APT Case Study - W32.Stuxnet Dossier

Nicolas Falliere, Liam O Murchu, and Eric Chien
Symantec Security Response

Presented by Christopher N. Gutierrez, Gaspar Modelo-Howard
Dependable Computing Systems Lab (DCSL)

PURDUE UNIVERSITY

Terminology

- Rootkit
  - A set of tools
    - Hides the activities of an attacker
    - Enables continuous root access
  - A system administrator may be "unable to see processes that the attacker is running, files or log entries that result from the attacker's activity, and even network connections to other machines created by the attacker" [1]
- Zero-day vulnerability
  - An exploit that is unknown to the owner of the code
- Dropper
  - "anything that can get the target system to execute code, be it a security vulnerability or tricking a user into opening an e-mail attachment"[2]
- Code injection
  - Forcing an application to execute malicious code

PURDUE UNIVERSITY

Introduction

- Stuxnet – A complex piece of malware written to target industrial control systems (ICS)
- Goal – To maliciously reprogram ICS by modifying programmable logic controllers (PLC) and hide changes from the operators
  - PLC usages: gas pipelines, power plants, etc.

- Siemens Simatic S7-300 PLC

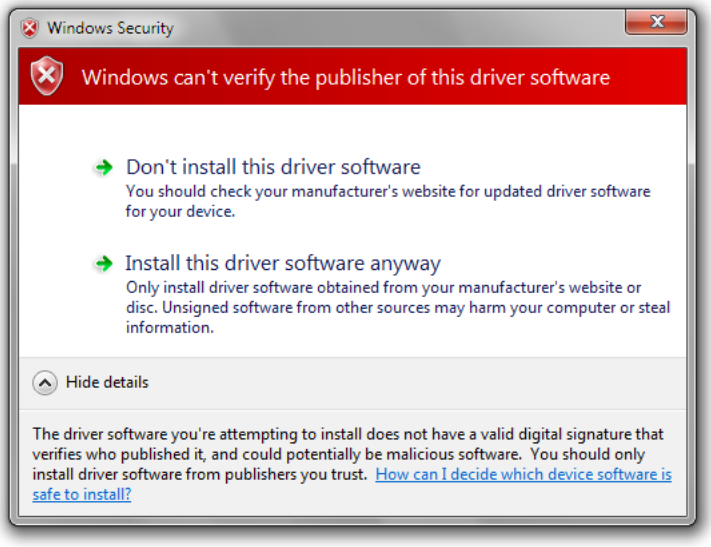
The Stuxnet Arsenal Highlights

- Multiple zero-day exploits
  - Enables privilege escalation
  - Self-replication through removable drives or LAN
- First ever PLC rootkit
- Antivirus evasion techniques
- Sophisticated updating mechanism
- Two compromised digital certificates

Attack Scenario "Speculation"

- ICS are operated by PLCs which are programmed by computers without network connectivity
- Reconnaissance to steal ICS schematics
  - Each PLC is configured uniquely
  - Possibly stolen by an insider or by other malware
- Attacker creates a mirrored environment
  - Includes necessary hardware/software
- Use stolen certificates to digitally sign malicious driver to avoid suspicion when deployed

PURDUE UNIVERSITY



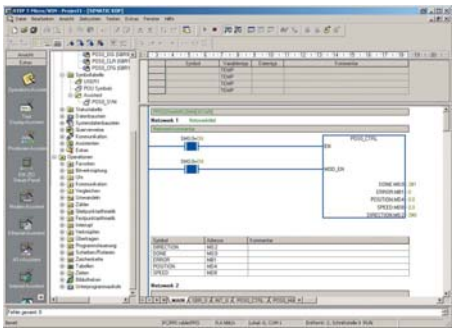
PURDUE UNIVERSITY

Attack Scenario Speculation Con't

- Introduce the malware into the target environment
  - Insider
  - Social engineering
  - May have been introduced by removable media
- Replicate and search for Field PG
  - Spread through LAN, hop to Field PG via removable media
- Field PG
  - Windows OS
  - Probably without networking
  - Used to program PLC

Attack Scenario Speculation Con't

- On the Field PG
  - Sabotage PLC by targeting STEP 7 projects
    - STEP 7 – the standard software package for configuring Siemans PLCs
  - Hides malicious modifications from operators
- Failures would be be confused for hardware malfunctions



Stuxnet Architecture

- Consists of a large .dll that contains different exports
  - Contains all the code to control the worm
- Also contains resources for the exports
  - May contain other .dll files
  - Exploit modules
  - Configuration files

PURDUE UNIVERSITY

Stuxnet Architecture Con't

Table 3
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

Table 4
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)

PURDUE UNIVERSITY

Stuxnet Architecture Con't

- Bypassing Behavior Blocking
  - Special method to load DLLs
  - Overcomes instruction protection that monitors "LoadLibrary" calls
- Injection Technique
  - When calling an export, the .dll is injected into another trusted process

Table 5
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

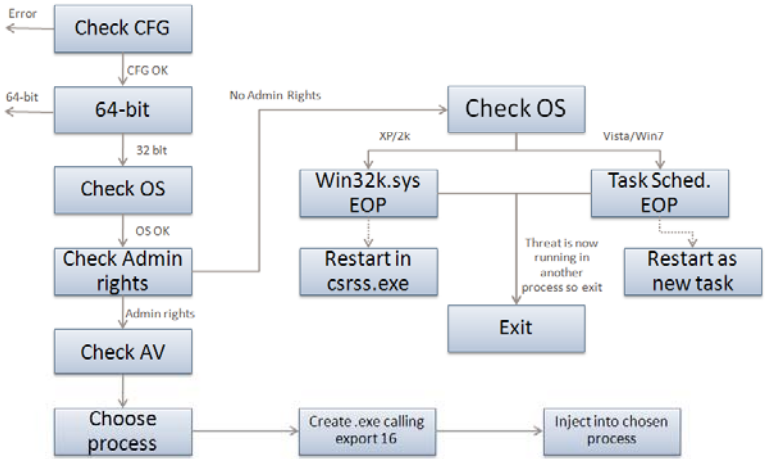
PURDUE UNIVERSITY

Stuxnet Architecture Con't

- Configuration Data Block
  - Setup deadline, URLs for C&C
  - Spreading behavior: number of files on USB need in order to infect, etc
- Computer Configuration Block
  - Computer name, domain name, OS version, infection date/time

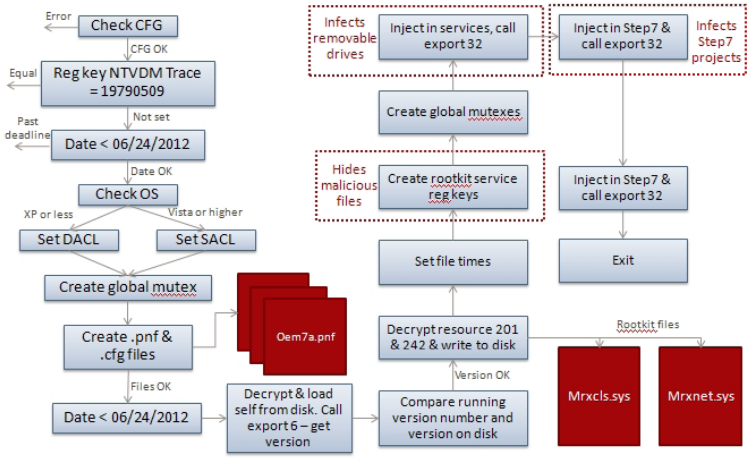
PURDUE UNIVERSITY

Installation



Slide 13

Infection Routine Flow



Slide 14

Load Point

- MrxCls.sys
  - A driver digitally signed with a compromised Realtek certificate or Jmicron
  - Realtek certificate revoked by Verisign July 16, 2010
  - Enables Stuxnet to execute during system boot
  - Goal: inject and execute Copies of Stuxnet into
    - services.exe and S7tgtopx.exe - Simatic Manager
    - CCProjectMgr.exe – WinCC manager
- WinCC
  - "SIMATIC WinCC is a supervisory control and data acquisition (SCADA) and human-machine interface (HMI) system from Siemen"[1]

[1]From: http://en.wikipedia.org/wiki/WinCC

PURDUE UNIVERSITY

Command and Control

- Communicates with a C&C on port 80 via HTTP
  - www.mypremierfutbol.com
  - www.todaysfutbol.com
  - Located in Malaysia and Denmark
- Compromise iexplore.exe to communicate with C&C
  - Check network connectivity – www.msn.com, www.windowsupdate.com
- Information to C&C
  - Payload: OS Version, Machine name, Workgroup Name
  - Obfuscation - XOR-ed with 31-byte string:
    0xF117FA1C, 0xE23C1D7, 0xBB776C0, 0xE49615C4, 0x622E2D18, 0x95F0D8AD, 0x4B23BADC, 0x4FD70C
  - Sent "Hexified" as
    - http://www.mypremierfutbol.com/index.php?data=<Hexified Data>

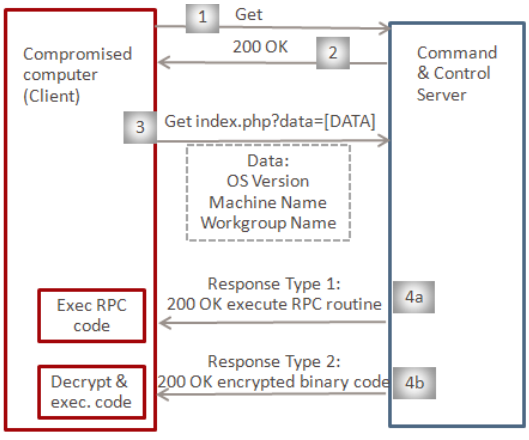
PURDUE UNIVERSITY

Command and Control con't

- Receive data from C&C
  - Located in the HTTP Content section
  - Pure binary data
  - Obfuscated with a different hex key
  - Data contains a payload module (windows executable)
- Implications
  - Ability to run any code on the infected machine
  - Distribution of additional tools to Stuxnet
  - Deliver updated versions of Stuxnet

PURDUE UNIVERSITY

Command and Control Flow



PURDUE UNIVERSITY

Windows Rootkit Functionality

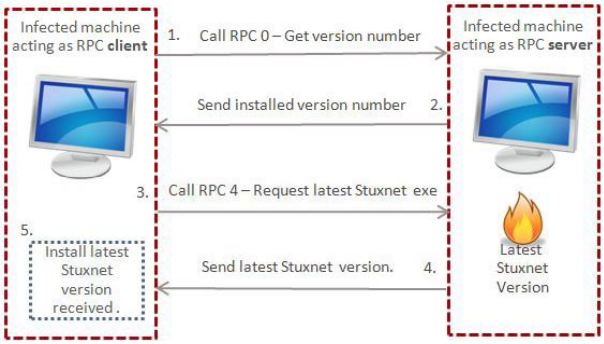
- Prevent users from noticing Stuxnet files on removable media
- MrxNet.sys
  - Driver signed by compromised Realtek certificate
  - Scans file system driver objects
    - \FileSystem\ntfs
    - \FileSystem\fastfat
    - \FileSystem\cdfs
  - Intercepts requests for read/write on NTFS, FAT, or CD-ROM devices
  - Filters query directory results so that Stuxnet files are not shown

Propagation Methods

- Network propagation routines
  - P2P communication and updates
  - Infect WinCC Machines
  - Propagation
    - Network shares exploit
    - Printer Spooler Zero-Day Vulnerability
    - Windows Server Service Vulnerability
- Removable media propagation
  - LNK zero-day vulnerability
    - Allows auto-execution when viewing removable drive
  - AutoRun.inf vulnerability

Peer-to-Peer Communcation

- Used for updating infected computers with updated Stuxnet
- Reach infected machines that do not have internet access but network access



Infecting WinCC Computers

- WinCC connects to a database server using a hardcoded password
- Stuxnet sends malicious SQL code to infect the WinCC database
- Stuxnet modifies view code by adding code that executes each time a view is accessed
- The Stuxnet binary is stored into a table

Removable Drive Propagation

- LNK vulnerability
  - Checks if drive is suitable for infection
    - The infection is less then 21 days old
    - There is at least 5MB of free space
    - Has at least three files
  - Different circumstances will cause Stuxnet clean an infected drive
    - Example: If the remove able drive has infected three different computers, delete the files
- AutoRun.Inf
  - Used by older versions of Stuxnet
  - Autorun.inf – a configuration file that instructs Windows to auto-execute a file when drive is inserted

PURDUE UNIVERSITY

AutoRun.Inf Exploit

Figure 15

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../
```

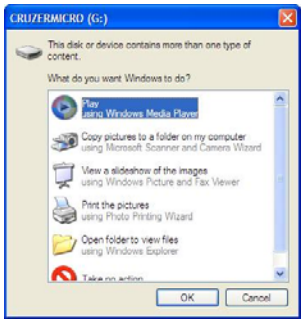
Figure 16

Autorun.inf footer

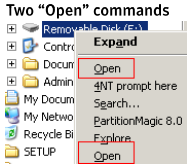
```
00041000: 0D0A5B61 75746F72 756E5D0D 0A6F626A  ..[autorun]..obj
00041010: 65637444 65736372 69707469 6F6E3D7B  ectDescription={B
00041020: 33313535 33372D36 3341422D 39353132  315537-63AB-9512
00041030: 2D393941 392D3246 34363737 32333541  -99A9-2F4677235A
00041040: 34347D0D 0A                          44}..
00041050: 636F6D6D 616E643D 2E5C4155 544F5255  command=.\AUTORU
00041060: 4E2E494E 460D0A                      N.INF..
00041070: 753D4025 77696E64 6972255C 73797374  u=@%windir%\syst
00041080: 656D3332 5C736865 6C6C3332 2E646C6C  em32\shell32.dll
00041090: 2C2D3834 39360D0A                    ,-8496..
000410A0: 55736541 75746F50 4C41593D 0D0A      UseAutoPLAY=..
000410B0: 300D0A                               0..
```

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

UseAutoPLAY=0
```



Two "Open" commands



PURDUE UNIVERSITY

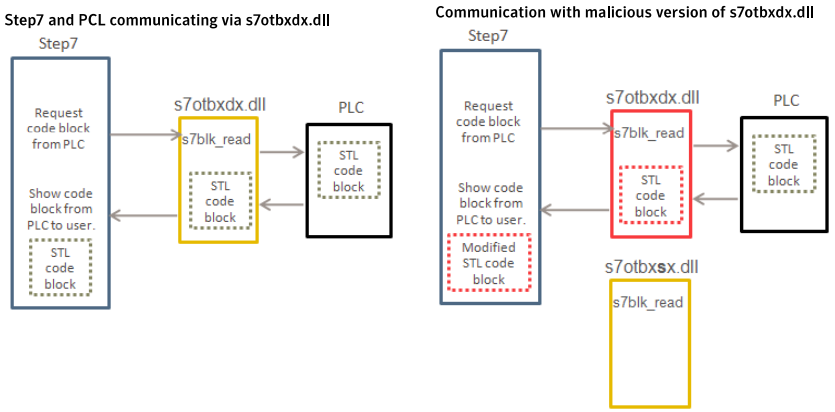
Step 7 Project File Infection

- Modifies the .dlls that creates and opens Step 7 project files
  - Record the location of .S7P and .MPC(encrypted)
  - Observe which .MPC files are used by the project
  - Infect the project
- .S7P
  - A Project file
  - Infect if
    - Not too old (used or accessed in the last 3.5 years)
    - Contains .MCP files
    - Not an example project
- .MPC
  - Created by WinCC
  - Infect if not too old, contains a .pdl file in it

Modifying PLCs

- End goal
  - Infect specific types of Simatic PLC devices
- PLC code is written in STL or SCL and is compiled into assembly code
- Code runs on PLC to execute, control, and monitor industrial processes
- Target - s7otbxdx.dll
  - Responsible for handling exchanges between the Field PG and the PLC
- Stuxnet replaces this .dll
  - Monitor PLC blocks
  - Infect PLC by inserting its own blocks
  - Mask the fact that the PLC is infected

Modifying PLCs con't



- Malicious driver
  - Intercept 16/109 exports are intercepted
  - Enables Stuxnet to modify the data sent to or returned from the PLC

PURDUE UNIVERSITY

PLC Infection Process

- Stuxnet injects data blocks into the PLC to alter its behavior
- Infection process handled by two threads
  - Infection Thread
    - Probes every 15 minutes
    - Check for a PLC connection of the target type
      - Look for System Data Blocks that have the Profibus communication processor
    - Malicious blocks are written to the PLC
  - Monitor Thread
    - Probes every 5 minutes
    - Queries PLC for a block that was injected by the infection thread
    - Has no purpose if the PLC is not infected
    - When the sabotage routine has begun, causes all the infected PLCs to begin simultaneously

PURDUE UNIVERSITY

The Sabotage

- Slowing down or speeding up motors to different rates at different times
  - Look for normal operating frequency: 807 – 1210 Hz
    - Limits the target scope
    - Observe for 13 days to 3 months
  - The motor speed is set to 1410 Hz
  - Resume normal operation
  - After ~27 days, set to 2 Hz initially, then to 1064 Hz
  - Resume normal operation
  - Repeat

PURDUE UNIVERSITY

PLC Rootkit

- Contained within s7otbxdx.dll
- Goal: Exist undetected on the PLC
  - Read requests for malicious blocks
  - Write requests that overwrites Stuxnet code
- If a read is requested
  - Provide a cleaned block on the fly
  - Provide an unaltered version of the block
- If a write is requested
  - Intercept and add malicious alterations before written

PURDUE UNIVERSITY

Conclusion

- Stuxnet is sophisticated
  - Development required significant resources
- Demonstrates a real world attack on critical infrastructure
- First malicious code to exploit four zero-day vulnerabilities

PURDUE UNIVERSITY

Citations

[1] Neil Daswani, Christoph Kern, and Anita Kesavan. 2007. Foundations of Security: What every Programmer Needs to Know. Apress, Berkely, CA, USA.

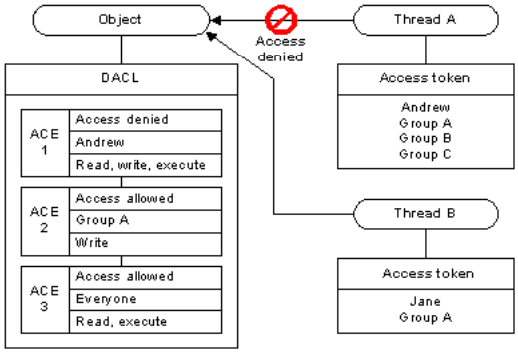
[2] Joel Scambray, Stuart McClure, and George Kurtz. 2000. Hacking Exposed (2nd ed.). McGraw-Hill Professional.

[3] Nicolas Falliere, Liam O Murchu, Eric Chien. 2011. W.32.Stuxnet Dossier. Symatec Security Response.

PURDUE UNIVERSITY

Appendix – DACL/SACL

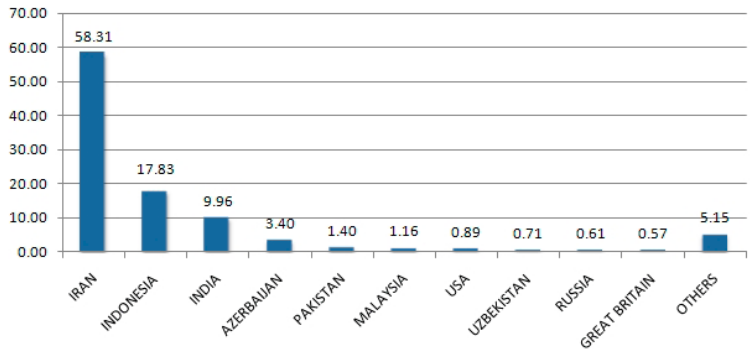
- DACL – Discretionary Access Control List



- SACL – System Access Control List
  - Log attempts when accessing secure objects

From: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx

Appendix - Geographic Distribution



Appendix – Video demo

- http://www.symantec.com/connect/blogs/stuxnet-breakthrough

PURDUE UNIVERSITY

Appendix - Timeline

Table 1
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.

PURDUE UNIVERSITY