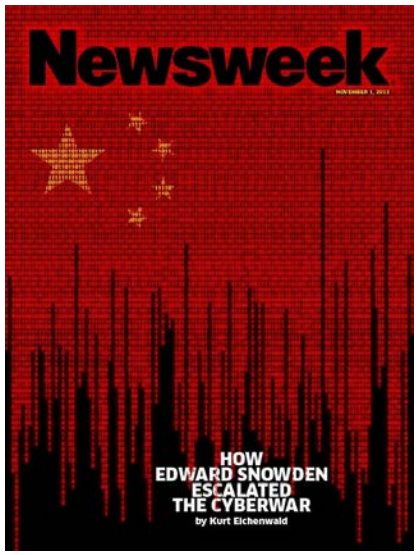
CS 161: Computer Security

Lecture 19

November 19, 2015

Cyberwar in magazine covers



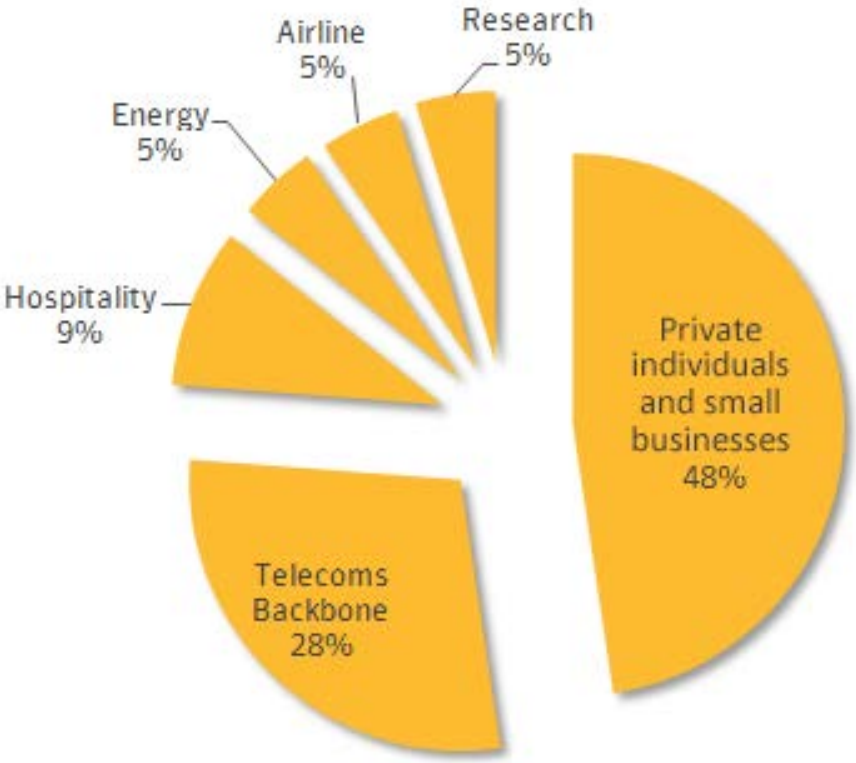
Advanced Persistent Threats (APT)

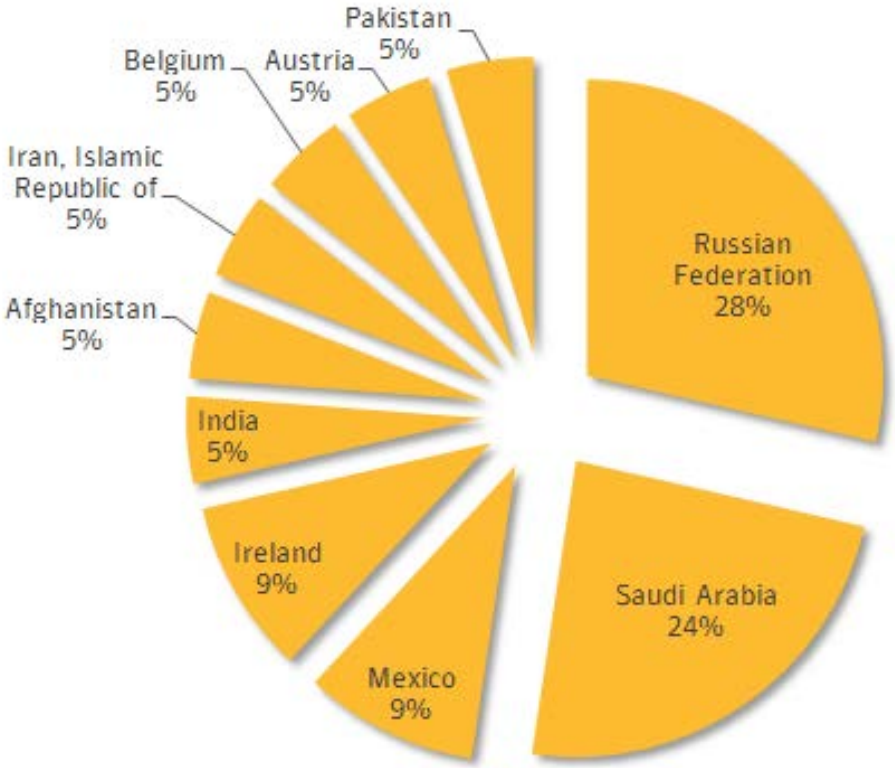
- Associated with large groups
  - Organized crime
  - Nation states
- Targeted rather than opportunistic
- Examples
  - Stuxnet: Industrial sabotage (Iranian uranium enrichment program)
  - Ghostnet: stole diplomatic communications (embassies, Dalai Lama)
  - Aurora: stole source code and other intellectual property (Google)
  - Night Dragon: industrial and commercial intelligence (large oil companies)

Regin

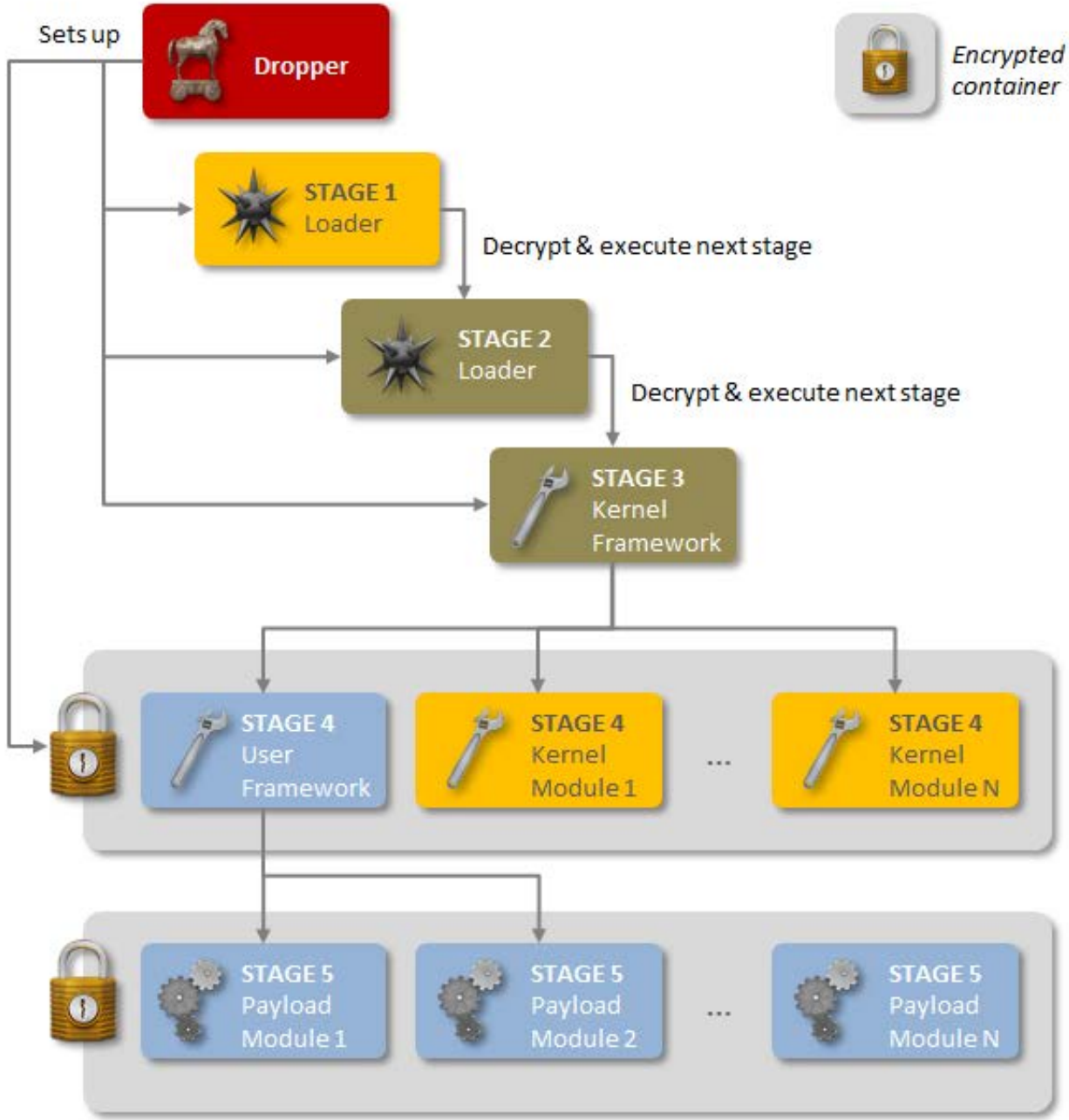
- Symantec announced discovery on Sunday, 24 November 2014.

Regin


Airline
5%
Research
5%
Energy
5%
Hospitality
9%
Private
individuals
and small
businesses
48%
Telecoms
Backbone
28%


Pakistan
5%
Belgium
5%
Austria
5%
Iran, Islamic
Republic of
5%
Afghanistan
5%
India
5%
Ireland
9%
Mexico
9%
Russian
Federation
28%
Saudi Arabia
24%

Regin


Sets up
Dropper
Encrypted container
STAGE 1 Loader
Decrypt & execute next stage
STAGE 2 Loader
Decrypt & execute next stage
STAGE 3 Kernel Framework
STAGE 4 User Framework
STAGE 4 Kernel Module 1
...
STAGE 4 Kernel Module N
STAGE 5 Payload Module 1
STAGE 5 Payload Module 2
...
STAGE 5 Payload Module N

Regin

THE // INTERCEPT FEATURES GREENWALD FROOMKIN DOCUMENTS STAFF CONTACT //

SECRET MALWARE IN EUROPEAN UNION ATTACK LINKED TO U.S. AND BRITISH INTELLIGENCE

BY MORGAN MARQUIS-BOIRE, CLAUDIO GUARNIERI, AND RYAN GALLAGHER @headhntr @rj_gallagher 24 NOV 2014

SHARE

TWITTER

FACEBOOK

GOOGLE

EMAIL

PRINT

Complex malware known as Regin is the suspected technology behind sophisticated cyberattacks conducted by U.S. and British intelligence agencies on the European Union and a Belgian telecommunications company, according to security industry sources and technical analysis conducted by *The Intercept*.

POPULAR


"BURN THIS SHIT DOWN": MAYHEM AND PROTESTS ENGULF FERGUSON


SECRET MALWARE IN EUROPEAN UNION ATTACK LINKED TO U.S. AND BRITISH INTELLIGENCE


THE NEWSROOM: SAUNAS ARE THE LAST BASTIONS OF FREE SPEECH


"DOWN OUTRIGHT MURDER": A COMPLETE GUIDE TO THE SHOOTING OF MICHAEL BROWN BY DARREN WILSON


WALL STREET IS TAKING OVER AMERICA'S PENSION PLANS

Regin

Complex malware known as Regin is the suspected technology behind sophisticated cyberattacks conducted by U.S. and British intelligence agencies on the European Union and a Belgian telecommunications company, according to security industry sources and technical analysis conducted by *The Intercept*.

Regin was found on infected internal computer systems and email servers at Belgacom, a partly state-owned Belgian phone and internet provider, following reports last year that the company was targeted in a top-secret surveillance operation carried out by British spy agency Government Communications Headquarters, industry sources told *The Intercept*.

The malware, which steals data from infected systems and disguises itself as legitimate Microsoft software, has also been identified on the same European Union computer systems that were targeted for surveillance by the National Security Agency.

The hacking operations against Belgacom and the European Union were first revealed last year through documents leaked by NSA whistleblower Edward Snowden. The specific malware used in the attacks has never been disclosed, however.

Regin

The Regin malware, whose existence was first reported by the security firm Symantec on Sunday, is among the most sophisticated ever discovered by researchers. Symantec compared Regin to Stuxnet, a state-sponsored malware program developed by the U.S. and Israel to sabotage computers at an Iranian nuclear facility. Sources familiar with internal investigations at Belgacom and the European Union have confirmed to *The Intercept* that the Regin malware was found on their systems after they were compromised, linking the spy tool to the secret GCHQ and NSA operations.

Ronald Prins, a security expert whose company Fox IT was hired to remove the malware from Belgacom's networks, told *The Intercept* that it was "the most sophisticated malware" he had ever studied.

"Having analyzed this malware and looked at the [previously published] Snowden documents," Prins said, "I'm convinced Regin is used by British and American intelligence services."

Regin

Origin of Regin

In Nordic mythology, the name Regin is associated with a violent dwarf who is corrupted by greed. It is unclear how the Regin malware first got its name, but the name appeared for the first time on the VirusTotal website on March 9th 2011.

Der Spiegel reported that, according to Snowden documents, the computer networks of the European Union were infiltrated by the NSA in the months before the first discovery of Regin.

Industry sources familiar with the European Parliament intrusion told *The Intercept* that such attacks were conducted through the use of Regin and provided samples of its code. This discovery, the sources said, may have been what brought Regin to the wider attention of security vendors.

Regin family

- Stuxnet
- Flame
- Duqu
- Regin

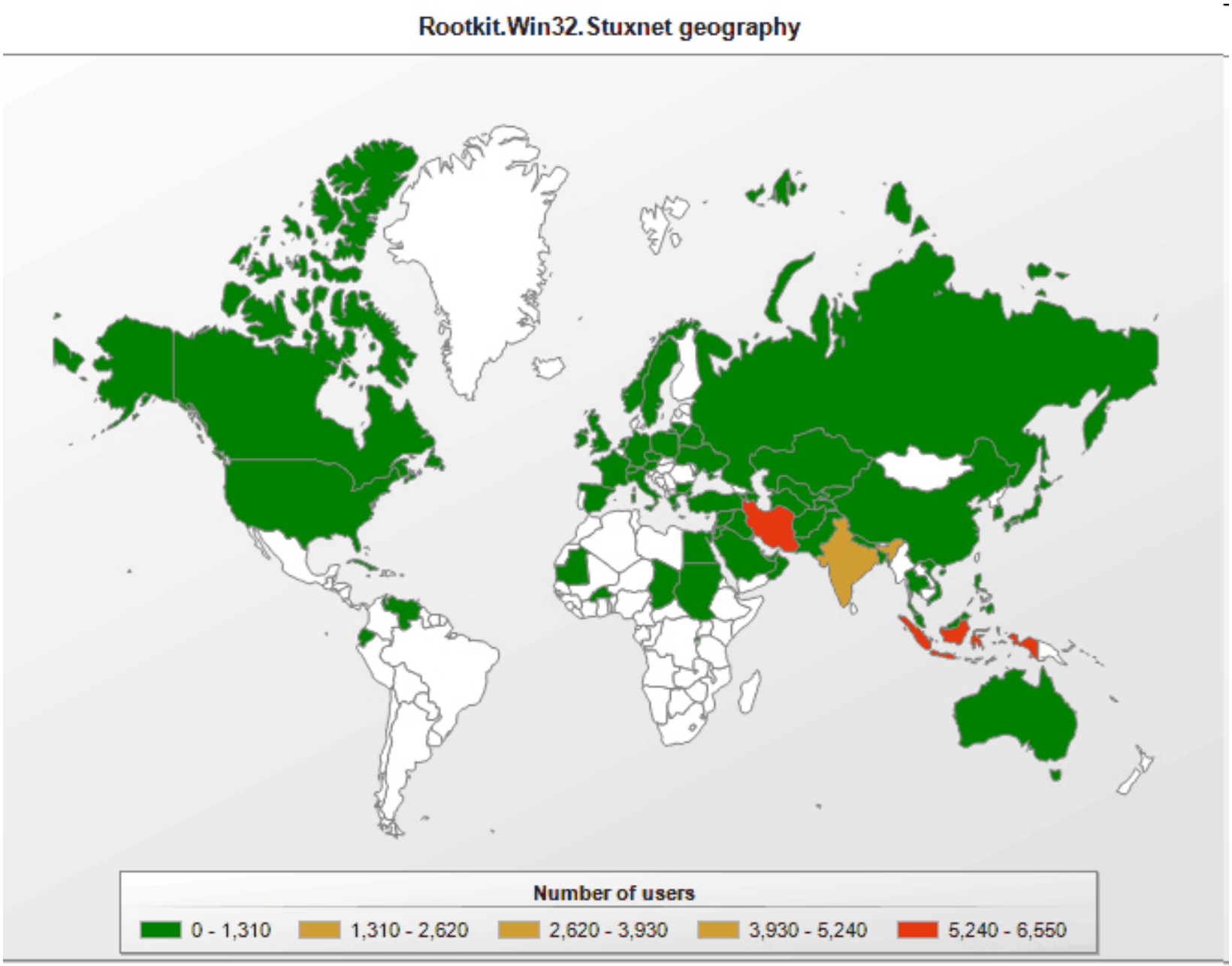
Natanz, Iran:
Uranium Enrichment Facility

Natanz, Iran:
Uranium Enrichment Facility

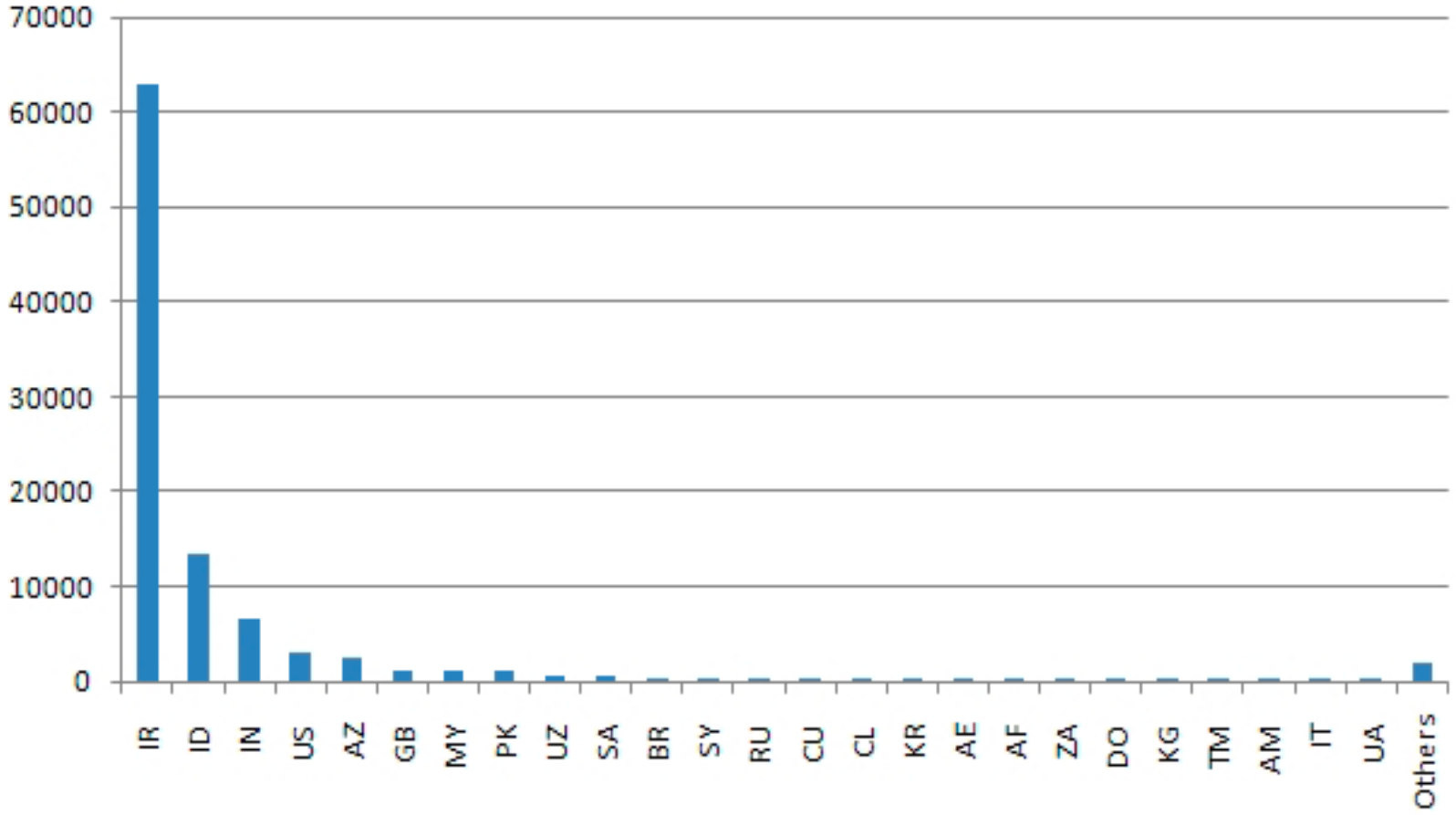
“Most Sophisticated Worm Ever”

- Targets Siemens S7/WinCC products, compromises S7 PLC's to sabotage physical process
- Exploited 4 Windows zero-day vulnerabilities
- Spreads via:
  - USB/Removable Media
  - 3 Network Techniques
  - S7 Project Files
  - WinCC Database Connections
- Drivers digitally signed with legitimate (stolen) RealTek and JMicron certificates
- Installs cleanly on W2K through Win7/2008R2
- Conventional OS rootkit, detects and avoids major anti-virus products
- Advanced reverse-engineering protections

Target: Iran


Rootkit.Win32.Stuxnet geography
Number of users
0 - 1,310
1,310 - 2,620
2,620 - 3,930
3,930 - 5,240
5,240 - 6,550

Infection stats (9/29/2010)

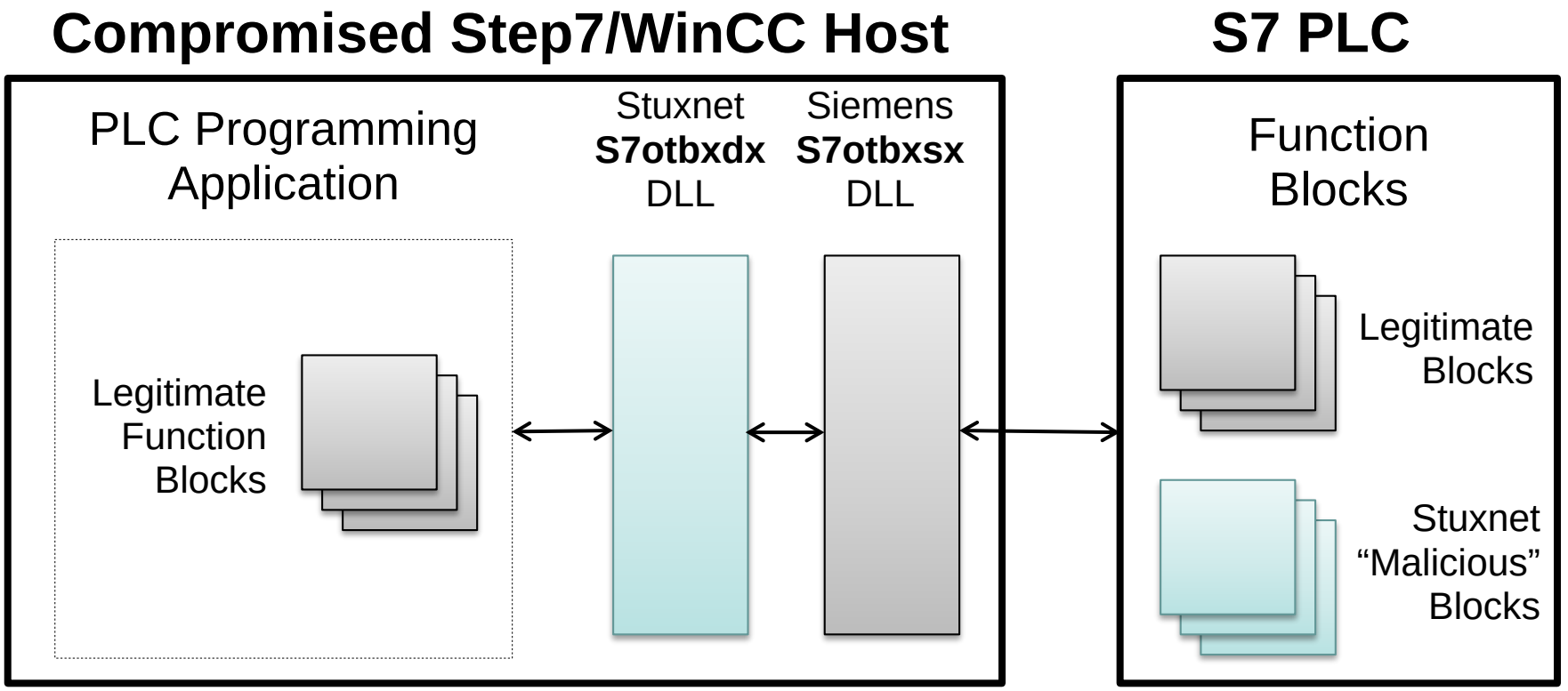


Nuclear Centrifuge Technology

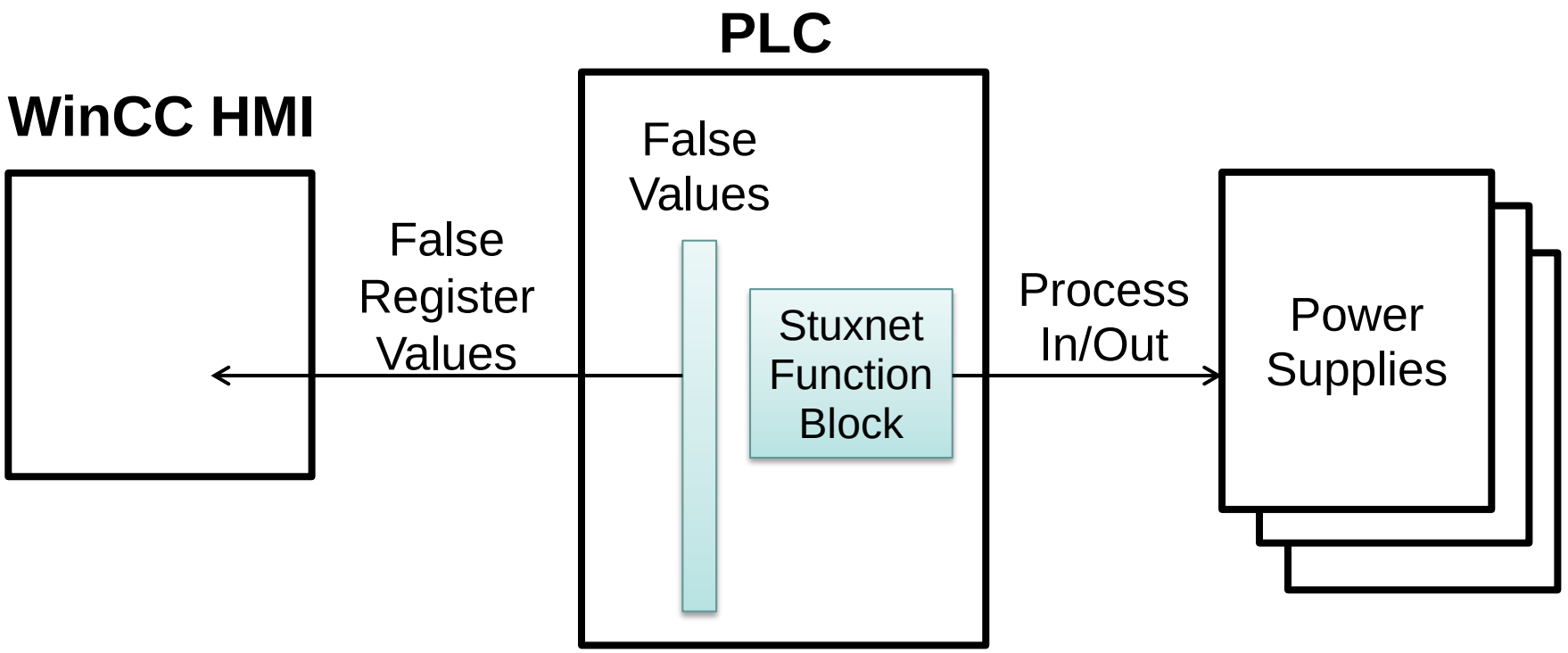
- Uranium-235 separation efficiency is critically dependent on the centrifuges' speed of rotation
- Separation is theoretically proportional to the peripheral speed raised to the 4th power. So any increase in peripheral speed is helpful.
- That implies you need strong tubes, but brute strength isn't enough: centrifuge designs also run into problems with "shaking" as they pass through naturally resonant frequencies
  - "shaking" at high speed can cause catastrophic failures to occur.
  - www.fas.org/programs/ssp/nukes/fuelcycle/centrifuges/engineering.html

“Shaking”

PLC Rootkit


Compromised Step7/WinCC Host
S7 PLC
PLC Programming Application
Stuxnet
S7otbxdx
DLL
Siemens
S7otbxsx
DLL
Function Blocks
Legitimate Function Blocks
Legitimate Blocks
Stuxnet "Malicious" Blocks

Man in the Middle



Siemens SIMATIC PCS7 Line

- “Functional” components:
  - Operator System (OS)
  - Automation System (AS)
  - Engineering System (ES)
- “Software” components:
  - OS Server + Client
  - WinCC Server + Client
  - Web Navigation Server
  - OS Web Server
  - Central Archive Server (CAS)
  - Engineering Station

How Stuxnet Infects a System

Infected Removable Media:

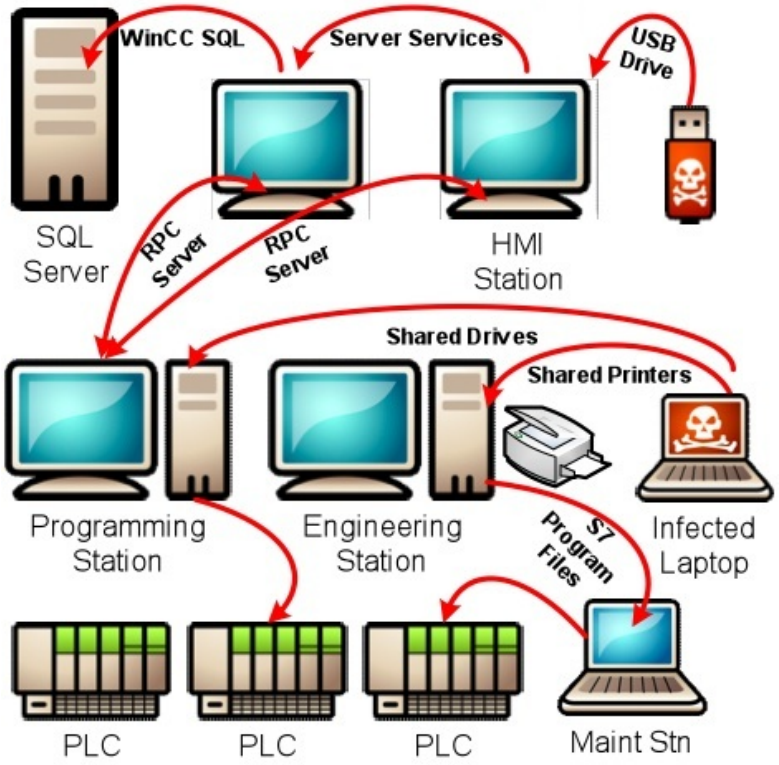
1. Exploits vulnerability in Windows Shell handling of .lnk files (0-day)
2. Used older vulnerability in autorun.inf to propagate

Local Area Network Communications:

3. Copies itself to accessible network shares, including administrative shares
4. Copies itself to printer servers (0-day)
5. Uses “Conficker” vulnerability in RPC

Infected Siemens Project Files:

6. Installs in WinCC SQL Server database via known credentials
7. Copies into STEP7 Project files



How Stuxnet Infects a System

- All Windows Hosts
  - Installs rootkit and loader
  - Creates configuration and data files
  - Propagates to other potential hosts

- Siemens PCS7 STEP7 Hosts
  - Wraps S7 Device OS driver (MitM + PLC rootkit)
  - Looks for specific PLC models
    - Infects S7 Project files
    - PROFIBUS driver replaced

- Siemens PCS7 WinCC Hosts
  - Infects WinCC SQL Server database files

- Target System
  - Injects 1 of 3 different payloads into PLC

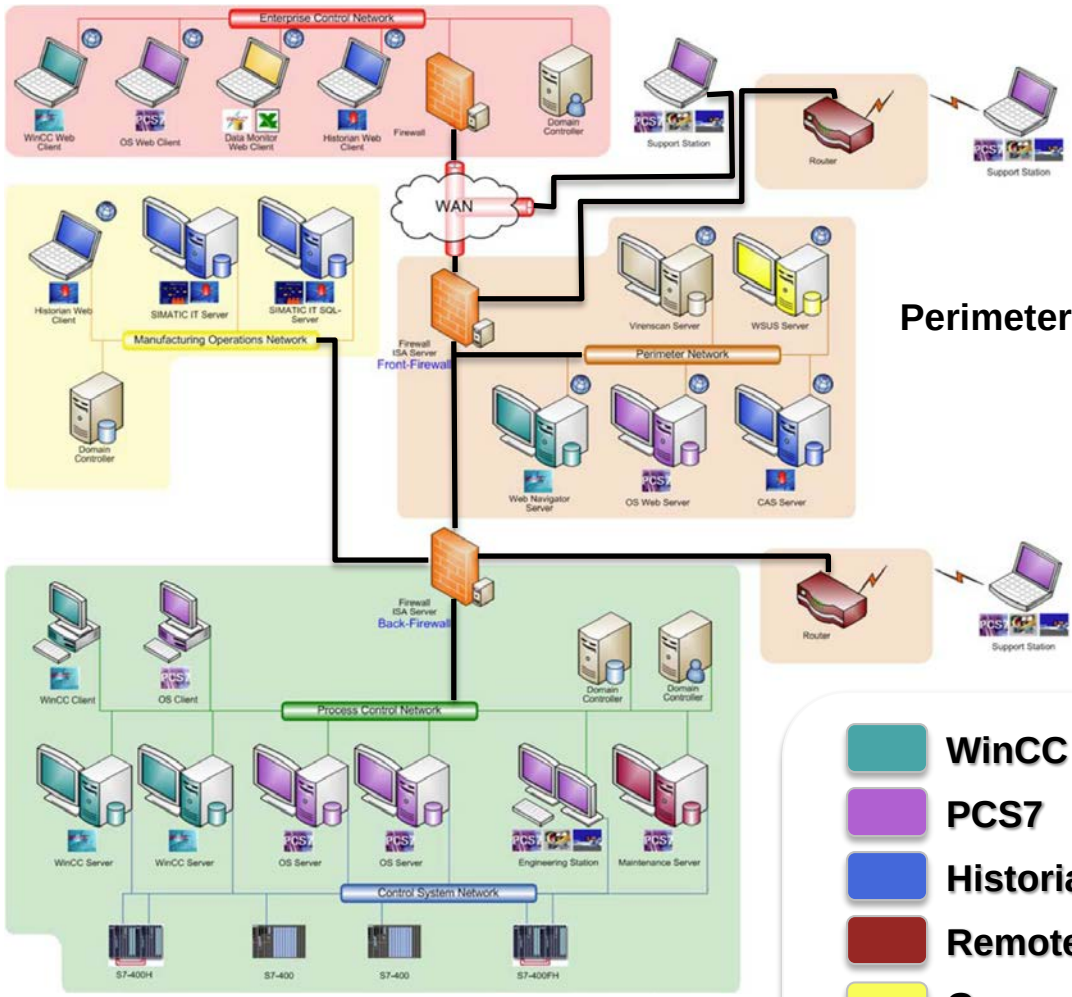
High Security Site

Enterprise Control Network

Manufacturing Operations Network

Process Control Network

Control System Network



Perimeter Network

WinCC

PCS7

Historian

Remote Access

General Purpose

Source: "Security Concept PCS7 and WinCC – Basic Document", Siemens, Apr. '08

Stuxnet Spreads

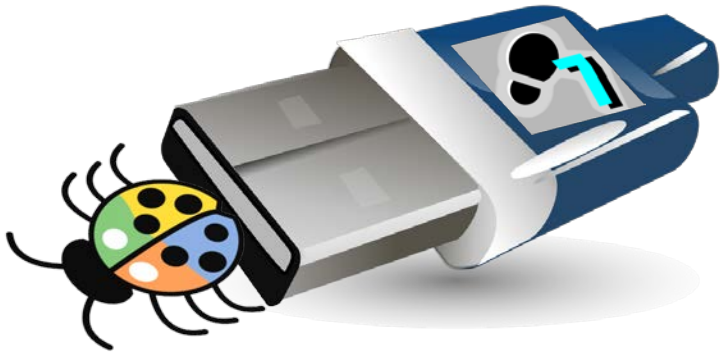
- Date is May 1, 2010
- Stuxnet has been refined for over 12 months
- Is installed on a single USB flash drive
- No patches exist for the 0-days used
- No anti-virus signatures exist
- Security researchers are unaware of the attack

Bypassing Intrusion Detection

- Stuxnet calls LoadLibrary
  - With a specially crafted file name that does not exist
  - Which causes LoadLibrary to fail.
- However, W32.Stuxnet has hooked Ntdll.dll
  - To monitor specially crafted file names.
  - Mapped to a location specified by W32.Stuxnet.
  - Where a .dll file was stored by the Stuxnet previously.

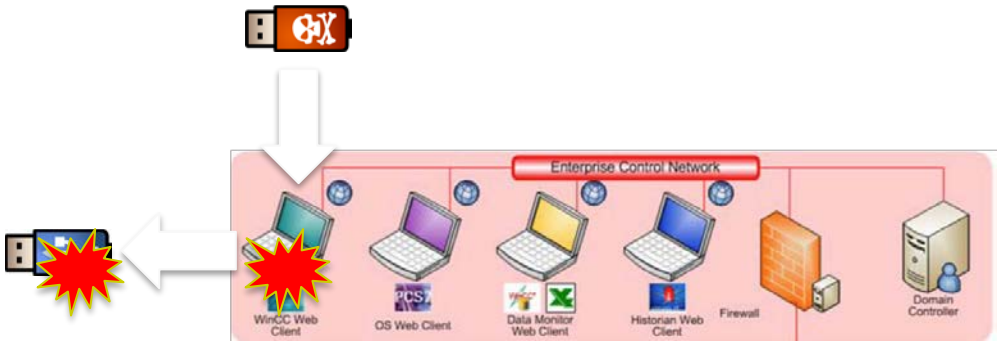
Initial Handoff of the Worm

- Employee is transmitted project files from an offsite contractor on a USB flash drive



First Infection: Enterprise Computer

- Infected USB drive inserted into computer
- Even though computer is fully patched and current with anti-virus signatures, worm successfully installs
- Rootkit installed to hide files
- Attempts connection to C&C server for updates
- Infects any new USB Flash drive inserted into computer

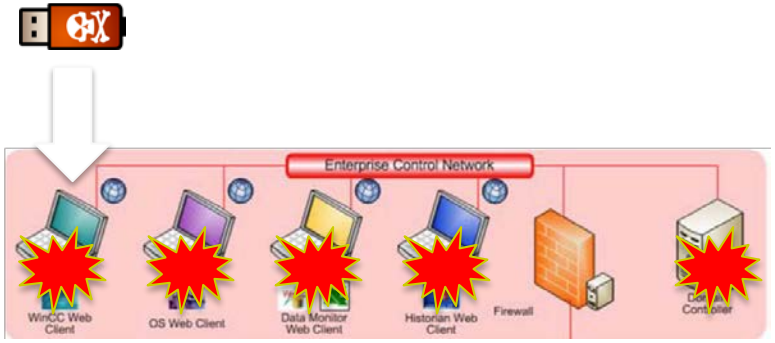


Code Injection

- Stuxnet used trusted Windows processes or security products
  - Lsass.exe
  - Winlogin.exe
  - Svchost.exe
  - 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)
- Stuxnet detects the version of the security product and based on the version number adapts its injection process

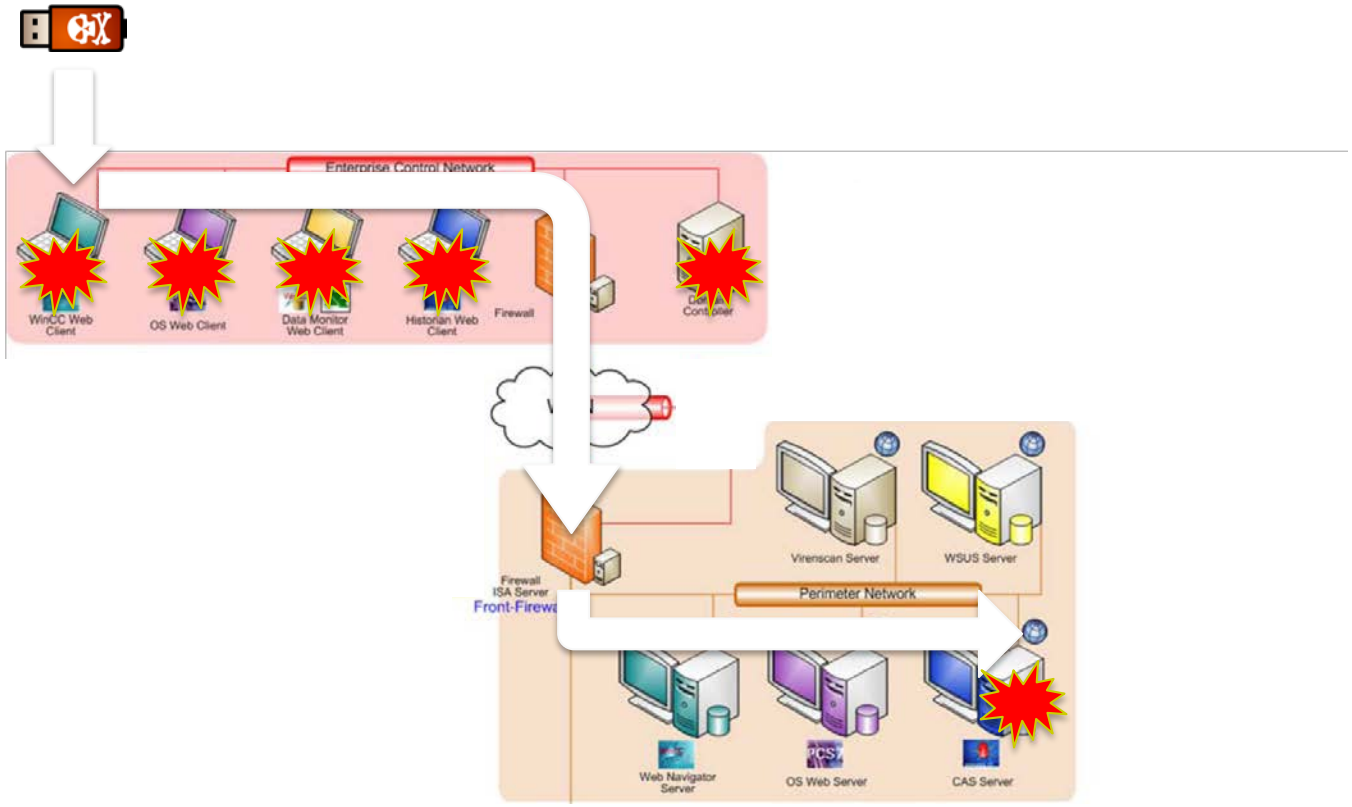
Propagation on Enterprise Network

- Rapidly spreads to Print Servers and File Servers within hours of initial infection
- Establishes P2P network and access to C&C server
- Infects any new USB Flash drive inserted into computer



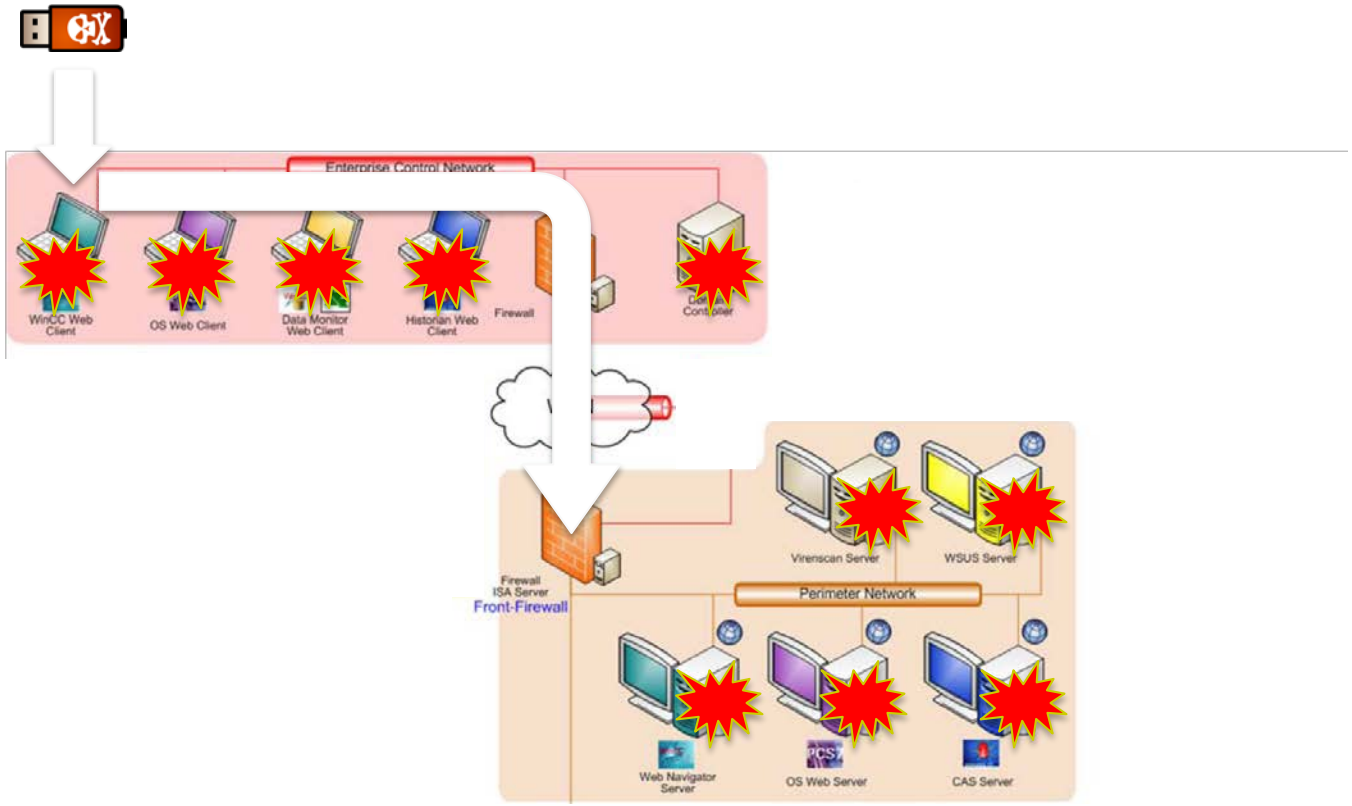
Penetrating Perimeter Network

- System Admin (Historian) becomes infected through network printer and file shares
- System Admin connects via VPN to Perimeter Network and infects the CAS Server and its WinCC SQL Server database



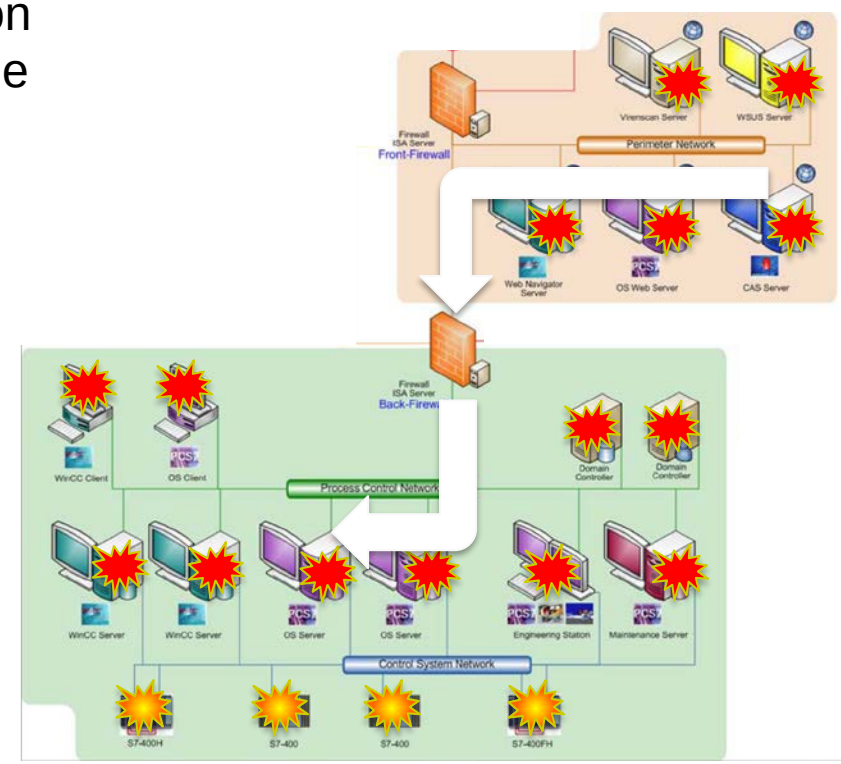
Propagation on Perimeter Network

- Infects Web Navigation Server's WinCC SQL Server
- Infects STEP 7 Project files used in Web Navigation Server Terminal Services feature
- Infects other Windows hosts on the subnet like WSUS, ADS, AVS



Propagation to Control Networks

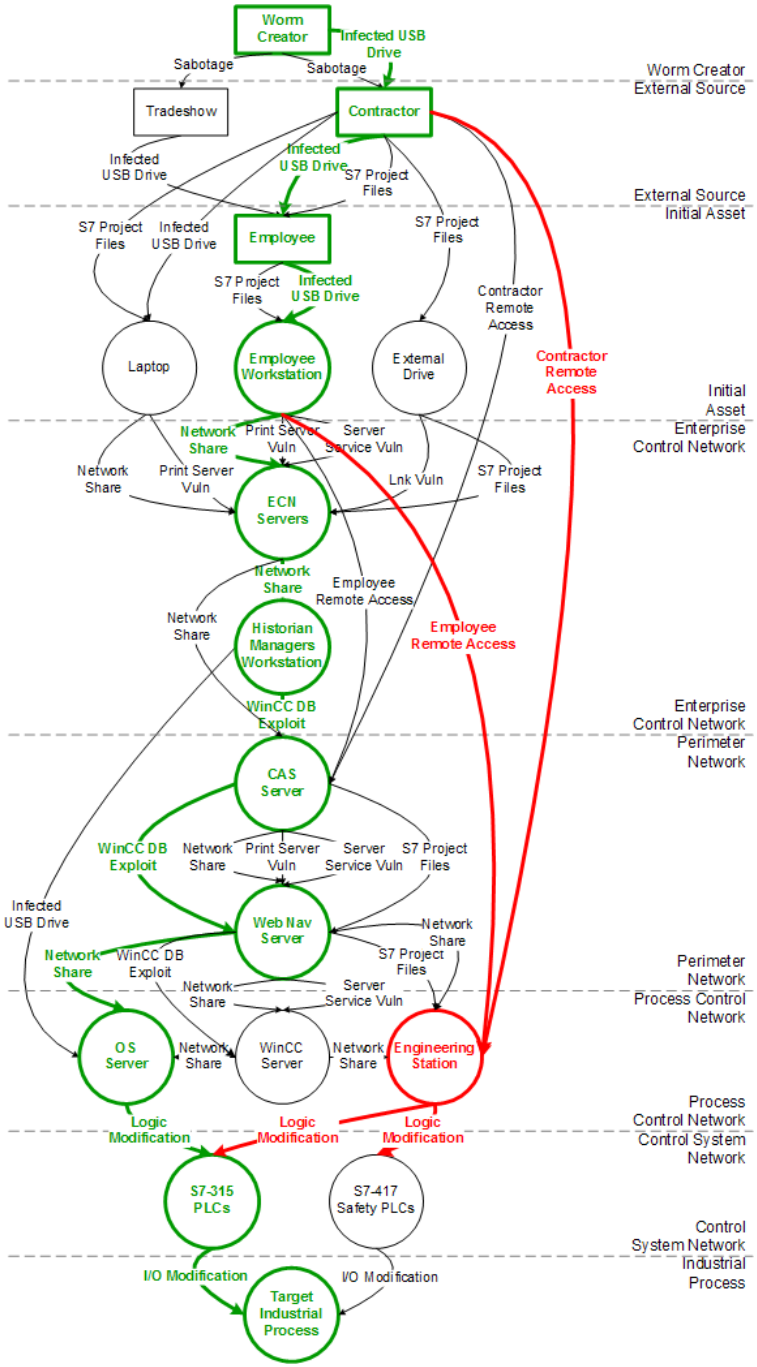
- Leverages network connections between Perimeter and Process Control Network
- Exploits database connections between CAS Server (Perimeter) and OS Server (PCN)
- Infects other hosts on PCN via Shares, WinCC or STEP7 methods
- Identifies target configuration and modifies PLC logic while hiding from users



Attack vectors

- Stuxnet used seven different infection methods

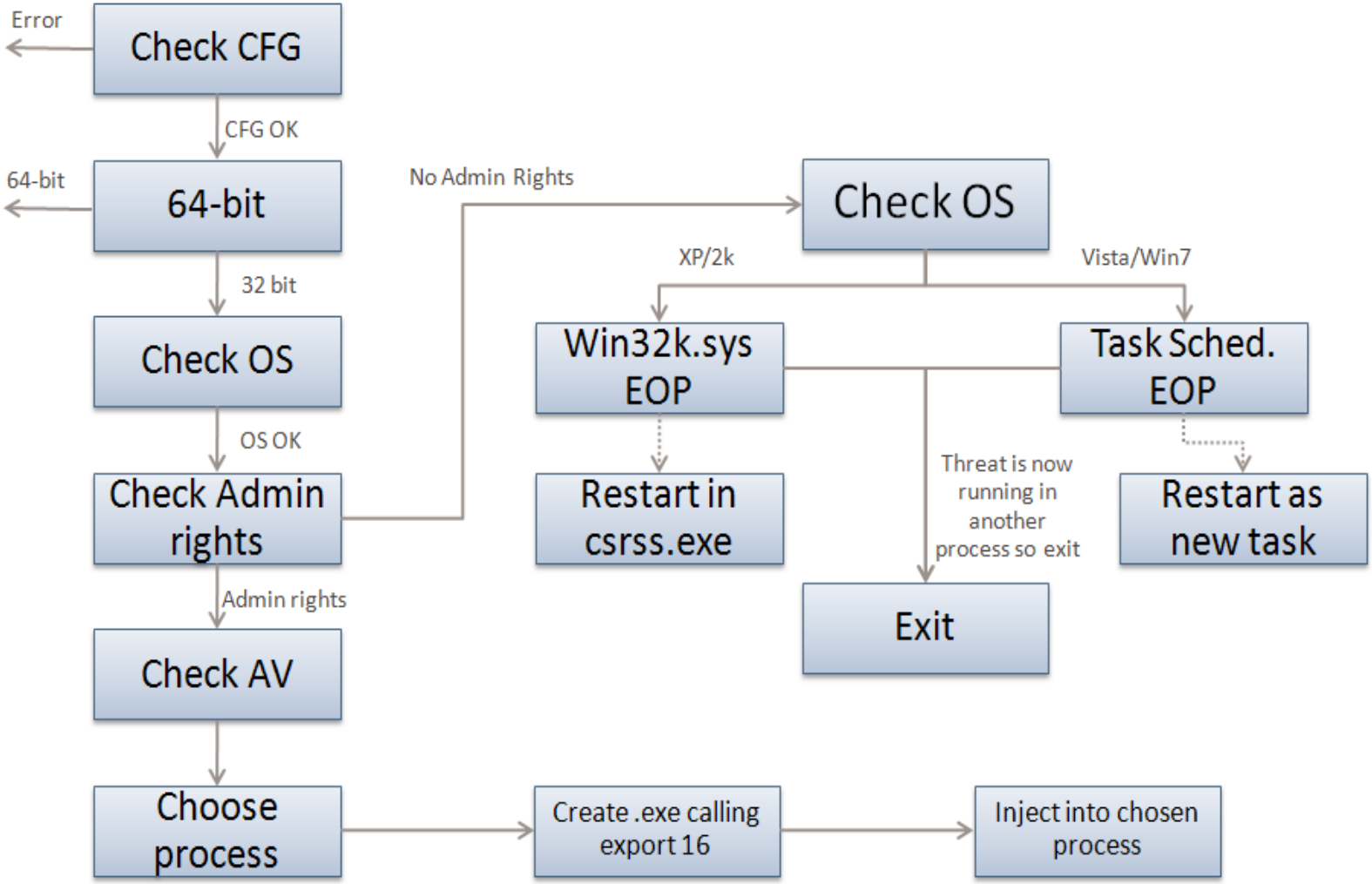
- How many attacks vectors do you think this exposes?


Worm Creator
Infected USB Drive
Sabotage
Sabotage
Worm Creator External Source
Tradeshow
Contractor
Infected USB Drive
Infected USB Drive
S7 Project Files
External Source Initial Asset
S7 Project Files
Infected USB Drive
Employee
S7 Project Files
S7 Project Files
Contractor Remote Access
Infected USB Drive
Laptop
Employee Workstation
External Drive
Contractor Remote Access
Initial Asset Enterprise Control Network
Network Share
Print Server Vuln
Server Service Vuln
Network Share
Print Server Vuln
Lnk Vuln
S7 Project Files
ECN Servers
Network Share
Employee Remote Access
Network Share
Historian Managers Workstation
Employee Remote Access
WinCC DB Exploit
Enterprise Control Network Perimeter Network
CAS Server
WinCC DB Exploit
Network Share
Print Server Vuln
Server Service Vuln
S7 Project Files
Infected USB Drive
Web Nav Server
Network Share
Network Share
WinCC DB Exploit
S7 Project Files
Perimeter Network Process Control Network
Network Share
Server Service Vuln
OS Server
Network Share
WinCC Server
Network Share
Engineering Station
Process Control Network Control System Network
Logic Modification
Logic Modification
Logic Modification
S7-315 PLCs
S7-417 Safety PLCs
Control System Network Industrial Process
I/O Modification
I/O Modification
Target Industrial Process

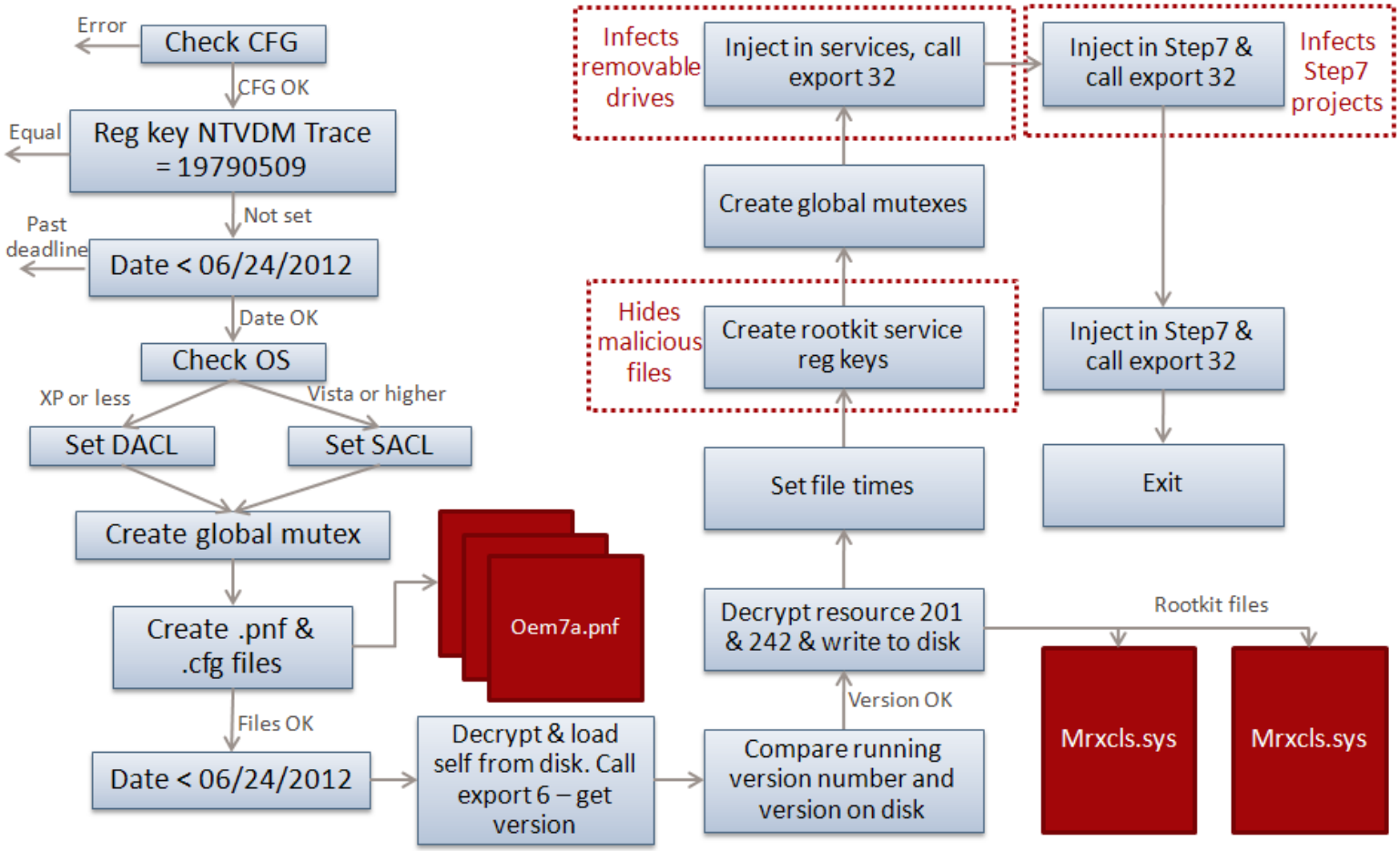
Configuration

- Stuxnet collects and stores the following information:
  - Major OS Version and Minor OS Version
  - Flags used by Stuxnet
  - Flag specifying if the computer is part of a workgroup or domain
  - Time of infection
  - IP address of the compromised computer
  - file name of infected project file

Installation: Control Flow



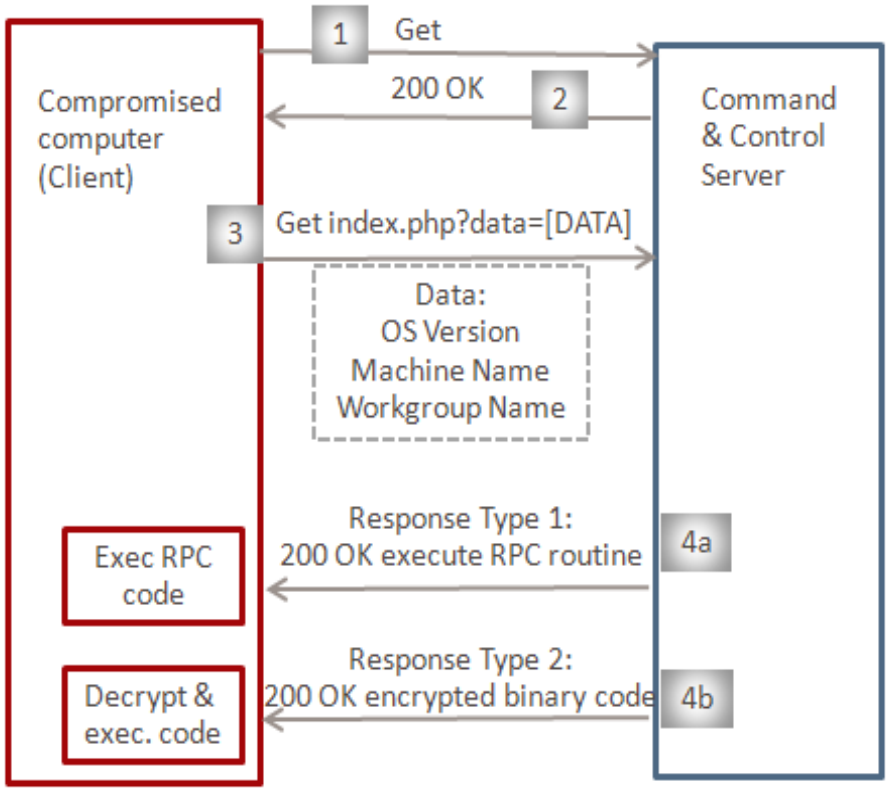
Installation: Infection routine flow



Command & Control

- Stuxnet tests if it can connect to
  - www.windowsupdate.com
  - www.msn.com
  - On port 80
- Contacts the command and control server
  - www.mypremierfutbol.com
  - www.todaysfutbol.com
  - The two URLs above previously pointed to servers in Malaysia and Denmark
  - Sends info about the compromised computer

Command & Control (2)



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

Command & Control payload

Part 1

0x00 byte 1, fixed value
0x01 byte from Configuration Data
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
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

Part 2

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 0x10 byte unused

0x11 string copy of S7P string from C. Data (418h)

Windows Rootkit Functionality

- Stuxnet extracts Resource 201 as MrxNet.sys.
  - Registered as a service:
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\”ImagePath” = “%System%\drivers\mrxnet.sys”
  - Digitally signed with a legitimate Realtek digital certificate.
- The driver then hides files that:
  - have “.LNK” extension.
  - are named “~WTR[four numbers].TMP”,
    - the sum of the four numbers, modulo 10 is 0.
  - size between 4Kb and 8Mb;
  - Examples:
    - “Copy of Copy of Copy of Copy of Shortcut to.lnk”
    - “Copy of Shortcut to.lnk”
    - “~wtr4141.tmp”

Propagation Methods: Network

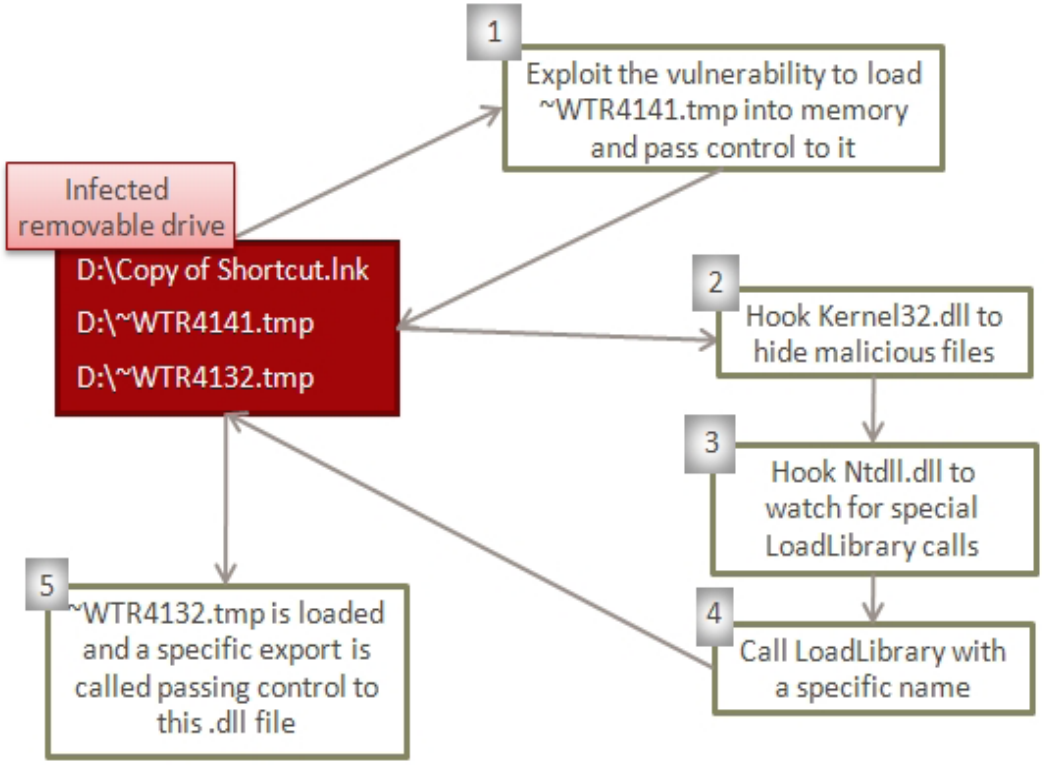
- Peer-to-peer communication and updates
- Infecting WinCC machines via a hardcoded database server password
- Network shares
- MS10-061 Print Spooler Zero-Day Vulnerability
- MS08-067 Windows Server Service Vulnerability

Propagation Methods: USB

- LNK Vulnerability (CVE-2010-2568)
- AutoRun.Inf

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

UseAutoPLAY=0
```



Modifying PLC's

- The end goal of Stuxnet is to infect specific types of PLC devices.
- PLC devices are loaded with blocks of code and data written in STL
- The compiled code is in assembly called MC7.
  - These blocks are then run by the PLC, in order to execute, control, and monitor an industrial process.
- The original s7otbxdx.dll is responsible for handling PLC block exchange between the programming device and the PLC.
  - By replacing this .dll file with its own, Stuxnet is able to perform the following actions:
    - Monitor PLC blocks being written to and read from the PLC.
    - Infect a PLC by inserting its own blocks

Modifying PLC's