BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session No: 16 (Stuxnet Virus)

Agenda

- Case Study: Stuxnet Virus
  - Overview
  - Technical Details

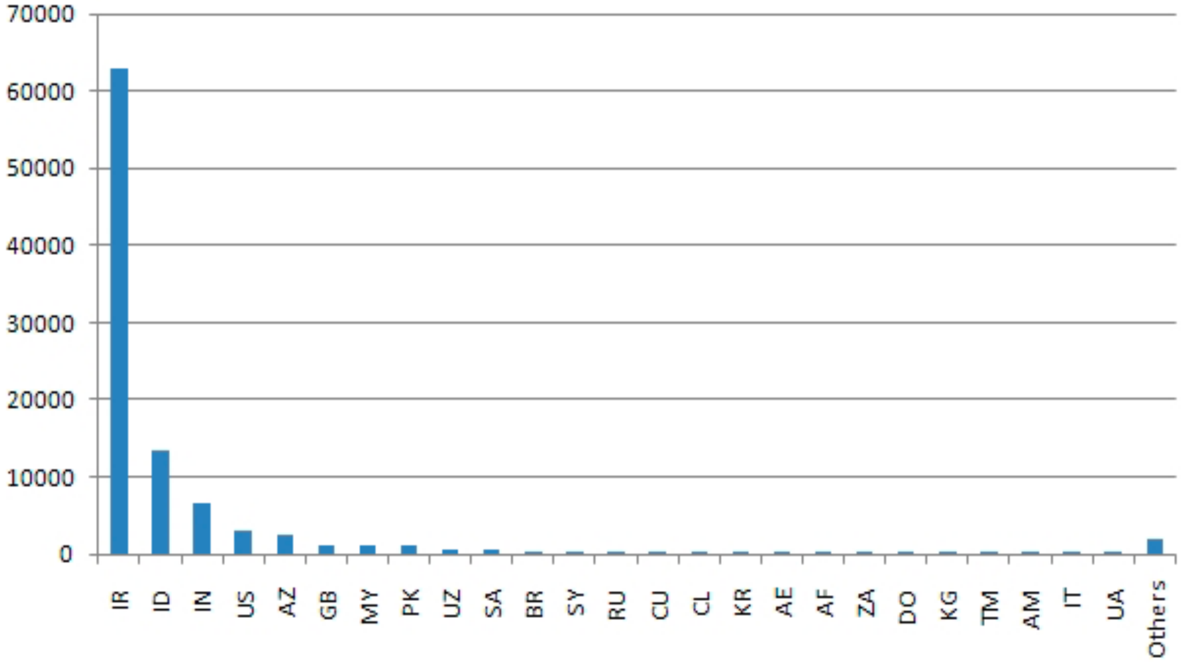
StuxNet

Overview

- June 2010: A worm targeting Siemens Win CC industrial control systems.
- Targets high speed variable program logic controllers from two vendors: Vacon (Finland) and Fararo Paya (Iran)
- Activates only when controllers are running at 807 Hz to 1210 Hz
- Makes the frequency of those controllers from 1410 Hz to 2 Hz to 1064 Hz (84600 rpm to 120 rpm to 63840 rpm)

Infection Status

- AS of 29-Sep-2010



Industrial Control Systems (ICS)

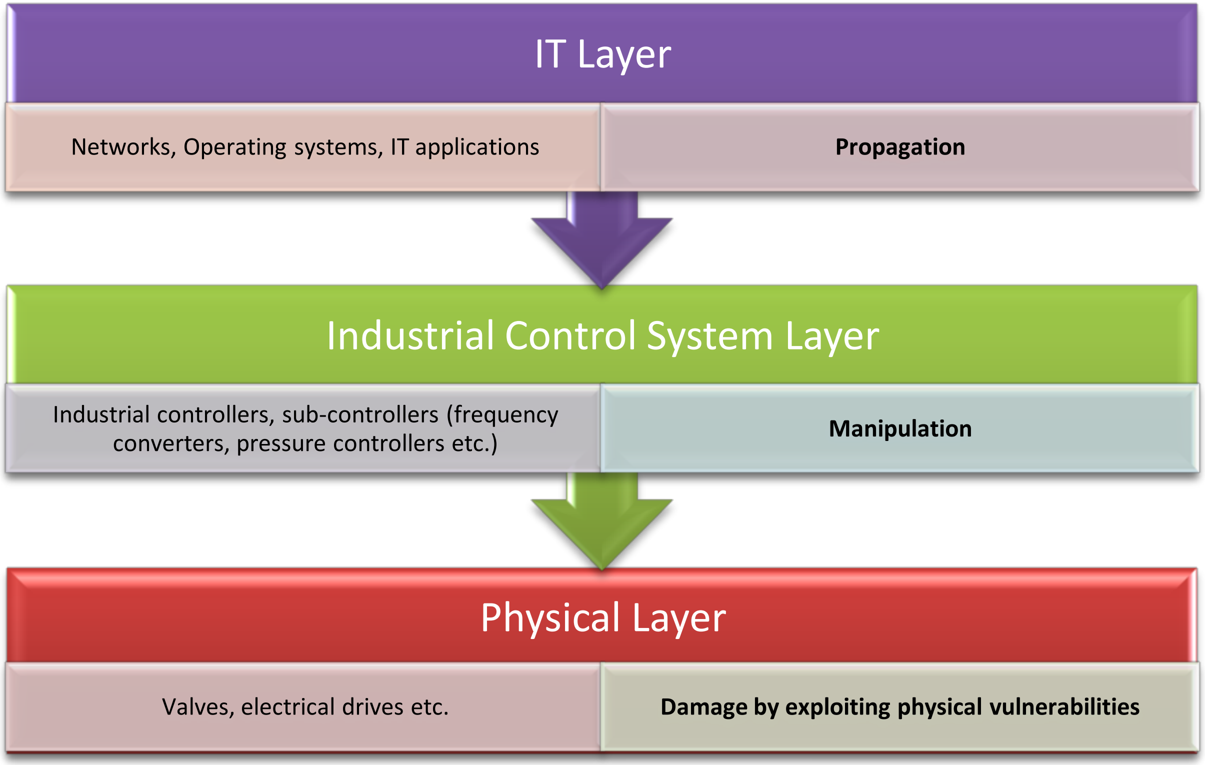
- ICS are operated by special Assembly like code on Programmable Logic Controllers (PLCs)
- The PLCs are programmed typically using Windows computers.
- The ICS are not connected to internet
- ICS usually consider availability and ease of maintenance first and security last
- ICS considers the “airgap” as sufficient security

ICS Environment

Denomination:	**PG/HMI** (Programming Gateway / Human-Machine Interface)	**PLC** (Programmable Logic Controller)	**Field Device**
Function:	Uploads executable instructions into the PLC (i.e. via a serial or Profibus interface), controls and monitors PLC operations	Manages the connected device and reports status of operations to a visualisation workstation	Ad-hoc operation. (i.e. regulates the rotation speed of an electric engine)
Example:	Intel-based computer with Windows XP O.S.	Simatic S7-300/400	Frequency driver for electric motors

- Siemens Sematic S7-300 PLC
- Hunted by Stuxnet

Three Layers of ICS Environment



IT Layer

Networks, Operating systems, IT applications

Propagation

Industrial Control System Layer

Industrial controllers, sub-controllers (frequency converters, pressure controllers etc.)

Manipulation

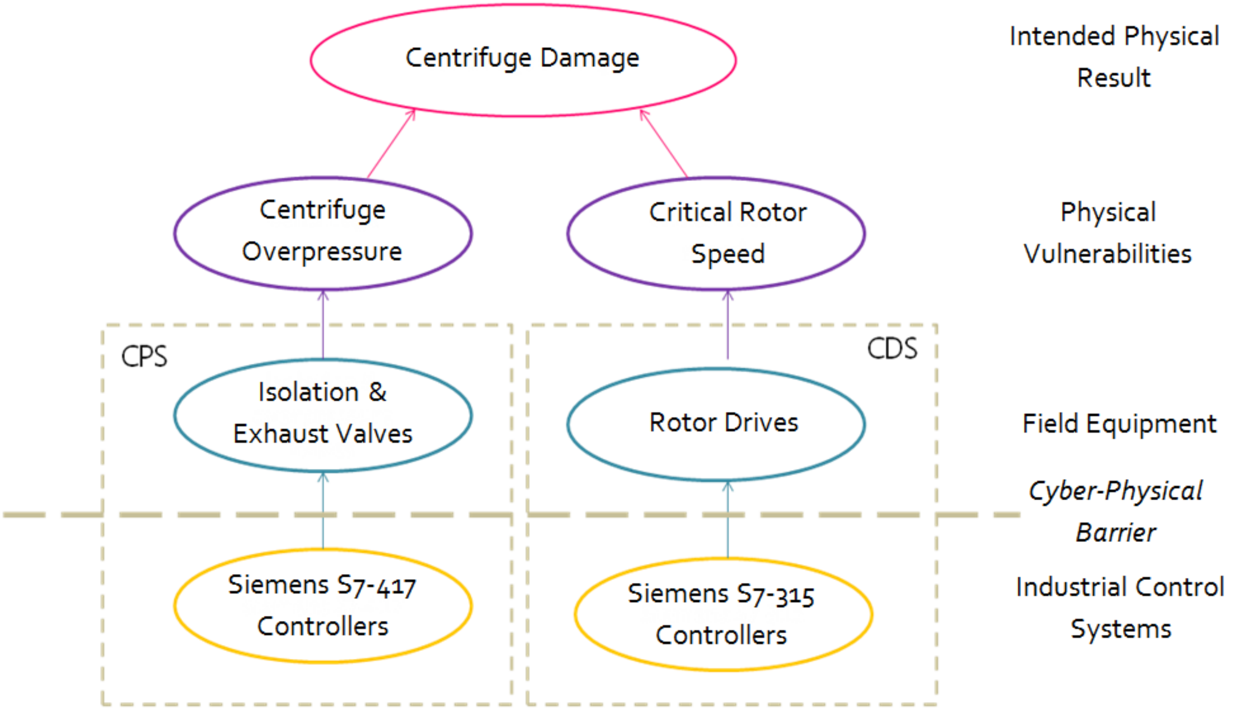
Physical Layer

Valves, electrical drives etc.

Damage by exploiting physical vulnerabilities

- Siemens Sematic S7-300 PLC
- Hunted by Stuxnet

Three Layers of ICS Environment



- Two different attack scenario in Stuxnet. Both use manipulation of ICS system to achieve physical damage exploiting different vulnerabilities of the centrifuge.

Nuclear Centrifuge Technology

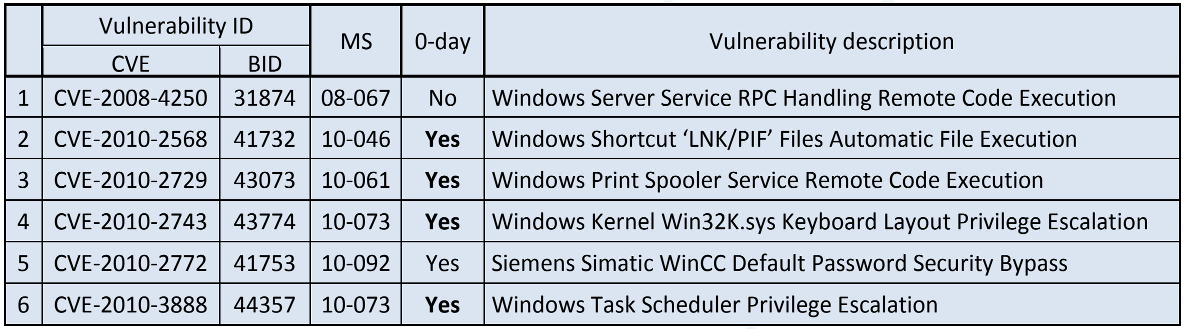
- Uranium-235 separation efficiency is critically dependent of centrifuge speed o rotation
- Higher the speed, the better separation efficiency
- However, higher speeds require strong tubes as the centrifuge starts “shaking’ at higher frequencies
- Shaking can cause catastrophic failure

Stuxnet Timeline

- 2009 Jun: Earliest Stuxnet seen, does not have signed drivers
- 2010 Jan: Stuxnet driver signed, with a valid certificate belonging to Realtek Semiconductors
- 2010 Jun: Virusblokada reports W32.Stuxnet, Verisign revokes Realtek certificate
- 2010 Jul: Anti-virus vendors Eset identifies new Stuxnet driver with valida certificate from JMicron Technology Corp
- 2010 Jul: Siemens reports they are investigating their SCADA system, JMicron certificate revoked by Verisign

Stuxnet Tech Overview

- Components used:
  - Zero day exploits
  - Windows rootkits
  - PLC rootkits (first ever)
  - Anti-virus evasion
  - Peer to peer updates
  - Signed drivers with a valid certificate



	Vulnerability ID		MS	0-day	Vulnerability description
	CVE	BID			
1	CVE-2008-4250	31874	08-067	No	Windows Server Service RPC Handling Remote Code Execution
2	CVE-2010-2568	41732	10-046	**Yes**	Windows Shortcut 'LNK/PIF' Files Automatic File Execution
3	CVE-2010-2729	43073	10-061	**Yes**	Windows Print Spooler Service Remote Code Execution
4	CVE-2010-2743	43774	10-073	**Yes**	Windows Kernel Win32K.sys Keyboard Layout Privilege Escalation
5	CVE-2010-2772	41753	10-092	Yes	Siemens Simatic WinCC Default Password Security Bypass
6	CVE-2010-3888	44357	10-073	**Yes**	Windows Task Scheduler Privilege Escalation

- Command and control interface
- Stuxnet consists of a large .dll fle
  - Designed to sabotage industrial process control system by Siemens SIMATIC WinCC and PCS 7 systems

Stuxnet Potential Attack Scenario

- Reconnaissance:
  - Each PLC is configured in a unique manner
  - Target ICS schematics are required
  - Design docs may have been stolen
  - Retrieved by an early version of Stuxnet
  - Developed with a goal of sabotaging a specific ICS
- Development
  - Mirrored development environment is required
  - ICS hardware
  - PLC modules
  - PLC development software
  - Estimates: 6+ man years of efforts by a experienced, skilled and well funded team

Stuxnet Potential Attack Scenario

- The malicious binaries need to be signed to avoid suspicion
  - Two digital certificates were compromised
  - High probability that the digital certificates/keys were stolen from the company premises
  - Realtek and JMicron are in close proximity
- Initial infection
  - Stuxnet needed to be introduced to the target environment
    - Insider
    - Third party or contractor
  - Delivery method
    - USB drive
    - Windows maintenance laptop
    - Target email attack
    - STEP 7 folders

Stuxnet Potential Attack Scenario

- Infection spread
  - Look for Windows computer that program the PLCs
    - The field PG are typically not networked
    - Spread the infection on computers on the local LAN
      - Zero day vulnerability
      - Two year old vulnerability
      - Spread to all available USBs
  - When a USB connects to a field PG, infection jumps to field PG
    - The “airgap” is breached

Stuxnet Potential Attack Scenario

- Target Infection
  - Look for particular PLC – running Step 7 operating system
  - Change PLC code
    - Sabotage system
    - Hide modifications
  - Command and Control not possible
    - due to “airgap”
    - functionality already embedded

Stuxnet Architecture: Resources

- 201 MrxNet.sys Load driver signed by Realtek/JMicron
- 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 of DLL
- 209 Data file (%windows%/help/winmics.fts)
- 210 Template PE file used for injection
- 221 Exploits MS08-067 to spread via SMB
- 222 Exploit MS10-061 print spooler vulnerability
- 231 Internet connection check
- 240 LNK template file built to exploit LNL exploit
- 241 USB loader DLL ~WTR4141.tmp
- 242 Mrxnet.sys rootkit driver
- 250 Exploit undisclosed Win32k.sys vulnerability

Bypassing Intrusion Detection

- Stuxnet calls load library
  - 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 toa location specified by W32.Stuxnet
  - Where a .dll file was stored by Stuxnet earlier

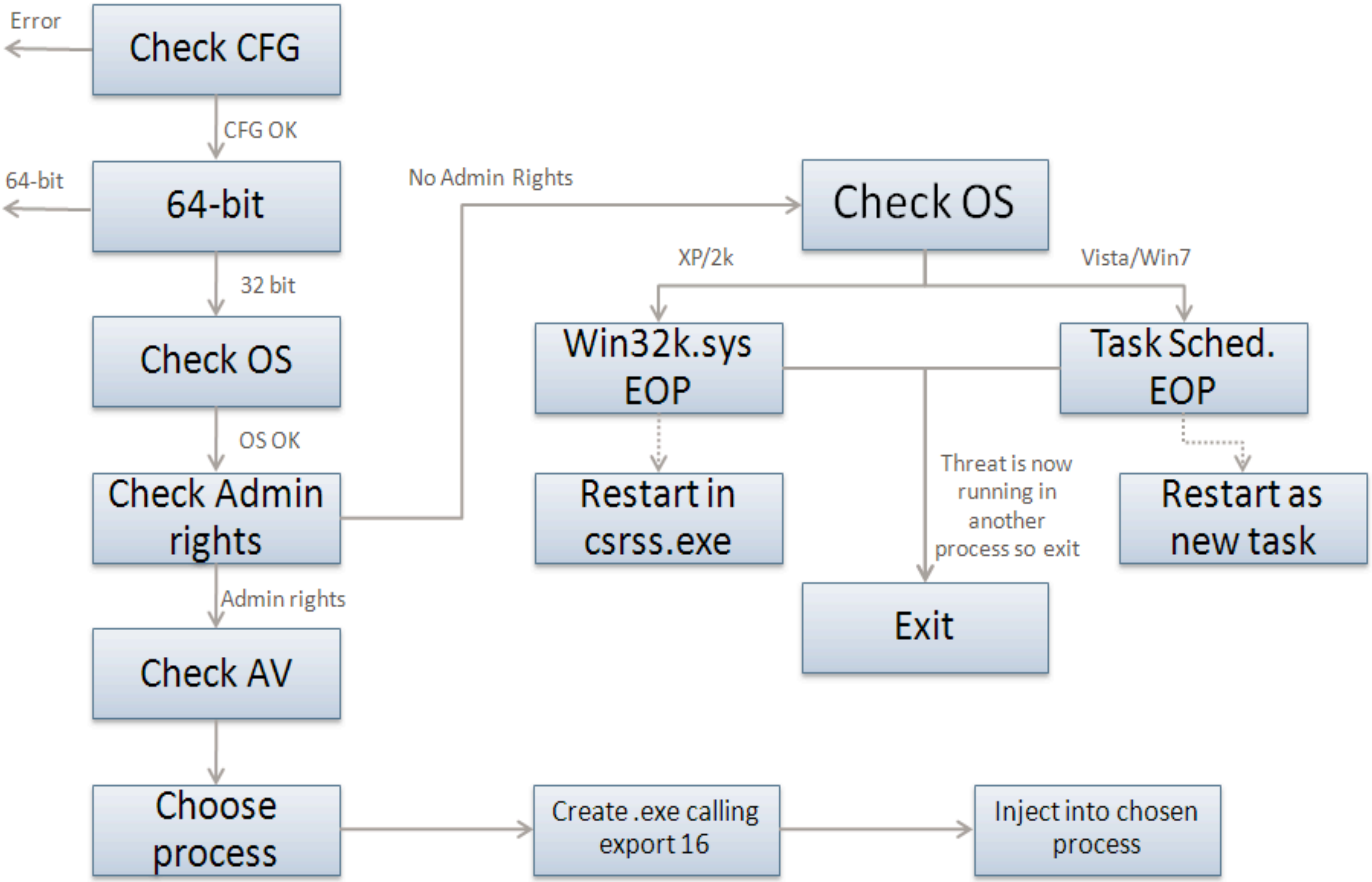
Code Injection

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

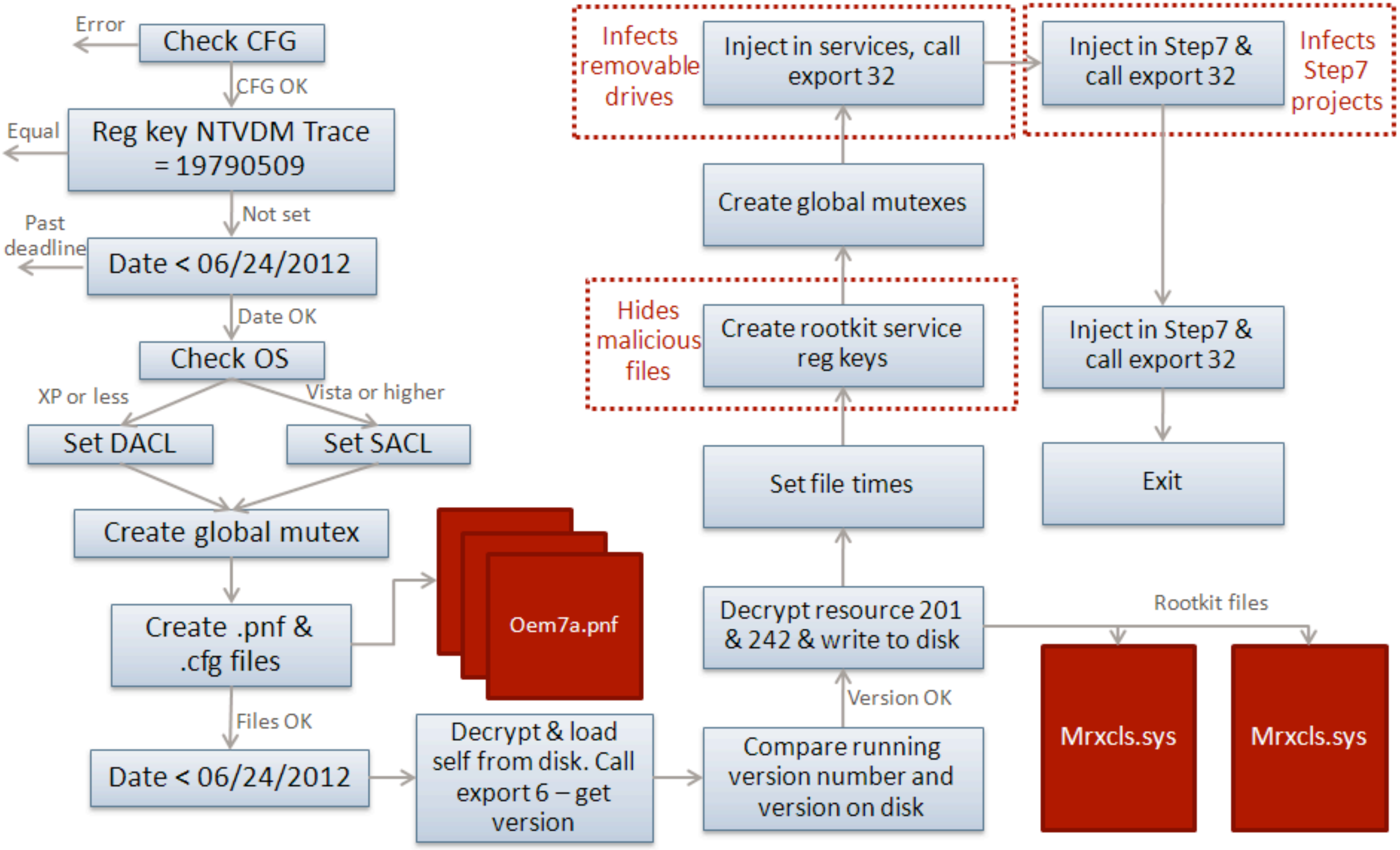
Configuration

- Stuxnet collects and stores following infirmation
  - Major OS version and Minor OS version
  - Flags used by Stuxnet
  - Flag specifying if computer is part of Workgroup or Domain
  - Time of infection
  - IP address of compromised computer
  - File name of infected project file

Installation: Control Flow

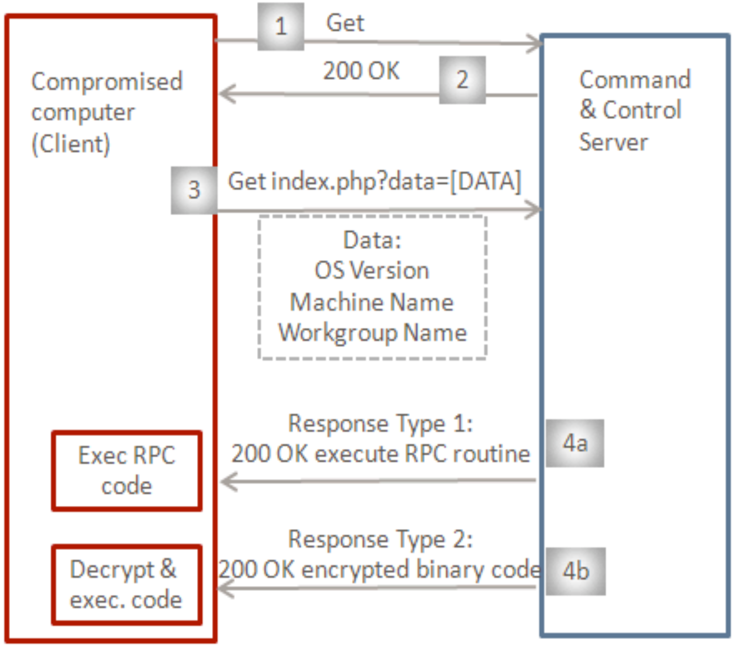


Installation: Infection Routine Flow



Command and 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 above URLs previously pointed to servers in Malaysia & Denmark
  - Send info about compromised computer



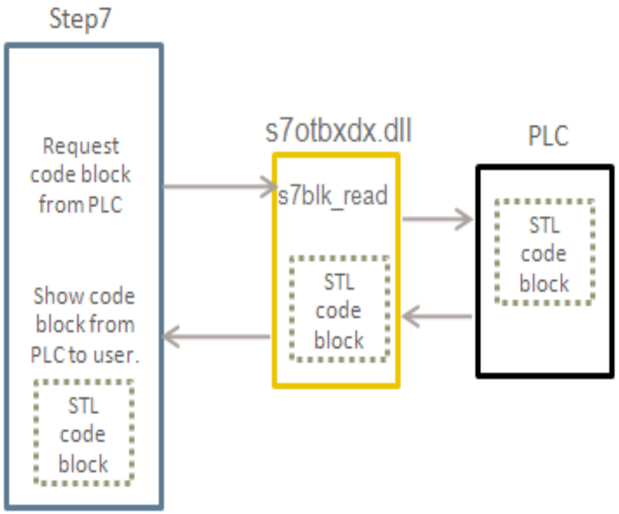
1 & 2: Check internet connectivity
3: Send system information to C&C
4a: C&C response to execute RPC routine
4b: C&C response to execute encrypted binary code

Command and 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 above URLs previously pointed to servers in Malaysia & Denmark
  - Send info about compromised computer

Modifying PLCs

- 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
- Compiled code is in Assembly called MC7
  - These blocks are run by the PLC, to execute, control and monitor an industrial process
- The original s7otbxdx.dll is responsible to handling PLC block exchange between the programming devices and the PLC
  - BY replacing this .dll with its own, Stuxnet is able to perform following actions:
    - Monitor PLC blocks being written to and read from PLC
    - Infect a PLC by inserting its own blocks



Demo

- The Stuxnet Story

  https://youtu.be/Joc0iTX9dyQ

- The Stuxnet Technical Analysis

  https://www.youtube.com/watch?v=qZcvsnkQOvI&t=2s

- Stuxnet – TED talk

  https://www.youtube.com/watch?v=CS01Hmjv1pQ

- Stuxnet – 60 Minutes

  https://www.youtube.com/watch?v=zEjUlbmD9kQ&t=17s

Thank You