

CERT Polska operates within the framework of the Research and Academic Computer Network

CERT POLSKA REPORT

ISSN 2084-9079

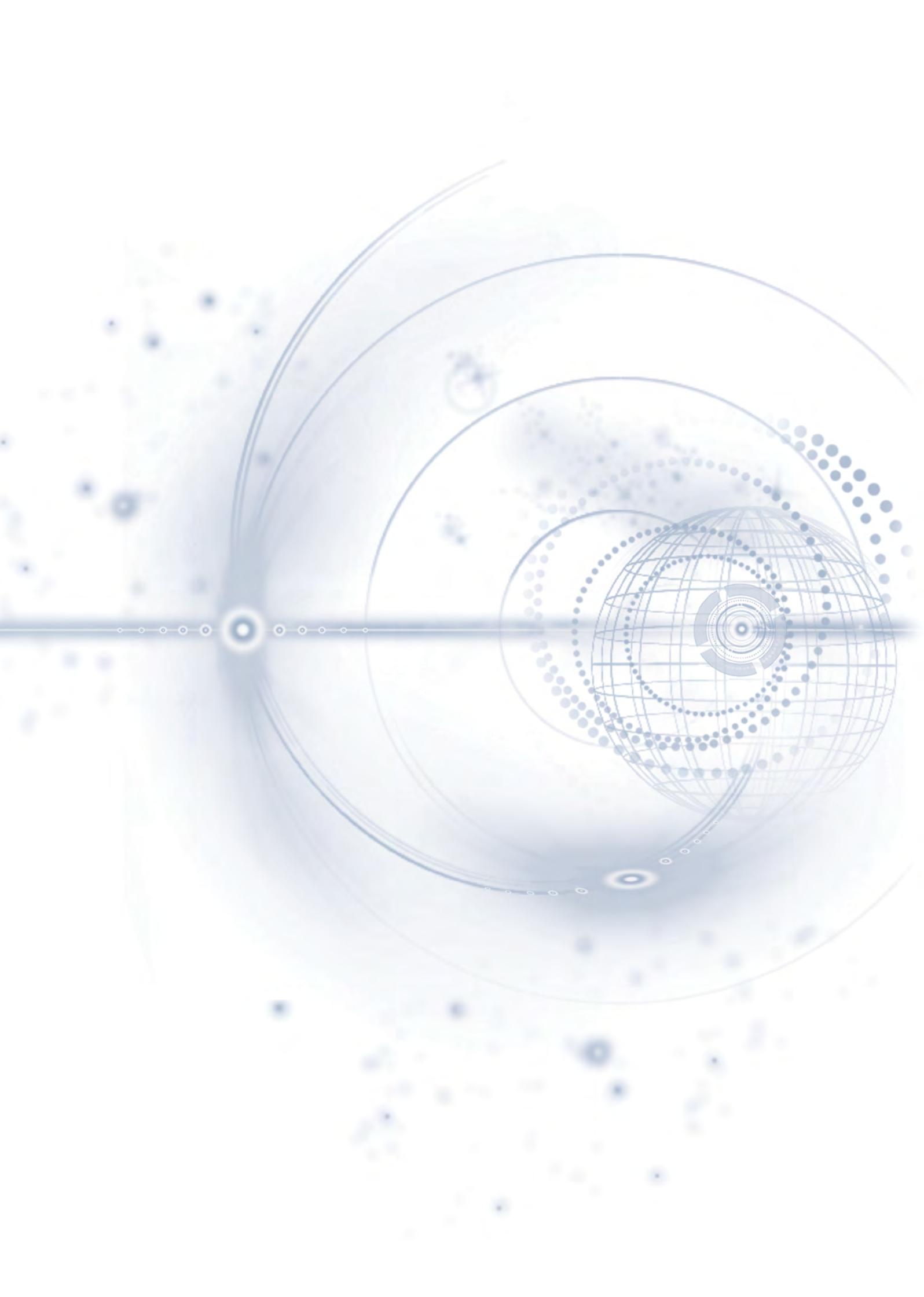


AN ANALYSIS OF NETWORK
SECURITY INCIDENTS

IN 2011

CERT
POLSKA

NASK



Contents	CERT POLSKA REPORT	3
1	Summary	5
1.1	How to read this document?	5
1.2	Key observations summarising the report	5
2	Information about CERT Polska	8
3	Introduction	9
4	Statistics of reports coordinated by CERT Polska	10
4.1	Amount of information in all categories	10
4.2	Phishing	11
4.3	Sites associated with malware	12
4.4	From a sandbox to Polish networks – addresses visited by malware	15
4.5	Spam from Polish networks	16
4.6	Scanning	17
4.7	Bots in Polish networks	21
4.8	Command & Control servers	22
4.9	DDoS attacks	23
4.10	Brute force attacks	23
4.11	Fast-flux servers	23
4.12	Open DNS servers	24
4.13	Other submissions	24
5	Statistics of incidents handled by CERT Polska	25
5.1	Number of cases of IT security breaches	25
5.2	Types of recorded incidents	25
5.3	Types of attacks recorded	26
5.4	Submitters, victims, attackers	27
6	Additional statistics related to submissions handled manually	30
6.1	Phishing in 2011	30
7	Trends in the following years	32
7.1	Number of incidents in years 1996 - 2011	32
7.2	Percentage split of incident sub-types in years 2003 - 2011	33
8	Key incidents according to CERT Polska	34
8.1	Zeus-in-the-Mobile – ZitMo	34
8.1.1	Symbian	37
8.1.2	BlackBerry	38
8.1.3	Windows Mobile	39

8.2	SpyEye in PDF	39
8.3	ZeuS – P2P+DGA variant – mapping out and understanding the threat	42
8.4	You’ve won a prize!!!	48
9	Key events in the activity of CERT Polska	51
9.1	CERT Polska communities	51
9.2	SECURE 2011 conference	51
9.3	CERT Polska report for ENISA “Proactive Detection of Network Security Incidents”	52
9.4	CERT Polska joins APWG	54
9.5	Public release of Capture-HPC as part of the Honeynet Project	55
9.6	Completion of WOMBAT project	56
9.7	Completion of FISHA project, preparation for NISHA project	57
	Report ARAKIS	58
	ARAKIS – Introduction	58
1.	Alarm statistics	59
2.	Attack statistics	61
3.	Notable network incidents observed	64
3.1	Morto – a new network worm	64
3.2	Strange traffic on port 0/TCP	69

1.1 How to read this document?

This report presents selected statistics representing data collected by CERT Polska in 2011, including a discussion and conclusions. The document is organised in a similar way to our report from 2010. This allows us to compare the observations indicated in this year's report with the ones from the previous year.

An important part of the report (section 4) is the information on threats in Polish networks, submitted to CERT Polska by various entities that monitor and respond to threats, as well as selected proprietary systems. As it covers almost all Polish operators, the report gives a wide overview of what goes on in networks allocated to Poland.

Sections 5 and 6 focus on the operational activity of CERT Polska. The data included in it are collected from incident management systems. They cover incidents which required an intervention from CERT Polska. The classification used in incident management allows comparison of the trends in subsequent years – see section 7.

Section 8 discusses in detail the key issues that emerged or developed in relation to security in 2011 and which were analysed by our team.

Section 9 discusses key developments within our team.

1.2 Key observations summarising the report



In 2011, we started using a number of new sources of data on incidents, which caused a substantial growth in the number of incidents submitted automatically.



In February, a new variant of Zeus emerged, targeting Polish users. It was unique, as apart from computers, it also attacked mobile phones. The attacker was able to read and modify information included in sms messages, including messages with transaction authorisation codes. It was the second fully documented case detected worldwide.



In April, a large scale attack targeting Polish Internet users was launched. A mass-mailed message included a PDF file with a fake invoice. After opening of the invoice, the SpyEye trojan was installed, taking over control of the infected computer. Subsequently, all confidential information entered by the user online was intercepted (including information entered to e-banking systems).



1. Summary

1.2 Key observations summarising the report



Between the end of April and June 2011, numerous leaks of data of electronic services customers occurred. The most serious incident happened in relation to Sony. The attackers stole data of over 100 million user accounts from databases of Sony-owned services PSN and SEN. In addition, about 10 million of users' credit cards had likely been compromised. User data also leaked from Nintendo, Codemasters, pornographic website pron.com, and Citibank (200 thousand accounts). Some of the attacks are attributed to Anonymous and LulzSec. These cases also affected Polish users.



In May, the source code of Zeus version 2.0.8.9 leaked out. Although it helped in fighting the malware by enhancing possibilities of analysis, concurrently new types of malware were reported, which were based on the Zeus source code.



In Autumn, a new version of Zeus appeared, propagating and communicating with the controller through a self-established peer-to-peer network. A domain name generation (a mechanism similar to that of the well known Conficker) is also used for a safe fallback.



This year, we recorded as much as 5.5 m bots (almost 10 m reports) with Polish operators. The highest number, almost 2.5 m, were located in networks belonging to Polish Telecom (TP).



Similarly to 2010, Conficker was the most frequent bot in Polish networks. We received as much as 2.1 m automated reports about this bot type.



Websites offering free aliases are more frequently used by fraudsters:

- as many as 84% of phishing sites in .pl used such services,
- 25% of malware analyzed in sandboxes that connected to Polish networks used free sub-domains.



Over half of incidents handled manually by CERT Polska represented phishing from Polish networks. We have recorded growth by one-third versus 2010. It should be emphasised that most of the cases affected foreign financial entities and did not pose any threat to Polish users.



An overwhelming majority of scans hit port 445/TCP, related to vulnerabilities in handling of RPC requests. However, the number of IP addresses scanning this port decreased in relation to 2010 by ca. 29%. Scans using other ports increased in comparison to the previous year.

-  The list of the most infected networks in Poland usually reflects the size of operators in terms of users. The position of mobile operators in the ranking seems to have stabilized.
-  Most IRC-type C&C servers in Poland were located within hosting services offered by large international entities (eg. LEASEWEB, OVH) with data centers located in Poland.
-  Most reports in relation to malicious websites were related to such domains as strefa.pl, friko.pl, interia.pl, republika.pl, i.e. those that offer website registration free of charge.
-  The number of DDoS attacks reported to us is relatively low. This does not mean such attacks do not occur – it is rather caused by unwillingness to report, also, such activity is often difficult to detect by a third party (therefore a low number of automated reports).
-  Polish Internet operators are unwilling to block port 25 TCP for end users, although such a measure was proved to be effective by Telekomunikacja Polska (Polish Telecom).
-  Mobile operators are increasingly used for spamming. Almost every fifth report is related to mobile networks.
-  In Poland, there are over 160 thousand incorrectly configured DNS servers which can be used in DDoS attacks. The issue applies basically to all operators.

2. Information about CERT Polska

CERT Polska team operates within the structures of **NASK** (Scientific and Academic Computer Network, Naukowa i Akademicka Sieć Komputerowa) – a research institute which conducts scientific activity, operates the national .pl domain registry and provides advanced IT network services. CERT Polska is the first Polish computer emergency response team. Active since 1996 in the environment of response teams, it has become a recognised and experienced entity in the field of computer security.

Since its launch, the core of the team's activity has been handling security incidents and cooperation with similar units worldwide. It also conducts extensive R&D into security topics. In 1997, CERT Polska became a member of the international forum of response teams – **FIRST**¹, and since 2000 it has been a member of the working group of European response teams - **TERENA TF-CSIRT**² and an associated organisation **Trusted Introducer**³. In 2005 on the initiative of CERT Polska, a forum of Polish abuse teams was created - **Abuse FORUM**, while in 2010 CERT Polska joined **Anti-Phishing Working Group**⁴, an association of companies and institutions which actively fight on-line crime.

The main tasks of CERT Polska include:

- registration and handling of network security incidents for Poland and the “.pl” domain name space;
- providing watch & warning services to Internet users in Poland;
- active response in case of direct threats to users;
- cooperation with other CERT teams in Poland and worldwide;
- participation in national and international projects related to IT security;
- research activity in relation to methods of detecting security incidents, analysis of malware, systems for exchanging information on threats;
- development of proprietary tools for detection, monitoring, analysis, and correlation of threat
- regular publication of CERT Polska Report on security of Polish on-line resources;
- information/education activities, aimed at increasing the awareness in relation to IT security, including:
 - publishing information on security at <http://www.cert.pl/> and Facebook and Twitter social networks;
 - organising the annual SECURE conference;
- performing independent analyses and testing solutions related to IT security.

¹ <http://www.first.org/>

² <http://www.terena.org/activities/tf-csirt/>

³ <http://www.trusted-introducer.org/>

⁴ <http://www.antiphishing.org/>

3. Introduction

For the last few years, we have observed a significant change in relation to the type of reports we receive, impacting the profile of operations of the CERT Polska team. The number of reports that require direct action within the team, which is the main type of reports that we registered, handled, and captured in the statistics in the past, is on a decline. Instead, we receive very large volumes of data related to Polish networks, which come mainly from the automated sources set up by entities dealing with on-line security. Such data, although not handled directly by us, is provided to relevant operators as part of our network of contacts. In this case CERT Polska acts as a coordinator. This is an optimal solution both for data providers, who do not have to seek contacts to individual abuse teams, and for Internet providers, who can get information, originating from many sources merged into one.

Taking into consideration the enormous amount of data shared with CERT Polska within the framework of coordination, we made an effort to standardize them and illustrate what actually happens on the “Polish” Internet. The formula is similar to our report for the year 2010. Such an approach allows us to make comparisons and detect trends in attacks. It is worth emphasizing though, that much more automated external sources provided us with information in 2011, making it difficult to compare the data from the preceding years. We tried to take that fact into account in our analyses, by making comparisons only in relation to data sources that report incidents occurring both in Poland and worldwide. Apart from coordinated reports, we also describe reports that require direct participation of our team in handling of an incident. Additionally, the report discusses a selection of the most interesting security-related issues in Poland – the ones we were directly involved in solving. We also include a description of other key areas of activity of the CERT Polska team in 2011.

4. Statistics of reports coordinated by CERT Polska

This part of the report describes the results of our analyses of information on security incidents collected automatically.

4.1 Amount of information in all categories

In 2011 we received 21 210 508 submissions from automated data feeds. Most of them concerned bots, scanning and spam. The share of all categories covered by the report is shown in the graph below (note the logarithmic scale!).

The data comes from various sources. These sources, in turn, use different methods for data collection and often present the collected data in different ways. Compared to the previous year, we have broadened report categories from 10 to

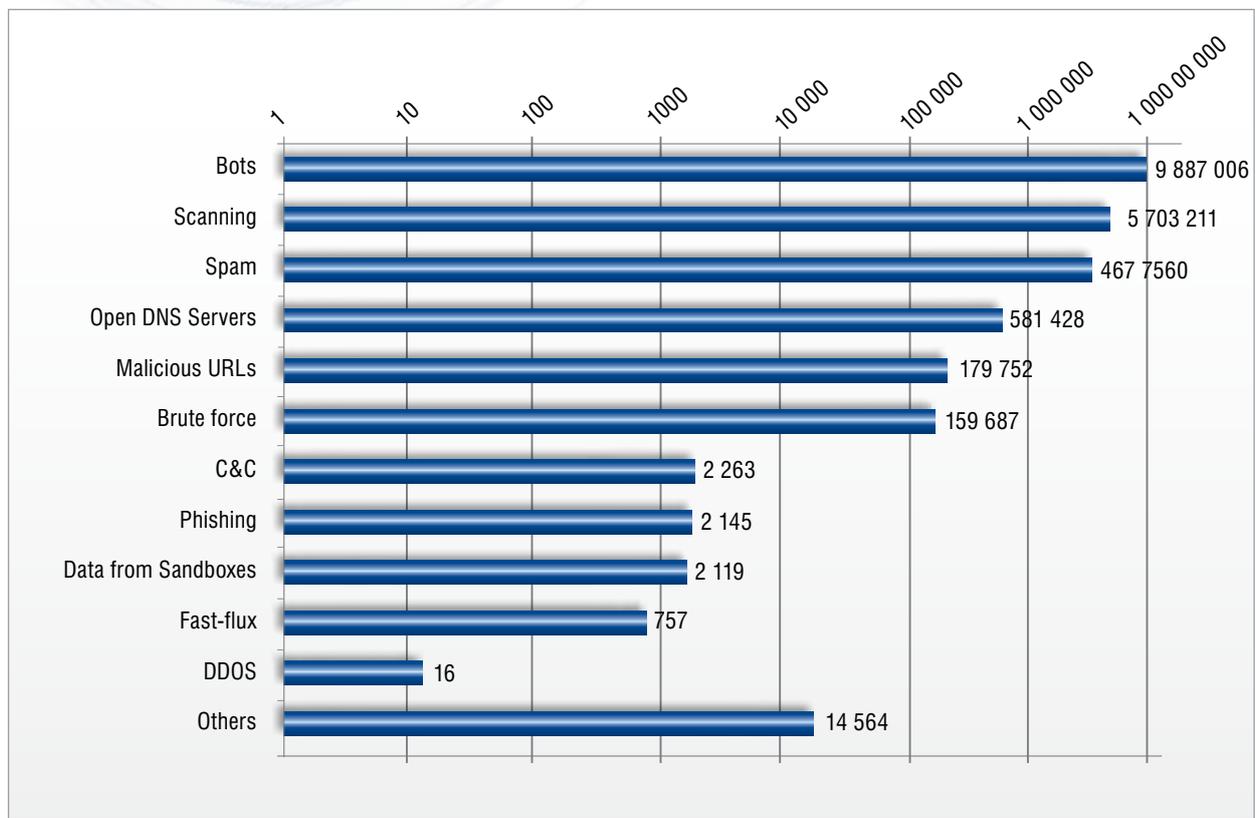


Chart 4.1.1. The Number of automated reports in individual categories

12 groups. The individual categories include: bots, scanning, spam, malware URLs, brute force attacks (new category), open DNS servers (new category), C&C servers, data derived from sandboxes, phishing, fast-flux, DDoS and others.

When comparing the above data with the data from 2010 (as well as with our semi-annual report from 1H 2011), a substantial increase in the number of events can be observed. This is mostly driven by the fact that we added numerous new sources of information in H2 2011.

In some cases, such as e.g. C&C in the graph above, we present submissions rather than unique addresses as was the case last year, therefore making the numbers higher. Adding new sources makes it difficult to compare with previous years, but provides a better picture of the degree Polish networks are infected and used for attacks.

Subsections that follow provide a detailed analysis of all types of threats listed above.

4. Statistics of reports coordinated by CERT Polska

4.2 Phishing

In 2011, we received 266 300 submissions on traditional phishing. Those submissions were related to 222 214 different URLs in 139 770 domains on 40 091 unique IP addresses. The share of phishing submissions by country is shown in Chart 4.2.1.

Ranking	Country	Phishing submissions	Percentage share in submissions
1	US	135 405	50,8%
2	HK	17 963	6,7%
3	DE	12 680	4,8%
4	CA	11 943	4,5%
5	GB	9 822	3,7%
6	CZ	8 706	3,3%
7	FR	6 492	2,4%
8	BR	6 240	2,3%
9	RU	5 580	2,1%
10	CH	5 358	2,0%
17	PL	2 120	0,8%

Chart 4.2.1. Number of submitted phishing cases in relation to geographical location

The share taken by US has grown compared to the last year, as the country has over half of all websites with phishing reported to us. This may be caused by a very favourable ratio of price to quality of hosting services, which are willingly used by the criminals if it is more profitable than hacking into existing websites. It should be emphasised that the administrators of such services are in a difficult position, as it is impossible to monitor all content kept on servers by their clients. On the other hand, even a short period of operation of a phishing website (from sending links offering it, to reporting and removing it) is sufficient for fraudsters to gain significant return on investments made. There are two other, quite untypical items that grab our attention. Ranking second in terms of the number of submissions is Hong Kong (17 963; 6.7%),

and sixth – Czech Republic (8 706; 3.3%). In both cases, websites were assigned to a relatively small number of IP addresses. In Czech Republic, 4 772 different URLs were located under 275 IP addresses (an average of 17.35 per one), and in Hong Kong 17 640 URL were located under 705 IP addresses (an average of 25.02 per one). Indeed, in both cases, a substantial number of websites were located in several host servers, under various addresses, mostly under free domains such as .co.cc or .tk. Both these domains were removed by Google from search engine results in 2011. This is an example confirming that allowing to register a domain free of charge without verifying the identity of the subscriber is not the best idea. Unfortunately, such reckless behaviour is also met in the Polish environment. For several years, we have seen the problem of companies offering free subdomains for unassisted management, with names generated in a discretionary way. Domains such as .osa.pl or bij.pl were used not only by Polish users, but by fraudsters from the entire world to register addresses such as 1tem.taebao.cem.d2wmj1o.osa.pl and used for phishing. In total, 5 980 (4.3%) of domains hosting phishing were under .pl domains. As many as 5 033 of those were free domains! In case of the remaining domains, it is probable that existing websites were hacked. Section 4.2.2 includes a list of domains used by fraudsters.

osa.pl	4 031
bij.pl	576
bee.pl	154
345.pl	118
122.pl	65
orge.pl	56
inn.pl	30

Chart 4.2.2. The list of domains most frequently used for phishing



4. Statistics of reports coordinated by CERT Polska

To reduce the interest among fraudsters, companies offering free aliases should ensure customers' accountability (i.e. an identity was verified – e.g. using a credit card) and prohibit using names of websites that are often targeted by phishing, especially related to banks.

free subdomains in .pl	528
other free subdomains	29
other submissions	69
compromises	208

Chart 4.2.3. Split of strategies used for phishing in the networks of Polish operators

In terms of phishing located in Polish networks (independent of the domain, in which a given URL was located), we obtained 2145 of such submissions, relating to 1464 URLs in 812 domains under 505 IP addresses. The split of strategies used for phishing in the networks of Polish operators is shown in Chart 4.2.3.

The next chart includes information on top ten operators in terms of submissions received. The predominant position of hosting operators should not come as a surprise, as it is with them that criminals usually purchase services or look for potential victims. The ratio of the number of submissions to the unique IP addresses can be related to the time and effectiveness of operators' response – the shorter the time, the faster a given address was removed.

	ASN	Name	Submissions	IP	Submissions/IP	URL
1	15 967	NetArt	514	167	3,08	352
2	12 824	HOME.PL	359	60	5,98	269
3	49 102	CONNECTED	186	1	186,00	104
4	5 617	TP	162	40	4,05	91
5	43 470	LiveNet-PL	75	6	12,50	42
6	29 522	KEI	70	24	2,92	60
7	29 314	VECTRA	65	4	16,25	36
8	6 714	GTS	46	8	5,75	34
9	43 333	CIS NEPHAX	40	10	4,00	25
10	15 694	ATM	40	4	10,00	19

Chart 4.2.4. The list of top operators in terms of submissions received

4.3 Sites associated with malware

This category includes submissions from automatic sources related to cases of malicious files hosted in networks of Polish operators. These mainly include:

- malicious code that compromises a browser or one of its plugins or extensions,
- malicious executables (including ones downloaded as a result of execution of code mentioned above),
- configuration files used to control malicious software.

4. Statistics of reports coordinated by CERT Polska

Due to the fact that we started using many new sources of information in the second half of 2011, the statistics have changed. We received many more submissions, counted as unique combinations of submission day/IP/URL. Not all of the data sources include information on the threats from servers located outside of Poland. Therefore, not always are we able to compare the situation of Poland in relation to the world – the comparisons are only done using sources that provide data on both Poland and the rest of the world. The analysis of the situation within Polish networks is done using all data available.

Ranking	Country	Percentage share of submissions
1	US	41,10%
2	CN	15,42%
3	KR	9,62%
4	RU	5,48%
5	DE	4,12%
6	CA	3,03%
7	FR	2,78%
8	UA	2,37%
9	BR	2,17%
10	EU	1,77%
11	GB	1,50%
12	PL	1,43%
13	IT	1,33%
14	CZ	1,12%
15	NL	1,11%
16	JP	0,65%
17	TR	0,65%
18	SE	0,59%
19	HU	0,48%
20	RO	0,35%
	OTHER	2,94%

Chart 4.3.1. Cases of malware on websites by geographical location (countries)

The statistics for the world have not changed substantially versus 2010. United States ranked first, with 41.10% of overall submissions. China came second – 15.42%. Poland, similarly to the previous year, ranked 12, with similar percentage of submissions – 1.43%.

Note the high position of China, Russia and Ukraine. When we confront the malware chart with the chart for phishing cases, it can be seen that the positions of these countries (in particular China) are significantly higher in the category of malicious software. This may imply that the malicious files in these countries do not appear solely as a result of blind hacking attacks (in this case we would expect the distribution to be similar to phishing cases) but that the countries are chosen on purpose. On the one hand, many Chinese and Russian hosting providers have a reputation for “bulletproof hosting” because of the difficulty in convincing them to remove malicious resources. On the other hand, there was intense speculation that cyber criminals act in China, Russia or Ukraine with the tacit consent of local influential circles. Of course, both theories are not mutually exclusive and are not the only possible explanations of the high position of these countries in these statistics.

In total, for Poland (domain .pl and/or those hosted in Poland) in 2011 we received 272546 submissions, including 3000 unique IPs, 38472 URLs and 6999 domains. Out of those submissions, 179 752 of the submitted cases were hosted in Poland, with 2576 IPs, 27991 URLs, and 5637 domains. Among submissions of malicious URLs from .pl domain hosted outside of Poland, the majority are represented Germany and France. Only 3 out of 424 IP foreign addresses were located in China – they contained malicious executable files.

The top positions in the summary lists of submissions, unique IPs, URLs and domains were taken by the largest providers of hosting services: Home.pl, Netart, and Krakowskie E-Centrum Informatyczne Jump. These observations are similar to those from 2010, but different from those received in H1 2011 – which might be driven by the fact that access to multiple new sources of information was gained.



4. Statistics of reports coordinated by CERT Polska

Sometimes also the top positions were taken by classic internet providers – e.g. Netia topped the ranking in the category of most unique malicious IPs. TP, on the other hand, ranked relatively low. It is worth mentioning no mobile network operators rank high in the list.

The chart above shows domains by the number of unique malicious URLs submissions. The first noticeable thing is that the free domains such as bee.pl/osa.pl, frequently used in phishing and also observed in sandbox data, are missing from the chart. Other free domains are used (see Chart

	Number of submissions	Percentage share	ASN	Operator
1	30 330	16,87%	12 824	HOME.PL
2	19 336	10,76%	29 522	KEI
3	14 960	8,32%	15 967	NETART
4	13 341	7,42%	16 138	INTERIA
5	10 853	6,04%	12 741	NETIA

Chart 4.3.2. Cases of malware submissions on Polish websites by autonomous systems

	Number of unique IPs	Percentage share	ASN	Operator
1	607	23,56%	12 741	NETIA
2	499	19,37%	12 824	HOME.PL
3	231	8,97%	15 967	NETART
4	163	6,33%	5 617	TP
5	96	3,73%	29 522	KEI

Chart 4.3.3. Cases of malware submissions on Polish websites by unique IPs with Polish operators

4.3.6). Usually, malware was distributed from a Chinese domain p-upfile.co.cc and mypromo-file.info. Malware from those domains usually was a file named SetupXXX.exe, where XXX represented its subsequent version. Antivirus software recognised it to be Zeus banking trojan, but depending on the version, also as software pretending to be an antivirus software (so called rogue antivirus). It seems the domains were registered specifically for that purpose (such as the last two domains in Chart 4.3.5). The case of the following six domains (items 3 to 7) is different, as these were legitimate domains hacked to host various malware.

Unfortunately, we have no precise statistics showing the split of the types of malware on those websites. In our view however, the major form of infecting end users are social engineering mechanisms – the user installs malware him/herself, after downloading and running an executable file. It should be noted though, that the second popular and much more dangerous attack category is drive-by download (an attack, in which the process of infecting a computer is done by exploiting a vulnerability in the browser or its plug-in is done automatically, unnoticed by the user). In 2011 attacks exploiting Java vulnerability in browsers were a significant element. We recommend to uninstall Java from your computer if it is not necessary to perform day-to-day operations.

	Number of unique URLs	Percentage share	ASN	Operator
1	4 622	16,51%	12 824	HOME.PL
2	3 832	13,69%	16 138	INTERIA
3	2 093	7,48%	29 522	KEI
4	2 012	7,19%	15 967	NETART
5	1 230	4,39%	12 741	NETIA

Chart 4.3.4. Cases of malware submissions on Polish websites by unique URLs

4. Statistics of reports coordinated by CERT Polska

Ranking	Unique URLs	Domain hosting malware
1	1 984	p-upfile.co.cc
2	1 040	mypromofile.info
3	926	kamp.nazwa.pl
4	558	esflores.kei.pl
5	493	noclegi-i.pl
6	375	dementia.waw.pl
7	367	www.sp2osiek.pl
8	336	www.teatr-pismo.pl
9	314	acletan.strefa.pl
10	295	canrilric.strefa.pl

Chart 4.3.5. Ranking of domains hosting malware by unique URLs

Number of unique IPs	Domain
2 402	strefa.pl
1 770	com.pl
1 124	friko.pl
1 081	interia.pl
1 064	republika.pl
1 041	nazwa.pl
815	w8w.pl
700	yoyo.pl
676	waw.pl
576	kei.pl
493	noclegi-i.pl

Chart 4.3.6. Ranking of second level domains hosting malware by unique URLs

4.4 From a sandbox to Polish networks – addresses visited by malware

This category of information is in many ways an extension of the previous one. It concerns addresses that were visited by malware installed for observation inside sandboxes – that is a specially prepared environment in which untrusted software can be safely run. In total, 2113 files attempted to connect to 2119 unique WWW and FTP addresses. Approximately 31% of them were recognised by antivirus programs as malware (based on Cymru Malware Hash Registry – <http://www.team-cymru.org/Services/MHR/>).

Most connections were observed to server geoloc.daiguo.com. We observed 429 requests. All were the same, but each of them was generated by a piece of malware with a different MD5 sum. These are queries aimed to obtain information on the geographical location of the infected machine.

Similar frequency (424 times) was recorded in relation to connections to www.bee.pl server. It is a server offering free aliases, often used by malware authors to redirect the victims to C&C servers. Similarly to phishing, we have noticed quite significant interest from fraudsters in that type

of services. In total, we recorded 520 such connections (Chart 4.4.2). Apart from bee.pl, the fraudsters used domains osa.pl, 345.pl, bij.pl and orge.pl.

Ranking	URL or IP contacted	Number of requests
1	geoloc.daiguo.com	429
2	www.bee.pl	424
3	212.33.79.77	275
4	pelcpawel.fm.interia.pl	167
5	www.bigseekpro.com	72
6	s1.footballteam.pl	61
7	mattfoll.eu.interia.pl	61
8	appmsg.gadu-gadu.pl	61
9	www.tibissa.com	58
10	213.108.56.140	58

Chart 4.4.1. Addresses affected by malware



4. Statistics of reports coordinated by CERT Polska

We recorded 275 connections to a server with IP address 212.33.79.77. All of them were generated by the same malicious file. This traffic represents communication of infected machines with their C&C.

Another very interesting situation relates to addresses in the interia.pl domain: pelcpawel.fm.interia.pl, radson_master.fm.interia.pl and mattfoll.eu.interia.pl. In all these cases, the culprit was a trojan horse named Salty. Again, as in the example described above, it attempted to connect to its command centers.

In the case of appmsg.gadu-gadu.pl, like in the previous year, we noticed initiating connections to gadu-gadu messenger network.

Ranking	Domain name	Number of connections
1	bee.pl	424
2	osa.pl	48
3	345.pl	32
4	bij.pl	8
5	orge.pl	8

Chart 4.4.2. Connections to free subdomains

With regard to the remaining addresses, it was impossible to clearly determine why they were visited. It could either represent activity of malware or traffic generated by regular applications checked by sandbox users.

4.5 Spam from Polish networks

In 2011 we received 4 677 560 submissions on spam from Polish networks. It should be emphasised that the majority of the submissions are not related to individual unsolicited messages, but sources – usually of infected or incorrectly configured machines, with many of them mailing tens of thousands of e-mails. The number of submissions is lower than a year ago, but the trend this year was slightly increasing, with a temporary drop in the summer holiday season. Over half of all submissions were related to only three operators – Netia (31%), Telekomunikacja Polska (17%), and Multimedia Poland (10%). The data we analysed are related to most, but not all Polish networks, therefore the result should not be translated to country-wide conditions. However, the relations between the operators included are factual. The disproportion between Telekomunikacja Polska and Netia is noticeable, especially given the market shares of both operators. It is driven by the technical solutions that have been applied for almost two years by Telekomunikacja Polska, especially blocking port 25 TCP by default for end users. Unfortunately, despite the great effectiveness of such solution, it has not been implemented by any other large operator in Poland to date.

If we divide the number of submissions by the number of unique cases they were related to (1 253 528), the result is 3.73. Given the fact that the number of submissions for one case is strongly correlated with time of operation of a given source, this number can be treated as the persistence ratio – with the same method of calculation applied for the individual autonomous systems, the longer the sources “stay alive” in a given network, the higher the ratio will be. Low values can be driven either by high effectiveness of the operator in dealing with issues quickly, or by dynamic IP assignment. In the latter case, the infected machines are simply identified as new sources each time they renew lease. Therefore, they should be interpreted along with the number of submissions. Persistence for ten networks the submissions were most often related to (89.5% in total) was between 1.23 and 23.51.

Note the high ranking of mobile operators. All of them ranked top ten by the absolute number of submissions, in total representing almost every fifth submission (19.5%). If unique IP addresses submitted as sources of spam are taken into account, almost every mobile operator ranks higher than Telekomunikacja Polska! Only T-Mobile ranks slightly lower.

4. Statistics of reports coordinated by CERT Polska

Obviously, the statistics are biased to some extent due to the method of IP assignment in those networks (short DHCP lease times). However, it should not be completely ignored, as coverage of address space with addresses considered to be spam might decide on placing large parts of the networks on blacklists. This is significant for users

who suddenly become unable to send e-mail from their legitimate servers. It seems that mobile operators will have to tackle the issue of spam from their networks in the immediate future. Even more so with mobile Internet access gaining on popularity. In many cases it is already considered as an alternative to a fixed line.

	ASN	Operator's name	Number of submissions	Share	Number of unique sources	Share	Persistence
1	12741	NETIA	1 452 218	31,0%	391 405	31,2%	3,71
2	5617	TP	797 275	17,0%	107 477	8,6%	7,42
3	21021	MULTIMEDIA	468 932	10,0%	70 265	5,6%	6,67
4	43447	ORANGE	360 078	7,7%	194 319	15,5%	1,85
5	29314	VECTRA	353 998	7,6%	19 664	1,6%	18,00
6	8374	PLUS	265 747	5,7%	188 951	15,1%	1,41
7	39603	PLAY	182 600	3,9%	147 554	11,8%	1,24
8	20960	Telekomunikacja Kolejowa	128 293	2,7%	5 458	0,4%	23,51
9	12912	T-MOBILE	97 283	2,1%	79 278	6,3%	1,23
10	12476	ASTER	78 451	1,7%	3 348	0,3%	23,43

Chart 4.5.1. Ranking of operators by the number of spam submissions

4.6 Scanning

All submissions included in the statistics below were received automatically. In total, we obtained 5 703 211 submissions on scans originating in Poland. The breakdown includes data sent by our partners from their monitoring systems, as well as from our ARAKIS system.

Most scanned services

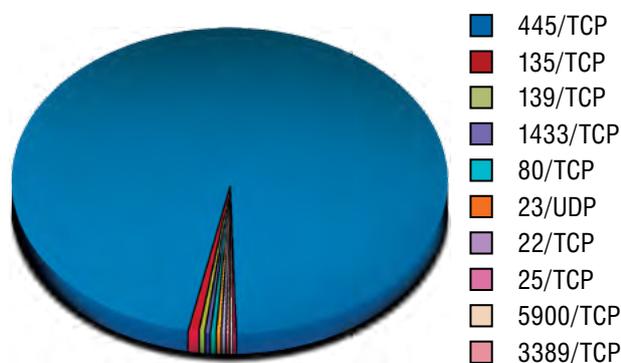
The statistics below present TOP 10 target ports by unique source IP addresses, where Polish IP addresses were the source.



4. Statistics of reports coordinated by CERT Polska

Ranking	Destination port	Number of unique IPs	Change versus 2010	Probable leading mechanism of attacks
1	445/TCP	205 243	-29,00%	Buffer overflow attacks on Windows RPC services
2	135/TCP	2 560	0,00%	Attacks on windows DCE/RPC service
3	139/TCP	2 062	95,00%	Attacks on NetBIOS service / sharing files and printers
4	1433/TCP	1 124	100,00%	Attacks on MS SQL
5	80/TCP	914	63,50%	Attacks on web applications
6	23/TCP	440	40,00%	Attacks on telnet service
7	22/TCP	435	-1,00%	Dictionary attacks on SSH servers
8	25/TCP	434	62,00%	Possible spamming attempts
9	5900/TCP	401	29,00%	Attacks on VNC
10	3389/TCP	394	166,00%	Dictionary attacks on RDP (remote desktop) – largely the activity of Morto worm

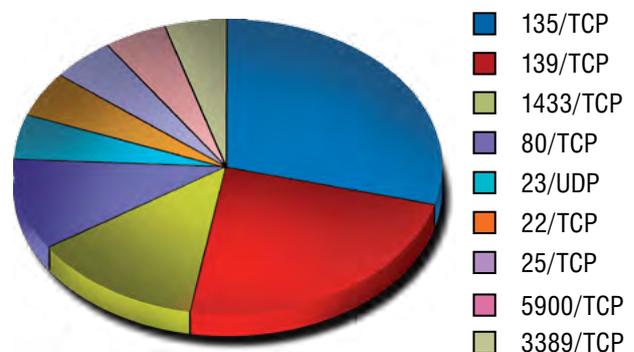
Chart 4.6.1. TOP 10 of destination ports by number of unique scanning sources



Graph 4.6.2. TOP 10: unique source IP per port

Ranking first, as in the previous year, is port 445/TCP. Most of the serious, and therefore most often exploited Windows vulnerabilities are located in services listening on this port. However, although this port significantly leads over the remaining ones, the gap has been narrowed in comparison to 2010. Also, the overall number of unique IPs scanning this port has been reduced. Would that indicate the slow fall of threats related to scanning?

Ranking second is port 135/TCP, not present in last year's TOP 10, on which windows service DCE/RPC (Distributed Computing Environment / Remote Procedure Calls) listens by default. Many vulnerabilities were repeatedly detected in it, one of them is exploited by the known and "aged" Blaster worm. However, in 2011 there were no new worms using port 135 to propagate.



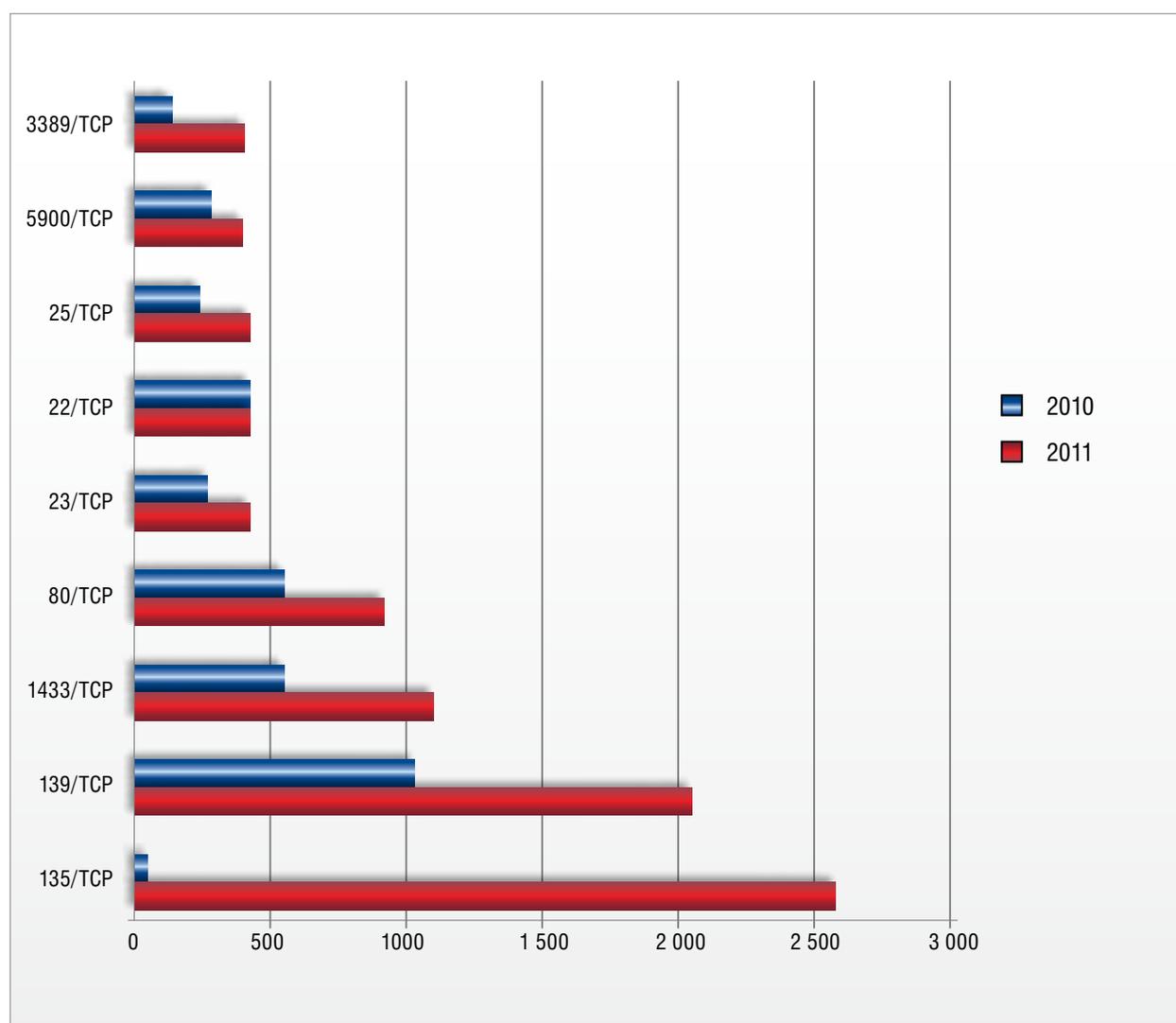
Graph 4.6.3. TOP 10: unique source IP per port (excluding 445/TCP)

4. Statistics of reports coordinated by CERT Polska

New entries in the TOP 10, apart from the above-mentioned 135/TCP, include port 25/TCP (SMTP mail service), and 3389/TCP. The latter port is related to windows service Microsoft Terminal Server using RDP protocol (used by the so called remote desktop). Its appearance in the ranking in most cases is caused by the Morto worm spreading in networks since August, which infected Windows systems on a mass scale. What is interesting, Morto does not exploit any vulnerability, but guesses users' passwords. Concurrently – apart from Morto's activity – we observed an increased number of scans on that port, unrelated to the worm.

Compared to the previous year, an increased interest was recorded in almost all ports included in the ranking, except for 445/TCP. A significant increase is observed mostly on ports 1443/TCP (by ca. +100%) - Microsoft SQL Server service, 139/TCP (ca. +95%) – NetBIOS service, 80/TCP (ca. 64%) – web applications, and 23/TCP (ca. +40%) – telnet service.

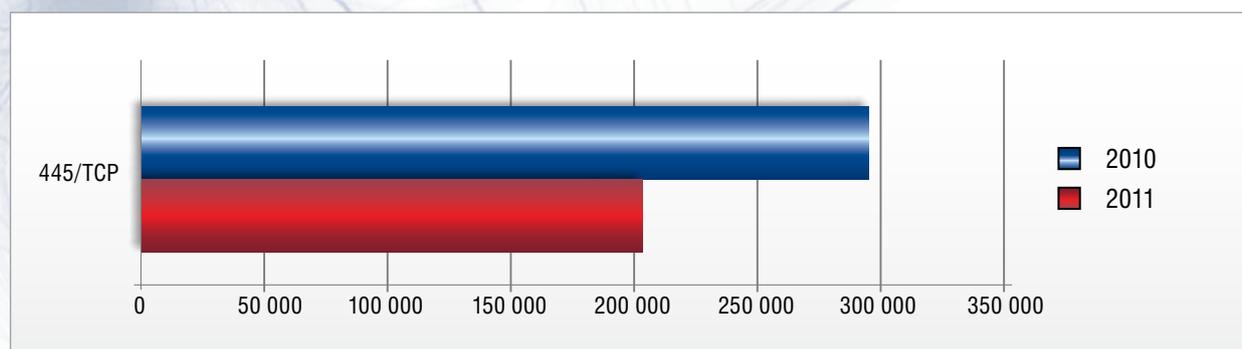
Similarly to the previous year, an interesting fact is the relatively high ranking of attacks on services "native" to Unix/Linux: telnet (23/TCP port), and SSH (22/TCP port). In the case of SSH, these are mainly dictionary attacks.



Graph 4.6.4. TOP 10: unique IPs per port 445/TCP – comparison with 2010



4. Statistics of reports coordinated by CERT Polska



Graph 4.6.5. Unique IPs per port 445/TCP – comparison with 2010

Most infected Polish networks (in terms of scanning)

The distribution of infected unique IP addresses amongst Polish operators is shown below.

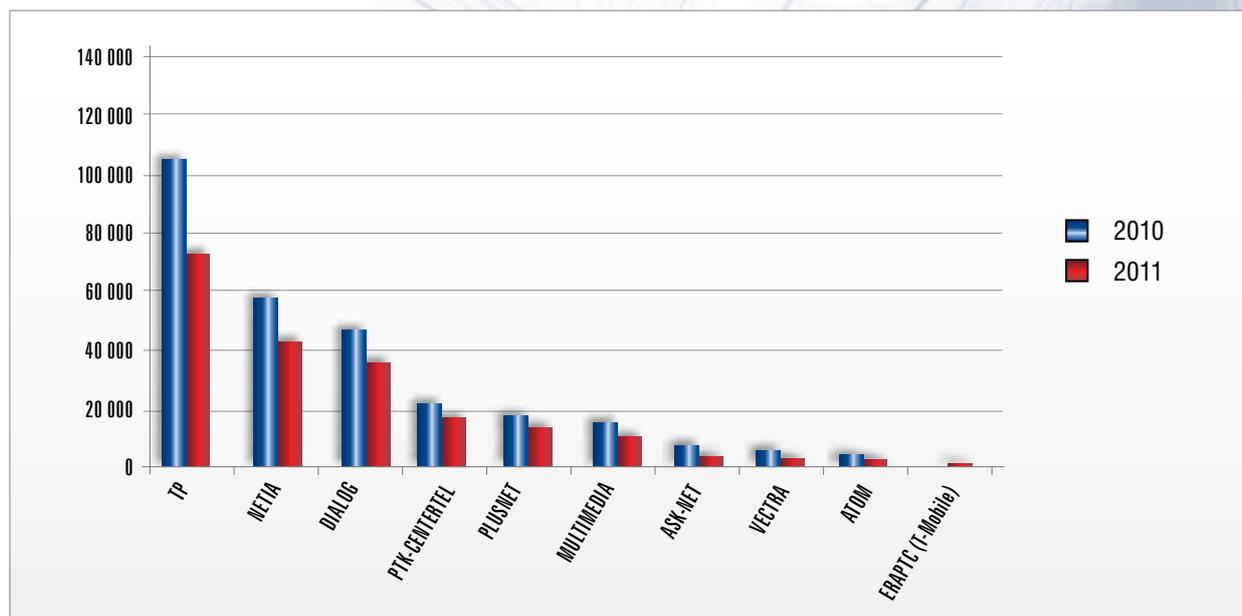
The ranking of Polish operators' AS numbers is almost identical as in the previous year – it also reflects the size of the individual operators in terms of the number of users. The only difference is UPC not being present in the ranking (AS9141).

In terms of the number of infected computers, an evident decrease versus 2010 is observed for all operators. The largest reduction can be observed for Vectra (decrease by 57%), ATOM (decrease by 46%), ASK (decrease by 44%), and topping the ranking, Telekomunikacja Polska (decrease by 41%).

Ranking	Operator's name	ASN	Number of unique scanning IPs	Change versus 2010
1	TP	AS5617	74 854	-41,00%
2	NETIA	AS12741	43 011	-24,00%
3	DIALOG	AS15857	34 684	-26,50%
4	ORANGE	AS43447	18 441	-25,00%
5	PLUS	AS8374	16 111	-12,40%
6	MULTIMEDIA	AS21021	11 762	-27,80%
7	ASK-NET	AS25388	2 739	-44,00%
8	VECTRA	AS29314	2 052	-57,50%
9	GTS	AS6714	1 749	-46,40%
10	T-MOBILE	AS12912	1 008	-

Chart 4.6.6. Distribution of infected IPs in Poland

4. Statistics of reports coordinated by CERT Polska

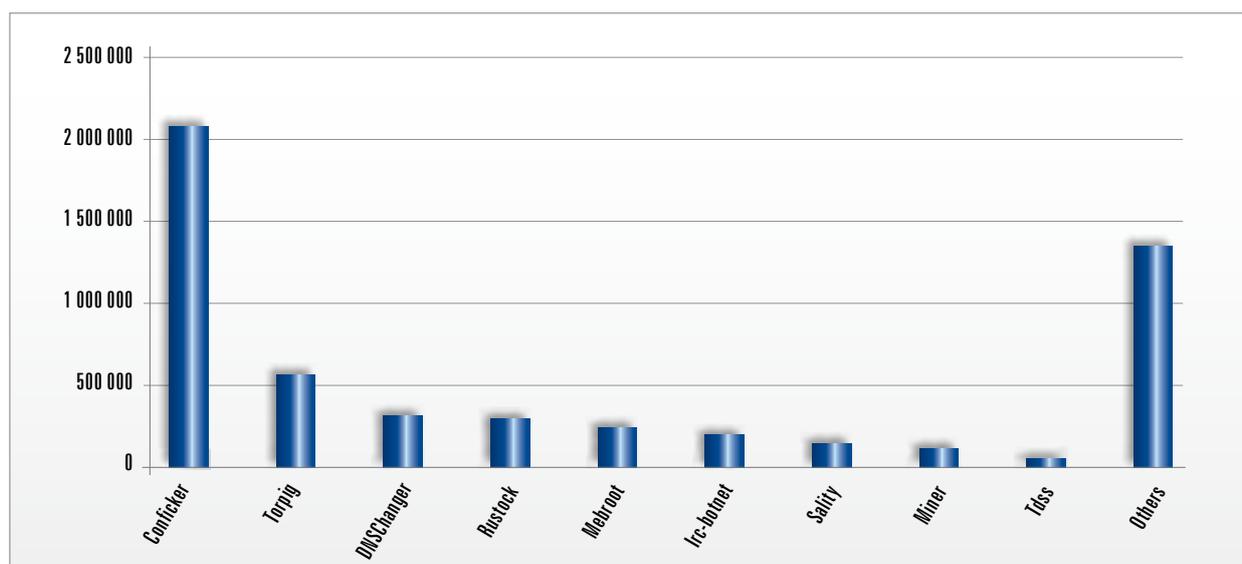


Graph 4.6.7. TOP 10 Polish operators by number of unique IPs scanning

4.7 Bots in Polish networks

This category includes computers in Polish networks that are part of botnets and are not included in other categories. Although the most popular use of botnets is to send spam, they can also be used for any other purposes, such as theft of user credentials, DDoS or simply to provide an additional layer of anonymity.

In 2011, we observed over 5.5 m bots (almost 10 m submissions). Conficker was the most popular. It was 3.5 times more common than Torpig, ranking second. It infected over 2.1 m machines. A particularly high number of submissions was recorded in the second half of the year (in the first it ranked only fifth), which not necessarily indicates higher activity,



Graph 4.7.1. Number of bots by type



4. Statistics of reports coordinated by CERT Polska

but might be caused by the fact that many new sources of information were added in the second part of the year. For Torpig, we recorded almost 600 k infections. In the second part of the year, DNSChanger also emerged, infecting over 360 k machines. Rustock was at a similar level (ca. 350 k). Over 1.3 m were other bots whose individual type could not be identified (data from sinkholes).

Most bots were detected in AS 5617 owned by TP. There were almost 2.5 m bots – almost four times the number of bots in AS 12741 owned by Netia (ca. 630 k). The highest amount of bots operate in networks of operators who provide Internet to individual users. These are large providers such as TP or Netia, mobile Internet providers – Orange, Play, Plus and T-Mobile and cable Internet providers - Multimedia and Vectra. Almost half of all bots (ca. 45%) were found in TP networks, while 12% were in Netia.

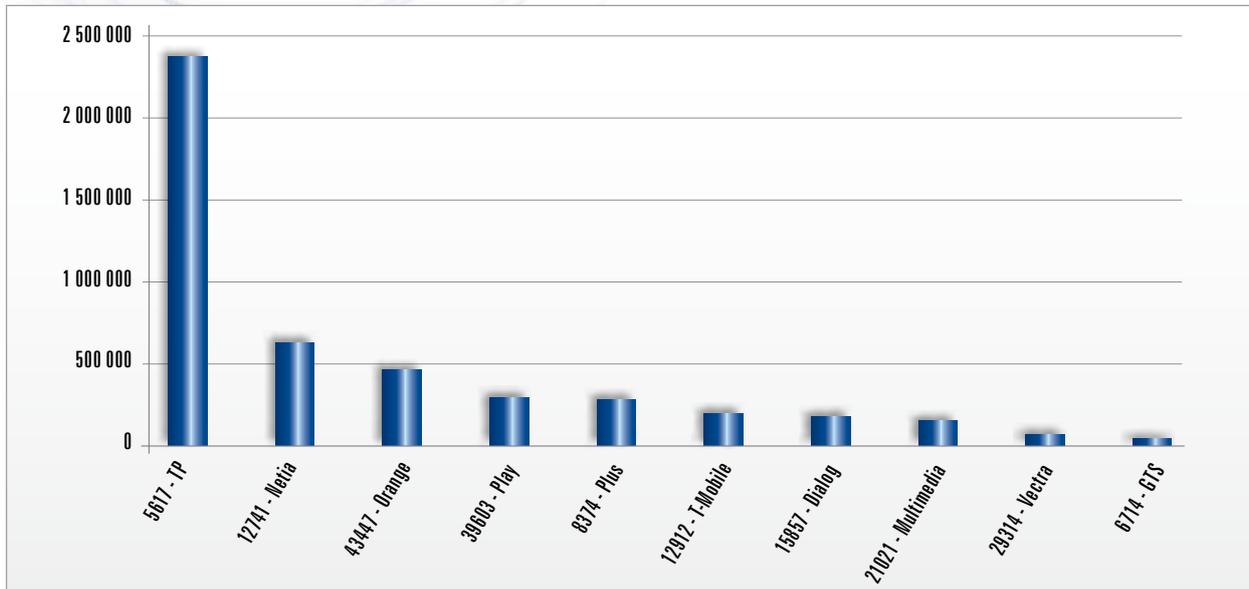


Chart 4.7.2. Distribution of bots by Polish ISP

4.8 Command & Control servers

In 2011, we received 2263 submissions (counted as unique day/IP combinations) from external automated data feeds with 59 unique Command & Control servers used to manage botnets.

This is more than in last year (2010) and in the semi-annual report for 1H 2011 due to the fact that new external data sources were included.

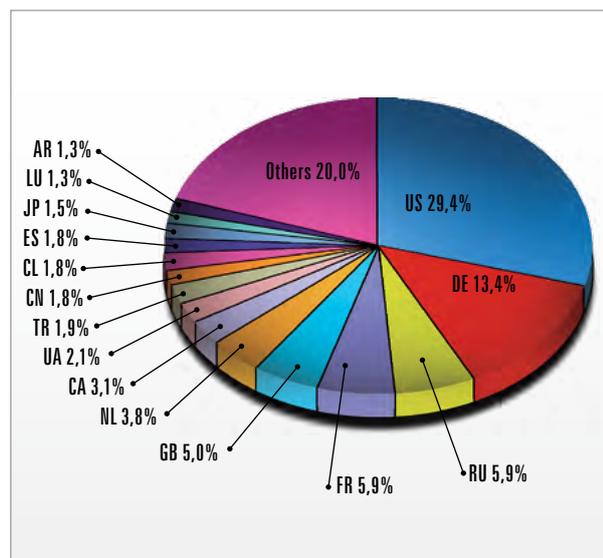
Position	ASN	Operator	Number of unique C&C servers
1	16 276	OVH	22
2	16 265	LEASEWEB	9
3	5 617	TP	5
4	12 741	NETIA	5
5	28 753	LEASEWEB	2

Table 4.8.1. Distribution of unique C&C servers in Polish networks

4. Statistics of reports coordinated by CERT Polska

As in the previous years, most of the submissions were related to IRC servers (most also on the standard port dedicated to that service – 6667/TCP). The dominating leader was French OVH, for the first time in our report under this category, which, similarly to Dutch LEASEWEB has private networks assigned to Poland in RIPE.

Worldwide, USA traditionally topped the ranking with 29.4%. Together with Germany, they host almost 50% C&Cs. Similarly to the previous year, West European countries rank at the top, such as France, Great Britain, and the Netherlands. Russia's ranking is higher than last year – at 3rd place. China takes a relatively low, 10th ranking. According to the data in our possession, also Poland's ranking is very favourable, only at 23rd place.



Graph 4.8.2. Countries where C&C servers were located the most often

4.9 DDoS attacks

In the first half of 2011, we received 14 automated submissions on DDoS attacks on hosts located in Polish networks. These were incidents of issuing a command to attack, registered on surveilled C&C servers. Four of the attacks were targeting online game servers. According to our analysis, other attacks were targeting individual users. The number of the attacks is higher than in 2010 when we

received 11 incidents, however still less in comparison with other categories. Unfortunately, this is not because such attacks are far and between. This is rather caused by lack of automatic monitoring of such attacks by third parties.

4.10 Brute force attacks

We received 159 687 submissions in relation to blind attempts of logging on to services. Such attacks, called “brute force”, are used to guess passwords by trial and error. Currently, they are usually related to attempts of getting access with the use of default passwords, errors in configuration, or the use of vulnerabilities in how the access control functionality was implemented.

All submissions were related to logging attempts to SSH service. Their number, however, does not reflect the scale of the problem. All attempts were made from only 127 unique IP addresses. This gives an average of 1 257 attempts per address. The distribution median is 11 and 85% of the addresses generated less than 1 000 attempts.

That data, aligned with the statistics in section 4.6 show attacks on services such as SSH are much less popular than a few years back. This is certainly a consequence of the increasing effectiveness of technical security features as well as security policies - at least with regard to remote access. The intruders rationally seek for easier targets, using for example social engineering or web applications, which by definition must be made available publicly.

Most of the discussed attempts took place between end of February and end of March 2011.

4.11 Fast-flux servers

Fast-flux is a technology used for dispersing the infrastructure (especially content servers) over multiple machines – usually acting as part of a botnet – in order to make it difficult to track and take down. This method is often used with phishing, spam (to keep websites to which users are directed) or distributing pornography. Fast-flux uses domains

4. Statistics of reports coordinated by CERT Polska

Unique IPs	ASN	Operator
613	5 617	TP
82	12 741	Netia
42	29 314	Vectra
16	21 021	Multimedia
3	12 476	Aster
1	13 119	ACI

Chart 4.11.1. Location of computers used in "Fast-flux" networks

administered by criminals. Relevant DNS records are frequently and regularly changed. As a result querying for a single hostname results in multiple IP addresses at a time – and a different set every few minutes. In 2011, we had 757 submissions of hosting fast-flux domains under IP addresses of Polish networks. As it is easy to guess, all hosts were located in networks providing Internet to end users, which is shown in Chart 4.11.1.

The submissions were related to 17 different domains, of which the most active was "serviced" by 336 Polish addresses. In the case of most domains, the used infrastructure was much smaller, covering not more than 52 Polish IP addresses (15 domains).

The observed time of a single fast-flux domain appearing in Polish networks (probably closely correlated with its life span) was not more than 2 months. What is interesting, we did not observe any case of one address being used for more than one domain. This might suggest that the individual botnets do not share their infrastructure and are not leased out to competition, at least in case of fast-flux services.

4.12 Open DNS servers

In this category there are incorrectly configured DNS servers, allowing recursive queries from any location in the network. Such setting allows miscreants to use them in DDoS attacks by increasing the

traffic volume (*traffic amplification*) resulting from DNS queries with false source address.

In 2011, we received 581 428 submissions on 160 682 unique IP addresses under which such servers were located. This indicated a material scale of this issue in Poland. A distribution of ten autonomous systems, in which most usually open DNS servers were located is presented below:

Unique IPS	Percentage share	ASN	Operator
63574	39,6%	5 617	TP
18667	11,6%	12 741	Netia
16941	10,5%	43 447	Orange
7023	4,4%	20 960	TKTELEKOM
6157	3,8%	6 714	GTS
4116	2,6%	50 994	E-SBL-AS e-SBL.net
3430	2,1%	21 021	MULTIMEDIA
2722	1,7%	29 314	VECTRA
1998	1,2%	29 665	SPEED-SOFT
1798	1,1%	13 000	LEON-AS

Chart 4.12.1. Distribution of ten autonomous systems, in which open DNS servers were located most often

4.13 Other submissions

The remaining 14.5 k submissions were related to various types of automatically detected threats, mainly incorrectly configured devices such as proxy servers or routers.

5.5 Statistics of incidents handled by CERT Polska

This part of the report discusses incidents registered in the submission management system, that is submissions which were handled directly by humans in CERT Polska. In many aspects, they act as a supplement to the picture presented in section 3, as they include incidents that are not covered by automatic data feeds – not effected on mass scale, but often serious, requiring human intervention.

5.1 Number of cases of IT security breaches

In 2010, we handled 605 incidents. The following sections present their detailed classification.

5.2 Types of recorded incidents

Incident type/subtype	Number	Total-type	Percent-type
Abusive Content	2	152	25,12
Spam	144		
Harassment	3		
<i>Child/Sexual/Violenceviolence⁵</i>	3		
Malicious Code	39	46	7,60
Virus	2		
Worm	0		
Trojan	5		
Spyware	0		
Dialer	0		
Information Gathering	1	46	7,60
Scanning	42		
Sniffing	0		
Social Engineering	3		
Intrusion Attempts	7	23	3,80
Exploiting of Known Vulnerabilities	11		
Login attempts	5		
New Attack Signature	0		
Intrusions	3	10	1,65
Privileged Account Compromise	4		
Unpriviledged Acoount Compromise	2		
Application Compromise	1		
Availability	0	14	2,31
Denial-of-service attack (DoS)	3		
Distributed denial-of-service attack (DDoS)	11		
Sabotage	0		
Information Security	0	3	0,50
Unauthorised Access to Information	2		
Unauthorised Modification of Information	1		
Fraud	1	307	50,74
Unauthorised Use of Resources	0		
Copyright	1		
Masquerade (including Phishing)	305		
Other	4	4	0,66
TOTAL	605	605	100

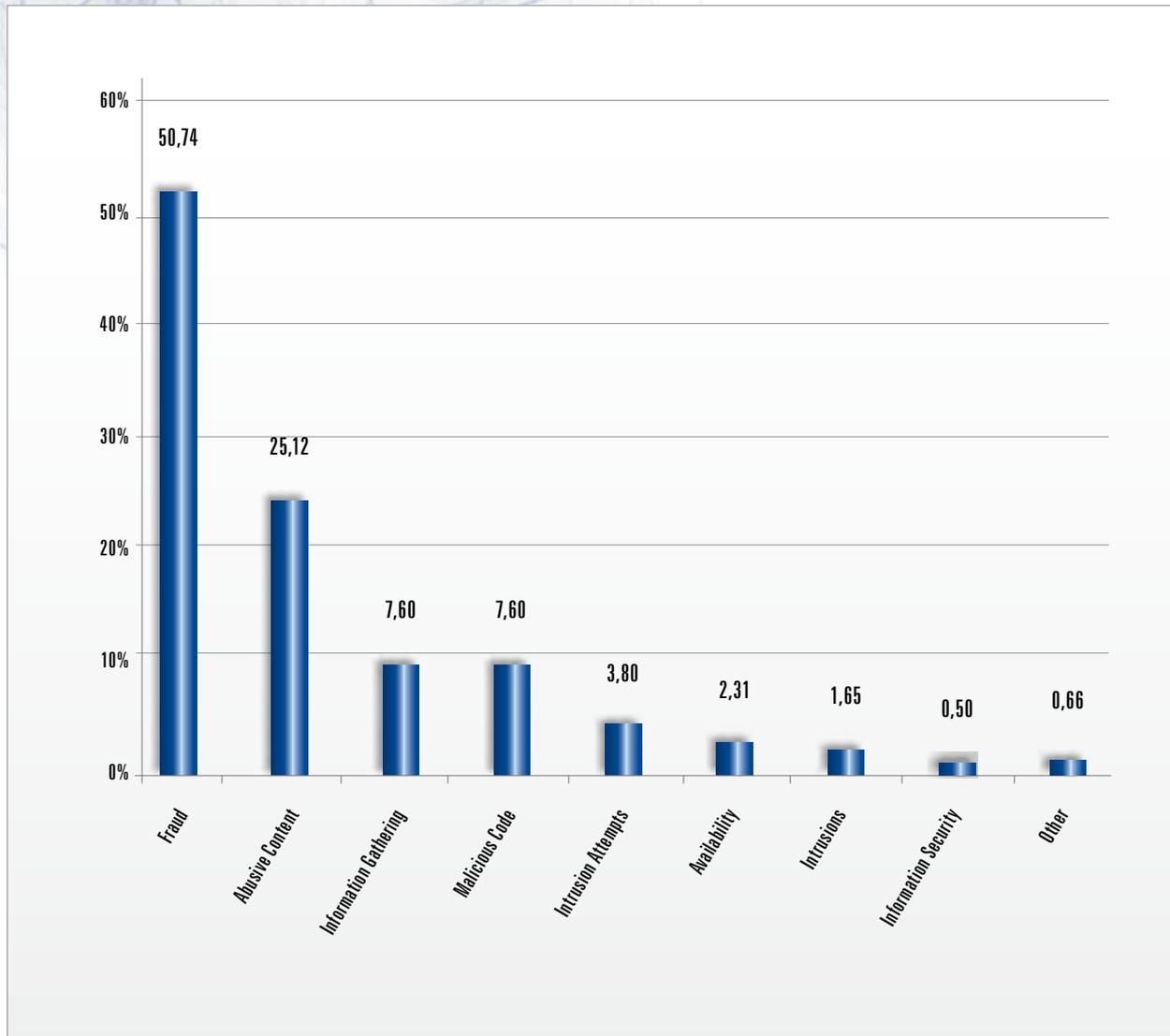
Chart 5.2.1. Incidents handled by CERT Polska by types

⁵ Reports related to abusive content – as defined by Polish law – are forwarded to the [Dyzurnet.pl](http://www.dyzurnet.pl) team, also operating within NASK (<http://www.dyzurnet.pl/>)



5. Statistics of incidents handled by CERT Polska

5.3 Types of attacks recorded

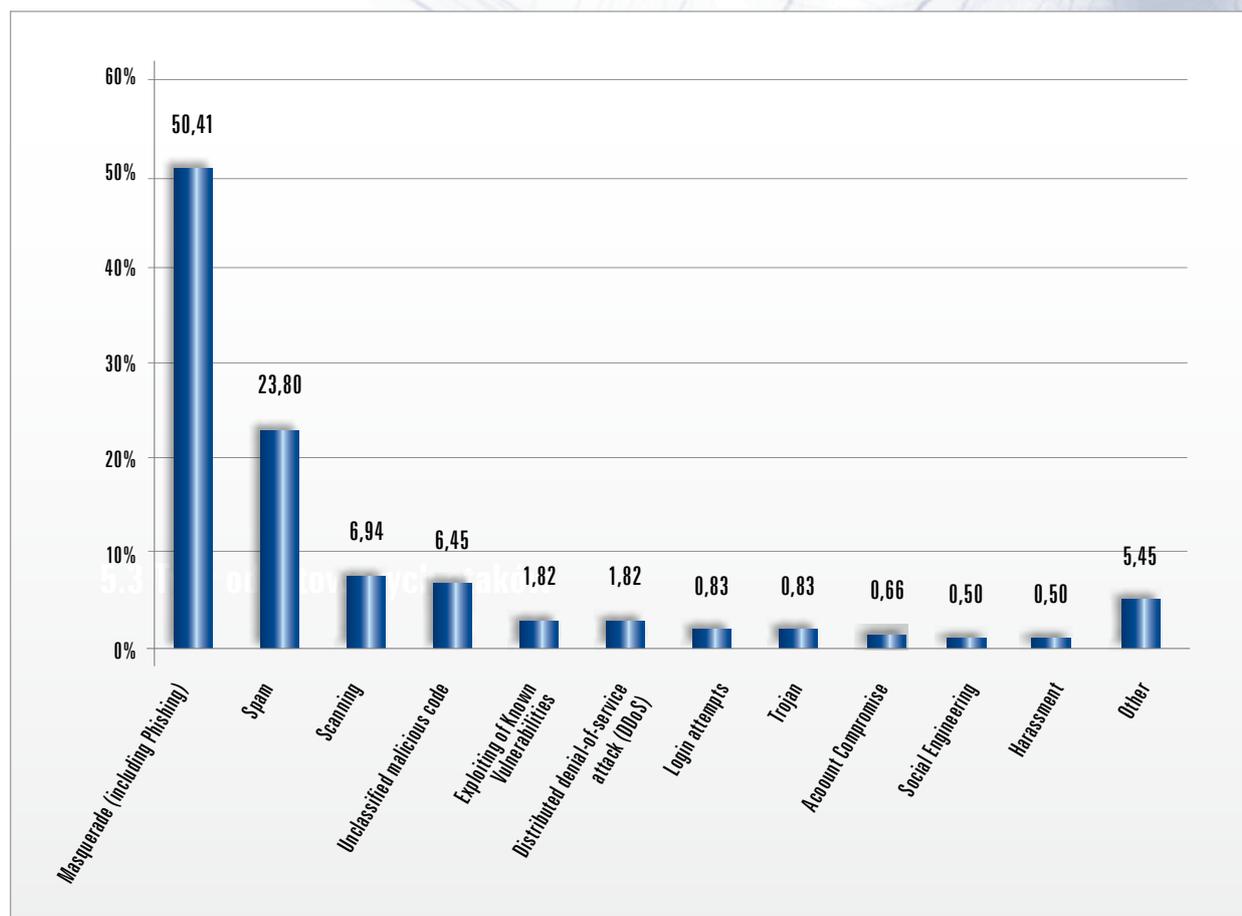


Graph 5.3.1. Percentage distribution of incident types.

Like in the previous year, the most common type of incident was *Fraud* (50.74 %). It should be emphasised that in 2011 we recorded one-third more than in 2010 (38.5 %). Mostly, submissions included threats related to *Masquerade*, especially those related to *Phishing*. *Fraud* has become the dominating type of incident. Ranking second is *Abusive Content*. Such incidents represented 25.12% of the registered cases.

The most frequent incidents in this category were related to sending spam. Ranking third ex aequo were *Information Gathering* and *Malicious Code* (7.6% each). Both types have smaller share than last year. *Malicious Code* share decreased by 5.9%, while *Information Gathering* by 2.19 %.

5. Statistics of incidents handled by CERT Polska



Graph 5.3.2. Percentage split of incident subtypes.

In the case of incident subtypes, the most frequent one was *Masquerade* (50.41%). This represents growth by one-third compared to 2010. Practically all incidents submitted were related to *Phishing* located on Polish servers. The victims were usually foreign financial institutions. We recorded 29 cases in relation to Polish entities. 23.8% of the incidents were related to *Spam*. Those were mostly submissions from SpamCop, relating to Polish computers sending unsolicited commercial offers.

Ranking third and fourth, we recorded respectively *Scanning* (6.49%) and *Unclassified malicious code* (6.45%). Compared to 2010, it is worth mentioning that incidents related to *Unclassified malicious code* decreased by half.

5.4 Submitters, victims, attackers

Three categories of entities are recorded for statistical purposes in relation to incidents: party submitting the incident, the party which fell victim in the incident, and the party responsible for the attack.

Additionally, those categories are broken down by domestic and foreign entities.

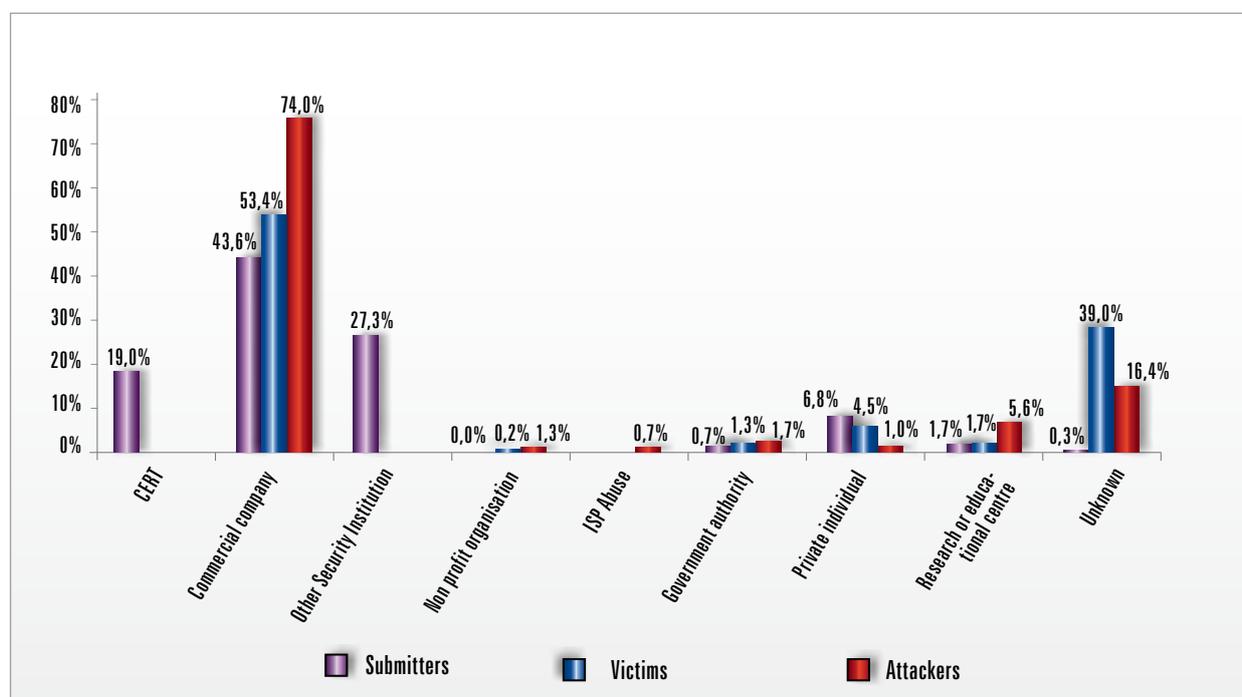
The chart 5.4.1 presents general data on the entities taking part in incidents.



5. Statistics of incidents handled by CERT Polska

Private individual	Submitters	%	Victims	%	Attackers	%
Private individual	41	6,78	27	4,46	6	0,99
CERT ⁶	115	19,01	0	0,00	0	0,00
ISP Abuse	4	0,66	0	0,00	0	0,00
Other Security Institution	165	27,27	0	0,00	0	0,00
Commercial company	264	43,64	323	53,39	448	74,05
Research or educational centre	10	1,65	10	1,65	34	5,62
Non profit organisation	0	0,00	1	0,17	8	1,32
Government authority	4	0,66	8	1,32	10	1,65
Unknown	2	0,33	236	39,01	99	16,36
Domestic	126	20,83	80	13,22	520	85,95
Foreign	478	79,01	299	49,42	13	2,15
Unknown	1	0,17	226	37,36	72	11,9

Chart 5.4.1. Types of entities included in the classification of incidents



Graph 5.4.2. Sources of submissions, attacks and victims

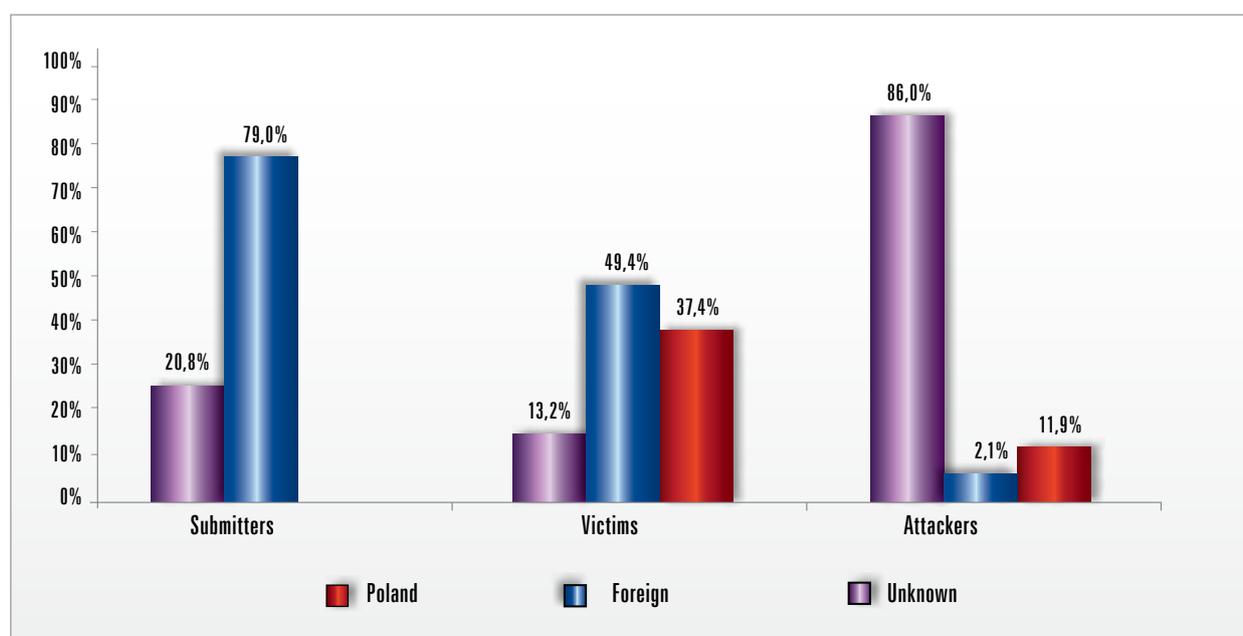
⁶Includes submissions for automated systems that are handled manually - including for the ARAKIS system <http://www.arakis.pl/>

5. Statistics of incidents handled by CERT Polska

In 2011, most submissions were received from *Commercial companies* (43.6%). These were mostly related to *Phishing* and were sent by financial institutions of entities representing them. 27.3% of the incidents were submitted by *Other security institutions*. Most of them were from SpamCop and related to spam being sent by Polish Internet users. 19% of the submissions were from other CERT teams. Usually, they were related to *Phishing*.

In over half of the cases (53.4 %) the *Victims* were *Commercial companies*. Usually, they fell prey to *Phishing*. In 39%, the *Victims* were *Unknown*. This is a result of submissions relating mostly to *Spam* and *Scanning*, which were sent by *Submitter* (e.g. SpamCop) on behalf of third parties.

In as many as 74% of cases, the attacker was a *Commercial company*. This result is largely influenced by local Internet providers and hosting companies. CERT Polska usually holds no information on end users, local provider, or on the owner of a website located in hosting farm. In that case, the attacker is assumed to be the last known entity, i.e. *Commercial company*. Usually it hosted *Phishing* and sent *Spam*. 16.4% of the *Attackers* remained unknown. Like in the previous years, they were hidden behind a Proxy server, botnet, TOR or compromised machines of unaware victims.



Graph 5.4.3. Location of submitters, victims, and attackers.

In 2011, 79% of the Submitters were from abroad. This is a result of a large amount of incidents related to *Phishing and Spam*, which were submitted by foreign entities. In only one-fifth of the cases, the *Submitter* came from Poland.

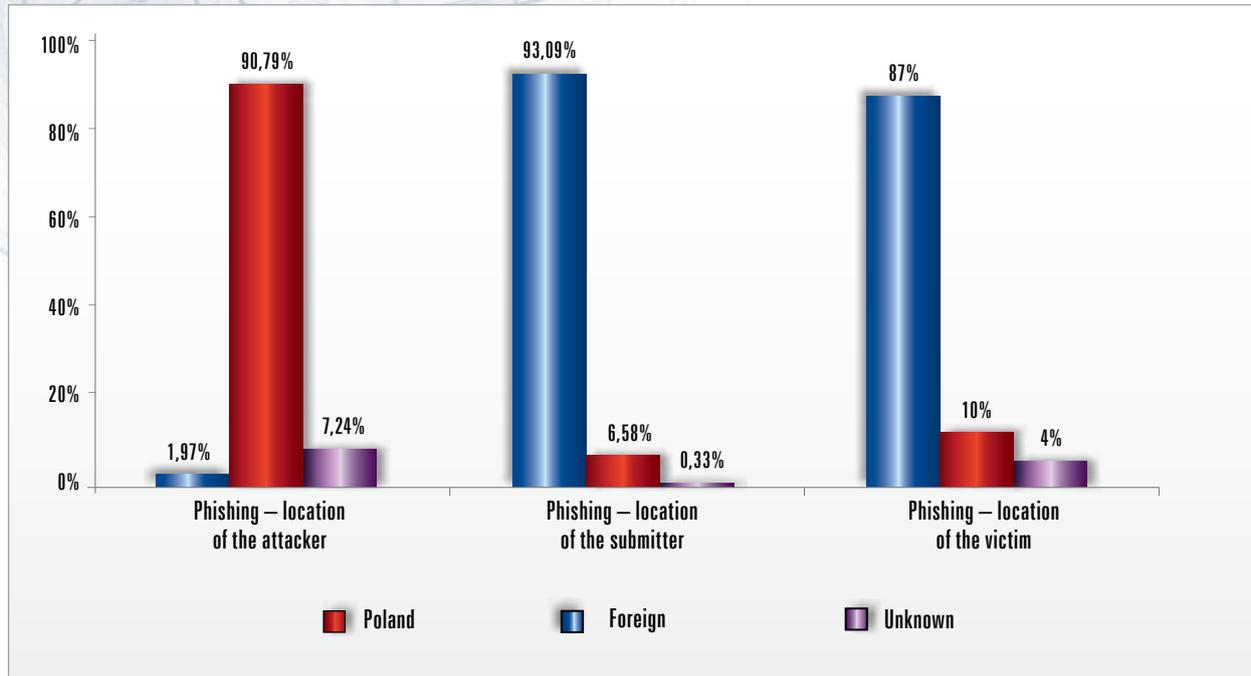
Almost half of the *Victims* were located abroad. Most of them fell prey to *Phishing*. In 37.4% of the cases, the location of the *Victim* was unknown. This is a result of the submissions mentioned ear-

lier, submitted through e.g. SpamCop on behalf of third persons. Only 13.2% of the *Victims* were from Poland.

In the case of *Attackers*, as many as 86% of them came from Poland. This is a natural consequence of managing submissions for .pl domain. Only 11.9% of the *Attackers* were located abroad. These were mainly involved in incidents related to hosting *Phishing*.

6. Additional statistics related to submissions handled manually

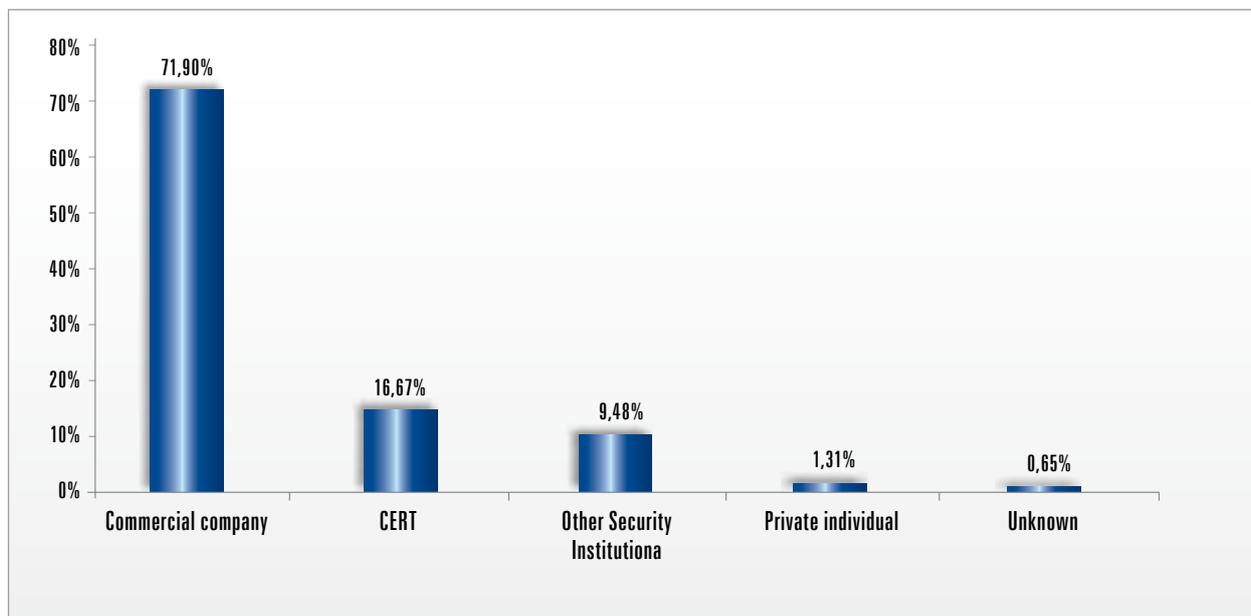
6.1 Phishing in 2011



Graph 6.1.1. Phishing – location of the attacker, submitter and victim.

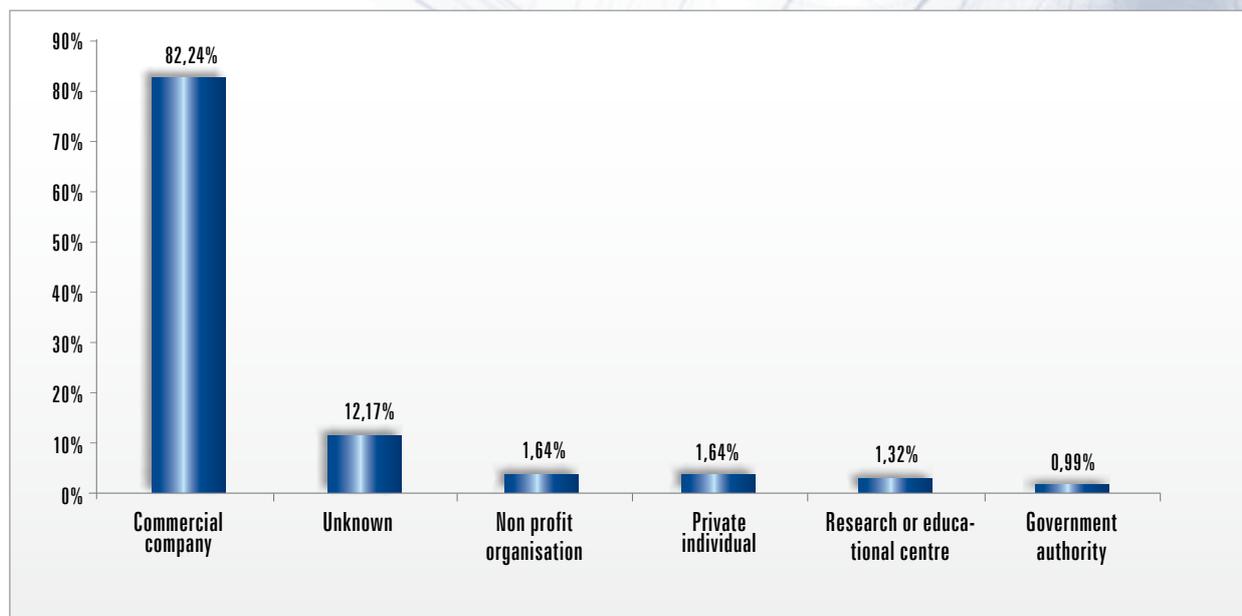
As we mainly receive submissions related to Polish networks, the most common incident was related to *Phishing* on Polish servers. It represented 90.97% of the total. Most of the submitters were located

abroad (93.09%). Most often, the victims were also foreign entities (87%). Only 10% of the incidents were related to Polish entities.



Graph 6.1.2. Phishing – submitters

6. Additional statistics related to submissions handled manually



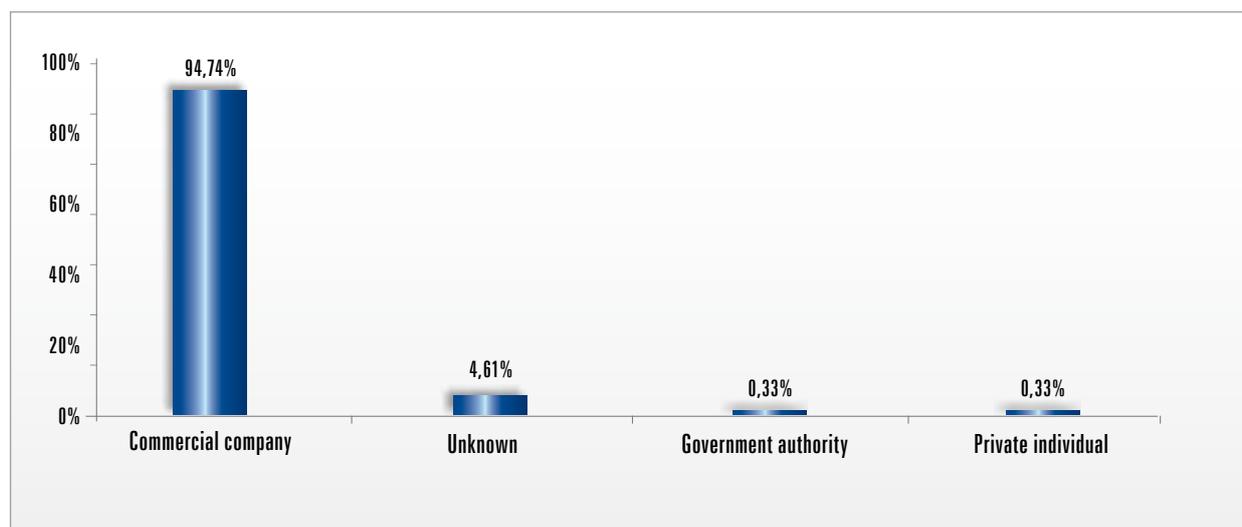
Graph 6.1.3. Phishing – attackers

Phishing was most often submitted by *Commercial companies* – in 71.9%. These were mainly attacked financial entities or companies representing them. 16.67% of the submissions were from CERT teams. 9.48% of the incidents were submitted by *Other security institutions*.

Most of the attackers were *Commercial companies* (82.24%). These were usually cases of Phishing on servers of companies providing hosting services. In over 12% of the cases, we were unable to determine the identity of the attacker. These were

usually machines hosting exclusively the web page that impersonated a trusted web page of another institution, and the record in ripe.net database included only ISP data.

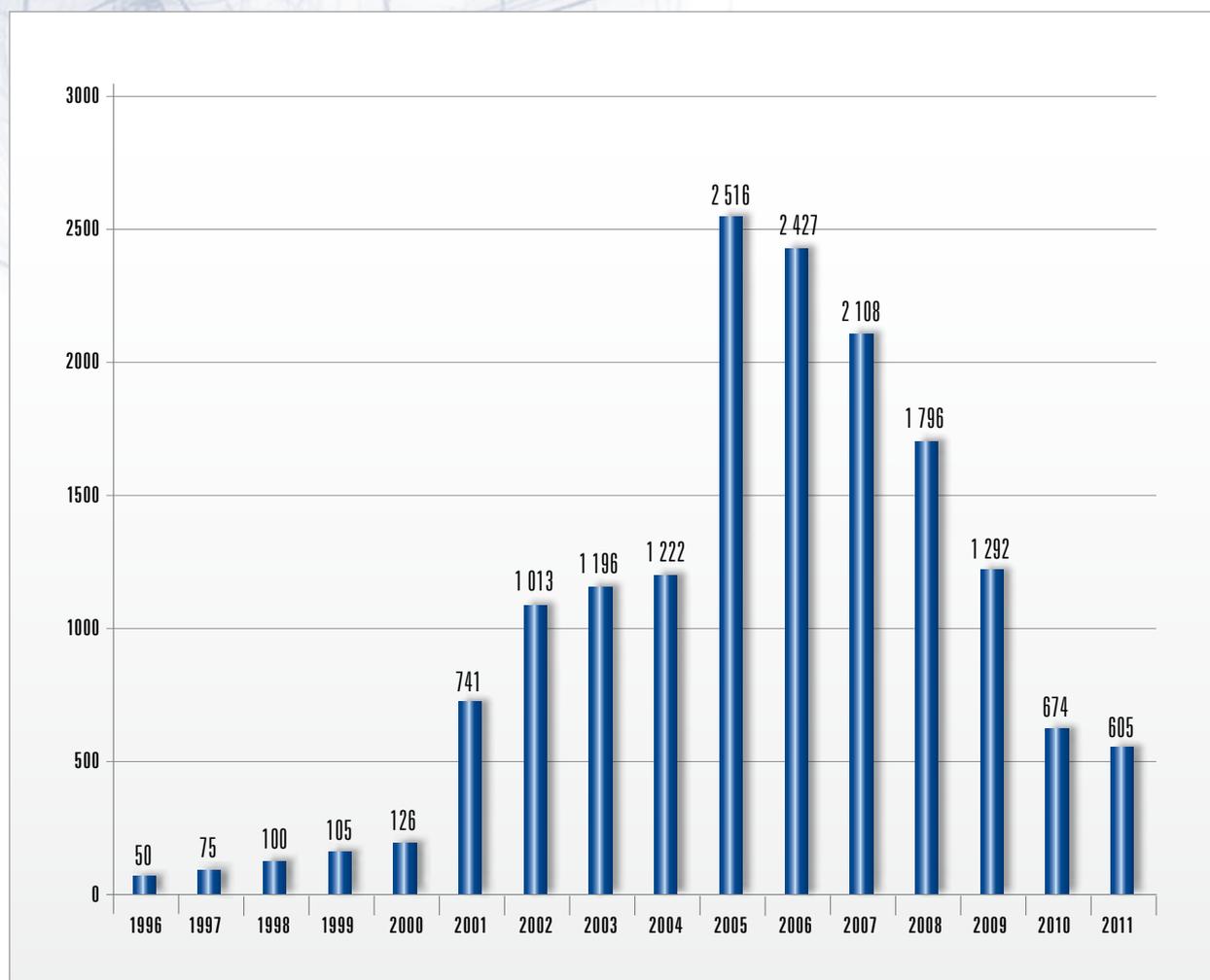
As many as 94.74% of the victims were *Commercial companies*. These were mainly foreign financial entities. In 4.61%, the victim was unknown. This means that when handling the submission, the fake website had already been blocked, and the content of the submission did not indicate a specific entity.



Graph 6.1.4. Phishing – victims

7. Trends in the following years

7.1 Number of incidents in years 1996 - 2011



Graph 7.1.1. Number of incidents handled manually in the years 1996 - 2011

Another year in a row, we recorded a lower number of incidents handled manually. For several years we have been noticing a decline in number of incident reports. In many cases, the reports are sent directly to network owners. Quality of incident handling by large ISPs, CSPs and hosting companies is increasing each year. Because of that, the number of requests for help recorded by CERT Polska caused by lack of response from them

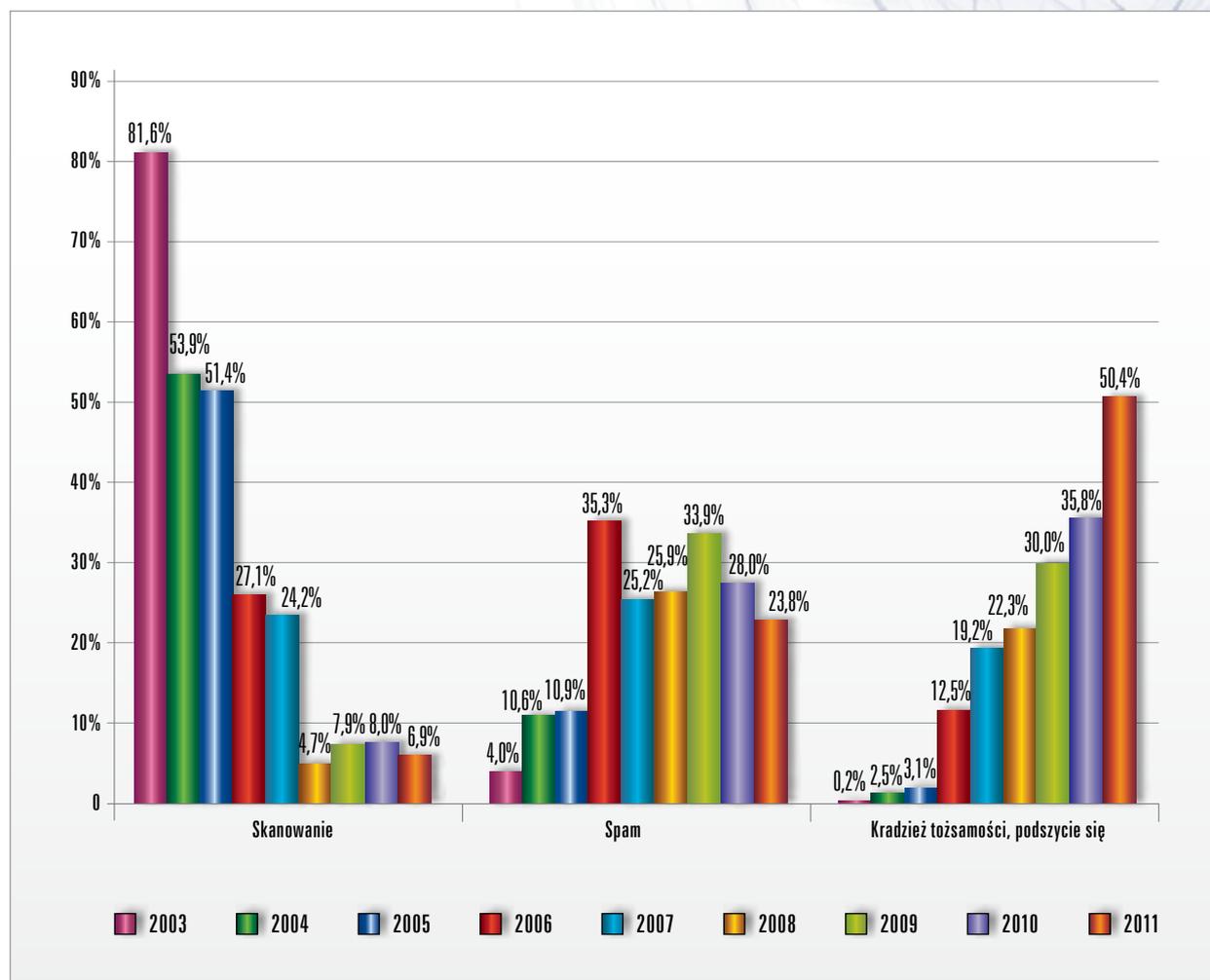
is decreasing. On the other hand, the incidents are more serious and complex, such as these related to Phishing and Malicious Code, and the process of handling them has become significantly longer. Handling a case related to a controller involved in attacks on customers of Polish banks may take as long as a few weeks.

7. Trends in the following years

7.2 Percentage split of incident sub-types in years 2003 - 2011

Since 2003, the statistics are based on the same classification. This allows us to compare the per-

centage share of incidents over time (see graph below).



Graph 7.2.1. Percentage split of incident subtypes that are handled manually in the years 2003 - 2011

In 2011, the trends observed in the previous years did not change significantly. Scanning is still marginal compared to 2003-2005. For several years, it has remained at the level of a few percent. In case of Spam, for several years we have not recorded large increases or declines. Regardless, Spam invariably represents a significant number of incidents. Additionally, it should be emphasised

that the scale of the issue is much larger (see: 4.5). CERT Polska records only submitted cases of spam sent by machines within the .pl domain. An evident growth can be still observed in incidents related to *Masquerade*. This is currently the most common incident. Compared to 2010, we recorded a 40% increase in this category.

8. Key incidents according to CERT Polska

This section lists key security-related issues in 2011, in which CERT Polska was directly involved.

8.1 Zeus-in-the-Mobile – ZitMo

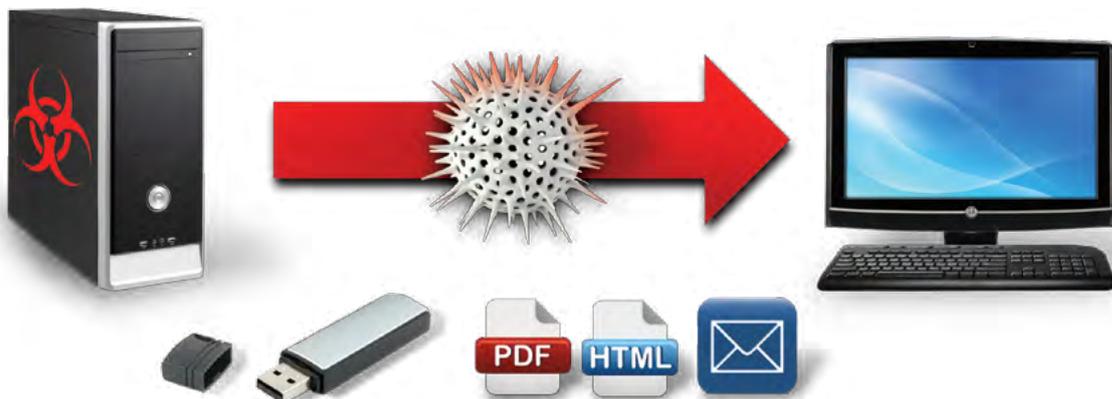


ZeuS is a popular banking trojan. ZITMO, or “Zeus In The MOBILE”, is a new threat that has been affecting customers of Polish banks early 2011.

This is a new variant of Zeus, targeting smartphones as well as PCs. Infecting a mobile device opens new possibilities to malware authors, allowing them to retrieve information from SMS messages such as mobile Transaction Authentication Numbers (mTANs) or SMS notifications from a bank.

How do mobile phones get infected?

1. After installation of malicious software, the attacker takes over control of the victim's computer. We do not know the original source of the infection – we assume there could be multiple ones, e.g. a prepared website, a .pdf file, an infected pendrive or an e-mail with malicious attachment.



2. The malware modifies contents of a legitimate bank website on the victim's computer. A new dialog asking for phone model and number is injected during login process.

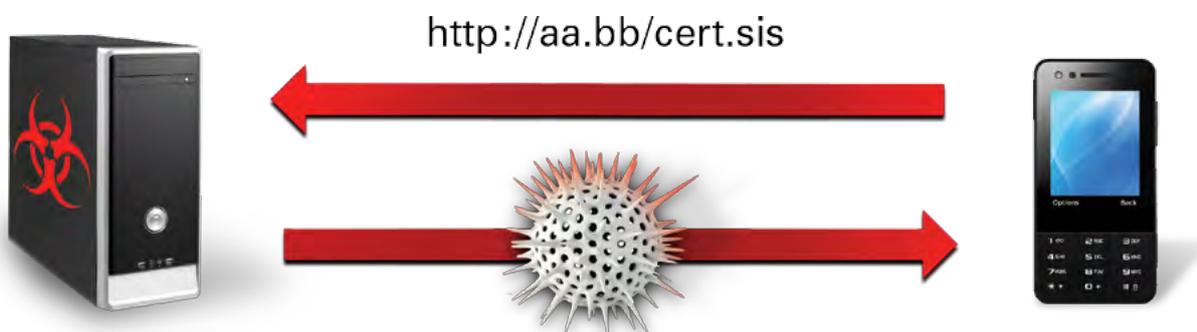


8. Key incidents according to CERT Polska

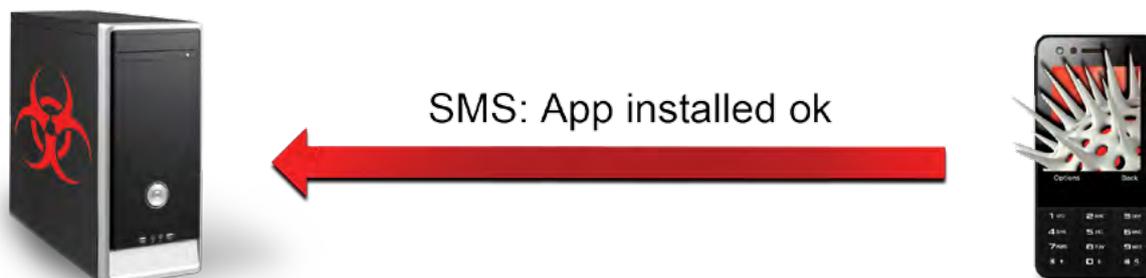
3. Once this information is obtained, the attacker automatically sends an SMS with a link to malicious software dedicated for the victim's smartphone.



4. The unaware user follows the link, ultimately gets the malware installed on their smartphone.



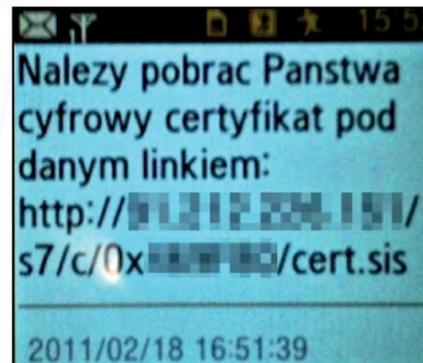
5. The infected smartphone sends an SMS back to the attacker to report a successful installation. From this moment the attacker can fully control both the PC and the smartphone of the victim.



8. Key incidents according to CERT Polska

Who can be a victim of ZITMO?

The following link contains a complete list of smartphones currently targeted by ZITMO: <http://www.cert.pl/wp-content/uploads/atakowanetel.html>. It includes phones running BlackBerry, Symbian or Windows Mobile operating systems. The message sent to a user during infection phase claims to contain a link to a “digital certificate” which ends with “cert.jad”, “cert.sis” or “cert.cab”, depending on the platform.



How to avoid getting infected (and avoid losing money)?

Be alert when logging in to your bank’s web interface. Watch out for unexpected dialogs and requests for information that the bank never

requested before (such as PIN numbers, mobile phone model, unnecessary TAN numbers etc.). When not sure, contact your bank immediately.

Screen requesting for providing phone number and selecting the make and model.

More information on the malware

When successfully installed on a smartphone, the application sends an SMS “App Installed OK” to a predefined phone number. All the malware we have seen contacts the same numbers starting with +4477. It is different from the number used in the September attacks in Spain just by a few digits. It should be noted that both the PC-infecting malware and its configuration files carry a 3.1 version number, which may indicate that a new version of Zeus has appeared.

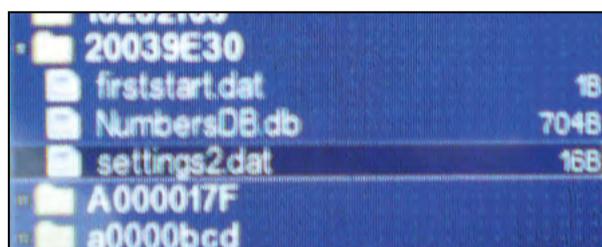
CERT Polska is investigating both the PC and the smartphone version of Zeus. After installation on the phone, the application (without the owner’s knowledge) sent an SMS reading “App Installed OK” to a defined phone number. All samples held by CERT Polska have the same phone number indicated. It started with 44778148**** and was registered in Guernsey. Below, we present short descriptions of how the software works on each of the platforms affected.

8. Key incidents according to CERT Polska

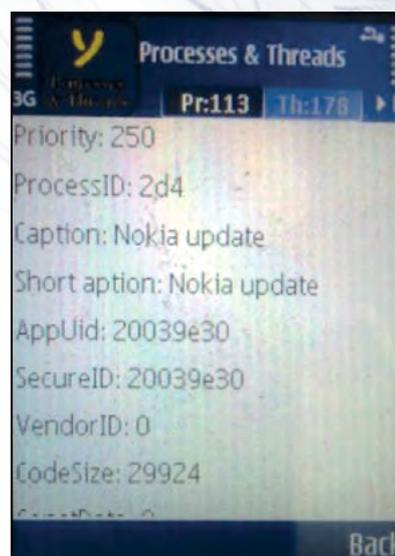
8.1.1 Symbian

Phones running Symbian received an SMS with a link to file cert.sis. After installation, malware created a process called "Nokia update" (picture on the right). It saved the following files in the phone's memory (picture below):

```
C:\private\20039E30\firststart.dat
C:\private\20039E30\NumbersDB.db
C:\private\20039E30\settings2.dat
```



They stored information on the settings and numbers that should be tapped by the Trojan.

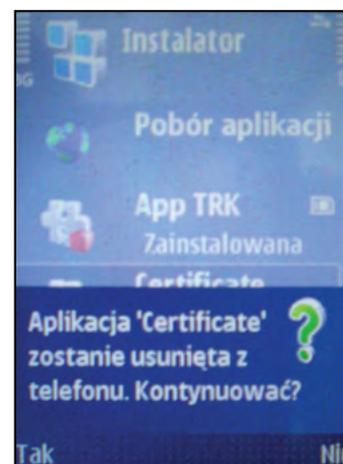
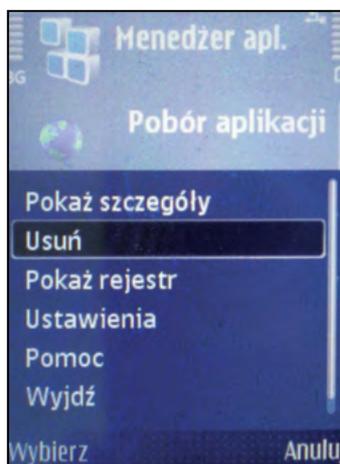


Uninstall

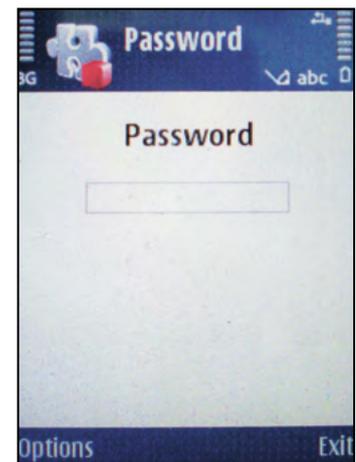
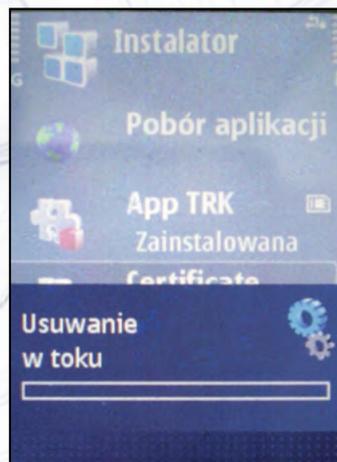
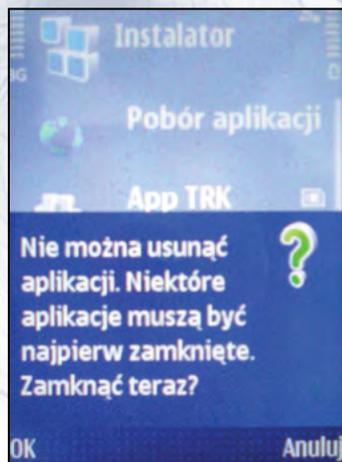
To uninstall malware, open application manager and find application "Certificate". Next, select Delete from context menu and confirm.

If a warning pops up to close the running applications, confirm (OK). After starting the process of

removing the application, a window will be displayed, asking for a code/password. This number is encoded in the malware. The code allowing to remove the malware (in case of February 2011 infection) is: **45930**



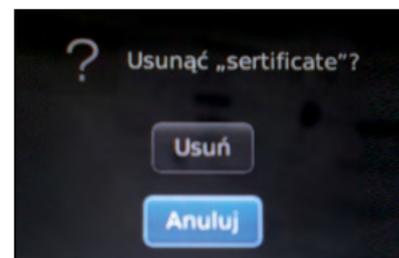
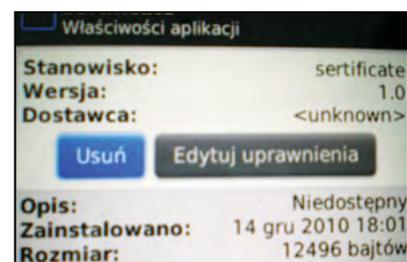
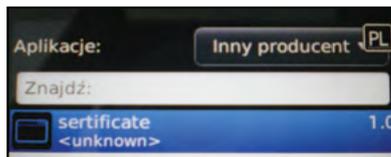
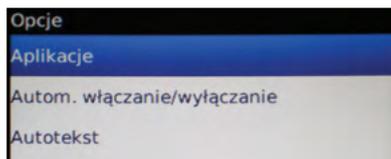
8. Key incidents according to CERT Polska



8.1.2 BlackBerry

The package infecting blackberry platform was sent in file "cert.jad". After opening, one of the following files was downloaded and installed: "sertificate.jar"

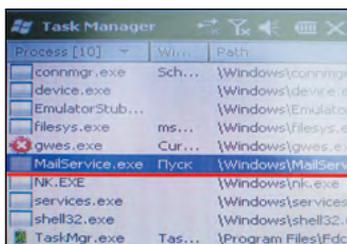
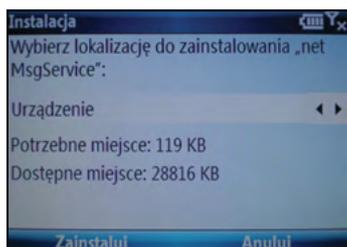
or "sertificate.cod". After installing, the application is displayed in menu "Options -> Applications" under name "sertificate". After selecting the item with the application, a window allowing to review detailed information on the application is displayed. In the same window, we can also remove the unwanted software by selecting "Delete". Only a confirmation message will be displayed. After completing the operation, the user regains control over the phone.



8. Key incidents according to CERT Polska

8.1.3 Windows Mobile

In the case of phones with Windows Mobile operating system, the installation file with malware was called cert.cab. During installation of ZITMO it was presented as "net MsgService". After installing, malware saved the settings in four files: settings.xml, senders.xml, listnumbers.xml, messages.xml. The malware itself was installed in file c:\Windows\MailService.exe. After launching, the program was not visible in the standard (built in) process manager. Only installing additional software allowed to detect the malware working in the background. What is interesting, the title of the main window related to the malware process was written in Cyrillic alphabet (see the photo). Unfortunately, the software is also not visible in the list of applications installed, making it much more difficult to remove the malware.



Its main purpose is stealing confidential information entered by the user on-line (including in e-banking systems). After opening the document and installing malware, the victim's computer connected to C&C server located under address u-buntu.com. After several days, the infected victims were directed to a new controller server, which seemed to operate as part of a larger botnet.

What did the malicious message look like?

The e-mail message had the following fields:

Subject: Your Order No ##### | Puremobile Inc.

Sender: PuremobileInc

Attachment: Order_#####.pdf

The samples analysed had content in Polish [*original quoted here*]:

Dziekujemy za zamowienie

Twoje zamowienie zostalo przyjete.

Numer zamowienia 123-123456789.

Bedziesz musial podac ten numer w korespondencji.

Wybrales opcje platnosci karta kredytowa.

Twoja karta zostanie obciazona oplata w wysokosci 1234,00 EUR.

Oplata za zamowienie bedzie opisana na wyciagu bankowym z karty kredytowej jako „Puremobile Inc.”

Ta wiadomosc nie jest dowod zakupu Po otrzymaniu przez nas potwierdzenia tej wpłaty, wyslemy Ci list zwrotny. W zalezności od tego jaka forme wysyłki wybierzesz otrzymasz go wprost na swój adres e-mail lub na adres domowy.

The message included an English translation as well:

Thank you for ordering from Puremobile Inc.

8.2 SpyEye in PDF



Thanks to the cooperation of many Polish operators' security teams, under the Abuse-Forum initiative, a new threat was detected and analysed. In the early April of 2011, Polish Internet users received an e-mail

with a malicious PDF document. After opening it, the computer was infected with SpyEye spyware.



8. Key incidents according to CERT Polska

This message is to inform you that your order has been received and is currently being processed.

Your order reference is 123456789. You will need this in all correspondence.

This receipt is NOT proof of purchase. We will send a printed invoice by mail to your billing address.

You have chosen to pay by credit card. Your card will be charged for the amount of 1234.00 USD and „Puremobile Inc.“

will appear next to the charge on your statement.

Your purchase information appears below in the file.

Puremobile Inc

Detailed analysis of the malicious PDF document.

After opening the attached PDF document, Adobe Reader starts to load and process it. The structure of a PDF document is an object tree, with one Root object. Adobe Reader processes subsequent objects in line with their sequence and position within the tree structure. Some objects are JavaScript scripts, which can be executed by ESript engine (JavaScript engine by Adobe). To examine a PDF document and display the objects included in it PDFID program can be used (Figure 8.2.1).

At first glance it seems this document contains no JavaScript objects. That is not true though, as the scripts are hidden in compressed streams. They are usually darkened and difficult to interpret. Such is the case here (a fragment of decompressed code is shown in the Figure 8.2.2 below).

The script hidden in the compressed stream becomes decompressed and executed. It is used to

```
PDFID 0.0.11 ./malicious.pdf
PDF Header: %PDF-1.5
obj          54
endobj       54
stream       20
endstream    20
xref         1
trailer      1
startxref    1
/Page        1
/Encrypt     0
/ObjStm      0
/JS          0
/JavaScript  0
/AA          0
/OpenAction  0
/AcroForm    1
/JBIG2Decode 0
/RichMedia   0
/Launch      0
/Colors > 2^24 0
```

Figure 8.2.1. Analysis of PDF document

```
function ttt4(zv, zt) {
    return ttt5(zv, zt);
}

function ttt5(zv, zt) {
    return f9FDCA5(zv, zt);
}

function f9FDCA5(zv, zt) {
    var c, gv, j, gf, zi, r, qd, qe, gm, qf, k, gm, qk, ql, v, qt, gp;
    p = 0.003;
    p++;
    q = 'XYiQBtme';
    g = 'seg';
    z = null;
}
```

Figure 8.2.2. Fragment of JavaScript code

8. Key incidents according to CERT Polska

Figure 8.2.3. AcroForm library code during execution

include a shellcode in the memory, using the “heap spray” technique. After the intrusion occurs, (by using the vulnerability in PDF reader), the victim’s processor starts executing the code.

How exactly is control taken over the processed code? AcroForm.api library has an error which caters for it. When processing AcroForm object (listed in pdfid programme – Figure 8.2.1), the procedure performed ends prematurely, which allows to jump to library icucnv34.dll (Figure 8.2.3).

The library will be used by ROP-type exploit (we wrote on that type of exploit in Dec 2010 article, under the link: <http://www.cert.pl/news/3078>), which previously was loaded to memory by the mentioned JavaScript.

What are the consequences of the malicious code being executed? We tested it by controlled opening of the document using a laboratory computer. Exploit loads system libraries (Figure 8.2.4 – on the right hand side) needed to transmit in the Internet and tries to connect from the attacked computer

to the remote server. After connecting, it downloads and runs an EXE file. It is SpyEye trojan, which is used to surveil the victim’s computer and steal data (e.g. e-banking passwords).

Figure 8.2.4. Loading of new libraries

How to safeguard against such attacks?

To safeguard against such type of attacks, several rules must be adhered to. Primarily, attachments in e-mails from unknown persons must not be opened. Of course, sometimes, we may receive an e-mail from known persons who have been infected. In such a situation, the e-mail must be scrutinised for suspicious content. Additionally, it is a good practice to disable JavaScript in Adobe Reader (Figure 8.2.5).

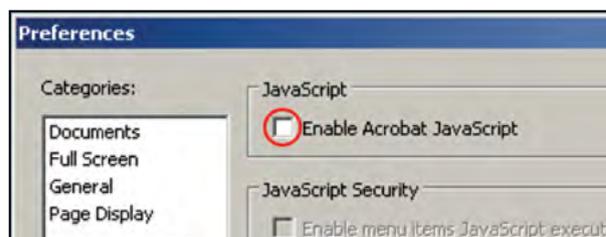


Figure 8.2.5. Disabling Acrobat JavaScript



8. Key incidents according to CERT Polska

If in the future Adobe Reader asks for permission for executing JavaScript included in a document, we may decline (Figure 8.2.6).



Figure 8.2.6. Dialog box asking whether to allow for JavaScript execution

8.3 Zeus – P2P + DGA variant – mapping out and understanding the threat



In the autumn of 2011 we observed new malware infections, which looked similar to Zeus. Subsequent analysis of the malicious software mechanism start up, the process of hiding and storing of configuration indeed verified that it was Zeus. However, monitoring of infected machines failed to uncover the characteristic communication with a C&C. After closer examination it appeared that the sample was probably a new version based on the source code of Zeus that was accidentally made public.

In the new version of the Trojan, the authors focus on eliminating the weakest link – a centralized system of information distribution. Previous versions of Zeus were based on one (or few) predefined addresses which were used for botnet management. This allowed for relatively easy tracking and blocking of servers, thus rendering the botnet useless. However, the analysed variant of the Trojan used two new channels of communication to receive orders (Figure on right):

1. Communication in a peer-to-peer network,
2. Domain Names Generation mechanism.

This variant has been analyzed to some extent by other researchers before – there is information on the web on the new variant of Zeus (eg abuse.ch). However, based on our knowledge, previous

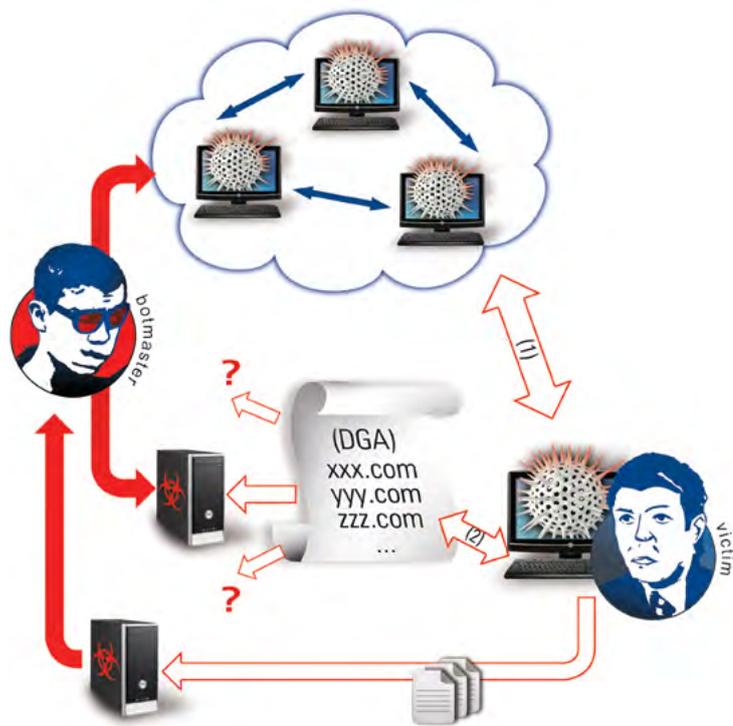


Figure 8.3.1. Visualization of a small fragment of the ZP2P network

research has focused on registering and monitoring traffic to Zeus domains. In our work we focus on understanding the P2P network communication mechanisms, mapping out the network, and monitoring the exchange of information in this particular network.

8. Key incidents according to CERT Polska

Information sharing over the Zeus-peer-to-peer (ZP2P) network

In the case of a model based on central (one – or many) point of management, it is possible to identify machines used for command & control. The new mechanism for distributing information is based on the direct exchange of data among infected computers – a model of communication based on peer-to-peer networks. The fact that there is no central management node in this model makes

it much harder to find which computer is used to distribute new orders – and the blocking of the information exchange channel is virtually impossible. This is well illustrated by the graph in Figure 8.3.2. You can see that the presented network does not contain any central point (single or multiple), and the connections between computers are random.

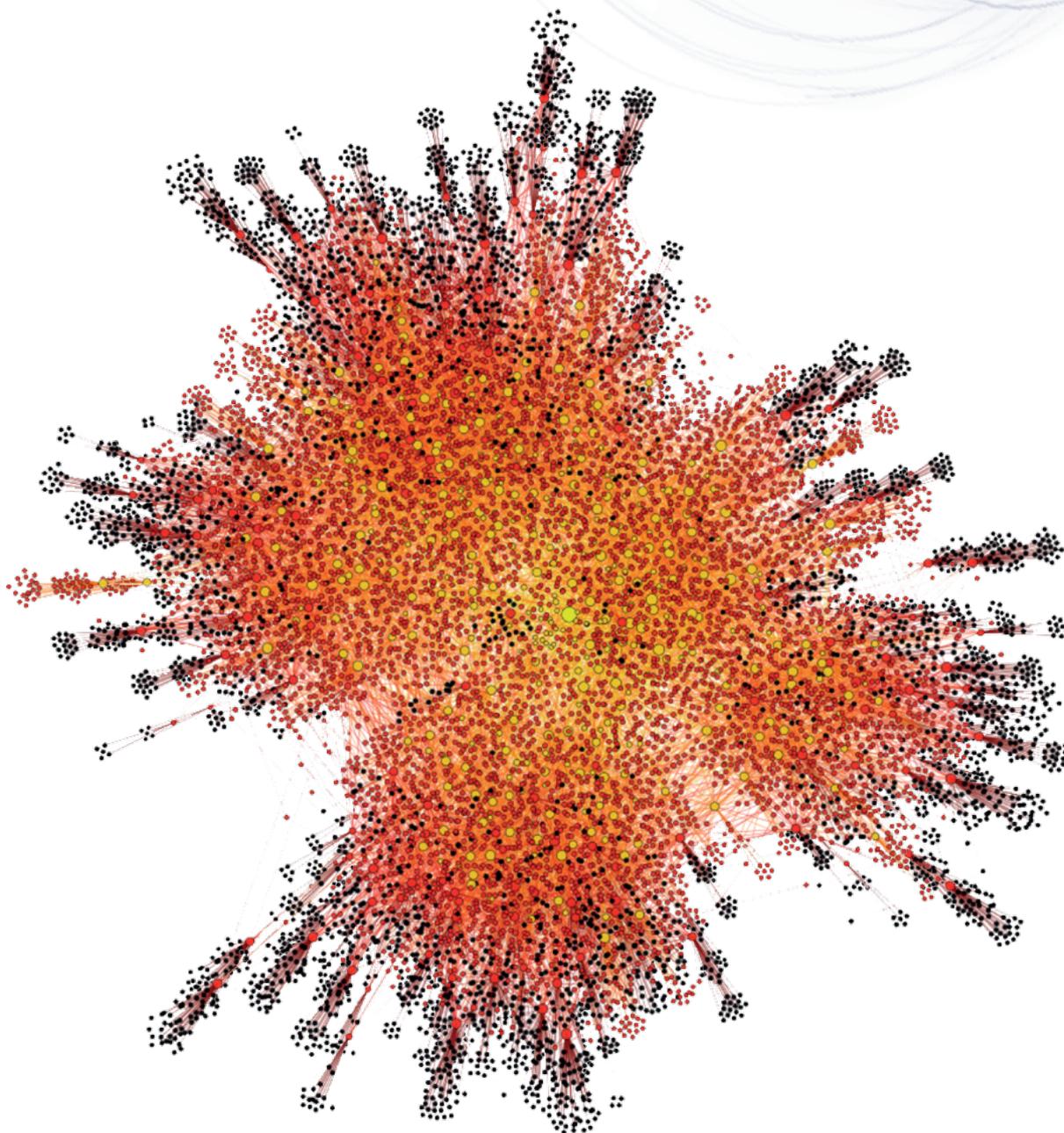


Figure 8.3.2. Visualization of network ZP2P (10 000 nodes)



8. Key incidents according to CERT Polska

How does the ZP2P network operate?

The network most likely is based on the Kademlia protocol standard. A single computer (node) in ZP2P network is identified by a unique identifier UID – which is generated during the first run of malicious software. Each of the computers belonging to the ZP2P has a “table of neighbors” stored in memory. This array contains a list of about 30 neighboring nodes in the ZP2P network – their UID, IP address and UDP port number. This list is used to exchange binary data and information.

In the ZP2P network, we can distinguish two types of communication:

- The exchange of administrative information (using UDP):
 - ▶ (QV) Exchange of information about version of the configuration files
 - ▶ (QN) Exchange of information about the nodes in the “table of neighbors”
- The exchange of binary data (using the TCP protocol)
 - ▶ Distribution of new configuration files

Charts 8.3.3 and 8.3.4 show the distribution of port numbers used for network communication by ZP2P on the network we mapped.

In the case of message type QN, only 10 records from the “table of neighbors” are sent back to client. This type of communication is dedicated for updating the local “table of neighbors”. After the query type QN, the bot saves information about nodes with UID similar to the bot’s own UID (XOR metric) on a local computer.

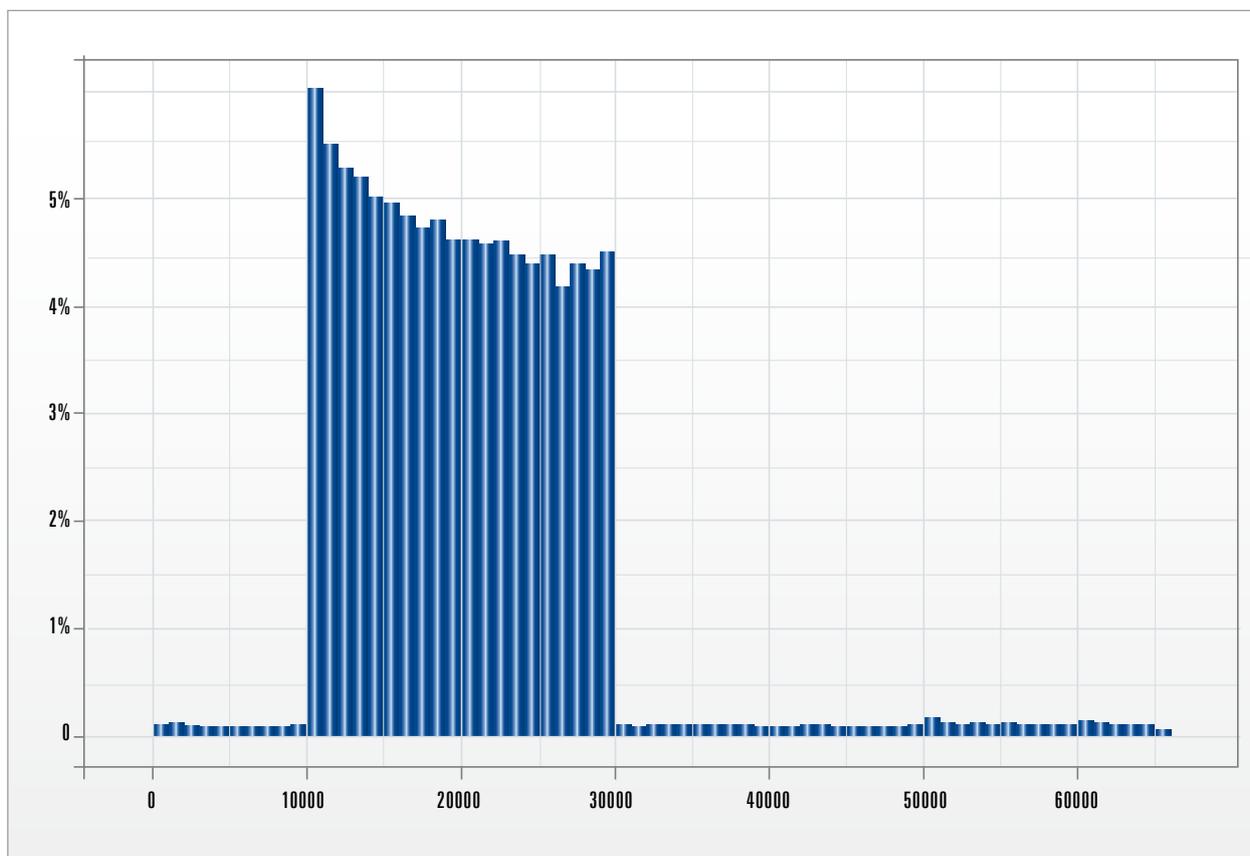


Chart 8.3.3. Distribution of UDP port numbers in the ZP2P network (800 000 samples)

8. Key incidents according to CERT Polska



Chart 8.3.4. Distribution of TCP port numbers in the ZP2P network (100 000 samples)

Messages of type QV are used to check for and propagate new versions of configuration files. If the node that performed the QV query has an older version of the configuration than the version given in response to this query – the bot performs a TCP connection to a remote computer asking for a newer version of the configuration.

Charts 8.3.5 and 8.3.6 show the distribution of the number of children and the number of parents in the ZP2P network. The data comes from the analysis of responses to QN queries during a 3 week period. The number of children (the number of entries in “table of neighbors”) may exceed the value 30, because (as already described), the table may be frequently updated.

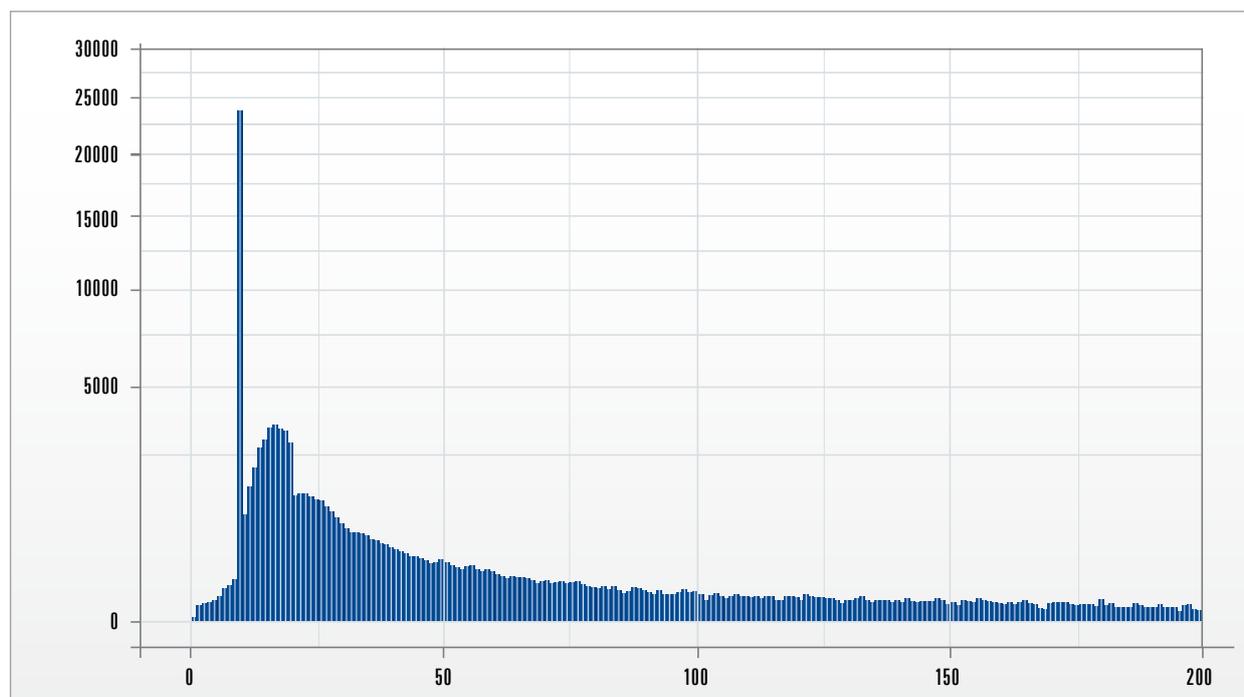


Chart 8.3.5. Distribution of number of children



8. Key incidents according to CERT Polska

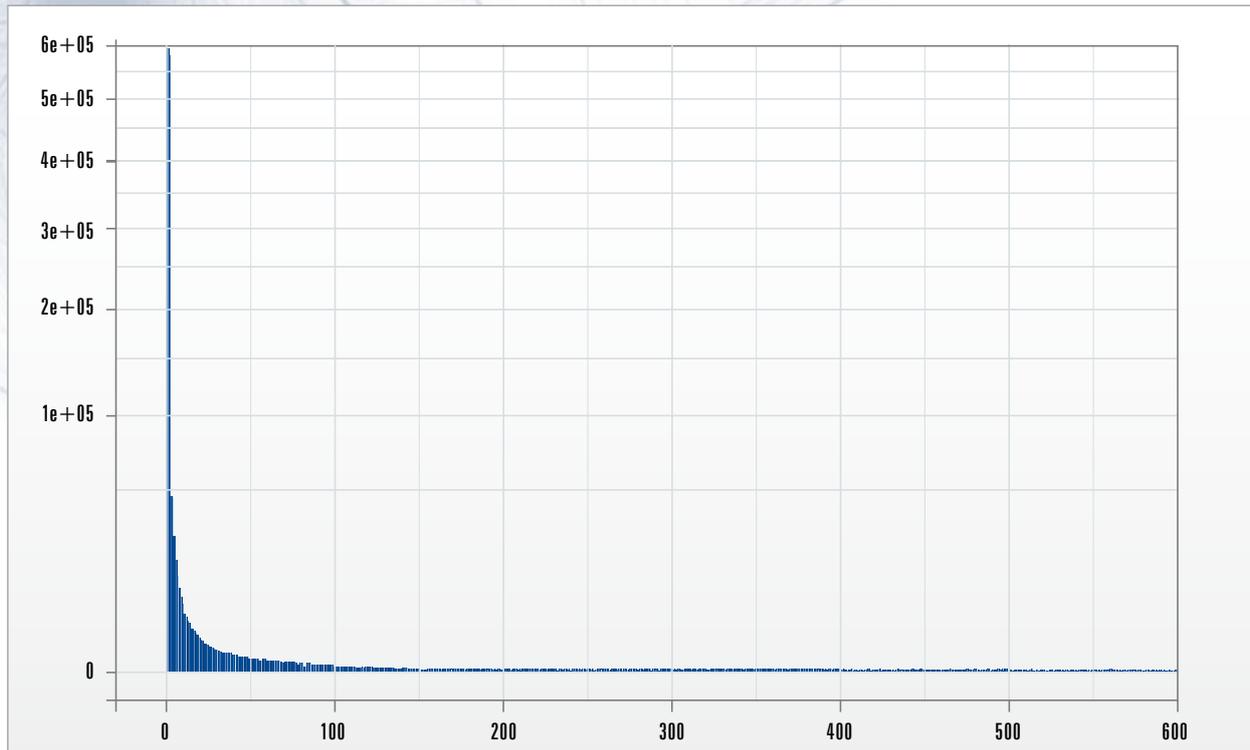


Chart 8.3.6. Distribution of number of parents

ZP2P network monitoring

In the CERT Polska laboratory, we managed to map the ZP2P network by monitoring responses to

QN queries. Collected IP addresses are plotted on a map:

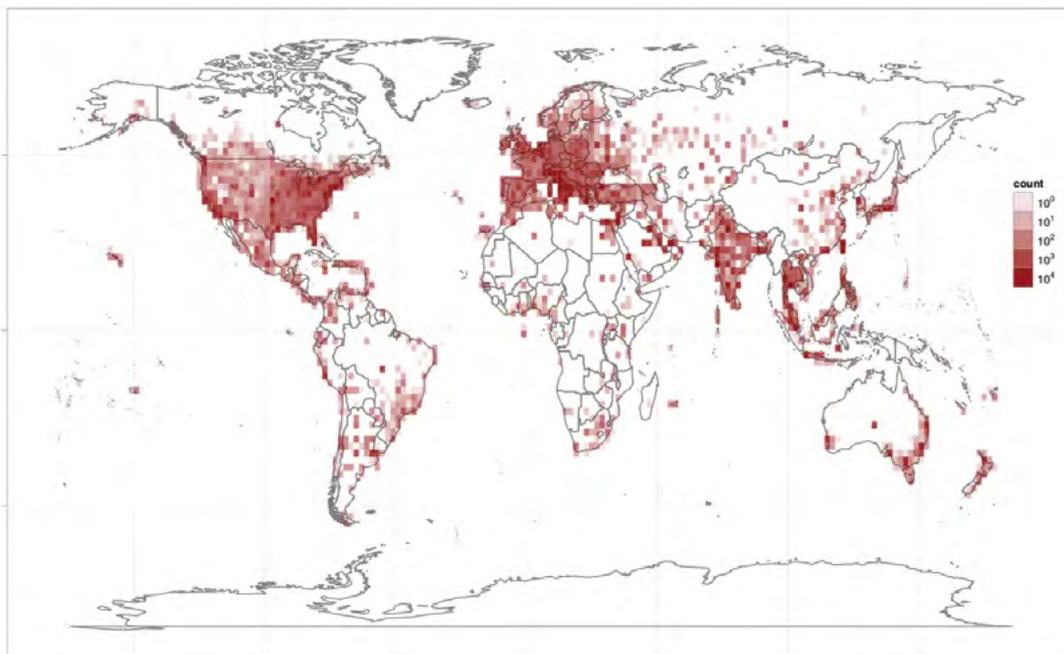


Chart 8.3.6. Map of density of number of computers infected with new variant of the Trojan

8. Key incidents according to CERT Polska

The DGA mechanism

If the communication mechanism of the ZP2P network is blocked (eg by blocking the appropriate TCP and UDP ports on a firewall) – the bot will automatically switch to the backup communication channel – Domain Generation Algorithm (DGA). DGA mechanism is another feature implemented in the new version of the Trojan. It significantly impacts the difficulty of finding and cutting-off of the miscreants behind the botnet. The DGA allows for the generation of a long list of domain names based on specified parameters, and subsequently

of attempts to communicate with each of the generated domains. DGA mechanism parameters are hidden inside the Trojan code – and are known only to the botmaster. The botmaster can manually generate such a list, select one position, register the selected domain, and wait for connection attempts from infected machines.

```
-- # ./dgaToday
DGA list for 2012-01-01 :
id:0000 : bse21b18etduawivfuhugwjwaub68juiulv.ru
id:0001 : l68lscvkwlyc69gsc39c59l18gud60c59n20kqg53.com
id:0002 : h54i25l28i55b28m19l68gvb38o21orh34nwglnrir.net
id:0003 : fro5lowbyhsb48csi65avm39bqf22lygsjzmw.org
id:0004 : d20hynuf32n32nawiy128d10cxm20nnp32a37ny.info
```

Zeus-DGA

In the case of this Zeus botnet, the parameter for the DGA mechanism is calculated from the current date. The list contains over 1000 domains and changes every 7 days. Each name consists of a string with a length of 32 to 48 chars, and one

of TLDs: ru, com, biz, info, net or org. It is worth noting that the domain names do not contain the “-” sign. Below is a regular expression for searching Zeus domains in log files:

```
[a-z0-9]{32,48}\. (ru|com|biz|info|org|net)
```

How to recognise a new Zeus infection?

The presence of a new variant of Zeus on the computer can be identified primarily by monitoring network traffic. As shown in Figure 8.3.8 – by using TCPView, it is possible to see the new open TCP and UDP ports of the explorer.exe process. In addition – to allow communication with the ZP2P network – the Trojan adds new rules to the system firewall. As shown in Figure 7, there are the two new exceptions to allow connections to specific TCP and UDP ports. The range of these ports can be read from Graphs 8.3.2 and 8.3.3.

Proc	Protocol	Local Address	Remote Address	State
explorer.exe	TCP	0.0.0.0:22226	0.0.0.0	LISTENING
explorer.exe	UDP	0.0.0.0:22226	**	LISTENING
explorer.exe	TCP	0.0.0.0:25917	0.0.0.0	LISTENING
explorer.exe	TCP	0.0.0.0:25917	0.0.0.0	ESTABLISHED

Figure 8.3.8. Open TCP and UDP ports used for P2P communication

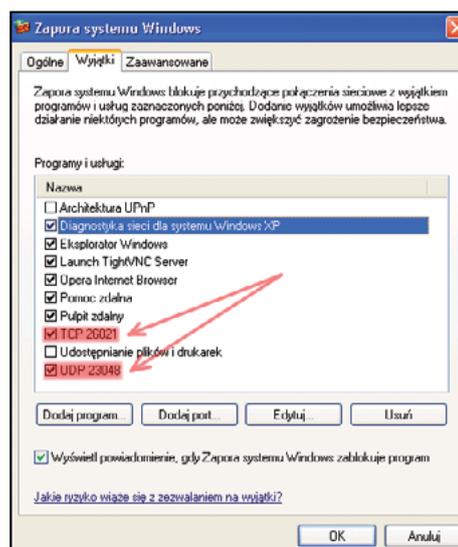


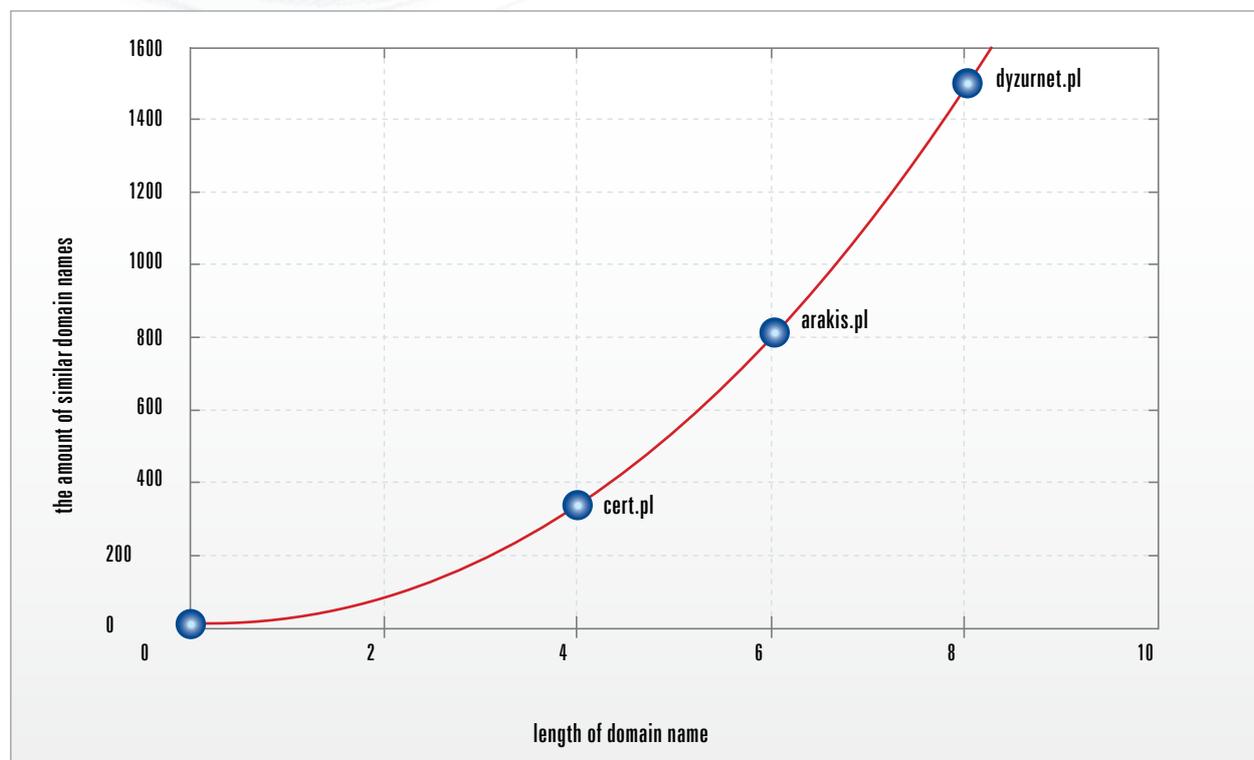
Figure 8.3.7. Added exceptions in the configuration of the system firewall

8. Key incidents according to CERT Polska

8.4 You've won a prize!!!

Typosquatting is based on mistyping the name of a domain an Internet user wants to visit. It is a well known mechanism that has been present for many years. With the increase of popularity of the Internet, registering domains with names slightly differing from the popular ones has become quite a profitable business. There are multiple options of making a typing error when entering an Internet

Domain names with typing errors were generated using simple approaches: replacing a character with another one, next to the correct one in the keyboard, skipping a character, typing the same character twice and a combination of the two approaches mentioned above.



Graph 8.4.1. Number of possible typing mistakes as a function of the length of domain name

address, such as skipping the dot or a single letter, hitting the key next to the correct one or the same character being typed twice. Of course, along with the length of the domain, the chance of making a mistake increases. Graph 8.4.1 presents the number of possible typing mistakes as a function of the length of domain name. For example, the domain for cert.pl can be typed with 341 different typing errors, for domain arakis.pl the number of typing errors increases to 826, while for dyzurnet.pl it is as many as 1502.

Typosquatting websites very often contain one or more of the following:

- ▶ a site with advertising links,
- ▶ a site of the competitive product,
- ▶ a site impersonating the original site, designed to collect user data (phishing),
- ▶ forwarding to the original site,
- ▶ website of another product, unrelated to the character of the original website.

8. Key incidents according to CERT Polska

Most frequently upon a visit one will find advertising links or will be redirected to a website with such links. In such case, the profit is made on pay-per-click (PPC) or pay-per-visit (PPV) basis. To make the income under the above schemes higher than costs, typosquatters register multiple domains. There are websites offering an entire infrastructure necessary to profit from domains with typing errors (domain parking, partner advertising programmes).

Particularly dangerous are websites impersonating the original site, designed to collect user data (classic phishing). In this case, cyber criminals profit directly from using the collected data (e.g. credit card data, login data to e-banking, etc.) or from selling them.

Quite often the typosquatting website forwards the visitor to the original site. This usually happens when the domain is purchased by the original owner or when an agreement is made with the owner of a typosquatting website. Large and popular Internet portals create partner programmes, making it easier to get in touch for the owners of domains with similar names. This is done directly or through a PR agency. In such case, the owner pays for each time an inattentive Internet user is forwarded to his site.

An interesting trend that may be observed from Q4 2011 was a combination of typosquatting with

Premium SMS payments. Usually, the website visited by a user has no connection with the original website. However, it contained potentially interesting content, such as e.g. information on winning an attractive prize. To become more credible in the eyes of the user, such websites often mimic the sites they impersonate by using a very similar graphic layout, colors, graphical symbols or similar address (Figure 8.4.2).

Such combination is exceptionally effective and many persons unaware of the danger will perform the instructions included in the individual sites. Those persons will be convinced that providing their phone number and sending back a text message is harmless, as in their opinion, the entire communication comes from a trusted source. An additional stimulus is the will to own an attractive gadget that not everyone can afford. Text messages received afterwards are usually regarded as advertising messages, often sent by mobile operators (so they are also not treated as suspicious). However, by sending an SMS message to a relevant number with specific content, the user purchases subscription under which a number of messages is sent via Return Premium SMS messages. In the case of Premium SMS messages, a fee is charged for sending a message. However, in the case of Return Premium SMS, the fee is charged per each message received. Charges may vary, detailed fees are presented in Graph 8.4.3.

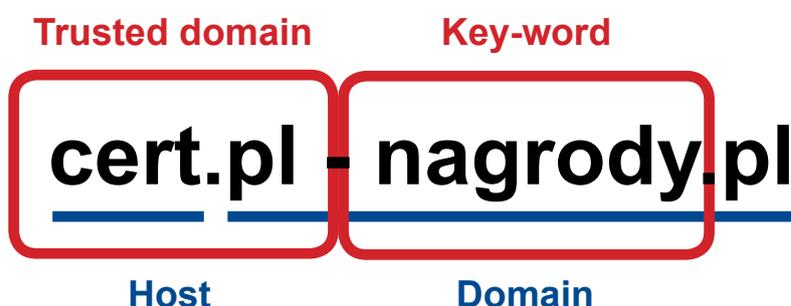


Figure 8.4.2. Construction of a typosquatting address



8. Key incidents according to CERT Polska

Premium SMS number	Net price	Gross price (VAT 23%)
70xx(x)	0,5 zł	0,62 zł
71xx(x)	1 zł	1,23 zł
72xx(x)	2 zł	2,46 zł
73xx(x)	3 zł	3,76 zł
74xx(x)	4 zł	4,92 zł
75xx(x)	5 zł	6,15 zł
76xx(x)	6 zł	7,38 zł
77xx(x)	7 zł	8,61 zł
78xx(x)	8 zł	9,84 zł
79xx(x)	9 zł	11,07 zł
8 000 - 8 099	bezpłatny	bezpłatny
80000 - 80999	bezpłatny	bezpłatny
81000 - 81099	0,10 zł	0,12 zł
81500 - 81599	0,15 zł	0,18 zł
82000 - 82099	0,20 zł	0,24 zł
82000 - 82099	0,25 zł	0,31 zł
83000 - 83099	0,30 zł	0,37 zł
83500 - 83599	0,35 zł	0,43 zł
84000 - 84099	0,40 zł	0,49 zł
84500 - 84599	0,45 zł	0,55 zł
85000 - 85099	0,50 zł	0,62 zł
910xx(x)	10 zł	12,30 zł
911xx(x)	11 zł	13,53 zł
912xx(x)	12 zł	14,76 zł
913xx(x)	13 zł	15,99 zł
914xx(x)	14 zł	17,22 zł
915xx(x)	15 zł	18,45 zł
916xx(x)	16 zł	19,68 zł
917xx(x)	17 zł	20,91 zł
918xx(x)	18 zł	22,14 zł
919xx(x)	19 zł	23,37 zł
921xx(x)	20 zł	24,60 zł
925xx(x)	25 zł	30,75 zł
50100 - 50199	0,01 zł	0,01 zł
50200 - 50299	0,02 zł	0,02 zł
50300 - 50399	0,03 zł	0,04 zł
50400 - 50499	0,04 zł	0,05 zł
50500 - 50599	0,05 zł	0,06 zł
50600 - 50699	0,06 zł	0,07 zł
50700 - 50799	0,07 zł	0,09 zł
50800 - 50899	0,08 zł	0,10 zł
50900 - 50999	0,09 zł	0,11 zł
51000 - 51099	0,10 zł	0,12 zł
52000 - 52099	0,20 zł	0,24 zł
53000 - 53099	0,30 zł	0,37 zł
54000 - 54099	0,40 zł	0,49 zł
55000 - 55099	0,50 zł	0,62 zł
56000 - 56099	0,60 zł	0,74 zł
57000 - 57099	0,70 zł	0,86 zł
58000 - 58099	0,80 zł	0,99 zł
59000 - 59099	0,90 zł	1,11 zł
60100 - 60199	1 zł	1,23 zł
60200 - 60299	2 zł	2,46 zł
60300 - 60399	3 zł	3,76 zł
60400 - 60499	4 zł	4,92 zł
60500 - 60599	5 zł	6,15 zł
60600 - 60699	6 zł	7,38 zł
60700 - 60799	7 zł	8,61 zł
60800 - 60899	8 zł	9,84 zł
60900 - 60999	9 zł	11,07 zł
61000 - 61099	10 zł	12,30 zł
61100 - 61199	11 zł	13,53 zł
61200 - 61299	12 zł	14,76 zł
61300 - 61399	13 zł	15,99 zł
61400 - 61499	14 zł	17,22 zł
61500 - 61599	15 zł	18,45 zł
61600 - 61699	16 zł	19,68 zł
61700 - 61799	17 zł	20,91 zł
61800 - 61899	18 zł	22,14 zł
61900 - 61999	19 zł	23,37 zł
62000 - 62099	20 zł	24,60 zł
62100 - 62199	21 zł	25,83 zł
62200 - 62299	22 zł	27,06 zł
62300 - 62399	23 zł	28,29 zł
62400 - 62499	24 zł	29,52 zł
62500 - 62599	25 zł	30,75 zł

Figure 8.4.3. Fees charged for Premium SMS received.
1 USD = ~ 3 PLN

Usually the user is not aware of high costs incurred until the phone bill comes. Finding the cause of high phone bills and unsubscribing from the service might take up to several months.

Summary

Combination of cybersquatting with typosquatting is particularly dangerous from the perspective of an Internet user. The basic method for defence is to enter domain addresses cautiously. Commercial solutions offered by antivirus software producers may also be applied. Additionally, OpenDNS name servers can be used.

Unfortunately, advertising links are often purchased to increase the chances of visiting "competition website". Providing personal data should be avoided (such as phone number or e-mail address), or enough time should be spared to read terms of use.

9. Key events in the activity of CERT Polska

9.1 CERT Polska communities




CERT Polska is present in social networks since 2010. Our Facebook profile is liked by over 300 users, while short messages on Twitter channels cert_polska (in Polish) and cert_polska_en (in English) perfectly supplement in-depth information and reports published at www.cert.pl. In 2011, we published several hundred posts on each of them, informing on potential vulnerabilities, curiosities, or spectacular events. We are happy to observe that many of them raise keen interest and are quoted by influential bloggers. What is interesting, the English language channel cert_polska_en enjoys a much higher popularity than its Polish counterpart. It is subscribed by over 460 users, over twice as many as the Polish language version.

In autumn 2011, our presence in social media was also broadened with SECURE conference profile on Facebook. It is used to publish practical information related to the conference, links to articles, photographs and selected presentations. For the first time, we also held a competition for the fans of the profile, with free invitations to the conference as prizes.

You are welcome to join us and follow discussions using the following portals.

<http://fb.com/CERT.Polska>
http://twitter.com/cert_polska
http://twitter.com/cert_polska_en
<http://fb.com/Konferencja.SECURE>

9.2 SECURE 2011 conference

The SECURE 2011 conference, which took place between October 24 and 26, 2011 was exceptional in many aspects. On the first day, four hands-on workshops were available, a consequence of the very high interest in that form of participation in the previous edition. Two of them were conducted by CERT Polska. Also, the programme of the conference was packed – on each day, the speakers' presentations lasted for seven hours, with the most persistent participants staying until late hours.

Among the highest rated speakers were Raoul Chiesa, whose presentation "Cyber Weapons in 2011: An F16 Just Flew Over a 1st World War Battlefield" discussed how the balance of power changed in the face of cyberconflicts, Dick Hardt – the co-author of OpenID 2.0 and OAuth 2.0 speci-



fications and on-line identity expert, and Piotr Koniczny – founder and owner of niebezpiecznik.pl portal, a pentester and security trainer.



9. Key events in the activity of CERT Polska

In total, we hosted 38 speakers, who gave 33 presentations in total, divided into three parallel sessions for most of the time. The plenary sessions included, among others, Brian Krebs – a renowned blogger, ex-investigative journalist of The Washington Post, and Ryan Seu with Facebook security team. The special guest of the conference was a multiple world champion, European champion and Olympic gold medallist in racewalking, who talked about the relationships of responsibility and accountability of sportsmen for doping with the online world.

The presentations in parallel sessions were equally interesting. Much attention was drawn by presentations related to threats to companies, including APT attacks, discussed by Gavin Reid from Cisco Systems or Wojciech Ledzion and Marcin Siedlarz from government team CERT.GOV.PL. At the same time, technical details of malware were discussed by Tomasz Bukowski and Tomasz Sałaciński from CERT Polska. After the lunch, one of the sessions was fully dedicated to legal issues, with presentations from Aleksander Gacek and Maciej Kołodziej from nk.pl social network, and Michał Kluska and Grzegorz Wanio from Olesiński i Wspólnicy legal firm.

The latter presented a brilliant idea on how to prosecute offences made on blogs and forums in the conditions of the Polish legal system. On the second day, attendees could choose between presentations on VoIP security (Sandro Gauci and Joffrey Czarny) and on current and future tools used by the army and secret services (Michał Młotek and Raoul Chiesa). Also, CERT Polska had a presentation – Paweł Krześniak spoke on use of passive data from DNS systems to analyse threats.

Similarly to the previous year, at the end of the second day we let the participants of the conference speak, allowing each of them to give a short “lightning talk”. We heard eight dynamic and very varied speeches.

Participants praised the variety of subjects as well as unique presentations, many of them including descriptions of specific, actual cases.

The conference was accompanied by an evening party in Vapiano restaurant, providing an occasion to more relaxed discussions, meeting new people and acquiring skills in preparing pizza and pasta.

9.3 CERT Polska report for ENISA “Proactive Detection of Network Security Incidents”

In December 2011, the European Network and Information Security Agency (ENISA) published a report prepared by CERT Polska titled “Proactive detection of network security incidents”.

Proactive detection of incidents is the process of discovery of malicious activity in a CERT’s constituency through internal monitoring tools or external services that publish information about detected incidents, before the affected constituents become aware of the problem. It can be viewed as a form of early warning service from the constituents’ perspective. Effective proactive detection of network security incidents is one of the cornerstones of an efficient CERT service portfolio capability. It can

greatly enhance a CERT’s operations, improve its situational awareness and enable it to handle incidents more efficiently, thus strengthening the CERT’s incident handling capability, which is one of the core services of national and governmental CERTs.

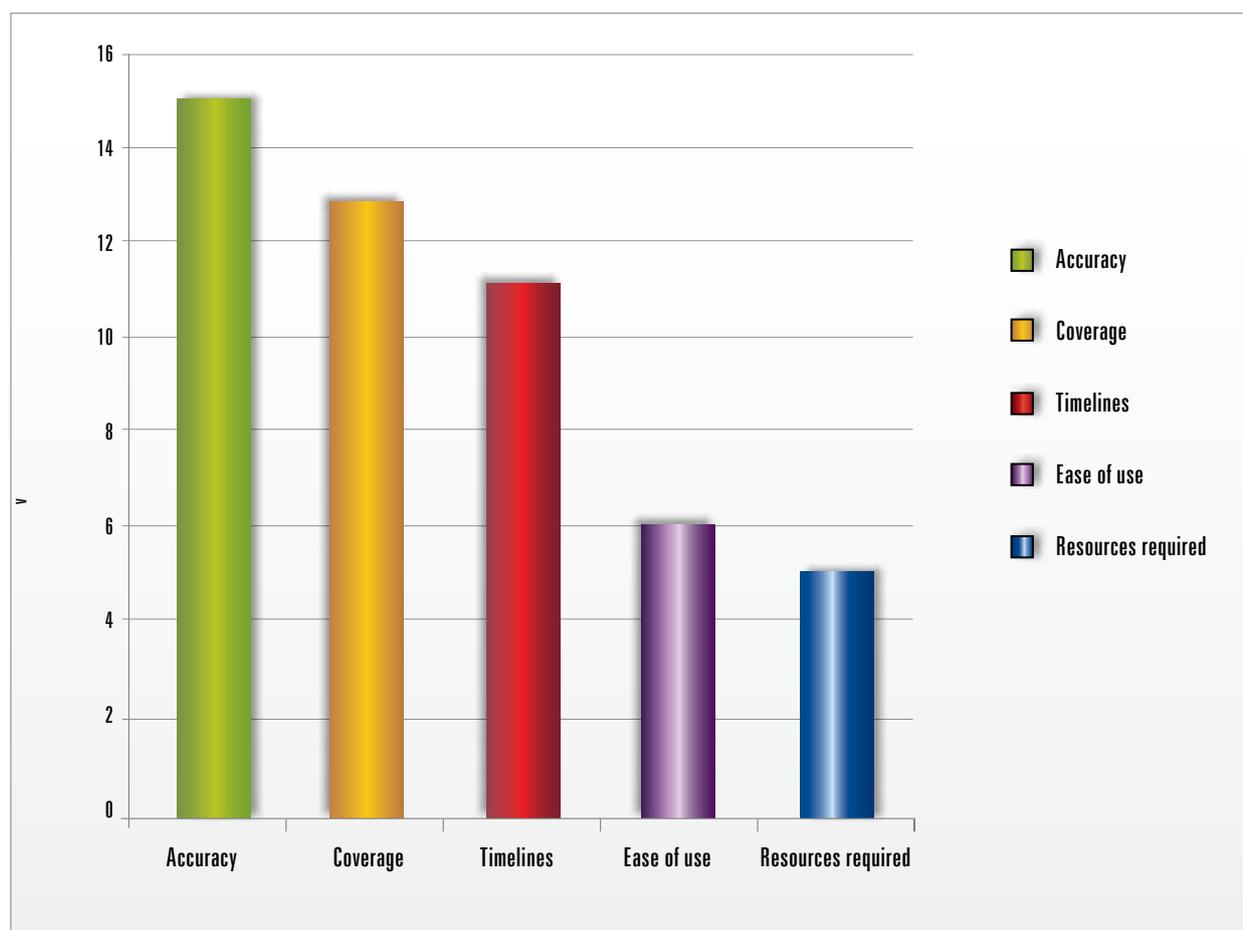
The document analyses methods used for proactive detection by CERTs, especially national and government, to detect incidents. The report also includes a set of best practices and usable tools for newly created CERT teams, analysis of problems which they might face and a set of recommendations for improving incident management by CERT teams.

9. Key events in the activity of CERT Polska

A strong aspect of the study is that it was created with the participation of specialists from European CERT teams and renowned experts on security. The report is based on the in-depth survey among 45 CERTs and experts' discussion which lasted throughout the time the document was being created. Their significant contribution, apart from experience and work of the authors, allowed for the creation of an exhaustive publication on incident management.

The report includes ratings and descriptions of external sources of proactive information on incidents and internal monitoring tools, which can be used by CERTs to increase their capacity to detect security incidents in their day-to-day operations.

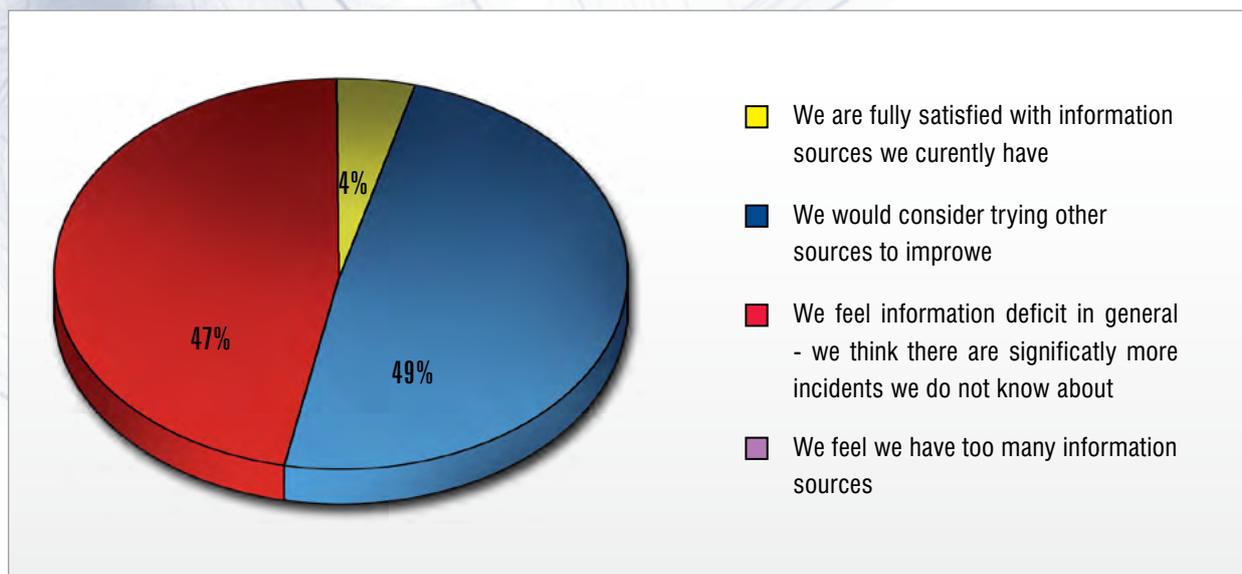
When collecting the materials for the report, 16 serious obstacles to the process of incident detection were identified and analysed, both in relation to technical issues and legal/organisational ones. Among the technical problems, the most frequent ones mentioned were low data quality, and no automation of processing and correlation. In the legal field, a frequent issue is related to regulations on privacy and personal data protection, which make it impossible or difficult to exchange data. For each of the identified issues, a number of potential solutions and recommendations was proposed for entities providing data feeds, their recipients and European or national organisations that can influence the process.



Graph 9.3.1. Features of the sources of data on incidents, which require improvement according to the members of response teams.



9. Key events in the activity of CERT Polska



Graph 9.3.2. Opinions of CERT teams regarding satisfaction with the sources of information from their area of activity.

The results of the published report will help both the newly created, and existing CERT teams find and use new, helpful sources of information, as well as consider using additional tools in their organisations. Improvement of proactive detection and processing of data on incidents promotes efficient operation of not only a single CERT, but everyone the data relates to. This in turn allows to tighten cooperation and exchange information between CERT teams, which are able to respond much

quicker and solve problems by improving security of the Internet.

For full information, download the report from: <http://www.enisa.europa.eu/act/cert/support/proactive-detection> and the results of the survey among CERT teams: <http://www.enisa.europa.eu/act/cert/support/proactive-detection/survey-analysis>.

9.4 CERT Polska joins APWG



At the end of 2010, CERT Polska joined the Anti-Phishing Working Group initiative. It is a forum for entities dealing with electronic crime, in particular with data theft. APWG is a cooperation of researchers, CERTs, as well as many commercial entities, especially vendors of commercial traffic filtering systems, antivirus software, etc. External goals of APWG include mainly analysis of threat trends and education – both for decision-makers shaping the law or regulations (e.g. with regard to domain registration) or end users.

A good example of the latter is the campaign conducted in the United States jointly with NCSA named “STOP. THINK. CONNECT”. For all members of APWG, it is equally important within the organisation to make contacts and ensure consistent knowledge sharing, which is supported by a unique combination of industry, academia, and law enforcement. CERT Polska is a “research member” of APWG.

In 2011, CERT Polska participated in two meetings organised by APWG – eCrime Researchers Sync Up in March, held in Dublin and eCrime Research Summit in November, held in San Jose, California.

9. Key events in the activity of CERT Polska

At the latter conference Przemysław Jaroszewski presented a case study of mobile Zeus infection (ZITMo).

For more information on Anti-Phishing Working Group, go to <http://www.apwg.org/>.

9.5 Public issue of Capture-HPC as part of the Honeynet Project



HONEYSPIDER
network

The Honeynet Project is an organisation associating experts from

various fields related to computer security, allowing them to share knowledge and jointly develop solutions aimed at improving the security of Internet users. Participation in the organisation is voluntary – the members devote their free time to analyse and detect new threats, create tools, educational materials and participate in discussions. Since the creation in 1999, it is one of the most recognised organisations in the international security community.

Experts associated in The Honeynet Project make a joint effort to enrich the existing knowledge on threats and methods to fight them. An example of their work is the almost thirty articles collected under the title „Know Your Enemy”. The series deal with such topics as tracking botnets, architectures of honeypots and their possible applications, threats such as phishing, net worms, malicious websites and many more. The articles are addressed mainly to experts who deal with computer security on a daily basis, but more advanced users will also find it to be a rich source of information.

The dynamic character of the threats security experts deal with requires them to constantly improve their skills in the field of detection and analysis. The best way to achieve that goal is hands-on practice. The Honeynet Project provides a set of advanced problems for everyone to check their skills in analysis of threats such as malicious PDF files, threats related to VoIP, analysis using reverse-engineering techniques and many more. Each of the tasks is based on an actual case, which was examined in-depth by the experts from the organisation. The summary indicates the steps to be taken to detect

the attack and presents examples of tools useful in the analysis. The additional incentive for participation in the task, which is organised as a competition, are small prizes sponsored by the organisers.

Knowledge gathered within the organisation translates directly to the tools created by its members. Currently, the set of projects conducted in the organisation exceeds 20. Due to the fact that it is a non-profit organisation, and the only source for its support are subsidies, the tools are developed on voluntary basis or act as a part of larger projects conducted by independent units, which agreed to make such tools available to the public. For several years The Honeynet Project has also been an active member of Google's programme Summer of Code, allowing students from the entire world work on creating open source tools. Thanks to such initiatives, new projects were launched and existing projects within the organisation were extended.

The Honeynet Project is an international organisation, consisting of over 40 chapters located worldwide. In Poland it operates since November 2011, and the Polish Chapter of The Honeynet Project is active thanks to the involvement of members of CERT Polska. Members of the chapter include a group of experts from CERT Polska, additionally supported by experts from the Scientific Division of NASK. The mission of the chapter is to popularise knowledge on the threats in today's Internet and to create tools supporting detection and analysis of the attacks. The contribution to date in the development of the organisation is creating a newer and more stable version of highly-interactive client Honeypot – Capture-HPC. Works was performed as part of the development under project Honey-Spider Network – a joint project of CERT Polska, GOVCERT.NL and SURFnet. The author of the original software is Christian Seifert, and the modifications were made by the Software Development



9. Key events in the activity of CERT Polska

Department at NASK. Capture-HPC under project HoneySpider Network is a new version, introducing a number of improvements and allowing to apply VirtualBox and KVM virtual machines (the original version used VMware). The software was stabilised and licensed under GPL 2.0. The source code of honeypot, installation instruction and user manual can be downloaded from the chapter's website.

The chapter consists of eight members, mainly involved in development of projects related to the use of honeypot technologies for detection and analysis of various types of attacks. Experts from CERT Polska also provide a number of trainings and courses on security in today's Internet. For more information on the mission of Polish Chapter of The HoneyNet Project, go to <http://cert.pl> and <http://pl.honeynet.org>. All persons interested in the development of the chapter and the tools we provide are welcome to contact us under hnp@cert.pl

9.6 Completion of WOMBAT project



April 2011 saw the completion of WOMBAT project – Worldwide Observatory of Malicious Behaviour and Attack Threats. The project was launched in January 2008 as part of 7th Framework Programme of the European Union. The goal of WOMBAT was to create a systematic framework for a system of monitoring and analysis of threats, especially malware, which in recent years has become a powerful tool in the hands of cybercriminals. Apart from NASK, participants included security specialists from such companies as: France Telecom R&D, Symantec, Hispasec Sistemas (who created project Virustotal) and scientific/research institutions: Institut Eurecom, FORTH, Politecnico di Milano, Technical University Vienna, Vrije Universiteit Amsterdam. The work was managed by CERT Polska team with cooperation of Scientific Department of NASK.

Project work focused on three different areas:

- collecting information on malware using crawlers and honeypots (including improving those techniques and proposing new ones),
- development of new techniques for enriching the collected information,
- advanced analysis of threats, based on correlation of information from project partners, in order to identify the causes and understanding the problem.

WAPI (WOMBAT API) was created, providing easy and trouble-free access to data from multiple systems participating and being developed under the project (incl. Virustotal, SGNET, Shelia, Wepawet, HoneySpider Network, HARMUR, Anubis). WAPI code was made available (and is still being improved!) under BSD license: <http://sourceforge.net/projects/wombat-api/>.

NASK's contribution in the project was related to:

- Analysing the state of the art in the subject matter and specifying the assumptions for WOMBAT environment,
- Work on a shared API (WAPI),
- Improving the system of client honeypots - HoneySpider Network,
- Development of a tool based on the techniques used by learning machines to reduce false alarms for Capture-HPC system,
- Development of the tools for visualisation and analysis of the interconnections between the detected malicious URLs.

Additionally, some instances of HoneySpider Network system fed data to a new threat detection system FIRE (FInding Rogue Networks) developed under the project: <http://maliciousnetworks.org/>.

9. Key events in the activity of CERT Polska

Apart from the development of tools and systems (as well as creating many new ones) by the partners in the project, numerous presentations were given on the project's achievements in scientific conferences (e.g. RAID, DIMVA) and techni-

cal ones (e.g. BlackHat, FIRST, Honeynet Project Workshop). Project documentation has been published on the official website of the project: <http://www.wombat-project.eu>.

9.7 Completion of FISHA project, preparation for NISHA project



FISHA is a project under which a prototype of EISAS was created (European Information Sharing and Alerting System). The project spanned from 2009 - 2011 as part of the EU programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks". It was a cooperation between CERT Polska, a Hungarian CERT team (CERT-Hungary) and German research institute Internet Security Centre from Gelsenkirchen University.

The main objective of the project was to improve awareness with regard to on-line security among home users and staff of small and medium enterprises. Focusing on those groups is driven by the fact that because of their volume, they play a key role in ensuring security of Internet, at the same time offering an easy target for attacks due to low awareness of security-related issues.

The project also covered technical activities, aimed at creating a platform for exchange and dissemination of information, as well as activities consisting in developing methods of reaching the target groups with accessible information. The result of the works as part of the syndicate is a prototype of a new Internet portal and proprietary implementation of a p2p network for exchange of information between entities from EU member countries and plan of communication with the users.

The system prototype created as part of FISHA will act as the basis for implementation of a pilot network under project NISHA (Network for Information Sharing and Alerting) in the years 2012-2014 by the three previously mentioned existing partners and a new member of the consortium - FCCN (Foundation for National Scientific Computing) from Portugal.

The logo for ARAKIS, featuring a stylized blue 'A' with a white checkmark inside, followed by the word 'ARAKIS' in a bold, blue, sans-serif font. To the right of the logo is a decorative graphic consisting of several horizontal blue lines of varying lengths, creating a sense of depth and movement.

ARAKIS

2011 Annual Report

Introduction

The ARAKIS system (from Polish: AgRegacja, Analiza i Klasyfikacja Incydentów Sieciowych – Aggregation, Analysis and Classification of Network Incidents) is a project operated by CERT Polska, a part of the Polish Research and Academic Computer Network (NASK). The system was developed in cooperation with NASK's Software Development and Scientific Departments. Its primary objective is to detect and describe network threats based on aggregation and correlation of data from multiple sources, including a dispersed network of honeypots, darknet, firewalls and anti-virus systems. As far as the main source of data is concerned, i.e. the honeypots, the system relies on data from non-production traffic. Hence, it is not possible to detect and analyze targeted attacks carried out specifically against production servers (e.g. DDoS). ARAKIS is a tool that has proven itself in analyzing (mainly automated) threats that propagate through active network scanning (where the chances of establishing the connection with a honeypot are high), such as, for instance, network worms or some bot types.

ARAKIS-GOV is a project implemented under the overall ARAKIS system framework, and is used to protect the IT resources of offices of public administration. It has been implemented in 75 various public administration institutions, in co operation with the Polish government

CERT - CERT.GOV.PL – operating within the structures of the IT Security Department of the Internal Security Agency (ABW).

This is the fourth annual report from ARAKIS. The main objective of the system is to protect network resources of the project participants by detecting sources of (scanning) infections at their early stages. The information gathered has also allowed to identify the mechanisms of both novel and previously known attacks on server applications. The ARAKIS project has been presented at numerous domestic and international IT security conferences concerned. It has often also been cited on a number of occasions, in publications of both Polish and foreign academics and IT security experts.

The report presents statistical data concerning alarms generated by the system. Those alarms play a central role in the daily operation of the system, by notifying operators about current threats and by describing – depending on their type and priority – the nature of the threats and events considered a violation of network security. Other statistical data presented herein relates to sources and types of threats. In addition, several interesting cases have been described that are related to observations made with the use of the ARAKIS system.

1. Alarm statistics

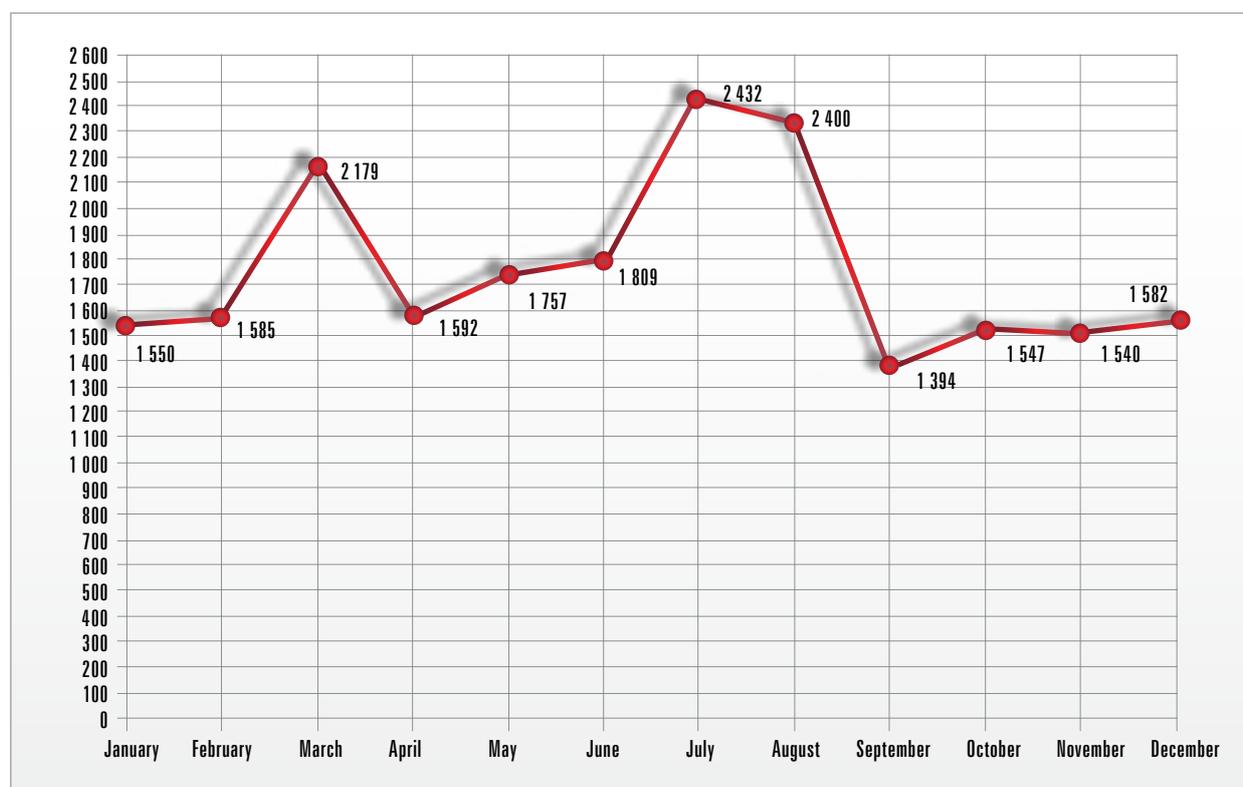
21,307 alarms were generated by the ARAKIS system in 2011. The number of alarms is by 6,000 lower than the one recorded in 2010. This decrease seems aligned, with a general trend observed worldwide, in which cyber criminals abandon attacks that use scanning in favor of attacks against client applications (Internet browsers, PDF readers, etc.), and in favor of precise and directed attacks on pre-defined targets.

The graph below shows the annual summary of all alarms, regardless of their type.

The greatest number of alarms was recorded during the summer holiday months. These comprised mainly low-priority events related to the increase in abnormal traffic at individual ports. The alarms related to events originating from the Internet (and did not involve infections of system participants' work stations). The sudden and temporary increase in the number of alarms observed in March resulted from problems with the connec-

tion between the probes and the center (diagnostic alarms are related with the status of probes) and did not involve any security-related events.

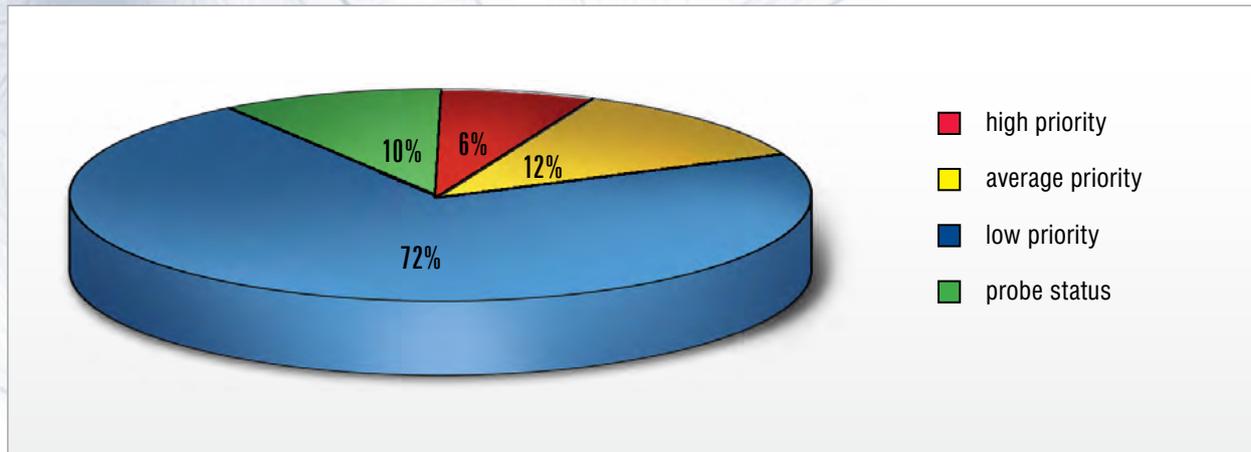
Great majority of all alarms generated in 2011 were of low-priority variety (72%). Low-priority alarms are usually caused by traffic anomalies and are not directly linked to any incidents. The rest were average priority alarms (12%), and alarms related to the status of individual ARAKIS probes (10%). Alarms related to serious network incidents were least frequent (6%). Compared to the previous year's results, one can clearly identify an increase in the percentage share of high- and low-priority alarms. It has to be stressed, however, that the majority of high-priority alarms observed in 2011 were not linked to actual attacks or infections, but were generated by a specific configuration of network hardware, the use of certain protocols or active network monitoring tools.



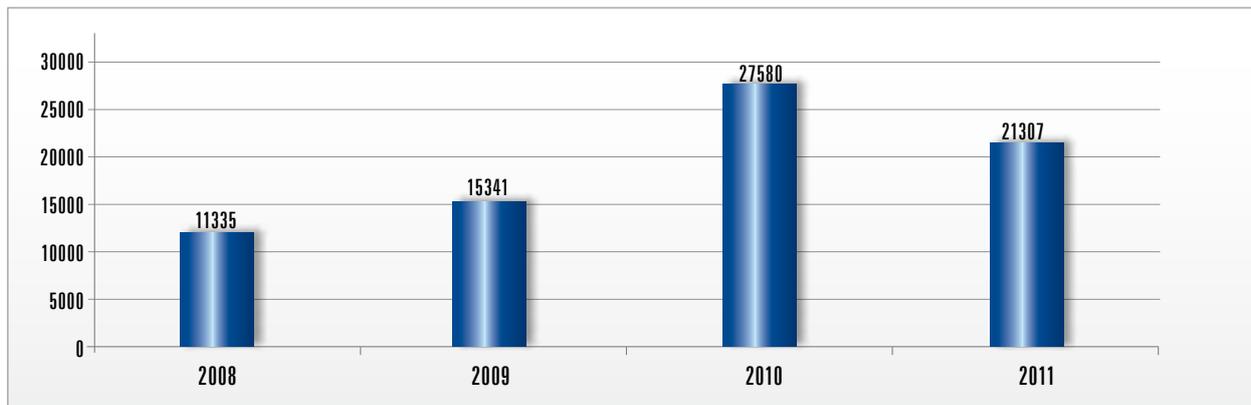
Graph 1.1. Alarms generated by the ARAKIS system in 2011



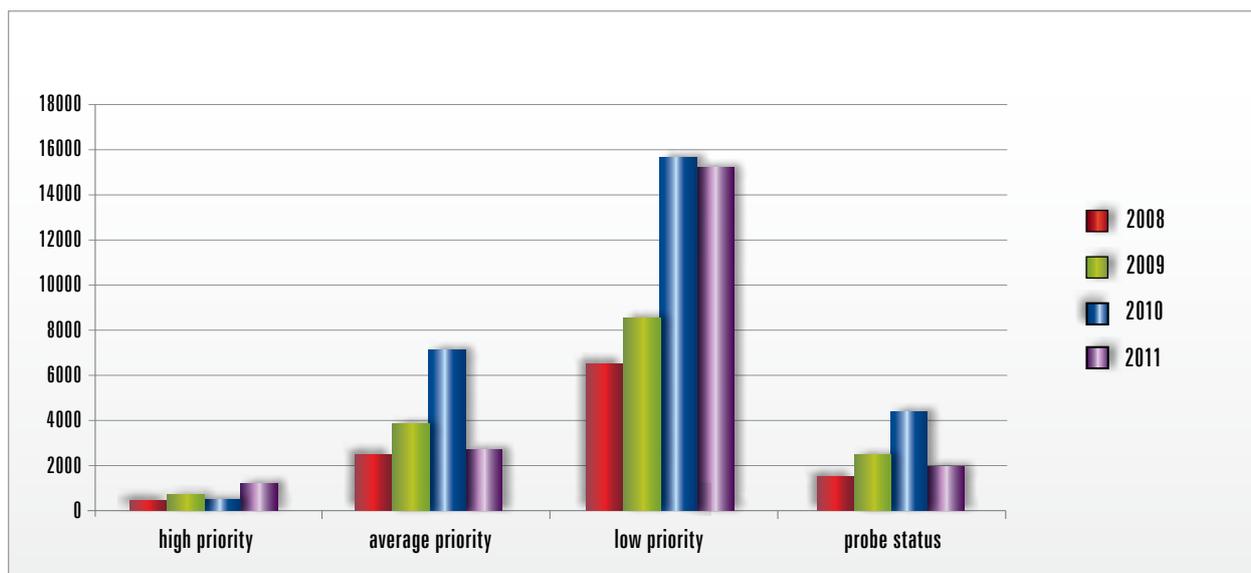
ARAKIS - 2011 Annual Report



Graph 1.2. Shares of alarms by priority levels in 2011



Graph 1.3. Number of all the alarms in the years 2008 - 2011



Graph 1.4. ARAKIS alarms by priority in the years 2008 - 2011

2. Attack statistics

Port scanning is one of the most important categories of attacks detected by honeypots deployed in ARAKIS. The table below presents the number of unique IP addresses, that attempted to establish a connection with individual ports. The data depicts the scale of interest in individual ports (and, hence, the services that use those ports). The 445/TCP port is the most popular. It is used by a number of applications related to Microsoft software, which contained numerous vulnerabilities efficiently taken advantage of by such worms as Sasser or Conficker. The second and fourth positions are also

interesting, as they concern ports related to services native to Unix systems, namely telnet and ssh.

The top 10 statistics concerning the most frequently matched Snort rules is also very interesting. In this case source IP addresses unique throughout the year were considered the primary indicator. Almost all rules (except for one) are related to attacks on Windows services. The first three rules concern RDP connections on 3389/TCP (used by the "remote desktop" service) and may indicate activity of the Morto worm, which surfaced in 2011.

Item	Destination port / protocol	Number unique source IP addresses seen	Description
1	445/TCP	79 925	Buffer overflow attacks on Windows RPC
2	23/TCP	56 908	Telnet service attacks
3	135/TCP	18 799	Windows DCE/RPC service attacks
4	22/TCP	15 665	SSH server dictionary attacks
5	139/TCP	11 273	Attacks NetBIOS / co-sharing of files and printers
6	1433/TCP	9 125	MS SQL attacks
7	80/TCP	7 677	Attacks on Web applications
8	3389/TCP	6 798	RDP (remote desktop) dictionary attacks – largely attributed to the activity of the Morto worm
9	5060/UDP	3 375	VoIP attacks
10	4899/TCP	3 010	Radmin service attacks

Table 2.1. Most often attacked ports



ARAKIS - 2011 Annual Report

Item	Snort rule	Number of unique source IP addresses seen
1	ET POLICY RDP connection request	85 994
2	MISC MS Terminal server request	80 910
3	ET POLICY Radmin Remote Control Session Setup Initiate	77 748
4	ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND	48 450
5	ATTACK-RESPONSES Microsoft cmd.exe banner	24 480
6	ET ATTACK_RESPONSE Possible MS CMD Shell opened on local system	22 487
7	ET POLICY Suspicious inbound to MSSQL port 1433	21 485
8	NETBIOS SMB-DS IPC\$ unicode share access	20 183
9	ET SCAN Potential SSH Scan	16 617
10	ET EXPLOIT LSA exploit	16 479

Table 2.2. Most often matched Snort rules

Analysis of the geographical locations of attack sources leads to very interesting results: as far as the number of unique IP addresses is concerned, position number one is occupied by the USA,

followed by Russia and Turkey, with China ranking as low as fifth. However, when the number of connections is taken into consideration, with the unique IP addresses left out, China will rank first, followed by the USA and Russia.

Item	Country	Number of unique IP addresses
1	US	19 313
2	RU	18 317
3	TR	16 102
4	KR	13 384
5	CN	11 866
6	PL	9 015
7	TW	8 450
8	UA	8 358
9	AE	7 873
10	DE	7 790

Table 2.3. TOP 10 most infected countries by unique source IP

This shows most attacks originate from China, but from a relatively low number of IP addresses.

The ranking of the most infected autonomous systems shows that the highest number of

Item	Country	Number of connections
1	CN	2 149 387
2	US	1 641 497
3	RU	631 184
4	UA	450 243
5	KR	432 089
6	TR	418 869
7	PL	386 186
8	DE	323 129
9	TW	207 125
10	GB	195 262

Table 2.4. TOP 10 most infected countries by number of flows

unique source IP addresses throughout the year belongs to the network of a Turkish operator Turk Telekomunikasyon Anonim Sirketi (AS number: 9121).

Item	Number of unique source IP addresses seen	ASN	Country	Operator's country
1	12 416	AS9121	TR	TTNET Turk Telekomunikasyon Anonim Sirketi
2	10 406	AS4766	KR	KIXS-AS-KR Korea Telecom
3	7 841	AS5384	AE	EMIRATES-INTERNET Emirates Telecommunications Corporation
4	6 767	AS12741	PL	INTERNETIA-AS Netia SA
5	6 174	AS3462	TW	HINET Data Communication Business Group
6	5 767	AS4134	CN	CHINANET-BACKBONE No.31,Jin-rong Street
7	4 632	AS6147	PE	Telefonica del Peru S.A.A.
8	2 862	AS8452	EG	TE-AS TE-AS
9	2 845	AS24863	EG	LINKdotNET-AS
10	2 602	AS5483	HU	HTC-AS Magyar Telekom plc.

Table 2.5. TOP 10 most infected ASNs by unique IP

Position number two was taken by a Korean ISP Korea Telecom (AS: 4766), and spot number three by Emirates Telecommunications Corporation (AS: 5384) from the United Arab Emirates.

When the number of connections is taken into consideration, the top positions are occupied, just as it was the case in the ranking of most infected countries, by Chinese operators.

Item	Number of connections	ASN	Country	Operator
1	983 239	AS4134	CN	CHINANET-BACKBONE No.31,Jin-rong Street
2	328 667	AS4837	CN	CHINA169-BACKBONE CNCGROUP China169 Backbone
3	290 53	AS9121	TR	TTNET Turk Telekomunikasyon Anonim Sirketi
4	270 021	AS4766	KR	KIXS-AS-KR Korea Telecom
5	219 077	AS23650	CN	CHINANET-JS-AS-AP AS Number forCHINANET jiangsu province backbone
6	153 623	AS5384	AE	EMIRATES-INTERNET Emirates Telecommunications Corporation
7	144 942	AS12741	PL	INTERNETIA-AS Netia SA
8	130 050	AS3462	TW	HINET Data Communication BusinessGroup
9	116 941	AS36351	US	SOFTLAYER - SoftLayer Technologies Inc.
10	114 696	AS5483	HU	HTC-AS Magyar Telekom plc.

Table 2.6. TOP 10 most infected ASNs by numer of flows



ARAKIS - 2011 Annual Report

The distribution of infected IP addresses within Polish networks is interesting as well. Unlike in the statistical data provided in the main part of the CERT Polska report (data from several reporting systems, not only from ARAKIS), position number

one is occupied not by Telekomunikacja Polska, but by Netia, with a huge advantage in the number of unique IP addresses observed throughout the year. Interestingly, the ranking does not list any mobile operators.

Position	Source IP addresses seen	ASN	Operator name
1	6 767	AS12741	NETIA
2	744	AS5617	TP
3	201	AS21021	MULTIMEDIA
4	167	AS15857	DIALOG
5	69	AS12476	ASTER
6	65	AS29314	VECTRA
7	58	AS35007	MICRONET
8	56	AS42709	BIELSAT
9	43	AS34337	ELPOS Cable TV
10	39	AS6714	GTS

Table 2.7. TOP 10 most infected networks by IP

3. Notable network incidents observed

Apart from the protection that the ARAKIS system has offered to the networks in which its sensors are installed, it has also contributed to increasing the level of awareness and understanding of numer-

ous types of threats common throughout the Internet. Below is a short description of what are, in our opinion, the most notable observations made by ARAKIS in 2011.

3.1 Morto – a new network worm

A new network worm known as Morto was born in mid-March 2011. It attacked weakly configured Microsoft Windows systems using the RDP (Remote Desktop Protocol) as an attack vector. Morto does not take advantage of any vulnerabilities in software, and the attack consists of an attempt to guess the username and password. Having infected a given machine, the worm looks for other computers within a given network with RDP service available and tries to infect them as well. This results in a considerable increase in network traffic on the 3389/TCP port typically used by the service.

On the infected machine, Morto kills all the processes it considers to be security-related applications (based on their names). This is a very popular course of action employed by malware following an infection. ARAKIS has been observing Morto propagating in mass-scale since the beginning of the process.

A continuous increase in traffic to 3389/TCP was first observed on 15 August 2011. A sudden and clearly distinguishable growth was observed on 24th August, and the high levels were maintained until 26th August.

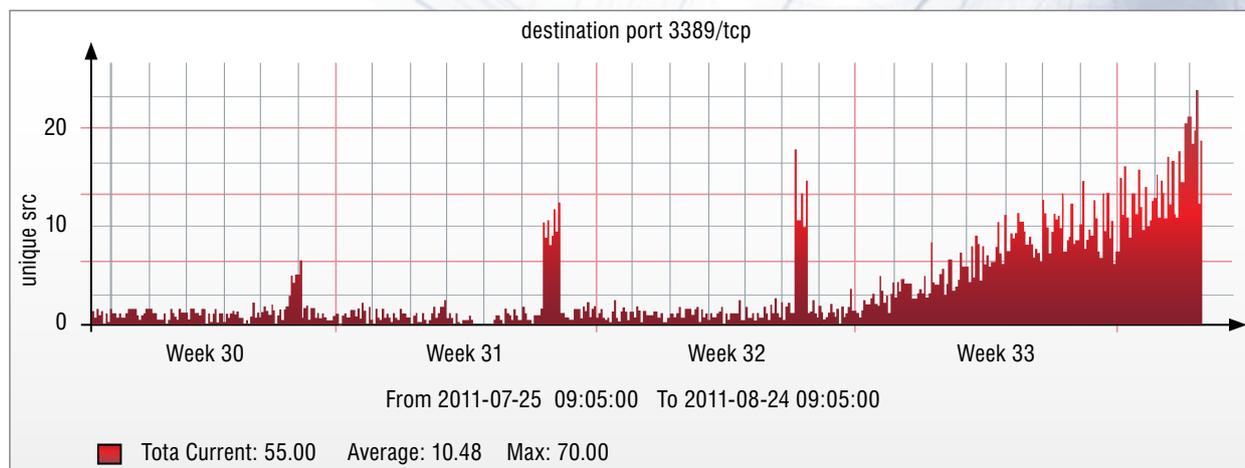


Chart 3.1.1. RDP traffic by unique source (honeynet view, one month)

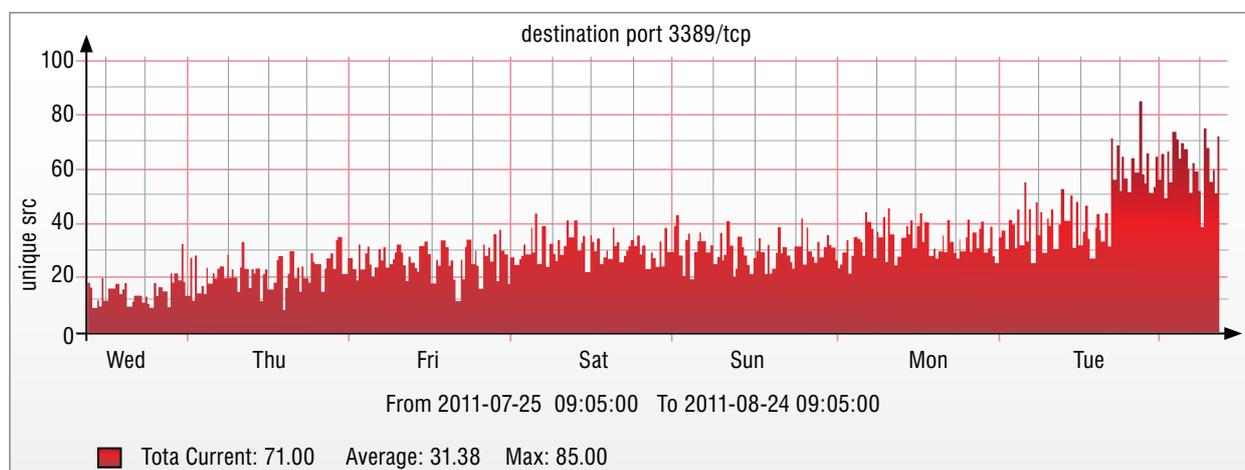


Chart 3.1.2. RDP traffic by unique source (honeynet view, one week)

On 28th August the port activity returned to normal levels, observed prior to the mass-scale propagation of Morto. The worm resurfaced several weeks

later, and its activity – although slightly lower – has been observed ever since.

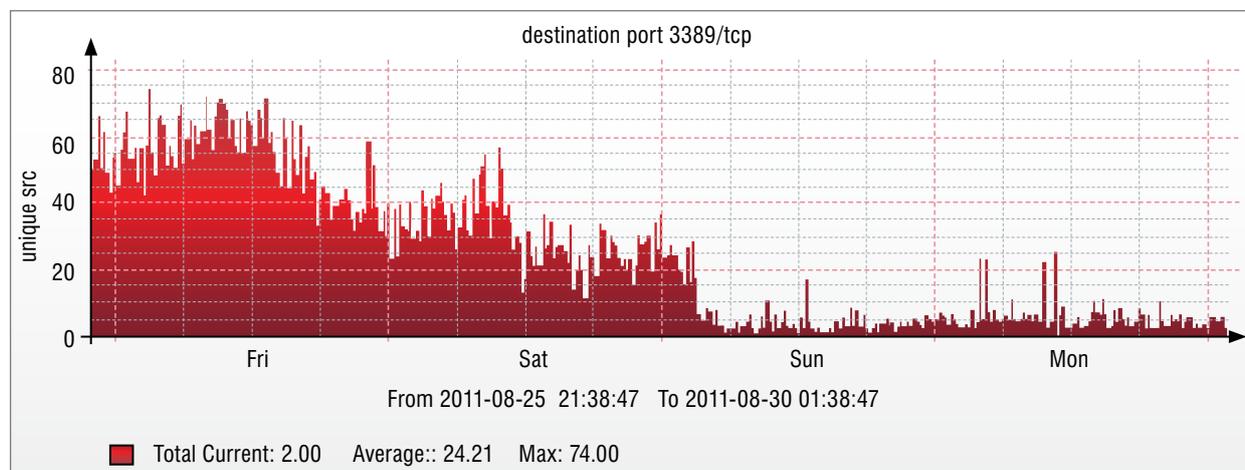


Chart 3.1.3. RDP traffic by unique source (honeynet) in August 2011



ARAKIS - 2011 Annual Report

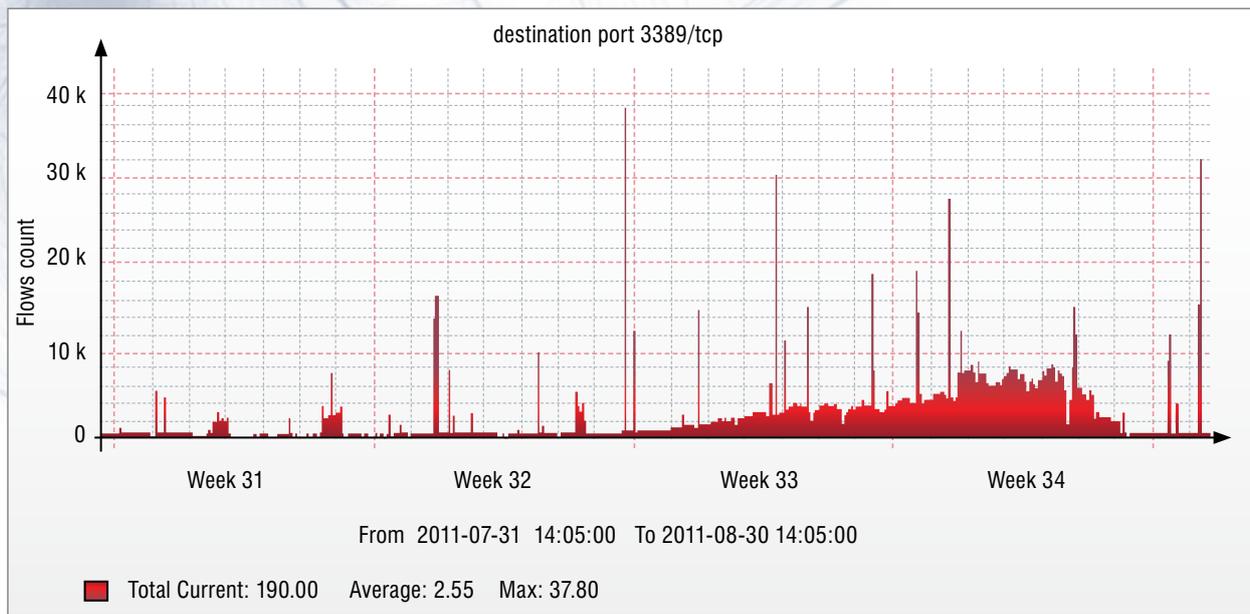


Chart 3.1.4. RDP traffic as seen in the ARAKIS darknet

RDP scanning was observed both in the honeynet (above) and in the darknet (below).

It is worth pointing out that activity of the Morto worm remains relatively high until the time of writing of this report, and that the 3389/TCP port remains in the TOP 10 of most frequently scanned ports.

Below is a sample of raw network traffic – “connection request” packet of the X.224 component, used to establish a connection (RDP connection initiation phase). The “user cookie” (starting with “mstshash”), which contains the username, is clearly visible.

Experts from other teams that analyzed the Morto worm stated that it always attempted to establish a connection using the “administrator” username and

a set of pre-defined passwords. However, ARAKIS honeypots received also connection attempts that used other usernames (great majority). We are not sure whether RDP connection attempts performed with the use of other usernames are the result of actions of the same worm, or perhaps we are dealing with another type of threat. Low-interaction traps used by ARAKIS do not allow for the establishment of a full session with the attackers (the Remote Desktop service is not fully simulated), which makes it impossible for us to determine whether all break-in attempts are caused by Morto.

Due to the huge amount of data, for subsequent analysis we use only a full record of the network traffic from five most frequently attacked probes of the ARAKIS system between 20th August and 28th August, unless stated otherwise.

```

03.017146 IP 85.200.109.21.3890 > 172.16.17.100.3389: P 2660092317:2660092360(43) ack 394
0x0000: 4500 005f 221a 4000 7406 a16d 0000 0000 E. _ ".@.t..m
0x0010: 0f32 0d3d 9e8d c99d 025a 25d4 0000 0000 ... .2.=.....Z%.
0x0020: 8018 ffff b534 0000 0101 080a 0050 3920 .....4.....P9.
0x0030: 0035 48f0 0300 002b 26e0 0000 0000 0043 .5H...+&.....C
0x0040: 6f6f 6b69 653a 206d 7374 7368 6173 683d ookie:.mstshash=
0x0050: 6164 6d69 6e69 7374 7261 746f 720d 0a administrator..
  
```

Graph 3.1.5. RDP initiation

¹ <http://msdn.microsoft.com/en-us/library/cc240470%28v=prot.10%29.aspx>

² <http://www.snakelegs.org/2011/02/06/rdp-cookies-2/>

Below is a list of most frequently used usernames:

Position	Count	Attempted username
1	33 692	Administrator
2	18 070	administrator
3	11 804	a
4	4 612	admin
5	3 474	..a (\xFF\xFE\x61)
6	3 265	usuario
7	2 884	support
8	2 074	NCRACK_USER
9	644	micros
10	624	pos1
11	369	adm
12	322	aloha
13	230	skannata
14	178	pos
15	129	Admin
16	126	fax
17	100	administrateur

Table 3.1.6. Most often attempted usernames

An interesting string of characters is presented in item 5 – it is a printable character (“a”) preceded by two non-printable ones (“FF” and “FE” in the

hexadecimal code). The use of “NCRACK_USER” is also interesting – someone has probably unskillfully tried to use an automatic scanner (most probably ncrack). The usernames also included names in many languages other than English, e.g. “usuario” (Spanish), “skannata” (Finnish), “administrateur” (French) or “Verwalter” (German).

Analysis of all data from the ARAKIS system collected in July and August has led to other interesting conclusions. In the case of a vast majority of scanning attempts, a single source IP address tried to establish a connection with numerous target addresses with the use of the same username. Out of 1,800 source addresses, only 24 tried to establish a connection with more than one username, with 21 of them with only two different usernames. So, our observations are not completely in line with former reports presented by experts of other teams monitoring Morto, according to which the worm attempts to log-on with the use of many different usernames.

The next step was to analyze the traffic load throughout the entire period in question. The graph below shows all RDP connections recorded by our honeypots, by usernames the worm attempted to use:

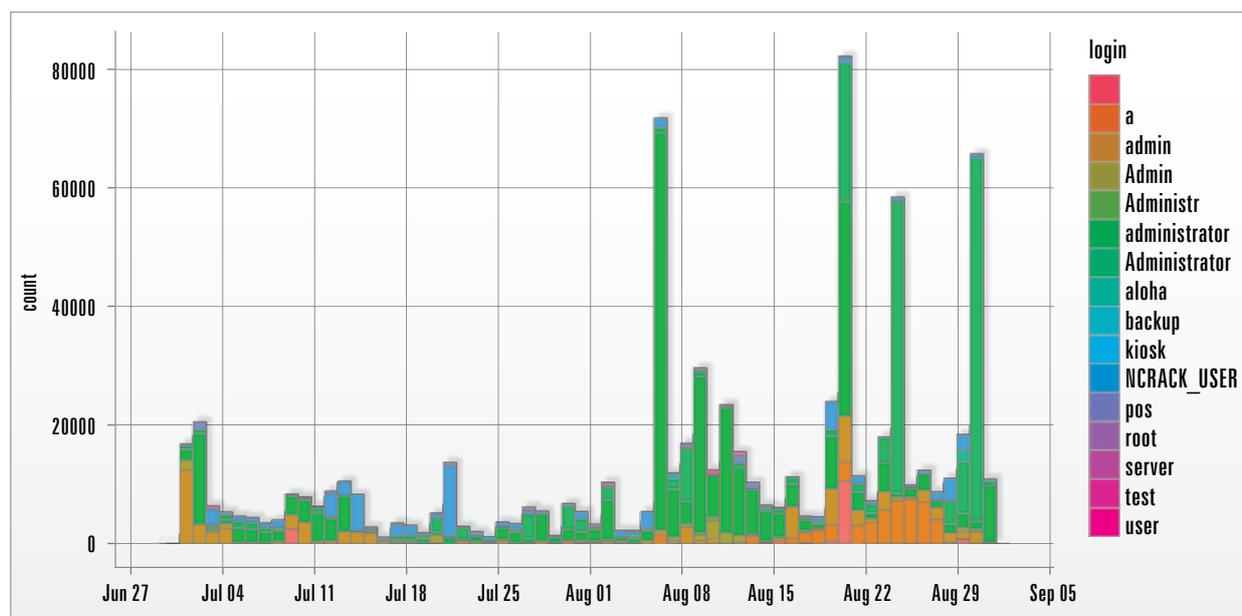


Chart 3.1.7. Mapping of most often used usernames observed by ARAKIS

³ <http://nmap.org/ncrack/>



ARAKIS - 2011 Annual Report

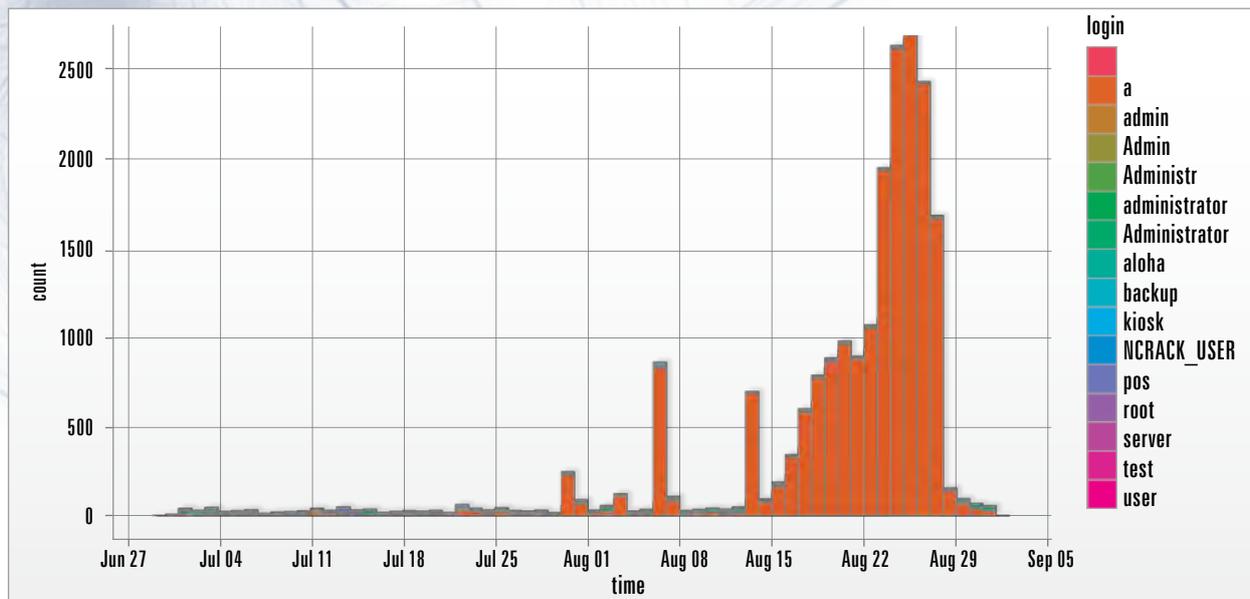


Chart 3.1.8. Mapping of most often used usernames in the first connection attempt by a source IP

The maximum number of connections per day exceeds 80,000, but no significant trend can be identified. It has turned out that the majority of the traffic is generated by single sources that attack large ranges of IP addresses. Therefore, we have analyzed the time distribution of connections from unique IP addresses – the graph below contains data on the first connection from a given IP only (new attackers).

It is easy to observe that the number of unique attack sources using the username “a” skyrocketed approximately on 15 August. Attackers using other logins are completely negligible here. A greatly increasing number of attacks is a typical feature of quickly propagating worms, so one can assume that the traffic observed was generated by Morto. The username “a” was known as one of the usernames used by Morto, but we are not certain why we have observed an increase in the number of attacks with this specific username only, and not with other usernames (e.g. “Administrator”). It is likely that having failed to establish a full RDP connection (on the application layer level) (low-interaction honeypots, as specified above), the worm was giving up other attempts with different usernames.

Below is a classification of countries with the highest number of visible RDP connection attempts attacks. The data is limited, again, to the five ARA-

KIS sensors attacked most frequently between 20 August and 28 August. Please bear in mind that although the list includes only those connections in which the username has been transmitted (we have rejected verification of 3389/TCP port's open status), we are uncertain, as mentioned above, whether all connections are related to the Morto worm. Moreover, it is likely that the source IP addresses are not direct attack sources – they may represent intermediaries behind whom the real attacker is hiding. It should be also noted that larger networks may be classified higher, due to the “effect of scale”.

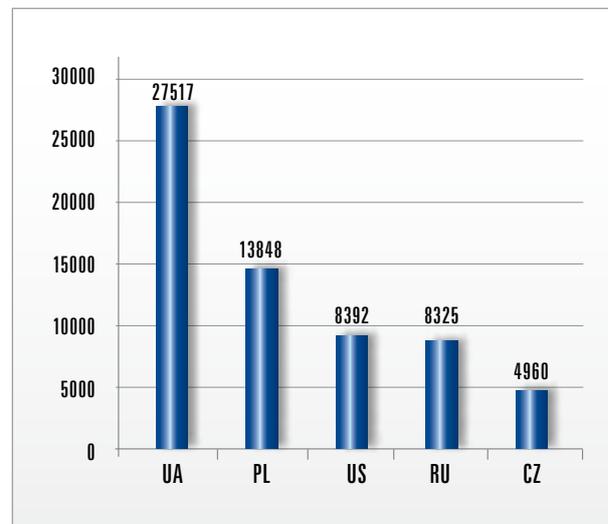
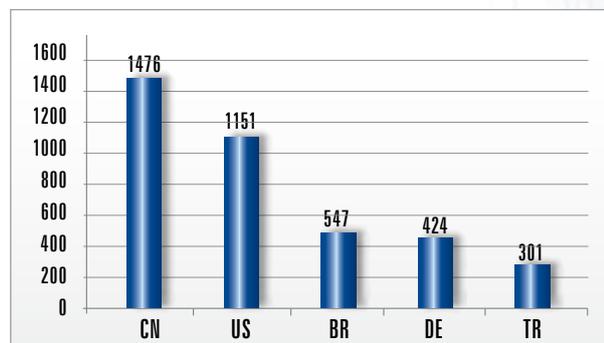


Chart 3.1.9. Number of scans per country

Below is a classification of countries from which the highest number of **unique** attacking IP addresses was observed:



Graph 3.1.10. Unique attacking IP addresses per country

Both the activity of Morto and other RDP scans may be detected with the use of **Snort** rules. In the ARAKIS system, the most frequently matching rules for the 3389/TCP port include the following:

- “ET POLICY RDP connection request” (sid:2001329),
- “ET POLICY MS Remote Desktop Administrator Login Request” (sid:2012709),
- “MISC MS Terminal server request” (sid:1448),
- „ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection” (sid:2001972).

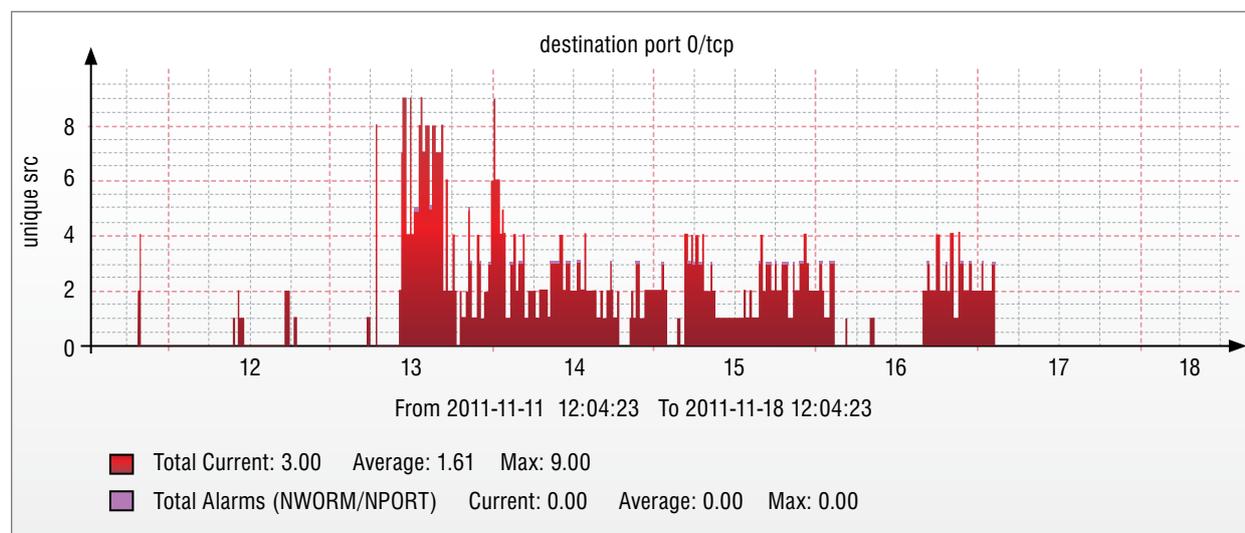
3.2 Strange traffic at the 0/TCP port

According to the IANA⁴ registry, the port 0/TCP is reserved. This means that no service should use this port for the purpose of network communication. The increased number of TCP packets directed to the “0” port, which was detected by ARAKIS system probes on 13 November 2011, raised our interest level. Connection attempts to this port were identified both by honeypots and by our darknet. The traffic returned to normal on 17 November 2011. We registered another short-term peak on 30 November 2011 and 1 December 2011.

Our observations related to the periods referred to above match the data from the DSHIELD⁵ system, which means that the anomaly could be observed globally.

Honeypot observations

Chart 3.2.1 presents the unique source addresses connecting to the port 0/TCP of ARAKIS honeypots.



Graph 3.2.1. Unique source addresses connecting to port 0/TCP

⁴<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

⁵<http://www.dshield.org/>



ARAKIS - 2011 Annual Report

Number of packets	Payload (hex)
640	00000000A0027D78
615	0000000000000000A0027D78
602	A0027D78
534	000000000000000000000000A0027D78
26	DB19F91B0000000000000000000000A0027D78
7	ED8DDA5E0000000000000000000000A0027D78
7	CE537D460000000000000000000000A0027D78
7	C9A7340E0000000000000000000000A0027D78
6	F080F25D0000000000000000000000A0027D78
6	F02FD77C0000000000000000000000A0027D78

Table 3.2.2. Payloads of packets sent to port 0/TCP

Between 13-17th November 2011 the honeypots observed approximately 15,000 packets to the 0/TCP port. Great majority of them (approximately 14,200) had a source port of "0" as well set in their headers. The majority of TCP headers themselves were mangled (i.e. incorrect header length) or made no sense at all (e.g. in the context of the flags set). The flag combinations seemed to make no sense as well.

When a TCP packet contained not just headers but data as well (the so-called payload), it always contained the hexadecimal A0027D78 string (usually this string was present on its own or was preceded by another string of varying length, made up of zeros and potentially random hexadecimal numbers – a typical expression describing this string is as follows: [0-9A-F]*0*A0027D78).

The payload's statistical data is presented below (TOP 10):

When analyzing the traffic characteristics, one may clearly observe that the string 000000000000000000000000A0027D78 is always present. Sometimes it is moved towards the beginning of the packet (far enough to make the "Data" field empty, as it contains only the 4 bytes A0027D78, or the string of zeros is shorter than 12 bytes). The original string may be also shifted to the right (then the string of zeros is preceded by random bytes). The random bytes impact the mangling of the TCP header, including the "strange" setting of flags. Below is an example of the packet in which the string is shifted in a manner that mangles the "options" field (marked) and flags of the TCP header.

```

Header length: 36 bytes
  > Flags: 0xba (SYN, PSH, ACK, URG, CWR)
    Window size: 80
  > Checksum: 0xff7f [validation disabled]
    Urgent pointer: 0
  < Options: (16 bytes)
    Unknown (0x6a) (option length = 197 bytes says option goes past end of options)
  > [SEQ/ACK analysis]
  < Data (4 bytes)
    Data: A0027D78
    [Length: 4]

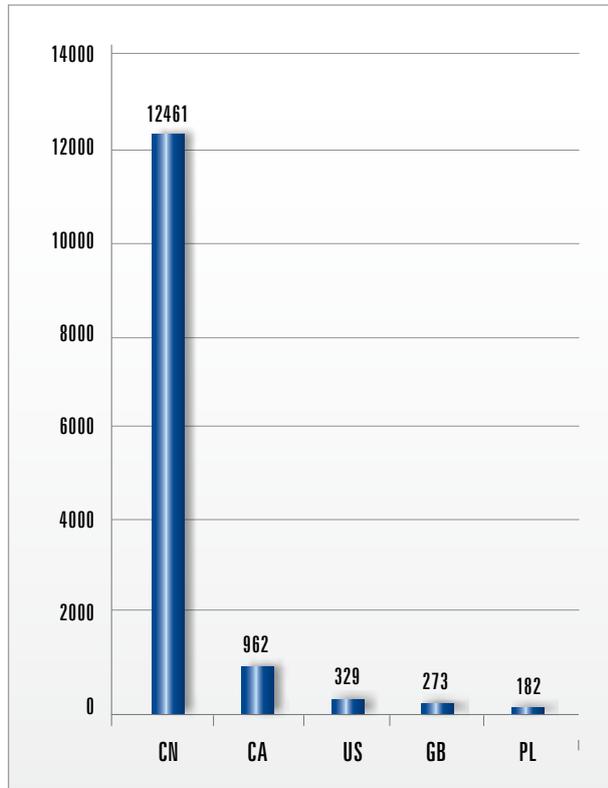
0000  00 1a 64 6e 13 a6 00 05 5d 6d a2 26 08 00 45 00  ..dn.... ]m.&..E.
0010  00 3c 82 80 40 00 34 06 6b d1 00 00 00 00 00 00  <..@.4. k
0020  00 00 00 00 00 2e 04 01 01 00 00 00 00 92 ba  ..P....]..G.....
0030  00 50 ff 7f 00 00 6a c5 20 47 00 00 00 00 00 00  .....}x
0040  00 00 00 00 00 00 a0 02 7d 78

```

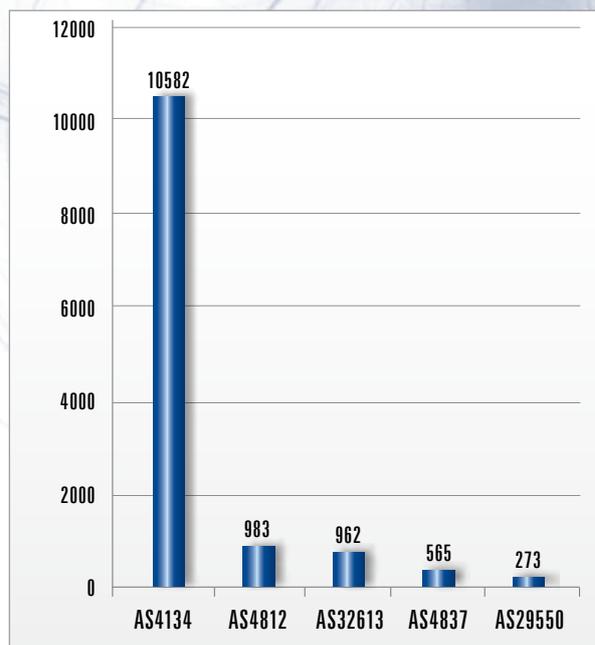
Chart 3.2.3. Mangled packet headed to port 0/TCP

The above may potentially mean that the bytes above the IP header are not the TCP protocol (despite the fact that the 0x06 value is set in the "protocol" field of the IP header). If so, someone was "testing" some kind of their own fourth layer protocol. Alternatively, reactions of various TCP/IP stacks to data mangled in a specific manner were tested.

In 84% of the cases the scans originated from addresses belonging to a Chinese ISP (mainly from a single autonomous system AS4134). Canada ranked second (6%), and the US third (2%). It has to be noted, however, that the source IP addresses may be spoofed. Attempts to establish a TCP connection with the 0 port should not usually trigger a reply (which was the case with our honeypots). If the persons responsible for generating such Internet traffic were aware of that fact, they did not expect any packets to be returned by the target IP address, so the source address could be spoofed. The graph below presents the statistical data concerning such abnormal traffic:



Graph 3.2.4. Number of packets per country (port 0/TCP traffic)



Graph 3.2.5. Number of packets per ASN (port 0/TCP traffic)

Below is the Snort system rule that matches the typical string of bytes. As the traffic described above is very peculiar, it cannot be ruled out that it may be detected at other ports as well. Therefore, the most general form is presented below:

```
alert tcp any any -> any any
msg:"Suspicious 0/TCP payload";
content:"|a0 02 7d 78|"; sid: 120003;
rev: 1;)
```

Snort rule describing the observed anomalous traffic on port 0/TCP

Summary

We are neither certain as to the cause nor to the objective of the abnormal traffic to the 0/TCP port. On the one hand, we could be dealing with a regular error, mistake or some kind of a research project, but on the other, we could be dealing with testing the behaviors of TCP/IP stacks when confronted with mangled TCP packets. As honeypots and the majority of "normal" services or systems do not generate any replies to this type of traffic, it remains unknown if the source IP addresses were fake (no interaction whatsoever). At present, the 0/TCP traffic is scarce and does not stand out against the so-called "background noise".

Kontakt

Address: NASK / CERT Polska
ul. Wąwozowa 18
02-796 Warszawa

Phone: + 48 22 3808 274

Fax: + 48 22 3808 399



Incident reporting: cert@cert.pl

Spam reporting: spam@cert.pl

Information: info@cert.pl

PGP key: <http://www.trusted-introducer.org/teams/0x553FEB09.asc>

Website: <http://www.cert.pl/>
<http://facebook.com/CERT.Polska>

RSS Feed <http://www.cert.pl/rss>

Twitter: [@CERT_Polska](https://twitter.com/CERT_Polska) http://twitter.com/CERT_Polska
[@CERT_Polska_en](https://twitter.com/CERT_Polska_en) http://twitter.com/CERT_Polska_en