The Era of Cyber Espionage & Cyber Warfare
(Case Study: Stuxnet)

2012.7 Forensic Insight

Kevin Koo
(kevinkoo001@gmail.com)

개요

- The Era of Cyber Espionage and Warfare
- [TED] Cracking *Stuxnet*, a 21st-century cyber weapon
- Demystifying Stuxnet
  Overview
  Brief Statistics
  Architecture
  Analysis in details
- [TED] Fighting viruses, defending the net
- Conclusion

Voice of concerns

- ✓ Forbes: The Flame Cyber Espionage Attack: Five Questions We Should Ask http://www.forbes.com/sites/johnvillasenor/2012/06/04/the-flame-cyber-espionage-attack-five-questions-we-should-ask/
  - What is the true scope of cyberattacks going on today?
  - Will infection with some form of malware soon become the rule rather than the exception?
  - In the future, will nations outsource domestic espionage?
  - Is forging digital certificates fair game for nation states?
  - Is Flame one more reason to increase cybersecurity spending?

[TED] Cracking *Stuxnet*, a 21st-century cyber weapon

Ralph Langner's Speech: Cracking *Stuxnet*

- ✓ German control system security consultant
- ✓ http://www.langner.com/en/
- ✓ http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/
- ✓ [2011.3] http://www.youtube.com/watch?v=CS01Hmjv1pQ (10m 40s)

Overview

Stuxnet: APT Attack

Who did it?

Relative Resources

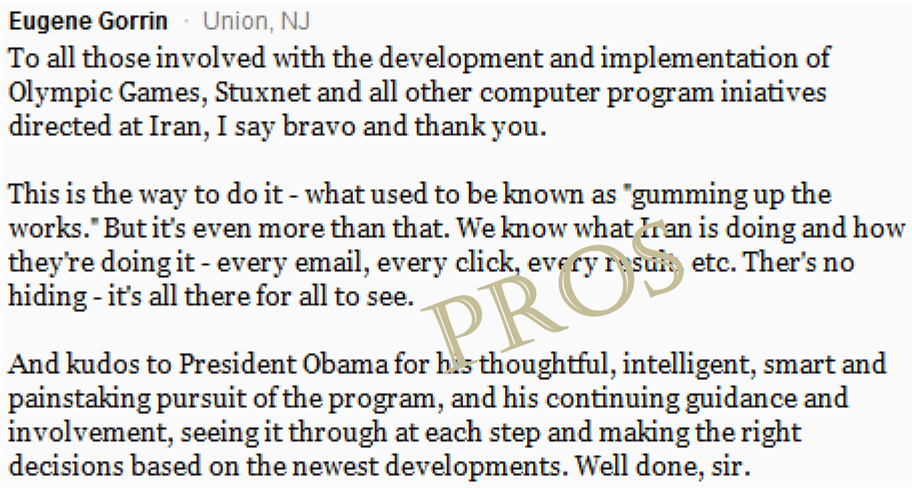
Analysis
(Ref#1) [Symantec] W32.Stuxnet Dossier
(Ref#2) [ESET] Stuxnet_Under_the_Microscope
(Ref#3) [SecureView] Magzine 2nd quarter in 2011

Overview: APT Attack

- ✓ Highly Advanced Persistent Threat (지능형 지속가능 위협)
- ✓ Large and complex chunk
- ✓ Who did it? Or Who could do this?
  → Iran 핵발전소 겨냥하여 원심분리기 중단
  → 목표 시스템은 독일의 지멘스(siemens) 사의 원심분리기
  → Five zero-day vulnerabilities and one known for Windows OS
  → Target이 없으면 동작하지 않도록 설계
  → 최소 10개 이상의 팀이 수 개월~수 년간 치밀하게 준비 필요
  → 자금확보는?
- ✓ http://en.wikipedia.org/wiki/Stuxnet
- ✓ Malware 종합세트(?)
  Hooking, Injection, Rootkit, 0-day, Virus&Worm, C&C, Application Hacking, …

Overview: WHO DID IT?

- ✓ It turns out that the attack was led by the US, code-named "Olympic Games" (2012.6.1) http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
- ✓ Imagine what happened if:
  → Power grid were crashed
  → Air control system was compromised
  → National intelligence was taken over
  → Military weapon was manipulated: nuclear weapons, intercontinental missiles

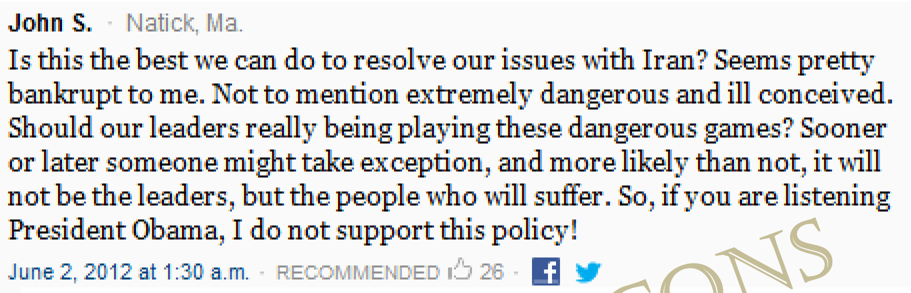


Eugene Gorrin · Union, NJ

To all those involved with the development and implementation of Olympic Games, Stuxnet and all other computer program iniatives directed at Iran, I say bravo and thank you.

This is the way to do it - what used to be known as "gumming up the works." But it's even more than that. We know what Iran is doing and how they're doing it - every email, every click, every result, etc. Ther's no hiding - it's all there for all to see.

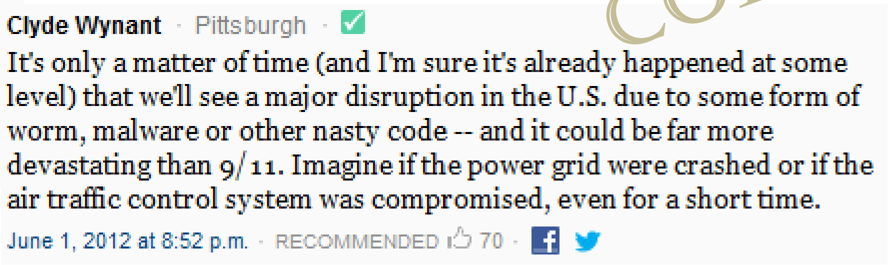
And kudos to President Obama for his thoughtful, intelligent, smart and painstaking pursuit of the program, and his continuing guidance and involvement, seeing it through at each step and making the right decisions based on the newest developments. Well done, sir.



John S. · Natick, Ma.

Is this the best we can do to resolve our issues with Iran? Seems pretty bankrupt to me. Not to mention extremely dangerous and ill conceived. Should our leaders really being playing these dangerous games? Sooner or later someone might take exception, and more likely than not, it will not be the leaders, but the people who will suffer. So, if you are listening President Obama, I do not support this policy!

June 2, 2012 at 1:30 a.m. · RECOMMENDED 26 ·



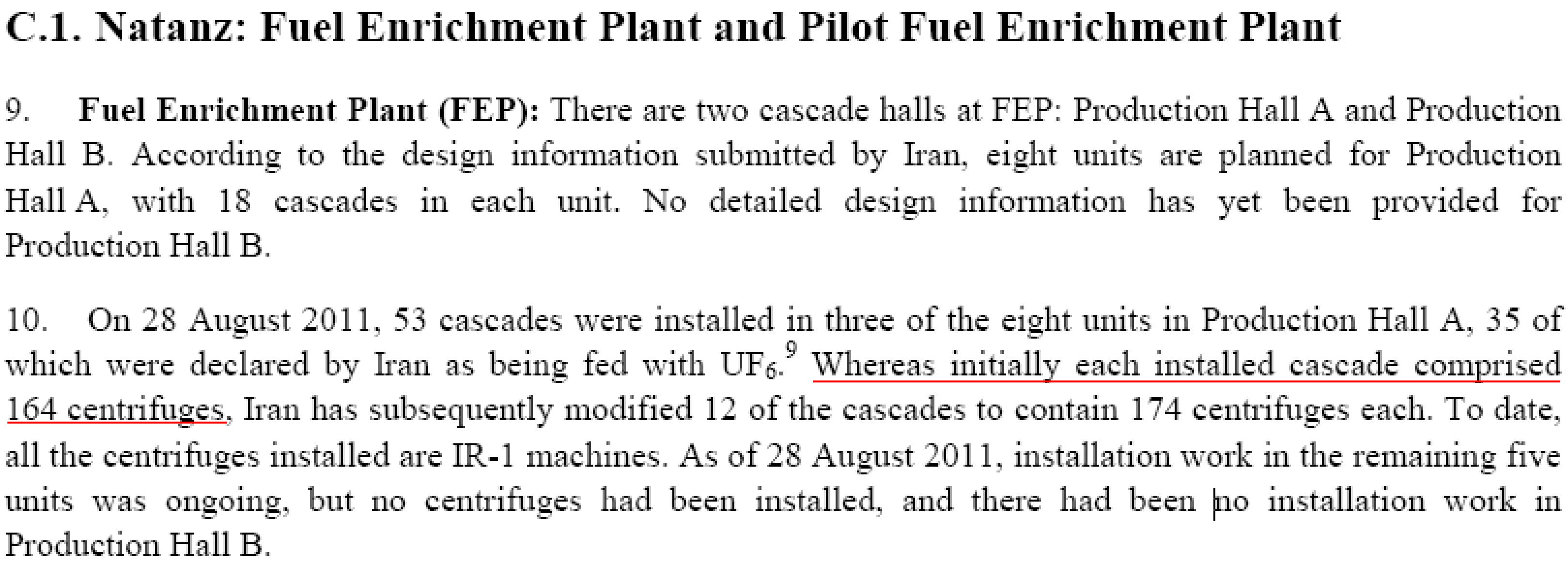
Clyde Wynant · Pittsburgh · ✓

It's only a matter of time (and I'm sure it's already happened at some level) that we'll see a major disruption in the U.S. due to some form of worm, malware or other nasty code -- and it could be far more devastating than 9/11. Imagine if the power grid were crashed or if the air traffic control system was compromised, even for a short time.

June 1, 2012 at 8:52 p.m. · RECOMMENDED 70 ·

Overview: Relative Resources (1)

- ✓ 국제 원자력 기구(IAEA, International Atomic Energy Agency)
  Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran (2/9/2011)



C.1. Natanz: Fuel Enrichment Plant and Pilot Fuel Enrichment Plant

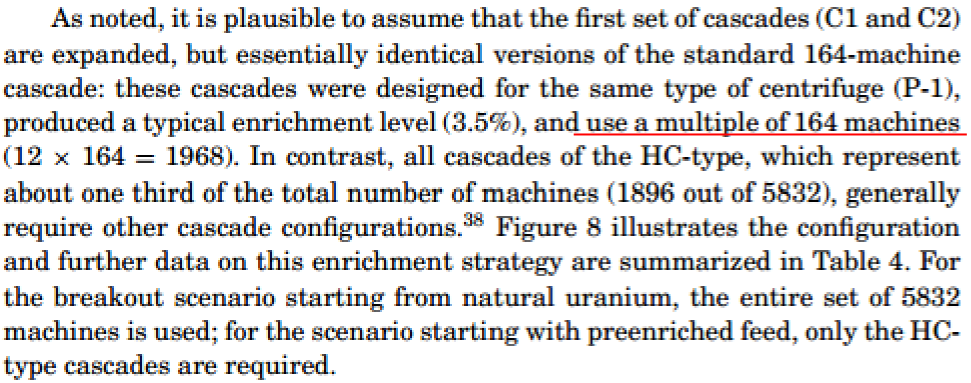
9. **Fuel Enrichment Plant (FEP):** There are two cascade halls at FEP: Production Hall A and Production Hall B. According to the design information submitted by Iran, eight units are planned for Production Hall A, with 18 cascades in each unit. No detailed design information has yet been provided for Production Hall B.

10. On 28 August 2011, 53 cascades were installed in three of the eight units in Production Hall A, 35 of which were declared by Iran as being fed with UF_6.[9] Whereas initially each installed cascade comprised 164 centrifuges, Iran has subsequently modified 12 of the cascades to contain 174 centrifuges each. To date, all the centrifuges installed are IR-1 machines. As of 28 August 2011, installation work in the remaining five units was ongoing, but no centrifuges had been installed, and there had been no installation work in Production Hall B.

- ✓ 지멘스사의 제어 시스템 (Siemens control solutions for utilities)
  http://www.buildingtechnologies.siemens.com/bt/global/en/market-specific-solutions/utilities/control-room/Pages/control-room.aspx

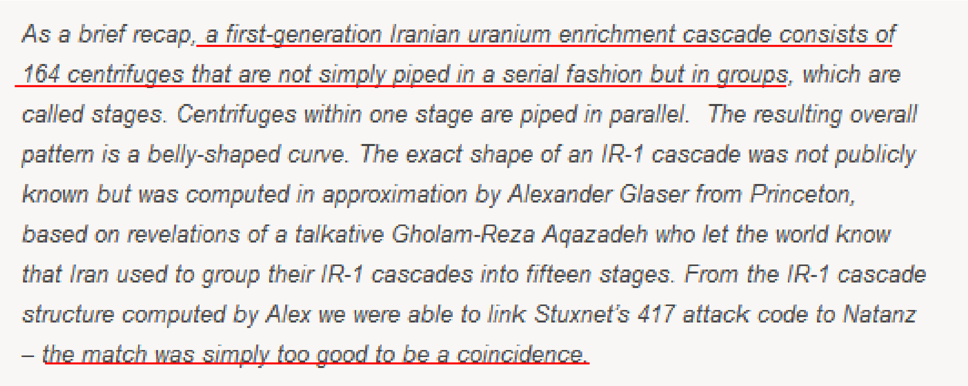
Overview: Relative Resources (2)

- ✓ Princeton 대학논문(2008.6)
  Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (우라늄 농축 가스 원심분리 특성과 핵무기 증설 관련성)
  http://www.princeton.edu/sgs/publications/sgs/archive/16-1-Glaser.pdf
  Cascade Interconnection with Partial Reconfiguration 부분 참조



As noted, it is plausible to assume that the first set of cascades (C1 and C2) are expanded, but essentially identical versions of the standard 164-machine cascade: these cascades were designed for the same type of centrifuge (P-1), produced a typical enrichment level (3.5%), and use a multiple of 164 machines (12 × 164 = 1968). In contrast, all cascades of the HC-type, which represent about one third of the total number of machines (1896 out of 5832), generally require other cascade configurations.[38] Figure 8 illustrates the configuration and further data on this enrichment strategy are summarized in Table 4. For the breakout scenario starting from natural uranium, the entire set of 5832 machines is used; for the scenario starting with preenriched feed, only the HC-type cascades are required.

- ✓ Mosaic theory: 보안 분석에서 기업 정보를 수집하는 방식
  http://securityaffairs.co/wordpress/566/cyber-crime/from-the-mosaic-theory-to-the-stuxnet-case.html



As a brief recap, a first-generation Iranian uranium enrichment cascade consists of 164 centrifuges that are not simply piped in a serial fashion but in groups, which are called stages. Centrifuges within one stage are piped in parallel. The resulting overall pattern is a belly-shaped curve. The exact shape of an IR-1 cascade was not publicly known but was computed in approximation by Alexander Glaser from Princeton, based on revelations of a talkative Gholam-Reza Aqazadeh who let the world know that Iran used to group their IR-1 cascades into fifteen stages. From the IR-1 cascade structure computed by Alex we were able to link Stuxnet's 417 attack code to Natanz – the match was simply too good to be a coincidence.

Overview: Analysis

- ✓ Target: a specific industrial control system (특정 산업 통제 시스템)
- ✓ **분석 보고서**

  [ESET]
  http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

  [Symantec]
  http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

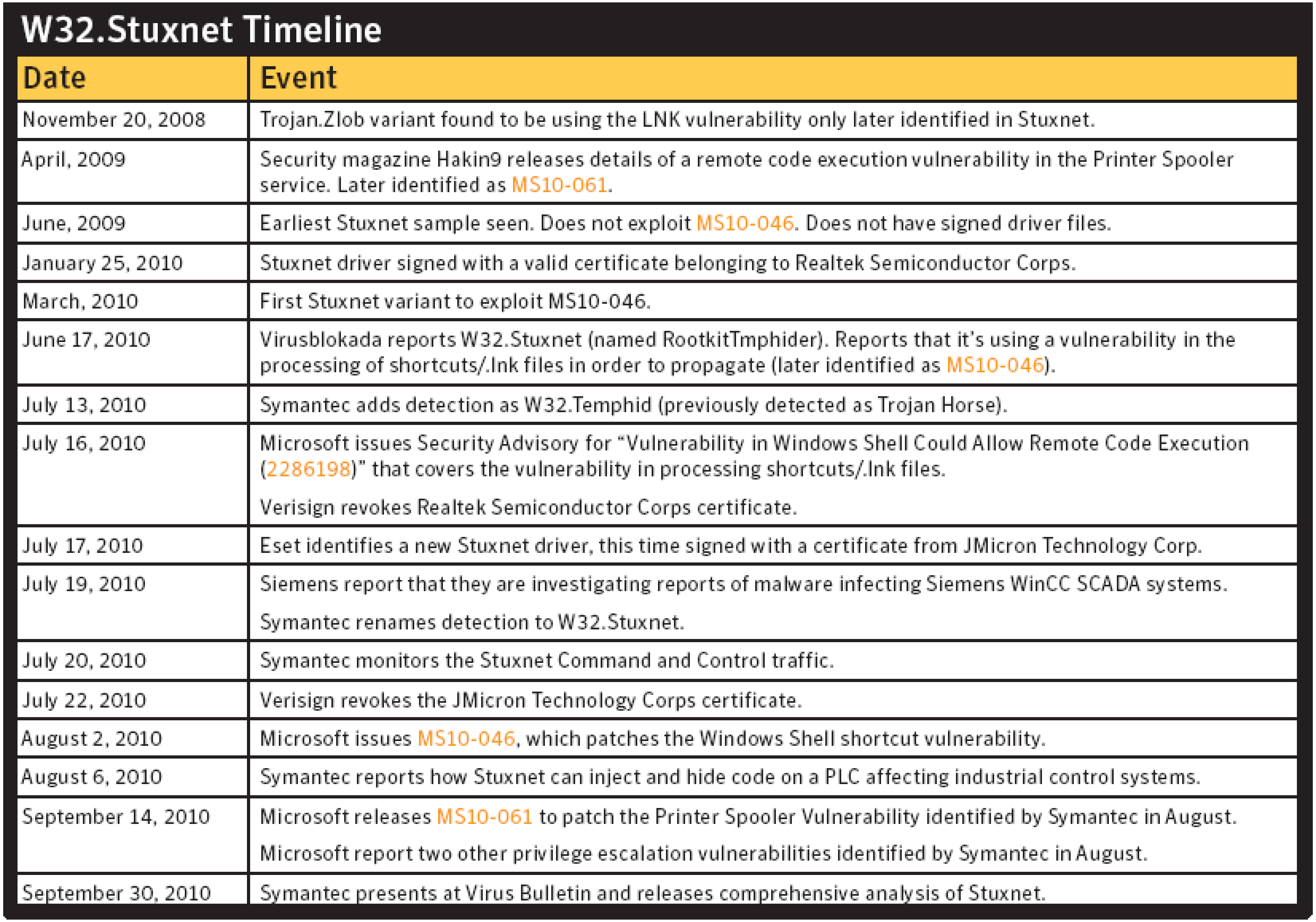
- ✓ Three Main Steps

  (1) Windows Infection using zero-day vulnerabilities:

  Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (MS08-067)
  Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (MS10-046)
  Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (MS10-061)
  Microsoft Windows Win32k.sys Local Privilege Escalation vulnerability (MS10-073)
  Microsoft Windows Task Scheduler Escalation of Privilege vulnerability (MS10-092)

  (2) Step7 Software Infection: Siemens' WinCC/PCS 7 SCADA control software

  (3) PLC(Programmable Logical Computer) infection

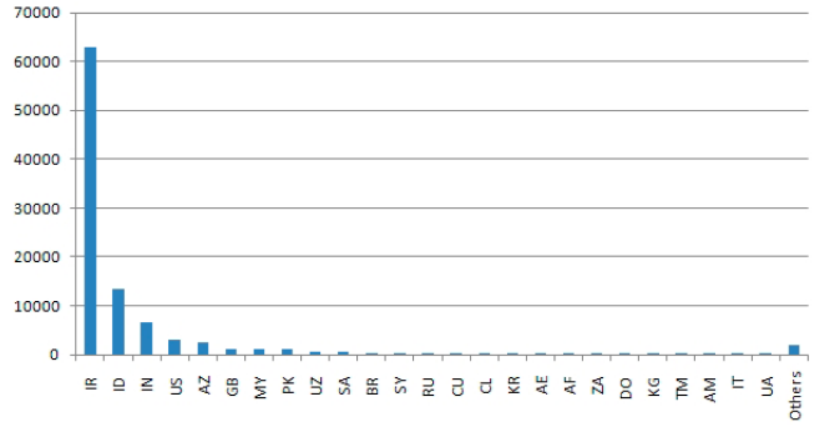


W32.Stuxnet Timeline

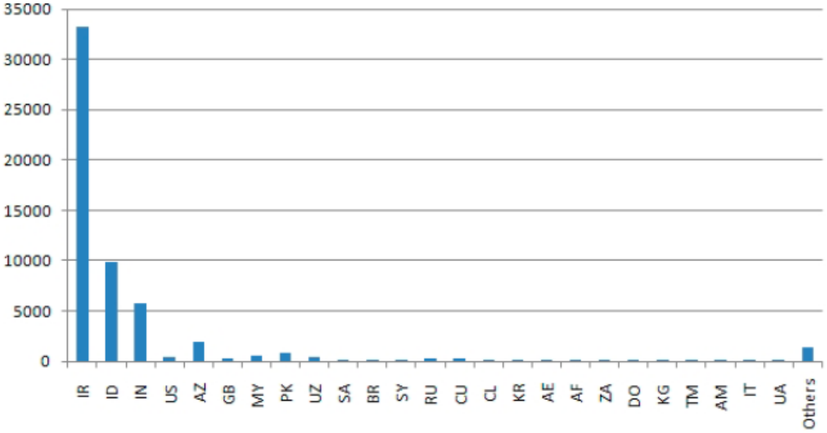
Date	Event
November 20, 2008	Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.
April, 2009	Security magazine Hakin9 releases details of a remote code execution vulnerability in the Printer Spooler service. Later identified as MS10-061.
June, 2009	Earliest Stuxnet sample seen. Does not exploit MS10-046. Does not have signed driver files.
January 25, 2010	Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corps.
March, 2010	First Stuxnet variant to exploit MS10-046.
June 17, 2010	Virusblokada reports W32.Stuxnet (named RootkitTmphider). Reports that it's using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).
July 13, 2010	Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).
July 16, 2010	Microsoft issues Security Advisory for "Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)" that covers the vulnerability in processing shortcuts/.lnk files. Verisign revokes Realtek Semiconductor Corps certificate.
July 17, 2010	Eset identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp.
July 19, 2010	Siemens report that they are investigating reports of malware infecting Siemens WinCC SCADA systems. Symantec renames detection to W32.Stuxnet.
July 20, 2010	Symantec monitors the Stuxnet Command and Control traffic.
July 22, 2010	Verisign revokes the JMicron Technology Corps certificate.
August 2, 2010	Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.
August 6, 2010	Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems.
September 14, 2010	Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August. Microsoft report two other privilege escalation vulnerabilities identified by Symantec in August.
September 30, 2010	Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.

Brief Statistics

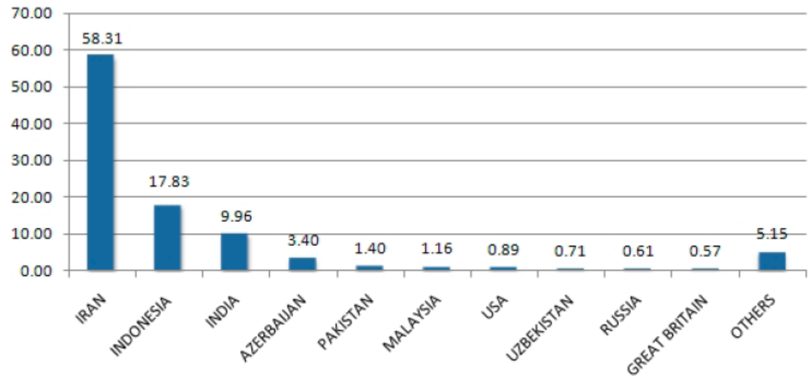
Infected Hosts



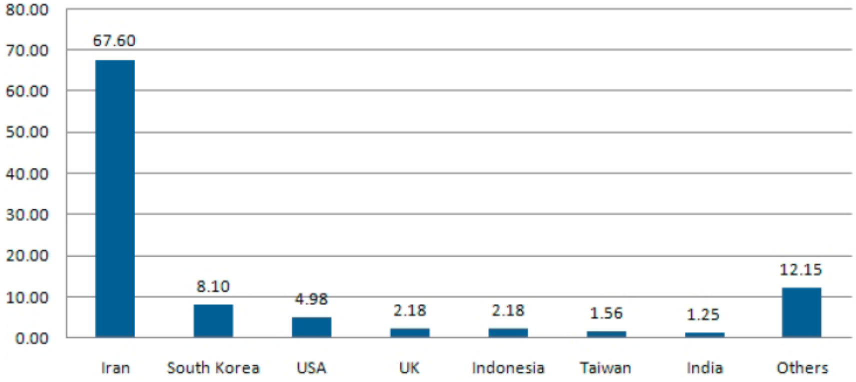
Infected Organizations (By WAN IP)



Geographic Distribution of Infections



Percentage of Stuxnet infected Hosts with Siemens Software installed



- **Architecture**

  Overview
  Exports & Resources
  Techniques to use

Architecture - Overview

* Stuxnet = a wrapper

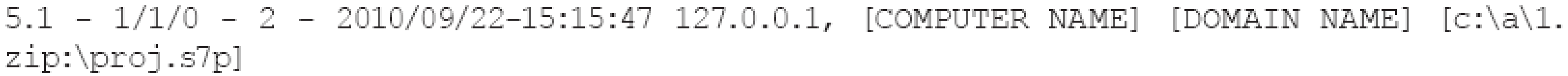
→ stored in a stub section

→ Consists of
: large .dll file

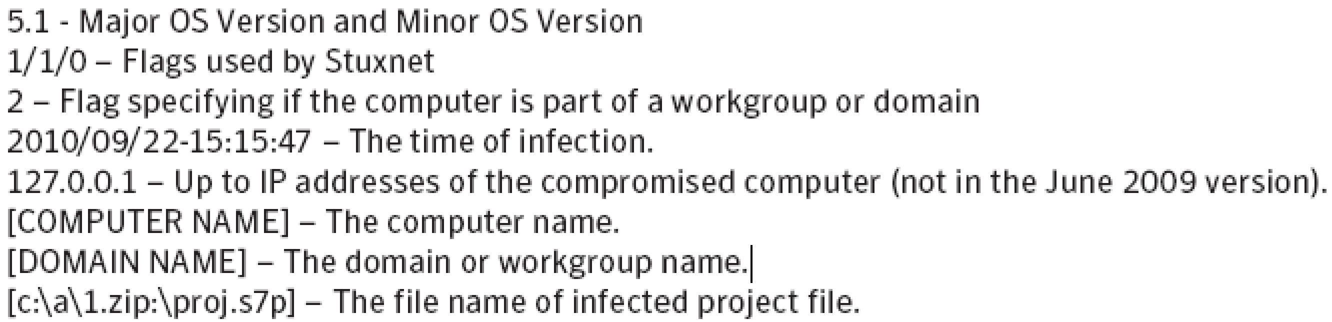
(1) A pointer to the original stub section is passed to exports as a parameter

(2) How to call exports in the main .dll file
→ Loading the .dll file into memory and calling an export **directly**
→ Reading an **executable template** from its own resources,
populate the template with appropriate data

: two encrypted configuration file

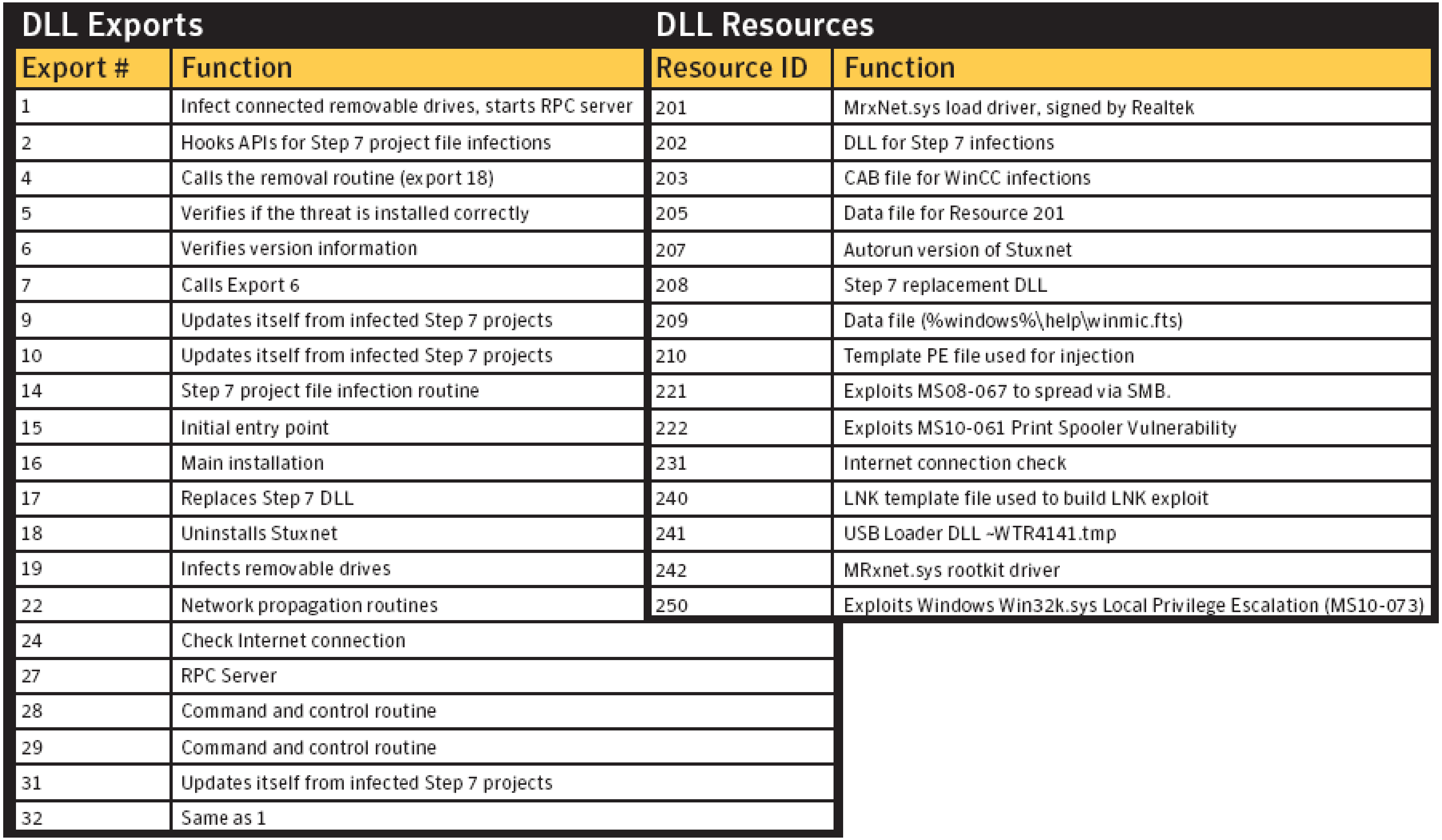


```
5.1 - 1/1/0 - 2 - 2010/09/22-15:15:47 127.0.0.1, [COMPUTER NAME] [DOMAIN NAME] [c:\a\1.
zip:\proj.s7p]
```



5.1 - Major OS Version and Minor OS Version
1/1/0 – Flags used by Stuxnet
2 – Flag specifying if the computer is part of a workgroup or domain
2010/09/22-15:15:47 – The time of infection.
127.0.0.1 – Up to IP addresses of the compromised computer (not in the June 2009 version).
[COMPUTER NAME] – The computer name.
[DOMAIN NAME] – The domain or workgroup name.
[c:\a\1.zip:\proj.s7p] – The file name of infected project file.

Architecture – Exports & Resources



DLL Exports

Export #	Function
1	Infect connected removable drives, starts RPC server
2	Hooks APIs for Step 7 project file infections
4	Calls the removal routine (export 18)
5	Verifies if the threat is installed correctly
6	Verifies version information
7	Calls Export 6
9	Updates itself from infected Step 7 projects
10	Updates itself from infected Step 7 projects
14	Step 7 project file infection routine
15	Initial entry point
16	Main installation
17	Replaces Step 7 DLL
18	Uninstalls Stuxnet
19	Infects removable drives
22	Network propagation routines
24	Check Internet connection
27	RPC Server
28	Command and control routine
29	Command and control routine
31	Updates itself from infected Step 7 projects
32	Same as 1

DLL Resources

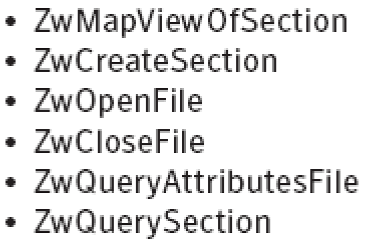
Resource ID	Function
201	MrxNet.sys load driver, signed by Realtek
202	DLL for Step 7 infections
203	CAB file for WinCC infections
205	Data file for Resource 201
207	Autorun version of Stuxnet
208	Step 7 replacement DLL
209	Data file (%windows%\help\winmic.fts)
210	Template PE file used for injection
221	Exploits MS08-067 to spread via SMB.
222	Exploits MS10-061 Print Spooler Vulnerability
231	Internet connection check
240	LNK template file used to build LNK exploit
241	USB Loader DLL ~WTR4141.tmp
242	MRxnet.sys rootkit driver
250	Exploits Windows Win32k.sys Local Privilege Escalation (MS10-073)

Architecture - Techniques to use: Hooking

* Bypassing behavior blocking when loading DLLs

→ Hooking ntdll.dll to monitor requests to load specially crafted file names
: KERNEL32.DLL.ASLR.[HEXADECIMAL] or SHELL32.DLL.ASLR.[HEXADECIMAL]

→ Hooked functions

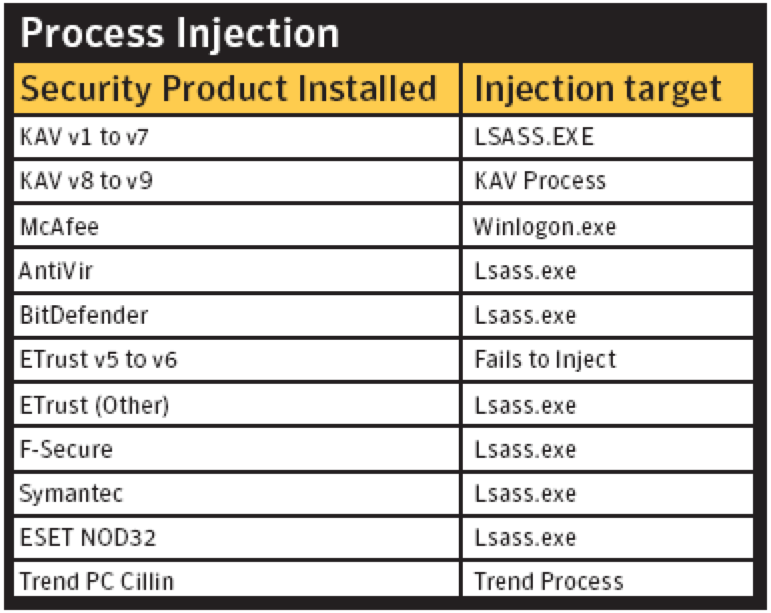


- ZwMapViewOfSection
- ZwCreateSection
- ZwOpenFile
- ZwCloseFile
- ZwQueryAttributesFile
- ZwQuerySection

Architecture - Techniques to use: Process Injection

* Keep injected code in the trusted process

* Instruct the trusted process to inject the code into another currently running process



Process Injection

Security Product Installed	Injection target
KAV v1 to v7	LSASS.EXE
KAV v8 to v9	KAV Process
McAfee	Winlogon.exe
AntiVir	Lsass.exe
BitDefender	Lsass.exe
ETrust v5 to v6	Fails to Inject
ETrust (Other)	Lsass.exe
F-Secure	Lsass.exe
Symantec	Lsass.exe
ESET NOD32	Lsass.exe
Trend PC Cillin	Trend Process

Ref. Symantec W32.Stuxnet Dossier p.14

<Running trusted process>

- Kaspersky KAV (avp.exe)
- Mcafee (Mcshield.exe)
- AntiVir (avguard.exe)
- BitDefender (bdagent.exe)
- Etrust (UmxCfg.exe)
- F-Secure (fsdfwd.exe)
- Symantec (rtvscan.exe)
- Symantec Common Client (ccSvcHst.exe)
- Eset NOD32 (ekrn.exe)
- Trend Pc-Cillin (tmpproxy.exe)

<Registry>

- KAV v6 to v9
- McAfee
- Trend PcCillin

<Potential Target Process>

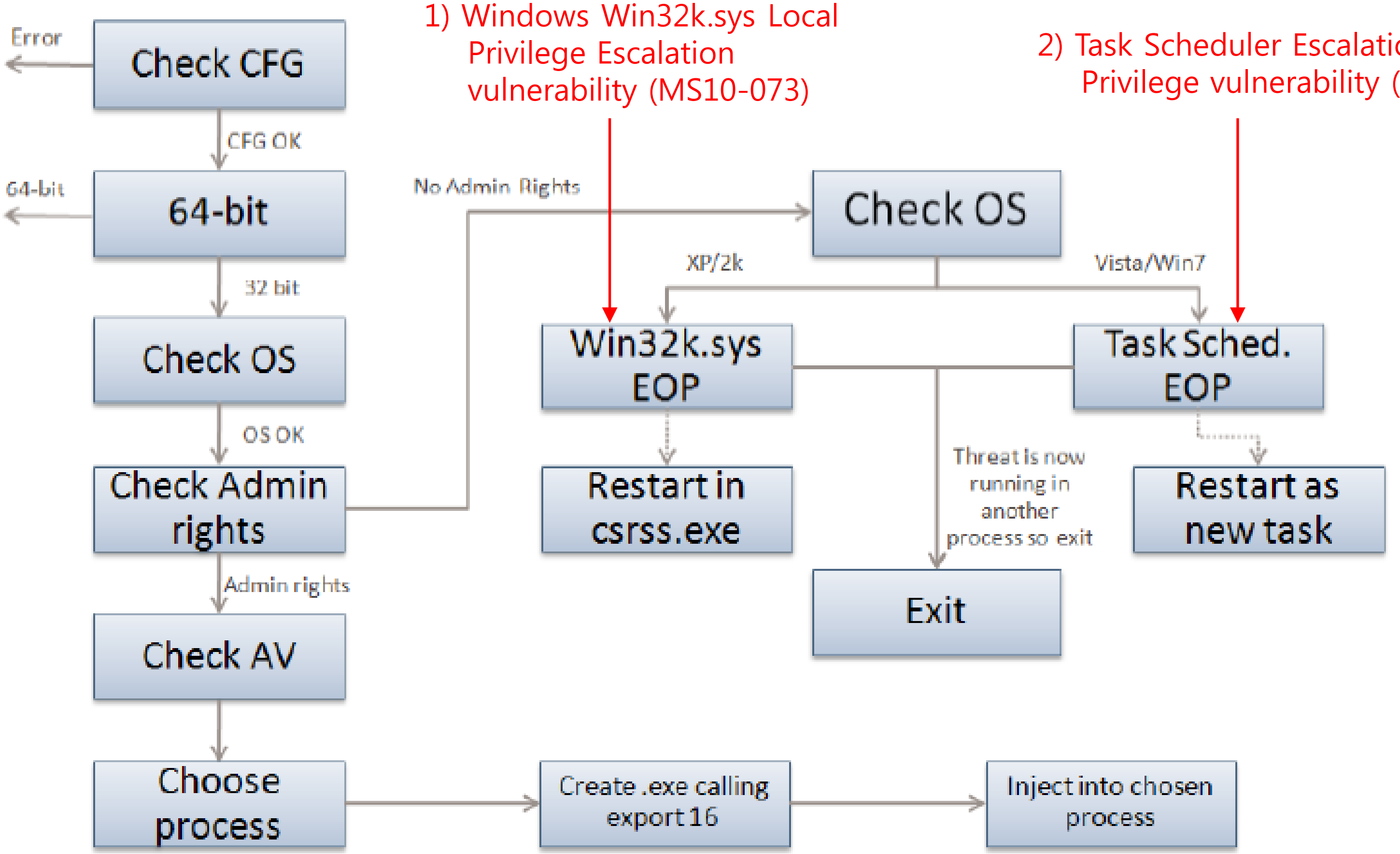
- Lsass.exe
- Winlogon.exe
- Svchost.exe
- The installed security product process

- **Analysis in details**

  Installation: Preparation, Injection
  Functionalities: Load point, C&C, Rootkit, Propagation
  Techniques to use

Analysis in details - Installation: Preparation

Control flow for export 15



1) Windows Win32k.sys Local Privilege Escalation vulnerability (MS10-073)

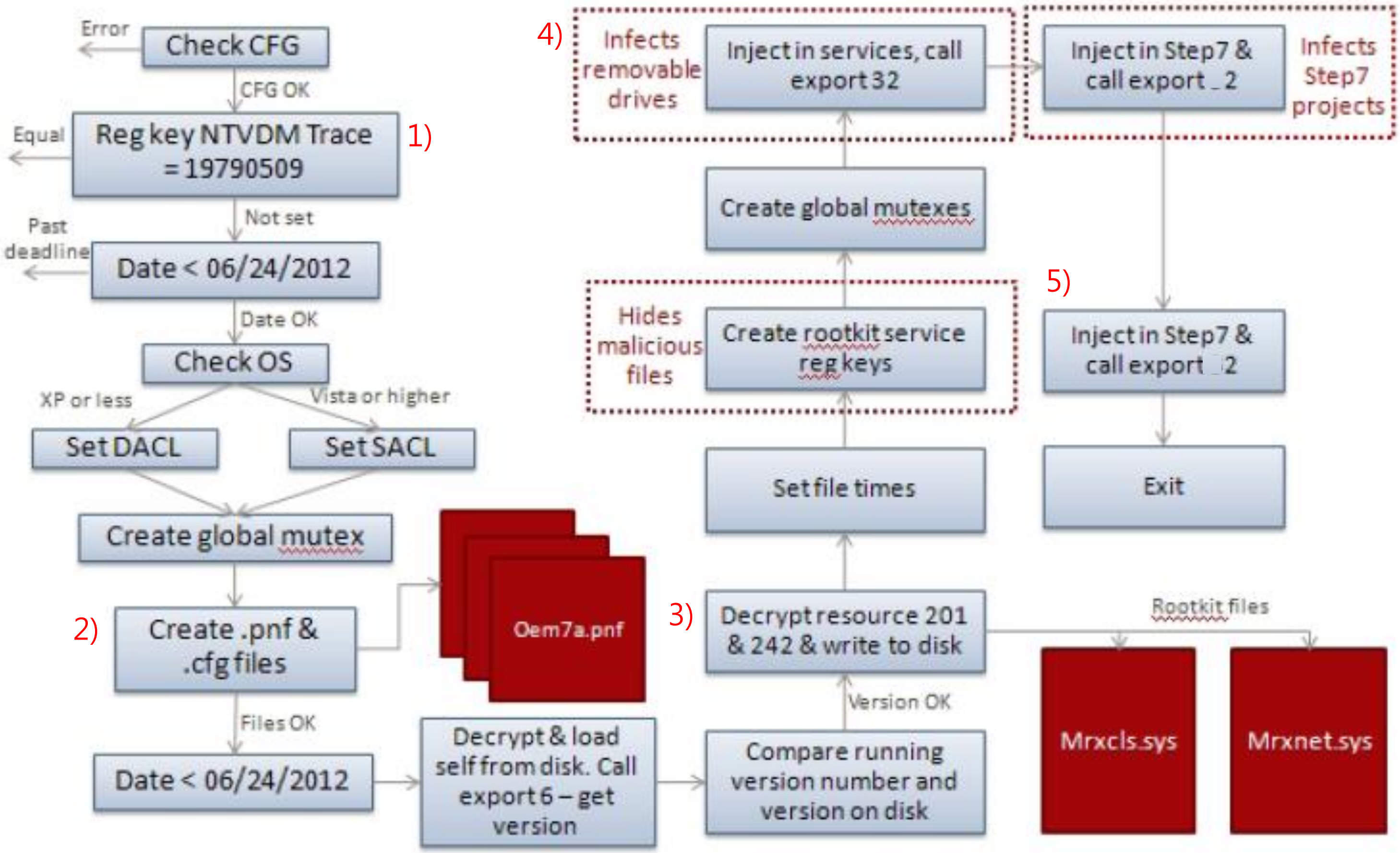
2) Task Scheduler Escalation of Privilege vulnerability (MS10-092)

Two privilege escalation (or Elevation of Privilege) vulnerabilities:

1) http://technet.microsoft.com/en-us/security/bulletin/MS10-073

2) http://technet.microsoft.com/en-us/security/bulletin/MS10-092

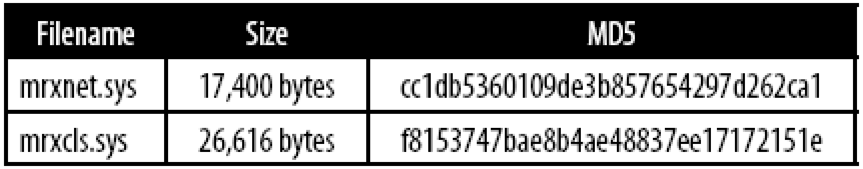
Analysis in details - Installation: Infection routine flow (Export 16)



1) HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩MS-DOS Emulation
2) %SystemDrive%₩inf₩mdmeric3.PNF, %SystemDrive%₩inf₩mdmcpq3.PNF, %SystemDrive%₩inf₩oem6C.PNF
3) %SystemDrive%drivers₩Mrxnet.sys, %SystemDrive%drivers₩Mrxcls.sys
4) Infecting newly connected removable drives and for starting the RPC server
5) Hooking APIs for Step 7 project file infections

Analysis in details - Functionality: Load Point

- ✓ Drops Resource 242 MrxCls.sys via Export 16
- ✓ The mrxcls.sys is a driver digitally signed with a compromised Realtek certificate. (suddenly revoked on July 16, 2010 by Verisign)
- ✓ File checksums



Filename	Size	MD5
mrxnet.sys	17,400 bytes	cc1db5360109de3b857654297d262ca1
mrxcls.sys	26,616 bytes	f8153747bae8b4ae48837ee17172151e

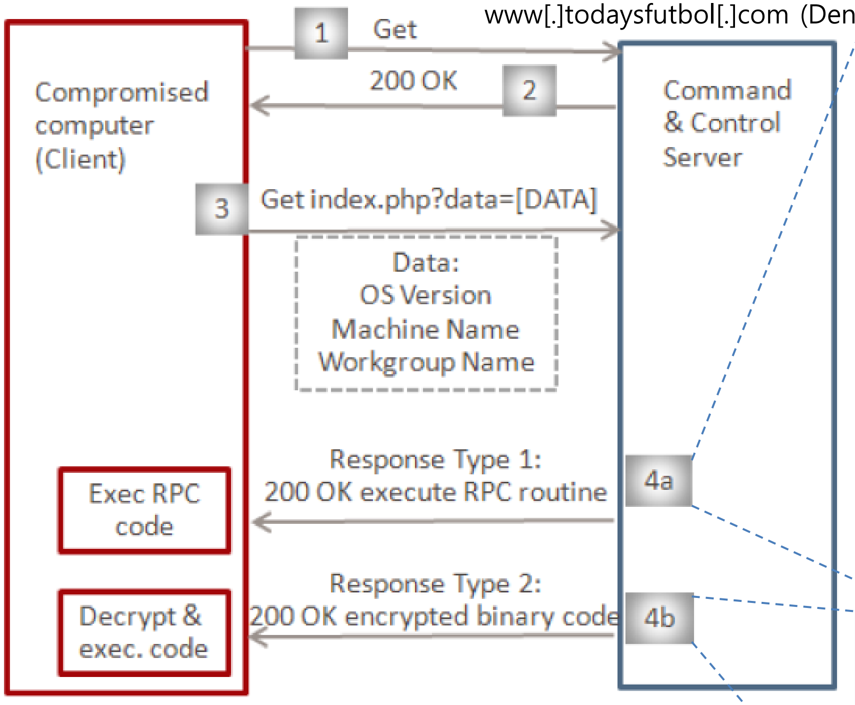
- ✓ Purpose of the rootkit drivers
  mrxnet.sys to hide the presence of the worm on removable drives
  mrxcls.sys to inject the worm into “services.exe” and two processes specific to Siemens software (Step7/S7 and WinCC)
- ✓ The driver contains an <u>encrypted data block</u>.
  services.exe — %Windir%₩inf₩oem7A.PNF
  S7tgtopx.exe — %Windir%₩inf₩oem7A.PNF
  CCProjectMgr.exe — %Windir%₩inf₩oem7A.PNF
  explorer.exe — %Windir%₩inf₩oem7m.PNF

Analysis in details - Functionality: Command and Control

- ✓ System data is gathered via Export 28, and Export 29 send payload to a target server.

www[.]mypremierfutbol[.]com (Malaysia)

www[.]todaysfutbol[.]com (Denmark)



Compromised computer (Client)

1 Get

200 OK 2

Command & Control Server

3 Get index.php?data=[DATA]

Data:
OS Version
Machine Name
Workgroup Name

Response Type 1:
200 OK execute RPC routine

4a

Exec RPC code

Response Type 2:
200 OK encrypted binary code

4b

Decrypt & exec. code

0x00	byte	1, fixed value
0x01	byte	from Configuration Data (at offset 14h)
0x02	byte	OS major version
0x03	byte	OS minor version
0x04	byte	OS service pack major version
0x05	byte	size of part 1 of payload
0x06	byte	unused, 0
0x07	byte	unused, 0
0x08	dword	from C. Data (at offset 10h, Sequence ID)
0x0C	word	unknown
0x0E	word	OS suite mask
0x10	byte	unused, 0
0x11	byte	flags
0x12	string	computer name, null-terminated
0xXX	string	domain name, null-terminated

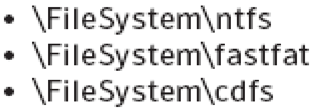
0x00	dword	IP address of interface 1, if any
0x04	dword	IP address of interface 2, if any
0x08	dword	IP address of interface 3, if any
0x0C	dword	from Configuration Data (at offset 9Ch)
0x10	byte	unused, 0
0x11	string	copy of S7P string from C. Data (418h)

1 & 2: Check internet connectivity
3: Send system information to C&C
4a: C&C response to execute RPC routine
4b: C&C response to execute encrypted binary code

The flags at offset 11h have the 4th bit set if at least one of the two registry values is found:
HKEY_LOCAL_MACHINE₩Software₩Siemens₩Step7, value: STEP7_Version
HKEY_LOCAL_MACHINE₩Software₩Siemens₩WinCC₩Setup, value: Version

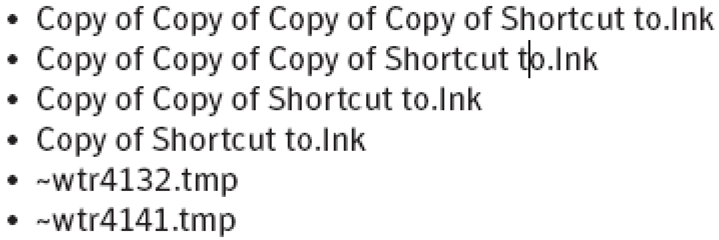
Analysis in details - Functionality: Windows Rootkit

- ✓ The ability to hide copies of its files copied to removable drives
- ✓ Registered as a boot start service
  HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩MRxCls₩"ImagePath" = "%System%₩drivers₩mrxcls.sys"
- ✓ Digitally signed driver file with a legitimate digital certificate
- ✓ Scans the filesystem driver objects:



- \FileSystem\ntfs
- \FileSystem\fastfat
- \FileSystem\cdfs

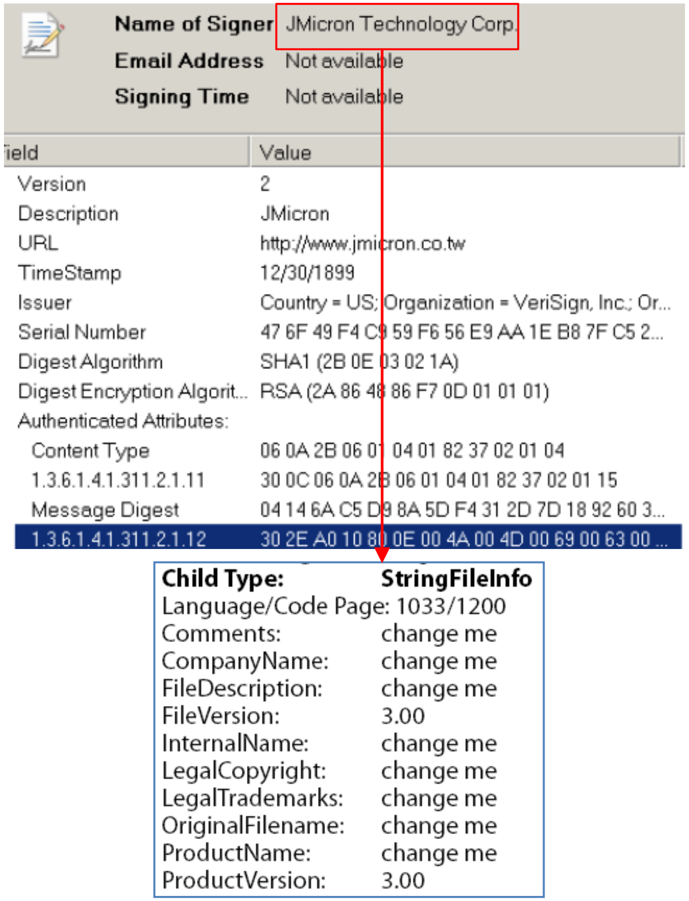
- ✓ The driver monitors "directory control" IRPs, in particular "directory query" notifications.
- ✓ Two types of files filtered out
  → Files with a ".LNK" extension having a size of 4,171 bytes.
  → Files named "~WTR[FOUR NUMBERS].TMP", whose size is between 4Kb and 8Mb;
  the sum of the four numbers modulo 10 is null.



- Copy of Copy of Copy of Copy of Shortcut to.lnk
- Copy of Copy of Copy of Shortcut to.lnk
- Copy of Copy of Shortcut to.lnk
- Copy of Shortcut to.lnk
- ~wtr4132.tmp
- ~wtr4141.tmp

Several questions about digital signatures (from SecureView Mags)

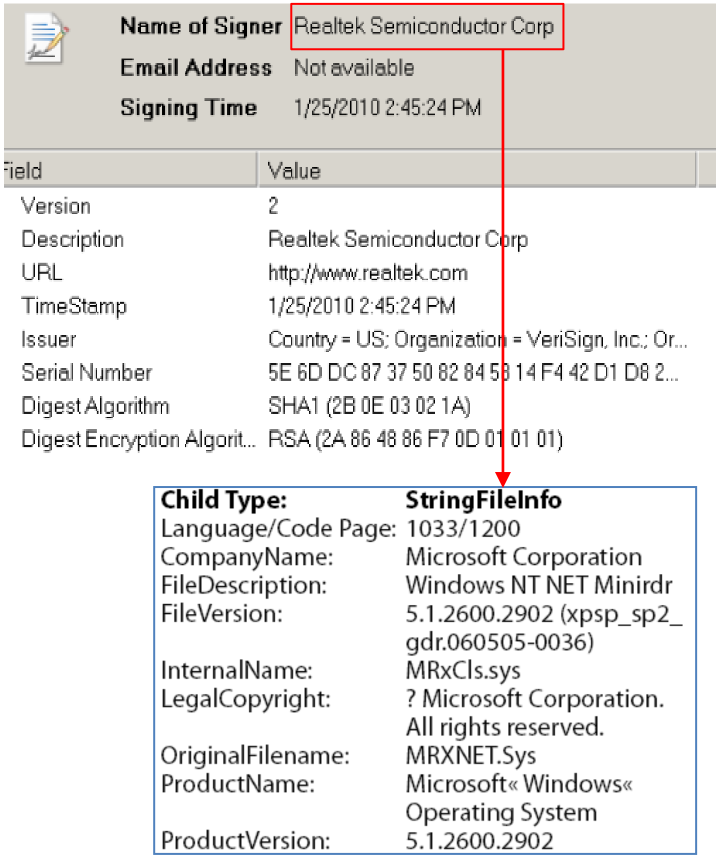
- ✓ Digitally signed driver file with legitimate Realtek and JMicron digital certificates



Name of Signer JMicron Technology Corp.
Email Address Not available
Signing Time Not available

Field	Value
Version	2
Description	JMicron
URL	http://www.jmicron.co.tw
TimeStamp	12/30/1899
Issuer	Country = US; Organization = VeriSign, Inc.; Or...
Serial Number	47 6F 49 F4 C9 59 F6 56 E9 AA 1E B8 7F C5 2...
Digest Algorithm	SHA1 (2B 0E 03 02 1A)
Digest Encryption Algorit...	RSA (2A 86 48 86 F7 0D 01 01 01)
Authenticated Attributes:	
Content Type	06 0A 2B 06 01 04 01 82 37 02 01 04
1.3.6.1.4.1.311.2.1.11	30 0C 06 0A 2B 06 01 04 01 82 37 02 01 15
Message Digest	04 14 6A C5 D9 8A 5D F4 31 2D 7D 18 92 60 3...
1.3.6.1.4.1.311.2.1.12	30 2E A0 10 80 0E 00 4A 00 4D 00 69 00 63 00 ...

Child Type:	**StringFileInfo**
Language/Code Page:	1033/1200
Comments:	change me
CompanyName:	change me
FileDescription:	change me
FileVersion:	3.00
InternalName:	change me
LegalCopyright:	change me
LegalTrademarks:	change me
OriginalFilename:	change me
ProductName:	change me
ProductVersion:	3.00



Name of Signer Realtek Semiconductor Corp
Email Address Not available
Signing Time 1/25/2010 2:45:24 PM

Field	Value
Version	2
Description	Realtek Semiconductor Corp
URL	http://www.realtek.com
TimeStamp	1/25/2010 2:45:24 PM
Issuer	Country = US; Organization = VeriSign, Inc.; Or...
Serial Number	5E 6D DC 87 37 50 82 84 58 14 F4 42 D1 D8 2...
Digest Algorithm	SHA1 (2B 0E 03 02 1A)
Digest Encryption Algorit...	RSA (2A 86 48 86 F7 0D 01 01 01)

Child Type:	**StringFileInfo**
Language/Code Page:	1033/1200
CompanyName:	Microsoft Corporation
FileDescription:	Windows NT NET Minirdr
FileVersion:	5.1.2600.2902 (xpsp_sp2_ gdr.060505-0036)
InternalName:	MRxCls.sys
LegalCopyright:	? Microsoft Corporation. All rights reserved.
OriginalFilename:	MRXNET.Sys
ProductName:	Microsoft« Windows« Operating System
ProductVersion:	5.1.2600.2902

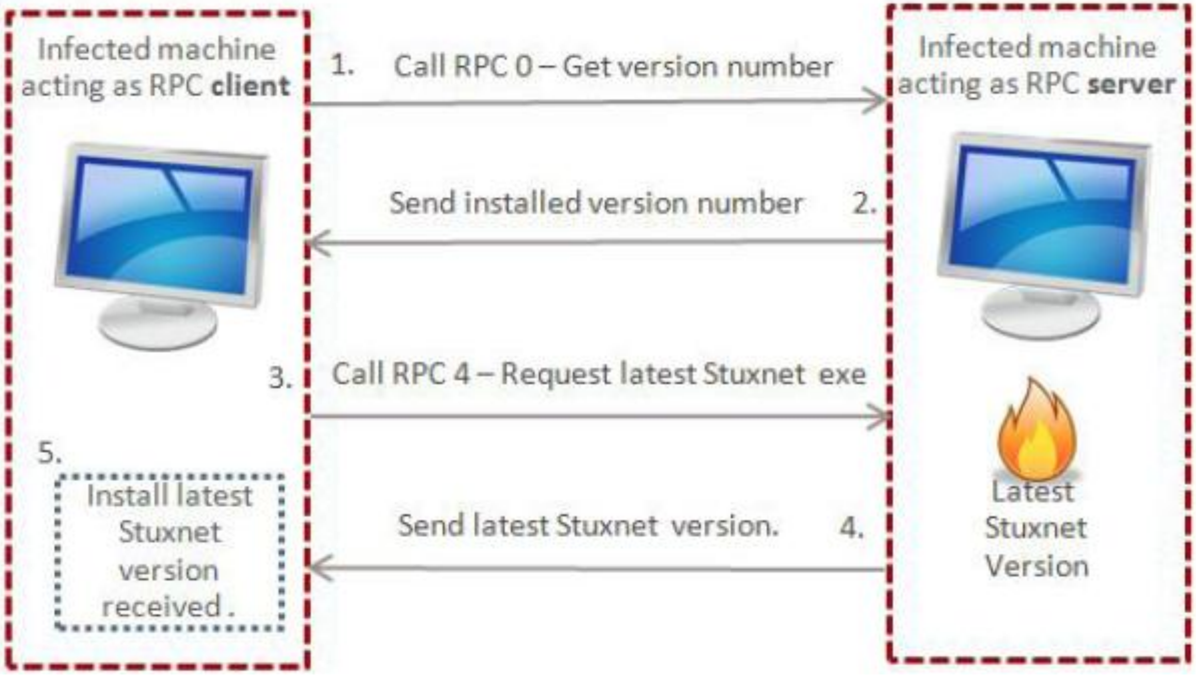
* How did the attackers manage to obtain the private keys required to sign them?
* Were Realtek and JMicron involved in the operation and willingly sign the files?
* Since both companies have development offices in China, are the Chinese involved?

- **Analysis in details - Functionality: Propagation Methods**
  Peer-to-Peer communication
  Infecting WinCC computers
  Through network shares
  Removable drives

Analysis in details - Functionality: Propagation Methods (P2P)

- ✓ RPC Server offers the following routines.
  0: Returns the version number of Stuxnet installed
  1: Receive an .exe file and execute it (through injection)
  2: Load module and executed export
  3: Inject code into lsass.exe and run it
  4: Builds the latest version of Stuxnet and sends to compromised computer
  5: Create process
  6: Read file
  7: Drop file
  8: Delete file
  9: Write data records

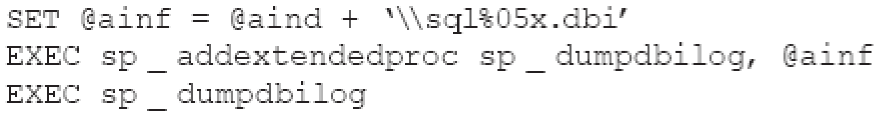
Example of an old client requesting latest version of Stuxnet via P2P



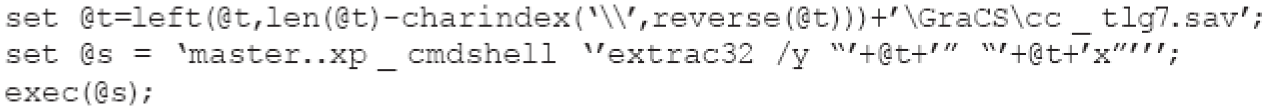
Infected machine acting as RPC **client**
1. Call RPC 0 – Get version number
Infected machine acting as RPC **server**
Send installed version number 2.
3. Call RPC 4 – Request latest Stuxnet exe
5.
Install latest Stuxnet version received.
Send latest Stuxnet version. 4.
Latest Stuxnet Version

Analysis in details - Functionality: Propagation Methods (Infecting WinCC computers)

- ✓ Connects to a remote server running the WinCC database using a password hardcoded within the WinCC software
- ✓ Two actions when found:
  → sends malicious SQL code
  → modifies an existing view
- ✓ Sends an SQL statement that creates a table and inserts a binary value into the table



```
SET @ainf = @aind + '\\sql%05x.dbi'
EXEC sp _ addextendedproc sp _ dumpdbilog, @ainf
EXEC sp _ dumpdbilog
```



```
set @t=left(@t,len(@t)-charindex('\\',reverse(@t)))+'\GraCS\cc _ tlg7.sav';
set @s = 'master..xp _ cmdshell ''extrac32 /y "'+@t+'" "'+@t+'x"''';
exec(@s);
```

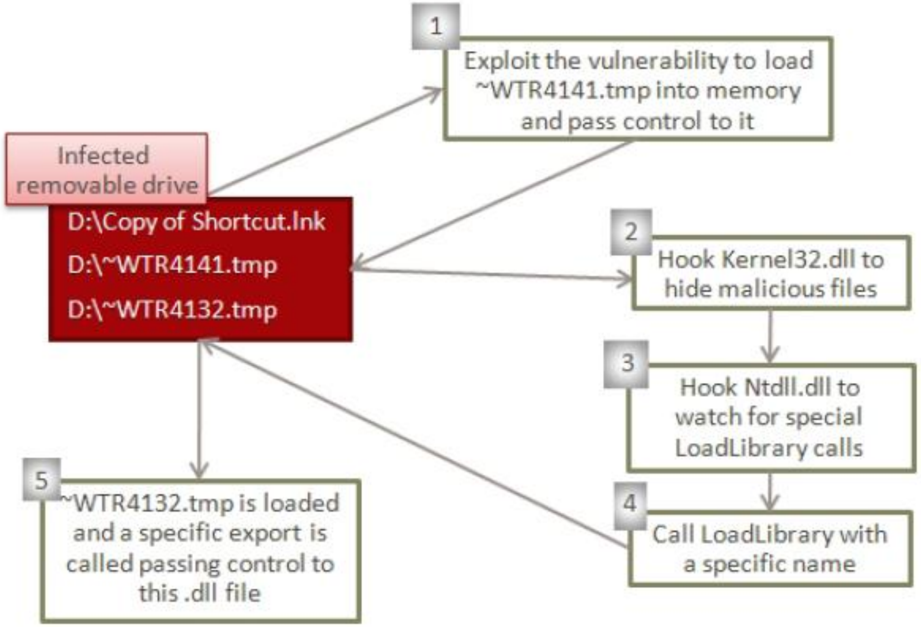
Analysis in details - Functionality: Propagation Methods (Through network shares)

- ✓ Through either a scheduled job or using Windows Management Instrumentation (WMI)
- ✓ Enumerate all user accounts of the computer and the domain, and try all available network resources either using the user's credential token or using WMI operations with the explorer.exe token in order to copy itself and execute on the remote share.

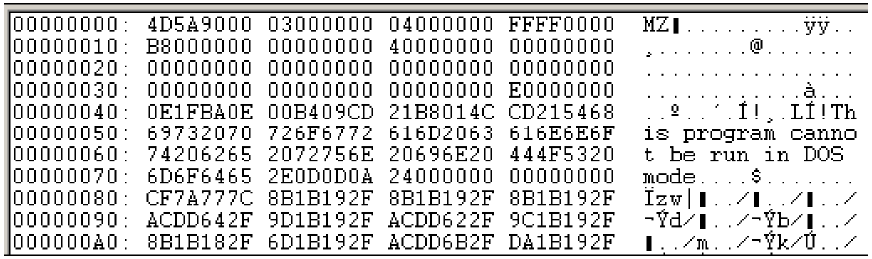
Analysis in details - Functionality: Propagation Methods (Removable drive)

- ✓ LNK Vulnerability (MS010-046, CVE-2010-2568)

USB Execution Flow

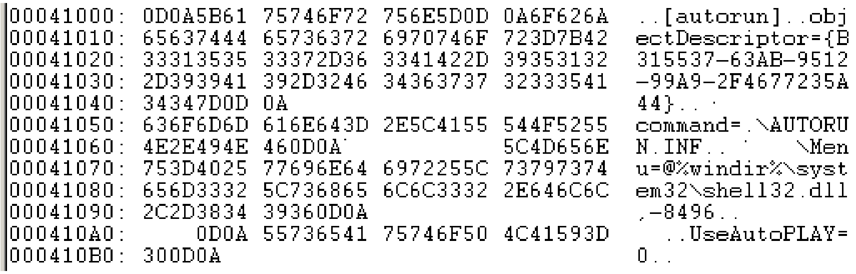

Infected removable drive
D:\Copy of Shortcut.lnk
D:\~WTR4141.tmp
D:\~WTR4132.tmp
1
Exploit the vulnerability to load ~WTR4141.tmp into memory and pass control to it
2
Hook Kernel32.dll to hide malicious files
3
Hook Ntdll.dll to watch for special LoadLibrary calls
4
Call LoadLibrary with a specific name
5
~WTR4132.tmp is loaded and a specific export is called passing control to this .dll file

Autorun.inf header

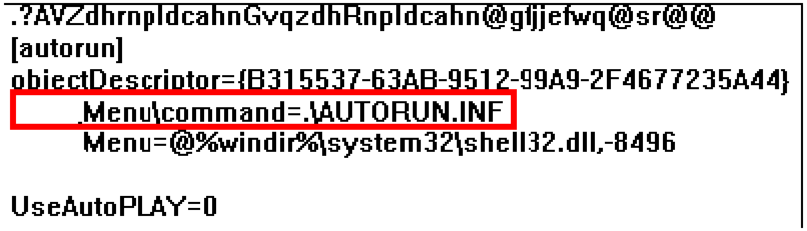


```
00000000:  4D5A9000 03000000 04000000 FFFF0000   MZ▌..........ÿÿ..
00000010:  B8000000 00000000 40000000 00000000   ¸.......@.......
00000020:  00000000 00000000 00000000 00000000   ................
00000030:  00000000 00000000 00000000 E0000000   ............à...
00000040:  0E1FBA0E 00B409CD 21B8014C CD215468   ..º..´.Í!¸.LÍ!Th
00000050:  69732070 726F6772 616D2063 616E6E6F   is program canno
00000060:  74206265 2072756E 20696E20 444F5320   t be run in DOS
00000070:  6D6F6465 2E0D0D0A 24000000 00000000   mode....$.......
00000080:  CF7A777C 8B1B192F 8B1B192F 8B1B192F   Ïzw|▌../▌../▌../
00000090:  ACDD642F 9D1B192F ACDD622F 9C1B192F   ¬Ýd/▌../¬Ýb/▌../
000000A0:  8B1B182F 6D1B192F ACDD6B2F DA1B192F   ▌../m../¬Ýk/Ú../
```

Autorun.inf footer



```
00041000:  0D0A5B61 75746F72 756E5D0D 0A6F626A   ..[autorun]..obj
00041010:  65637444 65736372 6970746F 723D7B42   ectDescriptor={B
00041020:  33313535 33372D36 3341422D 39353132   315537-63AB-9512
00041030:  2D393941 392D3246 34363737 32333541   -99A9-2F4677235A
00041040:  34347D0D 0A                           44}...
00041050:  636F6D6D 616E643D 2E5C4155 544F5255   command=.\AUTORU
00041060:  4E2E494E 460D0A            5C4D656E   N.INF...    \Men
00041070:  753D4025 77696E64 6972255C 73797374   u=@%windir%\syst
00041080:  656D3332 5C736865 6C6C3332 2E646C6C   em32\shell32.dll
00041090:  2C2D3834 39360D0A                     ,-8496..
000410A0:      0D0A 55736541 75746F50 4C41593D     ..UseAutoPLAY=
000410B0:  300D0A                                0..
```

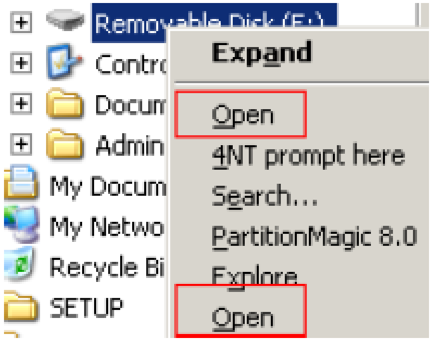


```
.?AVZdhrnpldcahnGvqzdhRnpldcahn@gljjefwq@sr@@
[autorun]
objectDescriptor={B315537-63AB-9512-99A9-2F4677235A44}
        .Menu\command=.\AUTORUN.INF
        Menu=@%windir%\system32\shell32.dll,-8496

UseAutoPLAY=0
```

Analysis in details - Functionality: Others (Removable drive)

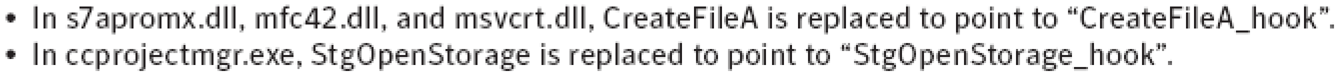
- ✓ Trick to enhance the chances to be executed
- ✓ Real one: %Windir%₩System32₩shell32.dll,-8496

Two "Open" commands



Analysis in details - Step 7 Project File Infections

- ✓ Export 16 (Installation) calls Export 2 to hook specific APIs in the s7tgtopx.exe

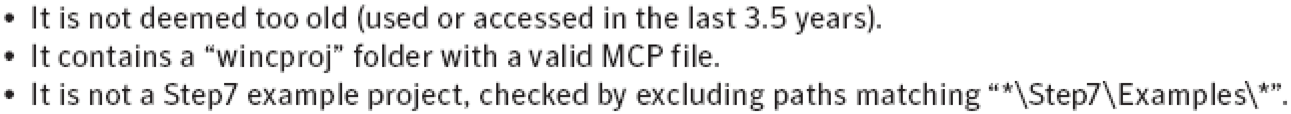


- In s7apromx.dll, mfc42.dll, and msvcrt.dll, CreateFileA is replaced to point to "CreateFileA_hook".
- In ccprojectmgr.exe, StgOpenStorage is replaced to point to "StgOpenStorage_hook".

- ✓ *CreateFileA_hook* to open S7P files for recording and infecting project folder
- ✓ *.S7P files → %Windir%₩inf₩oem6c.pnf
- ✓ *.MCP files → oem6c.pnf
- ✓ *.TMP files

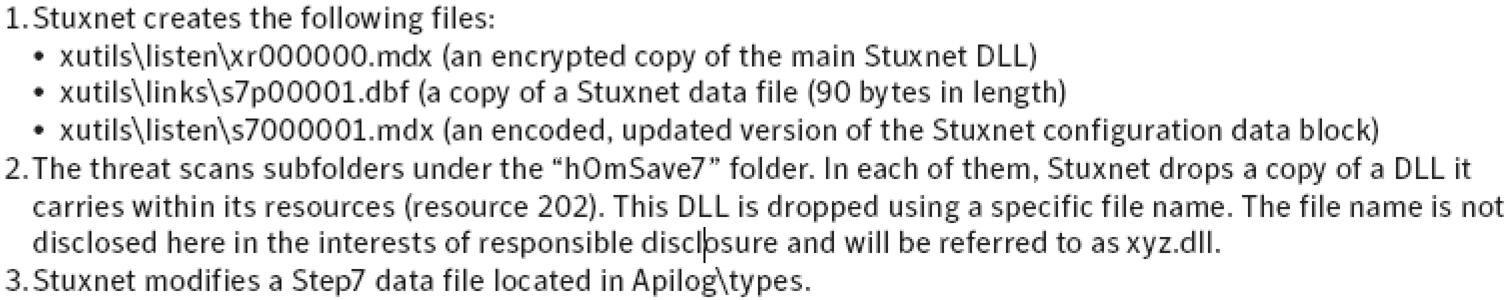
Analysis in details - Step 7 Project File Infections: S7P files

- ✓ Step 7 Project file
- ✓ A candidate for infection if:



- It is not deemed too old (used or accessed in the last 3.5 years).
- It contains a "wincproj" folder with a valid MCP file.
- It is not a Step7 example project, checked by excluding paths matching "*\Step7\Examples\*".

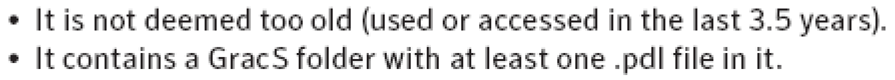
- ✓ Infection process consists of next steps:



1. Stuxnet creates the following files:
   - xutils\listen\xr000000.mdx (an encrypted copy of the main Stuxnet DLL)
   - xutils\links\s7p00001.dbf (a copy of a Stuxnet data file (90 bytes in length)
   - xutils\listen\s7000001.mdx (an encoded, updated version of the Stuxnet configuration data block)
2. The threat scans subfolders under the "hOmSave7" folder. In each of them, Stuxnet drops a copy of a DLL it carries within its resources (resource 202). This DLL is dropped using a specific file name. The file name is not disclosed here in the interests of responsible disclosure and will be referred to as xyz.dll.
3. Stuxnet modifies a Step7 data file located in Apilog\types.

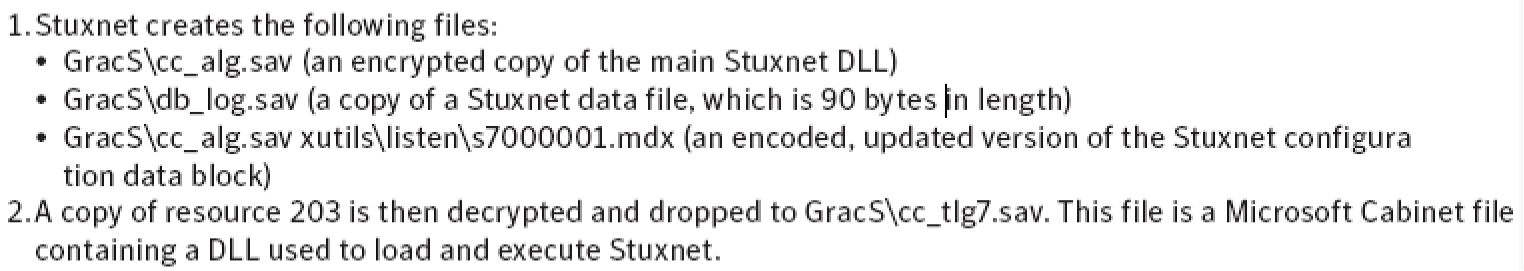
Analysis in details - Step 7 Project File Infections: MCP files

- ✓ Created by WinCC
- ✓ A candidate for infection if:



- It is not deemed too old (used or accessed in the last 3.5 years).
- It contains a GracS folder with at least one .pdl file in it.

- ✓ Infection process consists of next steps:

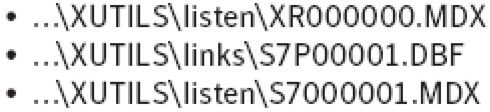


1. Stuxnet creates the following files:
   - GracS\cc_alg.sav (an encrypted copy of the main Stuxnet DLL)
   - GracS\db_log.sav (a copy of a Stuxnet data file, which is 90 bytes in length)
   - GracS\cc_alg.sav xutils\listen\s7000001.mdx (an encoded, updated version of the Stuxnet configura tion data block)
2. A copy of resource 203 is then decrypted and dropped to GracS\cc_tlg7.sav. This file is a Microsoft Cabinet file containing a DLL used to load and execute Stuxnet.

- ✓ WinCC DB is also infected during this infection process

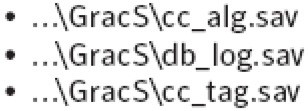
Analysis in details - Step 7 Project File Infections: TMP files

- ✓ Validated filename: ~WRabcde.tmp where (a+b+c+d+e) mod 16 = 0
- ✓ Magic string (1st 8Bytes): LRW~LRW~
- ✓ Export #9 takes a Step7 Project path as input, then build paths:



  - ...\XUTILS\listen\XR000000.MDX
  - ...\XUTILS\links\S7P00001.DBF
  - ...\XUTILS\listen\S7000001.MDX

- ✓ Export #31 takes a Step7 Project path as input, then build paths:

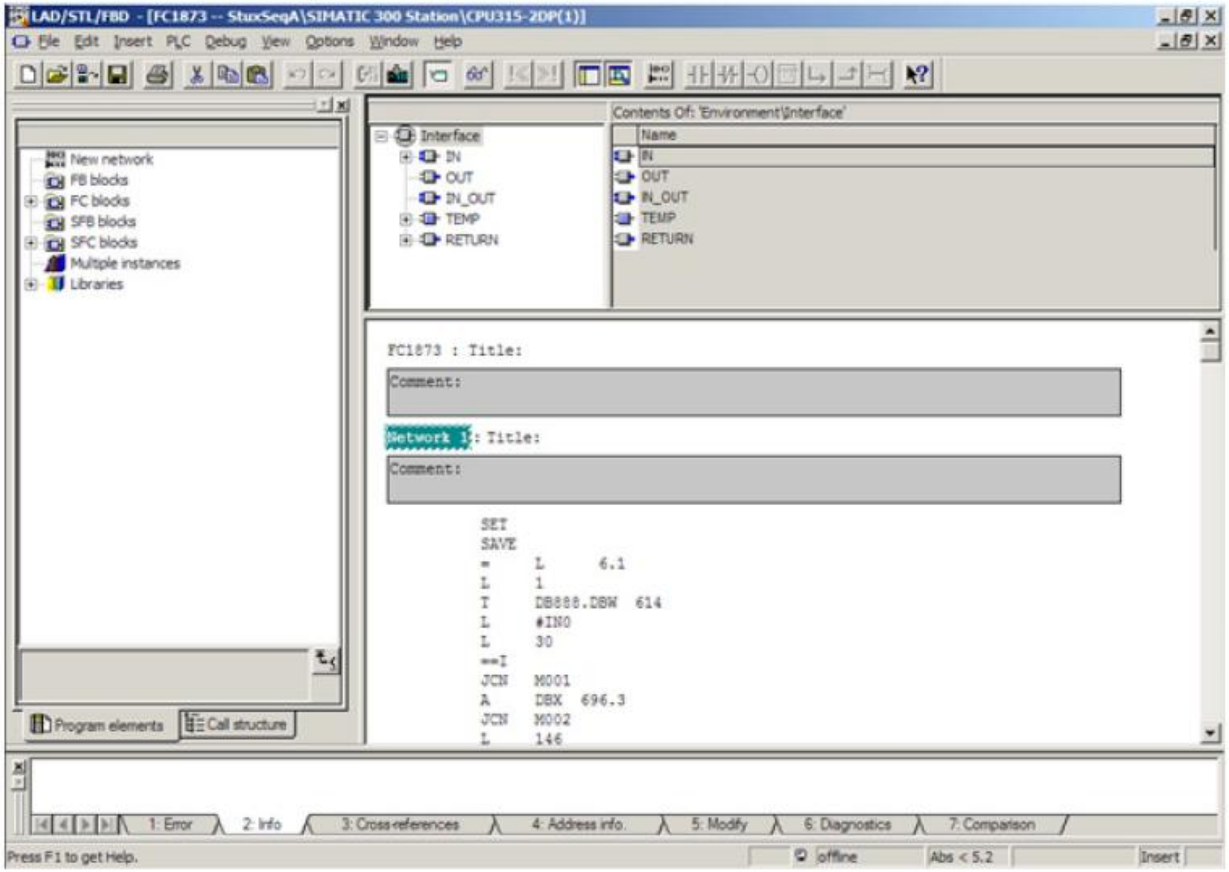


  - ...\GracS\cc_alg.sav
  - ...\GracS\db_log.sav
  - ...\GracS\cc_tag.sav

Analysis in details - Modifying PLCs (Terms)

- ✓ DB (Data Blocks):
  program specific data
  Ex) numbers, structures
- ✓ SDB (System Data Blocks):
  configuration info.
- ✓ OB (Organization Blocks):
  entry point of programs
  → OB1: main EP of the PLC
  → OB35: standard watchdog
- ✓ FB (Function Blocks):
  standard code blocks

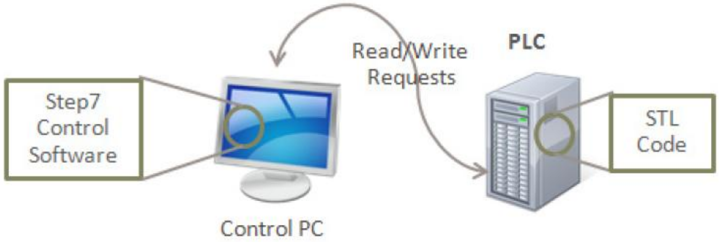
Stuxnet code in the Step7 STL editor



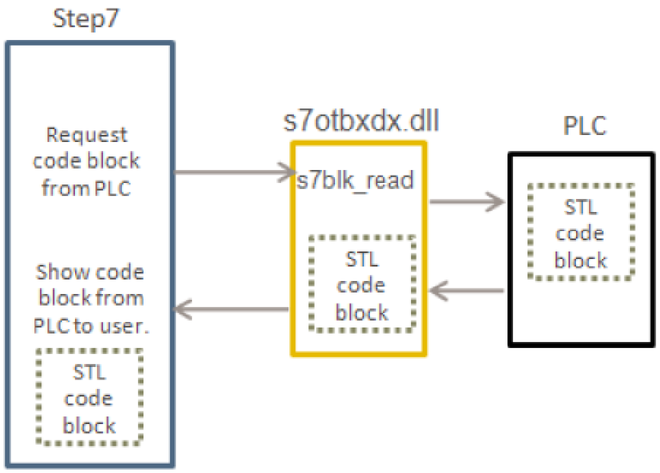
```
FC1873 : Title:
Comment:

Network 1: Title:
Comment:

      SET
      SAVE
      =     L      6.1
      L     1
      T     DB888.DBW  614
      L     #IN0
      L     30
      ==I
      JCN   M001
      A     DBX  696.3
      JCN   M002
      L     146
```

Analysis in details - Modifying PLCs (Infection)

- ✓ Resource 208 is dropped by export #17
- ✓ Replacement for Simatic's s7otbxdx.dll file.

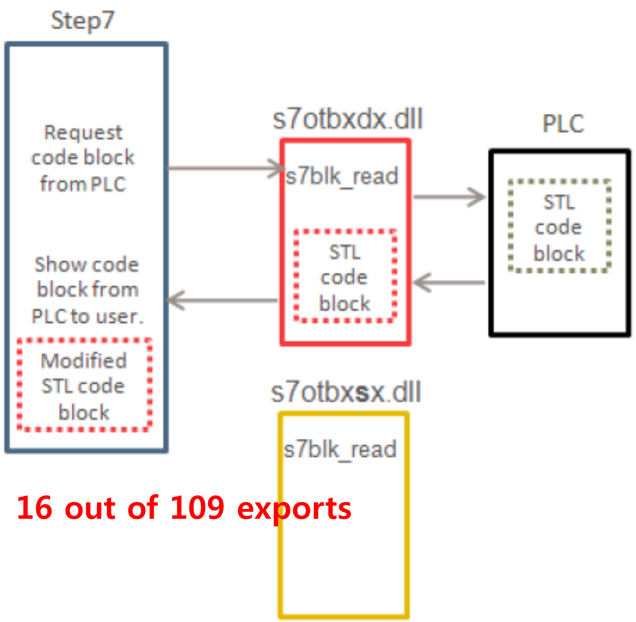


Step7 and PCL communicating via s7otbxdx.dll



93 out of 109 exports

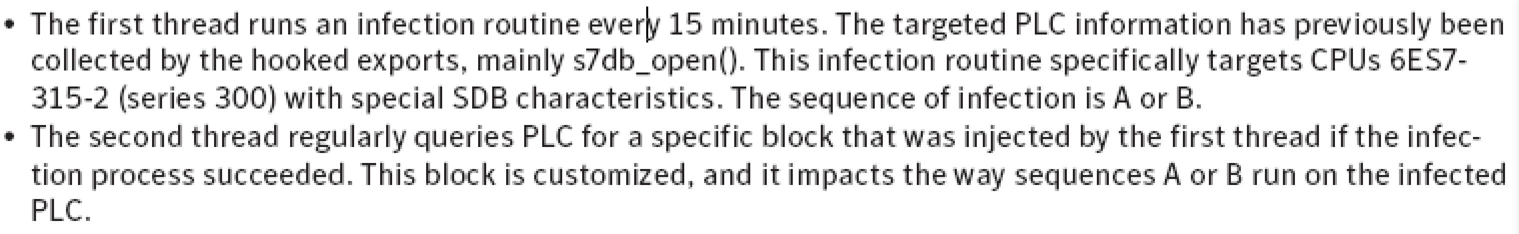
Communication with malicious version of s7otbxdx.dll



16 out of 109 exports

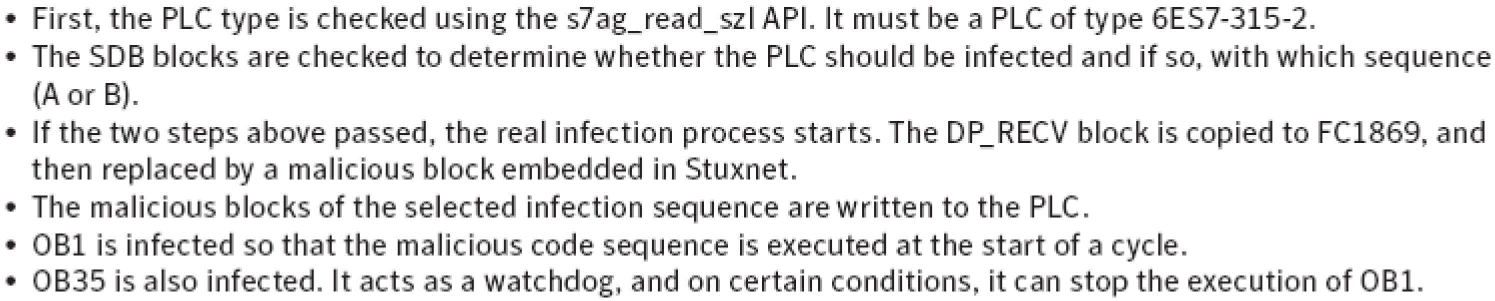
Analysis in details - Modifying PLCs (Sequence Blocks)

- ✓ Sequence A,B then C
- ✓ Initial Infection



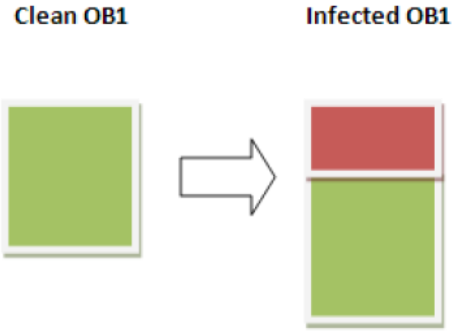
- The first thread runs an infection routine every 15 minutes. The targeted PLC information has previously been collected by the hooked exports, mainly s7db_open(). This infection routine specifically targets CPUs 6ES7-315-2 (series 300) with special SDB characteristics. The sequence of infection is A or B.
- The second thread regularly queries PLC for a specific block that was injected by the first thread if the infection process succeeded. This block is customized, and it impacts the way sequences A or B run on the infected PLC.

- ✓ The infection threat, sequences A and B



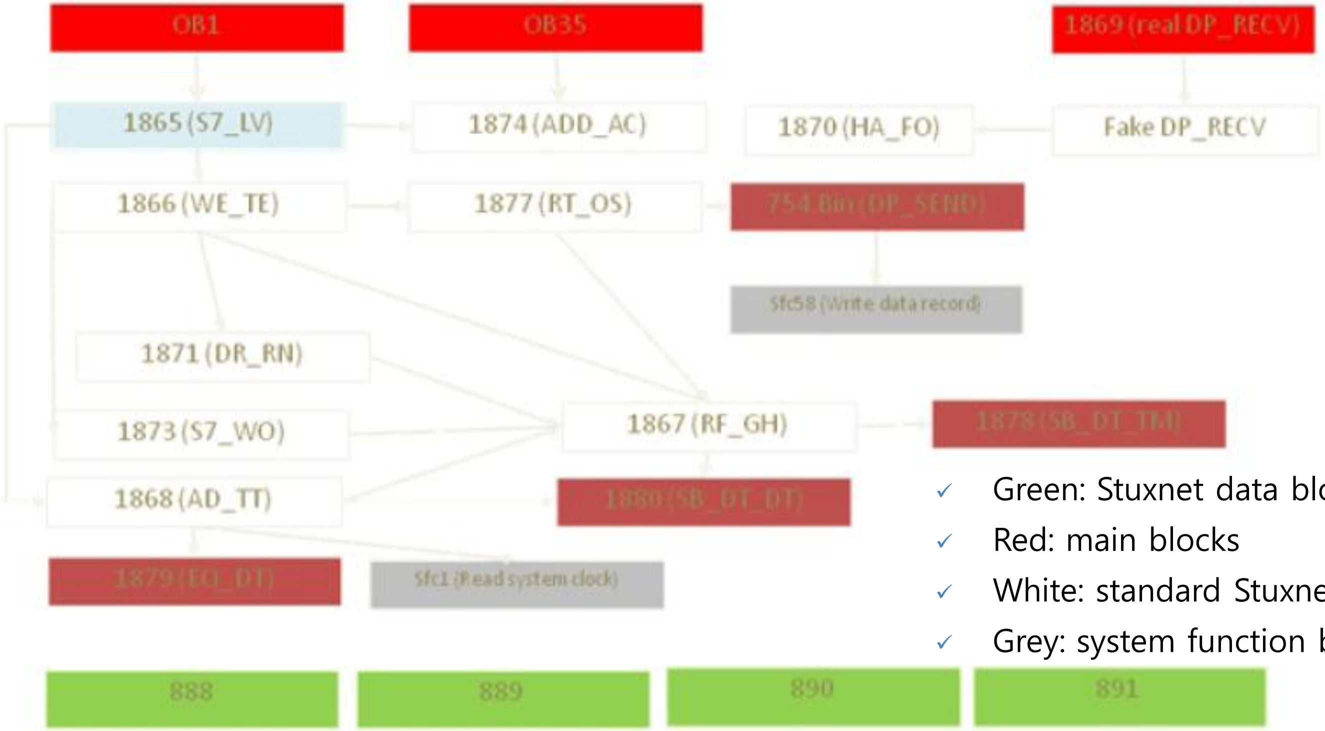
- First, the PLC type is checked using the s7ag_read_szl API. It must be a PLC of type 6ES7-315-2.
- The SDB blocks are checked to determine whether the PLC should be infected and if so, with which sequence (A or B).
- If the two steps above passed, the real infection process starts. The DP_RECV block is copied to FC1869, and then replaced by a malicious block embedded in Stuxnet.
- The malicious blocks of the selected infection sequence are written to the PLC.
- OB1 is infected so that the malicious code sequence is executed at the start of a cycle.
- OB35 is also infected. It acts as a watchdog, and on certain conditions, it can stop the execution of OB1.

- ✓ Summary (key steps)
  → SDB Check
  → DP_RECV replacement
  → OB1/OB35 infection



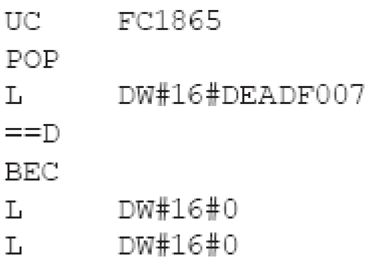
Analysis in details - Modifying PLCs (Sequence Blocks)

- ✓ Connections Between Blocks, Sequences A and B (targeting S7-315)



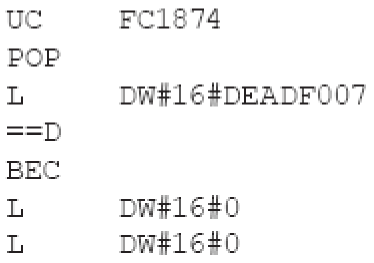
- ✓ Green: Stuxnet data blocks
- ✓ Red: main blocks
- ✓ White: standard Stuxnet blocks
- ✓ Grey: system function blocks

Infected OB1



```
UC      FC1865
POP
L       DW#16#DEADF007
==D
BEC
L       DW#16#0
L       DW#16#0
```

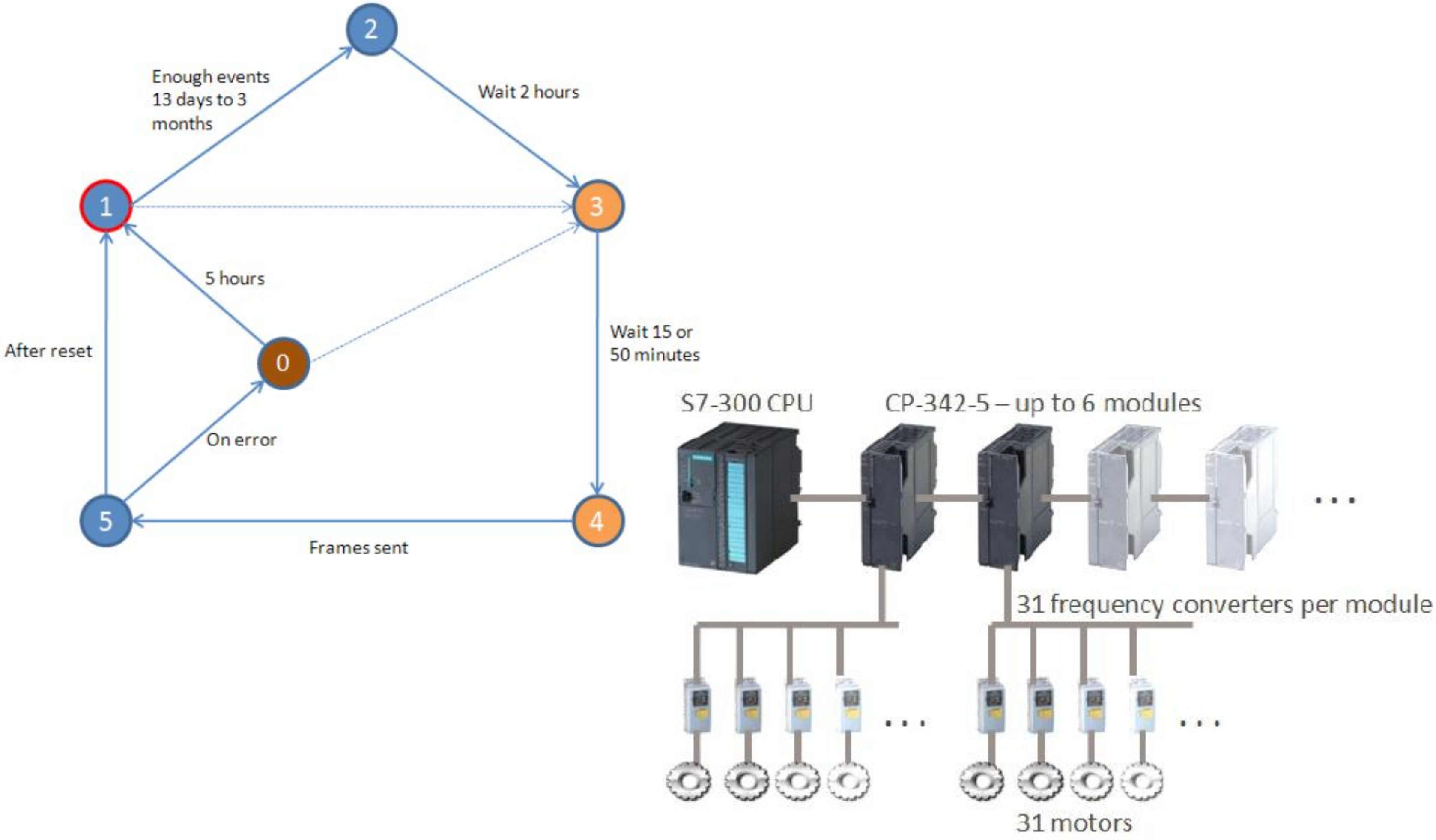
Infected OB35



```
UC      FC1874
POP
L       DW#16#DEADF007
==D
BEC
L       DW#16#0
L       DW#16#0
```

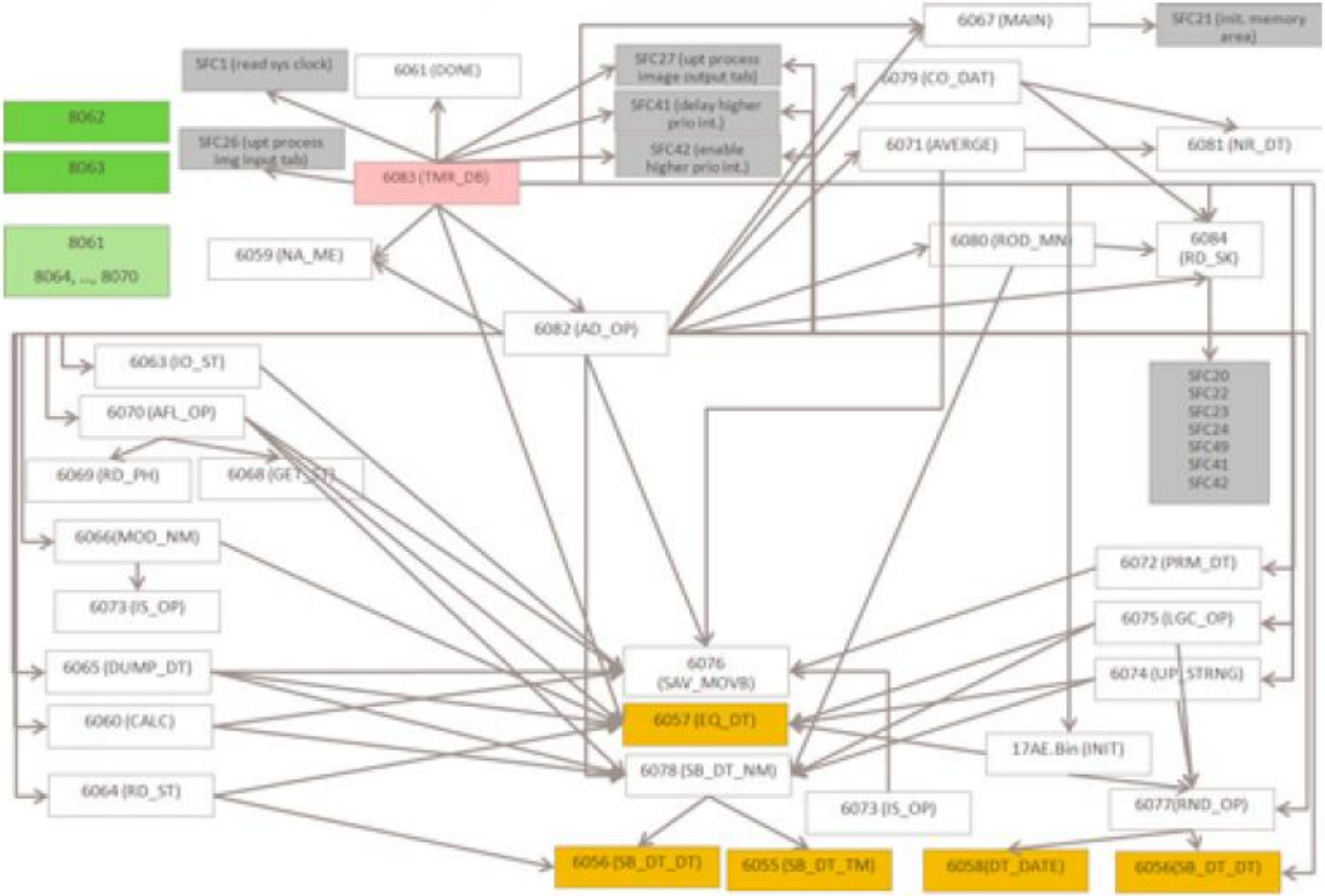
Analysis in details - Modifying PLCs (Sequence Blocks)

- ✓ State machine path of execution



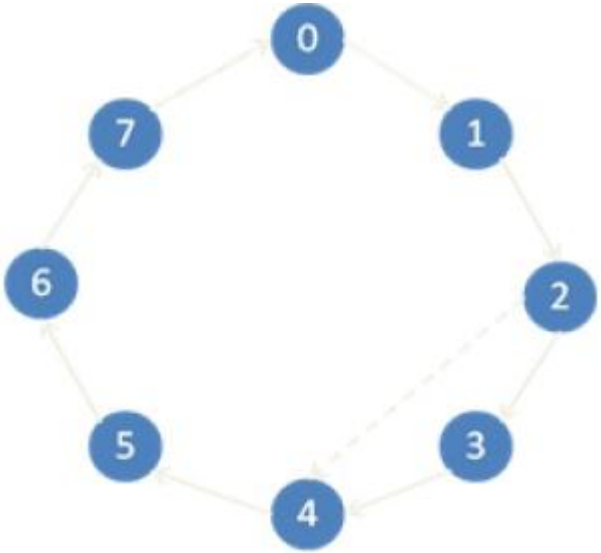
Analysis in details - Modifying PLCs (Sequence Blocks)

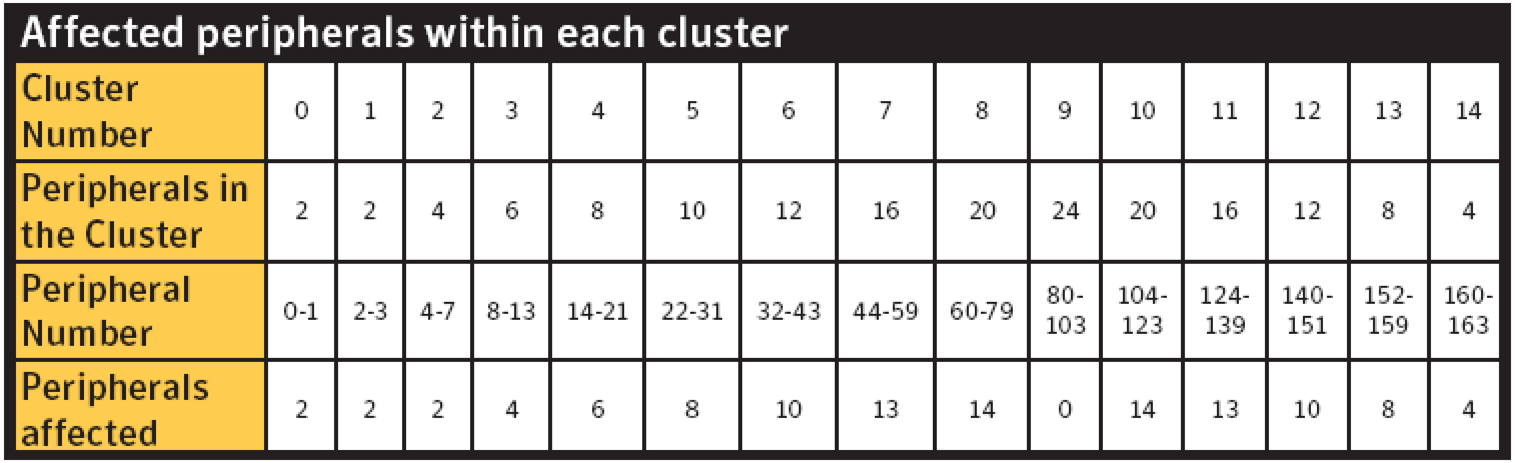
- ✓ Connections Between Blocks, Sequences C (targeting S7-417 PLCs)



Analysis in details - Modifying PLCs (Sequence Blocks)

- ✓ Eight states in sequence C
  → State 0: Wait
  → State 1: Recording
  → State 2-6: Sabotage
  → State 7: Reset
- ✓ Never happened due to the missing function in the DLL





Affected peripherals within each cluster

Cluster Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Peripherals in the Cluster	2	2	4	6	8	10	12	16	20	24	20	16	12	8	4
Peripheral Number	0-1	2-3	4-7	8-13	14-21	22-31	32-43	44-59	60-79	80-103	104-123	124-139	140-151	152-159	160-163
Peripherals affected	2	2	2	4	6	8	10	13	14	0	14	13	10	8	4

→ 164 total

→ 110 affected

[TED] Fighting viruses, defending the net

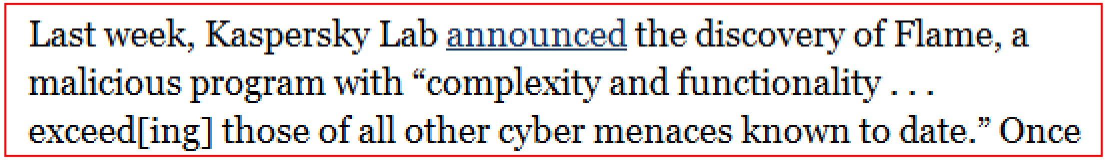
Mikko Hypponen's Speech: Fighting viruses, defending the net

- ✓ F-Secure CRO(Chief Research Officer)
- ✓ http://mikko.hypponen.com/
- ✓ [2011.7] http://www.youtube.com/watch?v=cf3zxHuSM2Y (17m 34s)
- ✓ https://www.clarifiednetworks.com/Videos

Conclusion

Lessons Learned

- ✓ Cyber warfare has begun.
- ✓ Stuxnet was a huge threat and very complicated, targeted and sophisticated.
- ✓ It has started national support to attack against targeted enemy.
- ✓ It is like a mission-impossible game.
- ✓ Now is the time to foster cyber warriors with cyber weapons.
- ✓ APT is evolving : Duqu (2011.10), Flame (2012.6)



Last week, Kaspersky Lab announced the discovery of Flame, a malicious program with "complexity and functionality . . . exceed[ing] those of all other cyber menaces known to date." Once

END

NO QUESTIONS?