Duqu– Threat Research and Analysis

McAfee Labs

Peter Szor

Sr. Director of Research

Agenda

- Stuxnet Overvieew
- Duqu Review-Current Intelligence, comparisons with Stuxnet,
- Best Practice recommendations
- Q&A

High Level Overview

- The executables share injection code with the Stuxnet worm and they were compiled after the last Stuxnet sample was recovered.
- The structure of Duqu is very similar to Stuxnet (uses of PE resources)
- There is no ICS specific attack code in Duqu.
- The primary infection vector for Duqu deployment has not yet been discovered/recovered (Duqu does not self-replicate or spread on its own)
- The infected organizations appear to be limited
- No known targeting of energy sector companies.
- The malware employed a valid digital certificate (revoked as of 14 OCT 2011)
- The malware is designed to self-delete after 36 days
- The known Command and Control server was hosted in India.

The First Industrial Control System Attack

A brief history of Control System Attacks

- DOS/Boot viruses change BIOS password settings, battery needs to be removed
- CIH virus overwrites flash-ROM, motherboard needs replacement
- Worms got faster than update and patch deployment, targeting vulnerabilities, often zero-Days
- Worms caused major DoS attacks

  (… Nuclear Power plants' safety monitoring system was disabled by Slammer)
- Blaster worm is a contributor to a major blackout
- Stuxnet combines 4 zero-day vulnerabilities with ICS knowledge to target an industrial process
- US Predator Drone Center gets infected with malware
- Duqu (by Stuxnet team) is used for targeted attacks in (UK, IRAN, US)

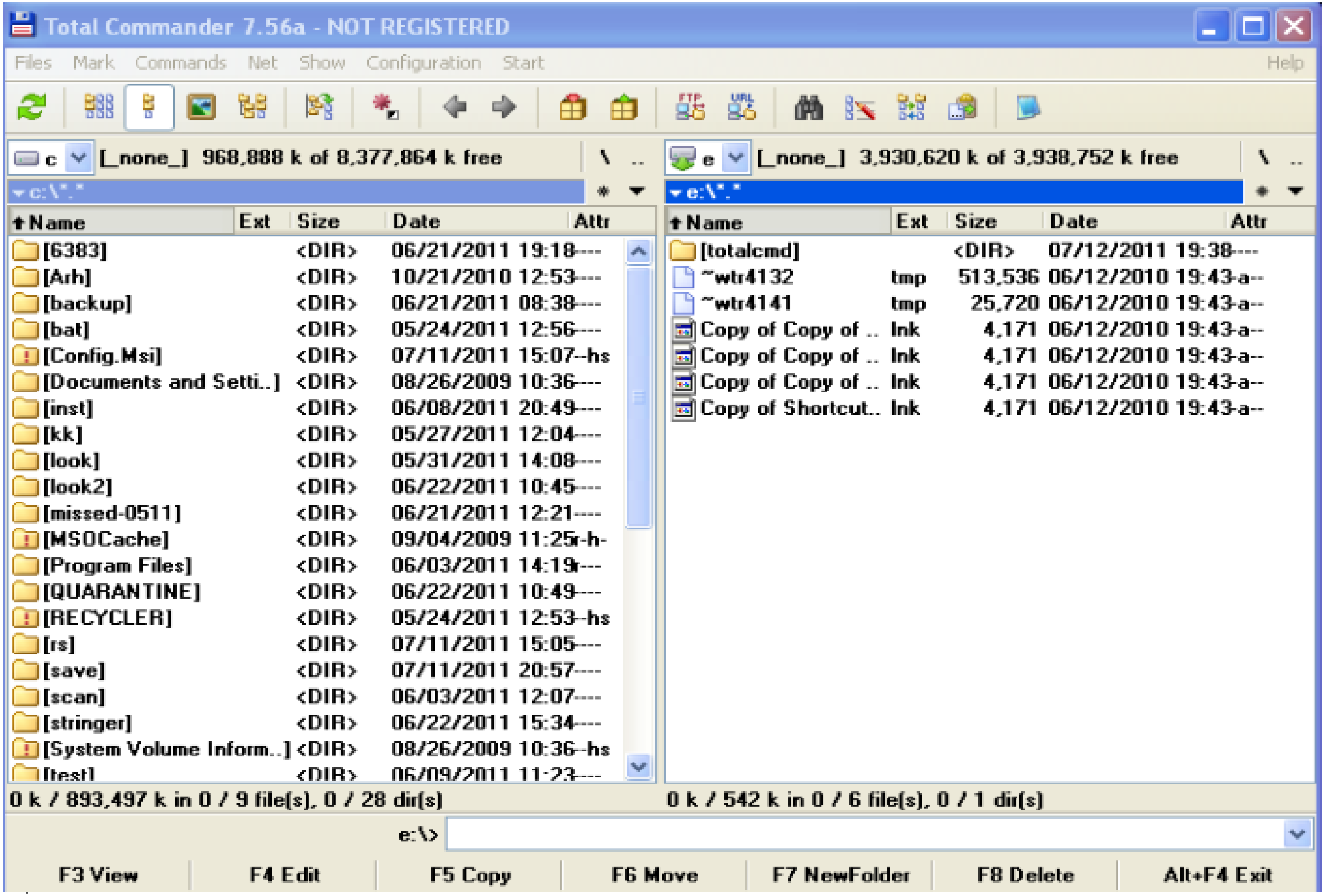
Stuxnet worm developed from November 2007

Exploits "Zero Days" vulnerabilities
- MS10-046 (LNK Vulnerability – Used by Zlob in 2008)
- MS08-067 (Server Service)
- MS10-061 (Print Spooler – Hackin9 magazine 2009)
- MS10-073 (Kbd Privilege Escalation)
- WinCC DBMS Password (hardcoded)

+ Stolen certificates (Realtek, JMicron)
+ ROP techniques in Exploits

Infection
- USB, Local Network, Siemens Step7/MC7
- Network Infection
- C&C operation (Weak! Mypremierfutbol.com, todaysfutbol.com)
- Anti Behavioral Blocking, avoids anti-virus detection
- Rootkit:
  - User mode hooks to hide files from Explorer – Total\Windows Commander(!)
  - User mode DLL replacement for Step7 (PLC Rootkit)
    - s7otbxdl.dll forwards to s7otbxsx.dll (except for 16 functions related to block Read/Write)
  - Filter driver to hide USB content

USB User Mode Rootkit: Hooks APIs, than Sends F5 (Refresh) also Deactivates/Reactivates Total Commander (and “Windows Commander”)



c [_none_] 968,888 k of 8,377,864 k free

c:\*.*

Name	Ext	Size	Date	Attr
[6383]		<DIR>	06/21/2011 19:18	----
[Arh]		<DIR>	10/21/2010 12:53	----
[backup]		<DIR>	06/21/2011 08:38	----
[bat]		<DIR>	05/24/2011 12:56	----
[Config.Msi]		<DIR>	07/11/2011 15:07	--hs
[Documents and Setti..]		<DIR>	08/26/2009 10:36	----
[inst]		<DIR>	06/08/2011 20:49	----
[kk]		<DIR>	05/27/2011 12:04	----
[look]		<DIR>	05/31/2011 14:08	----
[look2]		<DIR>	06/22/2011 10:45	----
[missed-0511]		<DIR>	06/21/2011 12:21	----
[MSOCache]		<DIR>	09/04/2009 11:25	r-h-
[Program Files]		<DIR>	06/03/2011 14:19	r---
[QUARANTINE]		<DIR>	06/22/2011 10:49	----
[RECYCLER]		<DIR>	05/24/2011 12:53	--hs
[rs]		<DIR>	07/11/2011 15:05	----
[save]		<DIR>	07/11/2011 20:57	----
[scan]		<DIR>	06/03/2011 12:07	----
[stringer]		<DIR>	06/22/2011 15:34	----
[System Volume Inform..]		<DIR>	08/26/2009 10:36	--hs
[test]		<DIR>	06/09/2011 11:23	----

0 k / 893,497 k in 0 / 9 file(s), 0 / 28 dir(s)

e [_none_] 3,930,620 k of 3,938,752 k free

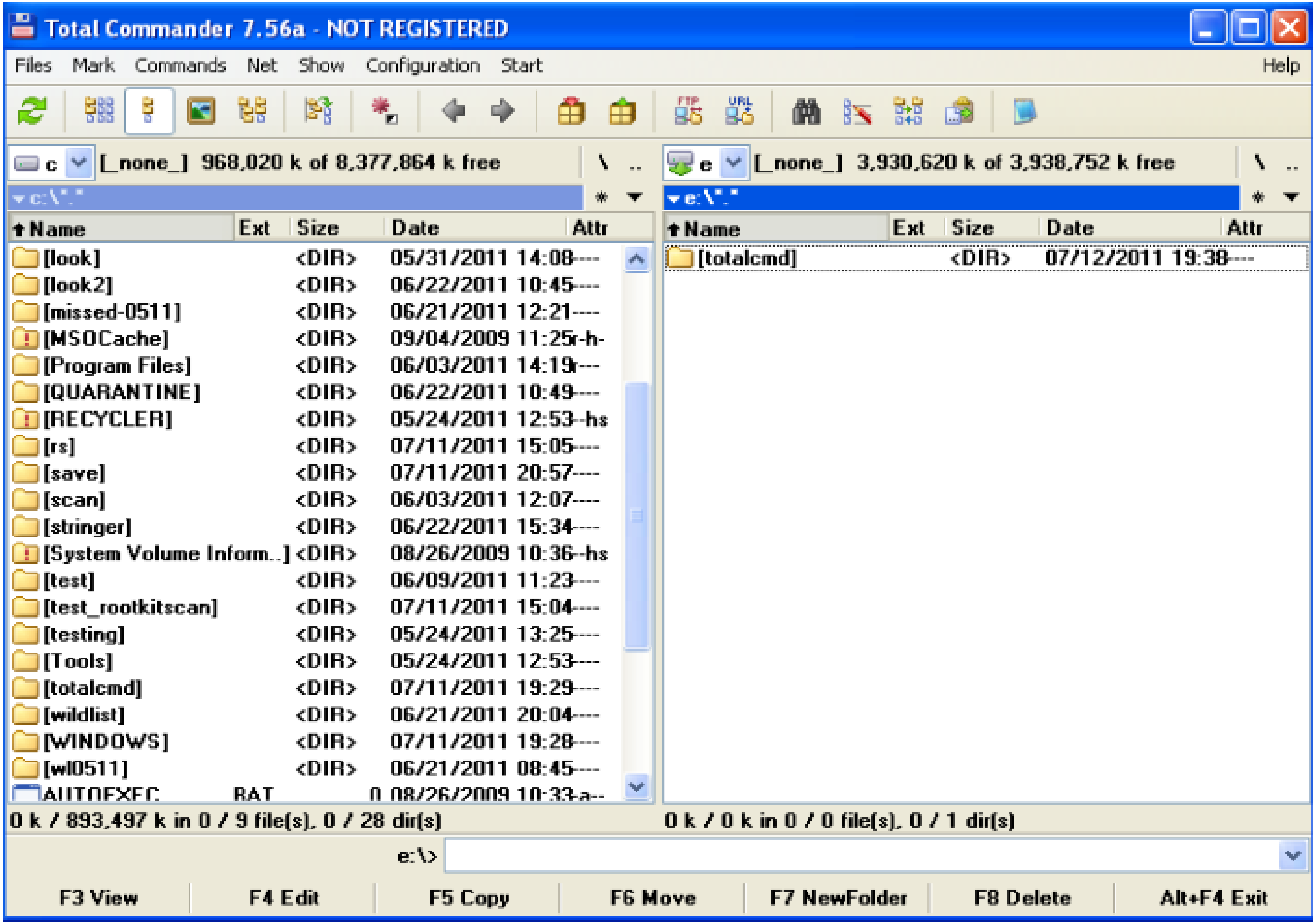
e:\*.*

Name	Ext	Size	Date	Attr
[totalcmd]		<DIR>	07/12/2011 19:38	----
~wtr4132	tmp	513,536	06/12/2010 19:43	-a--
~wtr4141	tmp	25,720	06/12/2010 19:43	-a--
Copy of Copy of ..	lnk	4,171	06/12/2010 19:43	-a--
Copy of Copy of ..	lnk	4,171	06/12/2010 19:43	-a--
Copy of Copy of ..	lnk	4,171	06/12/2010 19:43	-a--
Copy of Shortcut..	lnk	4,171	06/12/2010 19:43	-a--

0 k / 542 k in 0 / 6 file(s), 0 / 1 dir(s)

e:\>

USB User Mode Rootkit: Hooks APIs, than Sends F5 (Refresh) also Deactivates/Reactivates Total Commander (and “Windows Commander”)



c [_none_] 968,020 k of 8,377,864 k free

c:\*.*

Name	Ext	Size	Date	Attr
[look]		<DIR>	05/31/2011 14:08	----
[look2]		<DIR>	06/22/2011 10:45	----
[missed-0511]		<DIR>	06/21/2011 12:21	----
[MSOCache]		<DIR>	09/04/2009 11:25	r-h-
[Program Files]		<DIR>	06/03/2011 14:19	r---
[QUARANTINE]		<DIR>	06/22/2011 10:49	----
[RECYCLER]		<DIR>	05/24/2011 12:53	-hs
[rs]		<DIR>	07/11/2011 15:05	----
[save]		<DIR>	07/11/2011 20:57	----
[scan]		<DIR>	06/03/2011 12:07	----
[stringer]		<DIR>	06/22/2011 15:34	----
[System Volume Inform..]		<DIR>	08/26/2009 10:36	-hs
[test]		<DIR>	06/09/2011 11:23	----
[test_rootkitscan]		<DIR>	07/11/2011 15:04	----
[testing]		<DIR>	05/24/2011 13:25	----
[Tools]		<DIR>	05/24/2011 12:53	----
[totalcmd]		<DIR>	07/11/2011 19:29	----
[wildlist]		<DIR>	06/21/2011 20:04	----
[WINDOWS]		<DIR>	07/11/2011 19:28	----
[wl0511]		<DIR>	06/21/2011 08:45	----
AUTOEXEC	BAT	0	08/26/2009 10:33	-a--

0 k / 893,497 k in 0 / 9 file(s), 0 / 28 dir(s)

e [_none_] 3,930,620 k of 3,938,752 k free

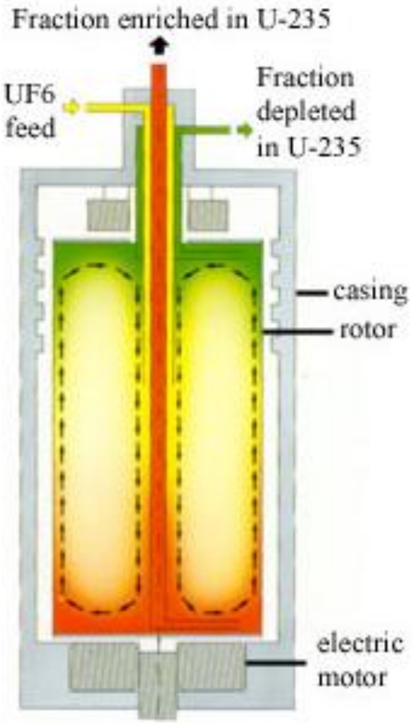
e:\*.*

Name	Ext	Size	Date	Attr
[totalcmd]		<DIR>	07/12/2011 19:38	----

0 k / 0 k in 0 / 0 file(s), 0 / 1 dir(s)

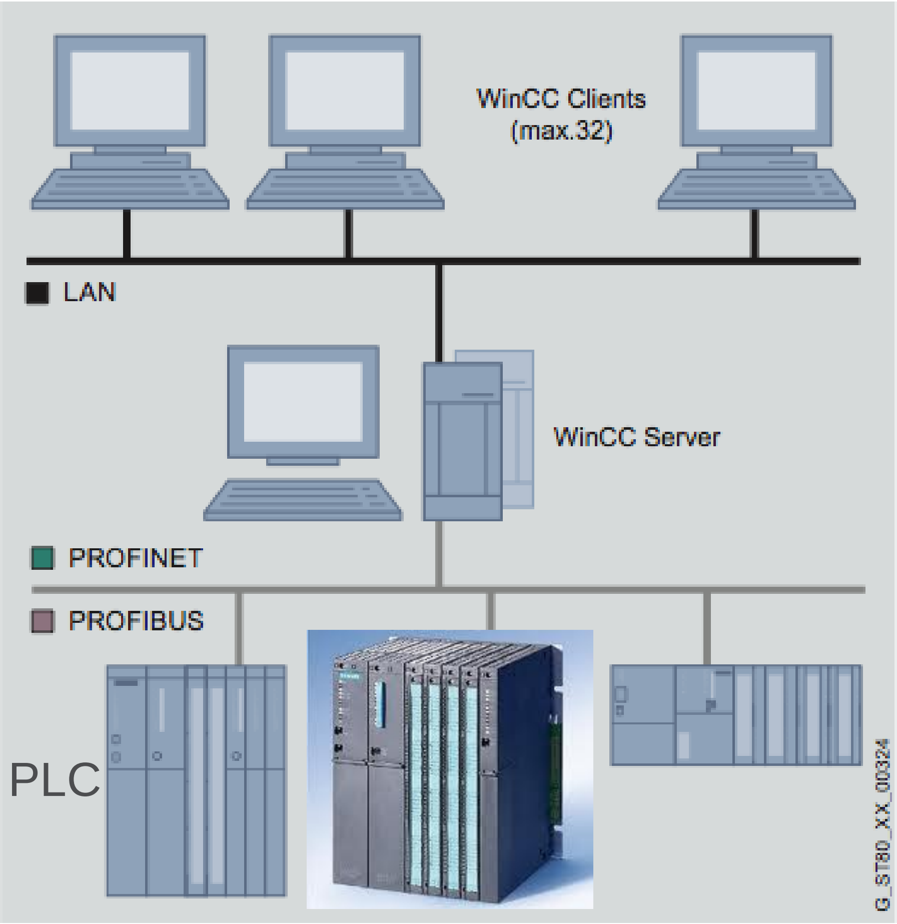
e:\>

The Target: - PLC CPUs 6ES7-417, 6ES7-315-2
At least 33 Frequency Converters, Operating between 807Hz and 1,210Hz.



Cascaded Centrifuges

Vacon + Local Iranian

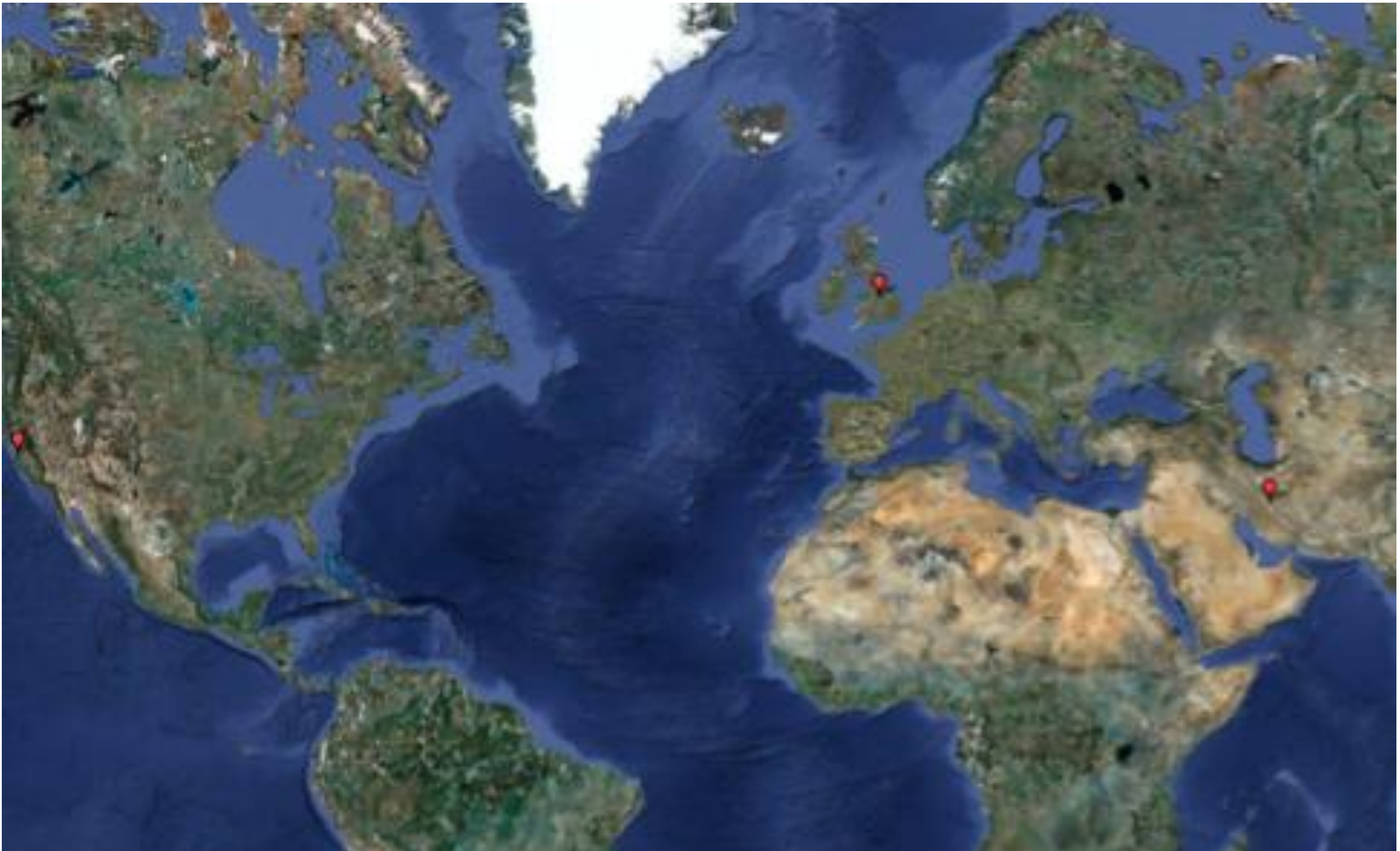


PLC

WinCC multi-user system

September, October 2011: Duqu

- Targeted attacks have been observed in Iran, England and US
- Other reports: Austria, Hungary, Indonesia
- C&C Server in India



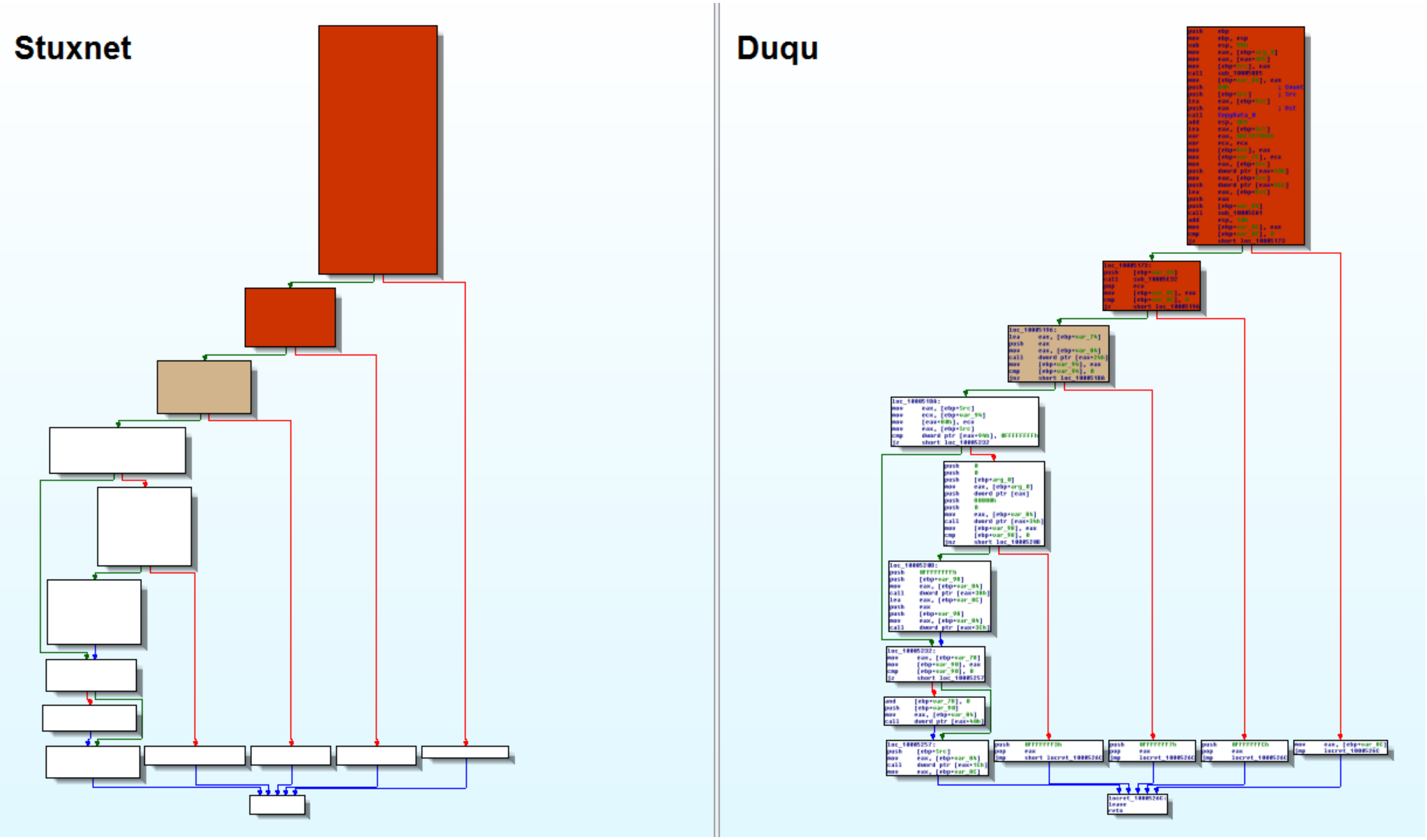
Duqu and Stuxnet

- Several similarities have been observed at the code level which led us to believe Duqu was based on the same source code as Stuxnet

Feature	Duqu	Stuxnet
Composed of multiple modules	Yes	Yes
Rootkit to hide its activities	Yes	Yes
System driver is digitally signed	Yes (C-Media)	Yes (Realtek, JMicron)
System driver decrypts secondary modules in PNF files	Yes	Yes
Decrypted DLLs are directly injected into system processes instead of dropped to disk	Yes	Yes
Date sensitive: functionality is controlled via complex, encrypted configuration file	Yes (36 days)	Yes
Use XOR based encryption for strings	Yes (key: 0xAE1979DD)	Yes (key: 0xAE1979DD)
Referencing 05.09.1979 in configuration file (http://en.wikipedia.org/wiki/Habib_Elghanian)	Yes (0xAE790509)	Yes (0xAE790509)
New update modules via C&C	Yes (keylogger)	Yes
Known Module to control PLC/SCADA systems	No	Yes

Duqu and Stuxnet (Code Graph Comparison)

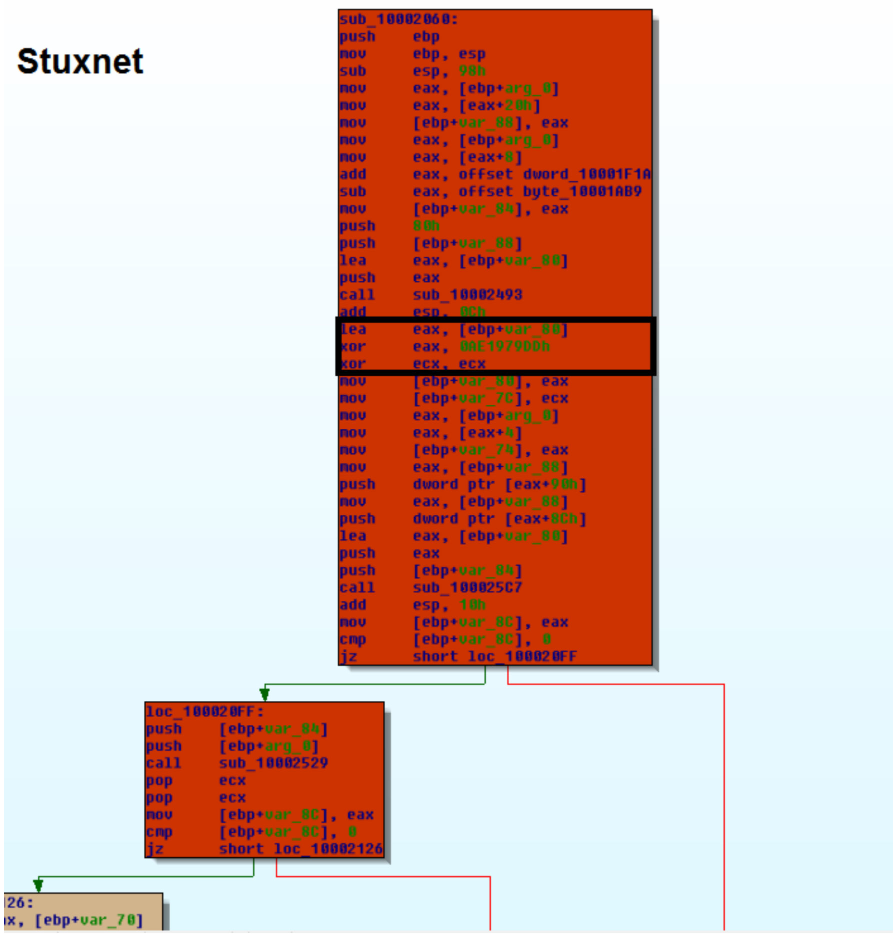
- DLL Injection code



Duqu and Stuxnet: Code Comparison

McAfee

- DLL Injection code

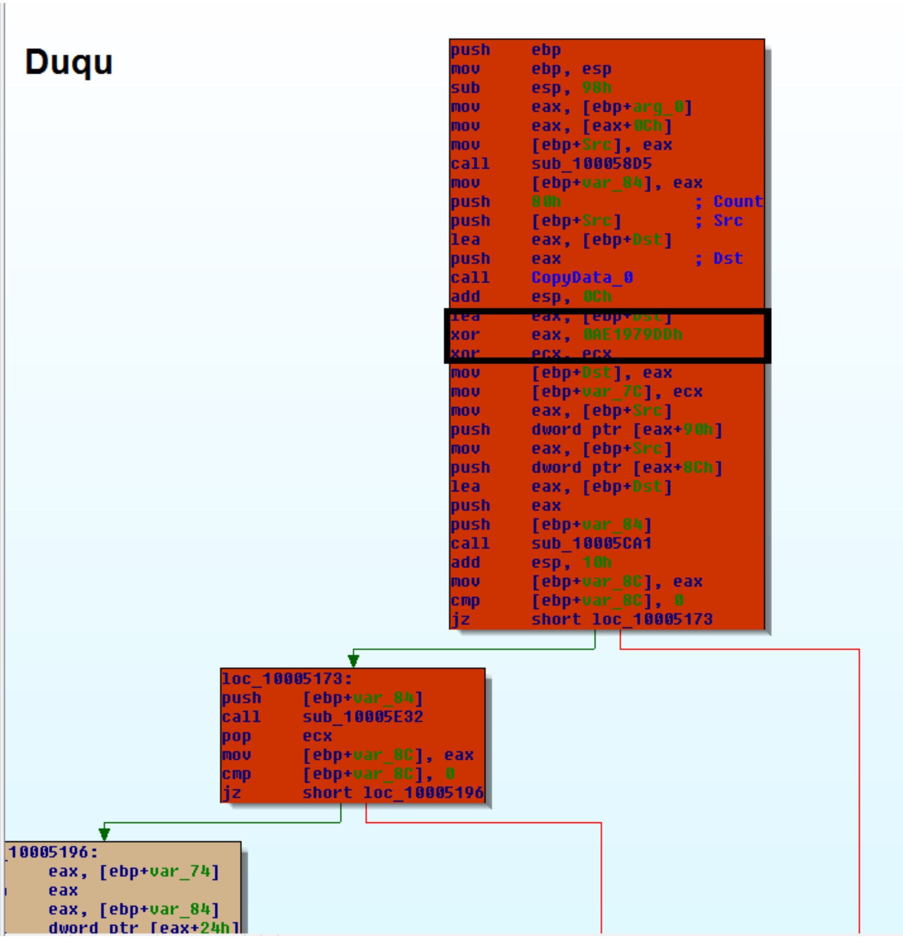


Stuxnet

```
sub_10002060:
push    ebp
mov     ebp, esp
sub     esp, 98h
mov     eax, [ebp+arg_0]
mov     eax, [eax+20h]
mov     [ebp+var_88], eax
mov     eax, [ebp+arg_0]
mov     eax, [eax+8]
add     eax, offset dword_10001F1A
sub     eax, offset byte_10001AB9
mov     [ebp+var_84], eax
push    80h
push    [ebp+var_88]
lea     eax, [ebp+var_80]
push    eax
call    sub_10002493
add     esp, 0Ch
lea     eax, [ebp+var_80]
xor     eax, 0AE1979DDh
xor     ecx, ecx
mov     [ebp+var_80], eax
mov     [ebp+var_7C], ecx
mov     eax, [ebp+arg_0]
mov     eax, [eax+4]
mov     [ebp+var_74], eax
mov     eax, [ebp+var_88]
push    dword ptr [eax+90h]
mov     eax, [ebp+var_88]
push    dword ptr [eax+8Ch]
lea     eax, [ebp+var_80]
push    eax
push    [ebp+var_84]
call    sub_100025C7
add     esp, 10h
mov     [ebp+var_8C], eax
cmp     [ebp+var_8C], 0
jz      short loc_100020FF
```

```
loc_100020FF:
push    [ebp+var_84]
push    [ebp+arg_0]
call    sub_10002529
pop     ecx
pop     ecx
mov     [ebp+var_8C], eax
cmp     [ebp+var_8C], 0
jz      short loc_10002126
```

```
26:
x, [ebp+var_70]
```



Duqu

```
push    ebp
mov     ebp, esp
sub     esp, 98h
mov     eax, [ebp+arg_0]
mov     eax, [eax+0Ch]
mov     [ebp+Src], eax
call    sub_100058D5
mov     [ebp+var_84], eax
push    80h                 ; Count
push    [ebp+Src]           ; Src
lea     eax, [ebp+Dst]
push    eax                 ; Dst
call    CopyData_0
add     esp, 0Ch
lea     eax, [ebp+Dst]
xor     eax, 0AE1979DDh
xor     ecx, ecx
mov     [ebp+Dst], eax
mov     [ebp+var_7C], ecx
mov     eax, [ebp+Src]
push    dword ptr [eax+90h]
mov     eax, [ebp+Src]
push    dword ptr [eax+8Ch]
lea     eax, [ebp+Dst]
push    eax
push    [ebp+var_84]
call    sub_10005CA1
add     esp, 10h
mov     [ebp+var_8C], eax
cmp     [ebp+var_8C], 0
jz      short loc_10005173
```

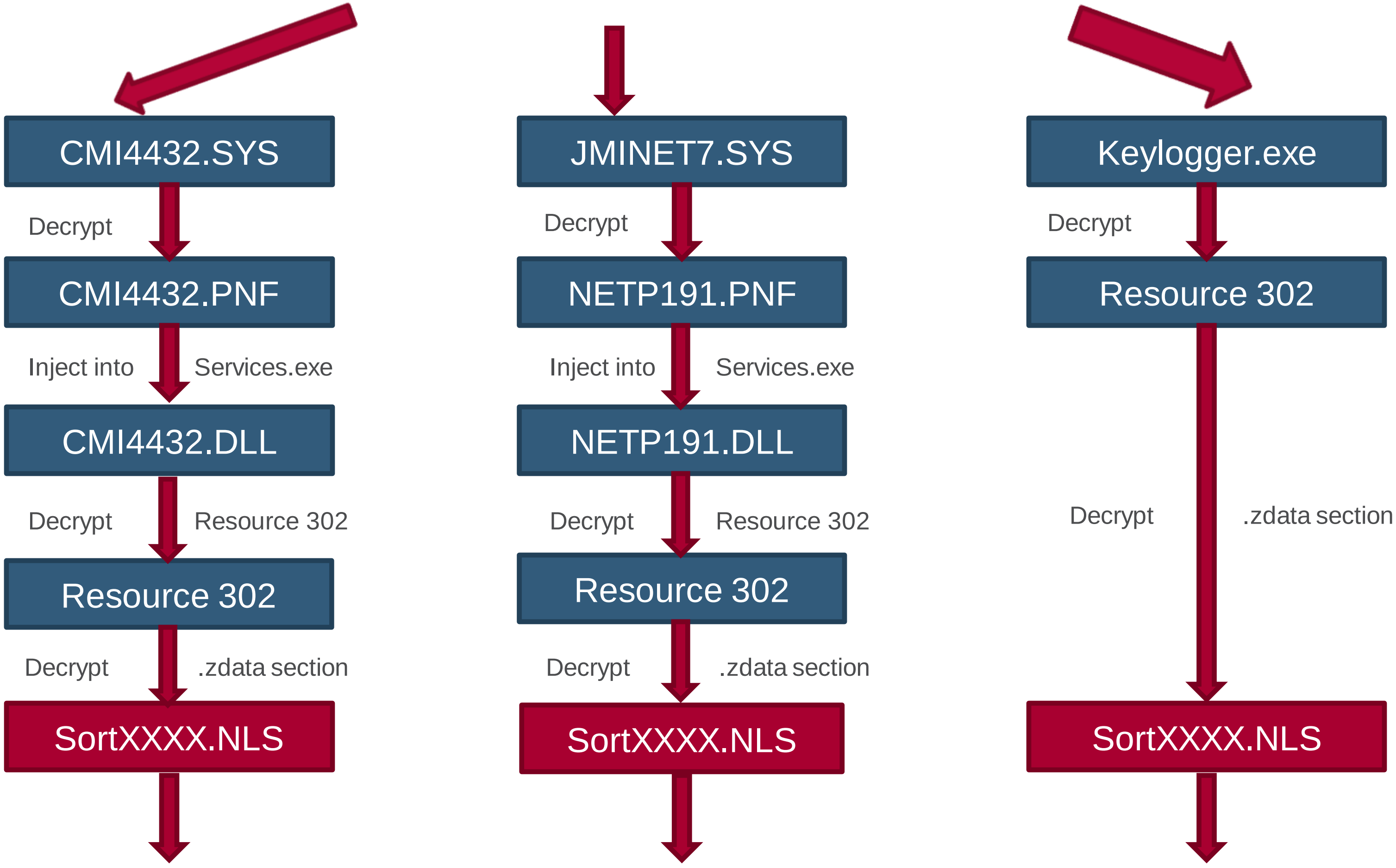
```
loc_10005173:
push    [ebp+var_84]
call    sub_10005E32
pop     ecx
mov     [ebp+var_8C], eax
cmp     [ebp+var_8C], 0
jz      short loc_10005196
```

```
_10005196:
        eax, [ebp+var_74]
        eax
        eax, [ebp+var_84]
        dword ptr [eax+24h]
```

Duqu module relationship

Unknown vector of exploitation, Installer

C&C Server



CMI4432.SYS

Decrypt

CMI4432.PNF

Inject into Services.exe

CMI4432.DLL

Decrypt Resource 302

Resource 302

Decrypt .zdata section

SortXXXX.NLS

JMINET7.SYS

Decrypt

NETP191.PNF

Inject into Services.exe

NETP191.DLL

Decrypt Resource 302

Resource 302

Decrypt .zdata section

SortXXXX.NLS

Keylogger.exe

Decrypt

Resource 302

Decrypt .zdata section

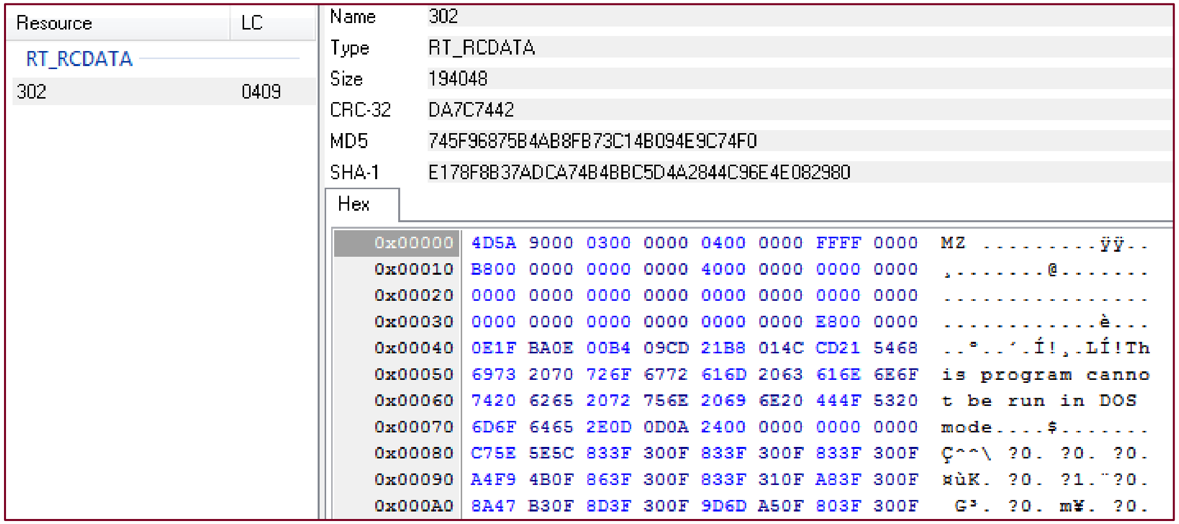
SortXXXX.NLS

Inject main modules into System Processes

Winlogon, Services, Explorer, Iexplore

Duqu Main Module

- The two variants of .SYS files are responsible for restarting the malware
- .SYS filenames mimic Jmicron and C-Media driver file names
- Jmicron mimic file is not signed, and it is the earlier variant
- Drivers are loaded at time of “Network group load”
- They decrypt the PNF files and inject the resulting DLL into Services.exe, etc
  - Anti-firewall feature, Anti-BB feature
- This DLL is responsible for decrypting the payload module from its resource section. The resource Id is the same for all modules: 302
- The payload module is directly injected into running processes using the same method as Stuxnet
- The DLL implement rootkit methods to hide this payload from user’s view



Resource	LC
RT_RCDATA	
302	0409

Name	302
Type	RT_RCDATA
Size	194048
CRC-32	DA7C7442
MD5	745F96875B4AB8FB73C14B094E9C74F0
SHA-1	E178F8B37ADCA74B4BBC5D4A2844C96E4E082980

```
0x00000  4D5A 9000 0300 0000 0400 0000 FFFF 0000  MZ ..........ÿÿ..
0x00010  B800 0000 0000 0000 4000 0000 0000 0000  ¸.......@.......
0x00020  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x00030  0000 0000 0000 0000 0000 0000 E800 0000  ............è...
0x00040  0E1F BA0E 00B4 09CD 21B8 014C CD21 5468  ..º..´.Í!¸.LÍ!Th
0x00050  6973 2070 726F 6772 616D 2063 616E 6E6F  is program canno
0x00060  7420 6265 2072 756E 2069 6E20 444F 5320  t be run in DOS 
0x00070  6D6F 6465 2E0D 0D0A 2400 0000 0000 0000  mode....$.......
0x00080  C75E 5E5C 833F 300F 833F 300F 833F 300F  Ç^^\ ?0. ?0. ?0.
0x00090  A4F9 4B0F 863F 300F 833F 310F A83F 300F  ¤ùK. ?0. ?1.¨?0.
0x000A0  8A47 B30F 8D3F 300F 9D6D A50F 803F 300F   G³. ?0. m¥. ?0.
```

Duqu Keylogger

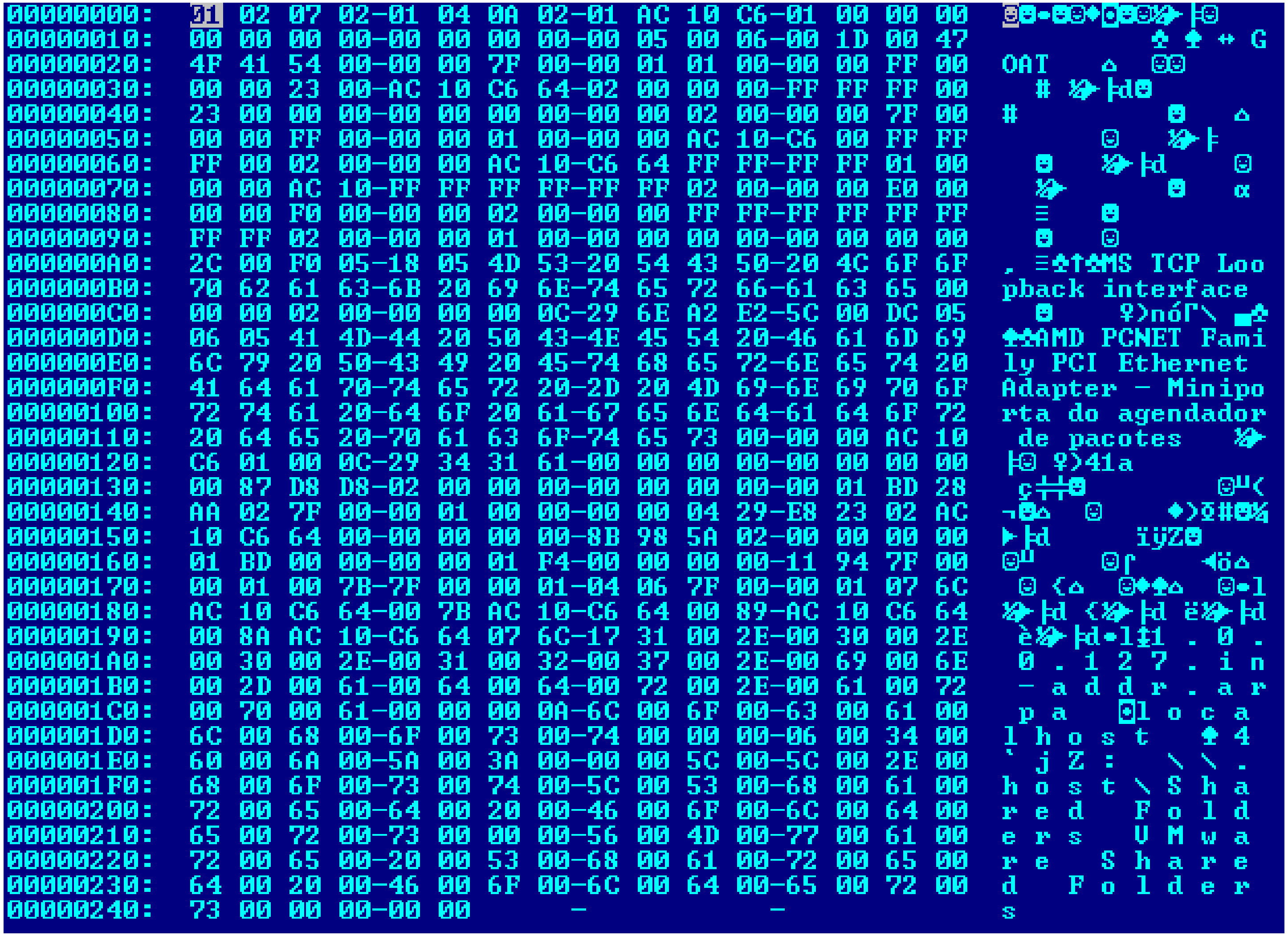
The Keylogger component is a standalone module. It was delivered via C&C Server to target after the initial infection.

It uses the same decryption routines as the other modules. It is capable of collecting different types of information from the target machine:

- Keystroke data
- Machine information (OS version, patches, machine name, users, etc)
- Process list
- Network information
- List shared folders
- List machines on the same network
- Screen shots

The Keylogger accepts command line parameter commands, and only works if the parameter “xxx” is the first parameter passed

Duqu Keylogger: Example of captured sensitive data



```
00000000:  01 02 07 02-01 04 0A 02-01 AC 10 C6-01 00 00 00   ☺☻•☻☺♦◙☻☺¼►╞☺   
00000010:  00 00 00 00-00 00 00 00-00 05 00 06-00 1D 00 47            ♣ ♠ ↔ G
00000020:  4F 41 54 00-00 00 7F 00-00 01 01 00-00 00 FF 00   OAT   ⌂  ☺☺     
00000030:  00 00 23 00-AC 10 C6 64-02 00 00 00-FF FF FF 00     # ¼►╞d☻       
00000040:  23 00 00 00-00 00 00 00-00 00 02 00-00 00 7F 00   #         ☻   ⌂ 
00000050:  00 00 FF 00-00 00 01 00-00 00 AC 10-C6 00 FF FF         ☺   ¼►╞   
00000060:  FF 00 02 00-00 00 AC 10-C6 64 FF FF-FF FF 01 00     ☻   ¼►╞d    ☺ 
00000070:  00 00 AC 10-FF FF FF FF-FF FF 02 00-00 00 E0 00     ¼►      ☻   α 
00000080:  00 00 F0 00-00 00 02 00-00 00 FF FF-FF FF FF FF     ≡   ☻         
00000090:  FF FF 02 00-00 00 01 00-00 00 00 00-00 00 00 00     ☻   ☺         
000000A0:  2C 00 F0 05-18 05 4D 53-20 54 43 50-20 4C 6F 6F   , ≡♣↑♣MS TCP Loo
000000B0:  70 62 61 63-6B 20 69 6E-74 65 72 66-61 63 65 00   pback interface 
000000C0:  00 00 02 00-00 00 00 0C-29 6E A2 E2-5C 00 DC 05     ☻    ♀)nóΓ\ ▄♣
000000D0:  06 05 41 4D-44 20 50 43-4E 45 54 20-46 61 6D 69   ♠♣AMD PCNET Fami
000000E0:  6C 79 20 50-43 49 20 45-74 68 65 72-6E 65 74 20   ly PCI Ethernet 
000000F0:  41 64 61 70-74 65 72 20-2D 20 4D 69-6E 69 70 6F   Adapter - Minipo
00000100:  72 74 61 20-64 6F 20 61-67 65 6E 64-61 64 6F 72   rta do agendador
00000110:  20 64 65 20-70 61 63 6F-74 65 73 00-00 00 AC 10    de pacotes   ¼►
00000120:  C6 01 00 0C-29 34 31 61-00 00 00 00-00 00 00 00   ╞☺ ♀)41a        
00000130:  00 87 D8 D8-02 00 00 00-00 00 00 00-00 01 BD 28    ç╪╪☻        ☺╜(
00000140:  AA 02 7F 00-00 01 00 00-00 00 04 29-E8 23 02 AC   ¬☻⌂  ☺    ♦)Φ#☻¼
00000150:  10 C6 64 00-00 00 00 00-8B 98 5A 02-00 00 00 00   ►╞d     ïÿZ☻    
00000160:  01 BD 00 00-00 00 01 F4-00 00 00 00-11 94 7F 00   ☺╜    ☺⌠    ◄ö⌂ 
00000170:  00 01 00 7B-7F 00 00 01-04 06 7F 00-00 01 07 6C    ☺ {⌂  ☺♦♠⌂  ☺•l
00000180:  AC 10 C6 64-00 7B AC 10-C6 64 00 89-AC 10 C6 64   ¼►╞d {¼►╞d ë¼►╞d
00000190:  00 8A AC 10-C6 64 07 6C-17 31 00 2E-00 30 00 2E    è¼►╞d•l↨1 . 0 .
000001A0:  00 30 00 2E-00 31 00 32-00 37 00 2E-00 69 00 6E    0 . 1 2 7 . i n
000001B0:  00 2D 00 61-00 64 00 64-00 72 00 2E-00 61 00 72    - a d d r . a r
000001C0:  00 70 00 61-00 00 00 0A-6C 00 6F 00-63 00 61 00    p a   ◙l o c a 
000001D0:  6C 00 68 00-6F 00 73 00-74 00 00 00-06 00 34 00   l h o s t   ♠ 4 
000001E0:  60 00 6A 00-5A 00 3A 00-00 00 5C 00-5C 00 2E 00   ` j Z :   \ \ . 
000001F0:  68 00 6F 00-73 00 74 00-5C 00 53 00-68 00 61 00   h o s t \ S h a 
00000200:  72 00 65 00-64 00 20 00-46 00 6F 00-6C 00 64 00   r e d   F o l d 
00000210:  65 00 72 00-73 00 00 00-56 00 4D 00-77 00 61 00   e r s   V M w a 
00000220:  72 00 65 00-20 00 53 00-68 00 61 00-72 00 65 00   r e   S h a r e 
00000230:  64 00 20 00-46 00 6F 00-6C 00 64 00-65 00 72 00   d   F o l d e r 
00000240:  73 00 00 00-00 00      -           -              s
```

Duqu Network Activities

Once the DLL module is started, the known variants will try to contact the command and control server at the address below on tcp ports 80 and 443 (http/https)

- 206.183.111.97 (India)

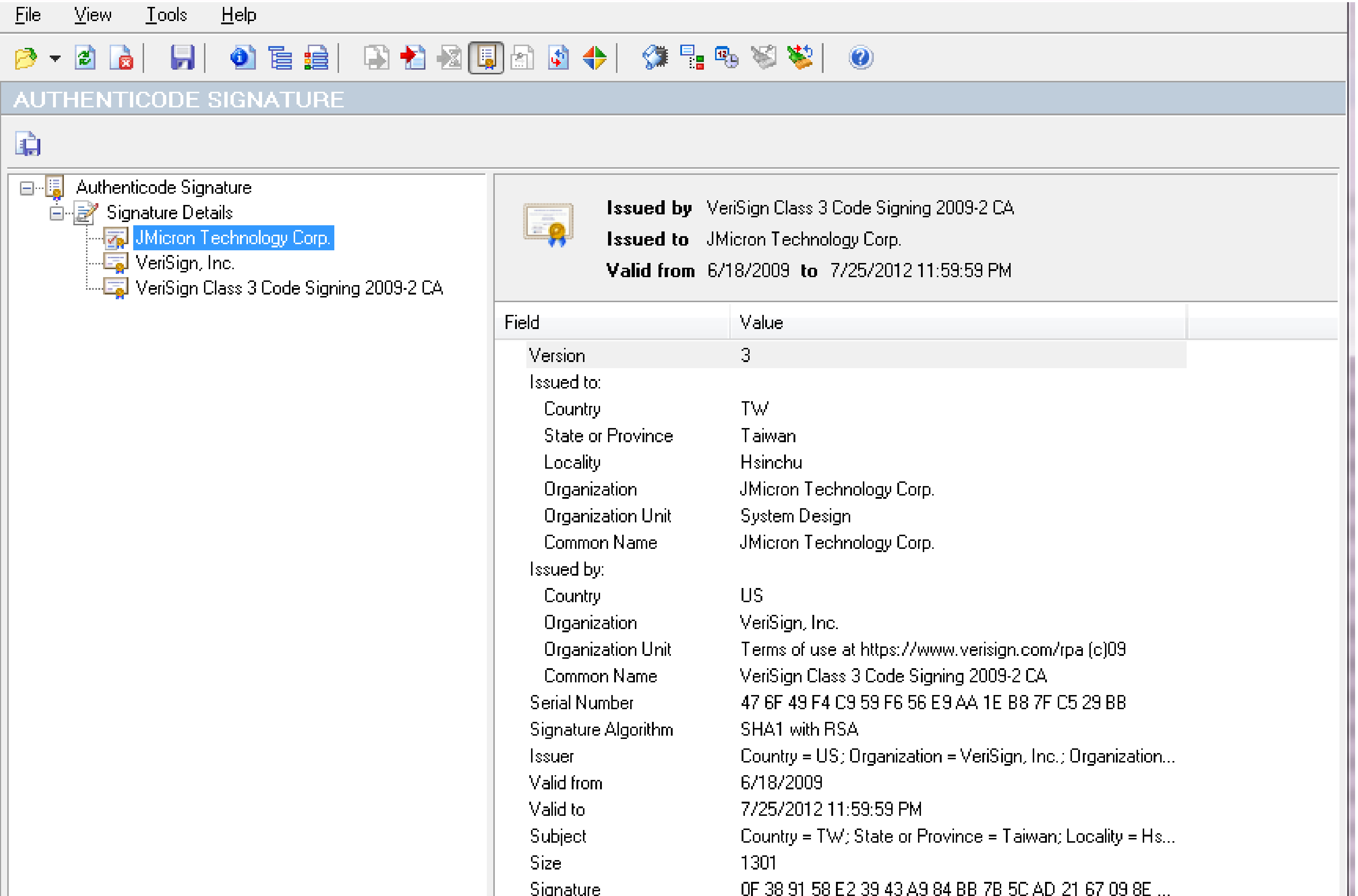
The request may look like the one below:

```
GET / HTTP/1.1
Cookie: PHPSESSID=o5ukre1ul0q6i2il1ij3ghi0j1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US;
rv:1.9.2.9) Gecko/20100824 Firefox/3.6.9 (.NET CLR 3.5.30729)
Host: x.x.x.x
```

The PHPSESSID is an encrypted message sent to the command and control server.

The User-Agent is hardcoded and may be used to identify machines infected with this malware.

Jmicron Certificate valid from 06/2009- Used to sign Stuxnet driver



AUTHENTICODE SIGNATURE

- Authenticode Signature
  - Signature Details
    - JMicron Technology Corp.
    - VeriSign, Inc.
    - VeriSign Class 3 Code Signing 2009-2 CA

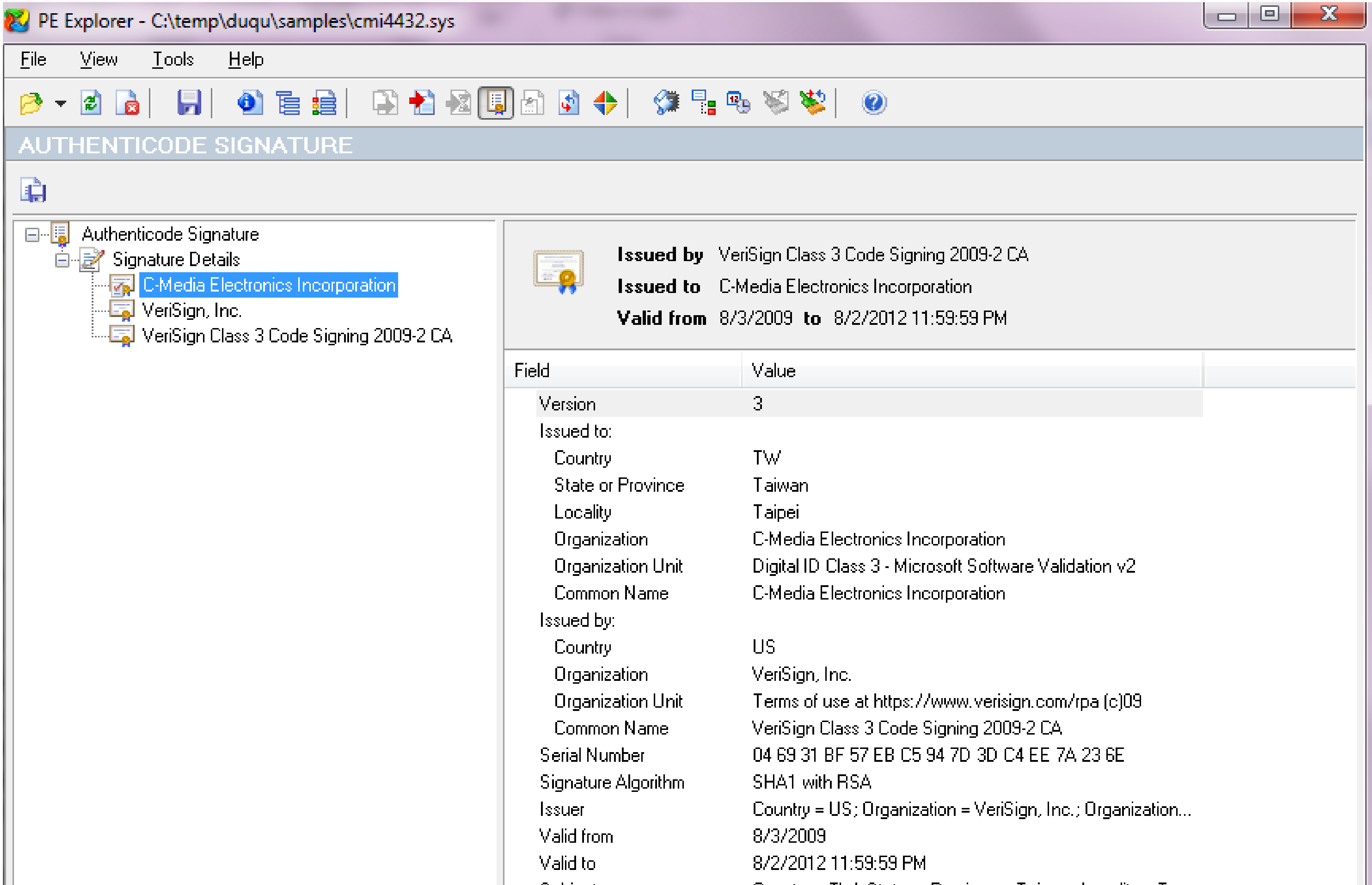
Issued by VeriSign Class 3 Code Signing 2009-2 CA

Issued to JMicron Technology Corp.

Valid from 6/18/2009 **to** 7/25/2012 11:59:59 PM

Field	Value
Version	3
Issued to:	
Country	TW
State or Province	Taiwan
Locality	Hsinchu
Organization	JMicron Technology Corp.
Organization Unit	System Design
Common Name	JMicron Technology Corp.
Issued by:	
Country	US
Organization	VeriSign, Inc.
Organization Unit	Terms of use at https://www.verisign.com/rpa (c)09
Common Name	VeriSign Class 3 Code Signing 2009-2 CA
Serial Number	47 6F 49 F4 C9 59 F6 56 E9 AA 1E B8 7F C5 29 BB
Signature Algorithm	SHA1 with RSA
Issuer	Country = US; Organization = VeriSign, Inc.; Organization...
Valid from	6/18/2009
Valid to	7/25/2012 11:59:59 PM
Subject	Country = TW; State or Province = Taiwan; Locality = Hs...
Size	1301
Signature	0F 38 91 58 E2 39 43 A9 84 BB 7B 5C AD 21 67 09 8E ...

C-Media’s Certificate valid from 08/03/2009- (used to sign one of the known variants of Duqu)



PE Explorer - C:\temp\duqu\samples\cmi4432.sys

- Authenticode Signature
  - Signature Details
    - C-Media Electronics Incorporation
    - VeriSign, Inc.
    - VeriSign Class 3 Code Signing 2009-2 CA

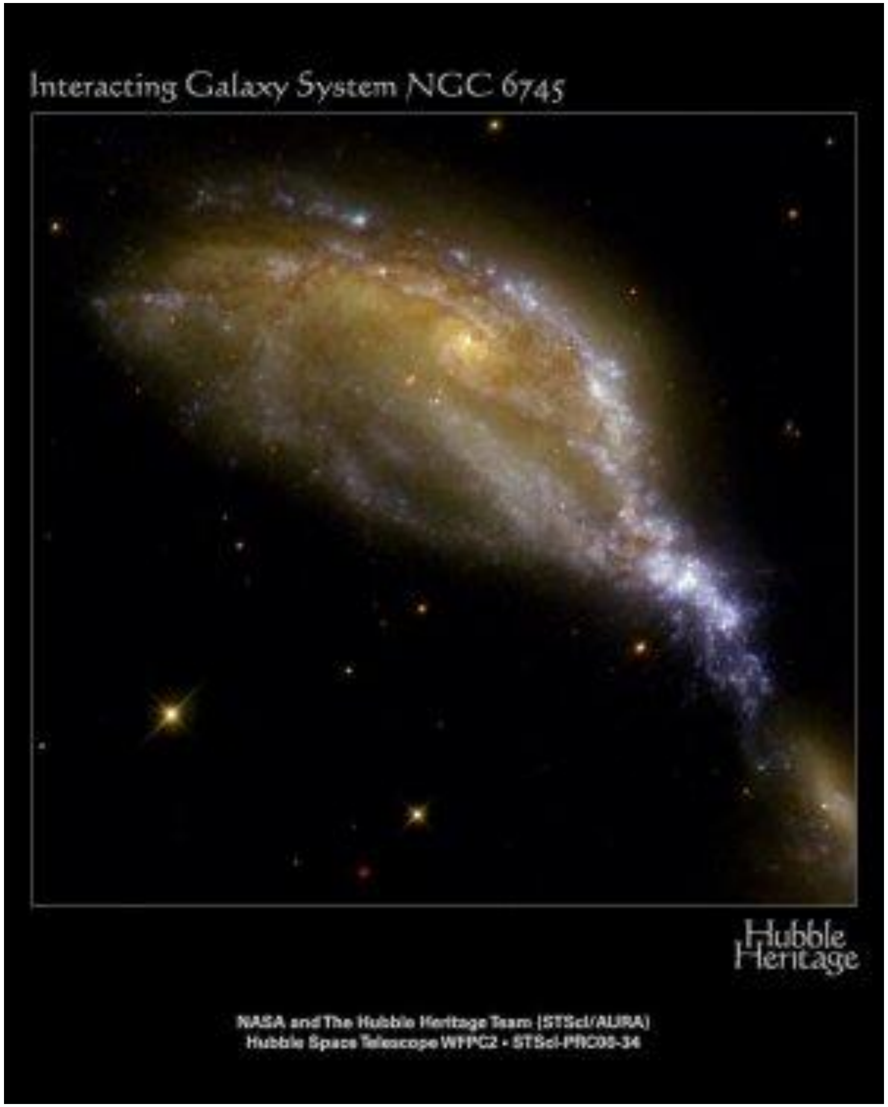
Issued by VeriSign Class 3 Code Signing 2009-2 CA

Issued to C-Media Electronics Incorporation

Valid from 8/3/2009 **to** 8/2/2012 11:59:59 PM

Field	Value
Version	3
Issued to:	
Country	TW
State or Province	Taiwan
Locality	Taipei
Organization	C-Media Electronics Incorporation
Organization Unit	Digital ID Class 3 - Microsoft Software Validation v2
Common Name	C-Media Electronics Incorporation
Issued by:	
Country	US
Organization	VeriSign, Inc.
Organization Unit	Terms of use at https://www.verisign.com/rpa (c)09
Common Name	VeriSign Class 3 Code Signing 2009-2 CA
Serial Number	04 69 31 BF 57 EB C5 94 7D 3D C4 EE 7A 23 6E
Signature Algorithm	SHA1 with RSA
Issuer	Country = US; Organization = VeriSign, Inc.; Organization...
Valid from	8/3/2009
Valid to	8/2/2012 11:59:59 PM

NGC 6745 – JPG picture referenced in Duqu


Interacting Galaxy System NGC 6745
Hubble Heritage
NASA and The Hubble Heritage Team (STScI/AURA)
Hubble Space Telescope WFPC2 • STScI-PRC00-34

Best Practices Against Duqu

- AV Signatures
- Application Whitelisting
- DeepSafe- McAfee/Intel techology targeting rootkits

Acknowledgments – Further Reading

- McAfee Labs Blogs
- Personal communication: Rob Meyers, Liam O Murchu, Guilherme Venere and Stuart McClure
- McAfee Threats Report
- Symantec Stuxnet File / Symantec Internet Security Threat Report
- Ralph Langner on Stuxnet
- Krebs on Security Blog
- “The Art of Computer Virus Research and Defense”