

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

CERT POLSKA REPORT

AN ANALYSIS OF NETWORK
SECURITY INCIDENTS
- FIRST HALF OF 2011

How to read this document?.....	3
The most important observations summing up the report.....	3
Information about CERT Polska	5
Introduction.....	6

Analysis of incident submissions coordinated by CERT Polska








Amount of information in all categories.....	6
„Traditional” phishing.....	7
Sites associated with malware	9
From a sandbox to Polish networks: addresses visited by malware.....	10
Spam from Polish networks.....	11
Scanning	12
Most scanned services	12
Most infected Polish networks	13
Bots	14
Command & Control servers	18
DDoS attacks, fast flux and other submissions	19

How to read this document?

This report presents selected statistics on security incident data handled by CERT Polska in the first half of 2011 along with discussion and conclusions. It is our first semi-annual report and our first report translated into English – up till now we have published only annual reports in Polish. As a result of this report, we hope that our readers can obtain a relatively up to date view of the Internet threat landscape as seen by our team.

This report covers threats observed in networks allocated to Poland and the “.pl” domain. It is based on data received from different entities engaged in monitoring and responding to threats. As the report takes into account data concerning all the Polish providers, it gives a wide overview of what goes on in the “Polish” Internet. We compare our observations with those made in the report for the year 2010 as well as compare - when possible – Poland to the rest of the world.

The most important observations summing up the report

-  Despite the increasing number of automated information sources, we received less than half of submissions concerning Poland than we expected.
-  In February a new version of Zeus appeared that targeted Polish users. It was unique, as it attacked not only computers but also cell phones. An attacker could read and modify information provided in an SMS, including transaction authorization codes. It was the second, fully documented case of such an incident in the world.
-  In April, a large scale attack targeting Polish Internet users took place. A fake invoice in PDF format was sent in a mass mailing. After opening the attached invoice, the trojan SpyEye was downloaded and took control over a user’s computer. Subsequently, all confidential information entered by user on websites (including e-banking sites) could be captured.
-  During the period between the end of April and June 2011 there were many serious leaks of customer data worldwide. The most serious data theft concerned Sony. Hackers took data of 100 million user accounts, and probably also about 10 million credit cards from the PSN and SEN services databases. User data leaked also from Nintendo, Codemasters, pornographic site pron.com and Citibank (200 thousand accounts). Some attacks are ascribed to Anonymous and LulzSec groups. These cases also affected Polish users.
-  Although hosting providers in Poland are far more affected by phishing than Internet access providers, they are much more effective at reacting to such threats.
-  More than every fifth (21%) domain in Poland involved in a phishing case, belonged to an e-commerce site.
-  Polish networks accounted for about 2% of malicious webpage cases worldwide. This was a percentage-wise increase compared to last year (1.4% for all of last year).



Summary

The most important observations summing up the report



Surprisingly, we discovered that a large majority of malicious websites were located on hosts belonging to Internet service provider networks, not hosting providers as was the case last year.



We identified 1,033,681 unique incidents of spam originating in Poland. More than half (573,721) originated from the Netia network.



We noted only 151,502 incidents of spam from Polish Telecom network. This observation is not surprising – this has been the case since the end of 2009 when Polish Telecom introduced filtering of port 25/TCP.



An overwhelming majority of scans hit port 445/TCP. These can be mostly attributed to attempts to exploit a vulnerability connected with an error in the handling of RPC requests – described in Microsoft bulletin number MS08-067.



The Top 10 list of infected networks in Poland largely reflects the size of the operators with respect to number of users.



In the first half of 2011, we observed over 1 million bots in Polish networks.



The most common bots reported to us were Torpig and Rustock. Their number was at least three times larger than that of other bots.



Most bots were observed in AS 5617 belonging to Polish Telecom (almost 560 thousand).



A large number of bots but a small amount of spam from Polish Telecom clearly indicates the effectiveness of blocking port 25/TCP - we would therefore recommend a similar measure for other ISPs.



The increase of sandbox related information is attributed to Sality trojan activity, which used Interia domains as C&C.



We did not receive any APT (Advanced Persistent Threat) reports regarding entities in Poland for the first half of 2011.



The United States and Canada dominated as a source of phishing cases. This dominance was even greater than in 2010. Together they accounted for 60% of submissions.



There was an increase in China's share in the statistics of countries in which malware URLs are located. In percentage terms, the United States has less malware URLs than last year. However, it still remains the lead location. Over 50% of malicious websites reported to us were located in the two countries mentioned above.



50% of C&C servers worldwide reported to us were located in the United States and Germany.

Information about CERT Polska

CERT Polska (Computer Emergency Response Team Poland - <http://www.cert.pl/>) is a security incident handling team operating in the framework of the Research and Academic Computer Network Research Institute (<http://www.nask.pl/>). CERT Polska was established in 1996 and since 1997 has been a member of FIRST (Forum of Incidents Response and Security Teams - <http://www.first.org/>) – an organization that associates response and security teams from all over the world. Since 2000 it has also been a member of TERENA TF-CSIRT (<http://www.terena.nl/tech/task-forces/tf-csirt/>) that brings together European response teams and Trusted Introducer (www.trusted-introducer.org), an initiative in the framework of the TERENA TF-CSIRT¹. Within these organizations CERT Polska cooperates with similar teams around the world - at an operational level and through research and development projects.

The main tasks of CERT Polska include:

- registering and handling network security incidents for Poland and the “.pl” domain name space;
- providing watch & warning services to Internet users in Poland;
- conducting analyses of advanced Internet threats;
- cooperation with other incident response teams, including those operating in the framework of FIRST and TERENA TF-CSIRT;
- conducting informational and educational activities aimed at raising awareness about IT security, maintaining a blog at <http://www.cert.pl/>, social networking accounts, and organizing an annual conference on IT security aimed at Polish users (SECURE conference – <http://www.secure.edu.pl/>);
- conducting research and preparing reports on security of the Polish Internet resources;
- independent testing of IT security products and solutions;
- work on creating standards of registration and handling of incidents;
- taking part in national and international projects in the area of IT security aimed in particular at developing tools to support intrusion detection and incident handling ;

¹ In 2001 CERT Polska Team was awarded the highest trust certification under TERENA's Trusted Introducer.



Introduction

This report is our first semi-annual report. It is also our first report made fully available in the English language. We decided to opt for a half year report as we believe in the importance of providing as up to date view as possible on threats in the Internet. We also believe in the necessity of sharing threat analysis information with the wider CERT and security community in general. Starting several years ago, we observed an important shift in the way incident information is submitted to our team. We receive a larger and larger volume of incident data from external automated data feeds, making manual incident handling an impossible task. This has forced us to prioritize, handling just the more serious cases, with the rest forwarded to entities directly responsible for security in their networks, such as Polish Internet providers. 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. In this report, as opposed to our annual reports, we focus mostly on the automated submissions. Incidents handled manually will be summarized in the full year report for 2011.

Amount of information in all categories

In the first half of 2011, we received 3,906,411 submissions from external automated data feeds attributed to Polish networks. Most of them concerned spam and other botnet related activities. The chart on the following page illustrates the distribution of the categories that we selected in the report (note the logarithmic scale!)

The data comes from various sources. These sources, in turn, use different methods for data collection – even for the same types of incidents – and often present them in different ways. This makes comparison difficult. Therefore, we distinguish only broad categories of submissions. Just like in 2010, submissions are divided into 10 categories that describe their common features in what we view as the most appropriate way: spam, botnets, scanning, malware URLs, C&C servers, data derived from sandboxes, phishing, fast flux, DDoS and others. These categories are discussed in more detail below.

Comparing these data with those from 2010, a decline in the number of events may be observed, even though we have an increasing amount of information sources. The most considerable decline can be seen in the botnet category - based on data from 2010 we would expect at least twice as many incidents. We also received almost 50% less submissions than we had expected in the following categories: spam, phishing, malware URLs, fast flux and C&C servers. We received more in the sandbox, DDoS and scanning

Analysis of incident submissions coordinated by CERT Polska

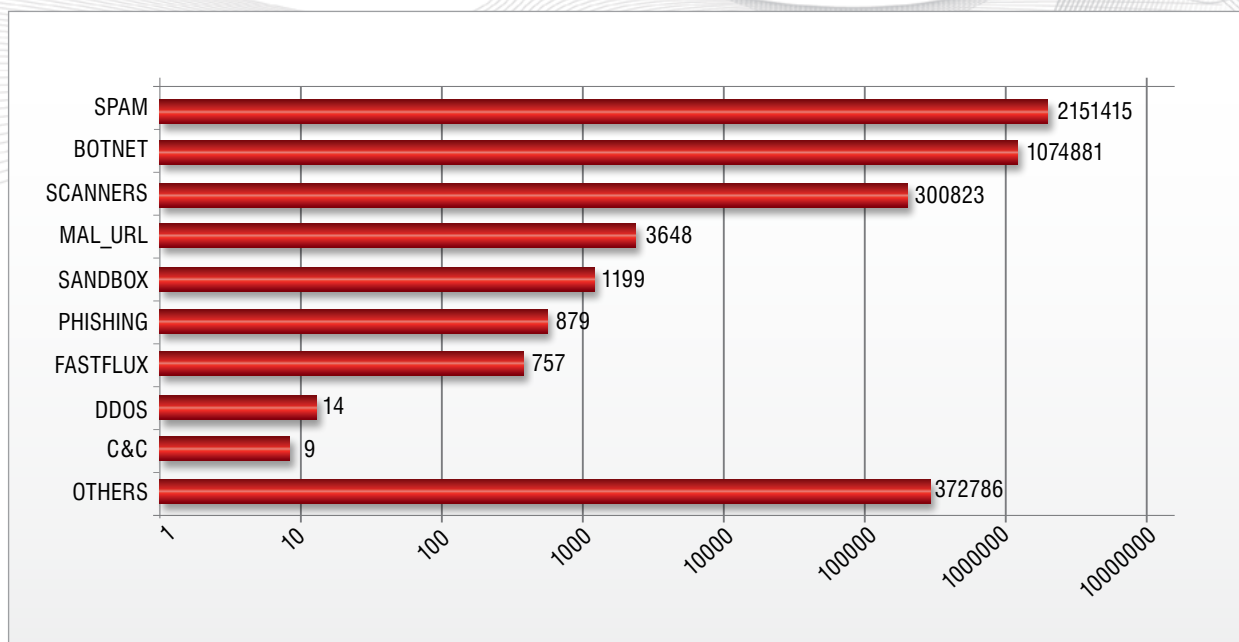


Chart 1. Number of the automated submissions in the categories categories.

„Traditional” phishing

In this category of incidents there were no significant changes in relation to the year 2010. The position of Poland compared to other countries is almost unchanged. This is despite the fact that the absolute numbers are lower than expected. In the first half of 2011, we had 879 phishing cases in Poland compared to 2,222 throughout all of last year. Thanks to the fact that we also often receive data for other countries, we can compare Poland to the rest of the world. From our observations, the United States and Canada dominate among the countries where phishing cases were found. Together they generated 60% of our submissions. Last year this percentage was 53%. The chart 2. illustrates the number of reported phishing incidents in Poland in comparison to other countries (from January to June).

1	US	91111	50,1%
2	CA	15567	8,6%
3	DE	9197	5,1%
4	GB	8703	4,8%
5	CL	7095	3,9%
6	RU	4813	2,6%
7	HK	4775	2,6%
8	FR	4311	2,4%
9	CZ	3925	2,2%
10	NL	3365	1,8%
20	PL	879	0,5%

Chart 2. Number of reported phishing cases in relation to geographical location



Analysis of incident submissions coordinated by CERT Polska

There was no change in the distribution of operators in whose networks phishing cases were detected. As in 2010, mostly hosting providers faced this problem.

The numbers shown above illustrate the number of phishing incident reports. They concern 507 unique URLs. We investigated more closely how many incidents involved the same URLs.

Average number of submissions / URL	Number of URLs	ASN
2,94	16	31242 (TKP)
2,83	6	6714 (GTS)
2,67	12	41508 (IWACOM)
2,50	20	49102 (CONNECTED)
2,38	8	29314 (VECTRA)
2,32	19	21021 (MULTIMEDIA)
2,03	36	5617 (TP)
1,85	26	29522 (KEI)
1,78	23	16265 (LEASEWEB)
1,63	8	12968 (CROWLEY DATA POLAND)
1,42	110	15967 (NETART)
1,40	10	43470 (NETWORK COMMUNICATION)
1,33	9	47544 (IQ PL)
1,33	61	12824 (HOME.PL)
1,25	12	44514 (INOTEL)
1,18	11	41079 (SUPERHOST.PL)
1,13	15	16138 (INTERIA)
1,00	15	9085 (SUPERMEDIA)

Chart 4. Number of traditional phishing cases in Poland grouped by autonomous systems

156	15967 (NETART)
81	12824 (HOME.PL)
73	5617 (TP)
50	49102 (CONNECTED)
48	29522 (KEI)

Chart 3. Number of phishing cases in Poland per autonomous system

The fact that most often the same sources report a given URL periodically until it is cleaned can be used as an indicator of how long a phishing site is hosted before being removed. On average, we received 1.72 submissions per URL. In the worst cases 6 submissions concerned a single URL. We made a comparison of this ratio among operators where more than 5 URLs were identified to contain a phishing webpage in a six month timeframe. The chart 4. – with “traditional” ISPs coming out on top seems to illustrate that although hosting providers are more often used for phishing, they are more efficient at taking it down.

The reported phishing sites were located in 346 different domains. The vast majority of sites are a result of a website compromise. This method was used for 228 (65.9%) domains. However, 55 (15.9%) domains were registered through sites offering free subdomains, for example www.paypal.de.blo.pl. More than every fifth (21%) domain where phishing case was observed, belonged to an e-commerce site.

Among the sites that are faked most often, PayPal (85 URLs) still dominates, but we also noted the presence of Western Union (9 URLs) and Amazon (6 URLs). Banks appeared in a total of 24 cases.

Analysis of incident submissions coordinated by CERT Polska

Sites associated with malware

This category describes incident reports obtained from external data feeds that involve cases of hosting malicious files in Polish operators' networks. These 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

The submissions do not concern phishing which is discussed in another category.

In this half-year, we had fewer incidents concerning malware sites than we expected (counted as a unique combination of date of submission, IP address and the URL). Based on statistics from last year, we expected at least twice as many submissions. We are unable to explain why we received fewer reports.

In the first half of 2011, we received 3,648 incidents concerning Poland (in the whole of last year we had 12,917 incidents). This was about 2% of submissions worldwide that we received. This is a percentage increase in relation to data from 2010 (when Poland was responsible for 1.4% of submissions worldwide).

Interestingly, even though the United States remain the predominant location of malware, there was a significant decrease of their percentage share: (34% percent vs. 48,2%), mainly due to a significant increase of China (last year also ranked second, but only with 11.9% share as opposed to the 20% first half of this year).

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

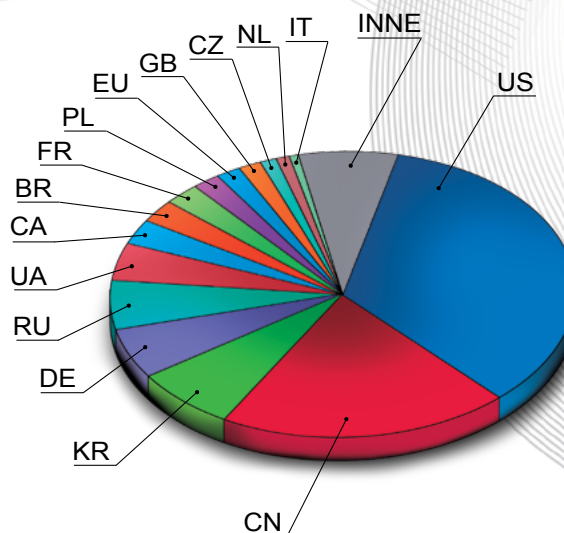


Diagram 1. Countries where malware were found the most often (by number of submissions)

Number of sub-missions	Country	Number of submissions	Number of Url/ IP
1	US	61187	34%
2	CN	36134	20%
3	KR	12867	7%
4	DE	10127	6%
5	RU	10039	6%
6	UA	7501	4%
7	CA	5078	3%
8	BR	4567	3%
9	FR	4213	2%
10	PL	3648	2%
11	EU	2949	2%
12	GB	2875	2%
13	CZ	1991	1%
14	NL	1671	1%
15	IT	1148	1%

Chart 5. Number of incidents of malware software on WWW sites by geographical location



Analysis of incident submissions coordinated by CERT Polska

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.

When we analyzed the results for Poland, they turned out to be quite surprising. The biggest perpetrators are the largest ISPs such as Polish Telecom, Netia and ATM. We expected something different – a ranking similar to the last year’s which was dominated by the largest hosting providers – HOME.PL, Netart or KEI. The average number of URLs per single address also decreased.

Number of sub-missions	Autonomous system	Operator	Number of URL/IP
986	5617	TP	3,5
415	6714	ATOM	6,9
344	12741	NETIA	5,1
257	12824	HOME.PL	2,7
231	15694	ATMAN	2,9

Chart 6. Number of malware cases on the Polish WWW sites grouped by autonomous systems

It is not clear to us why there were changes in the ranking of operators – whether they are a result of the way in which data concerning malicious sites is collected by our sources or whether the reason is that the hosting providers introduced better security policy which in turn resulted in the changing of the strategy of the cybercriminal underground.

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, 1,302 unique files attempted to connect to 1,199 unique WWW and FTP addresses (2,752 in the whole 2010). Approximately 25% of them (32% in 2010) were recognized by antivirus programs as malware (on the basis of Cymru Malware Hash Registry – <http://www.team-cymru.org/Services/MHR/>).

Most connections were observed to a server with an IP address of 212.33.79.77. We observed 275 unique requests. They were generated by a Trojan horse that, when installed on the victim’s system, attempted to connect to

its command center. Interestingly, this Trojan was never assigned a name by the antivirus vendors.

Another very interesting situation relates to addresses in the interia.pl domain: pelcpawel.fm.interia.pl, radson_master.fm.interia.pl, aanna74.eu.interia.pl and mattfoll.eu.interia.pl. In all these cases, the culprit was a trojan horse named Sality. Again, as in the example described above, it attempted to connect to its command centers.

In the case of appmsg.gadu-gadu.pl, as last year, we dealt with software initiating connections to gadu-gadu network. 23% of connecting files were identified as malware.

Unfortunately, we were unable to determine exactly why the rest of addresses were visited.

Analysis of incident submissions coordinated by CERT Polska

1	212.33.79.77	275	9	s1.footballteam.pl	25
2	pelcpawel.fm.interia.pl	85	10	hit.stat24.com	22
3	radson_master.fm.interia.pl	50	11	ftp.webpark.pl	18
4	webpark.pl	46	12	uaneskeylogger.hdo01.pdg.pl	18
5	footballteam.pl	38	13	mattfoll.eu.interia.pl	17
6	aanna74.eu.interia.pl	30	14	kluczewsko.gmina.pl	16
7	appmsg.gadu-gadu.pl	30	15	www.hotgame.za.pl	16
8	www.odlotek.ugu.pl	26			

Chart 7. Number of malware cases on the Polish WWW sites grouped by autonomous systems

Spam from Polish networks

In the first half of 2011, we received 2,151,415 incident reports about hosts sending spam from Polish networks. When we take into account all submissions concerning a single IP address, between which there was a break not longer than 3 days we can distinguish 1,033,681 incidents. More than half of these (573,721) related to the Netia network. By comparison, Polish Telecom which introduced filtering of port

25/TCP for its clients at the end of 2009, had only 151,502 incidents, almost the same as Plus network (138,591 incidents).

In the first quarter of 2011 we noticed an increase of spam cases originating in Poland. At the turn of April and May, the number dropped to similar levels as in the middle of 2010. Since then we have observed a slight decrease.

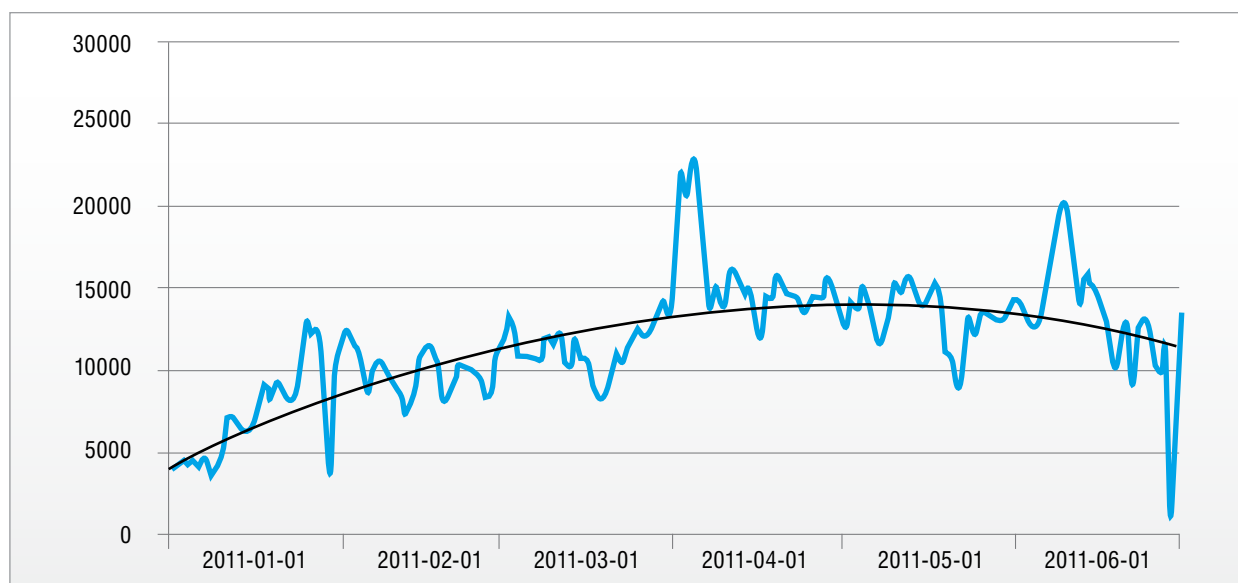


Diagram 2. Number of events concerning hosts sending spam from the Polish networks



Analysis of incident submissions coordinated by CERT Polska

Scanning

As in previous years one of the main categories of submissions is scanning. Scanning is usually related to botnet or worm activity, sometimes to network mapping tools. Over the years, scanning has become background noise on the Internet often ignored by many users and even dedicated security teams. Nowadays, many organizations detect and analyze information on scanning in a fully automated way, without manual intervention. If an incident is analyzed carefully it can be associated with the activity of a particular botnet and worm. If not, it remains classified as scanning and is reported to us as such.

We analyzed the most often scanned TCP/UDP ports and the most common sources of scanning from Poland. We examined scanning incidents first counting the unique source IP addresses that were registered by reporting systems in the first half of 2011 (globally or per destination port), and also counting unique combination of IP/ destination port scans seen per day. The first category allows for estimation of the number of infected computers, second one illustrates the aggressiveness of the scanning activity.

Most scanned services

As in the whole of 2010, the first half of 2011 saw a clearly dominant port 445 TCP as the most often attacked port. This is not surprising – a large amount of “wormable” serious vulnerabilities affecting Microsoft software can be found in applications listening on this port (MS08-067 in particular).

Lp.	Number of unique IP seen	Destination port/protocol	Probable leading mechanism of attacks
1	143009	445/TCP	Buffer overflow attacks on Windows RPC service
2	774	139/TCP	Attacks related to file sharing/Windows printers
3	752	1433/TCP	Dictionary attacks on MS SQL
4	648	135/TCP	Attacks on Microsoft Endpoint Mapper service
5	645	80/TCP	Attacks related to web applications
6	341	25/TCP	Possible spamming attempts
7	268	4899/TCP	Attacks on a remote control application, radmin
8	245	5900/TCP	Attacks on VNC
9	165	23/TCP	Dictionary attacks on telnet service
10	152	9988/TCP	Part of an attack sequence (loading of a worm)

Chart 8. TOP 10 of destination ports by number of unique scanning sources

In comparison to 2010, we observed fewer hosts scanning 22/TCP port (SSH service on which dictionary attacks are often carried out). Port 5060/TCP (SIP protocol) also dropped out of the TOP 10 list. However, port 135/TCP (Microsoft RPC Endpoint Mapper) and port 25/TCP related to STMP service (e-mail) made a reappearance.

Analysis of incident submissions coordinated by CERT Polska

Most infected Polish networks

The distribution of infected unique IP addresses amongst Polish operators is shown below. It sheds some light on the scale of malware infections in Poland.

Lp.	Number of unique IP	Autonomous system number	Operator
1	52834	5617	TP
2	27788	12741	NETIA
3	26340	15857	DIALOG
4	11691	43447	PTK CENTERTEL
5	11215	8374	PLUSNET
6	8876	21021	MULTIMEDIA
7	1950	25388	ASK-NET
8	1570	29314	VECTRA
9	1338	6714	ATOM
10	727	12912	PTC

Chart 9. TOP 10 of operators in Poland grouped by the number of scanning source IP

Like last year, we believe that the ranking reflects the size of operators user-wise – thus the top position of Polish Telecom is not surprising.

We also investigated the top operators with respect to frequency of observed scans – for this purpose we added up source IPs reported to us daily (effectively IPs that are reported to us most often).

Sum of all reported IP/day	Autonomous system number	Operator
77287	5617	TP
36171	15857	DIALOG
32564	12741	NETIA
15691	29314	VECTRA
14041	21021	MULTIMEDIA
12553	43447	PTK CENTERTEL
11827	8374	PLUSNET
10220	25388	ASK-NET
9315	35191	ASTA-NET
9140	16265	LEASEWEB

Chart 10. Ranking of operators in respect to frequency of observed scans



Analysis of incident submissions coordinated by CERT Polska

Bots

This category includes computers in Polish networks that are part of botnets and are not included in other categories. Botnets have become the „Swiss Army Knife” in the miscreant toolset, used for purposes such as theft of user credentials, ad fraud, spam, DDoS or simply as an additional layer of anonymity.

In the first half of 2011, we observed over 1 million bots in Polish networks. Torpig and Rustock dominated. Their number was at least three times larger than the other bots. We observed almost 380 thousand machines infected by Torpig and almost 350 thousand machines infected by Rustock. Other dominant bots included IRC bots, mebroot and Conficker. In the case of IRC bots there were many varieties with an IRC management channel as the common characteristic feature. Special attention should be devoted to mebroot that was used to steal confidential data from financial institutions.

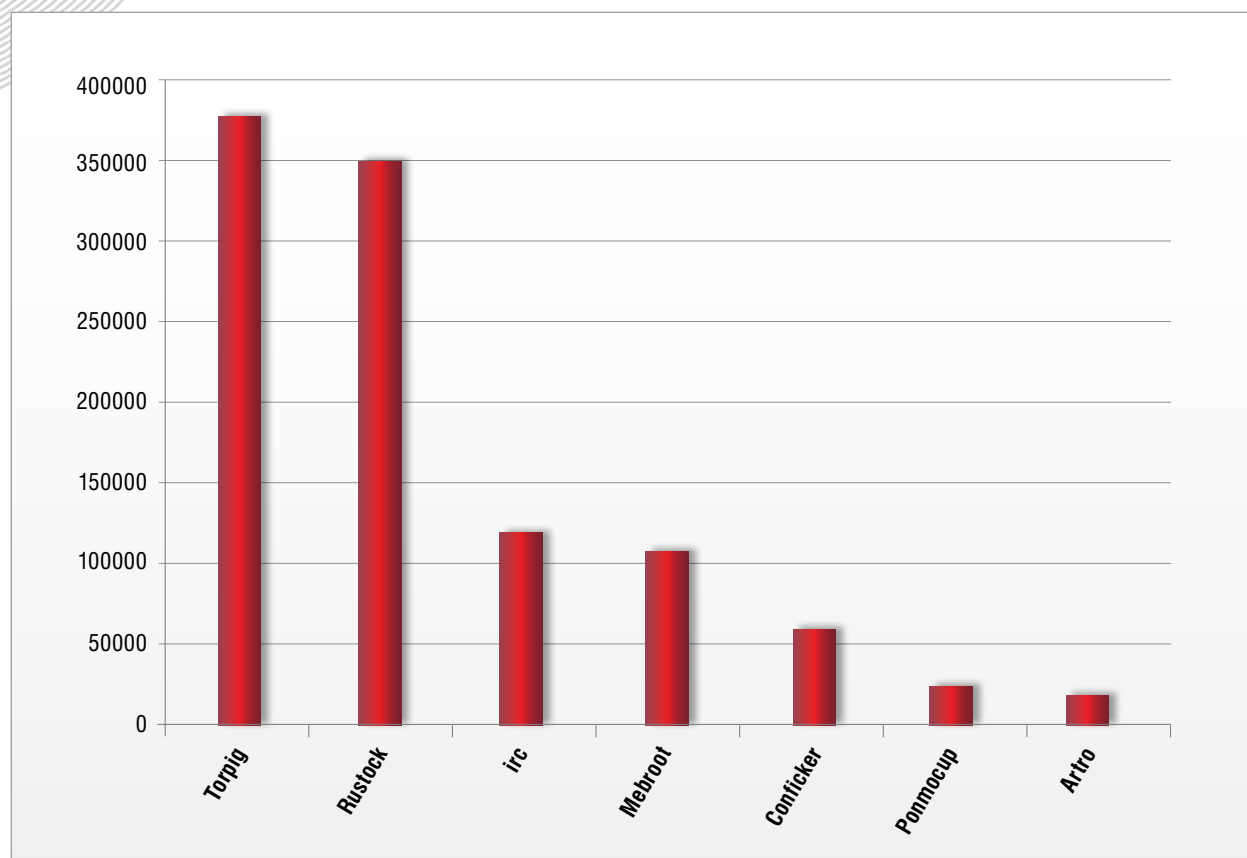


Diagram 3. Number of bots by types

In the first half of 2011, the daily distribution of bots was between two and four thousand machines. In the middle of March it increased to about 12 thousand. This was related to Rustock submissions that we started receiving from the 16th of March (see diagram 5.). At the turn of April and May, there was another important incident resulting in 14 thousand received submissions. This was the result of activities of security researchers from the University of California in Santa Barbara who took over the Torpig botnet. This allowed for more precise registrations of victims that connected to C&C servers. This peak can be observed on the diagram 6. showing the number of computers infected by Torpig.

Analysis of incident submissions coordinated by CERT Polska

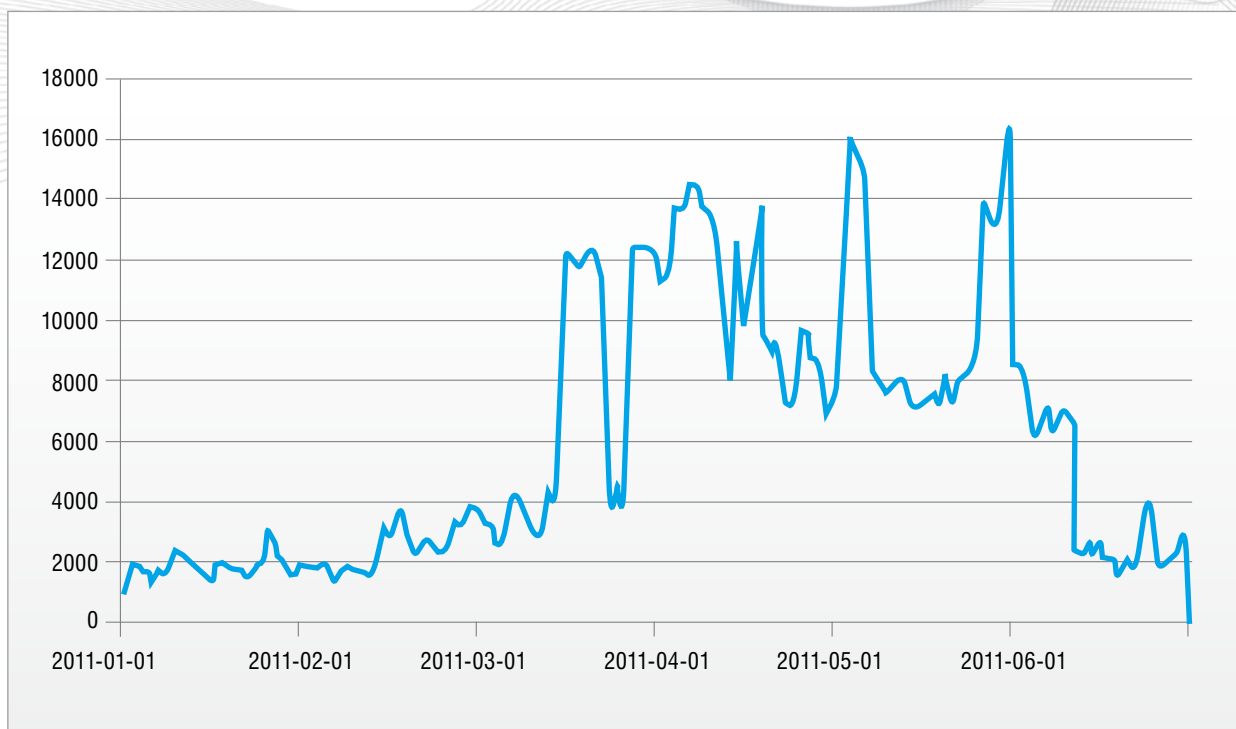


Diagram 4. Daily distribution of bots in the first half of 2011

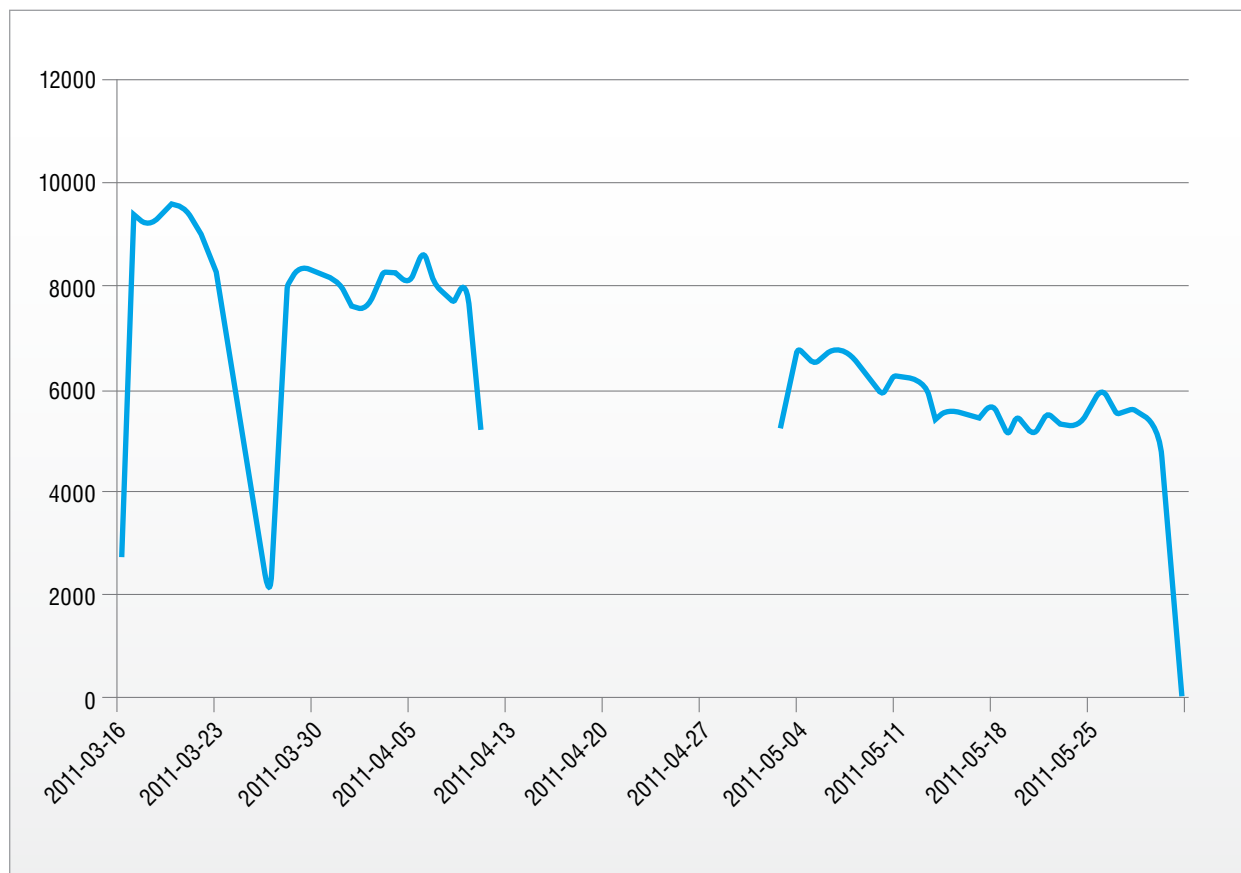


Diagram 5. Daily distribution of Rustock in the first half of 2011



Analysis of incident submissions coordinated by CERT Polska

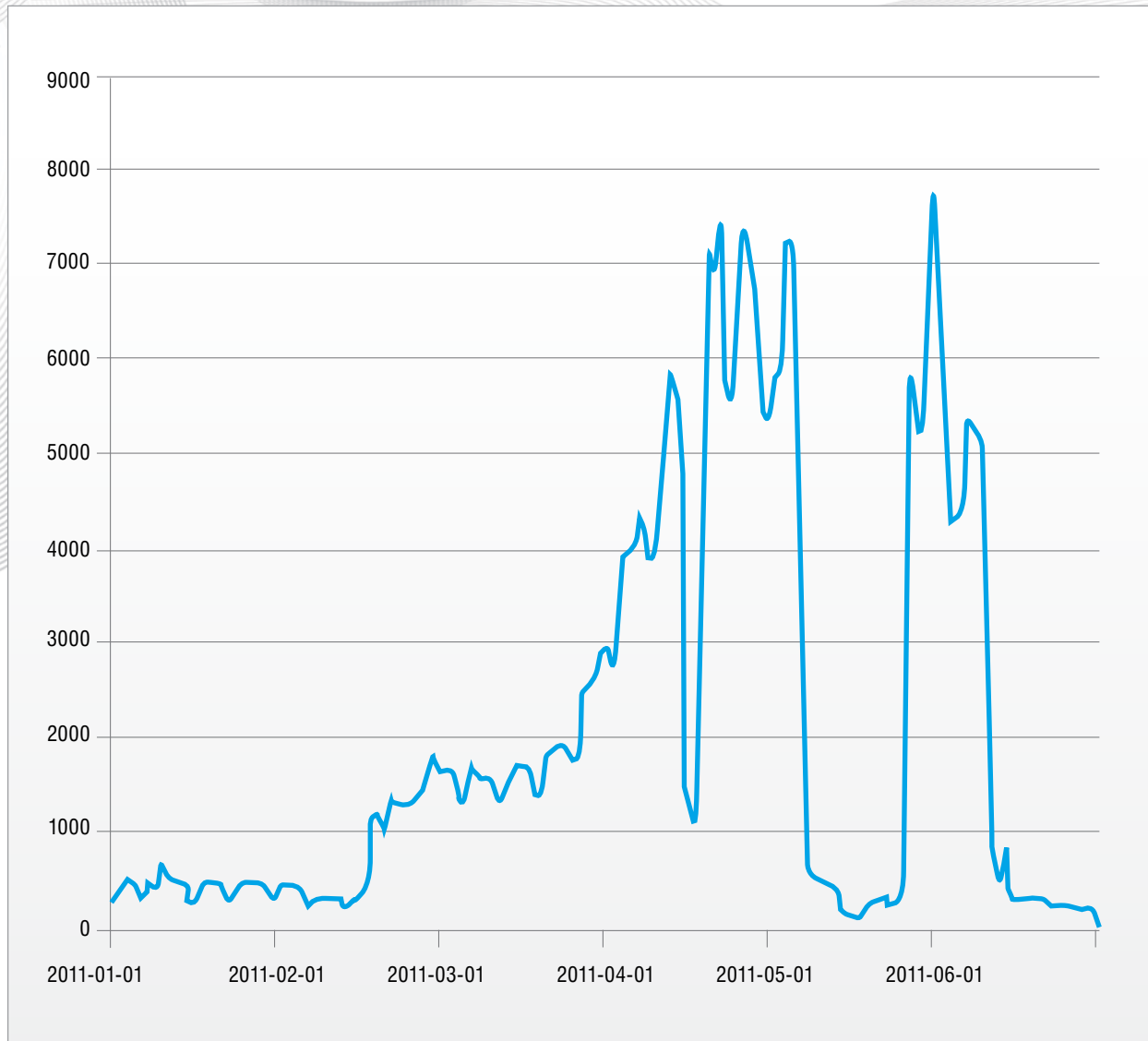


Diagram 6. Daily distribution of Torpig in the first half of 2011

In the case of IRC bots we registered 800 infected machines per day on average. When it comes to mebroot (diagram 7.), most of the time the number of infected machines fluctuated between a few hundred and 1,500 machines per day. However, two events are exceptions here. The first one took place between the 15th and 20th of April (over 8,500 computers), and the second one on the 31st of May (over 6,500 computers). We speculate that this might be due to an attack aimed at Polish users of financial institutions.

Most bots were observed in AS 5617 belonging to Polish Telecom (diagram 8.). It was a number close to 560 thousand and up to four times larger than the number of bots in AS 12741 belonging to Netia (about 140 thousand). In the networks of other operators there were less than 50 thousand infected computers. There is no doubt that most bots are located in the networks of the operators that provide Internet for individual users. These are large telecommunication companies like Polish Telecom or Netia, Internet providers in cable networks – Multimedia and Vectra and also mobile Internet providers – T-Mobile and Polkomtel. More than half of all bots (about 55%) were in the Polish Telecom network, while 15% were in the Netia network.

Analysis of incident submissions coordinated by CERT Polska

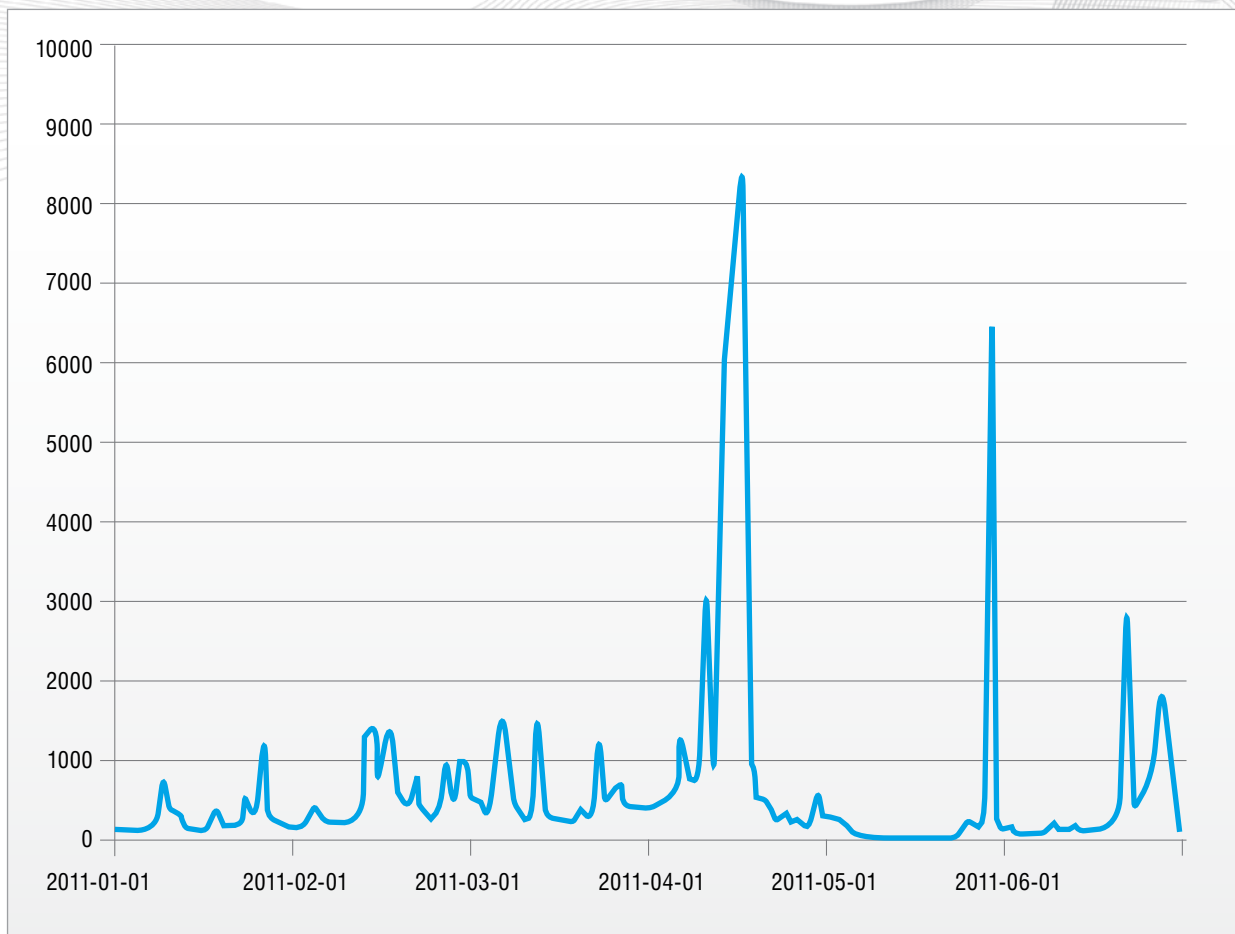


Diagram 7. Daily distribution of mebroot in the first half of 2011

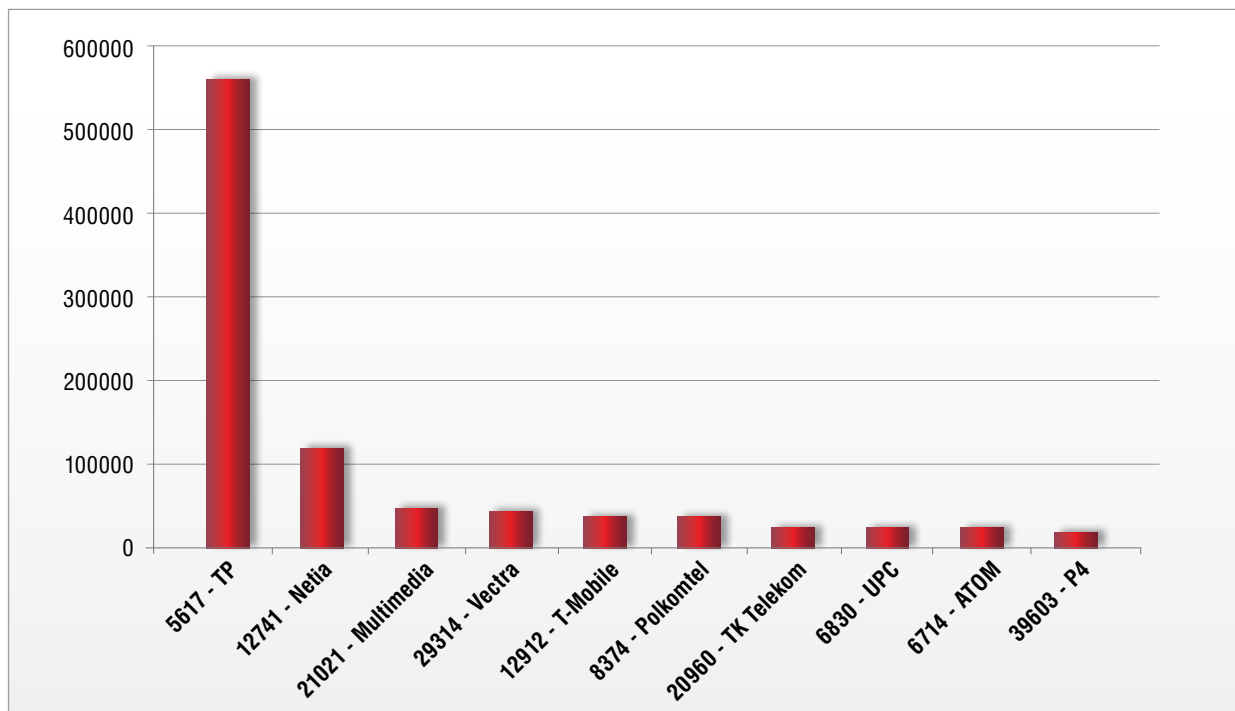


Diagram 8. Distribution of bots grouped by autonomous systems



Analysis of incident submissions coordinated by CERT Polska

Command & Control servers

In the first half of 2011, we received 1,565 submissions from external automated data feeds that concerned unique Command & Control servers used to manage botnets. They were located in 68 countries.

Most of these were in the United States – 32.1%. Together with Germany, the USA hosts almost 50% of C&C controllers. Like last year, the leaders in this category are the countries of Western Europe such as Great Britain, the Netherlands and France. China occupies a relatively low position – the 10th on the list. Based on this data Poland appears to be rarely used for C&C purposes – it is on the 30th position with 9 controllers, even lower than last year, when Poland was the 25th on the list.

Item	Country	Number of C&C	Percentage share
1	US	502	32,1
2	DE	209	13,4
3	GB	86	5,5
4	RU	78	5,0
5	NL	57	3,6
6	FR	57	3,6
7	CA	41	2,6
8	TR	37	2,4
9	CL	34	2,2
10	CN	29	1,9
11	CY	28	1,8
12	UA	25	1,6
13	LU	25	1,6
14	SG	22	1,4
15	KR	21	1,3
-	-	-	-
30	PL	9	0,6

Chart 12. C&C servers by geographical location

Number of C&C	AS	Operator
3	12741	NETIA
2	5617	TP
2	16265	LEASEWEB
1	29314	VECTRA
5	8256	LODMAN

Chart 11. Number of C&C servers in Poland

Most of the submissions from Poland related to IRC servers. In comparison to last year, the most affected provider is NETIA, not Polish Telecom. However, because of the small number of submissions it is difficult to draw any reasonable conclusions. It is interesting that controllers appeared in Leaseweb, a Dutch operator, whose some networks are registered in the RIPE database as being in Poland.

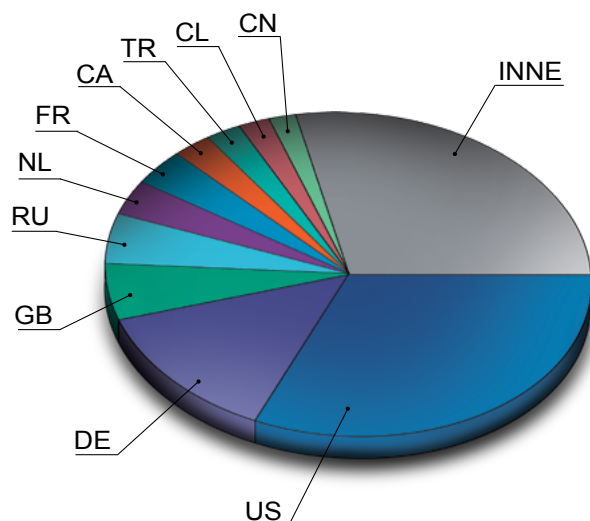


Diagram 9. Countries where C&C servers were located the most often

Analysis of incident submissions coordinated by CERT Polska

DDoS attacks, fast flux and other submissions

In this section of the report we present a brief overview of other types of submissions from which we distinguished two important categories: DDoS and fastflux.

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.

In the first half of 2011, we received 757 submissions (each with a different IP number) on usage of Polish computers for fast flux purposes by 17 domains. Like last year, the incidents mostly concerned networks with large number of individual users – almost half of the IP addresses belonged to Polish Telecom. However, the number of incidents is lower than in 2010. In our opinion the reason is that this technique is becoming less popular.

Other reported submissions concerned open DNS resolvers and brute force attacks. These incidents will be analyzed in the report at the end of this year.

Contact

Incident reporting: cert@cert.pl
Spam reporting: spam@cert.pl
Information: info@cert.pl
PGP key: <http://www.trusted-introducer.org/teams/0x553FEB09.asc>
WWW: <http://www.cert.pl/>
<http://facebook.com/CERT.Polska>
RSS feed: <http://www.cert.pl/rss>
Twitter: http://twitter.com/CERT_Polska_en

Address: NASK / CERT Polska
ul. Wąwozowa 18
02-796 Warszawa, Poland
Phone number: + 48 22 3808 274
Fax number: + 48 22 3808 399