CS 361S

Stuxnet

Vitaly Shmatikov

(based on Symantec’s “Stuxnet Dossier”)

CVE-2010-2772

“Siemens Simatic WinCC and PCS 7 SCADA system uses a hard-coded password, which allows local users to access a back-end database and gain privileges, as demonstrated in the wild in July 2010 by the Stuxnet worm”

MS10-046 Vulnerability

Microsoft Security Bulletin MS10-046

Vulnerability in Windows Shell Could Allow Remote Code Execution

The vulnerability could allow remote code execution if the icon of a specially crafted shortcut is displayed … This security update is rated Critical for all supported editions of Microsoft Windows.

First disclosed in CVE-2010-2568 (Jun 30, 2010)

Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer, as demonstrated in the wild in July 2010, and originally reported for malware that leverages CVE-2010-2772 in Siemens WinCC SCADA systems.

Stuxnet Pre-History

- November 20, 2008: Zlob Trojan exploits an unknown vulnerability in Windows shortcuts (LNK)
  - Later identified as MS10-046
- April 2009: security magazine Hakin9 describes a vulnerability in Windows printer spooler service
  - Later identified as MS10-061
- June 22, 2009: earliest version of Stuxnet seen
  - Does not use MS10-046, driver not signed

Stuxnet Timeline (2010)

- January 25: signed Stuxnet driver, valid certificate from Realtek Semiconductor
- June 17: Antivirus company from Belarus reports a new USB rootkit TmpHider
- July 16: Microsoft issues MS10-046
  - Shortcut vulnerability
- July 16: VeriSign revokes Realtek certificate
- July 17: Stuxnet driver with valid certificate from JMicron Technology

Stuxnet Timeline Cont'd (2010)

- July 19: Siemens says they are investigating malware affecting their WinCC SCADA system
  - SCADA = control of industrial machinery
- September 14: Microsoft issues MS10-061
  - Print spooler vulnerability

Stuxnet Firsts

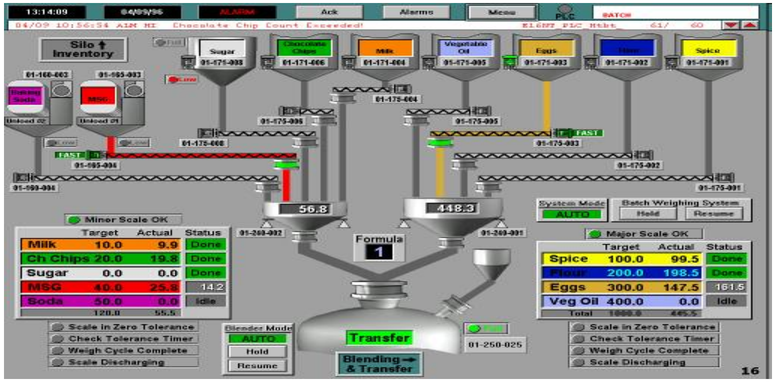
- First to exploit multiple zero-day vulnerabilities
- First to use stolen signing keys and valid certificates of two companies
- First to target industrial control systems – or not?

  … and hide the code from the operator

  … and perform actual sabotage
- First PLC (programmable logic controller) rootkit
- First example of true cyber-warfare?

Industrial Control Systems

- Run automated processes on factory floors, power and chemical plants, oil refineries, etc.
- Specialized assembly code on PLCs (Programmable Logic Controllers)
  - PLCs are usually programmed from Windows
- Not connected to the Internet (“air gap”)



Minor Scale OK

	Target	Actual	Status
Milk	10.0	9.9	Done
Ch Chips	20.0	19.8	Done
Sugar	0.0	0.0	Done
MSG	40.0	25.8	14.2
Soda	50.0	0.0	Idle
	120.0	55.5	

○ Scale in Zero Tolerance
○ Check Tolerance Timer
○ Weigh Cycle Complete
○ Scale Discharging

Major Scale OK

	Target	Actual	Status
Spice	100.0	99.5	Done
Flour	200.0	198.5	Done
Eggs	300.0	147.5	161.5
Veg Oil	400.0	0.0	Idle
Total	1000.0	445.5	

○ Scale in Zero Tolerance
○ Check Tolerance Timer
○ Weigh Cycle Complete
○ Scale Discharging

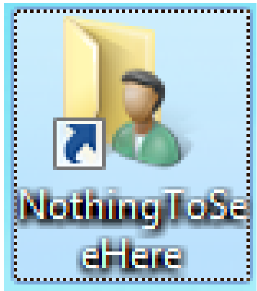
Target: SIEMENS SCADA

- Each PLC is configured and programmed in a unique manner
- Stuxnet targets a specific PLC control system
  - SIMATIC PCS 7 Process Control System
  - Programmed using WinCC/STEP 7

Stuxnet Propagation Methods

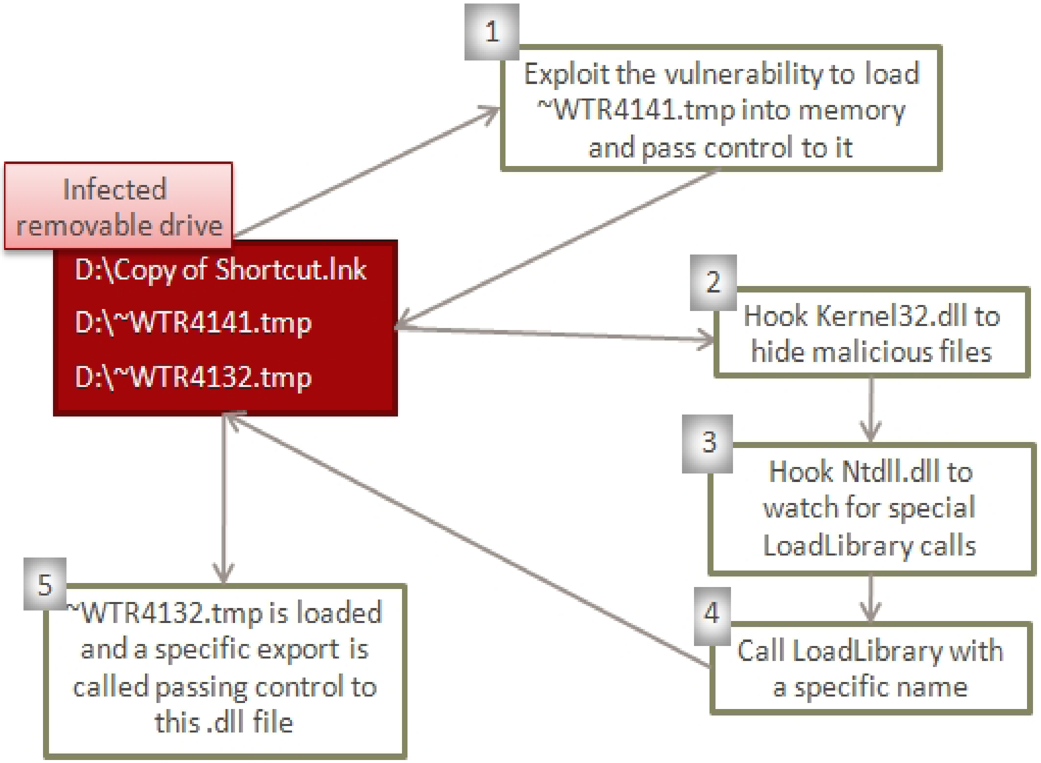
- Initial infection via USB drive (jumps "air gap")
  - Zero-day MS10-046 shortcut exploit + auto-execution
- Several network propagation methods
  - LAN: zero-day MS10-061 print spooler exploit or old MS08-67 RPC exploit (remember Conficker?)
  - Default password to Siemens WinCC database server
  - Network shares
  - Peer-to-peer communication and update mechanism
- Looks for and infects Windows machines running Step 7 control software

USB Infection Vectors



Loaded from a control panel file (CPL) pointing to malicious DLL

LNK Vulnerability (CVE-2010-2568)



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

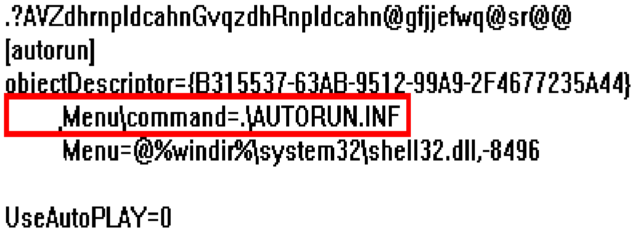
2 Hook Kernel32.dll to hide malicious files

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

Self-executing AutoRun.Inf



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

UseAutoPLAY=0
```

Bypassing Intrusion Detection

- Calls LoadLibrary with a special file name that does not exist
- LoadLibrary fails, but Ntdll.dll has been hooked to monitor for the special file names
- These names are mapped to another location where Stuxnet previously decrypted and stored a DLL file

Gaining Admin Privileges

- If running without administrative privileges, uses zero-day vulnerabilities to become an admin
  - Win 2000, XP: MS10-073 keyboard layout vulnerability
  - Vista, Windows 7: MS10-092 task scheduler vulnerability
- Injects code into a trusted Windows process
  - LSASS or Winlogon
- Injection method depends on the security product used on the infected host
  - Kaspersky KAV, McAfee, AntiVir, BitDefender, Etrust, F-Secure, Symantec, ESET NOD32, PC Cillin

Exploiting MS10-073

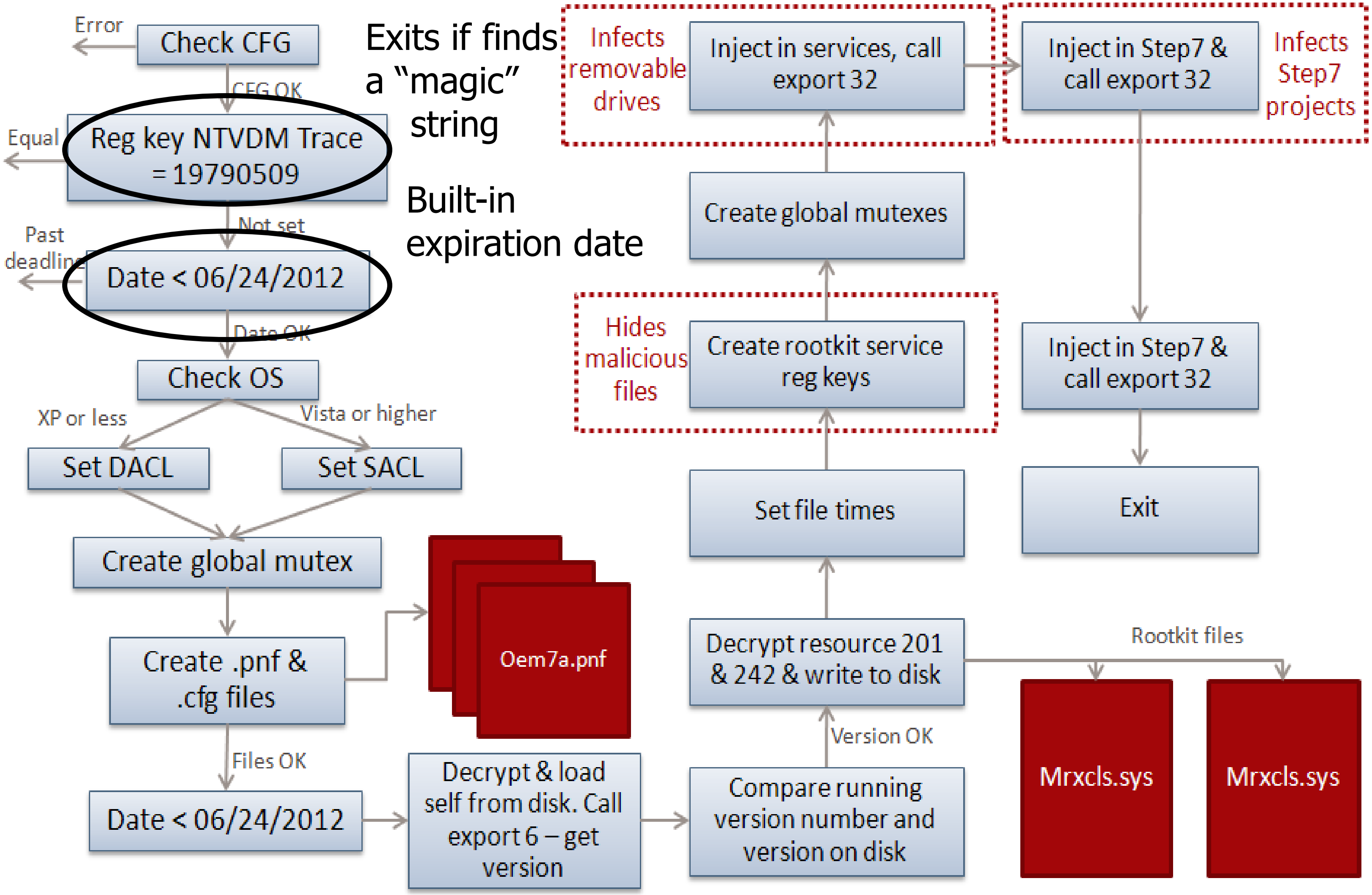
- In Windows XP, a user-level program can load keyboard layout
- Integer in the layout file indexes a global array of function pointers (no bounds checking, natch)
  - Can use this to call any function…
- Find a pointer to this array, find a pointer into user-modifiable memory, inject attack code there, use bad indexing to call modified function
  - Attack code will run with admin privileges

Exploiting MS10-092

[credit: iSEC Partners]

- Users can create and edit scheduled tasks
- CRC32 checksum to prevent tampering
  - "… not suitable for protecting against intentional alteration of data" --- Wikipedia
- Modify user definition in the task to LocalSystem, pad until CRC32 matches the original

Infection Routine Flow



Error

Check CFG

CFG OK

Equal

Reg key NTVDM Trace = 19790509

Exits if finds a “magic” string

Not set

Past deadline

Date < 06/24/2012

Built-in expiration date

Date OK

Check OS

XP or less

Vista or higher

Set DACL

Set SACL

Create global mutex

Create .pnf & .cfg files

Oem7a.pnf

Files OK

Date < 06/24/2012

Decrypt & load self from disk. Call export 6 – get version

Compare running version number and version on disk

Version OK

Decrypt resource 201 & 242 & write to disk

Rootkit files

Mrxcls.sys

Mrxcls.sys

Set file times

Create rootkit service reg keys

Hides malicious files

Create global mutexes

Inject in services, call export 32

Infects removable drives

Inject in Step7 & call export 32

Infects Step7 projects

Inject in Step7 & call export 32

Exit

32 “Exports” (Functionalities)

1	Infects connected removable drives, starts remote procedure call (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

15 “Resources” (Methods)

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 undisclosed win32k.sys vulnerability

Windows Rootkit

- Goal: hide itself when copied to removable drive
- Extracts “Resource 201” as driver MrxNet.sys
  - This driver is digitally signed and registered as a service creating the following registry entry:
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\”ImagePath” = “%System%\drivers\mrxnet.sys”
- Driver filters out (hides) following files:
  - Files with .LNK extension, size of 4,171 bytes
  - Files named “~WTR[four digits].TMP”, size between 4Kb and 8Mb, the sum of the four digits is a multiple of 10

Realtek and JMicron

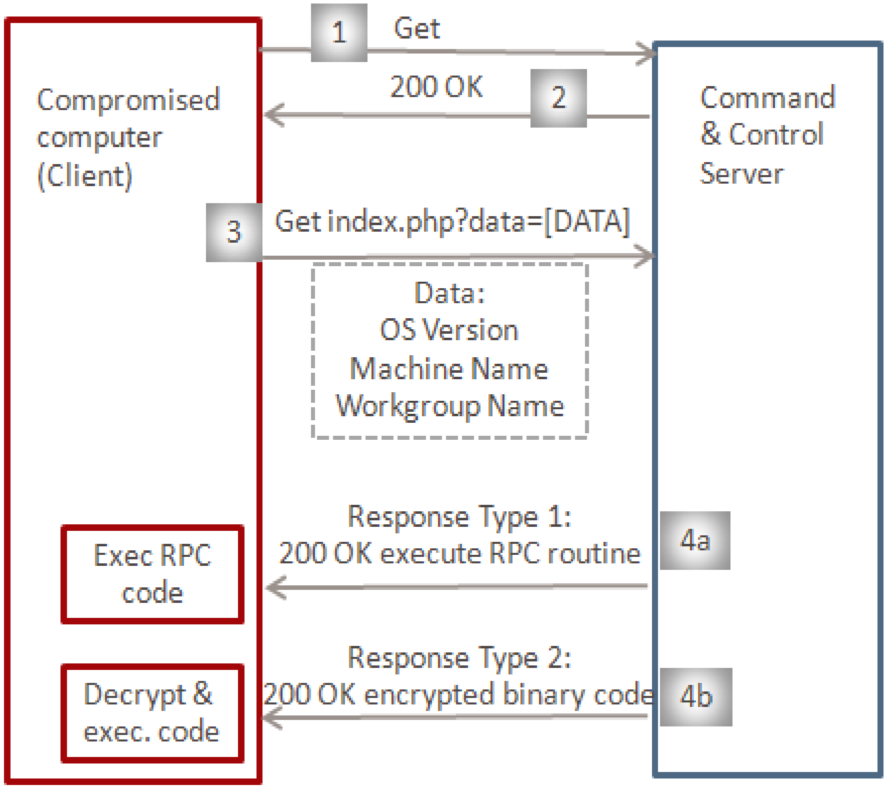
- Stuxnet drivers were signed using stolen keys of two Taiwanese semiconductor companies

- Allegedly located in the same office park
  - Why is this interesting?

Command and Control

- Tests if can connect on port 80 to www.windowsupdate.com, www.msn.com
- Connects to special domains
  - www.mypremierfutbol.com, www.todaysfutbol.com
    - Previously pointed to servers in Malaysia and Denmark
  - Can be updated with other domain names
- Sends encrypted information about infected host
  - Time of infection, IP address and OS version, flag specifying if the host is part of a workgroup or domain, file name of infected Step 7 project

Remote Control of Stuxnet



Compromised computer (Client)

Command & Control Server

1 Get

200 OK 2

3 Get index.php?data=[DATA]

Data:
OS Version
Machine Name
Workgroup Name

Response Type 1:
200 OK execute RPC routine 4a

Response Type 2:
200 OK encrypted binary code 4b

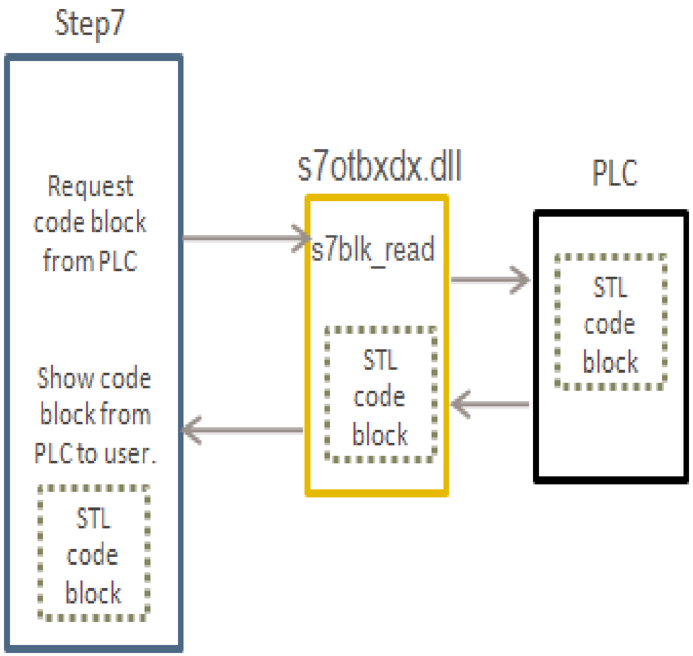
Exec RPC code

Decrypt & exec. code

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

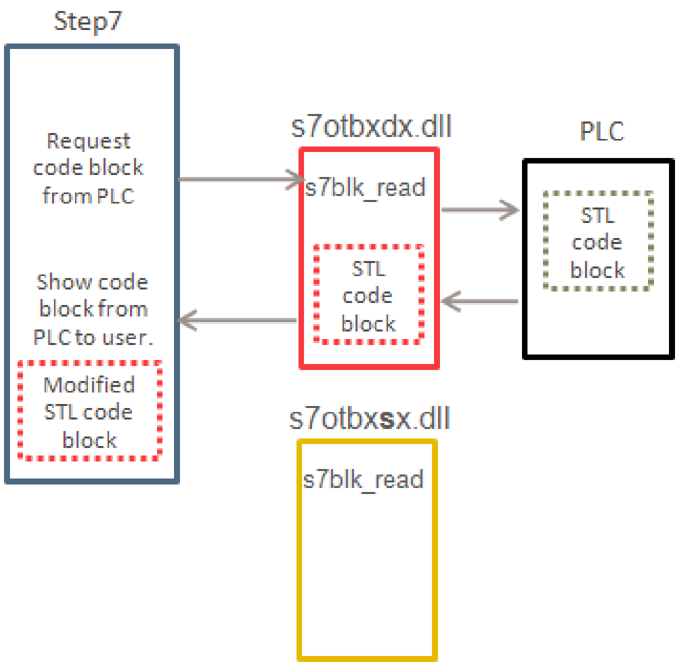
How PLCs Are Programmed

- PLC is loaded with blocks of code and data
  - Code written in low-level STL language
  - Compiled code is in MC7 assembly
- The original s7otbxdx.dll is responsible for handling block exchange between the programming device and the PLC



PLC "Rootkit"

- Stuxnet replaces s7otbxdx.dll with its own DLL
  - Records blocks written to and read from PLC
  - Infects PLC by inserting its own blocks
- PLC "rootkit"
  - Hooks routines that read, write, and enumerate code blocks on PLC
  - Hides infection from PLC operator



Sabotage

- Checks if PLC controls a cascade of at least 33 frequency converter drives manufactured by a specific Iranian or Finnish company
  - A frequency converter drive controls speed of another device – used in water systems, gas pipelines, etc.
- Records normal behavior of PLC
- Executes sequences of commands that rapidly slow down or speed up motors
  - Sequence depends on detected manufacturer
- … while replaying normal behavior to operator

Iranian Nuclear Program

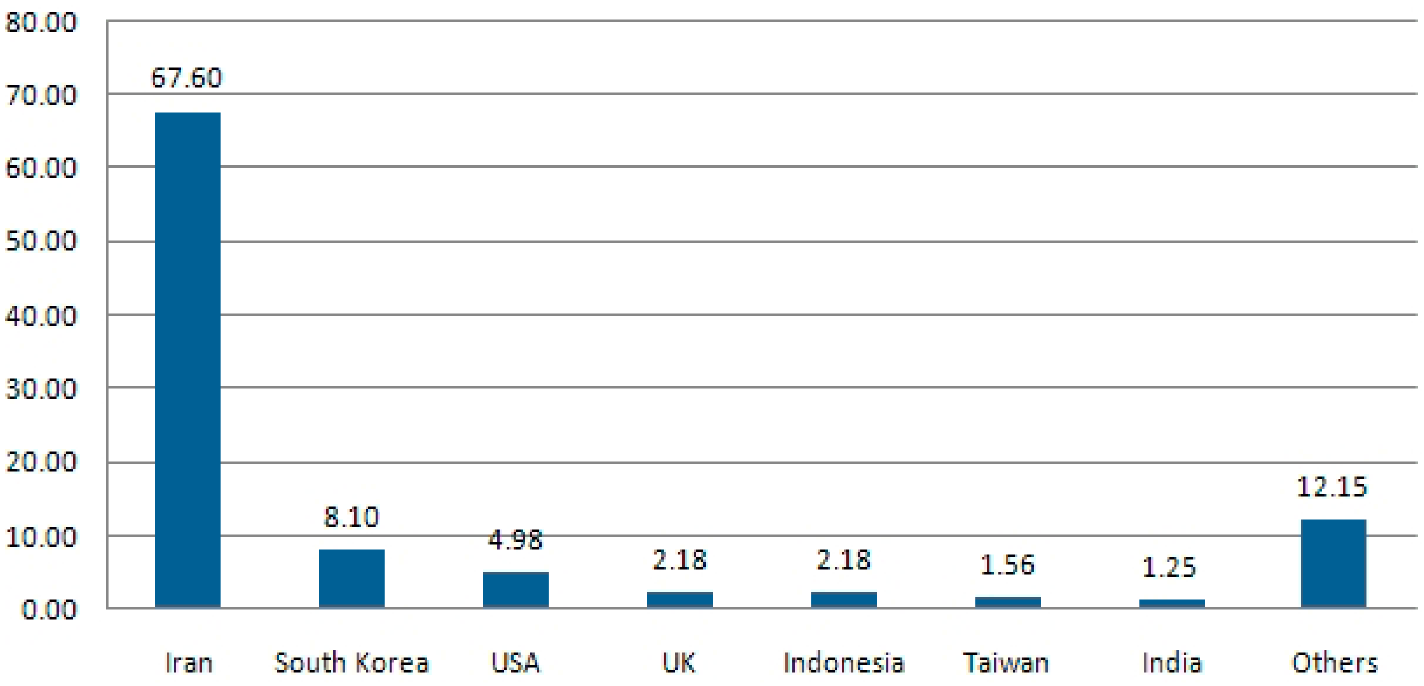
- Sep 2010: “delays”
  - Warm weather blamed
- Oct 2010: “spies” arrested, allegedly attempted to sabotage Iran’s nuclear program
- Nov 2010: Iran acknowledges that its nuclear enrichment centrifuges were affected by a worm
  - Foreign minister: “Nothing would cause a delay in Iran's nuclear activities”
  - Intelligence minister: “enemy spy services” responsible

History of Stuxnet Propagation

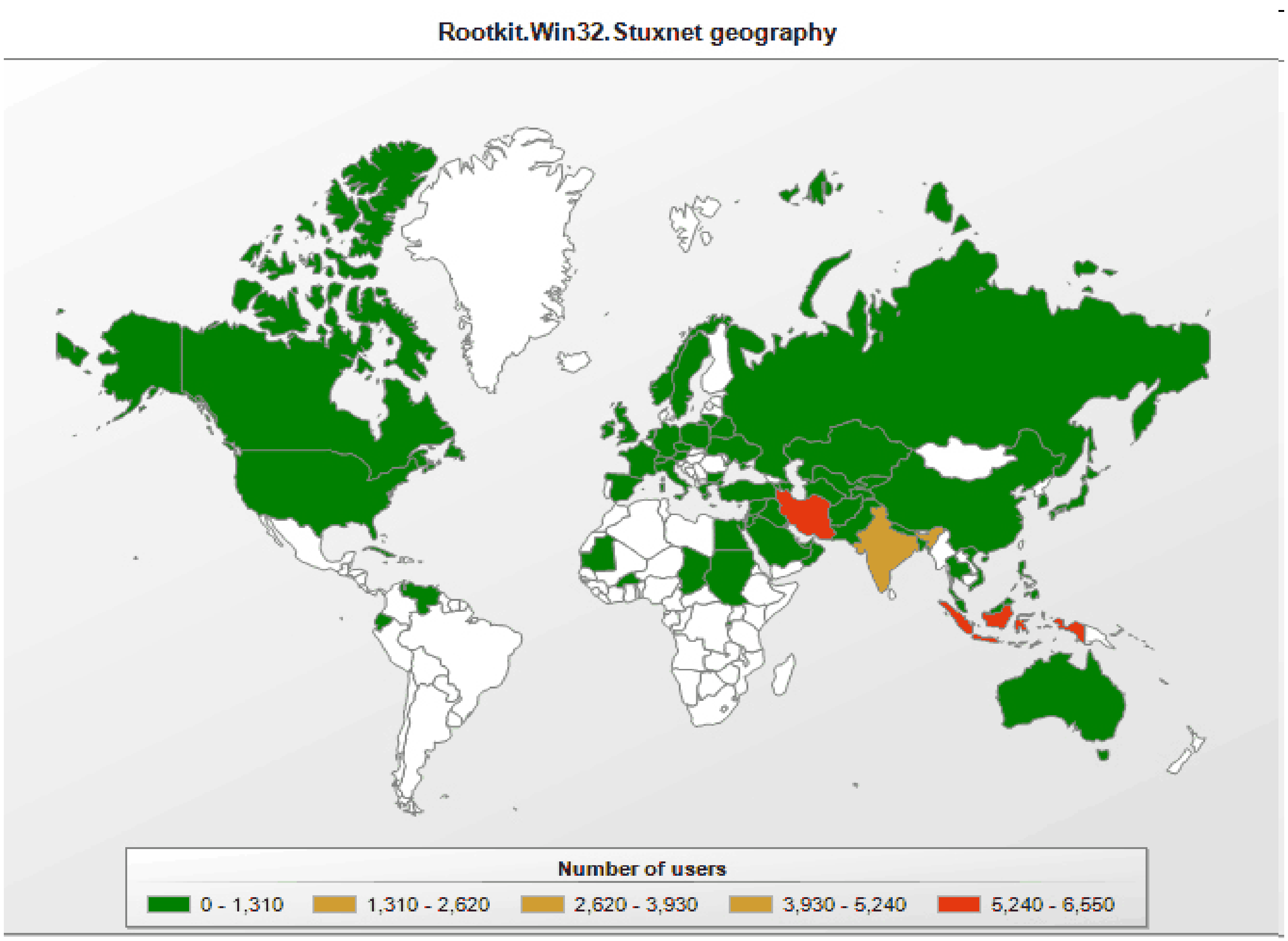
- First wave of attacks targeted 5 organizations inside Iran, starting in June 2009
  - 10 initial infections
  - Shortest span between compile time and initial infection = 12 hours (median = 26 days)
- Multiple propagation mechanisms from there
- 12,000 resulting infections
- True target unknown
  - Possibly the underground enrichment facility at Natanz

Affected Systems

Percentage of Stuxnet-infected hosts with Siemens software installed



Stuxnet Infections Worldwide



Whodunit?

- Stuxnet will not infect systems that contain safe code 19790509
- Habib Elghanian
  - Leader of Iran’s Jewish community
  - Executed by firing squad as an Israeli spy on May 9, 1979
  - One of the first victims of the Islamic revolution

- “Symantec cautions readers on drawing any attribution conclusions. Attackers would have natural desire to implicate another party.”

Another Clue?

"My RTUs" (Remote Terminal Units), similar to PLCs

- Project path in Stuxnet driver:

  b:\myrtus\src\objfire_w2k_x86\i386\guava.pdb

  - Guava is a plant in the myrtle (myrtus) family
- Book of Esther in the Hebrew Bible
  - Esther (born Hadassah) learns that Haman, Persian prime minister, is planning to exterminate all Jews, but foils his plot and has him impaled
  - "Hadassah" is "myrtle" in Hebrew
- "Symantec cautions readers on drawing any attribution conclusions. Attackers would have natural desire to implicate another party."

Flame

- Possibly related to Stuxnet, much more complex
- Exploits an MD5 hash collision attack on Microsoft Update code signing certificate
  - Much more about this later
- Targets mainly in Iran, but also in Lebanon, Syria, Sudan, Israel, and the Palestinian Territories
  - Purpose: espionage rather than industrial sabotage
    - Logs keystrokes, records audio, grabs GPS tags from photos...
  - Possibly developed by the NSA, CIA, and Israeli military as part of the "Olympic Games" campaign against Iranian nuclear program -- Washington Post