NASK

CERT POLSKA

Technical Report

An Analysis of Domain Silver, Inc. .pl Domains

Updated with sinkhole statistics

August 23, 2013

Contents

bit.ly link shortener usage

Some of the links in this report where shortened using `bit.ly` service in order to improve readability. If you want to see the whole address just add plus sign (+) at the end of the shortened link and you will be presented with the website that provides some information about the shortened url.

1 Introduction

This document gives an overview of domains registered through Domain Silver, Inc, a Seychelles-based registrar operating in the .pl domain. This Registrar started operating in May 2012. Since that time, the CERT Polska team started to observe a large increase in the amount of malicious domains registered in .pl and to receive many complaints concerning domains registered through Domain Silver. In May 2013, dozens of domains used for botnet C&C purpose were seized and sinkholed by NASK and CERT Polska. Most of the malicious domains present in the `.pl` were registered through Domain Silver. Following further unsuccessful attempts to remedy the situation, NASK (the .pl ccTLD registry) decided to terminate its agreement with the Registrar. In the following sections of the document we explain what the malicious domains registered were used for (as of 9th July 2013), what botnets used the domains and why they posed a threat to the Internet community.

Most important findings:

- Out of all the registered 641 domains (status as of 9th July 2013 plus previously sinkholed domains), only one active domain was benign (`domainsilver.pl` itself).
- 404 domains were malicious, with 179 being used for C&C purposes.
- The domains were used to manage and distribute botnets such as Citadel, Dorkbot, ZeuS Ice IX, Andromeda, RunForestRun and ransomware.
- We identified at least 16 instances of the above botnets.
- 179 domains were used to either sell pharmaceuticals or to recruit money mules and they were advertised using spam campaigns performed by botnets.

Currently all the changes to the domains registered through Domain Silver, Inc. are prohibited and no new domains may be added by this registrar. These domains have registrar is set to `vinask`. They will be systematically sinkholed by CERT Polska.

2 Registry, registrar and registrant

Due to the names similarity, the following three terms, connected with domain management, are often confused: *registry*, *registrar* and *registrant*. A domain name *registrant* is the person or organization that want to register a domain name. The relationship between a registry and registrar is more complex and described below.

A *Domain name registry* is a database containing all domain names registered in one top-level domain (e.g. `.pl`) and links it to their delegated name servers and registrants. Domain name registry can be created on different levels of the domain system (DNS) hierarchy. IANA (*Internet Assigned Numbers Authority*) is the operator of the highest level of DNS hierarchy (called *root-level*) and it delegates next level (called *top-level*) registers to specific organizations. The role of the Domain Name Registry (also called *NIC – Network Information Centre*) is to maintain the technical infrastructure of the registry, create domain registration policies and, most importantly, to keep the registry up to date. Research and Academic Computer Network (*NASK* in short) is the Domain Name Registry for the `.pl` domain.

Managing the domain name registration is within the duties of the domain name registrar. It is an organization or company that works closely with the domain name registry and has a direct access to editing and creating entries in the Domain Name Registry database. A registrar has a specific set of permissions that allows him to query the Registry database and manage domain names belonging to his clients. The Registry can also be a registrar, but this is not always the case. Often this role is granted to the other companies that are required to follow domain registry policy set up by the Registrar. In Poland, NASK has over 190 partners that are registrars. Some of them are foreign companies. A registrant can select any registrar among those partners. The registrant can also change the registrar for his domain name.

2.1 Rogue registrar

Registrars have a vast number of permissions that allow them to register new domain names, delegate their name servers, control the registrant contact information. This can of course be abused. Registrars can easily register a pool of domain names used to spread spam, phishing or manage a botnet. These domains can have unverified or even in some cases faked registrants data. If any abuse is discovered on a specific domain name, the registrar is usually the first point of contact. This allows him to drag the process of shutting down the domain name as long as it is required to move the malicious software to the other location. To the outside observer this can give the impression of inefficient domain name management. However, if this state persist for the long time, and most of the registered domain names are abused, this can lead to the conclusion that this registrar knowingly abuses the Registry database in order to perform malicious actions. Such a registrar is called a *rogue registrar* and in the most extreme cases this can be a company set up for the sole purpose to make the Domain Name Registry database more accessible to the cybercriminals.

2.2 Domain Silver

Domain Silver bacame a registrar in May 2012. Company lists the following contact information in the whois queries:

```
Domain Silver Inc.
1st Floor, Sham-Peng-Tong
Plaza Building, Victoria, Mahe
Seychelles
e-mail: support@domainsilver.pl
tel.: +1.3236524343
```

In the second half of 2012 CERT Polska received complains about domains registered through Domain Silver. These domains were used to host malware C&C or as a landing pages in the botnet spam campaigns. Overall, Domain Silver registered 2926 domains, as of 29 of July, 2013.

3 Domain names distribution

Table 1 below gives an overview of the classification of all abusive domains that had Domain Silver as their registrar and had registered status on 9th of July, 2013 including the domains that we previously sinkholed. Overall, 641 `.pl` domains had a registered status on the aforementioned date, abusive or not.

Content type	Number of domains	Share
C&C Servers[1]	179	27.9%
Pharma, recruiting money mules or spam[2]	179	27.9%
Malware[3]	20	3.1%
Blacklisted domains[4]	17	2.7%
Inappropriate Child-related images (Child Erotica)	5	0.8%

Table 1: Abusive domains distribution

63% (404 domain names) from all of the domains were classified as abusive. From all the other domains only one (namely `domainsilver.pl`) contained benign content. We were not able to find any content on other domains (or they simply did not resolve). Interestingly, 150 of these (inactive) domains were registered on the same day – 18th of March, 2013 during a 15 minute span.

Apart from these domains, we were also able to identify an additional 35 domains used for C&C (botnet Command and Control) purposes in the past and 19 domains used in spam

[1]Including name servers that contained NS records for this C&C servers.
[2]Including name servers that contained NS records for this servers.
[3]Including name servers that contained NS records for this servers.
[4]Excluding domains classified as having other content types.

campaigns for pharma products. Between 6th and 10th of July 2013 597 domains were registered through Domain Silver using a feature called *Domain Name Tasting*. This allows registrants to test the domain name for 14 days. All of these domains were than used to promote "miracle weight loss pills" using spam sent out by botnets.

4 Botnets

Below we present a short description of the botnet families that were found on the previously mentioned domains. Domains that had Domain Silver as a registrar were utilized in at least 16 different botnet instances.

4.1 Citadel

Citadel is a malware, which is distributed as a *crimeware kit* – a set of applications used by criminals to create their own botnet. Citadel is an evolution of another bot code – Zeus, which leaked in 2011. Citadel primarily targets financial institutions and uses social engineering techniques. To achieve this is utilizes a *man-in-the-browser* attack. Figure 1 present a scheme for this type of attack.

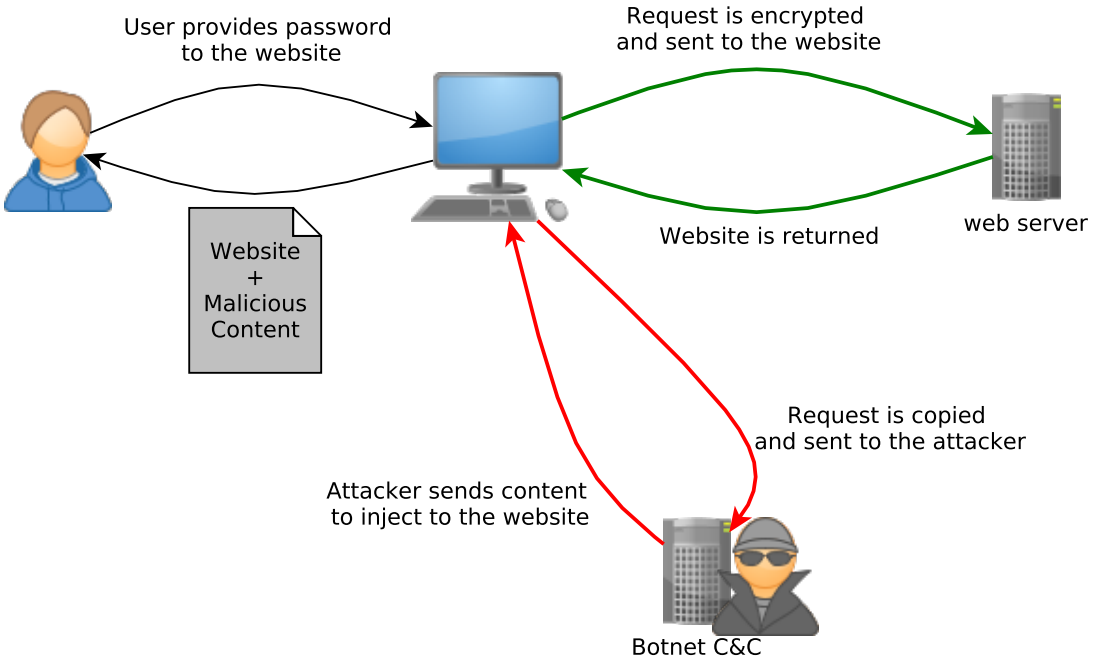

Figure 1: *man in the browser* attack

More information about the Citadel botnet can be found in our `plitfi` botnet takedown report: `http://www.cert.pl/news/6900`. This is one of the instances that was using domains registered through Domain Silver.

4.2 Dorkbot (NgrBot)

Dorkbot is a very versatile malware. It installs a user space rootkit in order to hide both the program file on the disk and its activity on the process list. Some of its most notable features are:

- infection of the USB drives,
- downloading and running an application from the specified URL address,
- stealing login data from social, hosting and other websites,
- spreading through Skype, MSN, Facebook or other social media,
- performing *flood* or *slowloris* attacks.

More information about the Dorkbot malware and its botnet instance, which utilized domains registered in Domain Silver can be found on our blog: `http://www.cert.pl/news/6434`.

4.3 Zeus Ice IX

Another strain of Zeus malware is Ice IX. It is roughly the same as Zeus, with some minor enhancements. It does the same man-in-the-middle attack as the one described previously

More information about this malware can be found on the RSA blog: `http://bit.ly/11WI8u7`.

4.4 Andromeda (Gamarue)

Andromeda is a modular bot designed as such to make it easier to extend its capabilities easily. Sales system for this botnet is based on selling plugins to the core software. These plugins include the following functionality:

- downloading and running additional software,
- stealing login data to some websites,
- creating a proxy out of the infected machine.

This bot also implements a large amount of techniques designed to detect the virtualization software (e.g. VirtualBox or VMWare) or debugger. This botnet was spread by e-mail messages suggesting that the attached PDF file was an e-ticket for the flight that user supposedly requested. It also used a popular *exploit kit*, i.e. a set of exploits using browser plugins or browser vulnerabilities to infect the computer.

More information about the malware and one of the spam campaigns that used domains registreed through Domain Silver can be found on Trend Micro blog entry: `http://bit.ly/SW2dr3`.

4.5 RunForestRun

RunForestRun is a malicious software that targeted Web servers. Every HTML file on this server had a malicious JavaScript appended. This JavaScript created an *iframe* that lead to the malicious code (most probably *exploit kit*). This software also included a Domain Generation Algorithm (DGA in short), which is rather unusual for Web server malware. In one of the versions, malware generated domain names couple of times a day, all in the `.waw.pl` domain. Of course, as with every DGA Algorithm, blocking the domain with which malware communicates is not effective. Couple hours later malware will generate a new domain and will regain connectivity to the C&C.

More information about this malware and the DGA that created domains that were registered through Domain Silver can be found in the Unmask Parasites blog: `http://bit.ly/OLynll`.

4.6 Ransomware

We were able to find additional 16 domains, registered after 9th of July 2013, that were hosting C&C server for the ransomware. This kind of malware uses social engineering to blackmail victims into paying ransom.

Figure 2: Polish version of the ransom website

This particular software connected to domains registered through Domain Silver and

download a DLL file, which contained a website. This website contained information that a user violated the law and is required 500 PLN (∼ $ 150) fine. The website was also localized so that user would see a message in his language, which made it look more trustworthy. Picture 2 presents a Polish version of tis website.

More information about this type of malware can be found on our blog: `http://www.cert.pl/news/5483`.

5 C&C proxy infrastructure

Some of the mentioned botnets used a proxy infrastructure to protect the real C&C location. Servers used as a proxy were most probably obtained in some attack (i.e. hacked into).

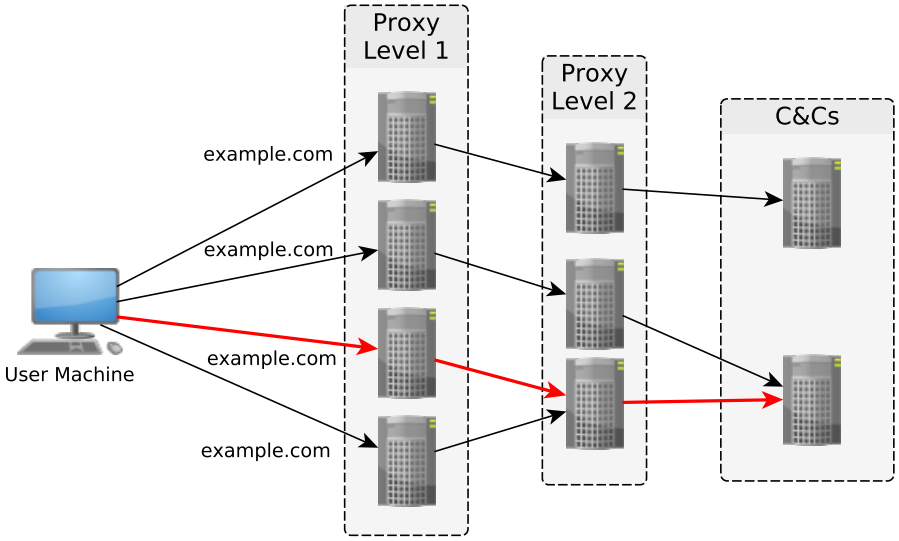

Figure 3: C&C proxy architecture

When the infected machines tries to connect with a configured domain (e.g. `example.com`) it has to choose one of the IP addresses this domain resolves to. Usually it chooses the first IP that appears on the list. This address is then used both to send gathered data and to fetch the configuration information. This address is one of the Proxy Level 1 machines depicted on the figure 3. This server directly communicates with the infected computer.

Proper software installed on every of the level 1 proxies takes care of the traffic redirection to one of the level 2 proxies. Then, using the same method, traffic is transferred to the real C&C server.

6 What will happen to the domains?

On 30th of July, 2013 NASK decided to terminate its agreement with Domain Silver, Inc. All of the domains registered through Domain Silver are currently in the de facto frozen state.

This means that all changes to the Registry regarding these domains are prohibited. These domains currently have `vinask` as their Registrar. They will be systematically sinkholed by CERT Polska.

7 Statistics

This section consists of an analysis of sinkhole data collected as a result of the above described actions. It concerns data gathered on the 23rd of July 2013.

On that day 101,831 unique IP addresses from 191 countries and 4,414 autonomous systems made connections to the sinkhole server. Statistics also include `plitfi` botnet which was described in our previous report and its C&C domains were registered through Domain Silver.

Name	Type	Domains	Number of IPs	Percentage
wrela[5]	ZeuS ICE IX	3	37,772	37.09%
spros[5]	ZeuS ICE IX	4	17,226	16.91%
MIX2	Citadel 1.3.5.1	9	10,202	10.01%
—	Andromeda	3	10,035	9.85%
imj/imr	Citadel 1.3.5.1	4	9,572	9.40%
D34	Citadel 1.3.5.1	5	8,125	7.98%
—	Dorkbot	3	7,335	7.20%
plitfi	Citadel 1.3.5.1	2	6,495	6.38%
h9/h14	Citadel 1.3.5.1	5	6,006	5.90%
rustin[5]	ZeuS ICE IX	2	3,907	3.84%
dasay[5]	ZeuS ICE IX	2	3,480	3.42%
mantuma[5]	ZeuS ICE IX	2	2,285	2.24%
ewq	Citadel 1.3.5.1	8	1,253	1.23%
stilos[5]	ZeuS ICE IX	2	1,173	1.15%
pinano[5]	ZeuS ICE IX	5	990	0.97%
CIT_{58}	Citadel 1.3.5.1	5	717	0.70%
gr10	Citadel 1.3.5.1	7	638	0.63%
yds/dsg	Citadel 1.3.5.1	3	481	0.47%
a1	Citadel 1.3.5.1	5	141	0.14%
CIT_{29}	Citadel 1.3.5.1	1	48	0.05%

Table 2: Botnets which were using domains registered through Domain Silver

Table 2 presents all botnets that were using Domain Silver as theirs C&C domain registrar and were sinkholed by CERT Polska on 23 of July, 2013. Some of the botnets were named based on the domains that they were using, while for others we used original names, i.e. same ones that were used by cybercriminals.

[5]Botnet name was created based on the C&C domain name.

Botnet owners often change the botnet name. In those cases we presented both names separates with a slash. Dorkbot and Andromeda are special cases – they do not have a name, because only one instance of these botnets was present.

Number of domains in the table 2 is the number of active domains i.e. domains with at least one connection. There may be other domains on which this botnet was present, but they were put in the bot configuration as a backup domain. Bots will try to connect with this backup domain only if primary one is not responding.

Country	Number of IP addresses	Percentage
Germany	20,231	19.86%
Poland	8,344	8.19%
France	5,152	5.05%
Australia	5,041	4.95%
Turkey	4,277	4.20%
Indonesia	4,043	3.97%
Saudi Arabia	3,890	3.82%
The Netherlands	3,867	3.79%
Italy	3,214	3.15%
Japan	3,183	3.12%

Table 3: 10 most common countries

Table 3 shows top 10 countries of origin for sinkhole connections. One third of all connections came from three countries: Germany, Poland or France. One fifth of the connections came from Germany. Maps 5 and 6 present a geographical distribution of IP addresses which connected to sinkhole.

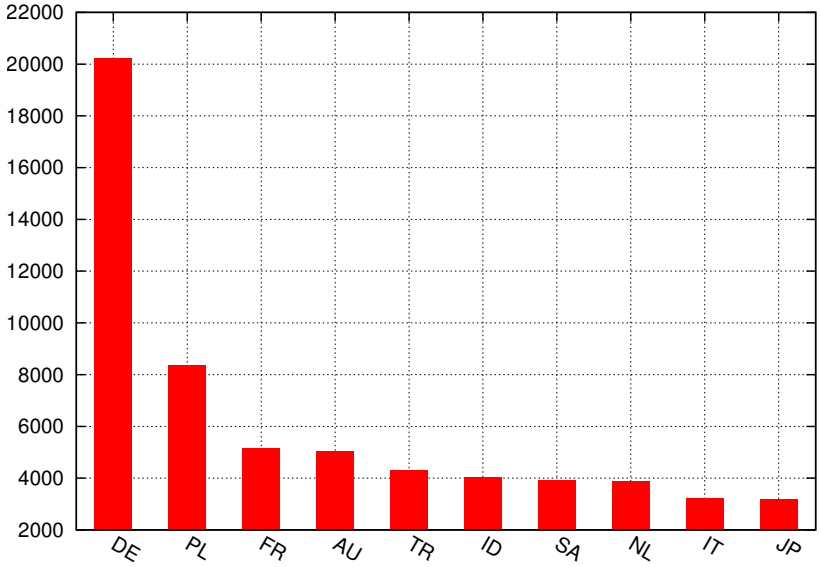

Figure 4: Top 10 countries of origin

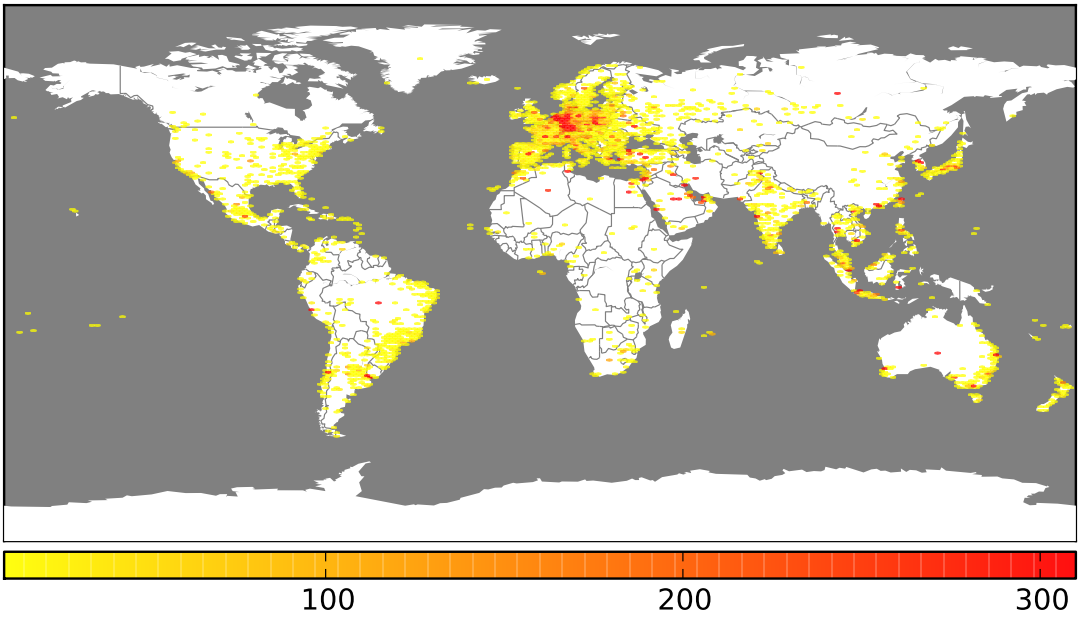

Figure 5: IP addresses geographical distribution

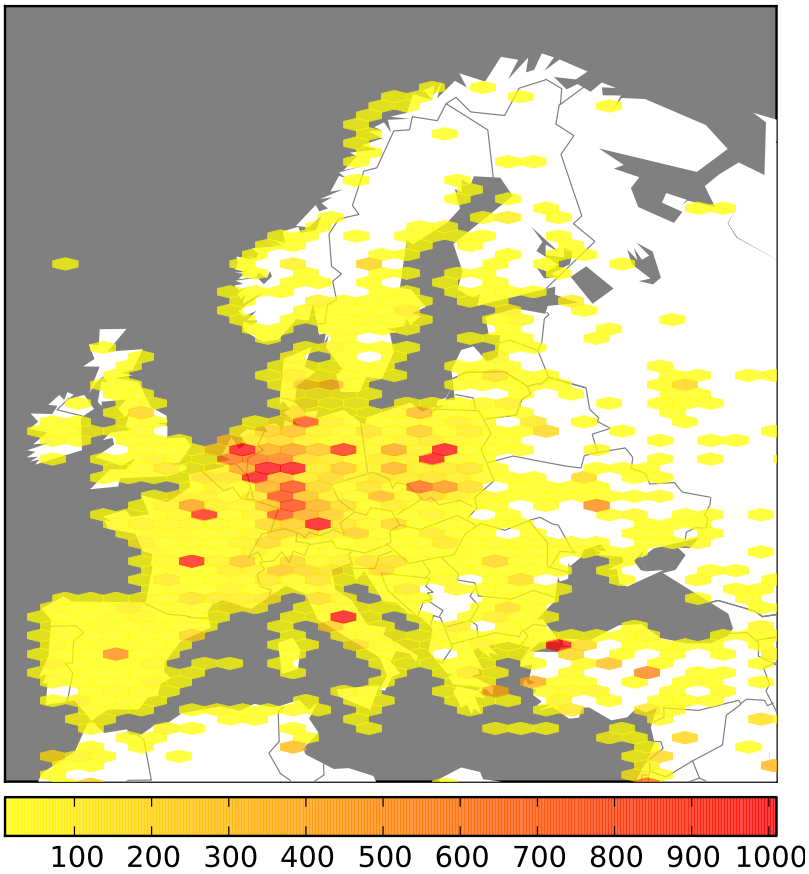

Figure 6: IP addresses geographical distribution in Europe

AS Name	AS Number	IP addresses	Percentage
Deutsche Telekom AG	AS3320	8,780	8.62%
Vodafone D2 GmbH	AS3209	3,326	3.26%
Turk Telekomunikasyon Anonim Sirketi	AS9121	3,001	2.94%
Telekomunikacja Polska S.A.	AS5617	2,849	2.79%
Autonomus System Number for SaudiNet	AS25019	2,414	2.37%
Telstra Pty Ltd	AS1221	2,146	2.10%
France Telecom S.A.	AS3215	2,017	1.98%
PT Telekomunikasi Indonesia	AS17974	1,852	1.81%
Unitymedia NRW GmbH	AS20825	1,590	1.56%
Telecom Italia S.p.a.	AS3269	1,370	1.34%

Table 4: Top 10 autonomous systems

Table 4 presents top 10 autonomous systems (*AS* for short) from which the connections originated. This data is consistent with previously presented geographical distribution of connections. Table 5 narrows down the statistics to top 5 Polish autonomous systems. Percentage in the second table refers to all of the Polish connections. Almost 2/3 of all connections originating from Poland came from these 5 autonomous systems.

AS Name	AS Number	IP addresses	Percentage
Telekomunikacja Polska S.A.	AS5617	2,849	34.14%
Netia SA	AS12741	892	10.69%
Polska Telefonia Cyfrowa S.A.	AS12912	711	8.52%
P4 Sp. z o.o.	AS39603	468	5.61%
Polkomtel Sp. z o.o.	AS8374	440	5.27%

Table 5: Top 5 Polish autonomous systems

Table 6 contains a list of all botnets and specifies, for every one of them, top 3 countries from which the connections originated. The botnets are presented in order which reflects their size, i.e. the same order as in table 2. In case of small botnets the real geographic coverage may have been distorted because of the monitoring systems. The botnets which have a really low connection count, usually are just abandoned and as such most of their victims are in fact controlled by researchers in order to monitor botnet activity.

Botnets h9/h14, plitfi and imj/imr were not geographically diverse, which can mean that the cybercriminals only targeted victims in the specific countries. On the other hand, spros, Andromeda or rustin botnets were almost uniformly distributed across the globe. In these cases cybercriminals did not seem to care about the geographical profiling, opting for as many machines possible instead.

Name	Country	IP addresses	Percentage
wrela	Turkey	3,464	9.17%
	Poland	2,932	7.76%
	The Netherlands	2,572	6.80%
spros	Indonesia	1,523	8.84%
	Poland	1,358	7.88%
	Italy	1,188	6.89%
MIX2	Saudi Arabia	3,602	35.30%
	Australia	2,215	21.71%
	United Arab Emirates	846	8.29%
Andromeda	Turkey	1,595	15.89%
	Germany	988	9.84%
	Italy	754	7.51%
imj/imr	Germany	5,357	55.96%
	France	2,026	21.16%
	Mexico	336	3.51%
D34	Germany	5,391	66.35%
	France	2,359	29.03%
	United States	82	1.00%
Dorkbot	Brazil	1,470	20.04%
	Russia	857	11.68%
	Indonesia	755	10.29%
plitfi	Poland	4,006	61.67%
	Japan	1,240	19.09%
	Sweden	417	6.42%
h9/hl4	Germany	5,549	92.39%
	Brazil	231	3.84%
	United States	40	0.66%
rustin	Japan	380	9.72%
	Indonesia	371	9.49%
	Poland	246	6.29%
dasay	Poland	336	9.65%
	Australia	308	8.85%
	Turkey	251	7.21%
mantuma	Poland	430	18.81%
	Turkey	332	14.52%
	Germany	267	11.68%
ewq	The Netherlands	397	31.68%
	Germany	290	23.14%
	Australia	161	12.84%

Table 6: Top 3 countries of origin for every botnet

Name	Country	IP addresses	Percentage
stilos	Poland	103	8.78%
	Australia	95	8.09%
	Singapore	62	5.28%
pinano	Poland	300	30.30%
	Australia	235	23.73%
	Germany	127	12.82%
CIT_{58}	Denmark	537	74.89%
	Norway	70	9.76%
	Finland	22	3.06%
gr10	Germany	345	54.07%
	The Netherlands	101	15.83%
	United States	36	5.64%
yds/dsg	Germany	236	49.06%
	Italy	47	9.77%
	Mexico	38	7.90%
al	Germany	129	91.48%
	United States	7	4.96%
	Ireland	2	1.41%
CIT_{29}	Finland	20	41.66%
	Denmark	16	33.33%
	United States	5	10.41%

Table 6: Top 3 countries of origin for every botnet