

From Flame&Red October to Miniduke

Dissecting High-end Cyberespionage
Campaigns

Costin G. Raiu

Director, Global Research & Analysis Team



Cybercriminals $\leftrightarrow$ Money



Nation states are driven by **something else**.
Espionage. Sabotage. Cyberwar.

2009 – The Aurora Operation



Attacked: Google, Adobe, Juniper, Yahoo,
Morgan Stanley, Dow Chemical, etc...

2010 – Stuxnet



First known Cyberweapon

2011 – Duqu

DUQU

Sophisticated. Stealthy. Elusive.
Nation state sponsored cyber-espionage.

2012 – Flame



2013 – Red October



THE HUNT FOR RED OCTOBER



October 2012



Source: KL customer in a EU country

Exploits – Chinese origin

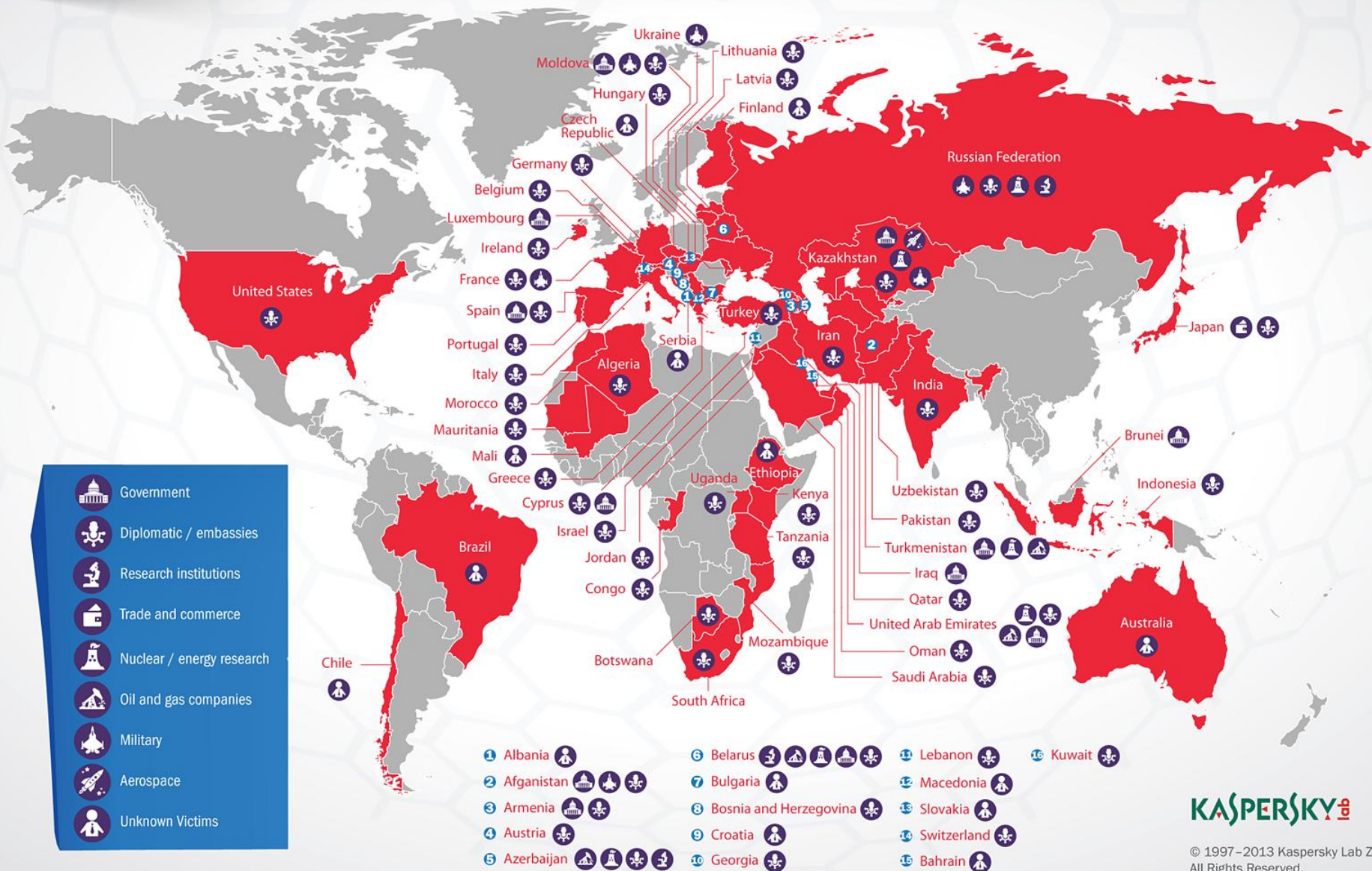
EXIF METADATA

=====

MIMEType	:	application/vnd.ms-excel
Company	:	
ModifyDate	:	2009:11:26 03:35:15
TitleOfParts	:	Sheet1
Author	:	
CodePage	:	Windows Simplified Chinese (PRC, Singapore)
Title	:	
AppVersion	:	11.9999
LastModifiedBy	:	qq
HeadingPairs	:	??????, 1
HyperlinksChanged	:	No
CreateDate	:	1996:12:17 01:32:42
FileType	:	XLS
Software	:	Microsoft Excel

Operation “Red October”

Victims of advanced cyber-espionage network



Filenames used in attacks

- Katyn_-_opinia_Rosjan.xls
- WORK PLAN (APRIL-JUNE 2011).xls
- EEAS-Staff New contact list (05-25-2011).xls
- tactlist_05-05-2011_.8634.xls
- EEAS New contact list (05-05-2011).xls
- Agenda Telefoane institutii si ministere 2011.xls
- FIEO contacts update.xls
- spisok sotrudnikov.xls
- List of shahids.xls
- Spravochnik.xls
- EEAS New contact list (05-05-2011) (2).xls

Diplomatic car for sale



MODEL: Mazda 323- 1998

DISPLACEMENT: 1800 cc

TRANSMISSION: Automatic

FUEL: Benzin

MILEAGE: 145.000 km

*Power Steering - Electric Windows - AM/FM Stereo-
Electric Mirrors - Air Conditioning - Remote central
locking with Alarm - Extra snow tires.*

PRICE: 2.700 \$ (USD)

CONTACT: &&&&&&&& - &&&&&&&&

THE CAR IS IN A VERY GOOD CONDITIONS

C&C comms

```
"E0 | E0 1E0 ÄE0 OE0 æE0 oE0
F0 $F0      ^>0 .>0 >>0 L>0 d>0 t>0 ,>0 ">0 ç>0 ,>0 æ>0 Ü>0 î>0 _>0 ÷?0 (?0 >?0 T
?0 b?0 r?0 ,?0 Z?0 o?0 ð?0 ¶?0 E?0 O?0 ä?0 ú?0 ï00 $00 800 R00 `00 l00 |00 ?00 z
00 ^00 E00 O00 î00 A0 J00 ^A0 ,A0 :A0 BA0 PA0 bA0 pA0 ,A0 -A0 A0 °A0 ¼A0 IA0 O
A0 æA0 ôA0 J00 $B0 :B0 TB0 nB0 ,B0 sB0 ıB0 _B0 IB0 ÜB0 êB0 ôB0 0C0 Q00 "C0 0C0 F
C0 UC0 dC0 rC0 SC0 xC0 ½C0 ÖC0 ìC0 ♦D0 İD0 ▲D0 8D0 RD0 dD0 xD0 -D0 ðD0 ðD0 ED0 O
D0 äD0 dD0 oD0 0E0 ↑E0 (E0 2E0 @E0 RE0 bE0 vE0 +E0      F00      `F0 jF0 lF0 ZF0
oF0      ♦ ?♥ ?t ?▶ ?‡ ?♂ ?4 ? ?s ?o ?♀ ?!! ?      4F0
.↓0▶?20▶ÉE0▶NL0▶a'0▶Gz0▶      xI0▶F→0▶      hz0▶      bestcrypt_update
nt-windows-online.com;nt-windows-update.com;nt-windows-check.com
START DATA
BEGIN DATA
END OF DATA /cgi-bin/nt/th kernel32.dll RegisterServiceProcess \ \
\ .exe wb wb dll wb BestCrypt Software\Microsoft\Windows\CurrentVersio
n\Run \ %c:\ %c:\ %c:\ %I64u . , Trun ProgramFilesDir Soft
ware\Microsoft\Windows\CurrentVersion CommonFilesDir Software\Microsoft\Windo
ws\CurrentVersion AppData SystemDrive Software\Microsoft\Windows\CurrentVersio
n\Explorer\Shell Folders ALLUSERSPROFILE SystemRoot ProgramFiles UserProf
ile Temp \Windows NT \Windows NT\Accessories \Windows NT\Pinball \Windows Med
ia Player \Web Publish \Outlook Express \Microsoft Office\Office10\Data
\Microsoft Office\Office10 \Microsoft Frontpage \Internet Explorer \ComPlus
Applications \Microsoft Shared\MsInfo \Microsoft Shared\Office10 \Proof
```

Domain name: **nt-windows-online.com**

Name servers:

ns1.nameself.com

ns2.nameself.com

Registrar: **Regtime Ltd.**

Creation date: **2011-04-01**

Expiration date: 2013-04-01

Registrant:

Ustuygov Denis Egorovich

Email: ustuygov_d@mail.ru

Organization: Ustuygov Denis

Address: Povorotnikova 19

City: Omsk

State: Omskaja obl.

ZIP: 644015

Country: RU

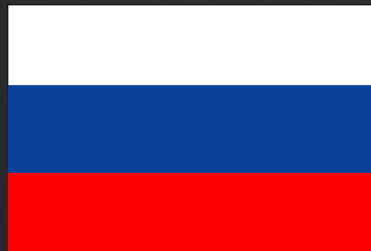
Phone: +7.3812557380

Fax: +7.3812557380

Servers in Germany

IP Information for **178.63.208.49**:

IP Location:	 Germany Nuremberg Hetzner Online Ag
ASN:	AS24940
Resolve Host:	static.49.208.63.178.clients.your-server.de
IP Address:	178.63.208.49     
Reverse IP:	2 websites use this address. (examples: genuine-check.com nt-windows-online.com)



Red October C2s

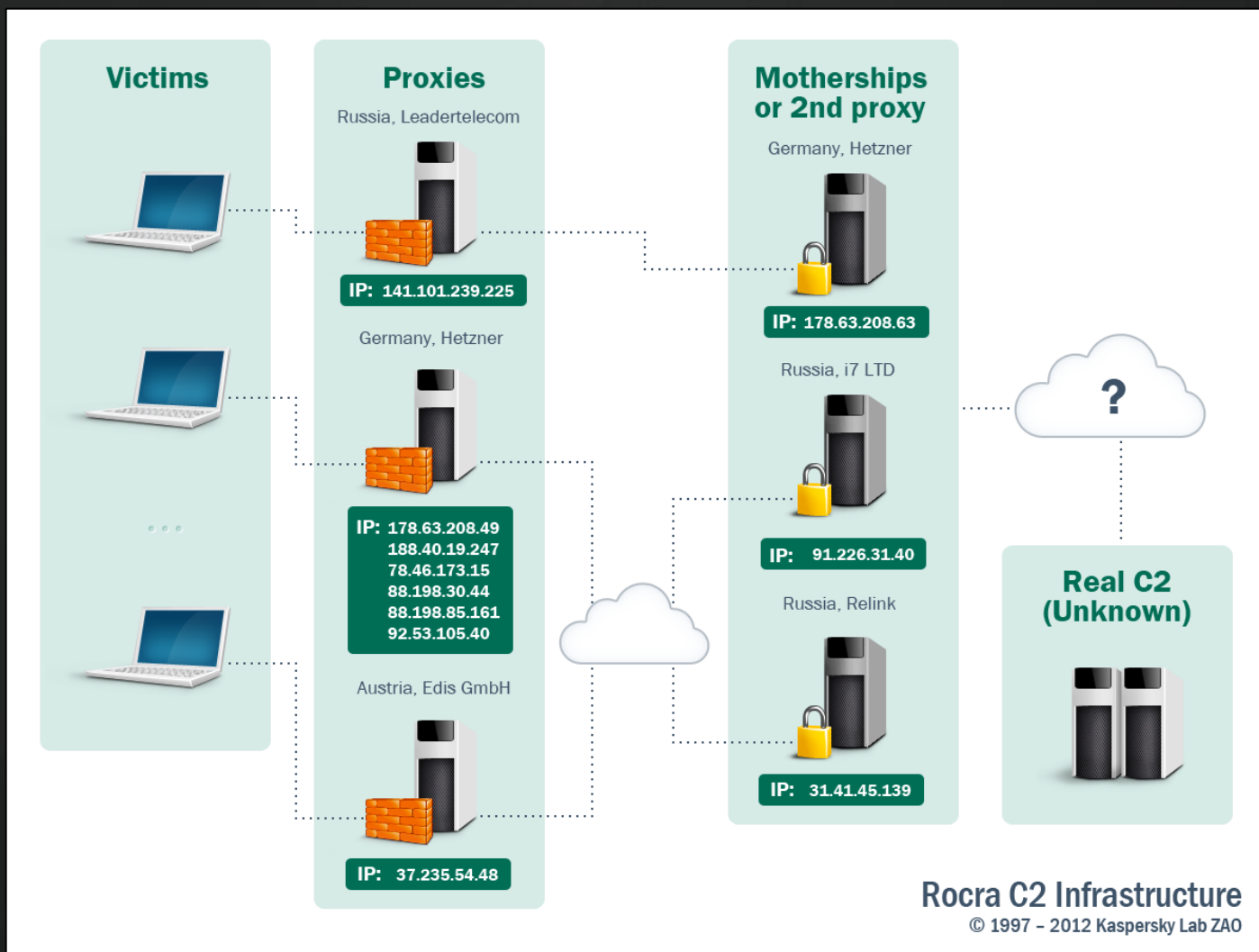
- Oldest known domain: May 2007
(msgenuine.net)
- Newest known domain: October 2012
(drivers-check.com)
- Total: +60 domains
- Sinkholed by KL: 9

First hit to msgenuine.net

5.144.210.x msgenuine.net - [19/Nov/2012:13:07:55 +0000]
"POST http://msgenuine.net/cgi-bin/view HTTP/1.1" 200 98
"_" "_"

```
inetnum:          5.144.192.0 - 5.144.223.255
netname:          COSMOTE
descr:            Cosmote Mobile Telecommunications S.A.
descr:            Cosmote Internet Services
descr:            APN internet
country:          Greece
admin-c:          CIA19-RIPE
tech-c:           CIA19-RIPE
status:           ASSIGNED PA
mnt-by:           COSMOTE-MNT
source:           RIPE # Filtered
```

Red October C2 infrastructure



Red October's
modules:

34 types

9 groups

1000+ files

maybe not all...

No	Name	Group	Size (Kb)	Summary
1	RegConn	Recon	~160	Query system software environment
2	WnHttp	Recon	~142	Get external IP and send to the C&C
3	SysInfo	Recon	~503	Get browser history,usb drives,processes,disks,...
4	GetWebFtp	Recon	~157	Get browser history,http/ftp credentials
5	AuthInfo	Recon	~660	Get file manager,browser,ftp,mail client credentials
6	Logic	Recon	~160	Get general information about current Windows machine and available remote network shares
7	ILogic	Recon	~150	Grab Internet Explorer URL history from the local system
8	Repeat2	Recon	~150	Get listing from remote shares available in Windows network neighborhood
9	Reference	Recon	~150	Grab directory/file listings of all drives attached to the local system
10	PswSuperMailru	Password	230-260	Steal Mail.ru account info and Outlook attachments
11	PswOutlook	Password	~31	Steal Outlook account info
12	MSHash	Password	400-550	Steal Windows account hashes
13	MAPIClient	Email	418-440	Steal e-mail data using local MAPI
14	POP3Client	Email	1100-1200	Steal e-mail data from POP3 server
15	USBContainer	USB drive	649-690	Loads and runs embedded USBStealer
16	USBRestore	USB drive	372-376	Recover and steal deleted files on USB drives
17	USBStealer	USB drive	448-504	Steal interesting files from USB drives
18	Keylogger	Keyboard	300-312	Makes screenshots, records keystrokes
19	Scheduler	Persistence	~620	Run various tasks from spec folders
20	DocBackdoor	Persistence	75-88	Runs an embedded module from MSOffice/PDF doc
21	OfficeBDInstaller	Persistence	~286	Installs DocBackdoor plugin in MS Office
22	AdobeBDInstaller	Persistence	~218	Installs DocBackdoor plugin in Adobe Reader
23	FilePutExec	Spreading	~305	Extract and run an embedded file locally or remotely
24	Netscan	Spreading	~315	Port scanner, vuln. scanner, Cisco cfg dumper
25	MSExploit	Spreading	~1200	Infect target host using MS08-067 exploit
26	DASvcInstall	Spreading	~276	Infect target host using admin credentials
27	Frog	Spreading	~102	Initial backdoor, used in MSExploit/DASvcInstall
28	iPhone	Mobile	329-331	Steals data from locally attached iPhone
29	Nokia	Mobile	~337	Steals data from locally attached Nokia phone
30	Winmobile	Mobile	~400-700	Infect locally attached Windows Mobile phones with a native backdoor/updater modules
31	Winmobile	Mobile	~7-100	Native mobile backdoor/utilites
32	WnFtpScan	Exfiltration	~209	Steals files from local FTP server
33	GetFileReg	Exfiltration	~340	Steals files from local/network disks
34	FileInfo	Exfiltration	339-340	Uploads various collected files to the C&C

-  - "online" module: all data is sent to the C&C; no local files created;
-  - "offline" module; no network communication; all data is stored locally;
-  - module with embedded script/config in resource named "AAA";
-  - module with all values hardcoded.

USBStealer – Acid Crypto

sa=/pubring.*/
sa=/secring.*/
sa=\\.

sa=\\.

sa=\\.

sa=\\.

sa=\\.

sa=\\.

sa=\\.

sa=\\.

sa=\\.

sa=\\.

sa=\\.

Acid Cryptofiler



Cet article est **orphelin**. Il a peu ou aucun article lié à lui.

(mars 2011)

Aidez à ajouter des liens dans les articles relatifs au sujet.

Acid Cryptofiler est un logiciel conçu par le département maîtrise de l'information (ex Centre Electronique de l'Armement, [CELAR](#)¹) de la **Direction générale de l'armement**.

Il est basé sur l'intégration de bibliothèques cryptographiques gouvernementales avec une [Interface de programmation CCSD](#) (Couches Cryptographiques de Sécurité de Défense).

Il offre les fonctions suivantes :

- **Chiffrement asymétrique** sous forme d'archive (Multi-fichiers, multi-destinataires) dites Archives Acid.
- **Chiffrement de volume (conteneurs) en mode symétrique et en mode asymétrique.**

Il dispose pour les clefs publiques d'une fonction d'annuaire de type [LDAP](#), [Active Directory](#), [Http](#), [File Transfer Protocol](#) et [Fichier informatique](#).

Red October – language use

```
mov     dword_47786C, eax
jnz     short loc_402847
call    dword_46E578
push    eax                ; ArgList
push    offset aCannotInjectZa ; "Cannot inject zakladka, Error: %u"
call    sub_403370
add     esp, 8
call    sub_404130
mov     eax, 3
pop     esi
mov     ecx, [esp+21Ch+var_4]
xor     ecx, esp
call    @_security_check_cookie@4 ; __security_check_cookie(x)
add     esp, 21Ch
retn
```

```
                                ; CODE XREF: sub_4026E0+131↑j
push    offset aZakladkaInject ; "Zakladka injected"
call    sub_403370
push    230h                  ; size_t
push    0                     ; int
push    offset dword_4771D0 ; void *
```

“Proga”?

```
73 5D 20 70 61 73 73 77 64 28 25 ..TMP.%s.uin(%d)[%s] passwd(%
73 52 65 61 64 20 6F 6B 21 0A 00 d)[%s]...%s.ProcessRead ok!..
25 64 5D 0A 00 00 25 73 09 4D 6F %s.SEARCH passnum[%d]...%s.Mo
75 6E 64 0A 00 25 73 09 45 52 52 dule magent.exe found..%s.ERR
6D 61 67 65 6E 74 2E 65 78 65 00 OR Read Process...magent.exe.
72 20 43 72 54 53 6E 61 70 0A 00 .%s.err Mt...%s.err CrTSnap..
65 6E 74 5F 6D 61 69 6C 2E 72 75 %s.OPEN PROCESS agent_mail.ru
72 6F 63 20 61 67 65 6E 74 0A 00 OK!...%s.err op proc agent..
20 43 6C 6F 73 65 48 61 6E 64 6C ..%s.err ProcFirst CloseHandl
6E 61 70 0A 00 00 00 25 73 09 65 e....%s.inv CrT32Snap....%s.e
09 2E 2E 2E 0A 00 25 73 2D 2D 2D rr op key:[%s]..%s.....%s---
0A 00 00 00 00 2D 2D 2D 2D 2D 2D ----PROGA END-----
00 00 00 00 53 55 50 45 52 20 4D -PROGA START-----SUPER M
30 32 64 25 30 32 64 25 30 32 64 UTEX.ab..%04d%02d%02d%02d%02d
3A 25 30 32 64 3A 25 30 32 64 3A %02d...."%04d:%02d:%02d:%02d:
00 28 00 6E 00 75 00 6C 00 6C 00 %02d:%02d"../\.*..(.n.u.l.l.
```

Conversation

8/26/2008 12:45: Смена статуса

Whoisprotect Вы заказали выключение статуса WhoisProtect

домена msinfoonline.org. Произошла ошибка и статус изменен не был.

Описание ошибки: "There is already a pending action for this order"

8/26/2008 12:54:

А как можно решить эту проблему?

8/26/2008 12:57:

а в чем проблема? Что означает

"Domain msinfoonline.org sync failed:

Ошибка API регистратора: Локальные данные не совпадают с реестром"???

The MiniDuke

Ukraine's NATO Membership Action Plan (MAP) Debates

PONARS Eurasia Policy Memo No. 9

Oleksandr Sushko

Center for Peace, Conversion, and Foreign Policy of Ukraine
March 2008

The North Atlantic Treaty Organization is expected to address Ukraine and Georgia's requests to upgrade their relationship with the alliance at the summit in April 2008, even if a direct response is not forthcoming. Ukraine submitted its official request to receive a Membership Action Plan (MAP) in January, setting off a new round of debates discussing the feasibility of Ukraine's ambitions to become a full-fledged member of the Euro-Atlantic community.

The debate over a MAP began in May 2002, when Ukraine's National Security and Defense Council (NSDC) approved a strategy later signed by President Leonid Kuchma stipulating Ukraine's objectives to become a full NATO member. Given substantial problems with democracy, human rights, and media freedoms within Ukraine, this ambition (considered mostly as an element of Kuchma's multi-vector policy) was not addressed by NATO at the time.

Following the Orange Revolution, President Viktor Yushchenko declared his desire to move forward toward NATO membership. NATO formally invited Ukraine to enter into an "Intensified Dialogue" (ID) at its meeting in Vilnius in April 2005. This created a forum to discuss Ukraine's membership aspirations and the reforms necessary without prejudicing an eventual decision by the alliance. A meeting of the NATO-Ukraine Commission also agreed on a series of concrete and immediate measures to enhance cooperation supporting Ukraine's reform priorities. Ukraine has pursued its

Ukraine's Search for a Regional Foreign Policy

One Year After the Orange Revolution

PONARS Policy Memo No. 377

Oleksandr Sushko

Center for Peace, Conversion, and Foreign Policy of Ukraine
December 2006

The Bucharest declaration of Ukraine and Georgia in August 2005, and the first summit of the widely-announced Community for Democratic Choice (CDC) scheduled for December 1-2, 2005, have set an ambitious agenda for Ukraine as a potentially influential regional power.

The Ukrainian experience has revitalized hope for the further spreading and maturing of democracy, rule of law, and other Western values in the institutionally fragile and fragmented eastern European margin. President Viktor Yushchenko proclaimed that Ukraine wishes to be a regional leader after his inauguration in early 2005. However, the content and instruments of this eventual leadership still remain unclear. Does Ukraine want to follow a Russian model of leadership by pursuing egoistic national interests? Or is it seeking a European model of leadership based upon common values and the responsibility of larger states before smaller ones?

The only means for Ukraine to become a center of gravity in eastern Europe and the Black Sea area is to become a true success story, not only in peaceful evolution toward freedom and democracy, but in converting those changes into consistent policies. This means strengthening the rule of law and market economy institutions within the country and promoting a new regional agenda that includes cooperation in

MiniDuke - Twitter



MiniDuke – C2's

Target location	C&C server	IP / location	path on C2
Hungary	arabooks.ch	194.38.160.153 / Switzerland	/lib/index.php
Luxemburg	artas.org	95.128.72.24 / France	/engine/index.php
Belgium	tsoftonline.com	72.34.47.186 / United States	/views/index.php
(Multiple)	www.eamtm.com	188.40.99.143 / Germany	/piwik/web/index.php

Stage 2 – GIF files

Index of /engine/img

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 bg afvd.gif	20-Feb-2013 21:16	24K	
 bg dafd.gif	20-Feb-2013 21:16	24K	
 bg dasfs.gif	20-Feb-2013 21:17	24K	
 bg dsaf.gif	20-Feb-2013 21:17	24K	
 bg dsaffe.gif	21-Feb-2013 09:18	24K	
 bg edf.gif	21-Feb-2013 09:19	24K	
 bg efd.gif	21-Feb-2013 09:19	24K	
 bg efdse.gif	21-Feb-2013 09:19	24K	
 bg fked.gif	21-Feb-2013 09:19	24K	
 bg fwds.gif	21-Feb-2013 09:19	24K	
 bg lkjkef.gif	21-Feb-2013 09:20	24K	
 bg sdef.gif	21-Feb-2013 09:20	24K	
 bg sdefk.gif	21-Feb-2013 09:20	24K	
 bg sfef.gif	21-Feb-2013 09:20	24K	

Apache Server at artas.org Port 80

Index of /views/img

- [Parent Directory](#)
- [1109821546.gif](#)
- [2627081433.gif](#)
- [3198217296.gif](#)
- [3946889701.gif](#)
- [3979106736.gif](#)
- [bg aek.gif](#)
- [bg dfdsh.gif](#)
- [bg dfell.gif](#)
- [bg dfesik.gif](#)
- [bg dfew.gif](#)
- [bg dfews.gif](#)
- [bg dflj.gif](#)
- [bg dfwe.gif](#)
- [bg dsef.gif](#)
- [bg dwed.gif](#)
- [bg edf.gif](#)
- [bg edfsa.gif](#)
- [bg edse.gif](#)
- [bg ekks.gif](#)

Stage 3 – custom backdoor

IP Information for 200.63.46.23

IP Location:  Panama Panama Panamaserver.com

ASN: AS52284

IP Address: 200.63.46.23     

```
inetnum: 200.63.40/21
status: allocated
aut-num: N/A
owner: Panamaserver.com
ownerid: PA-PANA2-LACNIC
responsible: Ch Group Corp.
address: Bella Vista, El ca
address: 00000 - Panama -
country: PA
phone: +507 263 3723 []
owner-c: MAC30
tech-c: MAC30
abuse-c: MAC30
inetrev: 200.63.46/24
nserver: NS1.PANAMASERVER.CO
nsstat: 20130224 AA
nslastaa: 20130224
created: 20080328
changed: 20080328
```

IP Information for 85.95.236.114

IP Location:  Turkey Izmir Inetmar Internet Hizmetleri San. Tic. Ltd. Sti

ASN: AS49467

Resolve Host: ip236.114.networkde.com

IP Address: 85.95.236.114     

```
inetnum: 85.95.236.0 - 85.95.236.255
netname: INETMAR
descr: inetmar internet Hizmetleri -izmir
remarks: *****
remarks: *** Abuse Reports to: abuse@inetmar.com ***
remarks: *** This IP block is used for web hosting, ***
remarks: *** dedicated and co-located servers. In ***
remarks: *** case of spam, please only deal with ***
remarks: *** originator IP only. ***
remarks: *** DO NOT DEAL WITH THE WHOLE IP BLOCK ***
remarks: *****
country: TR
```

Clues - 666

```

    add     esp, 400h
    retn
CRC32      endp
; -----
;          dw 666
; -----
; START OF FUNCTION CHUNK FOR DecryptURLWithSHA1
cGet128bytes:      call     Get128bytes      ; CODE XREF: DecryptURLWithSHA1+5fj
; END OF FUNCTION CHUNK FOR DecryptURLWithSHA1
; -----
    dd 0
    dd 0
    dd 8834222Dh
    dd 0CFE7AE70h
    dd 178888F4h

```

Dante Alighieri

Affreno, allodetta, apparenza, artigli, assunta,
asterisk, augelletti, benedetto, brigata, caccianli,
calliope, cappuccio, cardini, carpone, chiamato,
chiameranno, cinquanta, cocolle, compagnia,
concederebbe, consolare, contraria, cornute...

(Divine Comedy)

3. Paradiso

2. Purgatorio

1. Inferno



MiniDuke - summary

- Active since **May 2012**
- Victims in **20+ countries** (majority NATO)
- Government-related: Ukraine, Belgium, Portugal, Romania, Czech Republic, Ireland, Turkey, etc...
- **Same threat level** as “Red October”
 - (or higher, according to Romania’ S.R.I.)

The trend: number of 'Black Swans' is growing

2009

Aurora

2010

Stuxnet

2011

Duqu

2012

- ✦ **Flame**
- ✦ **Gauss**
- ✦ **miniFlame**
- ✦ **Shamoon**



See: 'Nassim Nicholas Taleb:
The Black Swan'

The 3 dangers of Cyberwar

- Ideas and techniques from cyberweapons can be re-purposed and copied.
- Companies become collateral victims in the cyberwar between superpowers.
- Cybercriminals start using weaponized exploits developed by or for governments.

The truth?



Threats are **everywhere**



Corporate Threat Landscape

Threats from all angles



Defense?

Against military grade weapons, you want the **best available** defense technologies.

Patch. Whitelist. Default Deny.

Exploit prevention. 0-day defense.

Realtime protection. Cloud protection.

Perimeter. Green zone. Raise awareness.

Access control. Education.

Thank You!

A teal-colored horizontal banner with a fine, woven texture. The right side of the banner is folded over, revealing a white underside. The text "Thank You!" is centered on the banner in a bold, white, sans-serif font.