ISSN 2084-9079

REPORT 2012

CERT Polska

An analysis of network security incidents

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

Contents

Contents

1 Introduction

Since 1996 CERT Polska has been preparing and publishing annual statistics on ICT security incidents in Polish on-line resources that have been reported to the team. This year's report gives a general overview of threats detected on and aimed at Polish networks and presents current trends in this field.

The report consists of five main sections. Section 2 and 3 presents in detail the statistics and analysis of incidents coordinated and handled by CERT Polska.

Section 2 contains information on threats in Polish networks, submitted to CERT Polska by various entities that monitor and respond to threats, as well asf rom its own systems. As it covers almost all Polish ISPs, the report gives a hopefully reasonable overview of what goes on in networks allocated to Poland.

Section 3 focuses on the operational activity of CERT Polska. These data are collected from incident management systems and involve incidents which required a manual intervention from CERT Polska (as opposed just to incident coordination with the appropriate parties, as in Section 2, often a fully automated process).

We identify seven key issues relating to security incidents observed in 2012 that were analyzed by our team and that we considered worth a closer look. These are described in section 4.

Section 5 focuses on various initiatives in the framework of national and international activities of CERT Polska that took place last year.

A special part of the report is dedicated to the early warning ARAKIS system – a nation-wide network of honeypot sensors. It contains among other the statistics on alarms generated by the system and descriptions of interesting network threats.

It should be emphasized that numbers from this year's report should not be directly compared to those from our previous studies, even though incidents have been divided into the same categories. This is due to several factors that are described in detail in the report, most important being that the statistics depend on the amount and type of data submitted by external entities: sources which come and go over time.

This year, in order to present a wider overview of security events in the networks of Polish operators, we took into consideration not only absolute numbers of security events in the operator's network, but we also tried to normalize the security events with respect to the network operator's size.

1.1 Key observations summarizing the report

- In 2012 CERT Polska registered over 10,500,000 automated submissions concerning IT security breaches. Most of these involved spam and bots.

- For the first time since 2005 the number of incidents handled manually by CERT Polska, which include the most serious incidents detected throughout the year, has increased. In 2012 there were 1,082 such incidents, an increase of nearly 80% more from the previous year, mainly due to malware and phishing.

- Poland compares favourably against other countries with regard to the number of websites used for phishing and hosting malware, outside the top ten in both statistics. Unfortunately, it is much worse in case of problems related to infected end user machines: ie. machines used by bots, for scanning and spam. Most affected are the networks of mobile operators and Netia – one of the largest telecommunication operators, which operates a large DSL network.

- Most reports concerning bots (infected machines centrally managed by miscreants), involved three types of malware: Virut, DNSChanger and various flavors of ZeuS. In total, we observed an average of 8 000 bots each day infected with these types of malware.

- We have been observing a steady growth in the number of phishing incidents – both in the traditional form, involving the creation of sites that pretend to be bank, e-store etc. services, as well as connected with malware that is able to modify the content of bank web pages served to user on the fly.

- SMB in Microsoft Windows (445/TCB) is still the primary service being scanned. Worms which propagate by using this service, such as Sasser or Conficker, are still doing well despite the fact that they were created five and more years ago!

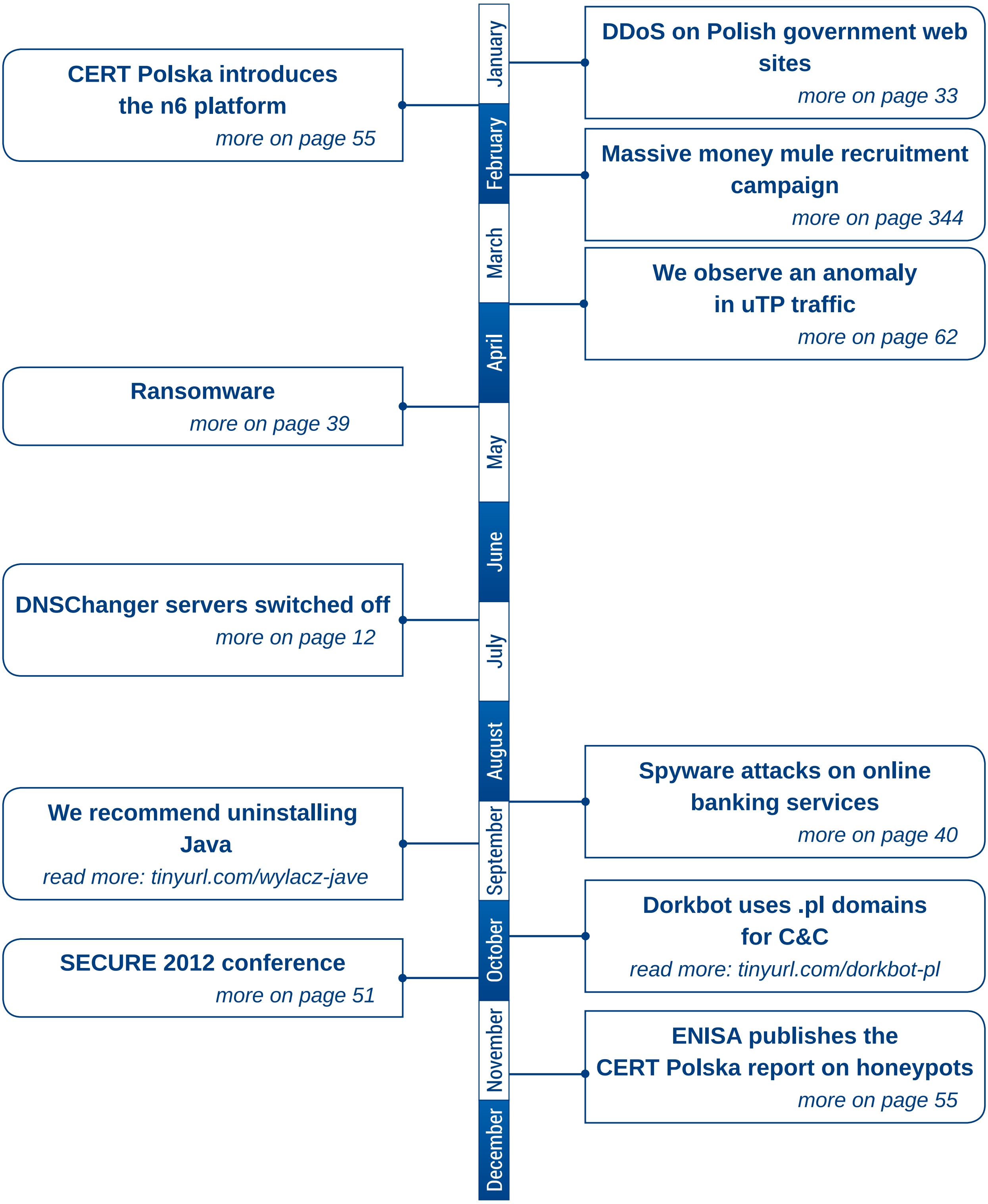
- Remote Desktop in MS Windows (3389/TCP) is a new entry among on the list of most scanned services, and is mostly attributed to dictionary attacks. Most of these attacks registered last year seemed to be connected with the Morto worm.

- There was a 56% reported increase in the number of DNS servers in Polish networks that are incorrectly configured as completely open, posing a serious threat to all Internet users, as they can be easily used to amplify DoS attacks. The main reason for this problem is the lack of awareness among administrators.

- The majority of incidents that were handled manually were reported by foreign commercial entities. Most of these incidents were related to spam and phishing.

1.2 Summary of the events

The diagram below shows a chronological arrangement of key events related to the activities of CERT Polska. These are discussed in the report.



DDoS on Polish government web sites
more on page 33

CERT Polska introduces the n6 platform
more on page 55

Massive money mule recruitment campaign
more on page 344

We observe an anomaly in uTP traffic
more on page 62

Ransomware
more on page 39

DNSChanger servers switched off
more on page 12

Spyware attacks on online banking services
more on page 40

We recommend uninstalling Java
read more: tinyurl.com/wylacz-jave

Dorkbot uses .pl domains for C&C
read more: tinyurl.com/dorkbot-pl

SECURE 2012 conference
more on page 51

ENISA publishes the CERT Polska report on honeypots
more on page 55

1.3 Information about CERT Polska

The CERT Polska team operates within the structures of NASK (Research and Academic Computer Network) – 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 recognized 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. CERT Polska also conducts extensive R&D into security topics. In 1997, CERT Polska became a member of the international forum of response teams – FIRST, and since 2000 it has been a member of the working group of the European response teams – TERENA TF-CSIRT, accredited by Trusted Introducer. In 2005 on the initiative of CERT Polska, a forum of Polish abuse teams was created - Abuse FORUM, while in 2010 CERT Polska joined the Anti-Phishing Working Group, 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
- 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 into methods of detecting security incidents, analysis of malware, systems for exchanging information on threats;
- development of proprietary and open source tools for detection, monitoring, analysis, and correlation of threat
- regular publication of an Annual CERT Polska Report on security of Polish on-line resources;
- information/education activities, aimed at raising awareness in relation to IT security, including:
  - □ maintaining a blog at **http://www.cert.pl** as well as Facebook and Twitter accounts;
  - □ Organization of annual SECURE conference;
- analysis and testing of IT security solutions.

2 Statistics of the submissions coordinated by CERT Polska

This part of the report describes the statistics concerning security incident reports received by CERT Polska, both from external sources as well as internal own systems in an automated fashion.

2.1 Amount of information in all categories

In 2012 we received 10,559,893 submissions from automated data feeds – almost exactly half as much as in 2011. One of the reasons for the lower number of submissions is changes in the number of sources as well as a shift in the type of data reported. A good example of this process is an significant decrease in Conficker botnet reports: not because Conficker is not present but because it is less actively monitored. Another reason is a change in ways we counted some of the reports, indirectly resulting from source changes. For the reasons mentioned above, comparison of the absolute numbers between subsequent years is not reliable neither for the total number of submissions nor for each category. The comparison of each category presented on Figure 1 can be used only to get a general a view on the amount of information handled, rather than on the real scale of the particular problem. It is worth noting that a lot depends on how effective the methods of detecting incidents used by entities that exchange data with us are, as well as on the current areas of focus of the security community.

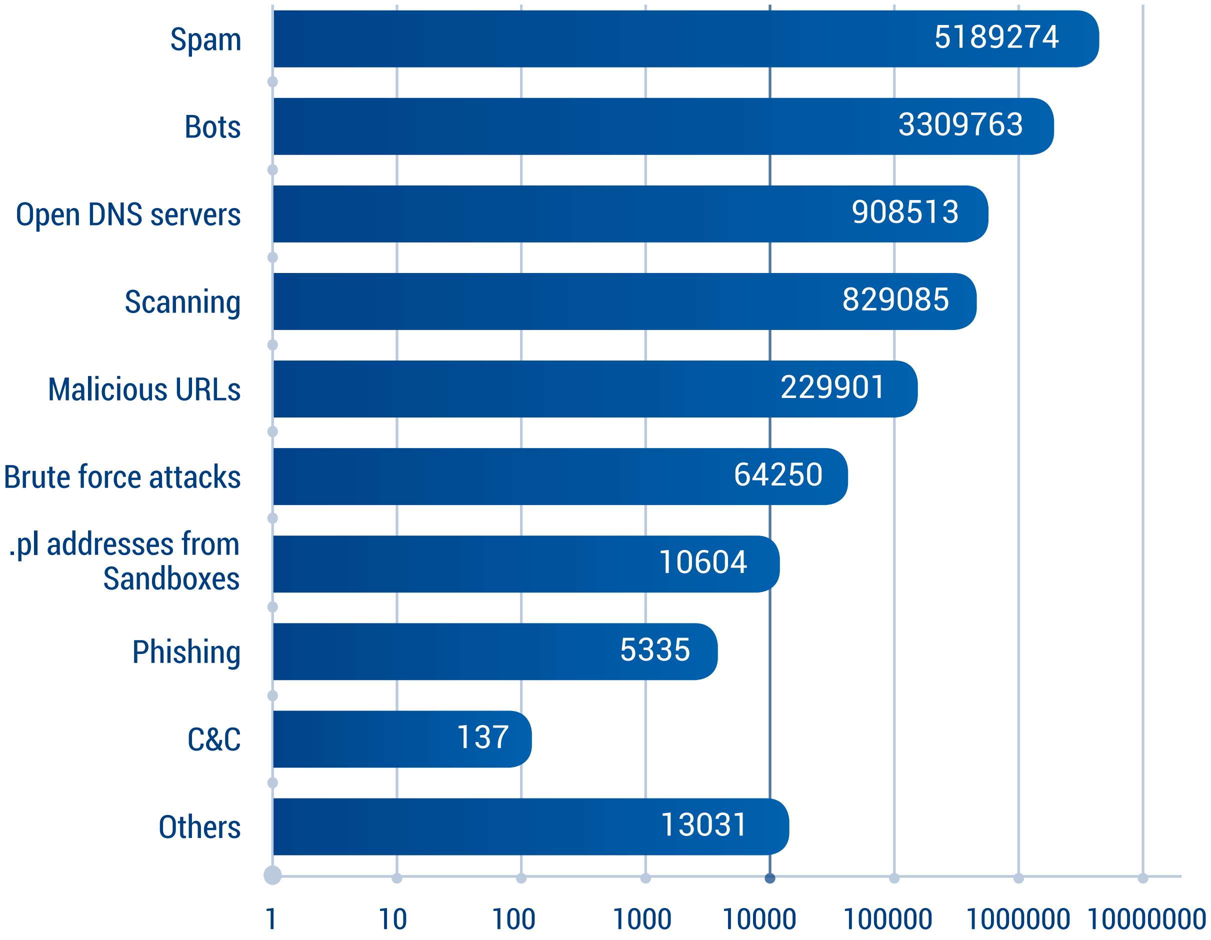


Figure 1. Number of automated reports in individual categories

2.2 Spam

The incidents described in these sections refer to machines in Polish networks that are used as sources of unsolicited messages. These are mostly computers infected with malware, thus bots used for mass mailing without the knowledge or consent of their legitimate owners.

In 2012 we received 5,189,274 submissions related to spam from Polish IP addresses, 10.9% more than in 2011. These are related to 1,648,009 IP addresses (an increase of 31.5% in comparison to 2011).

One of the reasons for the large increase in the number of IP addresses identified as sending spam is a growing trend that we indicated in previous years: more and more incidents relate to mobile networks that assign dynamic IP addresses for short lease periods. As a result, a user of the infected laptop who uses mobile Internet will be counted many times under different IP addresses, even within a single day. This year the scale of the problem appears alarming – as many as 36.7% of submissions relate to mobile networks. This is nearly 2,000,000 in absolute numbers! The problem is even more serious when we look at the pollution of particular networks measured as the share of IP addresses reported as sending spam to the total number of IPs assigned to the operator. In the case of P4 (the operator of the Play network) this is as much as 40.6%, which means that two out of every five IP addresses were used for sending spam. In the case of the other operators the statistics are a bit better, however 13.9-16% is still a significant percentage As a consequence, these networks may end up on various blacklists (RBLs).

Once again, the first place in the absolute number of submissions goes to Netia (nearly 972,000, 18.7%). Netia has also a very high percentage of addresses sending spam from its network (20.1%), however it should be noted that in the comparison to 2011 both the number of submissions and the number of unique IP addresses sending spam are significantly lower.

The largest cable networks: Multimedia Polska and Vectra also came off badly. They ranked top not only because of the number of submissions (8.2% and 5.3% respectively), which could be a result of the size of the network, but also because of the high percentage of IP addresses submitted as the spam sources (14.5% and 9.8% respectively) compared to all the IP addresses allocated to the network. The comparison does not take into account a major cable operator - UPC - because many sources send reports about abuse related to these addresses not to us but to the company headquarters, which is outside of Poland.

Once more the network of Telekomunikacja Polska (now under the Orange Polska brand) serves as a positive example in terms of being a spam source. The number of submissions related to this network fell by almost one third, to the level of 504,000 in comparison to 2011 which resulted in a lowering of the position of Telekomunikacja Polska in the top spam source ranking (from second to fourth). The submissions concerned about 43,000 unique IP which represent only 0.6% of the total network. Telekomunikacja Polska achieved this result thanks to the policy of blocking port 25 TCP which – as it turns out – works well. Unfortunately blocking port 25 TCP does not remove the source of the problem (infected machines) which is clearly visible in the high ranking of Telekomunikacja Polska in sections 4.5 and 4.2, yet is still beneficial for several reasons: firstly it reduces spam in the Internet, secondly it impacts the underlying business model of criminals. Again it’s worth asking when other providers in Poland are going to implement such a – seemingly simple - solution.

	Change	AS number	Operator's name	Number of submissions	Change	Share	Number of unique IP	Change	IP share
1	-	12741	Netia SA	971 682	▼ 480 536	18,7%	348 102	▼ 43 303	20,1%
2	▲ 2	43447	PTK Centertel Sp. z o.o.	829 094	469 016	16,0%	317 257	122 938	14,0%
3	▲ 4	39603	P4 Sp. z o.o.	507 940	325 340	9,8%	326 816	179 262	40,6%
4	▼ 2	5617	TP S.A.	503 714	▼ 293 561	9,7%	43 102	▼ 64 375	0,6%
5	▼ 2	21021	Multimedia Polska S.A.	425 417	▼ 43 515	8,2%	88 102	17 837	14,5%
6	▲ 3	12912	Polska Telefonia Cyfrowa S.A.	325 420	228 137	6,3%	21 6897	137 619	15,1%
7	▼ 2	29314	VECTRA	276 020	▼ 77 978	5,3%	43 213	23 549	9,9%
8	▼ 2	8374	Polkomtel S.A.	242 910	▼ 22 837	4,7%	21 1702	2 2751	16,0%
9	▼ 1	20960	TK Telekom	106 478	▼ 21 815	2,1%	4 287	▼ 1 171	1,6%
10	N	6714	ATOM SA	55 036	BD	1,1%	14 686	BD	3,4%

Table 1. Top 10 of most reported network (according to AS numbers).

The table below presents 13 largest Polish Autonomous Systems (over 250,000 addresses) by the percentage of IP addresses submitted as sending spam as compared to the total addresses assigned to the Autonomous System (without those belonging to UPC AS12476):

	AS number	Operator's name	Unique IP	Percentage
1	39603	P4 Sp. z o.o.	326 816	40,605%
2	12741	Netia SA	348 102	20,145%
3	8374	Polkomtel S.A.	211 702	16,002%
4	12912	Polska Telefonia Cyfrowa S.A.	216 897	15,130%
5	21021	Multimedia Polska S.A.	88 102	14,460%
6	43447	PTK Centertel Sp. z o.o.	317 257	13,954%
7	29314	VECTRA	43 213	9,854%
8	6 714	ATOM SA	14 686	3,424%
9	20960	TK Telekom	4 287	1,612%
10	5617	TP S.A.	43 102	0,623%
11	43939	Internetia Sp.z o.o.	1 382	0,336%
12	15857	Dialog S.A.	1 021	0,230%
13	8308	NASK Commercial	729	0,229%

Table 2. 13 largest Polish AS (over 250,000 addresses) by the percentage of IP addresses submitted as sending spam

2.3 Bots in Polish networks

This category includes computers in Polish networks that are part of botnets and are not included in other categories. The most popular use of botnets is to send spam, but 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.

Last year we received 3,309,763 submissions on 1,980,941 unique bots in the Polish networks. Virut was the most popular among them. Note that tt the beginning of 2012 NASK took over 43 .pl domains used to control Virut botnet.

In 2012 we observed 869,973 unique IP addresses that had machines infected with this malware. We registered 3,931 unique bots connected to this botnets per day on average.

DNSChanger – a malware changing the DNS servers used by infected machines (more: **http://www.cert.pl/news/4936**) – ranked as second. The DNSChanger servers (taken over earlier and thus used as a source of information on infected machines) were suspended by the FBI on the 9th of July 2012. Since then we have not received any submissions of Polish IP belonging to this botnet.

In the period from January to June, we registered 427,246 unique IP addresses of machines infected with DNSChanger. The third and fourth position in the ranking were held by two different types of banking Trojan ZeuS (246,564 unique IP addresses throughout the year) and ZeuS-P2P (39,630 unique IP addresses throughout the year). Citadel, belonged to the same type of malware, was at the ninth place (22,696 unique IP addresses throughout the year). Conficker that ranked top last year with over 2,000,000 bots, this year dropped to fifth place with only 37,349 bots. The list of the most popular botnets in Polish networks (as reported to us and monitored by us) is presented in the charts and tables below.

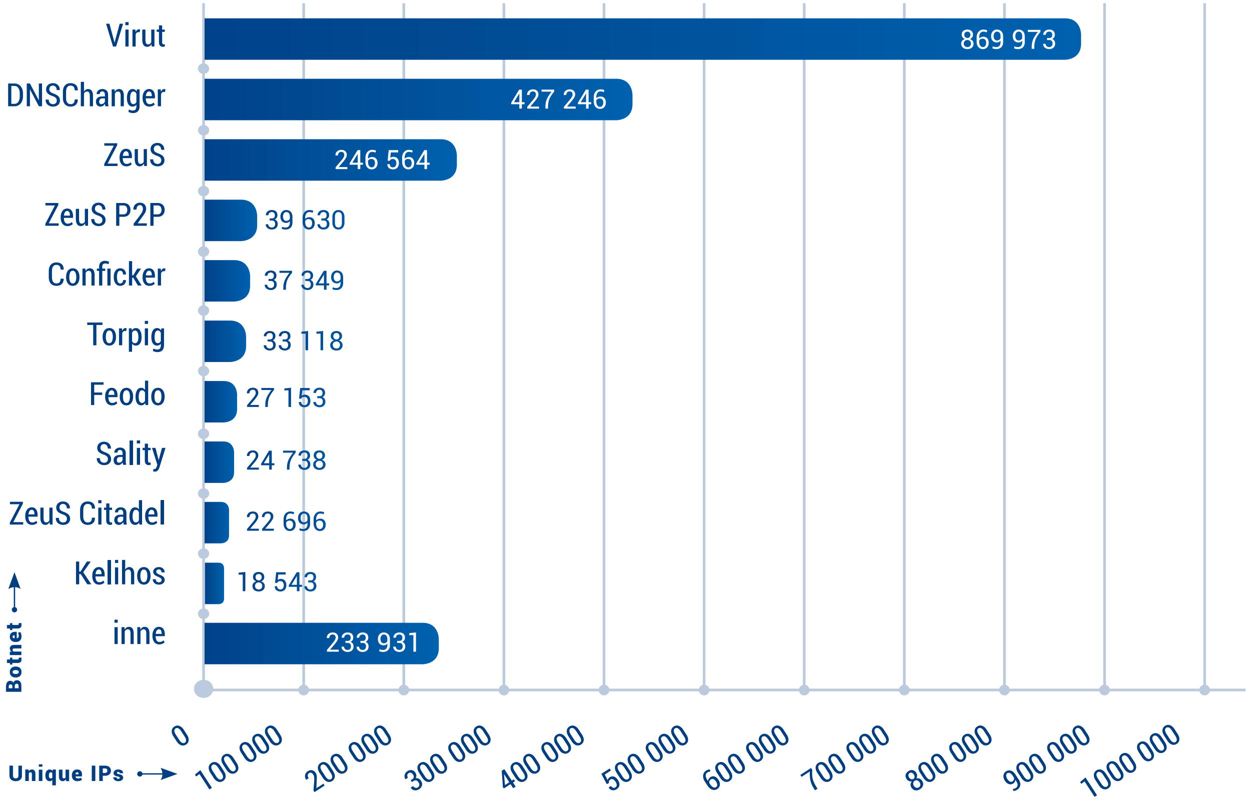


Figure 2. Most popular botnets in Polish networks

Most bots were detected in AS 5617 owned by Telekomunikacja Polska (TP). They totaled at 636,911 unique IPs throughout the year. This number is much lower than last year (nearly by 2,500,000) which is related to the lack of submissions on the Conficker worm. The second place was occupied by T-Mobile (AS12912) with a number of 417,377 unique IPs a year (last year this network ranked sixth). Netia is ranked third (decrease by one point) with 264,872 unique IPs. The absolute ranking presenting the networks with the largest number of infected unique IP addresses is presented below:

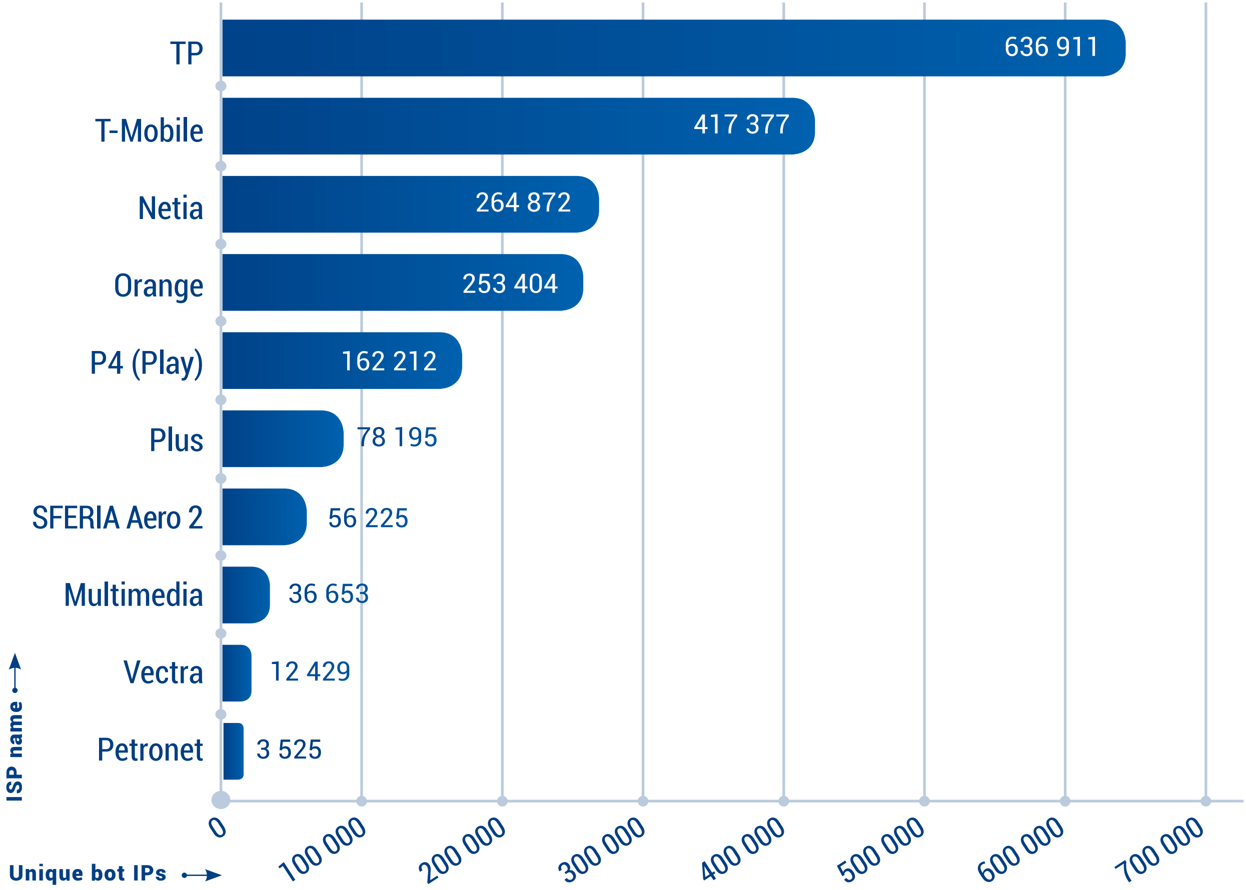


Figure 3. Absolute ranking presenting the networks with the largest number of infected unique IP addresses

In comparison to 2011 the number of unique IPs reported to us has dropped significantly. This is mainly due to the fact that the Conficker worm was not reported much anymore. Similarly to the previous year, mobile operators such as T-Mobile, Orange, Play and Plus rank at the top. Additionally, for the first time the list contains an operator of free Internet access service- Aero 2 (AS15855). There is no doubt that the largest numbers of bots operate in networks of operators providing Internet access to individual subscribers. These are the biggest providers such as TP, Netia and Multimedia. Dialog network (AS15857) and GTS (AS6714) have disappeared from the Top 10 statistics, while Petrotel (AS29007) has made its debut.

In the case of the absolute ranking presented above, the size of the autonomous systems has significant influence on the provider's position – the more IP addresses in the network, the larger number of unique bots. That is why we decided to prepare another table taking into account the size of the network. It introduces the percentage of IP addresses in a given AS which were reported as hosting bots, as compared to all the IP addresses assigned to an operator. The number of IP addresses belonging to a given autonomous system was estimated based on data in RIPE database. SFERIA Aero 2 (AS15855) topped this ranking. Pollution of their IP space was estimated at 83%. As small networks (5,000 IP addresses or less) made half of the top 10 of the list ranked by IP space pollution, we decided to take into account only the networks with more than 250,000 IP addresses. Note that as smaller networks may tend to use NAT more often, these statistics may be biased against them and favour larger networks. The relative ranking was presented in the table below.

Ranking	Percent of infected IP	Number of unique bots	AS number	Operator's name	Position in absolute ranking
1	29,1	417 377	12912	T-Mobile	2
2	20,2	162 212	39603	P4 (Play)	5
3	15,3	264 872	12741	Netia	3
4	11,1	253 404	43447	Orange	4
5	9,2	636 911	5617	TP	1
6	6,0	36 653	21021	Multimedia	8
7	5,9	78 195	8374	Plus	6
8	2,8	12 429	29314	Vectra	9
9	1,0	2 535	20960	TK Telekom	15
10	0,8	3 421	6714	GTS	11

Table 5. Ranking of operators according to percentage value of bots number in relation to the AS

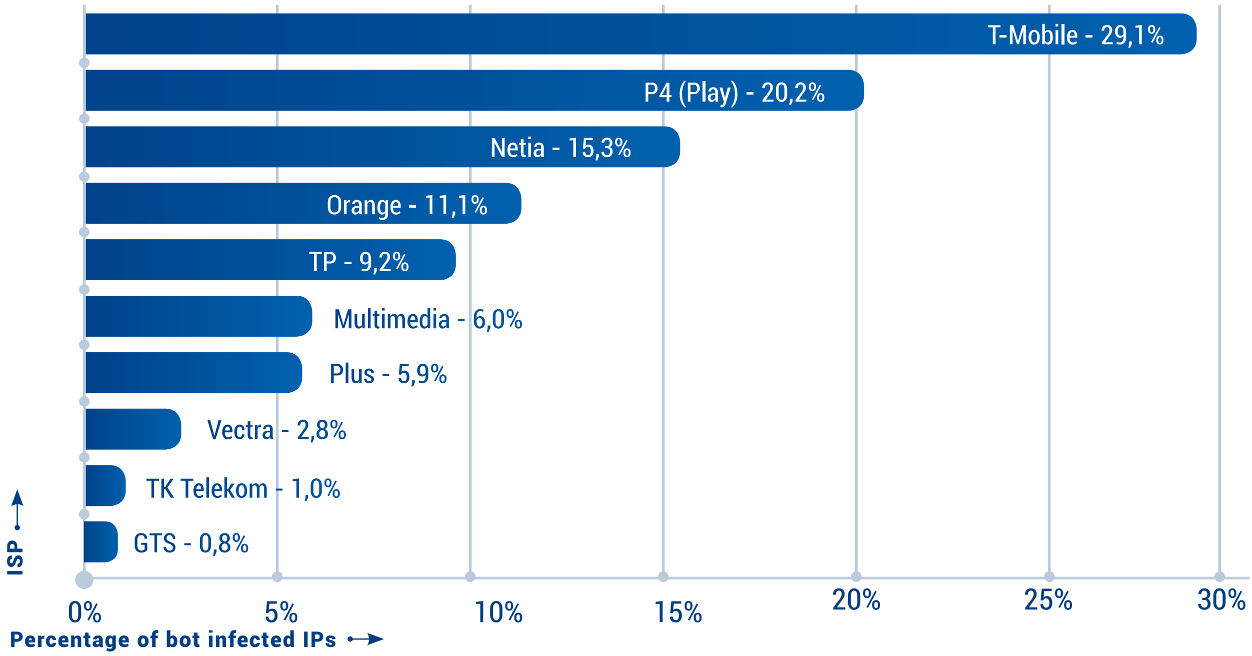


Figure 4. Ranking of operators according to percentage value of bots number in relation to the AS

In such a ranking the T-Mobile network is at the first place with 29% of all IP addresses reported as bots at least once. It is worth mentioning that mobile network operators ranked high in both lists. However, TP network is located at the first place in the absolute ranking, while it is in the middle of the list in the relative ranking.

2.4 Open DNS servers

In this category we have included DNS servers that, as a result of incorrect configuration or firewall policy, allow recursive queries from any location in the network. Such a setting allows them to be used in DDoS attacks by increasing the traffic volume (traffic amplification) resulting from DNS queries with spoofed source addresses.

The problem still exists and remains significant, because few administrators are aware of the fact that this configuration can lead to abuse. Internet providers could potentially play a bigger role in mitigation of this problem as they often receive all information about misconfigurated servers in their networks from us.

In 2012 we received 908,513 submissions on 220,666 unique IP addresses under which such servers were located. The number of open DNS servers is higher by 37% compared to last year. This indicates the growing scale of the problem in Poland. A distribution of ten Autonomous Systems, in which most open DNS servers were located, is presented in the Table 6. It is the absolute ranking and it does not take into account the size of the Autonomous System (the number of IP addresses belonging to AS).

Ranking	Change	Number of unique IP	% Share	AS number	Operator
1	0	82 148	37,2%	5617	TP/Orange
2	▲ 1	36 354	16,5%	43447	Orange
3	▼ 1	18 872	8,6%	12741	Netia
4	▲ 1	7 299	3,3%	6714	ATOM/GTS
5	▼ 1	7 006	3,2%	20960	TK Telekom
6	▲ 1	3 907	1,8%	21021	Multimedia
7	New	3 636	1,6%	13110	INEA
8	0	3 062	1,4%	29314	VECTRA
9	▲ 1	3 048	1,4%	13000	Leon
10	▼ 1	2 750	1,2%	29665	Speed-Soft

Table 6. Top 10 of Polish autonomous systems where open DNS servers were located the most often

When we take into account the size of the AS and we calculate the number of open DNS servers per each 10 IP addresses belonging to a given AS, we get a completely different list:

Ranking	Ratio	Number of unique IP	AS number	Operator	Position in absolute ranking
1	6.89	512	198098	ARTKOM	44
2	5.37	512	29665	Speed-Soft	10
3	4.10	512	47275	Torjon	77
4	3.81	512	47884	JPK	81
5	3.25	1 024	56783	ConnectIT	48
6	3.06	1 024	43607	STREFA	51
7	2.16	1 024	51648	GIGA-AS	69
8	2.00	768	197764	ADWA-NET	95
9	2.00	2 048	16110	Podkarpacki.net	42
10	1.94	2 560	50767	RADIONET-AS ELEKTRO-SYSTEM	30
54	**0.52**	**58 112**	**13000**	**Leon**	**9**
99	**0.26**	**265 984**	**20960**	**TK Telekom**	**5**
111	**0.21**	**168 704**	**13110**	**INEA**	**7**
127	**0.17**	**429 440**	**6714**	**ATOM/GTS**	**4**
130	**0.16**	**2 273 36**	**43447**	**Orange**	**2**
172	**0.12**	**6 916 160**	**5617**	**TP/Orange**	**1**
195	**0.11**	**1 728 000**	**12741**	**Netia**	**3**
291	**0.07**	**438 528**	**29314**	**VECTRA**	**8**
308	**0.06**	**609 280**	**21021**	**Multimedia**	**6**

Table 7. Ranking of 10 Polish autonomous systems where open DNS servers were located the most often (after taking into account the size of autonomous system).

Where: **ratio** is the number of open DNS server per each 10 IP addresses belonging to AS. The bolded AS numbers were included in both rankings. The data about the size of given Autonomous Systems was derived from the RIPE database (as of January 30, 2013).

2.5 Scanning

Scanning category covers reports of detected attempts of unauthorized connections. They may be caused by infected computers that initiated the connection (for example self-propagation of an Internet worm or actions of a botnet), otherwise compromised machines, or deliberate malicious activity of users. All submissions included in the statistics below were received automatically. The breakdown includes data sent by our partners, as well as from our monitoring systems.

In 2012 we received 829,085 cases of incidents concerning 360,871 IP addresses from Poland. The number of submissions is significantly different from that in the previous year when we had over 5,000,000 submissions. This is a result of changes in the way we handled submissions and counted them. If a given IP address was reported in a given day by many of our partners, as well as it was seen as attacking many times throughout that day (multiple destination addresses) or attacked different services (destination ports) it was still treated as a single report, while any submission on the following day that concerned the same IP addresses would be classified as a new report.

Furthermore, the number of submissions may be affected by changes of partners reporting data to us.

2.5.1 Most scanned services

The statistics below present Top 10 target ports by unique source IP addresses, where Polish IP addresses were the source. Note the logarithmic scale! The total number of reported unique IP addresses has increased in comparison to the last year.

Ranking	Number of unique IP address	Destination port	Change versus 2011	Description
1	315 672	445/TCP	0	Buffer overflow attacks on Windows RPC services
2	7 621	3389/TCP	▲ 8	Dictionary attacks on RDP (remote desktop)
3	7 300	23/TCP	▲ 3	Attacks on telnet service
4	4 529	210/TCP	new	Applications using Z39.50 protocol
5	3 939	80/TCP	0	Attacks on web applications
6	2 817	135/TCP	▼ 4	Attacks on windows DCE/RPC service
7	2 282	5900/TCP	▲ 2	Attacks on VNC
8	2 145	139/TCP	▼ 5	Attacks on NetBIOS service/ sharing files and printers
9	1 163	22/TCP	▼ 2	Dictionary attacks on SSH servers
10	1 043	1433/TCP	▼ 6	Attacks on MS SQL
	12 360			other

Table 8. Top 10 of destination ports by number of unique scanning IPs

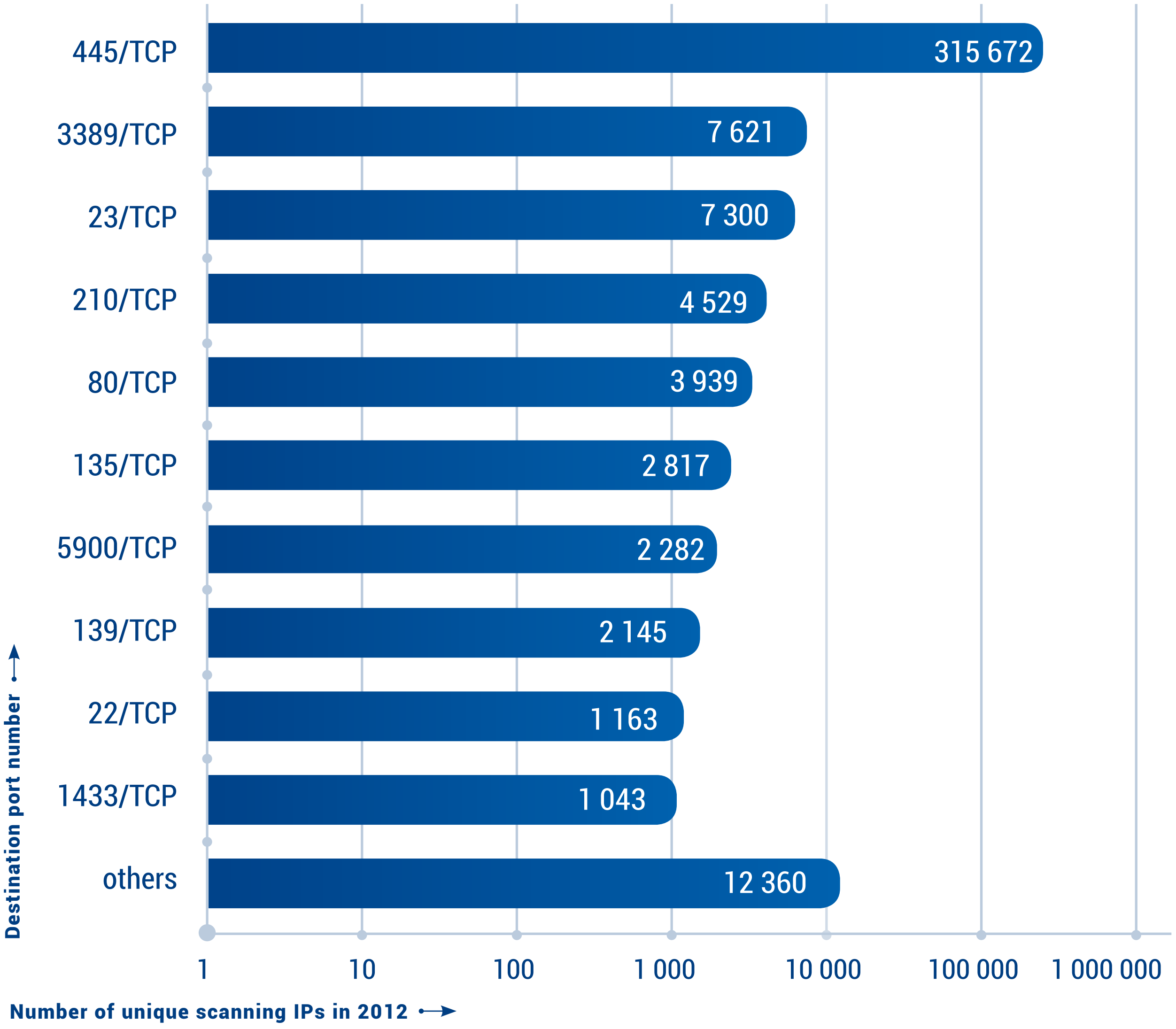


Figure 5. Top 10 of most scanned destination ports according to unique source IP addresses originating in Poland

Ranking first, as in the previous years, is port 445/ TCP. Most serious and therefore most often exploited Windows vulnerabilities are located in services listening on this port. Many worms use this port to propagate. Hence, it is much more popular than other ports. The number of unique IP addresses scanning this port was over 315,000 which represents 70% of the total number of IP addresses in this category. Port 3389/TCP comes second which only 17% of all unique IPs connected to.

Other ports related to default Windows services, namely 135/TCP (service DCE/RPC), 139/TCP (NetBIOS, files and printer sharing) and 1433/TCP (MS SQL server) fell respectively to the sixth, eighth and ninth place (in 2011 these ports were respectively at the second, third and fourth place). This does not mean, however, these services are less attacked. The number of unique IP addresses connecting to them has not changed significantly in comparison to 2011. Simply, the attacks on all other ports in the ranking increased in numbers.

The second position in the Top 10 ranking is occupied by port 3389/TCP with 7,500 unique IP addresses. In 2011 it was ranked tenth place with a relatively small number of under 400 unique IP addresses.

The increase in attacks on this port is significant. The port is related to the Windows service Microsoft Terminal Server using RDP protocol (used by 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. Interestingly, Morto does not exploit any vulnerability, but guesses users' passwords. At the same time - apart from Morto worm activity – we observed non-worm attempts to crack passwords in Remote Desktop service.

There is a new port in the Top 10 ranking – 210/TCP, on which the service operating Z39.50 protocol listens by default (a client–server protocol for searching and retrieving information from remote computer databases).

2.5.2 Polish networks

Most of unique IP addresses in Polish networks submitted to our team throughout the year - slightly over 180,000 - came from the network of Telekom Polska (now Orange Polska) (AS5617), similarly to the previous year. Slightly less came from Netia network that ranked second with over 116,000. Last year TP and Netia also occupied the first two positions in the ranking but the difference between them was much bigger. Plus (AS8374) with 33,000 unique IP addresses is at the third place. You can see that there is a noticeable difference between the top two and the rest of networks in the ranking.

The absolute ranking of Top 10 networks with the largest number of unique IP addresses submitted to our team is presented below. After a year's break, UPC (AS6830) and Petrotel (AS29007) networks (the latter) belonging to Netia Group appeared in the Top 10 ranking. Dialog network (AS 15857), joined Netia Group last year, and T-Mobile (AS12912) dropped out of the top ranking. The number of unique IP addresses increased in all networks specified in the ranking.

Ranking	Number of unique scanning IPs throughout the year	Average number of unique scanning IPs per day	AS number	Operator's name	Change versus 2011
1	118 108	612	5617	TP	0
2	116 565	532	12741	Netia	0
3	33 457	101	8374	Plus	▲ 2
4	30 876	101	43447	Orange	0
5	19 258	120	21021	Multimedia	▲ 1
6	9 144	134	29314	VECTRA	▲ 2
7	5 014	86	25388	ASK-NET	0
8	3 003	82	6830	UPC	new
9	2 697	16	29007	Petrotel	▲ 2
10	2 349	34	6714	GTS	▼ 1
	20 400		others		

Table 9. Top 10 of networks with the largest number of unique IP addresses submitted to CERT Polska

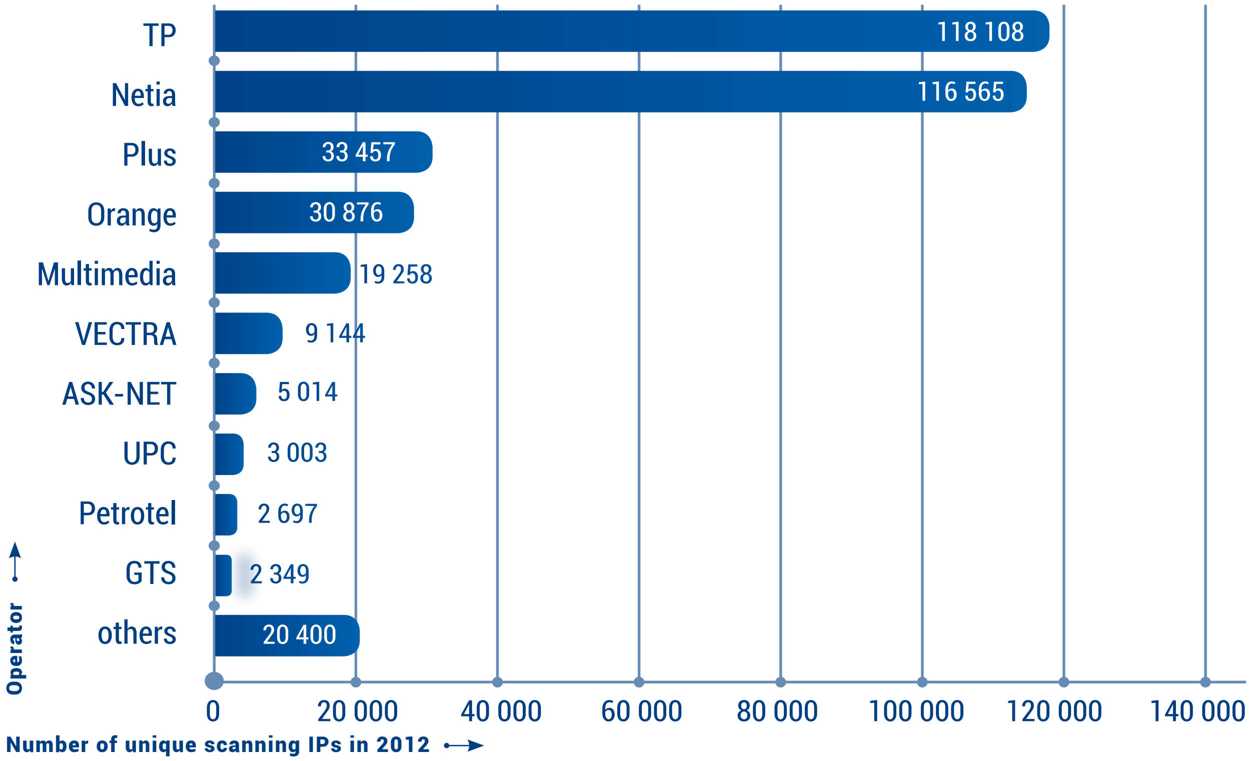


Figure 6. Top 10 of networks with the largest number of unique IP addresses submitted to CERT Polska

In the case of the absolute ranking presented above, the size of the Autonomous Systems has significant influence on the provider's position – the more IP addresses in the network the larger number of unique scanning IP addresses. This is why we decided to prepare one more statistic taking into account the size of the network. We added the new factor defining the percentage share of scanning IP addresses in relation to all IP addresses belonging to a given AS. In this ranking there were as many as 5 networks having less than 5,000 IP addresses, and only one network having more than 250,000 IP addresses. The first position was held by the Netia network (11.23% of infected IPs), and TP, top in the absolute ranking, was at fifth (3.23% of infected IPs). The absolute ranking is shown below.

Ranking	Percentage of infected IPs	ASN	Operator's name	Place in the absolute ranking
1	11,23	12741	Netia	2
2	11,18	29314	VECTRA	6
3	7,18	21021	Multimedia	5
4	4,87	20960	TK Telekom	14
5	3,23	5617	TP	1
6	2,86	6714	GTS	10
7	2,78	8374	Plus	3
8	1,62	43447	Orange	4
9	1,57	6830	UPC	8
10	0,81	43939	Internetia	19

Table 10. Ranking of operators by the share of unique scanning IP addresses in relation to all IP addresses belonging to a given AS

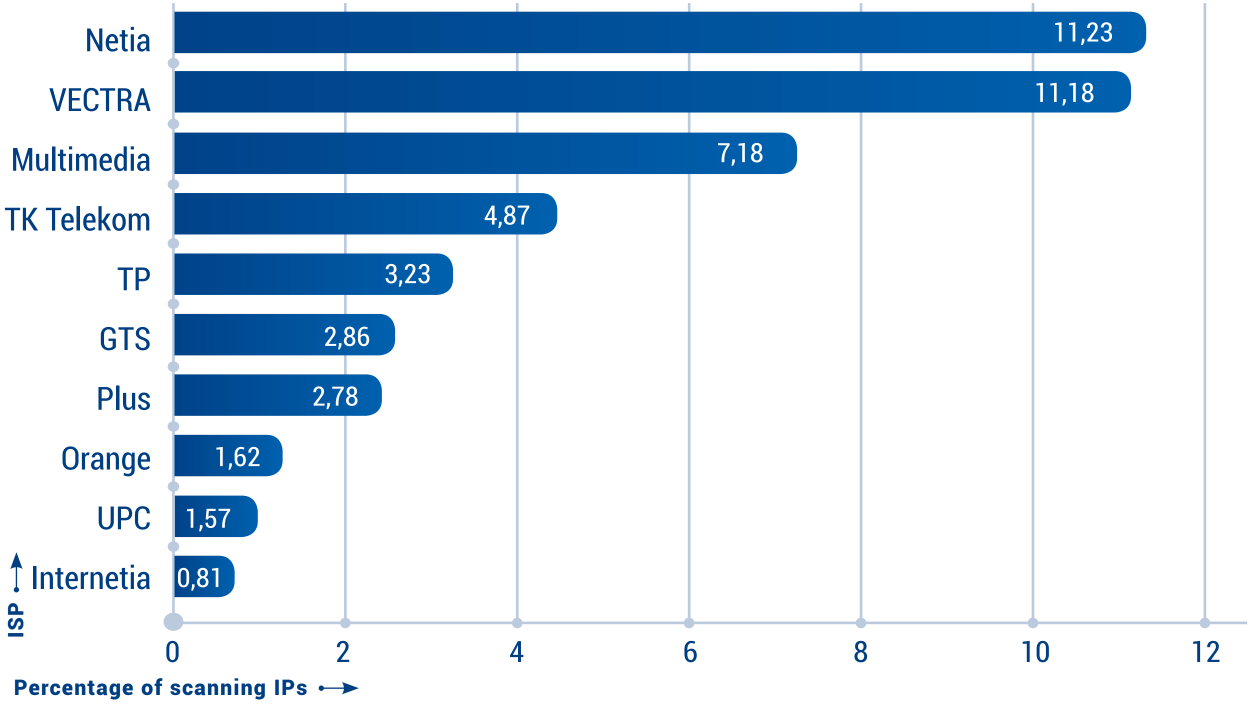


Figure 7. Ranking of operators by the share of unique scanning IP addresses in relation to all IP addresses in a given AS

Below we present the statistics concerning the most scanned destination ports in specific networks. We took into account only networks from the Top 10 absolute ranking.

	TP		Netia		Plus		Orange		Multimedia	
1	445/TCP	67,9%	445/TCP	83,7%	445/TCP	96,5%	445/TCP	95,4%	445/TCP	81,6%
2	3389/TCP	3,5%	139/TCP	1,1%	161/UDP	0,6%	5900/TCP	0,5%	135/TCP	2,5%
3	23/TCP	2,4%	23/TCP	1,1%	143/TCP	0,3%	23/TCP	0,3%	23/TCP	1,0%
	other	26,2%	other	14,1%	other	2,7%	other	3,8%	other	14,9%

	Vectra		ASK-NET		UPC		Petrotel		GTS	
1	445/TCP	71,6%	445/TCP	90,6%	445/TCP	16,8%	445/TCP	95,2%	445/TCP	54,1%
2	3389/TCP	1,6%	139/TCP	0,7%	23/TCP	8,6%	3389/TCP	0,5%	23/TCP	2,3%
3	23/TCP	1,1%	135/TCP	0,5%	139/TCP	3,5%	23/TCP	0,5%	210/TCP	1,6%
	other	25,8%	other	8,2%	other	71,1%	other	3,8%	other	42,0%

Table 11. Ranking of destination ports in particular networks scanned the most often (only networks from the Top 10 absolute ranking).

2.6 Sites associated with malware

In 2012 we registered 229,901 URLs in the .pl domain that contained malware. These mainly included malicious software, malicious Java Scripts or iframes pulling content from other servers.

2.6.1 .pl domains with most malicious URLs

Most malicious URLs we received reports for were in the katalog.onet.pl domain. In this case the situation is complicated and requires explanation. Katalog.onet.pl is a search engine of web sites usually located outside Onet networks. The results displayed by Onet do not contain malicious content themselves, but the searched sites do. This is why they appeared in the ranking. It should be noted that the directory in itself is safe but visiting searched sites may result in an infection of the computer.

Other names, apart from **www.vodca.pl**, were probably used to host advertising sites. We consider two scenarios: either the sites contained malicious content themselves or they contained URLs to malicious sites.

In the case of **www.vodca.pl** it seems that the site was compromised, resulting in injection of malicious code.

Item	Domain	Number of unique malicious URLs
1	katalog.onet.pl	7 426
2	www.przepisane.ilawa.pl	2 531
3	cudownystyl.pl	1 993
4	www.numery.pwy.pl	1 921
5	outlet1st.za.pl	1 839
6	www.helweg.waw.pl	1 701
7	www.vodca.pl	1 498
8	super-zdrowo.pl	1 440
9	adamantczak.friko.pl	1 326
10	valenciaswigert.w8w.pl	1 193

Table 14. Number of malicious URLs on one address

2.6.2 Autonomous systems with most malicious URLs

Not surprisingly, the top Autonomous Systems (AS) with malicious URLs belong to large providers of hosting services. It is interesting that the first two positions are occupied by autonomous systems located outside Poland, respectively OVH in France and Hetzner in Germany. This is the effect of great popularity of these hosting facilities. There was also another foreign entity, the Dutch Leaseweb in the top ten. The rest of the list contains the largest Polish hosting providers, such as Interia, Home, NetArt and Onet.

Item	AS number	AS owner	Number of unique malicious URLs
1	217.74.66.183	INTERIAPL	24 702
2	213.180.146.24	ONET-PL-AS1	7 426
3	194.9.24.158	CRMEDIA-AS	6 234
4	178.19.104.228	LIVENET-PL	4 941
5	213.180.150.17	ONET-PL-AS1	3 725
6	94.23.93.10	OVH	3 545
7	94.23.93.156	OVH	2 536
8	66.96.221.165	NOC	2 387
9	94.23.95.68	OVH	2 206
10	188.40.38.212	HETZNER-AS	2 026

Table 14. Number of malicious URLs on one address

2.6.3 Geographical distribution of malicious URLs in .pl domain

Most malicious sites in .pl domain were located on Polish severs that belonged to large hosting providers. Sites in Germany were located mainly on the servers at Hetzner, while those in France were at OVH.

Item	AS number	AS owner	Number of unique malicious URLs
1	16276	OVH	38 216
2	24940	HETZNER-AS	29 624
3	16138	INTERIAPL	27 583
4	12824	HOMEPL-AS	19 957
5	15967	NETART	12 391
6	12990	ONET-PL-AS1	11 181
7	59491	LIVENET-PL	10 401
8	16265	LEASEWEB	6 944
9	41406	CRMEDIA-AS	6 635
10	196763	KEY-SYSTEMS-AS	5 796

Table 15. Number of unique malicious URLs in AS

2.6.4 Geographical distribution of malicious URLs in .pl domain

Most malicious sites in .pl domain were located on Polish severs that belonged to large hosting providers. Sites in Germany were located mainly on the servers at Hetzner, while those in France were at OVH.

Ranking	Country	Number of unique malicious URLs
1	PL	137 681
2	DE	40 078
3	FR	38 216
4	NL	6 982
5	US	5 010
6	CZ	1 055
7	GB	336
8	EU	134
9	RU	120
10	CA	80
11	AT	79
12	CH	51
13	ES	27
14	IT	16
15	SE	8
16	LT	8
17	IE	7
18	DK	6
19	HU	2
20	FI	2
21	VN	1
22	RO	1
23	BG	1

Table 16. Geographical distribtion of malicious URLs hosted in .pl domain

2.7 Brute-force attacks

"Brute-force" attacks 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.

In 2012 we received 64,250 submissions relating to blind attempts of logging in to services. This is less than half of what was reported to us in 2011. All submissions were related to logging attempts to SSH service (default port: 22/TCP). Their number, however, does not reflect the scale of the problem. All attempts were made from only 112 unique IP addresses (a number similar to that in 2011). Note that in the scanning statistics (section 4.5) port 22/TCP is ranked quite high, so the popularity of attacks on SSH service is not as low as it may seem from the submissions reported as brute-force attacks. Perhaps this is the result of the fact that few attempts of brute-forcing SSH are identified as such, instead more often reported as scanning. Perhaps this is due to the tools used to monitor the traffic and detect attacks – only in the case of using high-interactive or specialized honeypots, or the observation of SSH production server traffic, we can be sure of identifying a bruce-force attack. In other cases (such as using of low-interactive, unspecialized honeypots or relying only on information about connections dropped by firewall) brute-force attacks can be categorized as scanning.

We received the most submissions (over 2,000) in February. They were related to only 16 addresses. This means that a relatively large number of attacks were made from a low number of addresses. Most unique IP addresses (both per day as well as throughout the month) were reported in April, while in July we got the least submissions and unique IPs).

2.8 Addresses visited by malware

Running the executable files in a controlled environment (sandbox) and monitoring its behavior is one of the main methods of automated analysis of untrusted software. Thanks to this technique it is possible to receive a wide range of information on tested programs, especially to check whether they connect to remote servers without user's interaction which may be a result of malicious activity. This category includes all cases when an untrusted program connects to a server located in Poland.

In previous years, we received information on this kind of connections only from the external sources. However, at the beginning of 2012 we introduced our own system for the automated software analysis that allows us to select tested files. All statistics presented below relate to combining data obtained from the external and internal systems.

The table 16 contains the comparison of 10 domains which the largest number of analyzed programs connected to. According to our analysis most of addresses, particularly in benjaminstrahs.com, filesfrog.com, etype.com, domains, were used to download adware software (displaying unwanted advertisements) or spyware software (sending user's data without his/her knowledge). There are also botnet controllers (command & control servers), such as pelcpawel.fm. interia.pl, or gim8.pl and IP addresses to which bots connect directly by using IP addresses, among others 79.96.81.234, 192.166.218.217 i 192.166.218.218. Some of these addresses, in particular `pelcpawel.fm.interia.pl`, have been inactive for several years, yet malware connecting to them is still in the wild.

Malware authors often make use of sites offering free subdomains to register addresses which afterwards are used to communicate with botnet controller, to download files containing Trojans, etc. After checking how fully qualified domain names unfolded to second-level domains it turned out that the site osa.pl was used for such registrations most often. We observed as many as 640 unique malicious subdomains in osa. pl. Next positions in the ranking of the number of subdomains was held by home.pl with 36 and interia.pl with 19 names.

Domain	number of files
download.benjaminstrahs.com	4 293
pelcpawel.fm.interia.pl	1 732
www.bee.pl	768
gim8.pl	552
79.96.81.234	516
download.filesfrog.com	478
software.filesfrog.com	443
192.166.218.218	429
version.etype.com	400
192.166.218.217	378

Table 17. Domains that are visited by malware the most often

2.9 Phishing

Phishing in Poland

In 2011, we received 5,335 submissions on phishing in Polish networks. These submissions were related to 2,576 different URLs in 1,026 domains, including 673 with the .pl TLD.

As opposed to the last year, there was no problem with mass scale abuse of free subdomains with the .pl TLD. In general, all incidents related to phishing on addresses with .pl ending turned out to be the result of break-ins.

A third of 353 domains had names ending with .org, .net, .eu and .biz, registered probably by a single group. For phishing they always used subdomains consisting of six numbers that may be the specific campaign ID. An example address: `953959.master-formular-bestaetigungen.biz`. Concluding from the names, these sites were used to collect data of PayPal users and owners of Mastercard from Germany. The sites were hosted in networks of various providers. Sometimes they also changed their locations.

The table below shows the distribution of reports of phishing in Polish networks split by the Autonomous System Number. High positions of the two largest hosting providers should not come as a surprise because phishing is usually located on either services purchased specifically for this purpose or – much often – as a result of a compromise at ordinary websites owned by small companies or institutions that also use hosting services.

ASN	Name	Number of phishing submissions	IP	URLs	Submission number/IP	Number of submissions/IP
1	12824	Home.pl	1153	176	621	6,55
2	15967	NetArt	779	140	426	5,56
3	41079	Superhost	339	19	172	17,84
4	5617	TP S.A.	294	52	150	5,65
5	21021	Multimedia	272	19	134	14,32
6	15694	ATM S.A.	234	12	141	19,50
7	12741	Netia S.A.	167	25	100	6,68
8	49792	IONIC	140	7	72	20,00
9	29522	KEI	137	15	78	9,13
10	43333	CIS NEPHAX	97	16	52	6,06

Table 18. Number of traditional phishing cases by Autonomous System

The last column indicates the ratio of the number of submissions to the unique IP addresses. It allows for estimation of how long phishing sites were hosted in a given autonomous system – the fewer submissions of one address the faster the sites were removed.

Poland and the world

We analyzed 342,091 reports because we wanted to look at traditional phishing globally and compared individual countries objectively. Therefore, we did not take into account sources providing information about Poland exclusively. In table 18 we presented the distribution of number of submissions split by countries where the sites were located (the criterion is geolocation of IP address, not domain address). The distribution has not changed substantially in comparison to 2011. The dominating country is traditionally US which we explain with the availability of cheap hosting services. The only surprise is the high position of Australia, with a large absolute number of submissions in relation to small number of IP addresses or URLs, which suggests the problems with removing these sites quickly. The structure of Australian phishing sites shows that in some cases there was a compromise at individual websites where many phishing pages were injected by using known phishing kits.

Poland takes a relatively low, 15th position, with the share of 0.8% in the total number of submissions. (The number of 2,675 is a result of omission of some sources that we have explained above).

Item	Country	Number of submissions	Percentage share in submissions	Number of unique URLs	Number of unique IPs
1	US	164 850	49,0%	136 850	22 637
2	AU	15 482	4,6%	7 327	544
3	DE	15 073	4,5%	12 616	3 099
4	GB	13 646	4,1%	11 792	1 776
5	CN	13 081	3,9%	1 004	1 452
6	CA	12 001	3,6%	10 654	1 132
7	FR	10 941	3,2%	9 298	1 462
8	BR	10 075	3,0%	9 062	2 031
9	RU	6 794	2,0%	5 667	1 102
10	CZ	6 126	1,8%	4 259	260
15	**PL**	**2 675**	**0,8%**	**2 140**	**654**

Table19. Number of submissions concerning traditional phishing by countries

2.10 Command & control servers

In 2012 we registered 137 cases of locating C&C server under IP addresses in Polish networks. This is twice as many as last year, mostly because of inclusion of new sources of information. For the same reason we decided not to count all reports (in 2012 there were 2,263 submissions in this category) – some sources do not stop reporting even if the controller is not active anymore, so taking them into account would have resulted in a false picture.

Table 20 shows the distribution of number of detected C&C servers by autonomous systems:

LNumber of C&C servers	AS	Operator
21	5 617	TPNET Telekomunikacja Polska S.A.
13	21 021	MULTIMEDIA-AS Multimedia Polska S.A.
11	6 830	LGI-UPC Liberty Global Operations B.V.
7	12 741	INTERNETIA-AS Netia SA
7	12 824	HOMEPL-AS home.pl Sp. z o.o.
6	29 314	VECTRANET-AS VECTRA S.A.
72	other	other

Table 20. Autonomous systems of Polish operators where C&C servers were located the most often

In comparison to the last year, there are none of the large hosting providers that dominated in 2011. In Polish networks belonging to OVH and LEASEWEB there was only one IP address of a botnet controller. The reason for that may be prosaic – changes in network descriptions and administrative assignment to countries.

Apart from C&C servers maintained in IP networks of Polish operators we also registered many cases of using Polish domains (most often the servers were located in other countries). We examine this in more detail in section 4.7.

2.11 Other submissions

The remaining 13,031 submissions were related to various types of automatically detected threats, mainly incorrectly configured devices such as proxy servers or routers, and a few DDoS attacks carried out through monitored C&C servers. There were not enough incidents to compare and analyze them. Larger number of DDoS attacks were reported to us individually and are presented in the statistics in section 3. The section 4.1 is devoted to DDoS attacks in Poland by Anonymous that took place in January.

We have not observed any clear trends in the case of the rest of submissions. The scale and importance of them does not give a reason for describing them in detail.

3 Statistics of incidents handled by CERT Polska

Trends in manually handled Incidents

In 2012 CERT Polska handled manually 1,082 incidents. Like in the previous years, most of them related to phishing (about 50%), malware (about 20%) and spam (nearly 10%). Mostly, Submitter, Victims and Attackers were IPs belonging to Commercial companies (respectively 53.8%, 59.6%, 75.7%). Submitters and Victims usually came from abroad (78.8% and 54.4%), while Attackers were unknown (ie. it was not determined where attacks came from) in 78.7% of the cases.

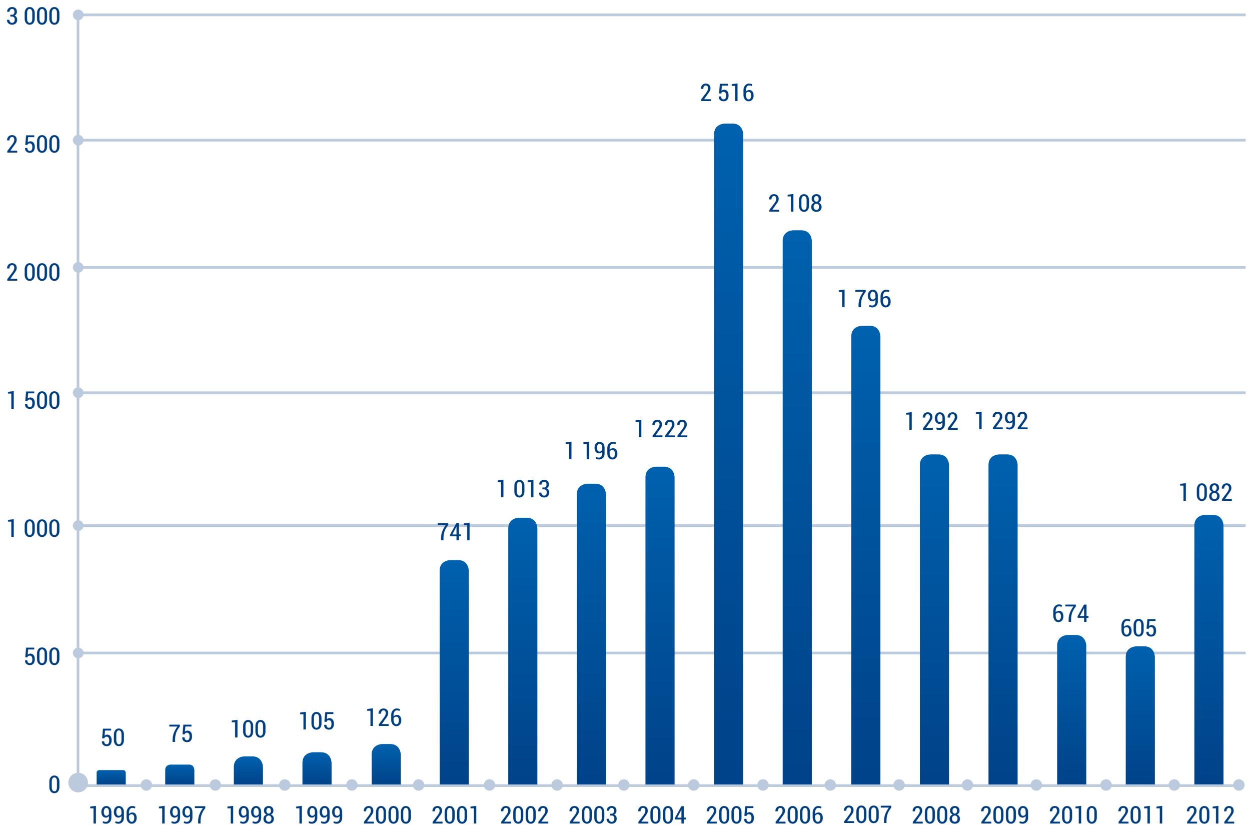


Figure 8. Number of incidents in years 1996-2012

			%	%
Abusive content	**5**	**114**	**0,50**	**10,54**
Spam	107		9,89	
Harassment	0		0,00	
Child/Sexual/Violence	2		0,18	
Malicious code	**216**	**226**	**19,96**	**20,89**
Virus	0		0,00	
Worm	0		0,00	
Trojan	10		0,92	
Spyware	0		0,00	
Dialer	0		0,00	
Information gathering	**4**	**41**	**0,37**	**3,79**
Scanning	37		3,42	
Sniffing	0		0,00	
Social Engineering	0		0,00	
Intrusion Attempts	**9**	**44**	**0,83**	**4,07**
Exploiting of known vulnerabilities	11		1,02	
Login attempts	24		2,22	
Exploiting of unknown vulnerabilities	0		0,00	
Intrusions	**4**	**14**	**0,37**	**1,29**
Privileged Account Compromise	9		0,83	
Unprivileged Account Compromise	1		0,09	
Application Compromise	0		0,00	
Availability	**0**	**25**	**0,00**	**2,31**
Denial-of-service attack (DoS)	8		0,74	
Distributed denial-of-service attack (DDoS)	17		1,57	
Sabotage	0		0,00	
Information Security	**35**	**44**	**3,23**	**4,07**
Unauthorized Access to Information	9		0,83	
Unauthorized Modification of Information	0		0,00	
Fraud	**13**	**559**	**1,20**	**51,66**
Unauthorized Use of Resources	0		0,00	
Copyright	5		0,46	
Masquerade	541		50,00	
Other	**15**	**15**	**1,39**	**1,39**

Table 21. Incidents handled by CERT Polska by type

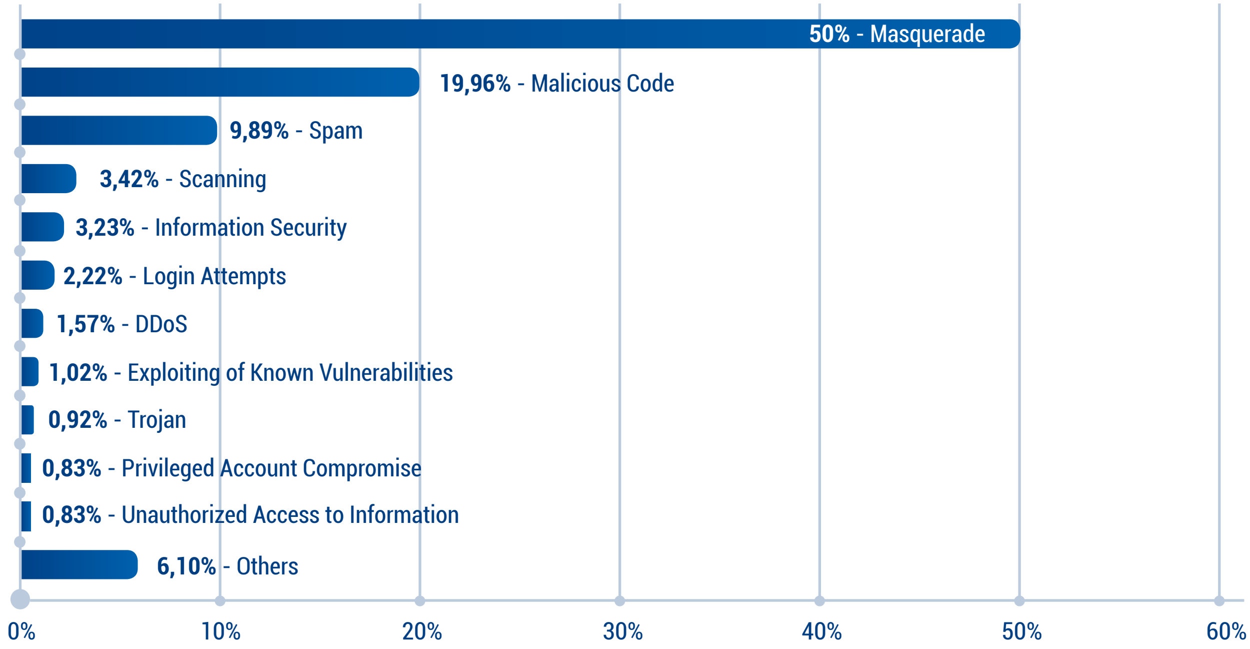


Figure 9. Percentage distribution of subtypes of incidents

The statistics of percentage share of the incidents haven't changed much for several years so we decided to compare the absolute values for the last four years. Here are the most interesting conclusions:

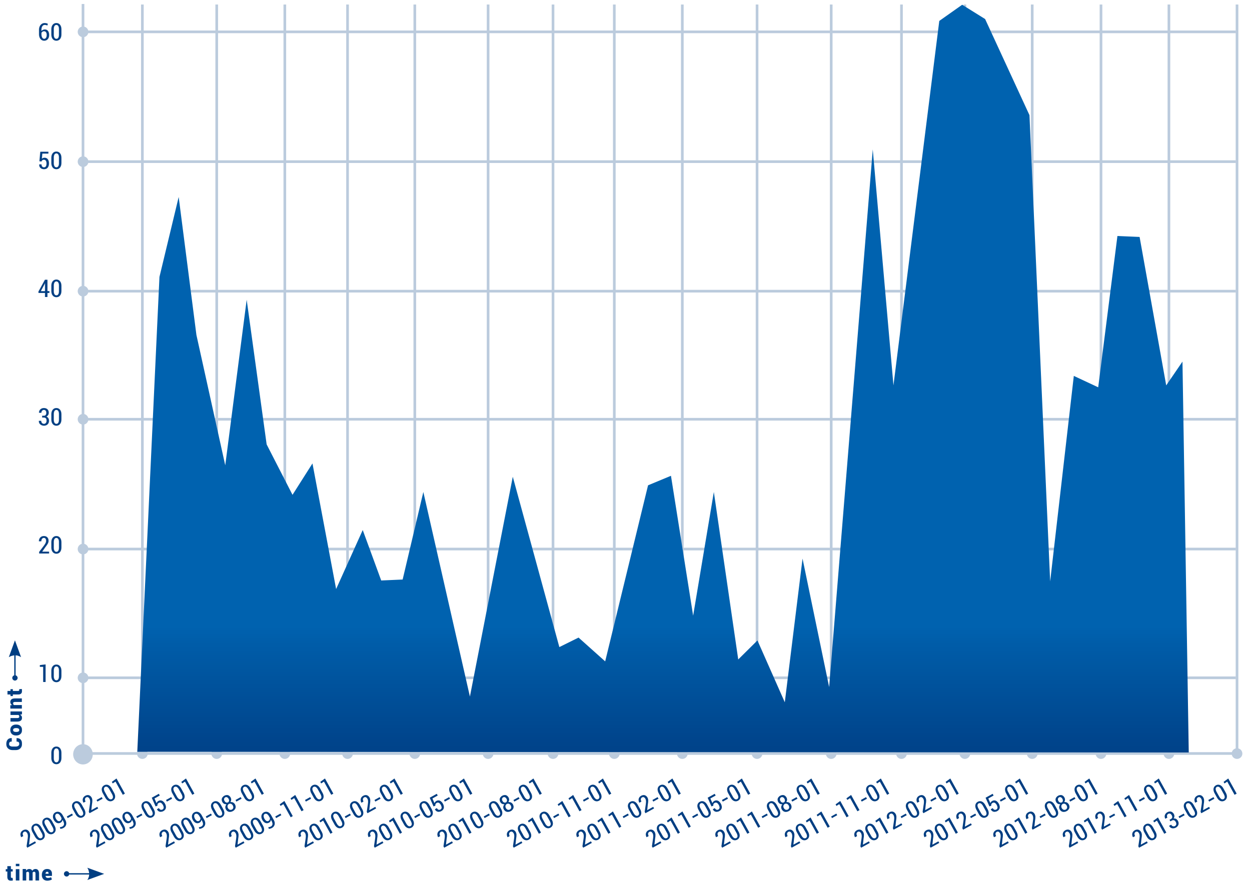


Figure 10. Number of incidents relating to phishing for the last four years

- at the end of 2011 the number of phishing incidents increased significantly. From 2010 to August 2011 we registered less than 30 incidents a month, afterwards the number had increased to more than 60 incidents.

- in 2012 the number of incidents related to malware increased significantly. The growing trend is observed throughout the year. The incidents related to malware had influenced significantly the number of handled incidents in 2012.

- since the middle of 2012 the number of commercial companies that became the victims has grown. In 2010 there were about 200 of them, while in 2012 nearly 500. This is mainly the result of phishing incidents with sites located on Polish servers.

- the number of foreign submissions concerning spam decreased from 300 incidents in 2009 to less than 100 in 2012.

- the number of submissions from private individuals from Poland dropped, especially in case of those related to spam and phishing.

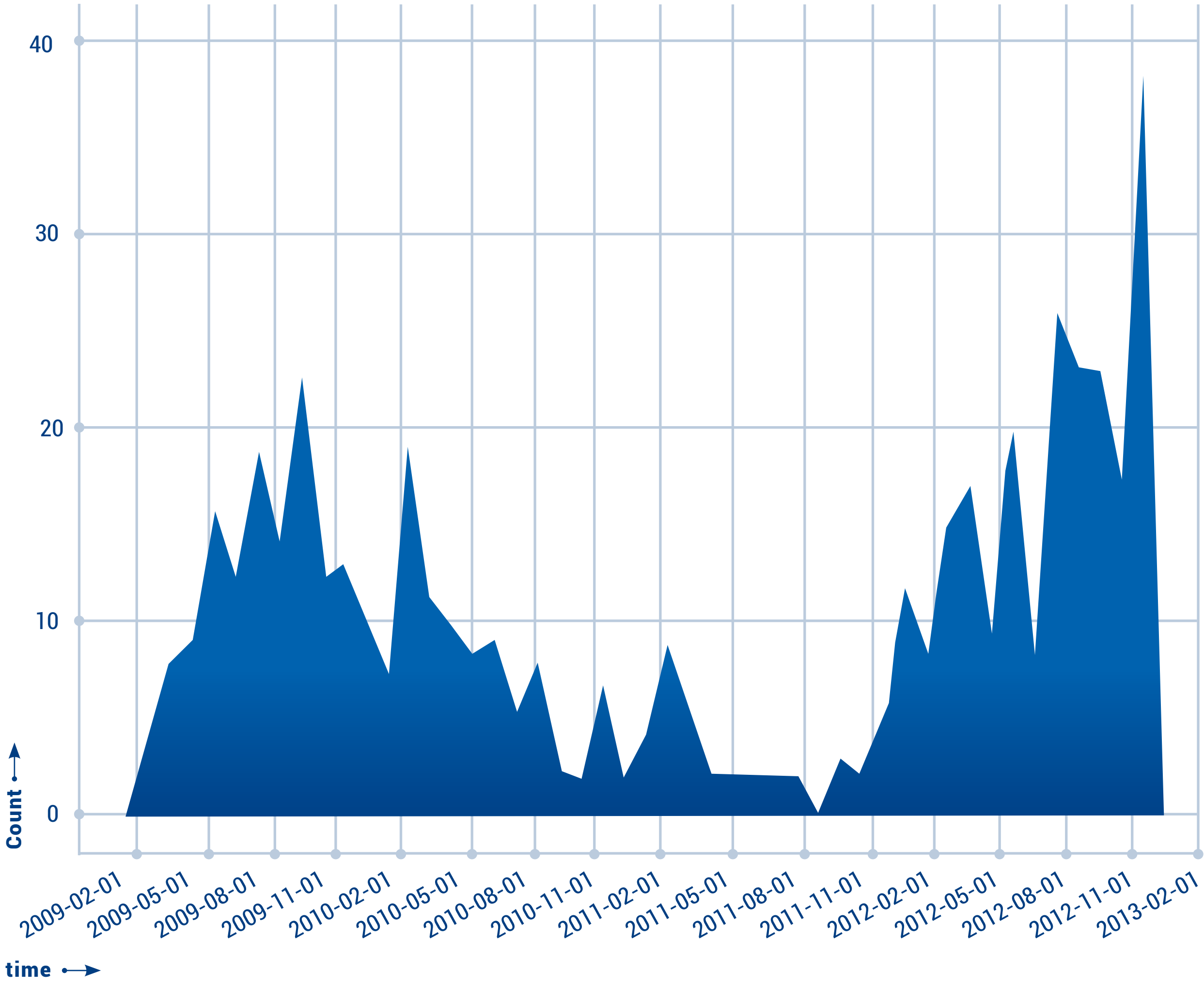


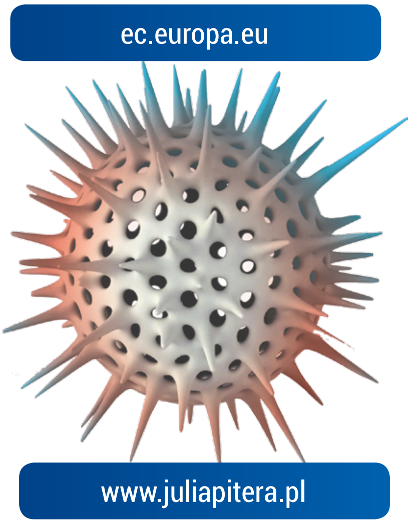
Figure 11. Number of incidents relating to malware for the last four years

4 Key incidents according to CERT Polska

4.1 Attacks connected with ACTA

At the end of January 2012 we observed multiple attacks on government websites. The attacks were connected with the protests after the Polish government revealed plans to sign the ACTA treaty, and were attributed to the Anonymous Polska group that exhorted to block the websites of the institutions responsible for studies on ACTA. Therefore, websites of the Polish Parliament, Ministry of Foreign Affairs and Internal Security Agency were among victims of these attacks. The list of targets, as well as links to LOIC-based software for launching the attacks and VPN clients for anonymisation were distributed via twitter, Facebook and the dedicated IRC channels The attacks lasted one week, from 21st to 28th January, and were effective in many cases. According to analysis by CERT Polska the traffic responsible for blocking the websites came mainly from Poland. It is evident that individuals using tools such as LOIC running on client side, had significant influence on the attacks, rather than traffic from botnets that is often used to launch these types of attacks.

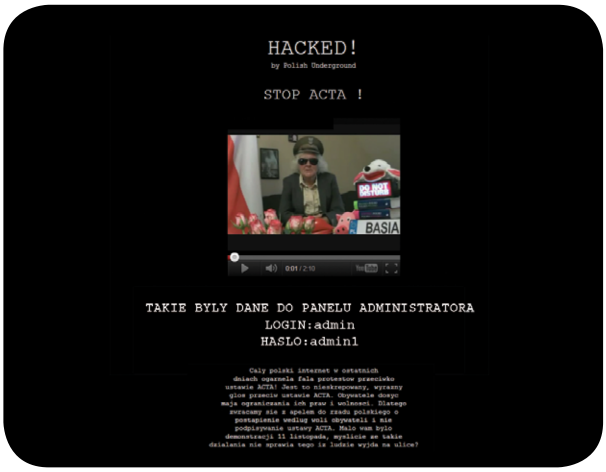
- sejm.gov.pl
- mac.gov.pl
- msz.gov.pl
- www.tesco.pl
- ec.europa.eu
- nfz.gov.pl
- www.ms.gov.pl
- holdys.pl
- zbigniewholdys.blip.pl
- justice.gov.sk
- www.radeksikorski.pl
- www.juliapitera.pl
- zaiks.org.pl
- www.bundeskanzler.at
- polish.poland.usembassy.gov
- www.minv.sk



The level of technical knowledge of the attackers varies greatly. Among the victims of the attacks there were also several various domains, often not related to ACTA (for example tesco.pl).

The list of domains that were the targets of Anonymous Polska in January 2012

Apart from the DDoS attacks, there were at least two confirmed defacements of government websites, namely Polish Prime Minister’s and the Ministry of Defense.



HACKED!
by Polish Underground

STOP ACTA !

TAKIE BYLY DANE DO PANELU ADMINISTRATORA
LOGIN:admin
HASLO:admin1

Caly polski internet w ostatnich dniach ogarnela fala protestow przeciwko ustawie ACTA! Jest to nieskrepowany, wyrazny glos przeciw ustawie ACTA. Obywatele dosyc maja ograniczania ich praw i wolnosci. Dlatego zwracamy sie z apelem do rzadu polskiego o postapienie wedlug woli obywateli i nie podpisywanie ustawy ACTA. Malo wam bylo demonstracji 11 listopada, myslicie ze takie dzialania nie sprawia tego iz ludzie wyjda na ulice?

Figure 12. Prime Minister's website with defaced content

4.2 The hunt for money mules

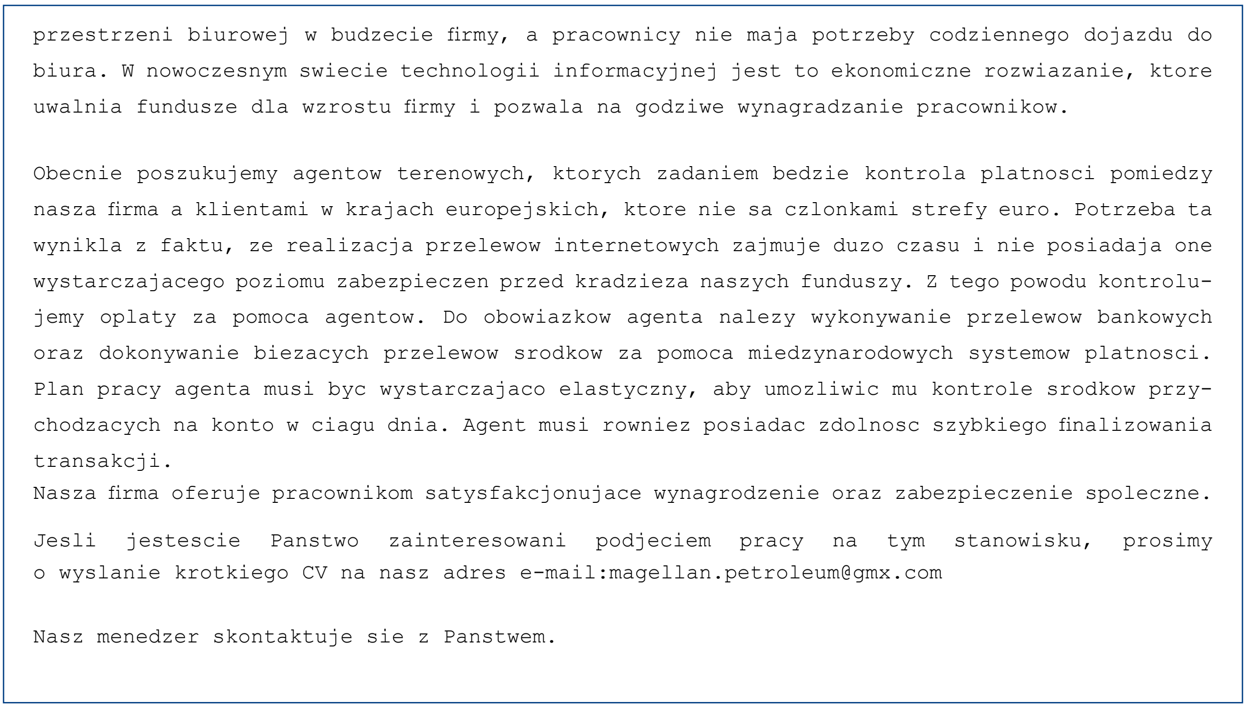
In 2012 there were several campaigns aimed at recruiting persons to cash out money stolen from on-line bank accounts.

Fraudsters look for people who would help them transfer stolen funds eg. through money orders. A recruited persons should be aware that they might be accused of complicity in the theft. When the stolen money travels through several countries, investigation becomes more complicated and requires contacts of prosecuting authorities from various countries which makes the entire process much longer. It is worth to mention the case of MoneyGram here. In November 2012 MoneyGram, one of the largest money transfer company, agreed to pay 100 million dollars as part of a government settlement in which the company admitted failing to maintain an effective anti-money-laundering program. This amount was estimated to be a minimum of money that was defrauded through MoneyGram in years 2004-2009.

“Identity theft”

The first large campaign recruiting agents took place in February 2012. The most interesting aspect of this case was the usage of the image of Magellan Pertoleum Corporation. Internet users received messages containing detailed descriptions of job and of company itself. It was advertised as a remote job as agents responsible for controlling money transfers between the company and its customers who were not residents of the eurozone. The company offered a very good salary.

```
Szanowni Panstwo!
Wydzial Magellan Petroleum Corporation, duzej miedzynarodowej firmy, przyjmuje aplikacje na
stanowisko w swoim dziale Kontroli Kredytowej dla Europy Wschodniej. Obecnie potrzebujemy
pracownikow w terenie, poniewaz nasz wydzial rozprowadza produkty firmy w krajach europejskich.

Dzieki poprawie koniunktury po kryzysie ekonomicznym co raz wiecej duzych firm zatrudnia
pracownikow do pracy zdalnej. Praca zdalna w znaczacym stopniu obniza koszty utrzymania
```



przestrzeni biurowej w budzecie firmy, a pracownicy nie maja potrzeby codziennego dojazdu do biura. W nowoczesnym swiecie technologii informacyjnej jest to ekonomiczne rozwiazanie, ktore uwalnia fundusze dla wzrostu firmy i pozwala na godziwe wynagradzanie pracownikow.

Obecnie poszukujemy agentow terenowych, ktorych zadaniem bedzie kontrola platnosci pomiedzy nasza firma a klientami w krajach europejskich, ktore nie sa czlonkami strefy euro. Potrzeba ta wynikla z faktu, ze realizacja przelewow internetowych zajmuje duzo czasu i nie posiadaja one wystarczajacego poziomu zabezpieczen przed kradzieza naszych funduszy. Z tego powodu kontrolujemy oplaty za pomoca agentow. Do obowiazkow agenta nalezy wykonywanie przelewow bankowych oraz dokonywanie biezacych przelewow srodkow za pomoca miedzynarodowych systemow platnosci. Plan pracy agenta musi byc wystarczajaco elastyczny, aby umozliwic mu kontrole srodkow przychodzacych na konto w ciagu dnia. Agent musi rowniez posiadac zdolnosc szybkiego finalizowania transakcji.
Nasza firma oferuje pracownikom satysfakcjonujace wynagrodzenie oraz zabezpieczenie spoleczne.

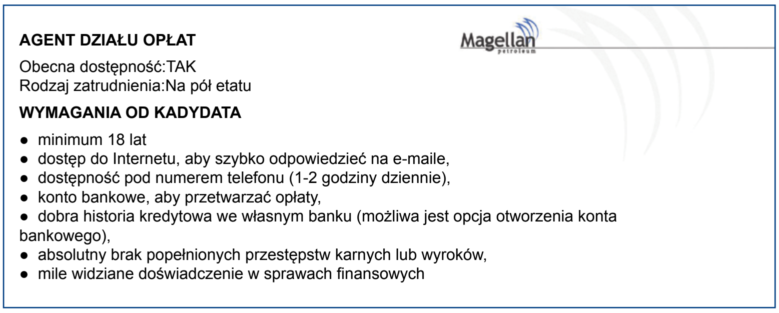
Jesli jestescie Panstwo zainteresowani podjeciem pracy na tym stanowisku, prosimy o wyslanie krotkiego CV na nasz adres e-mail:magellan.petroleum@gmx.com

Nasz menedzer skontaktuje sie z Panstwem.

In the field „From" there were many various addresses, of course all of them were fake. The contact with the miscreants s was established by sending back an e-mail to the address given in the message. We have observed five e-mail addresses provided as contact points for sending the resume:

```
m.petroleum@secretary.net
magellan.cv@europe.com
magellan.petroleum@gmx.com
magellan.petroleum@yahoo.com
magellan.resume@juno.com
```

After making the contact with the miscreants, the victim would receive a detailed job description (see Figures 13 and 14) and an application form containing questions about very detailed personal information. Afterwards, the form should be scanned and sent back by email.



AGENT DZIAŁU OPŁAT

Obecna dostępność:TAK
Rodzaj zatrudnienia:Na pół etatu

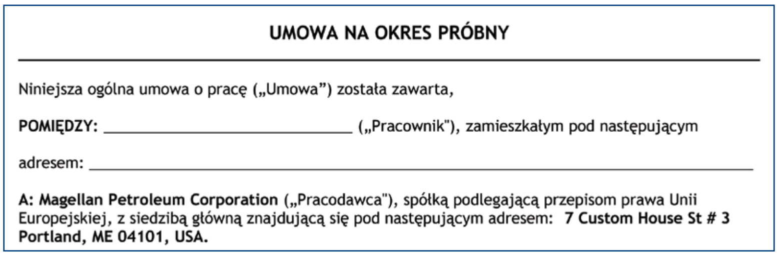
WYMAGANIA OD KADYDATA

- minimum 18 lat
- dostęp do Internetu, aby szybko odpowiedzieć na e-maile,
- dostępność pod numerem telefonu (1-2 godziny dziennie),
- konto bankowe, aby przetwarzać opłaty,
- dobra historia kredytowa we własnym banku (możliwa jest opcja otworzenia konta bankowego),
- absolutny brak popełnionych przestępstw karnych lub wyroków,
- mile widziane doświadczenie w sprawach finansowych

Figure 13. Job description - requirements

In some cases the victims were asked to give additional information such as phone number, home address of a family member or requested to send a scanned copy of a passport or other identity document. The job description contained information about salary and responsibilities. There was also a FAQ where it was explained in a clear way how to take money out of a bank account and to transfer it through either Western Union or MoneyGram.

When the victim got through this stage of recruitment he/she had to sign an eight-page probation contract (Figure 14). In the final stage of the recruitment it was necessary to send back a scanned copy of a driver's license or a passport.



UMOWA NA OKRES PRÓBNY

Niniejsza ogólna umowa o pracę („Umowa") została zawarta,

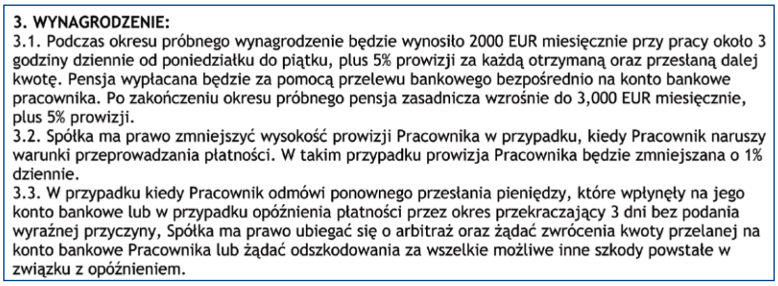
POMIĘDZY: ____________________________ („Pracownik"), zamieszkałym pod następującym

adresem: ____

A: Magellan Petroleum Corporation („Pracodawca"), spółką podlegającą przepisom prawa Unii Europejskiej, z siedzibą główną znajdującą się pod następującym adresem: **7 Custom House St # 3 Portland, ME 04101, USA.**

Figure 14. Contract

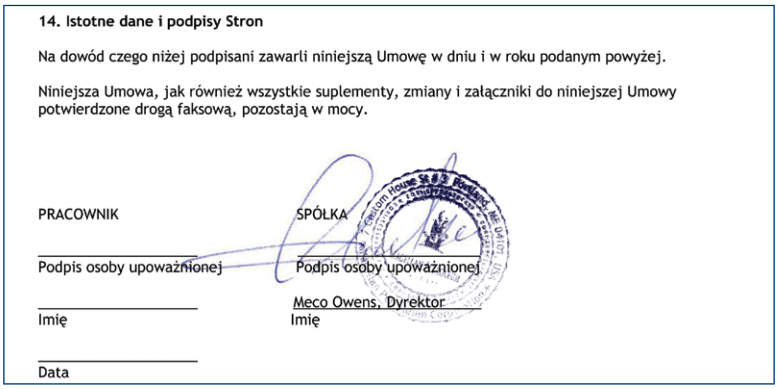
The contract contained detailed information on salary (Figure 15)



3. WYNAGRODZENIE:
3.1. Podczas okresu próbnego wynagrodzenie będzie wynosiło 2000 EUR miesięcznie przy pracy około 3 godziny dziennie od poniedziałku do piątku, plus 5% prowizji za każdą otrzymaną oraz przesłaną dalej kwotę. Pensja wypłacana będzie za pomocą przelewu bankowego bezpośrednio na konto bankowe pracownika. Po zakończeniu okresu próbnego pensja zasadnicza wzrośnie do 3,000 EUR miesięcznie, plus 5% prowizji.
3.2. Spółka ma prawo zmniejszyć wysokość prowizji Pracownika w przypadku, kiedy Pracownik naruszy warunki przeprowadzania płatności. W takim przypadku prowizja Pracownika będzie zmniejszana o 1% dziennie.
3.3. W przypadku kiedy Pracownik odmówi ponownego przesłania pieniędzy, które wpłynęły na jego konto bankowe lub w przypadku opóźnienia płatności przez okres przekraczający 3 dni bez podania wyraźnej przyczyny, Spółka ma prawo ubiegać się o arbitraż oraz żądać zwrócenia kwoty przelanej na konto bankowe Pracownika lub żądać odszkodowania za wszelkie możliwe inne szkody powstałe w związku z opóźnieniem.

Figure 15. Principles of remuneration

Of course, the contract was confirmed by giving the signature of "Director" and company stamp (Figure 16).



14. Istotne dane i podpisy Stron

Na dowód czego niżej podpisani zawarli niniejszą Umowę w dniu i w roku podanym powyżej.

Niniejsza Umowa, jak również wszystkie suplementy, zmiany i załączniki do niniejszej Umowy potwierdzone drogą faksową, pozostają w mocy.

PRACOWNIK

____
Podpis osoby upoważnionej

____
Imię

____
Data

SPÓŁKA

7 Custom House St # 3 Portland, ME 04101, USA
Magellan Petroleum Corporation

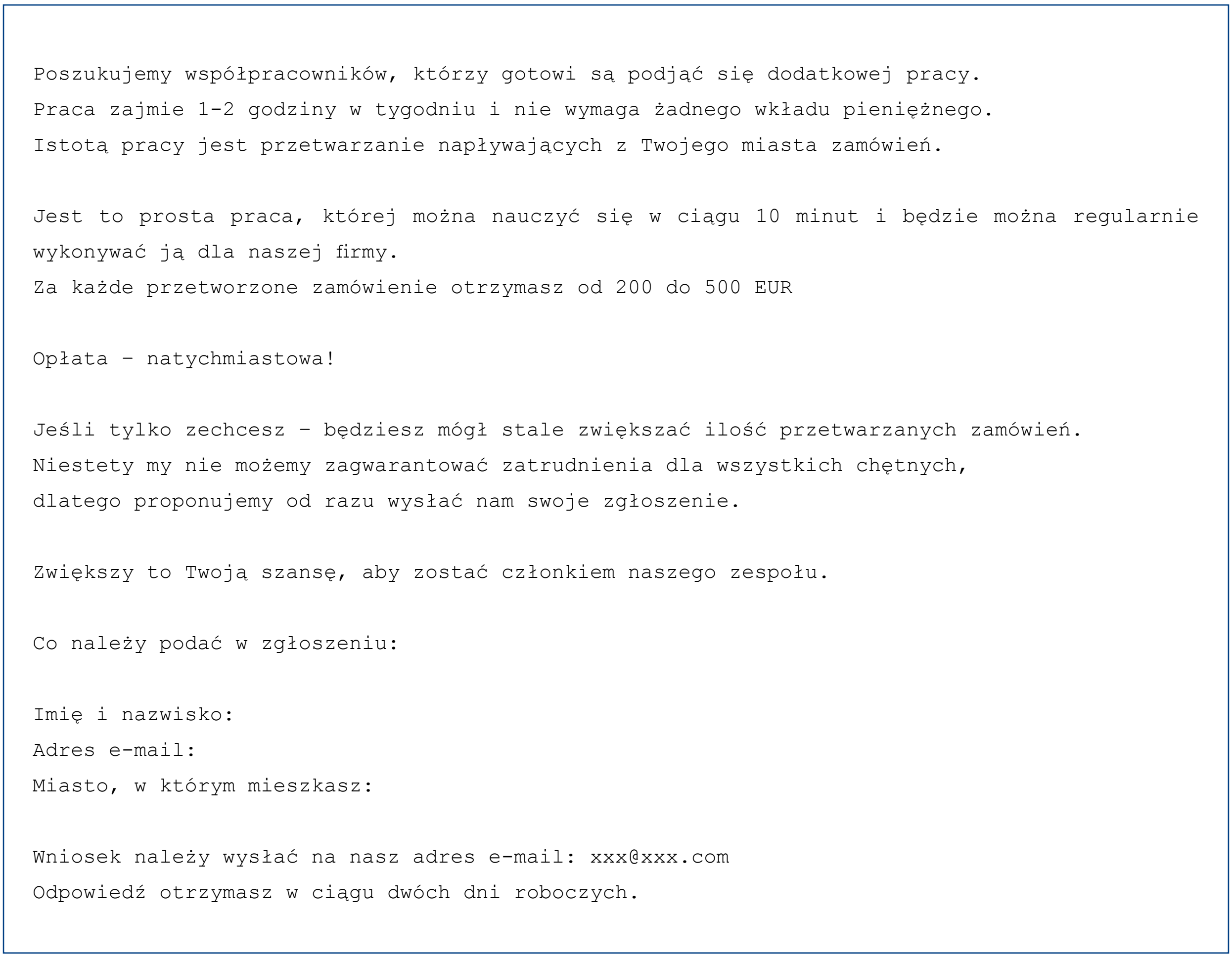
____
Podpis osoby upoważnionej

Meco Owens, Dyrektor
Imię

Figure 16. The part of contract with signature and stamp

How to earn 400 euros for two-hour work

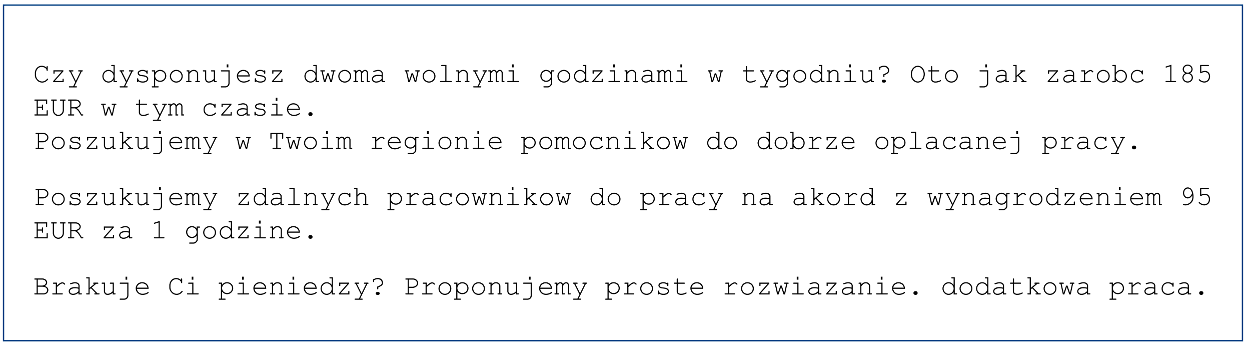
Other campaigns that followed usually did not use the image of any specific company. They are characterized by a simple message with a job offer that guaranteed high salary with a little effort. The sender of the spam message ensured that the job was very easy and it was possible to learn everything in 10 minutes. The work would take 1-2 hours a week and it did not require any investments. The application form should have been sent immediately because the number of free positions was limited.



```
Poszukujemy współpracowników, którzy gotowi są podjąć się dodatkowej pracy.
Praca zajmie 1-2 godziny w tygodniu i nie wymaga żadnego wkładu pieniężnego.
Istotą pracy jest przetwarzanie napływających z Twojego miasta zamówień.

Jest to prosta praca, której można nauczyć się w ciągu 10 minut i będzie można regularnie
wykonywać ją dla naszej firmy.
Za każde przetworzone zamówienie otrzymasz od 200 do 500 EUR

Opłata – natychmiastowa!

Jeśli tylko zechcesz – będziesz mógł stale zwiększać ilość przetwarzanych zamówień.
Niestety my nie możemy zagwarantować zatrudnienia dla wszystkich chętnych,
dlatego proponujemy od razu wysłać nam swoje zgłoszenie.

Zwiększy to Twoją szansę, aby zostać członkiem naszego zespołu.

Co należy podać w zgłoszeniu:

Imię i nazwisko:
Adres e-mail:
Miasto, w którym mieszkasz:

Wniosek należy wysłać na nasz adres e-mail: xxx@xxx.com
Odpowiedź otrzymasz w ciągu dwóch dni roboczych.
```

Sample message

Depending on the campaign the messages looked nearly identical. The email subject encouraged users to open it.



```
Czy dysponujesz dwoma wolnymi godzinami w tygodniu? Oto jak zarobc 185
EUR w tym czasie.
Poszukujemy w Twoim regionie pomocnikow do dobrze oplacanej pracy.

Poszukujemy zdalnych pracownikow do pracy na akord z wynagrodzeniem 95
EUR za 1 godzine.

Brakuje Ci pieniedzy? Proponujemy proste rozwiazanie. dodatkowa praca.
```

```
Zapraszamy do podjecia w wolnym czasie dodatkowej pracy z wynagrodze-
niem 95 EUR za 1 godzine.

Zarob 200-400 EUR za dwie godziny pracy juz w nastepnym tygodniu.
```

Sample message subjects

Similarily to the previous case user was asked to send back an email using the address given in the message. The domains used for these purpose were registered recently and belonged to recruitment companies or jobs portals.

```
jobrapidopl.com
jobspilotpl.com
graftonpl.com
toppolandjobs.com
topeuropajobs.com - EN
toppolandjobs.com
fastpolandjob.com
fasteurojobs.com - EN
jobspolska.com
quintcareerseu.com - EN
warszawaitpl.com
eurojobbnet.com - EN
artjobseu.com - EN
justpolandjob.com
pracainteria.com
totaljobspl.com
pracamoneypl.com
pracakariera.com
jobpilotpoland.com
```

Sample domains with the addresses where the applications should be sent

The messages were sent to users in Poland on a mass scale. Some emails were written in English, however, the scheme of recruiting “remote employees” was always the same.

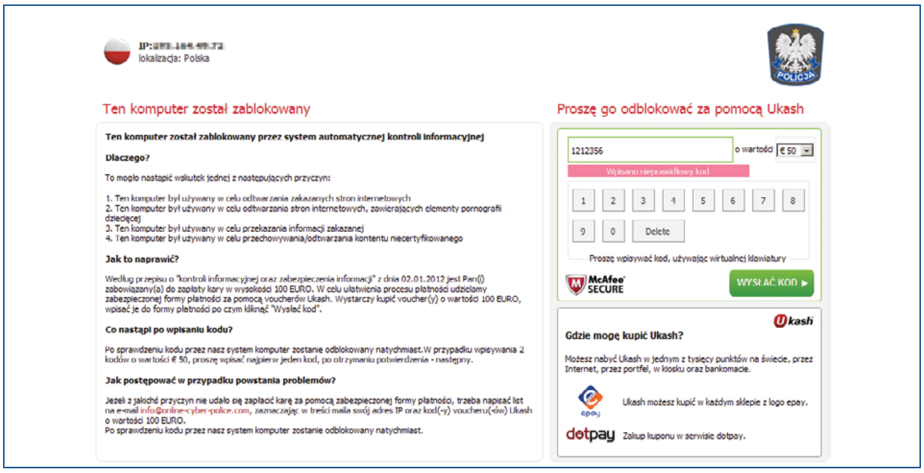
Summary

The use of correct Polish language as well as email addresses referring to Polish sites clearly show that the focus was on Poles and possibly had Poles somehow involved with the miscreants. The advertisements appeared also in university career offices and on legitimate sites with job offers, so they could be interesting for many people who did not realize in good time that the job offers were suspicious.

4.3 Ransomware – your computer has been locked!

Since May 2012 we have been observing the activity of Weelsof malware that uses quite crafty social engineering to extort money from the user. Weelsof restricts access to the computer system that it infects, and displays a note demanding a “fine” that should be paid in exchange for unlocking the system. The payment is 100 euro and should be paid through voucher service such as UKASH. The offenders refer to non-existent rules about ”information control and security information”. The message is written in correct Polish language and has the logo of Polish police to make it more believable.

This type of malicious software is called ransomware. It blocks some computer functions (for example it encrypts files, locks some programs), and then demands ransom for unlocking the system. After the ransom is paid, user usually receives unlocking key/code. An amount of ransom is relatively small which causes users to choose this method of solving the problem.



IP:[redacted]
lokalizacja: Polska

Ten komputer został zablokowany

Ten komputer został zablokowany przez system automatycznej kontroli informacyjnej

Dlaczego?

To mogło nastąpić wskutek jednej z następujących przyczyn:

1. Ten komputer był używany w celu odtwarzania zakazanych stron internetowych
2. Ten komputer był używany w celu odtwarzania stron internetowych, zawierających elementy pornografii dziecięcej
3. Ten komputer był używany w celu przekazania informacji zakazanej
4. Ten komputer był używany w celu przechowywania/odtwarzania kontentu niecertyfikowanego

Jak to naprawić?

Według przepisu o "kontroli informacyjnej oraz zabezpieczenia informacji" z dnia 02.01.2012 jest Pan(i) zobowiązany(a) do zapłaty kary w wysokości 100 EURO. W celu ułatwienia procesu płatności udzielamy zabezpieczonej formy płatności za pomocą voucherów Ukash. Wystarczy kupić voucher(y) o wartości 100 EURO, wpisać je do formy płatności po czym kliknąć "Wysłać kod".

Co nastąpi po wpisaniu kodu?

Po sprawdzeniu kodu przez nasz system komputer zostanie odblokowany natychmiast.W przypadku wpisywania 2 kodów o wartości € 50, proszę wpisać najpierw jeden kod, po otrzymaniu potwierdzenia - następny.

Jak postępować w przypadku powstania problemów?

Jeżeli z jakichś przyczyn nie udało się zapłacić karę za pomocą zabezpieczonej formy płatności, trzeba napisać list na e-mail info@online-cyber-police.com, zamaczając w treści maila swój adres IP oraz kod(-y) voucheru(-ów) Ukash o wartości 100 EURO.
Po sprawdzeniu kodu przez nasz system komputer zostanie odblokowany natychmiast.

Proszę go odblokować za pomocą Ukash

1212356 o wartości € 50

Wpisano nieprawidłowy kod

Proszę wpisywać kod, używając wirtualnej klawiatury

Gdzie mogę kupić Ukash?

Możesz nabyć Ukash w jednym z tysięcy punktów na świecie, przez Internet, przez portfel, w kiosku oraz bankomacie.

Ukash możesz kupić w każdym sklepie z logo epay.

Zakup kuponu w serwisie dotpay.

Figure 17. Weelsof software

Weelsof installs in the system using a drive-by-download method. This means that the user can get infected simply by visiting a (compromised) website which is hosting a so-called “exploitpack”. It takes control over the system of victim’s computer through vulnerabilities in the browser or one of its plugins to download and execute malware. After starting the computer, ransomware adds a number of entries to the system registry, turns off Explorer process (there is no menu “start”), hides all windows and then displays a message asking the user to pay fee.

The analysis of Weelsof and the ways of removing some types of this malware are presented in our site: **http://www.cert.pl/news/5483** and **http://www.cert.pl/news/5707**.

If you run into problems with malware such as ransomware we recommend staying calm and contacting the police and a specialized computer service. We absolutely do not recommend paying the ransom.

The problem does not relate only to Poland. Similar cases appeared at the same time all over the world, and sometimes software had hidden different messages in many languages that were activated depending on the language version of the computer system. In many cases operators of payment systems used for the ransom payment decided to put warnings on vouchers against using them to do that.

4.4 Sophisticated spyware attacks on-line banking customers - ZeuS Citadel, ZeuS P2P

At the beginning of September 2012, we observed entries appearing in the configuration files of spyware that related to transaction systems of Polish banks. The software attacked computers with Windows operating system. Once installed the software collected some pieces of information (mainly logins and passwords), and - if it had additional instructions in the configuration file – changed the content of selected web pages just before they are displayed in the browser.

These are the newest variants of ZeuS: Citadel and ZeuS P2P (malware based on the code of Zeus 2.0.8.9 which leaked in spring 2011).

The attacks were targeted at end users, whose computers were infected and spied by the attackers. Since the beginning of September we have observed in the malware configuration files entries related to 15 different transaction systems.

What kind of attacks can be launched against on-line banking customers?

Infecting the computer allows attackers to modify the content of bank websites. Attackers can display any message on the victim's screen. The method of attack and the content of messages are limited only by the creativity of criminals who have full control over your computer. This is a perfect example of a combination of social engineering methods and technical methods used together to achieve the goal of miscreants. A user will be convinced that he/she is reading messages from the bank. The messages appear after logging in to the bank account and are signed by the bank security department. Because the changes are made at the stage of displaying information in the browser, they will not trigger any alarms connected with securing the transmission with SSL encryption.

Below is a list of observed effects of changes made by malware:

- Replacing the destination account number and amount just prior to approval of the transfer
- Replacing the current account balance
- Modifications in the list of transactions
- A window asking a customer to enter one-time codes to activate/check security features
- A window asking a customer to enter his/her phone number and select the phone model (ZitMo/2011 attack)
- A prompt to return funds from an erroneous/suspicious transfer
- A prompt to make a test transfer to activate/test new security features

What is really going on in the computer?

After installation of malicious software, the attacker takes over full control of the victim's computer. The malware then has the ability to modify the website content displayed on the screen of an infected computer. It does not matter whether the connection was encrypted (https, a padlock icon displayed) because the changes are made after the data decryption. User does not have any possibility to verify if the website was modified before being displayed. Changes can be different: from one single word to huge scripts containing thousands of lines of code.

Figure 18 shows how the mechanism to modify content on the fly works. The information is prepared in the banking system, and then sent encrypted (green) to the user's computer, where the content is decrypted before the browser can display it. Malicious software may capture the decrypted content and introduce pre-programmed changes. In some cases, these changes can result in injection of additional elements into the banking system webpage displayed on the user's screen. Those elements may even be retrieved from a server controlled by criminals (red).

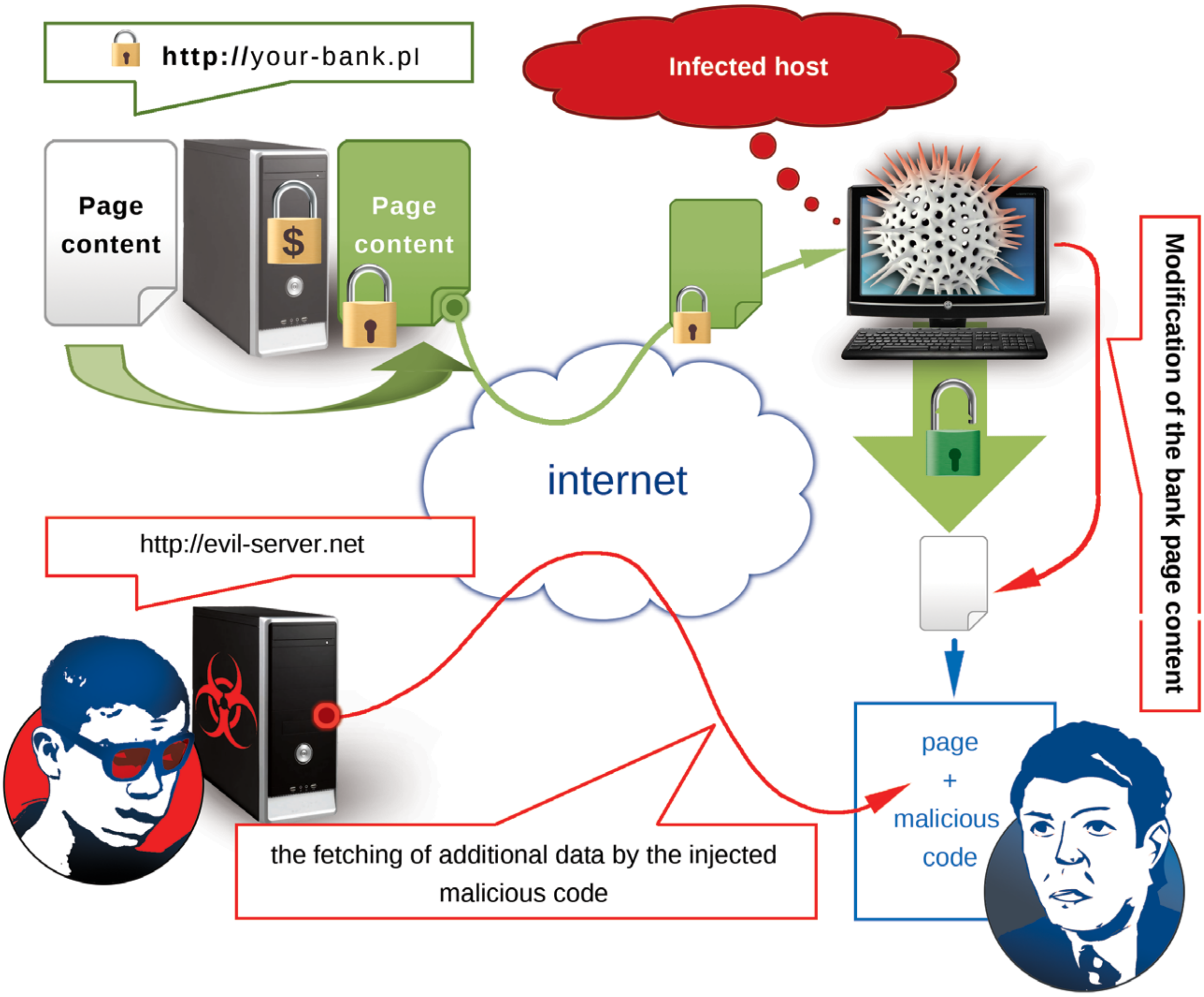


Figure 18. Mechanism to modify content on the fly

How to protect against attacks?

The only effective method of defense is vigilance. New and previously unknown messages in an online transaction system may be reported and discussed with the support of the bank. The use of the second channel (be it a phone call or a visit to the facility) to report such an incident can verify if the message on the screen really came from our bank. In addition, it is worth noting that banks rarely (if ever) introduce substantial changes in their systems without a prior extensive information campaign.

4.5 ZeuS-p2p and attacks on its network

Introduction

Zeus-p2 is not the first malicious software to utilise its own p2p network for communication. Undoubtedly, the implementation of this method of communication makes fighting malware much more difficult and allows a botmaster to remain hidden much longer.

On the other hand, p2p networks can be subject to invigilation as a computer that is a part of the network can connect to any other node. Crawling of the network in such way allows for identification of IP addresses belonging to infected machines.

Real threat to Polish users

September to December 2012, the configuration files of ZeuS-p2p contained entries related to addresses of transaction systems of Polish banks. Miscreants have prepared code injection rules for 10 different systems. On 26th of December these entries were removed from configuration files. However, since the attack had been active for 4 months, it targeted a large number of victims.

How does Zeus-p2p operate?

The new version of ZeuS-p2p still uses two channels of communication. The main channel is the peer-to-peer network. It is used for exchange of data related to the maintenance of the p2p network, as well as for sending configuration files and reports to the C&C. The second (back-up) channel is the DGA – Domain names Generation Mechanism.

DGA is activated when there is a problem with the p2p network communication, like a lack of active nodes in the "table of neighbors". It generates a list of domain names in the following TLDs: .ru, .biz, .org, .net, .com. The list contains over 1,000 domains and changes every 7 days. When the list is generated the bot attempts to connect with each generated name using the HTTP protocol. If the connection is successful, a new list of p2p network nodes is downloaded and added to the "table of neighbors".
At the beginning of 2012 the code of ZeuS-p2p was updated significantly. The most significant changes took place in the mechanism of sending data to the C&C servers. The previous version of ZeuS was based on one (or few) predefined addresses which were used for botnet management. After the update, data is sent by using a set of chosen supernodes of the p2p network. Therefore, finding the ultimate destination for data dumps without invigilation of the network is simply impossible. This innovation entailed the need for another mechanism – maintenance of packets broadcasting addresses of the supernodes. The updated malware also includes functionality to download resources (the resources in the p2p network are configuration and binary files) with UDP protocol (previously it had been possible only by using TCP protocol).

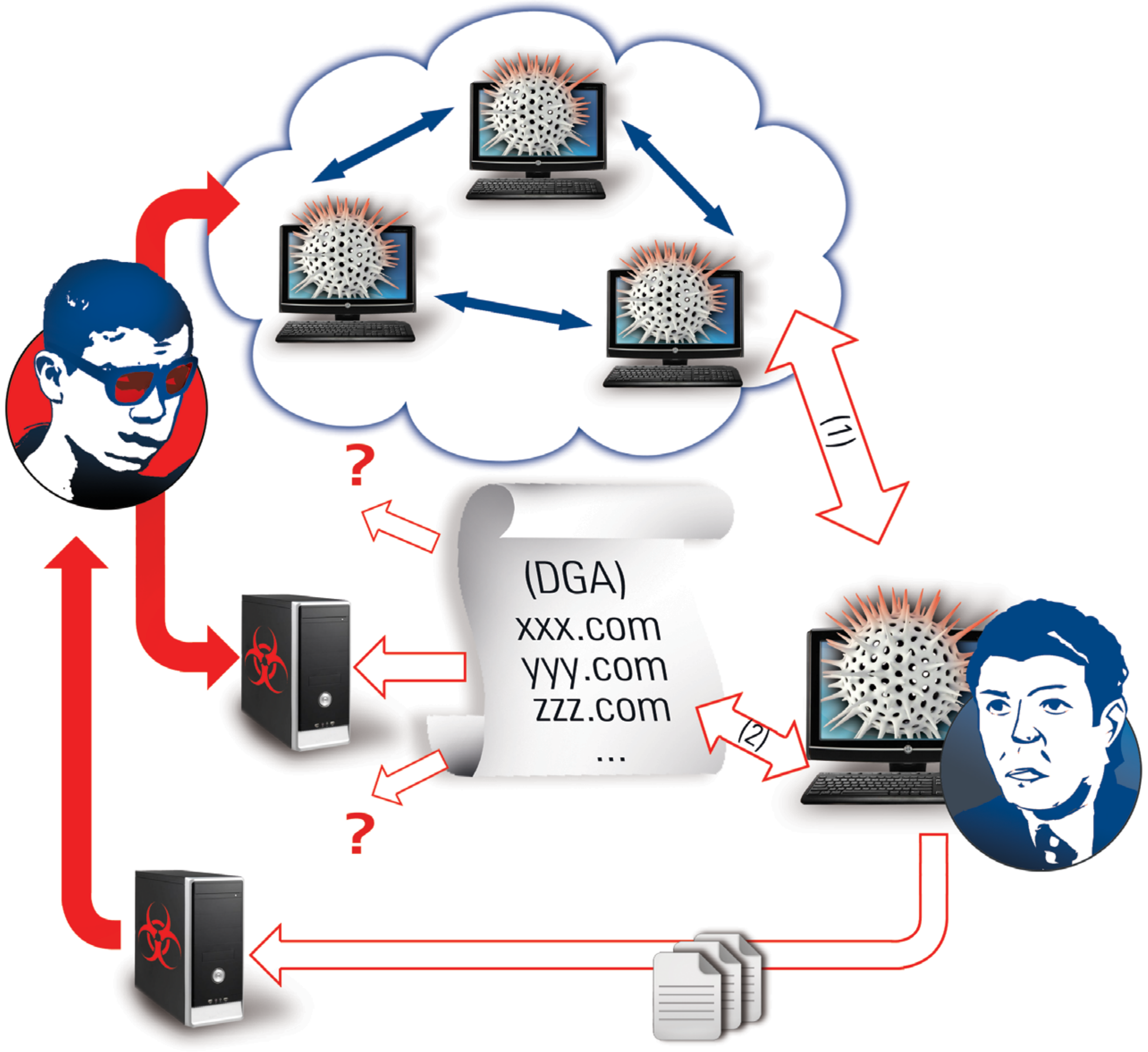
How does the p2p network operate?

Messages transported in the p2p network can be divided into two groups: messages to maintain the p2p network and messages to exchange data. The first category includes three types of packets:

- Exchange of information about the neighbors – used to exchange information about addresses of other active nodes in the p2p network
- Exchange of information about available versions of resources
- Distribution of information about supernodes – broadcasting information about addresses and identifiers of nodes in the p2p network used for data sending.

Among the messages used for exchanging data we can distinguish:

- Downloading of new resources (using TCP and/or UDP protocols)
- Sending data through the proxy supernodes.
- Remote upgrades of resources (PUSH)



Upgrade of resources

The process of upgrading the bot's resources is done in stages. First the malware chooses a node from its "table of neighbors". Then it queries it for available version of resources. In response it receives a packet containing version numbers of the configuration file, the binary file and the TCP port number. If the node that performed the query has an older version of the configuration than the version given in response to this query – the bot initiates a TCP connection to the remote computer asking for the newer version of the configuration. In case the connection fails, the bot repeats the attempt using the UDP protocol. Due to characteristics and limitations imposed on the UDP protocol, download of resources when it is in use is effectively a transmission of a sequence of fragments sized 1 KB.

Attacks on the p2p network and DGA

Below is a list of possible scenarios of attacks on the ZeuS p2p network that were examined by CERT Polska.

Attack: Using domains from DGA

The attack is based on the generation of a long list of domain names by using the same domain generation algorithm implemented in Zeus p2p and registering selected ones. The names can be used to host an HTTP server, responding to infected computers with a false list of nodes.

Defence: Data served from the back-up servers under the generated domain names is expected to be digitally signed. After the data is downloaded, bots verify the signature and drop the crafted list.

Attack: Distribution of false resources in the p2p network

The attack is based on distributing false resources in the p2p network

Defense: After retrieving resources from the p2p network the bot checks if they are digitally signed and if the signature is valid. This prevents the distribution of unsigned resources in the p2p network.

Attack: Falsifying version of the resource

The attack is based on sending a false response to a query about the version, causing malware to go into update mode and start downloading new resources.

Defence: To successfully download a resource it is necessary to distribute data with a correct digital signature. It is possible to give higher value of the version number in the response to a query, and afterwards supply old data with correct signature. Unfortunately the exchanged data has additional field with the version number. After downloading data and verifying the signature, the version number is checked again (this time with the value coded in the resource). Due to version number mismatch, this fake update will be rejected despite the correct digital signature.

Attack: Poisoning the network by false nodes

This is the most common attack on the p2p network. It is based on responding to the query about the neighbor nodes with a specially crafted list of addresses. The list contains addresses of computers controlled by attackers. As a result, nodes searching for new neighbors will likely contact the attackers, and in the end the “table of neighbors” will be filled with the crafted addresses. In that case it is necessary to know the mechanism deciding which addresses and in which situation will be added to the local table of neighbors.

Defence: this type of attacks poses a significant challenge for botmaster. Exchanging the neighbors’ addresses is one of the basic mechanisms maintaining proper operation of the p2p network. Therefore, the only defense is to program the mechanism updating the local list of neighbors in such way that it would reject suspicious entries or duplicate addresses.

Registered attacks on the p2p network

In 2012 our system which monitors the p2p networks registered two nearly successful attacks. Nearly – because in a short time the botnet recovered with an update which made it more resilient. Both attacks were based on poisoning of the neighbor list of computers belonging to the botnet.

The figure below shows the activities in the p2p network according to our monitoring system. As you can see, “the spring poisoning” caused slow but steady decrease in the activity. The lowest level of activity had lasted for 11 days until a new version of bot was distributed. It resulted in blocking the attack and rapid increase in the registered activity.

The main change introduced with the spring update was adding the blacklist mechanism. The blacklist is coded in the bot's binary file and contains 22 networks. If the address of a bot computer belonged to one of these networks, its advertisements will be ignored.
The autumn poisoning affected the network much faster. The attack caused a rapid decrease in the activity – and after few days levels observed in the monitoring system reached almost zero. However, once again the botmaster managed to launch and distribute an update that restored the p2p network. This time it took 13 days.

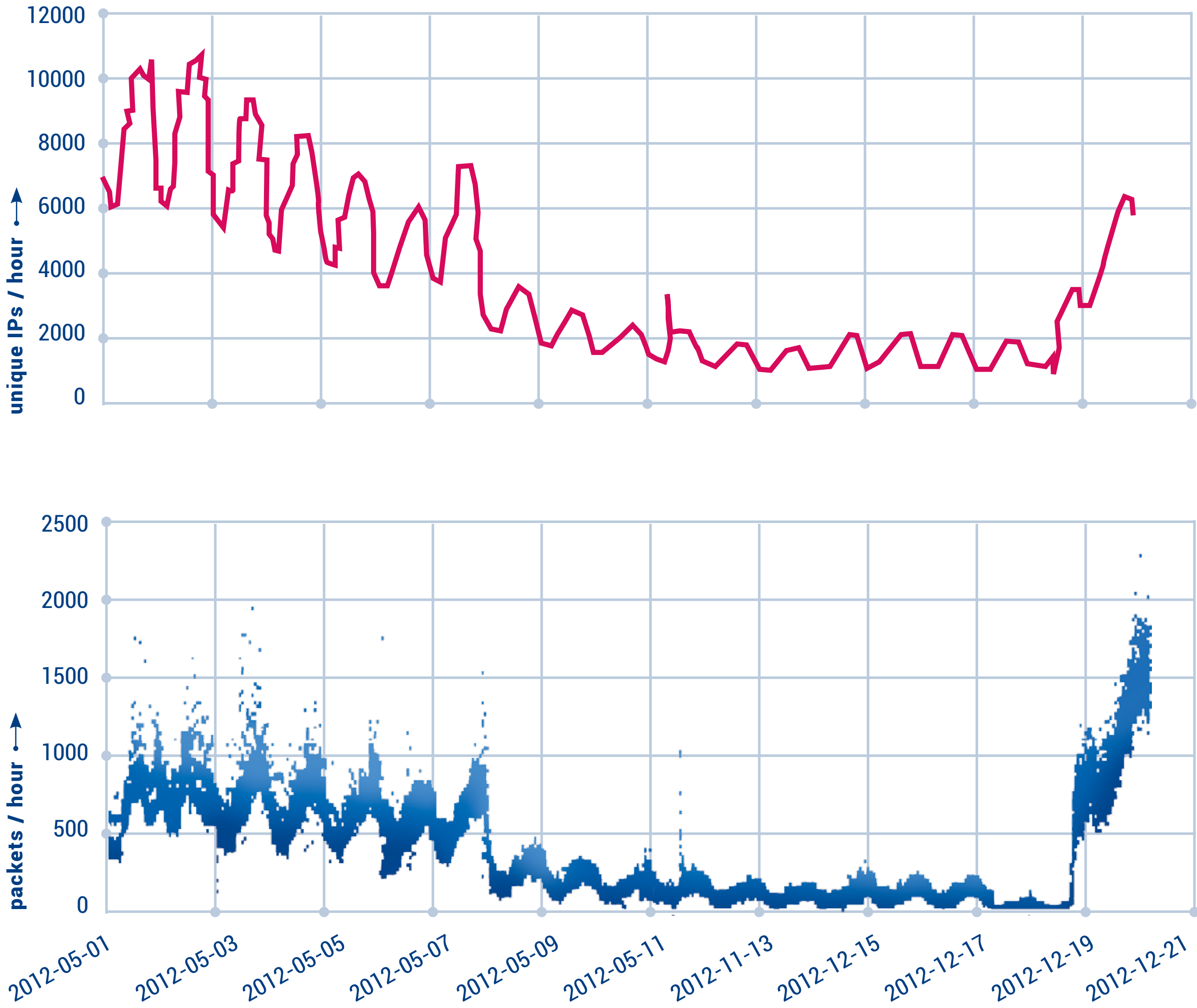


Figure 19. Activity in the p2p network in the monitoring systems of CERT Polska – „Spring poisoning"

The update introduced new mechanisms that make poisoning of the p2p network with false neighbors even more difficult. The first one reduces the permitted number of addresses belonging to the same sub-network (255.255.255.0) on the neighbor list. Another one limits the number of packets getting from one IP address to 10 per 60 seconds.

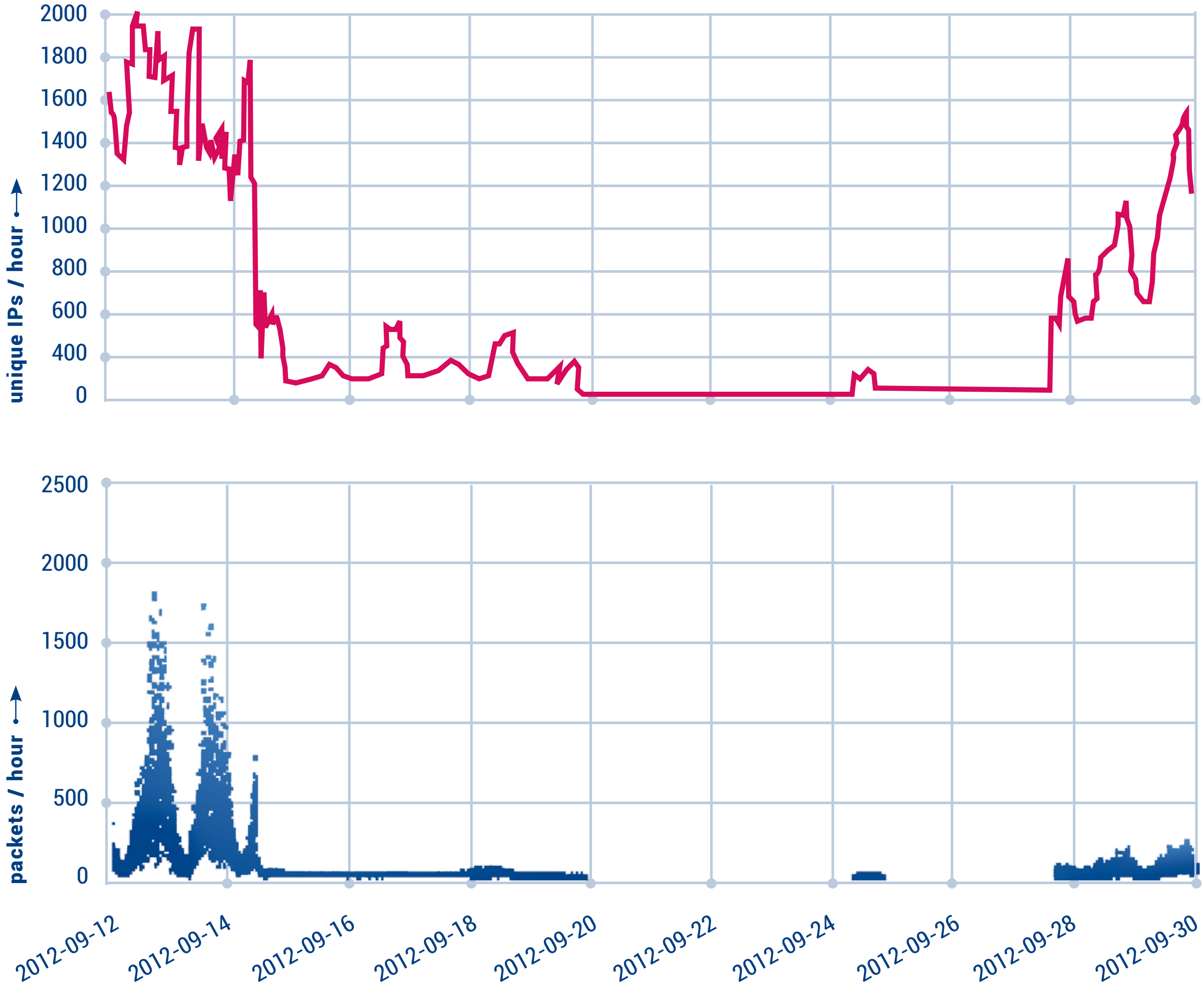


Figure. 20. Activity in the p2p network in the monitoring systems of CERT Polska – „Autumn poisoning"

4.6 Flame

Flame (also known as Flamer, Skywiper) is a sophisticated Trojan application discovered in 2012. Since then it has been the subject of extensive analysis[1] by malware research community. The Trojan has been recognized as extraordinarily complicated, with a modular design and advanced algorithms. The degree of Flame's complexity raised many theories about its origins[2]. One of the earliest reports about Flame was published by CrySyS Lab[3] and contained mostly behavioral observations, i.e. interactions with OS, file system, network, and interaction timings. This inspired us to delve a little bit more into its internal operations, so as to gather insight that has not, to our knowledge, yet been published.

[1] *http://www.securelist.com/en/blog/208193522/*
http://blog.eset.com/2012/07/20/flame-in-depth-code-analysis-of-mssecmgr-ocx

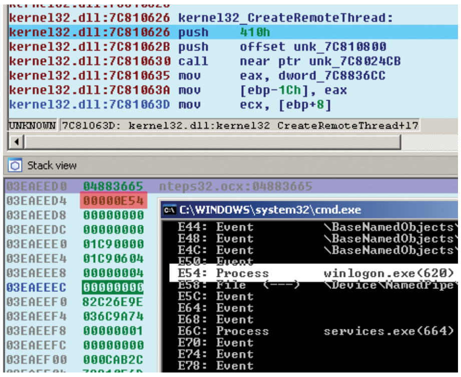
[2] *http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html*

[3] *http://www.crysys.hu/skywiper/skywiper.pdf*

4.6.1 Code injection

Code injection is a long known and popular technique employed by malware authors to distribute malicious operations into various operating system elements, ranging from ring 3 structures, such as processes & threads (thread injection, hooks) to ring 0 objects (deploying drivers, GDT hooking, overwriting kernel memory).

Thread injection can also be observed in the Flame installation process, but in this case simple thread injection is turned into a precise tool for transferring code into other processes and threads and is used extensively throughout the bot's lifecycle (since installation until suicide). Flame uses this technique to move and copy its elements around a victim's operating system with a stunning agility. In course of our analysis we encountered that it employs an elaborate technique to inject some sensitive parts of code.



```
kernel32.dll:7C810626 kernel32_CreateRemoteThread:
kernel32.dll:7C810626 push    410h
kernel32.dll:7C81062B push    offset unk_7C810800
kernel32.dll:7C810630 call    near ptr unk_7C8024CB
kernel32.dll:7C810635 mov     eax, dword_7C8836CC
kernel32.dll:7C81063A mov     [ebp-1Ch], eax
kernel32.dll:7C81063D mov     ecx, [ebp+8]
UNKNOWN 7C81063D: kernel32.dll:kernel32 CreateRemoteThread+17
```

```
03EAEED0  04883665  nteps32.ocx:04883665
03EAEED4  00000E54
03EAEED8  00000000
03EAEEDC  00000000
03EAEEE0  01C90000
03EAEEE4  01C90604
03EAEEE8  00000004
03EAEEEC  00000000
03EAEEF0  82C26E9E
03EAEEF4  036C9A74
03EAEEF8  00000001
03EAEEFC  00000000
03EAEF00  000CAB2C
```

```
E44: Event           \BaseNamedObjects
E48: Event           \BaseNamedObjects
E4C: Event           \BaseNamedObjects
E50: Event
E54: Process         winlogon.exe(620)
E58: File   (---)    \Device\NamedPipe
E5C: Event
E64: Event
E68: Event
E6C: Process         services.exe(664)
E70: Event
E74: Event
E78: Event
```

Figure 21. Code injection by CreateRemoteThread() function

4.6.2 Chain of injections

As we can read in the CrySyS report:

"At startup, mssecmgr.ocx is loaded as LSA Authentication Package. About 2 minutes later advnetcfg.ocx is loaded by services.exe. It is repeated every 2 to 3 minutes 3 times in total. About 2 minutes later services.exe loads nteps32.ocx from mssecmgr.ocx, and then winlogon.exe also loads nteps32.ocx. This file is loaded several times. In the meantime, explorer.exe starts 5 iexplore processes that subsequently create wpgfilter.dat."

[CrySyS Skywiper report, Activation and propagation, Startup sequence, tłum. aut.]

The fact that the explorer.exe process creates several iexplore.exe instances all of a sudden is especially interesting. Let us clarify what that means: Flame has propagated its elements through four processes in order to perform its Trojan operations! We decided to investigate this process in detail.

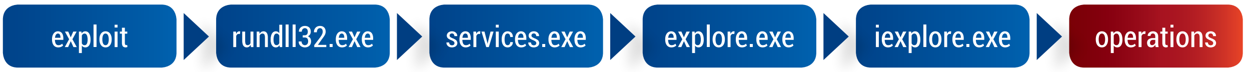
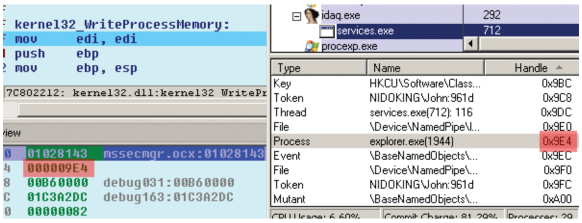


Figure 22. Propagation of Flame code

Injection process

The victim's computer is infected, among other possible vectors, through exploitation of the MS10-061[4] vulnerability. Upon a successful break-in, rundll32.exe module is started and ordered to load and execute Flame's main module – mssecmgr.ocx. It performs various installation operations (including registering LSA service, so that the bot will be loaded during startup after reboot) and then finds services.exe process and injects parts of its code into it.



```
kernel32_WriteProcessMemory:
mov     edi, edi
push    ebp
mov     ebp, esp

7C802212: kernel32.dll:kernel32 WritePr

iew
0  01028143  mssecmgr.ocx:01028143
4  000009E4
8  00B60000  debug031:00B60000
C  01C3A2DC  debug163:01C3A2DC
0  00000082
```

```
idaq.exe            292
  services.exe      712
procexp.exe
```

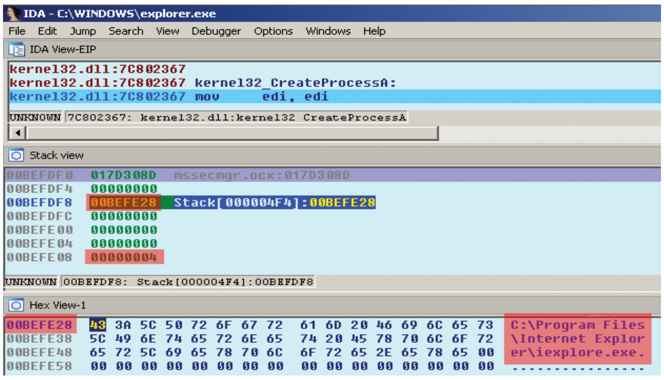
Type	Name	Handle
Key	HKCU\Software\Class...	0x9BC
Token	NIDOKING\John:961d	0x9C8
Thread	services.exe(712): 116	0x9DC
File	\Device\NamedPipe\l...	0x9E0
Process	explorer.exe(1944)	0x9E4
Event	\BaseNamedObjects\...	0x9EC
File	\Device\NamedPipe\...	0x9F0
Token	NIDOKING\John:961d	0x9FC
Mutant	\BaseNamedObjects\...	0xA00

CPU Usage: 6.60% Commit Charge: 81.29% Processes: 29

Figure 23. Code injection to explorer.exe

Then, services.exe distributes subsequent parts of code through regular injections into various elements of the operating system. It also prepares and injects the code for explorer.exe.

We tracked this injection in order to research its purpose. Injected thread waits for a signal from services.exe and then creates an iexplore.exe process with main thread suspended.


IDA - C:\WINDOWS\explorer.exe
File Edit Jump Search View Debugger Options Windows Help
IDA View-EIP
Stack view
Hex View-1

```
kernel32.dll:7C802367
kernel32.dll:7C802367 kernel32_CreateProcessA:
kernel32.dll:7C802367 mov     edi, edi

UNKNOWN 7C802367: kernel32.dll:kernel32 CreateProcessA
```

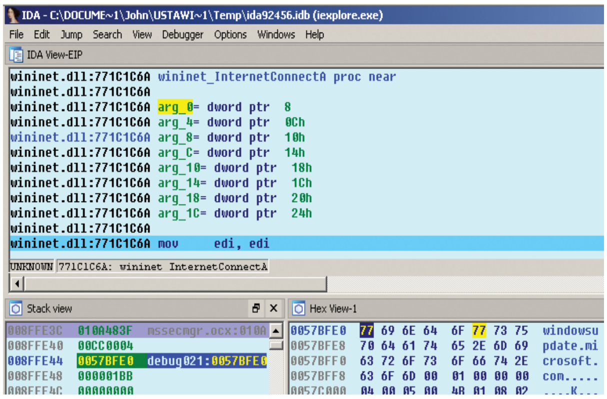
```
00BEFDF0  017D308D  mssecmgr.ocx:017D308D
00BEFDF4  00000000
00BEFDF8  00BEFE28  Stack[000004F4]:00BEFE28
00BEFDFC  00000000
00BEFE00  00000000
00BEFE04  00000000
00BEFE08  00000004

UNKNOWN 00BEFDF8: Stack[000004F4]:00BEFDF8
```

```
00BEFE28  43 3A 5C 50 72 6F 67 72  61 6D 20 46 69 6C 65 73  C:\Program Files
00BEFE38  5C 49 6E 74 65 72 6E 65  74 20 45 78 70 6C 6F 72  \Internet Explor
00BEFE48  65 72 5C 69 65 78 70 6C  6F 72 65 2E 65 78 65 00  er\iexplore.exe.
00BEFE58  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Figure 24. Starting the process iexplorer.exe

[4] *http://www.securelist.com/en/blog/208193522/*

From now on, services.exe and iexplore.exe communicate with each other over a named pipe (in our case: **PipeGx16**, but this name could be constructed from randomly chosen characters and could differ among installations). A thread running in services.exe context writes its orders into the pipe. Then iexplore.exe process reads and executes them. One of the orders being executed is to connect to windowsupdate.microsoft.com, as shown in the pictures. This is a proof of one of Flame's Trojan operations – setting up covert connection. This activity might be checking for Internet connectivity or, more likely, a prelude to sophisticated man-in-the-middle attack, so called "Gadget" attack[5]. The iexplore.exe process remains running and executing orders until PipeGx16 is being closed. After that, explorer.exe terminates iexplore.exe.


IDA - C:\DOCUME~1\John\USTAWI~1\Temp\ida92456.idb (iexplore.exe)
File Edit Jump Search View Debugger Options Windows Help
IDA View-EIP
Stack view
Hex View-1

```
wininet.dll:771C1C6A wininet_InternetConnectA proc near
wininet.dll:771C1C6A
wininet.dll:771C1C6A arg_0= dword ptr  8
wininet.dll:771C1C6A arg_4= dword ptr  0Ch
wininet.dll:771C1C6A arg_8= dword ptr  10h
wininet.dll:771C1C6A arg_C= dword ptr  14h
wininet.dll:771C1C6A arg_10= dword ptr  18h
wininet.dll:771C1C6A arg_14= dword ptr  1Ch
wininet.dll:771C1C6A arg_18= dword ptr  20h
wininet.dll:771C1C6A arg_1C= dword ptr  24h
wininet.dll:771C1C6A
wininet.dll:771C1C6A mov     edi, edi
UNKNOWN 771C1C6A: wininet InternetConnectA
```

```
008FFE3C  010A483F  mssecmgr.ocx:010A
008FFE40  00CC0004
008FFE44  0057BFE0  debug021:0057BFE0
008FFE48  000001BB
008FFE4C  00000000
```

```
0057BFE0  77 69 6E 64  6F 77 73 75  windowsu
0057BFE8  70 64 61 74  65 2E 6D 69  pdate.mi
0057BFF0  63 72 6F 73  6F 66 74 2E  crosoft.
0057BFF8  63 6F 6D 00  01 00 00 00  com.....
0057C000  04 00 05 00  4B 01 08 02  ....K...
```

Figure 25. Initiating the connection with the address windowsupdate.microsoft.com

4.6.3 Evading detection

This is the most elaborate use of code injection we've ever seen in malware. Usually the process of executing a Trojan routine (such as creating an internet covert connection) involves only one thread injection. This is true even in the case of advanced banking Trojans. The Flame's process that we analyzed involved three injections and it's one of several evidences of its advanced architectural design. But, one may ask, why do this in such a complex way? The answer is obvious: to remain undetected for long time. Let us examine some of the significant features of Flame's injections.

First, Internet connection is being set by the iexplore.exe process. This way Flame evades many automated checks and superficial analysis. For example, the explorer.exe process trying to setup an internet connection (which is the case in SpyEye) is a suspicious sign, because creating connections with the network is simply not its purpose; contrary to iexplore.exe, whose major purpose is to interact with the web.

Also, connection attempts made to Windows Update site are hardly going to raise an eyebrow even in restricted segments of corporate or government networks, because everyone knows that Windows systems are expected to contact that site. After all, it was supposed to be protected by "secure" cryptographic routines … which we now know were circumvented with the already mentioned Gadget attack.

[5] *http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified/*

This is a sophisticated attack employing an excellent 0day exploit, very unlikely to be detected for a long time, as indeed turned out to be the case.

Also, the fact that iexplore.exe is being created and terminated by explorer.exe is the most natural thing! When the user launches her favourite browser, she does so via explorer.exe interface. That is why Flame uses explorer.exe as a proxy, so that process hierarchy remains completely consistent.

4.6.4 Summary

Flame employs the most sophisticated system of code injections we've observed in malware. It distributes its elements throughout the OS processes using chains of up to three injections involving up to four processes in order to perform its Trojan operations. The distribution among various processes, with respect to natural process hierarchy, renders behavior-based detection very hard. This system is one of Flame's exceptional features which allowed it to operate undetected for months and years and the reason for its widespread recognition.

4.7 Malicious registrations in .pl domain name space

In 2012 we observed an increasing number of incidents concerning the usage of .pl domain names for malware and botnet management, as well as for other criminal activities (for example hosting fake pharmacy sites).

The criminals often refer to the C&C controllers through their domain names (rather than directly by IP numbers), which allows them for greater flexibility in managing their infrastructure – they may easily move servers to other suppliers, as well as use mechanisms such as fast-flux. Although the removal of a problematic domain name is a simple thing from a technical point of view, it is often associated with legal uncertainties. The criminals exploit this weakness and instead of using free subdomain names, they pay for names in the national domains of different countries, including Poland. In a single case RunForestRun which compromised websites using Plesk Panel, used domain generation algorithm to create unique domain names ending with waw.pl. Previously, the same malware used names in the .ru domain.

In Table 21 a breakdown of bots using .pl domains is provided according to the number of domain names. In most of cases the domains resolved to IP addresses located abroad, mainly in China, Russia or Latvia.

Virut	43
ZeuS/Citadel	28
Dorkbot	4
SpyEye	4
other	39

Table 22. Botnets using .pl domains which are observed the most often (according to the number of domains)

5 Key events in the activity of CERT Polska

5.1 Secure 2012 conference

The 16th international SECURE 2012 conference was organized on 23-24 October by NASK and CERT Polska team operating in the NASK framework. The event, which was held at Copernicus Science Centre in Warsaw, brought together a record number of 46 speakers dealing with cyber threats, along with over 300 participants from Poland and all around the globe. The international line-up of speakers at the SECURE 2012 conference included Dr Jose Nazario of the Honeynet Project, who gave a talk on how to measure botnet networks, Chris Novak from Verizon who, together with his co-speakers, presented cases of data leaks from large companies and presented available remedial methods as well as Robert McArdle from Trend Micro, who gave two talks, one attempting to define the value of a user's online identity, and discussing HTML5 weaknesses in the other. The conference also featured the very first talk in Poland from a Twitter representative - Alek Kołcz. Conference highlights included also talks by Rik Ferguson (Trend Micro) and Ryan Pittman, who described NASA activities in the scope of fighting cybercrime.

SECURE 2012 was also an occasion to get familiar with the work of local experts dealing with network security and cybercrime. Piotr Konieczny, the owner of the website niebezpiecznik.pl, showed the audience what information users leave behind on the Internet, how it can be recovered and used against them. Allegro representative Błażej Szymczak discussed how human weaknesses affect the world of e-commerce. The talks delivered by NASK and CERT Polska representatives enjoyed a special interest. Paweł Pawliński of CERT Polska presented the Honey Spider Network 2.0 client honeypot system. Tomasz Bukowski and Radosław Żuber in turn, presented an overview of the most interesting incident reports received in the previous year by the CERT Polska team. Anna Rywczyńska, a “Safer Internet” project coordinator in Poland, presented the participants a project titled “Become a friend of your child".

On 22nd and 25th October, SECURE Hands-on workshops took place. Six workshops, including two led by CERT Polska experts, brought together 86 participants. The thematic scope of the meetings included detection of network attacks, threats to e-banking customers, and IT forensics.

Patronage of the conference was received from: PAP Nauka w Polsce (PAP Science & Scholarship in Poland), Gazeta Technologie, Niebezpiecznik.pl, eGospodarka, Bank, Business Security Magazine, IT Professional, IT w Administracji (IT in Public Administration), and the Zaufana Trzecia Strona portal.

The partners of SECURE 2012 conference were: Chartis Europe branch office in Poland, Dr. WEB, EmiTel, EURid, HP, Integrated Solutions, PaloAlto, RSA, Symantec, Systemics PAB, Qualis, Matic, Websense, CSIRT.SK and CESNET CERT.

5.2 NISHA

At the beginning of 2012, CERT Polska initiated the NISHA project (Network for Information Sharing and Alerting). The objective of Network for Information Sharing and Alerting (NISHA) is to increase the awareness of the on-line security by further developing the existing prototype of the information sharing and alert system, achieved under FISHA project in years 2009-2011. The expected outcome of the NISHA will be the pilot network consisting of 4 local portals that will operate in the framework of each institution taking part in the project, will exchange information on security and popularize it locally in national languages. Subsequently the network will be expanded with external portals interested in processing information to/from the NISHA network through their own websites.

Apart from exchanging information each node of the system aims at providing home users and staff of small and medium enterprises with information published in the NISHA network. 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. Simple mechanisms of sharing information in the system will allow national information websites, which are not members of the NISHA network, for easy access to information without requiring excessive technical effort from them. It is believed that the idea of involving information brokers allows narrowing the communication gap between Internet users and security professionals.

In 2013, as a part of national activities related to NISHA, we are going to look for partners among information brokers so that they can freely use the information in the portal and provide them to their customers.

NISHA project is co-financed by the European Commission under the program “Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks”. It is carried out by three partners: PTA/CERT-Hungary, NASK/CERT Polska, FCCN – Foundation for National Scientific Computing from Portugal and University of Gelsenkirchen/Institute for Internet Security.

The source code of the software created in the framework of the project will be available on the Public License of the European Union (EUPL)[6].

5.3 EISAS

To raise the awareness about cyber security among citizens and companies in the UE, the European Commission decided to promote the cooperation between the member countries that concerns the increase of the security awareness. In 2006 the European Commission initiated the creation of EISAS, the European Sharing and Alert System. It aims at strengthening the cooperation among the security institutions in order to effectively reach to users and employees of small and medium enterprises with important information about security. The NISHA project is the technical implementation of EISAS (see the section 5.2).

In 2012 the European Network and Information Security Agency (ENISA) launched the pilotage of EISAS that depended on creating interesting materials on security in several languages and afterwards distributing them by organizations in selected member countries. CERT Polska participated in preparing the materials for Polish users. Apart from CERT Polska, the project was supported by CERT teams from Germany, Norway, Hungary, Portugal and Spain by adjusting them to needs and specific character of each country, and by taking part in promoting them.

[6] *http://joinup.ec.europa.eu/system/files/PL/EUPL%20v.1.1%20-%20Licencja.pdf*

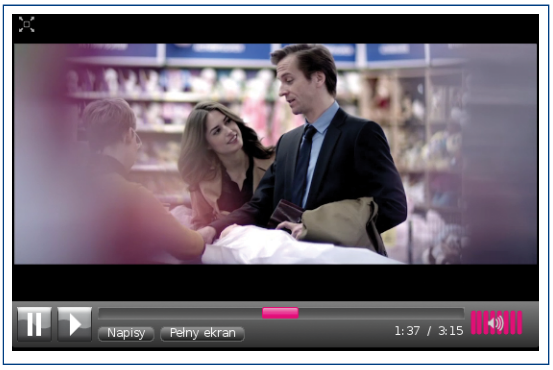


Figure 26. "Bluff City" film

The subject of the educational materials were issues related to the most critical threats which average Internet users could face: ID theft, social engineering and botnets. The handbooks written in everyday language were enriched by interactive test checking the susceptibility to ID theft and the film „Bluff City" about the dangers of social engineering. EISAS materials are available on our blog under **http://www.cert.pl/news/6193**.

The conducted pilot led to the conclusions that the public-private cooperation in getting good quality awareness materials is really important and also it is necessary to promote such information through local entities. The NISHA project was pointed to be the best solution supporting the information exchange.

5.4 ENISA report on honeypots

On 22 November 2012 the European Network and Information Security Agency (ENISA) published a report on the use of honeypots to detect network threats titled: „Proactive Detection of Security Incidents: Honeypots". The study was prepared by CERT Polska. It is the first such comprehensive study on this technology in terms of its usefulness for CERT teams and at the same time a first such detailed study on available free and open-source solutions. As opposed to previous academic research on honeypots we tried to take a very practical approach to evaluation of existing solutions such as honeypot.

Generally speaking, honeypot is a resource located in the network whose only task is to be attacked, compromised and tested or used in other unauthorized way. The resource can be of various types : a site, application, system or combination of all, as well as simply just a piec of information. The basic assumption is that anyone who tries to connect to or use of this resource is suspicious. The whole interaction between the honeypot and entity that connects to it is monitored and analyzed in order to detect and confirm malicious actions.

Honeypots can be used for many purposes, for example for monitoring botnet and worm activity in the network, collecting information about infected computers in the network, identifying new exploits and vulnerability in systems, detecting and collecting malware, gaining an understanding of hacker behavior, looking for internal infections in the network or internal attacks.

In our research we focused on evaluation and analysis of existing free honeypots. To achieve this goal we developed new evaluation criteria of honeypots, focusing on practical aspects of these solutions. We downloaded and tested 30 standalone honeypots, that is honeypots that you can install yourself in your home network. We distinguished many solutions: **Dionaea**, **Glastopf**, **Kippo** and **Honeyd** were identified as the most useful and easiest to install. For entities that can afford to use more resources to support their honeypot installations – in return gaining the ability to detect malicious web pages – there are Thug and Capture-HPC NG client honeypots.

Apart from defining the usefulness of particular stanalone honeypots we also identified online solutions and sandboxes. We examined early warning systems based on honeypots and we defined various strategies of the implementation. We pointed to weaknesses of honeypot technology and proposed many recommendations that can help with their wider application. Additionally, we presented possible directions of development. The report also contains a honepot training course.

In summary, the study found that honeypots are a very important tool for CERT teams. They offer an insight into network attacks, can be used to provide early warning on infections and malware behaviors, and are an excellent platform to find out about the changes in attackers tactics. They can also be use for creating larger sensors networks or as the additional source for implemented SIEM tools.

The full report is available under **http://www.enisa.europa.eu/activities/cert/support/proactive-detection-of-security-incidents-II-honeypots**. We hope that the report will contribute to the popularization and development of honeypot technology.

5.5 n6 – network security incident exchange

In February 2012, we launched the n6 project. n6 was designed and developed entirely at CERT Polska as a platform for acquisition, processing and exchange of information regarding Internet threatsCurrently, millions of security events are processed daily in an automated manner.

The goal is efficient, reliable and fast delivery of large volumes of network incident data to interested parties: network owners, administrators and Internet Service Providers. The project disseminates information gathered from various security systems operated by security organizations, software vendors, independent researchers, etc. Most of the data feeds are at updated at least once daily and often more frequently. An additional source of network incident data comes from daily operations of CERT Polska and its own systems.

The core element of n6 is its engine responsible for sorting and managing the flow of data. Sorting and delivering data to appropriate parties is made possible by a flexible tagging system, which defines categories of incoming data and serves to reroute traffic to the appropriate party. Original format of information is kept unchanged but all data regarding specific recipient is aggregated into one custom package.

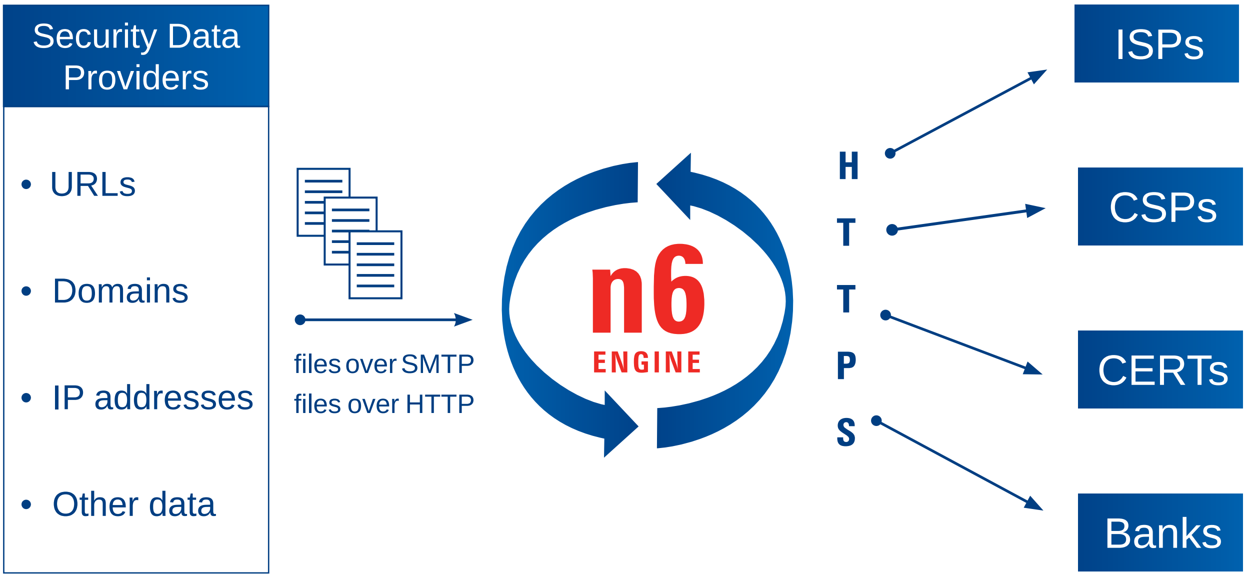


Figure 27. General overview of n6

Sample data feeds in the n6 platform

- malicious URL addresses
- malware and other artifacts
- infected hosts (bots)
- C&C servers
- scanning
- DDoS
- brute force attacks
- participation in a fast flux network
- phishing
- spam
- special data (as a result of CERT Polska activities)

The special source of information about a given network can be the results of operational activities of CERT Polska. These types of data published in 2012 covered lists of computers infected by Zeus P2P and Citadel. Special data can be also derived from the operational activities of other entities – such data received from the outside, with the consent of the source, can be added to the system for redistribution.

The platform exchanges information on the source of attacks in the form of URL addresses, domains, IP addresses or names of malicious software, and also information on special data. It should be noted that most of the data originates from external systems and may include false alarms. Data verification depends entirely on the receiving party.

Over 100 network owners, operators and administrators participate in n6 andreceive information on threats in their infrastructure on a daily basis. Every CERT, ISP and network owner who would like to receive information from the n6 platform concerning their network may contact CERT Polska at n6@cert.pl for instructions. Access to n6 is free and it does not require installing any sensors or software.

6. ARAKIS report

6.1 Introduction

The ARAKIS system (in Polish: AgRegacja, Analiza i Klasyfikacja Incydentów Sieciowych –Aggregation, Analysis and Classification of Network Incidents) is a project operated by CERT Polska. Its primary objective is to detect and describe network threats based on aggregation and correlation of data from multiple sources, including a distributed network of honeypots, darknets, 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 nonproduction 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 botnets.

ARAKIS-GOV is a project implemented under the overall ARAKIS system framework, and is used to protect the IT resources of the public administration. It has been implemented in over 75 various public administration institutions, in cooperation 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 fifth annual report from ARAKIS. The report includes statistics on threat sources, most scanned ports and services, and types of threats according as identified by Snort system rules. In addition, it includes analysis of an interesting anomaly in the BitTorrent network observed by the ARAKIS system. This year we did not prepare statistics of alarms generated by the system because their number does not reflect the threat level directly.

6.2 Observed threats

Port scanning is one of the most important categories of attacks detected by honeypots deployed in the ARAKIS system. Table 22 presents 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 top position is held by the 23/TCP port related to Telnet service. The second position belongs to the 445/TCP port which is used by a number of applications related to Microsoft Windows services, which contained numerous vulnerabilities efficiently taken advantage of by such worms as Sasser or Conficker. In comparison to the previous year these ports exchanged their positions and, for the first time since we published the statistics from the ARAKIS system, 445/TCP is not the dominating port.

Item	Number of unique IPs per year	Destination port/ protocol	Changes versus 2011	Description of attacks on port
1	69869	23/TCP	▲ 1	Telnet service attacks
2	54383	445/TCP	▼ 1	Buffer overflow attacks on Windows RPC
3	26661	3389/TCP	▲ 5	RDP (remote desktop) dictionary attacks – largely attributed to the activity of the Morto worm
4	25238	22/TCP	0	SSH server dictionary attacks
5	15050	139/TCP	0	Attacks on NetBIOS / files and printers sharing
6	14795	80/TCP	▲ 1	Attacks on Web applications
7	10729	1433/TCP	▼ 1	MS SQL attacks
8	9779	135/TCP	▼ 5	Windows DCE/RPC service attacks
9	6544	25/TCP	▲ 2	Scanning for open relay mail servers
10	6280	8080/TCP	▲ 1	Scanning for open web proxy server or attacks on web applications

Table 23. Most often attacked ports

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. In comparison to the last year, the first four positions of the ranking have not changed, only the number of unique IP addresses used for launching the attacks has increased. Much like in the previous year, almost all rules (except for one related to dictionary attacks on the SSH service) are related to attacks on Windows services. The one rule describing attacks on SSH ranked higher by four positions.

In the analysis of geographical locations of scanning sources the first position is held by China. This applies both to the number of unique IP addresses as well as the number of all the connections. In 2011 the largest number of unique scanning IP addresses was located in the United States, while China ranked as low as fourth. In 2012 it moved in front of other countries as the number of unique Chinese IP addresses the attacks originated from has almost tripled. At the same time the number of suspicious connections from China has also increased – in this case almost by a factor of two. Apart from China, we registered an increasing number of attacks originating in the following countries: the United States, the United Arab Emirates, Germany and India. On the other hand, the number of attacks coming from Poland, Ukraine and South Korea has decreased.

Item	Snort rule	Change versus 2011	Number of unique IP addresses
1	ET POLICY RDP connection request	0	174504
2	MISC MS Terminal server request	0	164714
3	ET POLICY Radmin Remote Control Session Setup Initiate	0	95174
4	ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND	0	32116
5	ET SCAN Potential SSH Scan	▲ 4	26838
6	ET POLICY Suspicious inbound to MSSQL port 1433	▲ 1	24122
7	NETBIOS SMB-DS IPC$ unicode share access	▲ 1	21144
8	ATTACK-RESPONSES Microsoft cmd.exe banner	▼ 3	20905
9	ET EXPLOIT MS04011 Lsasrv.dll RPC exploit (WinXP)	▲ 2	20031
10	ET EXPLOIT LSA exploit	0	20031

Table 24. Most often matched Snort rules

Item	Country	Change versus 2011	Number of the unique IP addresses
1	CN	▲ 4	33762
2	US	▼ 1	30840
3	TR	0	15101
4	RU	▼ 2	15094
5	AE	▲ 4	15094
6	TW	▲ 1	10423
7	DE	▲ 3	9007
8	IN	▲ 17	7521
9	UA	▼ 1	6883
10	KR	▼ 6	6133

Table 25. Top scanning countries by number of unique IP addresses

Item	Country	Change versus 2011	Number of connections
1	CN	0	4865733
2	US	0	3826534
3	RU	0	811973
4	DE	▲ 4	688854
5	KR	0	486521
6	TR	0	478638
7	UA	▼ 3	442061
8	TW	▲ 1	421963
9	GB	▲ 1	402343
10	FR	▲ 1	401807

Table 26. Top scanning countries by number of flows

The ranking of the most infected autonomous systems shows that the highest number of unique attacking IP addresses came from the network of a Chinese operator – Chinanet (AS4134). AS17908 (Tata Communications) made a debut in the top 10 by a jump of 412 positions as compared to last year.

Item	Change versus	Number of unique IP addresses	AS number	Country	Operator's name
1	▲ 5	17603	AS4134	CN	CHINANET-BACKBONE No.31,Jin-rong Street
2	▼ 1	11922	AS9121	TR	TTNET Turk Telekomunikasyon Anonim Sirketi
3	0	10682	AS5384	AE	EMIRATES-INTERNET Emirates Telecommunications Corporation
4	▲ 1	8121	AS3462	TW	HINET Data Communication Business Group
5	▲ 9	5552	AS4837	CN	CNCGROUP China169 Backbone
6	▲ 1	3080	AS6147	PE	Telefonica del Peru S.A.A.
7	▼ 3	3051	AS12741	PL	Netia SA
8	▼ 6	2738	AS4766	KR	KIXS-AS-KR Korea Telecom
9	0	2663	AS24863	EG	LINKdotNET-AS
10	▲ 412	2503	AS17908	IN	TCISL Tata Communications

Table 27. Top scanning autonomous systems by unique IP addresses

When comparing sheer numbers of connections rather than unique source IP addresses, Chinese operators occupy the top 3 positions. Overall, the top ten list of operators from which the largest number of suspicious connections originated contains five Chinese and two American operators.

Item	Change versus	Number of connections	AS number	Country	Operator's name
1	0	2040530	AS4134	CN	CHINANET-BACKBONE No.31,Jin-rong Street
2	0	875613	AS4837	CN	CHINA169-BACKBONE CNCGROUP China169 Backbone
3	▲ 2	401613	AS23650	CN	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone
4	▲ 36	397591	AS32475	US	SINGLEHOP-INC - SingleHop
5	▲ 3	327697	AS3462	TW	HINET Data Communication Business Group
6	▼ 3	292274	AS9121	TR	TTNET Turk Telekomunikasyon Anonim Sirketi
7	▲ 4	238063	AS4812	CN	CHINANET-SH-AP China Telecom (Group)
8	▲ 26	218162	AS4808	CN	CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network
9	0	202472	AS36351	US	SOFTLAYER - SoftLayer Technologies Inc.
10	▼ 4	184133	AS5384	AE	EMIRATES-INTERNET Emirates Telecommunications Corporation

Table 28. Top scanning autonomous systems by the number of flows

The table below shows the distribution of the infected IPs within Polish networks. In general, the number of unique IP addresses from Polish networks has decreased. The largest decrease in the number of the observed scans (almost by half) was noticed in the network of Netia (AS12741). Unfortunately, this operator still occupies the top position in the ranking with a considerable advantage over UPC, despite the fact that the number of unique IPs from the networks of the following three operators (UPC, TP and OVH) increased significantly.

Item	Change versus 2011	Number of unique IP addresses	AS number	Operator's name
1	0	3051	AS12741	Netia
2	▲ 19	1887	AS6830	UPC
3	▼ 1	1148	AS5617	TP
4	New	1142	AS16276	OVH
5	▼ 2	226	AS21021	Multimedia
6	0	68	AS29314	Vectra
7	New	52	AS56475	DATA-COM
8	▲ 5	51	AS25388	ASK-NET
9	New	50	AS43929	ASN
10	0	44	AS6714	GTS

Table 29. Scanning IP addresses from Polish networks

6.3 Selected network incidents observed by ARAKISNotable

Apart from the protection that the ARAKIS system has offered to the networks in which its sensors are installed, it has also contributed to observing interesting trends in Internet traffic. Below is a short description of what is, in our opinion, the most interesting observation in 2012 not directly related to protection of networks of the project participants. It concerned an anomaly observed in the BitTorrent network.

Anomaly in uTP traffic

In April 2012 we observed a significant increase of uTorrent (uTP protocol based) network activity on our honeypots. Some parts of recorded traffic triggered high-level alerts in ARAKIS, which could be information about possible infected nodes. Moreover, according to traffic data, two of the ARAKIS honeypot sensors were involved in a conversation, which is highly unlikely. This means that IP addresses in those packets were incorrect or spoofed.

6.3.1 What is uTP exactly?

The uTP protocol uses the UDP protocol for transportation and complements it with connection-oriented features. It encapsulates standard BitTorrent packets. This means, that regular BitTorrent traffic takes place inside a communication channel created in the uTP layer. This channel has some features typical to the TCP channels, including connection-orientation and congestion control. Standard BitTorrent packets rely on such TCP facilities as received data acknowledgements, regulation of window size, etc., in this case however these facilities are provided by uTP. Why do we need another protocol for that, when you can use TCP instead? UDP/uTP/BT stack is also responsible for bandwidth congestion control. When a user is downloading data from HTTP or FTP server, the download speed is limited on the server side. The distributed BitTorrent network does not have such limitations. That is why it often happens that when a user downloads a large amount of data, BitTorrent traffic consumes a large portion – or whole – of network bandwidth and effectively denies access to other networking applications. One possible solution is to apply built-in restrictions on the client side. However, these functions are not very sophisticated and users often tend to forget about them altogether. uTP on the other hand allows BitTorrent nodes to dynamically adjust bandwidth congestion at the protocol level and also provides some additional functions, like support clients using low bandwidth or sharing ADSL line with a web browser.

6.3.2 Our uTP observations (statistical)

According to our data the uTP activity (and, as an effect BT activity as well) has increased significantly in recent months – for example, when compared to the year 2011. We selected traffic samples from the 1st April 2011 and from the same day in 2012, from the same location. These are statistical parameters of the analyzed traffic:

	01-04-2011	01-04-2012
Number of all packets:	103,546 (8.7MB)	2,142,296 (201MB)
Number of UDP packets:	183 (~0.2% of traffic)	957,047 (~45% of traffic)
Anomaly:	393,862 (~18% of the whole traffic and ~41% of the UDP traffic)	

When creating this summary we made the following assumptions that the analyzed traffic (packets forming the traffic anomaly) is formed from packets matching characteristic of packets that triggered the ARAKIS alerts. This characteristic is as follows:

- The packet creating the anomaly is an uTP packet with DATA flag set.
- This packet encapsulates BT packet which contains the following data:
    - □ BitTorrent protocol hash: `057a315b89b54e53e2ee583dd5cd9ef60648805e`
    - □ BitTorrent protocol peer: `0000000000000000000000000000000000000000`

We can weaken these assumptions and agree that the uTP SYN packets with the same source and destination sockets as uTP DATA packets are also part of the anomaly. Then the summary of traffic from 1st April 2012 that can be attributed to the anomaly is as follows: **787,724 of packets (~37% of the whole traffic and ~82% of the UDP traffic**). To every packet of this kind our sensor replied with an ICMP message informing about a closed UDP socket. If we add these to our summary, it becomes even more noticeable**: 1,575,448 of packets (~73% of the whole traffic)**.

It is easy to observe that uTP and related traffic share of the whole is disproportionately large if compared to sample from 2011 that we selected for comparison. It is also a 23-fold overall increase of the whole traffic. We observed similar symptoms (high-level alerts, statistical disproportions in traffic) in various locations.

6.3.3 Packet analysis

Below we present a comparison of the TCP/BT and the UDP/uTP/BT stacks. We will examine data found in particular layers.

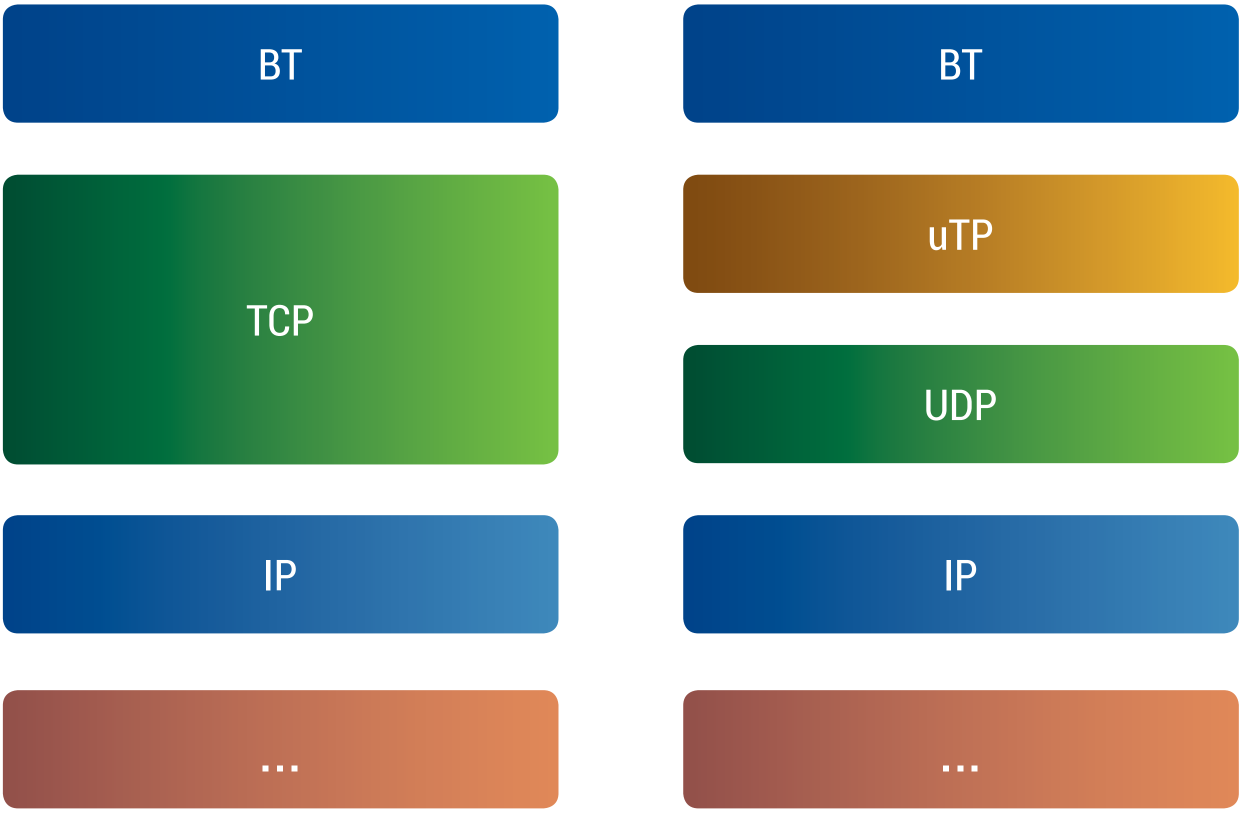


Figure 28: Comparison of the BT and uTP stacks

IP/UDP layer

Let us start with the IP/UDP layer. Below is a summary of source and destination addresses and ports of the analyzed transmissions (incoming uTP traffic)

Source hosts (Top 10):

Number	IP address
613	xxx.xxx.192.40
463	xxx.xxx.67.237
463	xxx.xxx.17.54
459	xxx.xxx.115.38
373	xxx.xxx.40.233
367	xxx.xxx.158.104
362	xxx.xxx.183.36
360	xxx.xxx.177.102
360	xxx.xxx.102.55
347	xxx.xxx.221.41

Destination hosts (all samples):

Number	Port
393850	xxx.xxx.xxx.34
4	xxx.xxx.xxx.27

Source ports (Top 10):

Number	Port
133014	45571
79677	62100
39658	60598
35461	55025
30830	47013
29605	45770
11555	36610
9697	57902
5996	20995
4989	32692

Destination ports (Top 10):

Number	Port
133007	45571
79672	62100
39657	60598
35461	55025
30829	47013
29604	45770
11554	36610
9697	57902
5996	20995
4989	32692

Source addresses have a rather uniform distribution if we omit some addresses from the top of the list. These addresses originate from various autonomous systems from different geographic locations (including: Russia, Canada, China, Australia, and USA). This distribution has characteristic of a sum of a uniform and a certain non-uniform distribution. It might mean that part of these addresses are used in a uniform way (e.g. in turns) or that they are randomly chosen (forged).

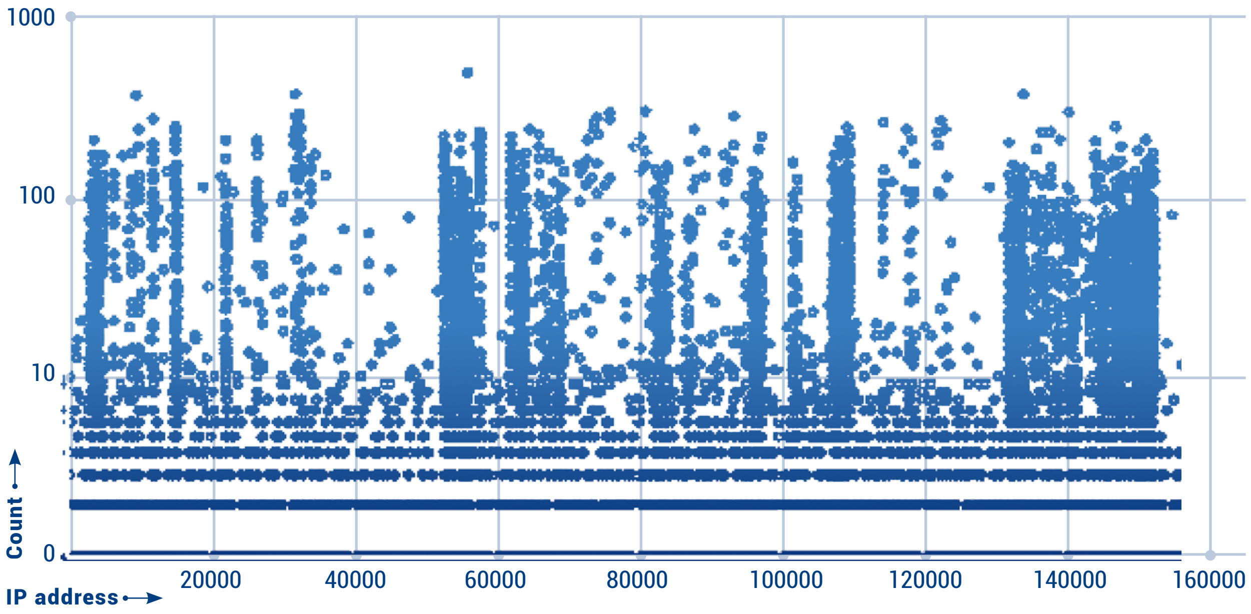


Figure 29 : Distribution of the source IP addresses

High geographical differentiation makes the second explanation rather more convincing. Possibly some kind of distributed anonymising network is being employed. Randomly chosen addresses fail a test for the TOR nodes, however, there are other possibilities like: other anonymising networks, VPN services, botnets.

When it comes to source and destination ports, we observe that high ports are preferred. Similar ports are chosen as source and destination of transmission.

uTP layer

Incoming traffic forming the anomaly can be viewed as series of flows originating from various sources, consisting of two uTP packets: uTP SYN and uTP DATA. These packets are parts of the uTP handshake mechanism used to set up an uTP session. However, parts of them do not follow the protocol. These are:

- **Transmission source ignores ICMP messages informing about closed port.**
  There is no explicit proper reaction to ICMP in the uTP specification. But this kind of message should be interpreted as information for the client that the connection it's trying to make is impossible.
- **Transmission source ignores the lack of uTP STATE packet and sends a DATA packet.**
  Without the STATE packet, there is no proper acknowledgement number and it is not possible to create a proper connection. Instead of a correct acknowledgement number the number 0 is placed, thus violating the protocol. During our research we were sending packets with similar construction to uTorrent client and it responded with FIN packet, that is, it terminated the connection. We suspect this is an effect of not following the protocol.

Other interesting or otherwise unusual properties of uTP packets:

- Most of the packets have value 0 in timestamp difference field:

Values of timestamp difference microseconds (Top 10):

Number of occurrences	Hex value
392850	00 00 00 00
10	6f 63 6f 6c
4	fd 7a 9f f1
4	Fb 26 16 d3
4	fa 5b c0 83
4	f9 e9 d8 6d
4	f9 46 4a 14
4	f9 37 8d f9
4	f8 3c a3 1a
4	f6 9a ec df

- Transmission source ignores the lack of uTP STATE packet and sends a DATA packet.

Value of window size (Top 10):

Number of occurrences	Hex value
393017	00 38 00 00
738	00 04 00 00
50	00 00 00 00
46	00 03 20 00
4	00 03 99 99
4	00 03 33 33
4	00 00 13 02
3	00 01 93 7c
3	00 00 0e 32
2	00 02 1d fd

Values of timestamp field in two consecutive packets in each flow differ by multiple of 10,000 microseconds.

Some of these properties can result from different protocol implementations, but other make the use of this protocol pointless. It is very unlikely that with such high time resolution these values are legitimate. If these values are forged, the protocol loses its congestion control features and using it for transportation makes no sense.

BitTorrent layer

Encapsulated BT packets contain hash value of `057a315b89b54e53e2ee583dd5cd9ef60648805e`. This hash corresponds to information about files containing a film "Avgust. Vosmogo". This is a Russian action movie, which had its premiere on the 21st February 2012. During analysis of traffic to other locations we registered similar packets (in UDP/uTP/BT stack) containing hashes corresponding to information about files containing this film and files containing other Russian film: "Shpion" (more on hash field in BT packets: http://wiki.theory.org/BitTorrentSpecification#Tracker_Request_Parameters).

Below we present some interesting time correlations between torrent publication and registered transmissions containing the corresponding hashes:

Hash	Date of torrent publication	Date of registered transmissions
c11ba392ef3dd57942112641ce8f1d9b96f0ddd5	26.02.2012	17.03.2012
057a315b89b54e53e2ee583dd5cd9ef60648805e	17.03.2012	01.04.2012

In analysed traffic of the 1st April 2012 99.99% of uTP DATA packets contained hash `057a315b89b54e53e2ee583dd5cd9ef60648805e`.

These packets also contained BT peer IDs (more on peer ID field in BT: http://wiki.theory.org/BitTorrentSpecification#peer_id).

Values of the peer IDs field (Top 10):

Number	Peer ID
329755	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
399	2d54 5232 3432 302d xxxx xxxx xxxx xxxx xxxx xxxx
214	2d54 5232 3530 302d xxxx xxxx xxxx xxxx xxxx xxxx
213	2d54 5232 3432 302d xxxx xxxx xxxx xxxx xxxx xxxx
100	2d55 5432 3231 302d xxxx xxxx xxxx xxxx xxxx xxxx
97	2d55 5431 3737 302d xxxx xxxx xxxx xxxx xxxx xxxx
95	2d54 5231 3933 302d xxxx xxxx xxxx xxxx xxxx xxxx
93	2d54 5231 3933 302d xxxx xxxx xxxx xxxx xxxx xxxx
91	2d55 5433 3132 302d xxxx xxxx xxxx xxxx xxxx xxxx
90	2d4d 4732 3125 302d xxxx xxxx xxxx xxxx xxxx xxxx

As you can see, most of the packets contained only zeroes.

Avgust. Vosmogo

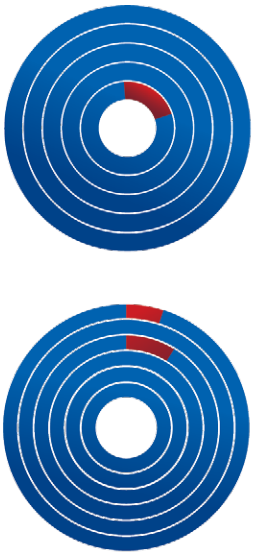


Figure 30: statistics of seeders and leechers per tracker for torrent with hash c11ba392ef3dd57942112641ce8f1d9b96f0ddd5

Avgust. Vosmogo

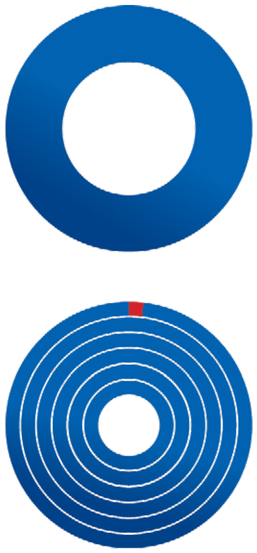


Figure 31: statistics of seeders and leechers per tracker for torrent with hash ab53cb0d665b34fcdf1939b271660b48297b5a74

Lost

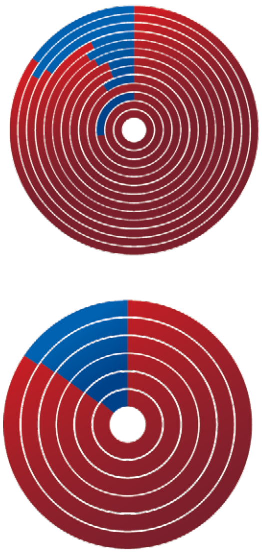


Figure 32: statistics of seeders and leechers per tracker for torrent with hash 799db5ad3c746823a8df170bb1a717835c1dccc8

Naruto

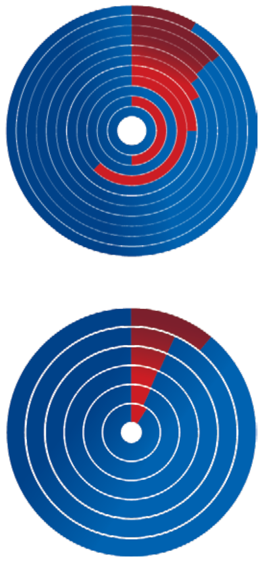


Figure 33: statistics of seeders and leechers per tracker for torrent with hash 057a315b89b54e53e2ee583dd5cd9ef60648805e

● seeders ● leechers

Below we present the statistics on the distribution of leechers and seeders relating to discussed torrents gained from torrent trackers (among other torrentproject.com, torrenttz.eu and bitsnoop.com).

It is clear to see that leecher counts are very low. For comparison, we present information about other torrents, very popular (relating to Lost series) and less popular as well (Naruto, Nocznoj Dozor) where the same torrents were used.

When examining analyzed torrents data we can usually see a large number of so called seeders and very small amount of leechers (usually – 0). It's a rather uncommon distribution. In most of other cases these proportions are much fuzzier (if not reversed).

6.3. Hypotheses

Our analysis of traffic forming the anomaly in our honeynet did not clearly determine its source and purpose. However, we were able to construct several hypotheses on this traffic.

Sources of anomaly

We identified five potential sources of anomaly.

- **Addresses are forged.**

This possibility is confirmed by a uniform characteristic of a component of address distribution and – above all – source addresses belonging to our honeynet nodes, which do not initiate transmissions.

- **Source addresses are legitimate.**

During detailed analysis we discovered a connection-oriented TCP session transporting BT packets that partially match anomaly characteristic (they contain the same hash value). Creating a TCP session using forged source IP addresses is possible, but very difficult and virtually impossible in the WAN networks, that is why we suspect that source address of this transmission is legitimate. It is also very unlikely (mainly due to time correlations), that this session is completely unrelated to anomaly. It contained a similar BT packet (the same hash value) but it also contained non-zero peer value. It is possible that node using this address is a common uTP or BT client.

- **Source addresses set contains forged addresses alongside legitimate ones.**

This is the most likely hypothesis.

- **Source and destination ports are standard ports for the uTP conversations.**

According to our observations during tests with uTorrent this client listens to connections on port 12144 by default. This port can be changed by user or randomly chosen. It is possible that a set of ports was created on the basis of information from public trackers.

- **Source of transmission is not a legitimate uTP client but other program or script whose purpose is different from data sharing.**

Properties of the uTP packets indicate this – round differences between timestamps, breaking the protocol, ignoring ICMP messages. Also choosing destination addresses from ARAKIS honeynet supports this hypothesis.

Anomaly aims

The most likely aims of observed anomaly include the following:

The purpose is uTP/BT network poisoning

According to data collected from open trackers, seeders to leechers ratio of torrents containing hash `057a315b89b54e53e2ee583dd5cd9ef60648805e` and other hashes corresponding to film "Avgust. Vosmogo" is uncommon and can be a result of poisoning uTP/BT network elements (e.g. by distributing forged data about peers – series of zeroes).

The purpose is uTP/BT network mapping

It is possible that these transmissions are used to create some kind of mapping of uTP/BT network nodes. A mapping program or a script would classify tested node as an uTP client based on its responses:

- Correct uTP response – node is an uTP client
- Incorrect uTP response – node is not an uTP client

But some facts render this hypothesis unlikely: Despite the ICMP Port unreachable message, the source sends another packet, although the classification can be made on the basis of the first response. Some packets contain forged source address, which makes receiving an answer and classification virtually impossible.

Transmissions constitute an attack on IT systems

It is possible that packets we're observing are capable of introducing the corruption conditions in some applications – they are exploits. The results of superficial research on uTorrent vulnerabilities, however, do not support this hypothesis, but we have not got enough knowledge on other client or unpublished vulnerabilities to reject it completely. It is possible that some properties of the uTP packets (e.g. zeroes in ack_nr fields) or the BT packets (e.g. series of zeroes in peer ID field) could lead to create corruption conditions in some applications.

Anomaly by its nature (large share in daily network traffic) produces visible a disruption in IT systems and large amount of our false-positive high-level alerts is a good proof. In terms of the Polish law, the European Convention on Cybercrime and U.S. Codes (and probably many other sources of domestic law) the legality of process producing the anomaly may be questionable.

Observed traffic is – at least partially – an echo

It is possible that part of the recorded packets is an echo of the remote network events (incidents) that appeared in other networks.

Anomaly meaning

These are the most likely meanings of the observed anomaly:

Network poisoning/mapping

Data collected from public trackers supports this hypothesis. Without delving into details of the torrent client reactions it is clear to see that trackers register small amount of peers downloading analyzed resources. It is possible that it is an effect of a process which we are currently unable to understand fully and which produce the anomaly. There is one group that would benefit from the uTP poisoning: multimedia companies and their subcontractors. Conducting this kind of campaign by these institutions wouldn't be the precedent.

It is also possible that generated traffic is used for the BitTorrent network mapping and data gathering for later use in other projects.

- **Broken implementation/ experiment**

Failure in following the uTP protocol could be an effect of errors in the uTP protocol implementation in less popular or immature BitTorrent client. It is also possible that this anomaly is an effect of some kind of network experiment.

- **Camouflaging traffic**

Assuming that incoming traffic consists of legitimate and forged source addresses we consider the possibility that the part of the traffic has a specific reason and purpose while other part of it makes up camouflaging traffic. Traffic containing legitimate addresses and acknowledgement numbers (not terminating the session), despite its small share, could be effective in poisoning or mapping the uTP network.

- **Echo from attacks on other networks**

It is possible that parts of traffic we're observing in our honeynets is an echo from attacks conducted in other networks. Parts of traffic that support this hypothesis are: packets with uTP STATE flags set (equivalent of TCP SYN/ACK flags in DDoS echoes) and connection-oriented transmissions with seemingly legitimate peer IDs.

6.3.5 Summary

During our analysis of discussed traffic we have not reached a clear conclusion on its source or purpose. The registered packets are so complex that you can make reasonable assumption that they are crafted. The only doubt is whether their form and amount are the result of the intentional action (for example poisoning network) or a bug in the software.

Kontakt

Incident reporting:	cert@cert.pl
Spam reporting:	spam@cert.pl
Information:	info@cert.pl
PGP key:	http://www.trusted-introducer.nl/teams/0x553FEB09.asc
Website:	http://www.cert.pl/
	http://facebook.com/CERT.Polska
RSS Feed:	http://www.cert.pl/rss
Twitter:	@CERT_Polska
	@CERT_Polska_en
Address:	NASK / CERT Polska ul. Wąwozowa 18 02-796 Warszawa Poland
Phone::	+48 22 3808 274
Fax:	+48 22 3808 399