a cryptographic network protocol
TCP (Transmission Control Protocol) – a communication protocol
TCP-SYN FLOOD – a form of a DoS attack by which an attacker sends a large number of SYN requests to the target system with the intent to exhaust server resources so that the system does not respond to legitimate traffic requirements
TF-CSIRT (Task Force of Computer Security and Incident Response Teams) – a grouping of government, national, academic, and private CERT/CSIRT teams in Europe. The main task is to promote cooperation of such teams on the international level, exchange of information and experience in the field of information security.
TLEX (Technical Level Exercise) – the first phase of the Cyber Europe 2014 exercise
UDP (User Datagram Protocol) – a communication protocol
VIRUT – a malicious code used for cybercrime, for example DDoS attacks, spam, data theft, fraud, etc.
ZERO-DAY EXPLOIT – a special program, data, or sequence of commands that exploits a newly discovered programming error of a system or application and that is not known to the authors or that has not yet been fixed
ZEUS – a trojan horse-type malware for MS Windows that is able to perform numerous malicious and criminal activities such as stealing banking information, installing CryptoLocker ransomware, phishing, etc.

CSIRT.SK
DataCentrum
Cintorínska 5
814 88 Bratislava
Slovak Republic
incident@csirt.gov.sk
info@csirt.gov.sk
+421 2 59278 514
Fax: +421 2 52926 870
www.csirt.gov.sk

CSIRT.SK PGP Key Fingerprint:
DFB9 E47B 4304 CB18 AF97
E49D EC51 77D3 E4E1 1CE2