Stuxnet

Gian Piero Siroli, Physics Dept., Univ. of Bologna and CERN

What is Stuxnet?

- It is a “worm” designed to sabotage a specific industrial process. It penetrates a particular subsystem of a SCADA industrial control systems of a single producer (Siemens). Once injected, it spreads silently in the Windows/SCADA infrastructure looking for specific Programmable Logic Controllers (PLC) and reprogram them to alter the functionality, showing at the same time normal running conditions to the monitoring system
- Reported in June 2010, first example of a precision military-grade cyberweapon, deployed to seek and damage a real world physical target
- Worm analyzed in public conferences, papers from various authors, probably the best studied piece of malware in history. Executable code available on the network

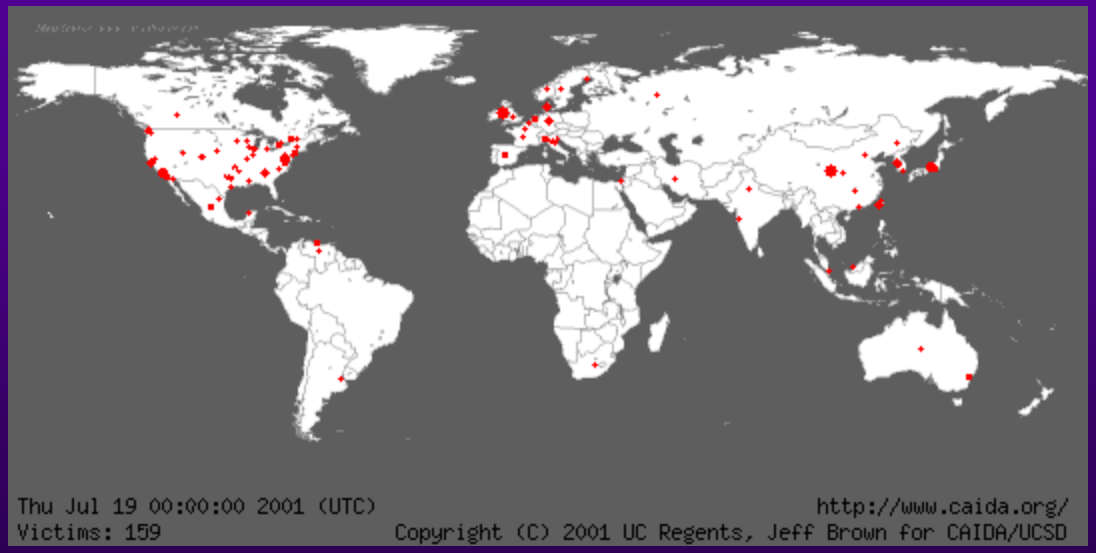
What is Stuxnet?

- **How: Stuxnet intercepts communications with the PLC, determines whether the system is the intended target, modifies the existing PLC code to change the operational parameters. It hides the PLC infection from the operator using rootkit functionality. All these activities take place in two different environments: the Windows environment where the control software (WinCC/STEP7) is running AND at the PLC level, where the malicious code in assembly language (MC7) is injected and executed. Stuxnet determines the target asap and looks for specific configuration before activating**

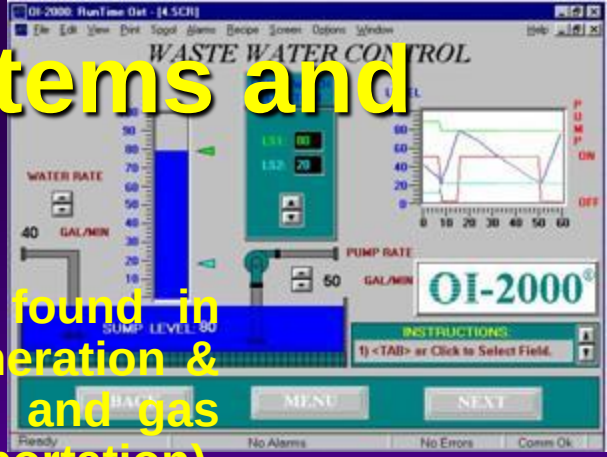
What is a worm

- Self-replicating segment of code able to autonomously spread travelling across networks without any human intervention. Usually containing a “payload” (malware) activating on target systems. A computer virus needs human activity (email, distribution of infected files) and an application to attach to

Code Red worm propagation during 24h following release (2001)

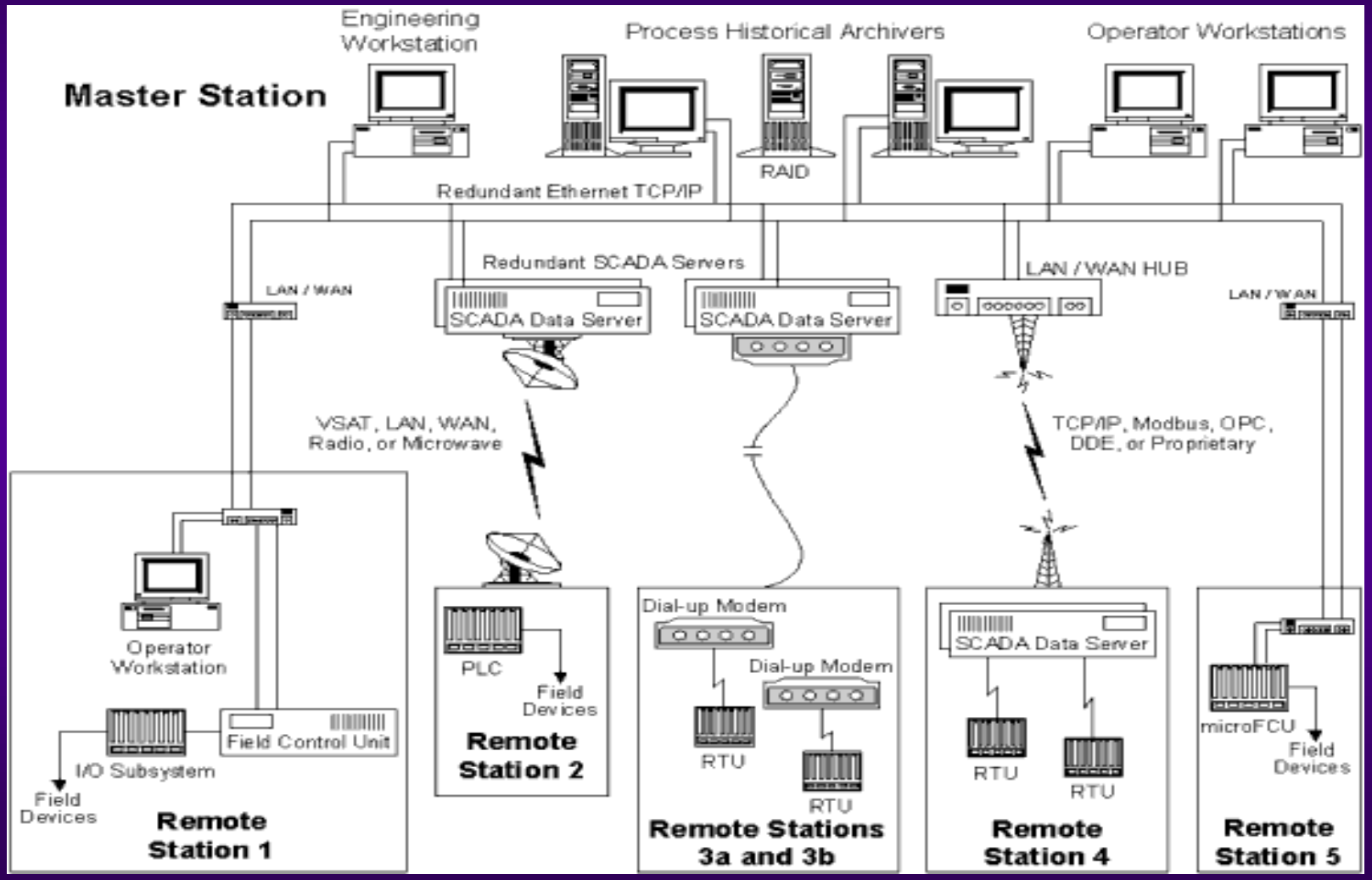


Industrial Control Systems and SCADA



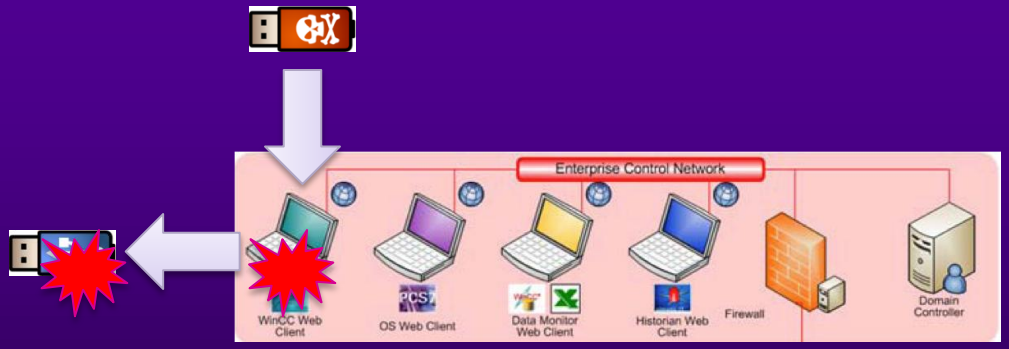
- ICSs assist in the management of equipment found in critical infrastructure facilities (electric power generation & distribution, water and wastewater treatment, oil and gas refineries, chemical and food production, transportation). Acting on real daily life equipment
- SCADA (Supervisory Control and Data Acquisition) systems: highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation
- DCS (Distributed Control Systems): control of production systems within a local area (localized processes). Smaller scale, factory level. Multiple, integrated sub-systems
- PLC (Programmable Logic Controllers): computer-based low level devices that control real world processes and equipment, used throughout SCADA and DCS. Automation of field "sensors" and "actuators" (motor starters, pumps, solenoids, pilot lights/displays/devices, speed drives, valves, motion control). Hard real time system

Many intrusion vectors and open doors



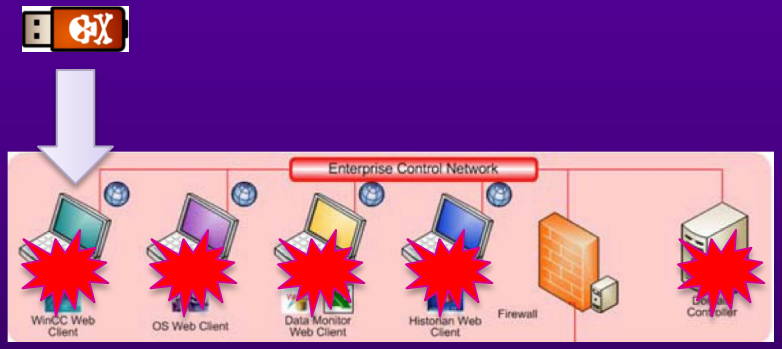
First Infection: Enterprise Computer

- Infected USB drive infiltrated into the plant and inserted into computer (employees laptop infected off-site, infected project files from contractor). Malicious act or through social engineering. “Air-gap” overcome
- Stuxnet successfully installs even though computer is fully patched and current with anti-virus signatures
- Rootkit installed to hide files and activities
- Attempts connection to Command-and-Control server for updates
- Infects any new USB Flash drive inserted into computer



Propagation on Enterprise Network

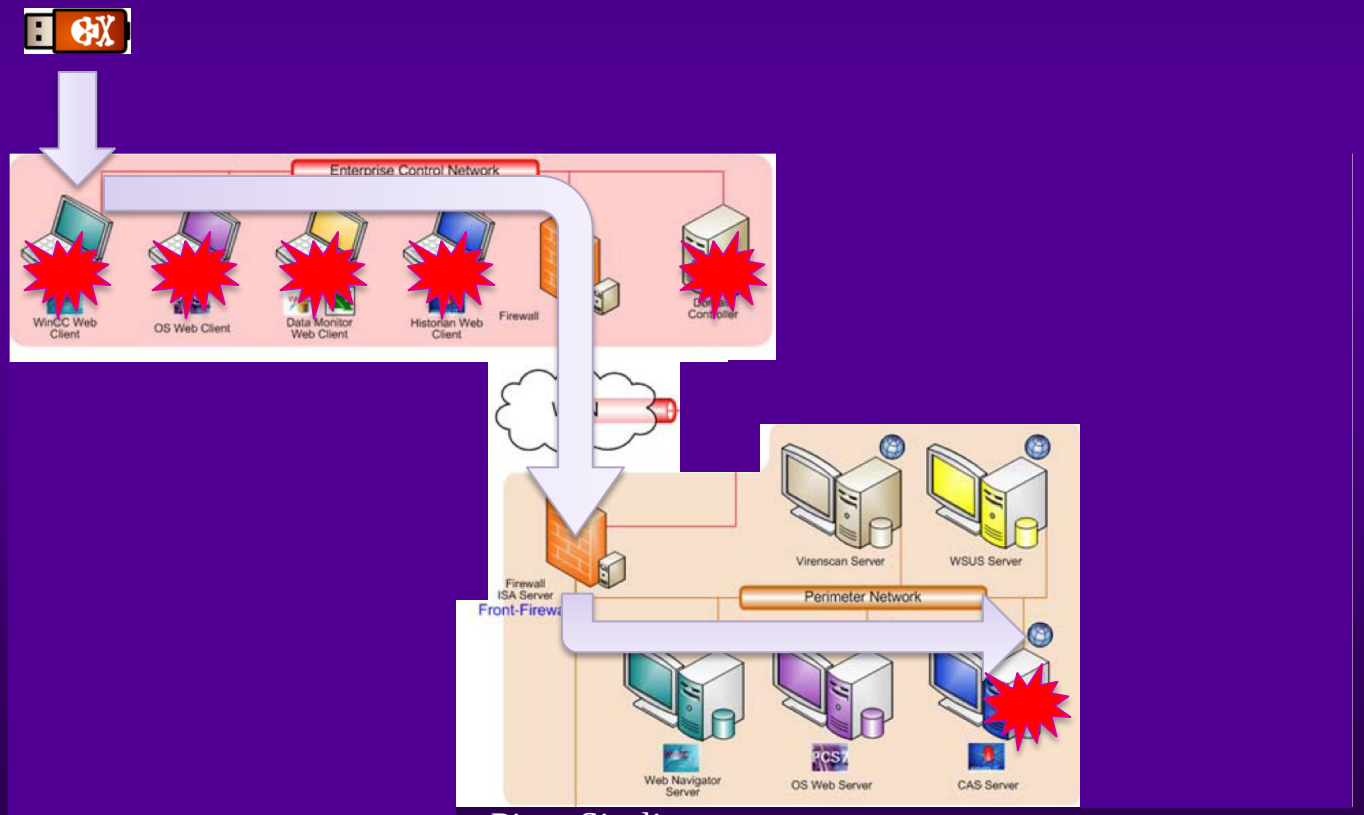
- Rapidly spreads to Print Servers and File Servers within hours of initial infection
- Establishes P2P network and access to C&C server (but the worm is autonomous, no remote control, “Launch and Forget”)
- Infects any new USB Flash drive inserted into any computer



(animation from E.Byres, Tofino Security)

Penetrating Perimeter Network

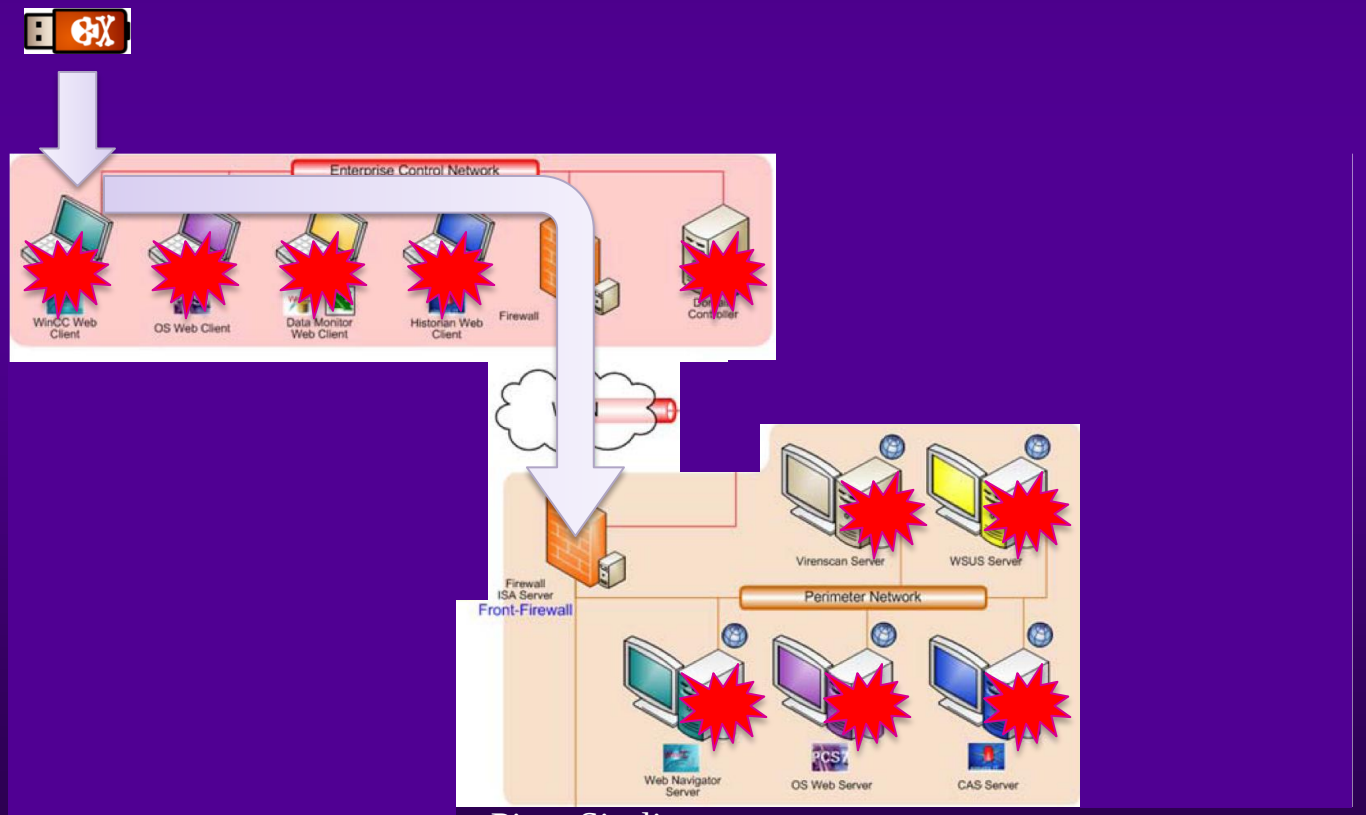
- System Admin (Historian) becomes infected through network printer and file shares
- System Admin connects via VPN to Perimeter Network and infects the CAS Server and its WinCC SQL Server database



(animation from E.Byres, Tofino Security)

Propagation on Perimeter Network

- Infects Web Navigation Server's WinCC SQL Server
- Infects STEP7 Project files
- Infects other Windows hosts on the subnet like WSUS, AVS etc

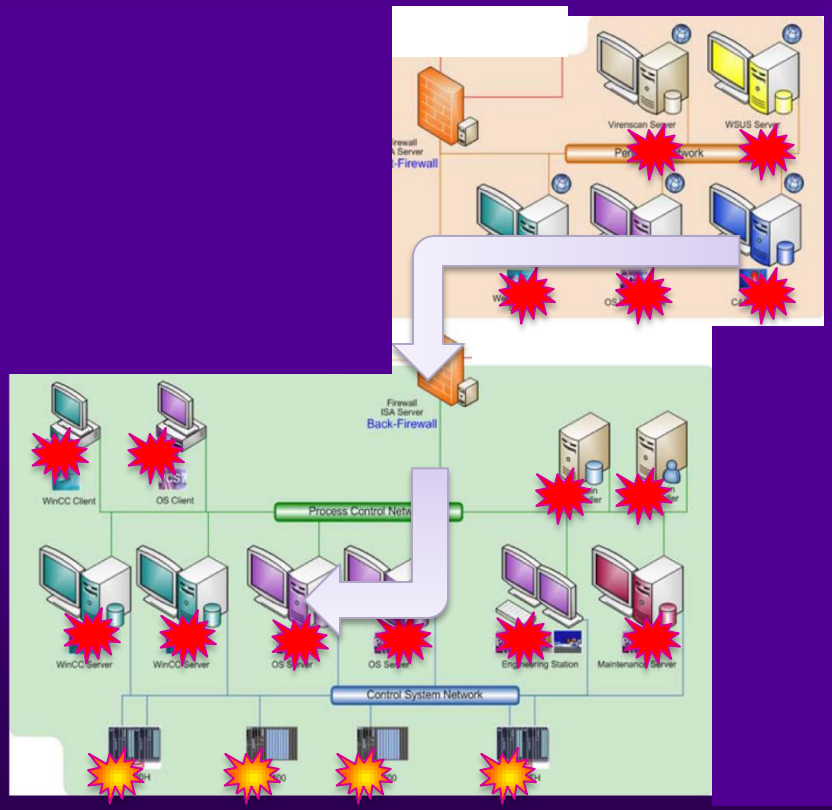


(animation from E.Byres, Tofino Security)

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

- …until it gets at the interface of the PLC level, and propagates further crossing it…

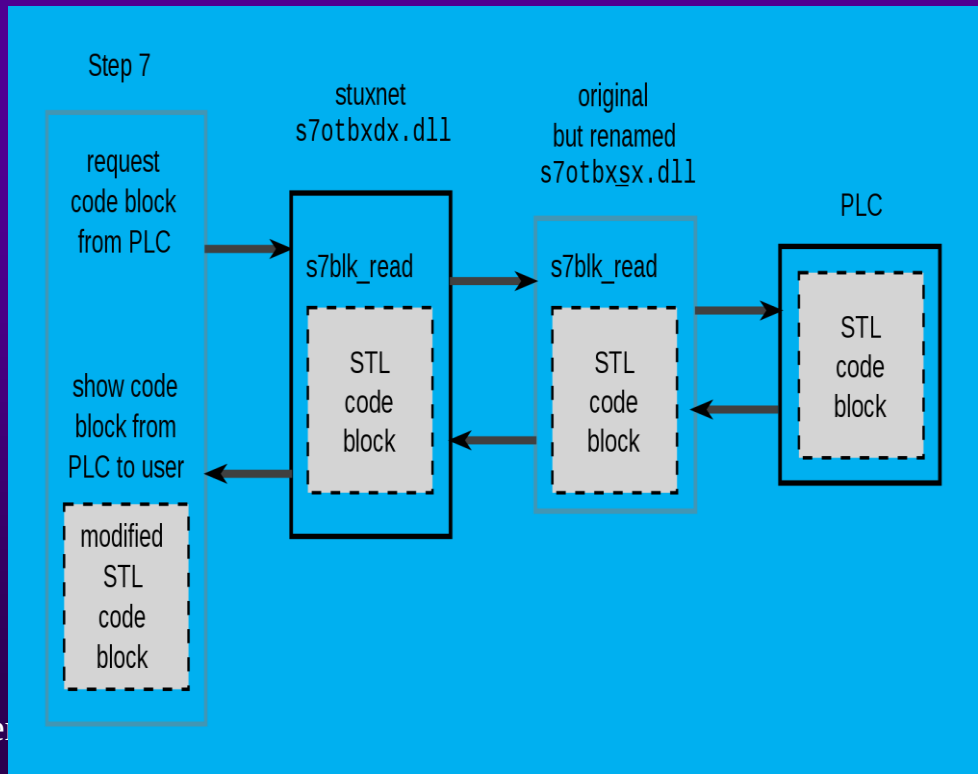


Gian Piero Siroli

(animation from E.Byres, Tofino Security)

Final steps - I

- Stuxnet “fingerprints” the connected PLCs
- If the right PLC is found (only two Siemens CPUs are infected), it replaces the S7 communication libraries (DLLs) used for exchanging data with PLCs adding hidden functionality. Stuxnet is the vector to deliver the attack code (15000 LOC) to the PLCs
- Stuxnet is now controlling the communication between SCADA & PLC (“Man in the Middle”). It intercepts the input values from sensors and give fake (prerecorded) data to legitimate programs



Final steps - II

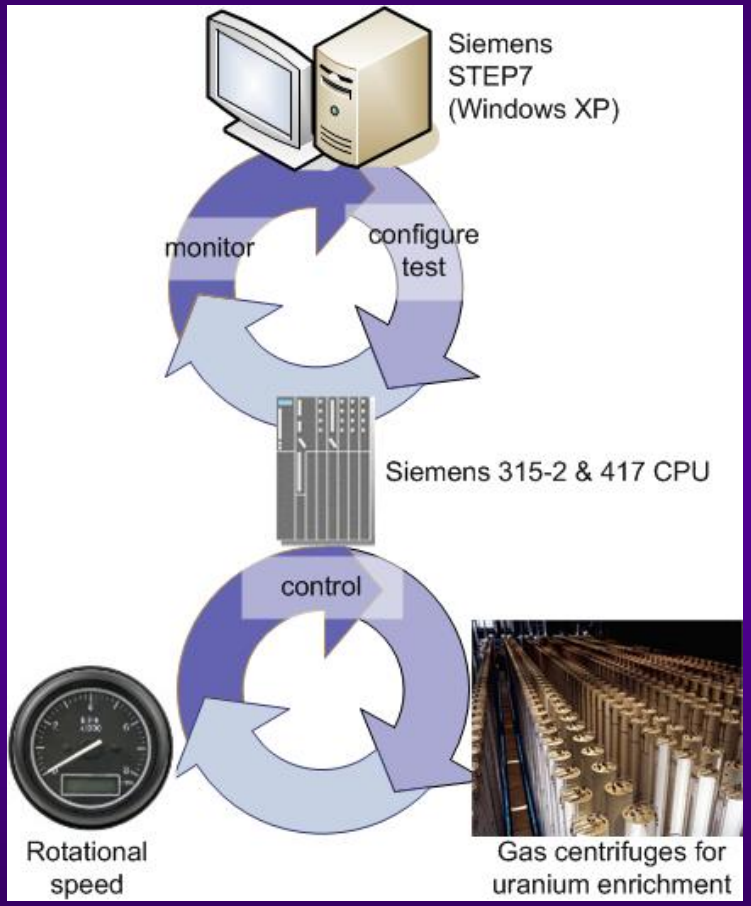
- **Stuxnet downloads and replaces code and data to alter PLC behavior**

This code varies the rotational speed of the centrifuges over months,

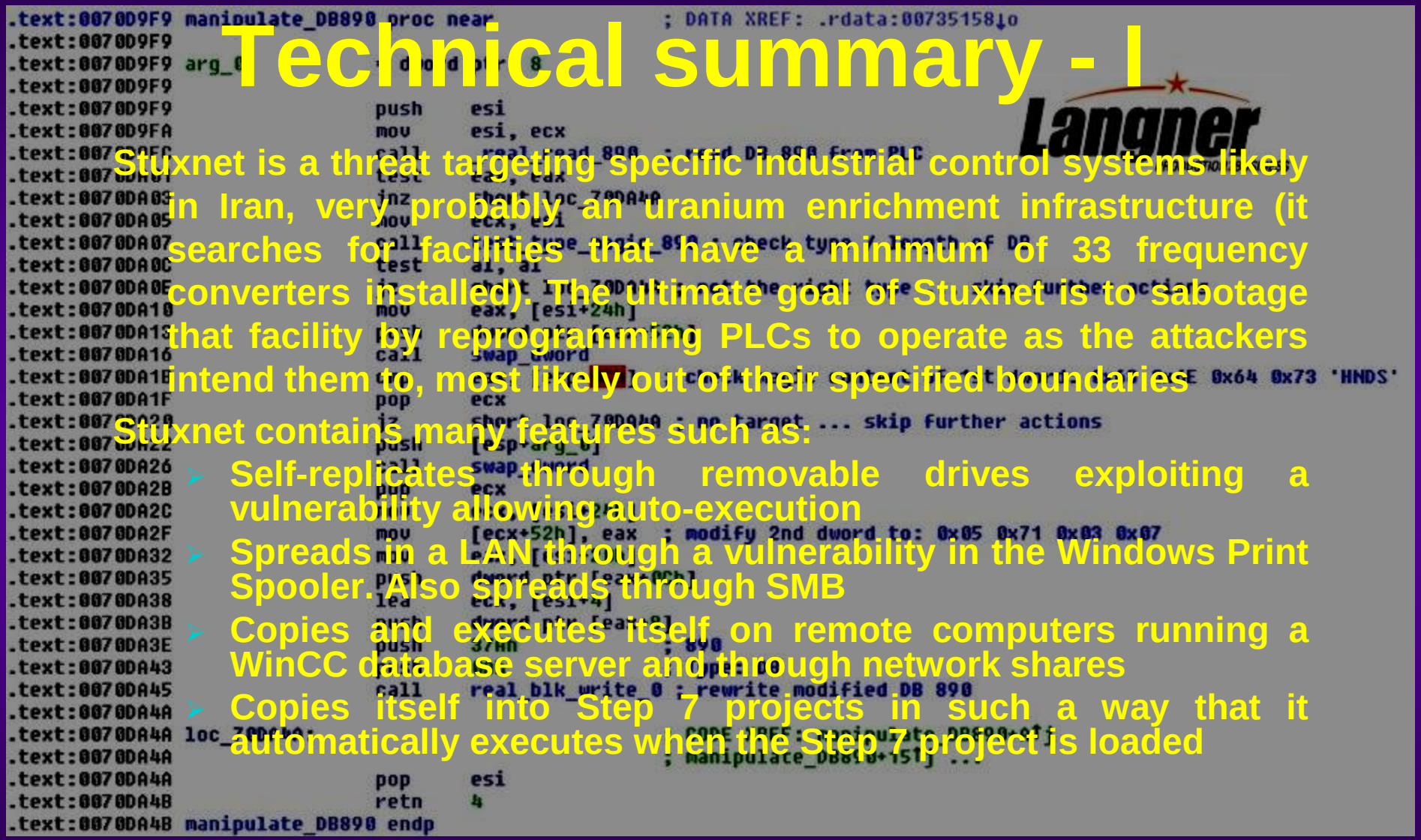
wearing them out by slowly cracking centrifuge rotors and inhibiting uranium enrichment

…in the meantime…

everything looks normal at the SCADA supervisor level



Technical summary - I



Stuxnet is a threat targeting specific industrial control systems likely in Iran, very probably an uranium enrichment infrastructure (it searches for facilities that have a minimum of 33 frequency converters installed). The ultimate goal of Stuxnet is to sabotage that facility by reprogramming PLCs to operate as the attackers intend them to, most likely out of their specified boundaries

Stuxnet contains many features such as:

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution
- Spreads in a LAN through a vulnerability in the Windows Print Spooler. Also spreads through SMB
- Copies and executes itself on remote computers running a WinCC database server and through network shares
- Copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded

Technical summary - II

- Updates itself through a P2P mechanism within a LAN, just injecting a new version of the worm
- Compromises the O/S by exploiting a total of four(!) zero-day exploits (unpatched MS vulnerabilities worth >$100k, two for self-replication and two for escalation of privilege) and it takes advantage of seven different propagation processes
- Establishes a P2P connection to a C&C server that allows the hacker to download and execute code, including updated versions
- Contains a Windows rootkit that hides its binaries. Hides modified code on PLCs, first PLC rootkit ever seen
- Attempts to bypass security products. Signed with two trusted (stolen) digital certificates (for drivers) to avoid being detected
- 4-5 different versions starting 6/2009
- Sophisticated techniques to limit/avoid reverse engineering of the code
- One of the most complex and carefully engineered worms ever seen. Science-fiction code

Comments

- **Stuxnet code is sophisticated, incredibly large (about 0.5MB), mostly bug-free. Probably assembled by a large team of highly qualified experts in different fields with control system expertise, working during an extended period of time, with specific hardware equipment available for testing. The kind of resources needed to stage such an attack seems to point to a nation state. Early versions in/before 2009(?)**
- **The attack involves heavy insider knowledge. Combination of cyberwar and intelligence**
- **The worm "very likely" responsible for disruption of Iran's nuclear program by damaging centrifuges at uranium enrichment facility in Natanz (no other targets). Iranian President acknowledged the damage from the worm (distribution of infected hosts: 59% Iran, 18% Indonesia, 8% India)**
- **Model for simple, destructive SCADA worms. Many ICS and SCADA systems have many exploit opportunities (it exploits inherent PLC design issues)**

Comments

- One more cyber-weapon? Duqu (Remote Access Trojan, not self-replicating, missing component?). Discovered in 2011, code very similar to Stuxnet but targeting computers rather than ICS. Probably built for information gathering (installs a back door and an info-stealer recording keystrokes and system information). Custom protocol to communicate between infected systems and C&C server. Additional variants with compilation time as of October 2011. Precursor of next Stuxnet-like attack on critical infrastructures? Cyber-reconnaissance (for Stuxnet)? Designed to last 36 days and then remove itself from the system
- Security community divided:
  - Stuxnet and Duqu developed by the same team, single software development platform to build both (Kaspersky Labs)
  - Duqu developed by a separate team who studied the Stuxnet code and adapted it (McAfee)

More general comments

- Most dangerous parts of Stuxnet are generic, nothing specific to uranium enrichment plants, and can be copied and modified to work in different environments. Delivery could be done in different ways than USB sticks (remember Code Red). Cyber-weapons of mass destruction??
- Executables using the Stuxnet source code have been discovered. They appear to have been developed since the last Stuxnet version was recovered
- Cyber-weapons proliferation? Cyber is a “once-only” weapon (lost after delivery)? Digital arms race??
- Cyberwar <- Battlefield digitization <- EW warfare

  ICT & microelectronics (r)evolution in warfare techniques and battlefield

More general comments

- Cyber-only-war will never exist (support to conventional operation, espionage, sabotage) but cyber is an autonomous warfare domain
- Is “cyber” different from land, sea, air, and space warfare operative domains? Artificial dimension created by man. Cyber-space is both a weapon AND a target at the same time?! Space/topology of the weaponry can be affected by the weapon (like if weapons used in warships could change the geography of oceans). Cyber-topology VERY volatile: regions of cyberspace appear/disappear on command or under (cyber/conventional) attack. Different “geography” from different locations
- Deterrence probably non applicable to cyber domain (offense is dominant over defense)

Back to this society…??

…basic infrastructures,
almost ICT / ICS independent…

Comments / Questions

A few references

W32.Stuxnet Dossier (Version 1.4 February 2011), N.Falliere, L.O Murchu, E.Chien, Symantec Corp. (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)

"Stuxnet is a directed attack -- hack of the century", R.Langner, Langner Communications GmbH (http://www.langner.com/en/)

"Exploring Stuxnet's PLC Infection Process", N.Falliere (http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process)

Dr. Stefan Lüders (CERN Computer Security Officer), private communication