BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

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

Agenda

innovate achieve lead

- Case Study: Stuxnet Worm
  - Industrial Control System Overview
  - Stuxnet – General Details
  - What is Stuxnet
  - Stuxnet Penetration
  - How does Stuxnet Work?
  - Siemens Step 7 Software and PLC Interface
  - Stuxnet Exploited Vulnerabilities
  - Stuxnet Attack Scenarios
  - Stuxnet Resources & Configuration
  - Stuxnet Control Flow

Industrial Control Systems (ICS)

Industrial Control Systems (ICS)

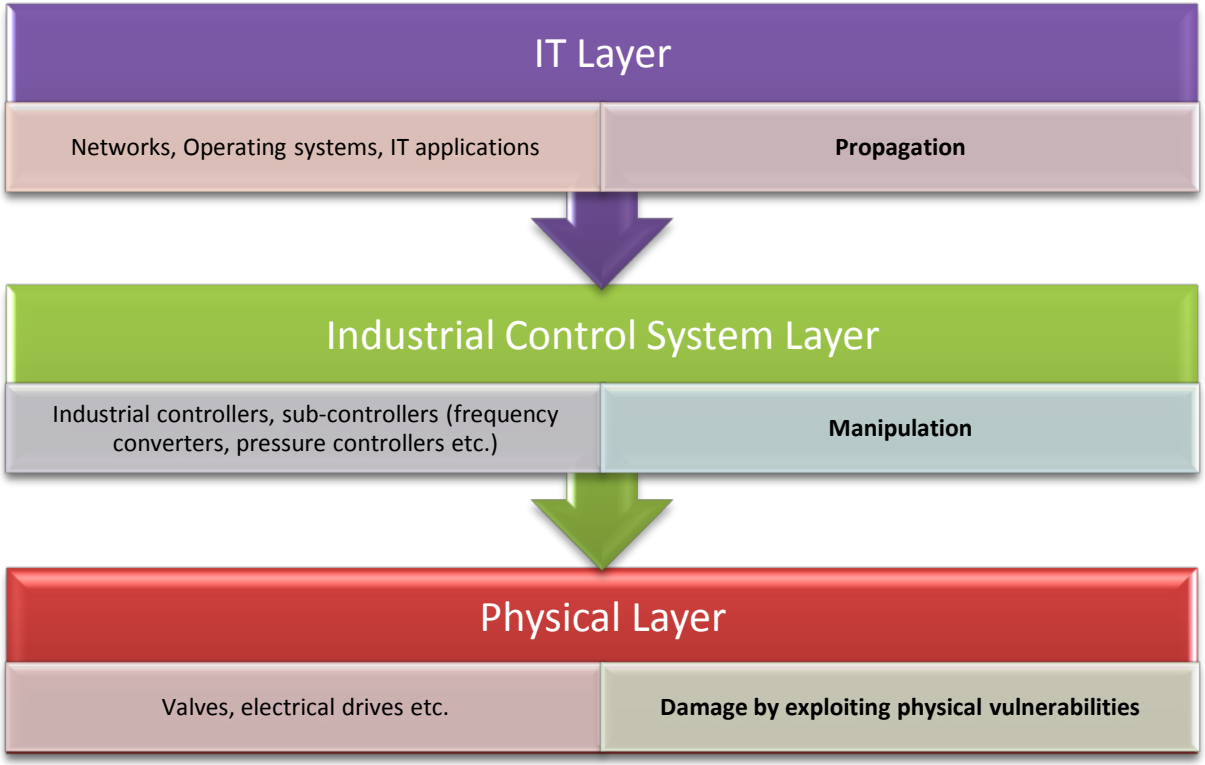
- ICS are operated by special Assembly like code on Programmable Logic Controllers (PLCs).
- PLCs are programmed typically using Windows computers.
- ICS usually consider availability and ease of maintenance first and security last.
- ICS are normally not connected to internet.
- ICS considers the “airgap”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

ICS Environment

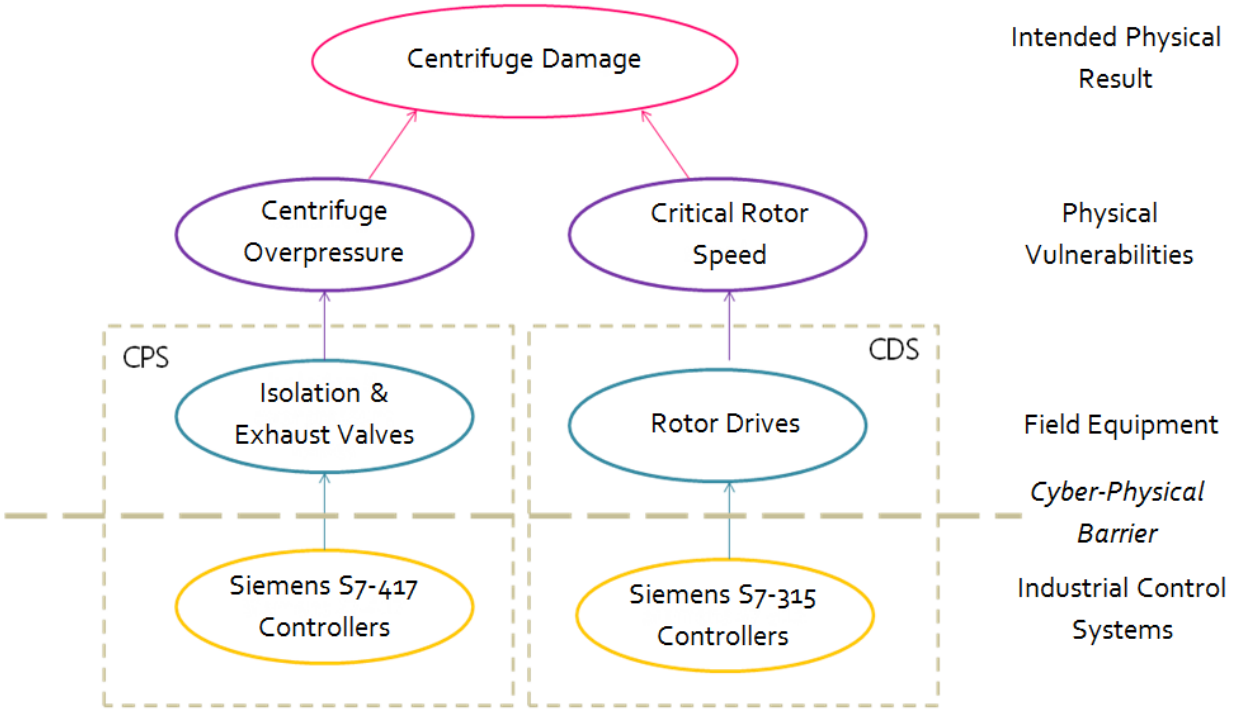
Denomination:	**PG/HMI** (Programming Gateway / Human-Machine Interface)	**PLC** (Programmable Logic Controller)	**Field Device**
Function:	Uploads executable instructions into the PLC (i.e. via a serial or Profibus interface), controls and monitors PLC operations	Manages the connected device and reports 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
- Used by Iranian nuclear program

Three Layers of ICS Environment



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.

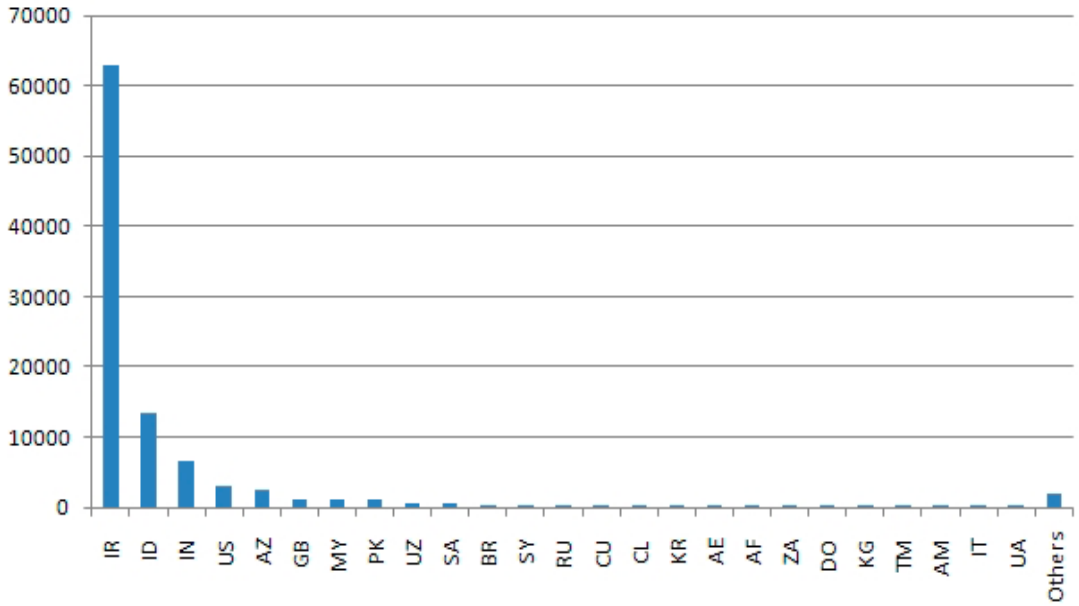
Nuclear Centrifuge Technology

- Uranium-235 separation efficiency is critically dependent of centrifuge speed of 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

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)



Stuxnet Timeline

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

What is Stuxnet?

- Stuxnet is a computer malware specifically designed for Industrail Control Systems made by Siemens
- These systems were used by Iran to enrich Uranium which can be used for nuclear bomb
- The aim of the worm is to damage or destroy the controlled equipment
- A worm can infect a computer system and then automatically spread to other systems without any user intervention

Stuxnet Worm

- Stuxnet worm was designed to affect SCADA systems and PLC controllers of the uranium enrichment centrifuges
- Very specific targeting – Stuxnet would affect only one specific type of Siemens controllers used by Iranian centrifuges
- It could spread to other Industrial Control Systems but will not damage them
- Takes over operation of centrifuges from SCADA controllers
- Sends control signals to PLC managing the equipment
- Causes the spin speed of centrifuge to vary wildly and very quickly causing extreme vibrations and as a consequence damage to equipment
- Block signals and alarms from PLC to control centre

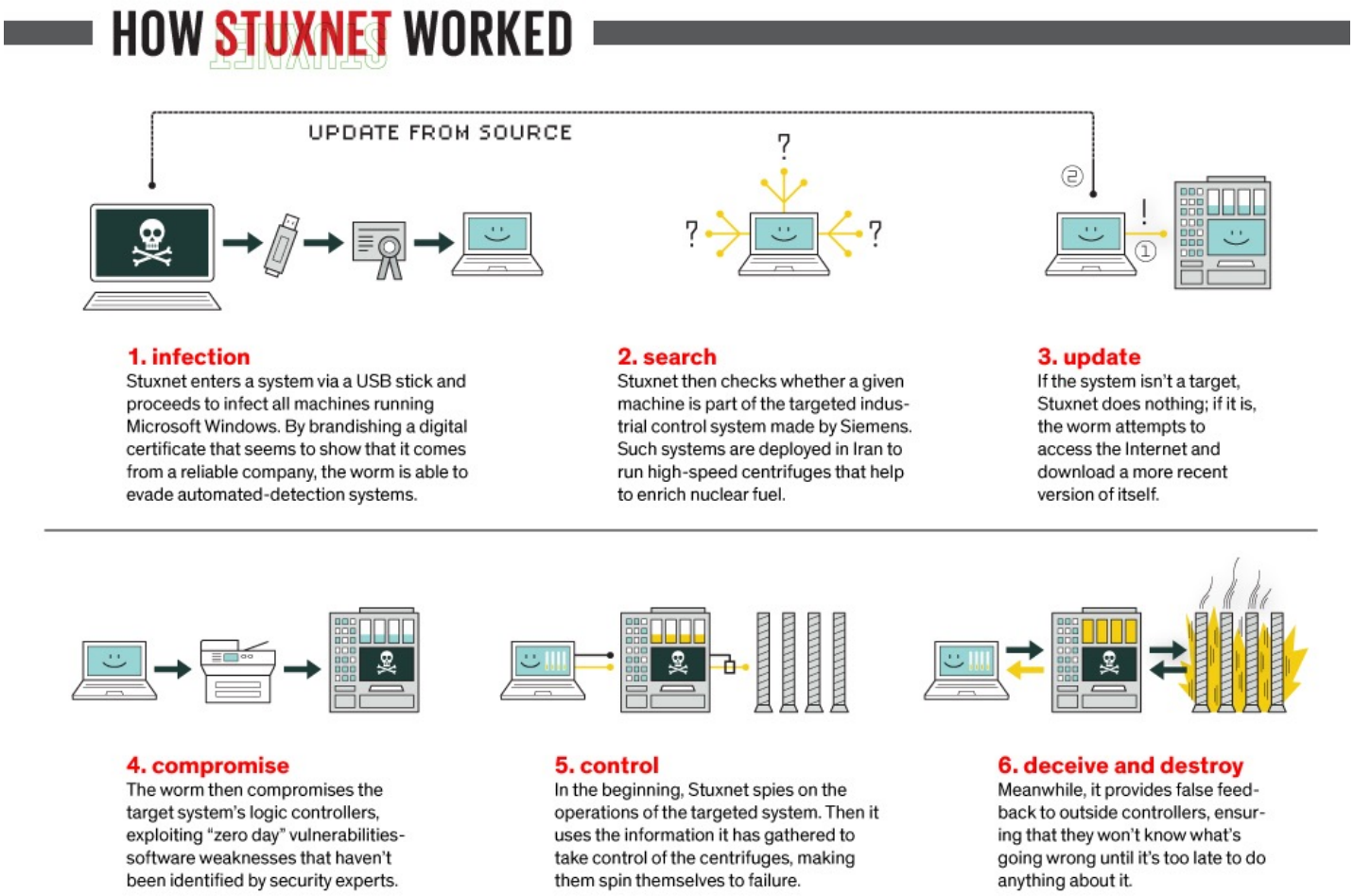
Stuxnet Penetration

- Targets Windows systems used to configure the SCADA system
- Uses 6 different vulnerabilities to affect the system
  - 5 of these were previously unknown (zero day)
  - So if it encountered some systems where some of vulnerabilities had been fixed, it still had potential to infect them
  - Spread can not be stopped by fixing one vulnerability
- Spreads to Siemens Win CC/PCS 7 SCADA control software and takes over configuration of the system
- Uses a vulnerability in the print system to spread from one system to another
- Uses peer-to-peer transfer – no need for systems to be connected over internet

Myth of "Airgap"

- Centrifuges control systems were not connected to Internet
- Initial infection is suspected to be through USB drives taken into plant by unwitting operators (may be supplied as freebies!)
- It is thought that 900 of the 1000 centrifuges were destroyed by Stuxnet
- This caused significant slowdown in nuclear enrichment programme due to:
  - Centrifuge damage
  - Enrichment shutdown while the worms were cleared from the equipment
- Because of the sophistication of Stuxnet, it is suspected to be a cyber warfare by nation state actors against Iran
- Other countries with Stuxnet infection were India, Indonesia and Azerbaizhain

How does Stuxnet Work?



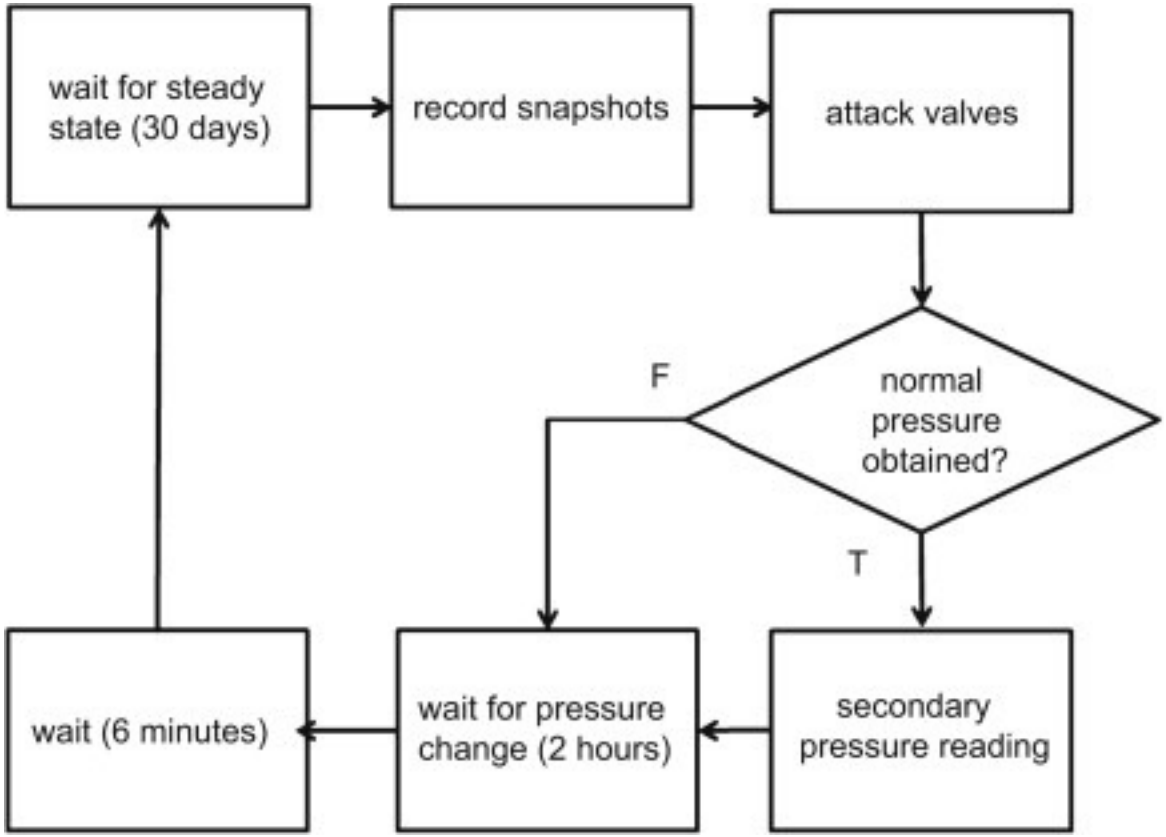
How does Stuxnet Work?

- The most commonly cited mechanism Stuxnet uses to gain access to the computer network is though an infected USB drive, and automatically load itself to computers with open file sharing.
- From there, it used the default password of the Siemens Step 7 to gain access to the database and load itself onto the computer.
- To propagate to other computers on the network, it was able to infect PLC datafiles and copy itself to the datafile.
- It also has a peer-to-peer update mechanism to update all instances once one of them gains control at the system level.
- The last step of gaining access is to check that the PLC is controlling at least 155 total frequency converters, a little under the known amount of Iranian centrifuge control.
- This verifies that Stuxnet is specifically targeting the Iranian centrifuges only.
- Once it loads malicious code to the PLC, it also verifies that the motors are 800Hz-1200Hz as an additional check that it is indeed on the correct centrifuge controller.

How does Stuxnet Work?

- At this point, Stuxnet is ready to execute the attack.
- It increases the centrifuge frequency to 1410Hz for 15 minutes, then sleeps to avoid detection.
- After 27 days, it slows the frequency to 2Hz and sleeps again.
- The process is repeated, speeding up and slowing down the centrifuge.
- To avoid detection, it would send the correct frequency of 800-1200 Hz back to the database, and in the case of a failsafe, it would run the centrifuges at normal frequency.
- Stuxnet used stolen RealTek certificates to avoid detection from antivirus software.
- Stuxnet used five different zero-day vulnerabilities in two different operating systems, in a highly complex and targeted cyber attack that was completely unprecedented in scope and ultimately effective in its attack and stealth.

How does Stuxnet Work?



Stuxnet Vulnerability Components

- As per Symantec and Kaspersky Stuxnet is a very sophisticated attack, they ever analysed
- Designed to sabotage industrial process control system by Siemens SIMATIC WinCC and PCS 7 systems
- Command & Control interface
- Creation of state level sponsors
- Components used:
  - 5 Zero day exploits
  - Windows rootkits
  - First ever PLC rootkits
  - 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

Stuxnet CVE Vulnerabilities Exploited

CVE Number	Details
CVE-2008-4250	The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, aka "Server Service Vulnerability."
CVE-2010-2568 (Zero day)	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.
CVE-2010-2729 (Zero day)	The Print Spooler service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, when printer sharing is enabled, does not properly validate spooler access permissions, which allows remote attackers to create files in a system directory, and consequently execute arbitrary code, by sending a crafted print request over RPC, aka "Print Spooler Service Impersonation Vulnerability."

Stuxnet CVE Vulnerabilities Exploited

CVE Number	Details
CVE-2010-2743 (Zero day)	The kernel-mode drivers in Microsoft Windows XP SP3 do not properly perform indexing of a function-pointer table during the loading of keyboard layouts from disk, which allows local users to gain privileges via a crafted application, as demonstrated in the wild in July 2010 by the Stuxnet worm, aka "Win32k Keyboard Layout Vulnerability".
CVE-2010-2772 (Zero day)	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.
CVE-2010-3888 (Zero day)	Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm and identified by Kaspersky Lab researchers and other researchers.

Stuxnet Method of Penetration

- **Via the local network**
  - Using the zero-day Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (CVE-2010-2729 / BID 43073)5
  - Two-year old Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (CVE-2008-4250/ BID 31874)6.
  - The Print Spooler vulnerability consists of the acceptance of a specially crafted print request sent to a networked printer, containing arbitrary executable code which is run by the computer sharing the printer (the host computer is forced to write a dropper named winsta.exe in the %SystemRoot%\system32 directory, and a file named sysnullevent.mof in the %SystemRoot%\system32\wbem\mof directory, which is then automatically executed as a WMI binary managed object file).
  - Note also that Stuxnet will attempt to use this vulnerability only if the current date is before June 1, 2011.
  - By copying itself in accessible shared folders (using the security credential tokens of the users found in the local computer / domain or through a WMI Explorer impersonation).
  - By copying and executing itself on remote computers running a WinCC database server.

Stuxnet Method of Penetration

- **Via USB removable storage devices (mainly USB memory sticks)**
  - If Stuxnet detects that a USB storage device is connected to the system on which it resides, then it copies itself and generates on the USB device a specially crafted .LNK file, and waits for users of other systems to display its content.
  - By doing so, they also get infected because of the (0-day) Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (CVE-2010-2568 / BID 41732)7 that Stuxnet is capable of exploiting.
  - In earlier versions of Stuxnet, the worm was spreading via USB removable media through the usage of autorun.inf.
- **Via infection of STEP 7 folders**
  - Stuxnet searches for STEP 7 projects (.S7P files) in the infected system.
  - If it finds any of these, it modifies the main index files and copies itself in their folders.
  - STEP 7 folders are often copied from one computer to another for documentation or development purposes.
  - When a user opens such an infected folder on a clean system, the worm is executed and spreads the infection.

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

Stuxnet Operation Method

- Once inside a new system, depending on the Windows version found, the worm uses the 0-day vulnerability Windows Task Scheduler Privilege Escalation Vulnerability (CVE-2010-3888)8 or Windows Win32K Keyboard Layout Vulnerability (CVE-2010-2743)9 to gain elevated privileges and install a rootkit.
- In order to be undetectable by anti-virus software and to have very privileged access to the host system, the rootkit functionality is installed as two hardware driver-level executable modules (device drivers mrxnet.sys and mrxcls.sys), which run in kernel mode.
- As this is a "suspicious" operation, to do this Stuxnet uses counterfeit identification certificates to prove their origin from a trusted source to Windows.
- In order to be executed on every system start, the worm then sets the Windows registry entries HKLM\System\CurrentControlSet\Services\MRXCLS and HKLM\System\ CurrentControlSet\Services\MRXNET so that the two drivers are started as services.

Stuxnet Operation Method

- Stuxnet then starts its Remote Procedure Call (RPC) server and listens for incoming connections from other infected machines possibly residing on the local network.
- This feature enables an infected system to execute the following functions within any other infected machine to which it it can connect:
  - get the malware version
  - send a module and have it executed remotely in a new or in an existing (e.g. lsass.exe) process
  - download the worm dropper (built on-demand right at the time of the request)
  - run any specified application
  - read a file
  - write a file
  - delete a file

Stuxnet Operation Method

- The RPC server installed by Stuxnet in the infected systems is identified as a unique software object through the Globally Unique IDentifier (GUID) 000204e1-0000-0000-c000-000000000046.
- Using this GUID, those systems are enabled to identify, communicate with, and update one another.
- This feature allows all malware instances to automatically update each other over the LAN, even if they cannot reach to the command-and-control (C&C) server due to a firewall or lack of Internet connectivity.

Stuxnet Operation Method

- Finally, it searches on the local computer for the Siemens WinCC software, which would indicate that the machine is a computer used for controlling an industrial PLC, also known as a "Human-Machine Interface" workstation.
- To determine if WinCC is installed, Stuxnet looks in the Windows system folder for the file S7OTBXDX.DLL, used by WinCC systems.
- Once found, it renames the file to S7OTBXSX.DLL and then replaces it with a modified version (extracted from the main wrapper file as resource 208).
- The new .DLL has the same exports as the original but with code modifications on the following functions:
  - s7db_open
  - s7blk_write
  - s7blk_findfirst
  - s7blk_findnext
  - s7blk_read
  - s7_event
  - s7ag_test
  - s7ag_read_szl
  - s7blk_delete
  - s7ag_link_in
  - s7db_close
  - s7ag_bub_cycl_read_create
  - s7ag_bub_read_var
  - s7ag_bub_write_var
  - s7ag_bub_read_var_seg
  - s7ag_bub_write_var_seg

Stuxnet Operation Method

- These functions are generally used to access, read, write, and delete code blocks on the PLC.
- In an infected system, when these functions are called, Stuxnet will execute additional instructions before calling the true functions contained in S7OTBXSX.DLL.
- By intercepting these functions, it can modify the data sent to or received from the PLC, acting as an MITM-like attack.
- Next, Stuxnet tries to contact a remote server. In attempting to do this, it first tests for an active Internet connection by trying to open an HTTP session to the following non-malicious URLs:
  - www.windowsupdate.com
  - www.msn.com
- After a connection is established, it then connects to the following URL(s) to send and receive commands from a remote user:
  - www.mypremierfutbol.com
  - www.todaysfutbol.com

Stuxnet Operation Method

- It then generates the following URL and posts it to the server:
  - http://www.mypremierfutbol.com/index.php?data={data}
  - Where {data} is a XOR encrypted hexadecimal value that contains the IP address, computer name, domain, OS version of the infected machine and whether WinCC or STEP 7 are installed or not.
  - The server may respond to the infected machine by sending back arbitrary code to be executed (most likely an updated version of the malware).
- As a next move, Stuxnet start a search for STEP 7 projects.
- At this point, all the install and setup operations are done.
- Using the S7OTBXDX.DLL and the WinCC default credentials (userid= WinCCConnect password=2WSXcder) (CVE-2010-2772), Stuxnet accesses the PLCs and verifies what type of CPU they have.
- If CPUs are type 6ES7-315-2 or 6ES7-417, then it checks what type of field devices are connected to them by reading the PLC's system data blocks (SDB).
- If the devices found are Vacon or Fararo Paya frequency drive converters, Stuxnet records the frequency configuration data set in the PLC, and then it begins intercepting commands, altering their operation.

Stuxnet Operation Method

- Stuxnet has the ability to upload its own attack code to the PLCs.
- By doing so, "Stuxnet changes the output frequency [of the converters] for short periods of time to 1410 Hz and then to 2 Hz and then to 1064 Hz.
- Modification of the output frequency essentially sabotages the automation system from operating properly, causing mechanical stress to the centrifuges (which can lead to failure) and corrupting the quality of the processed uranium.
- The attack sequence – intended as the commands given to the frequency converters – is different depending on the CPU type.
- As a last move, to cover its tracks and finish its attack in a truly impeccable way, Stuxnet – after hijacking the sent commands – replays reassuring fake data to the operator (previously recorded), discarding the real ones coming from the PLC's sensors, so that everything on the HMI station looks to be in order.
- This is a PLC rootkit functionality, and so far seems to be the first one of its kind to appear in the wild.

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
  - Team had sufficient resourcing (funding, logistics & influencing) capabilities

Stuxnet Potential Attack Scenario

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

Stuxnet Potential Attack Scenario

- Infection propagation
  - Look for Windows computer that program the PLCs
    - Field Programmable Gateways are typically not connected to a network
    - Spread the infection on computers on the local LAN
      - Zero day vulnerability
      - Two year old vulnerability
      - Spread to all available USBs
  - A malicious USB infects a field Programmable Gateway when connected to the Programmable Gateway
    - USB used to breach the “airgap”

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

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 to a location specified by W32.Stuxnet
  - Where a .dll file was stored by Stuxnet earlier

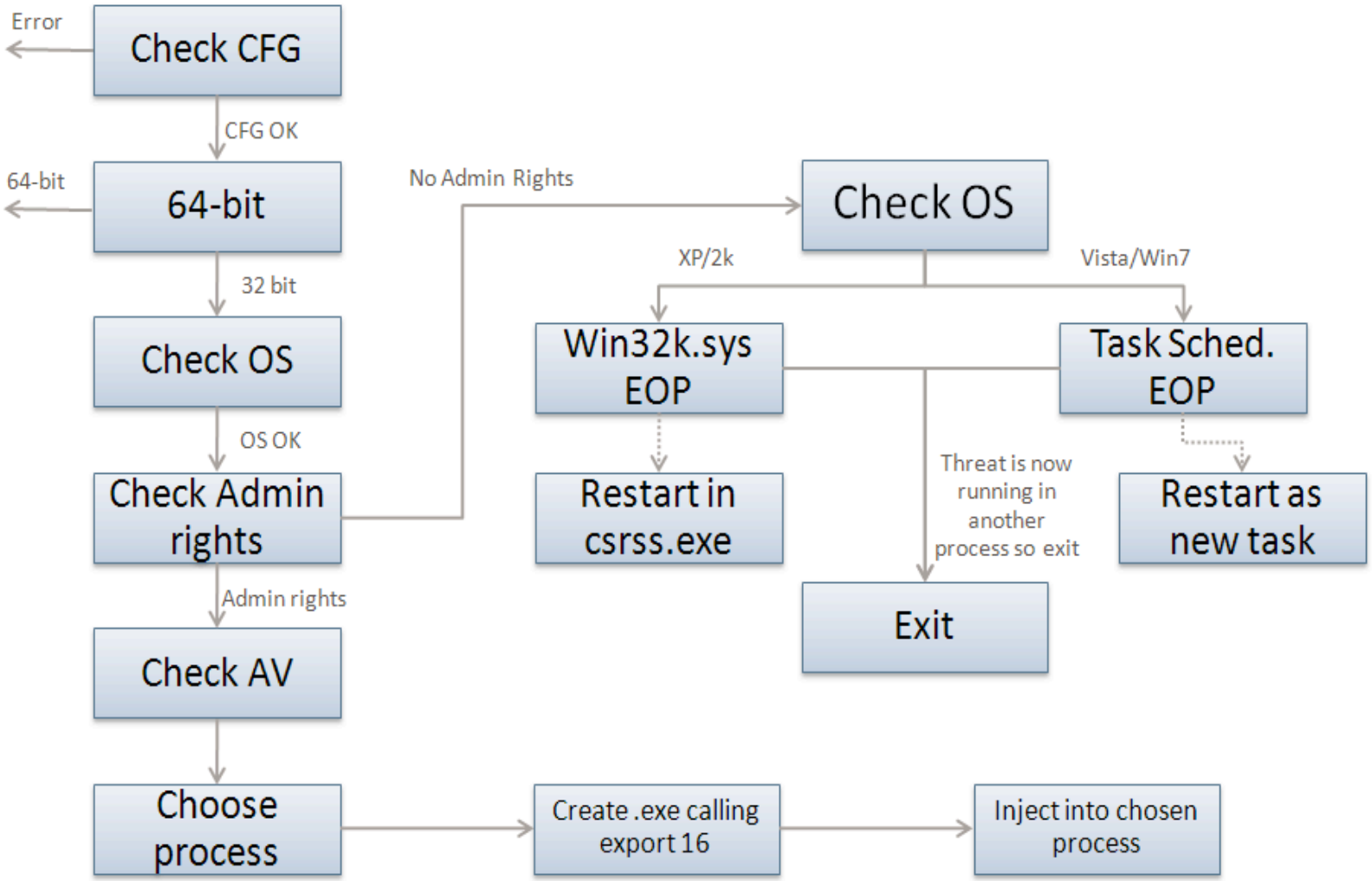
Code Injection

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

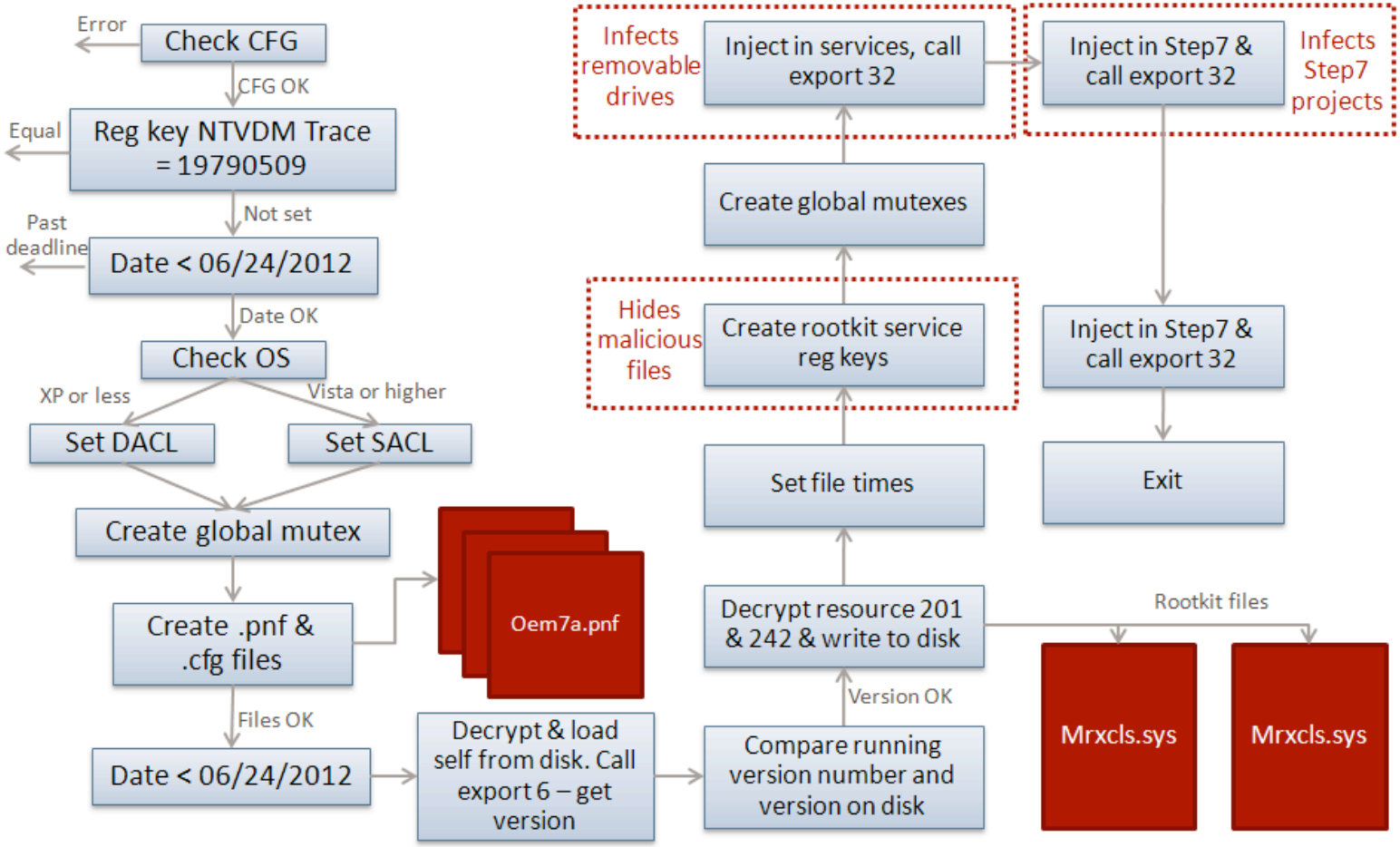
Configuration

- Stuxnet collects and stores following information
  - 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

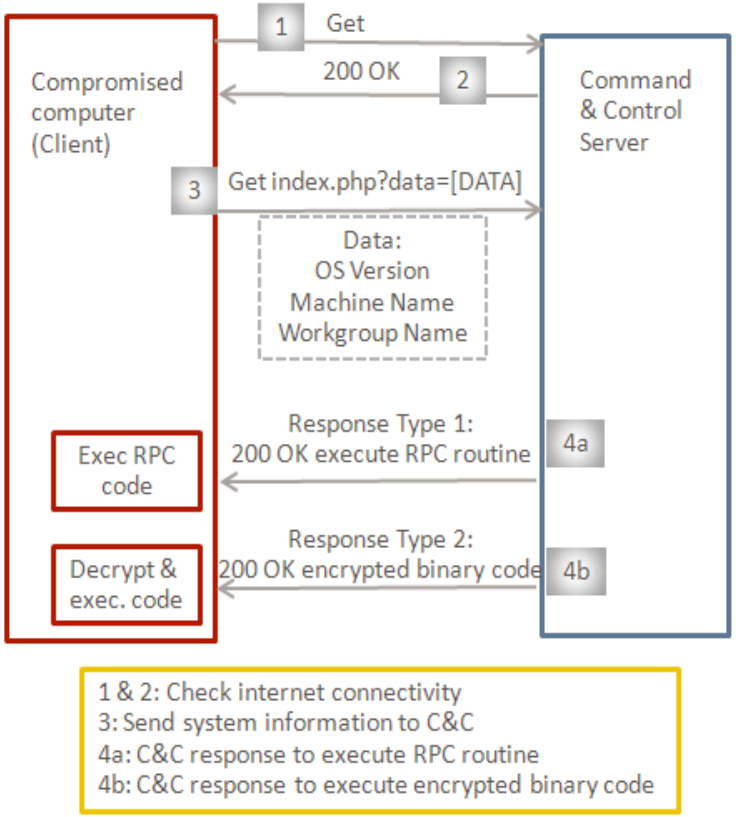


Installation: Infection Routine Flow



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

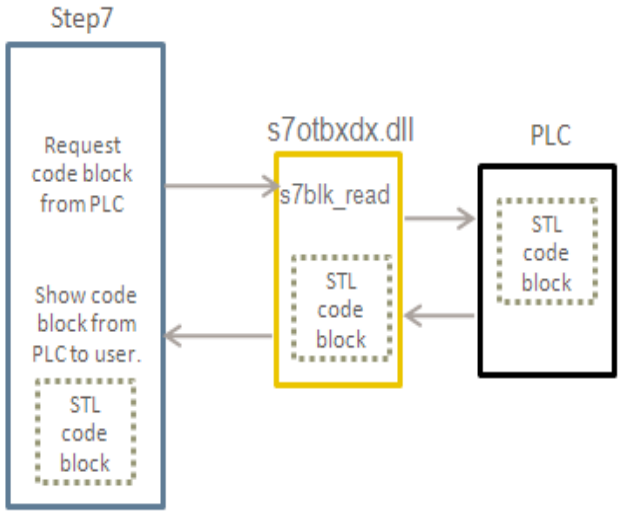


Command and Control

- 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

innovate achieve lead

- 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