Cyber-warfare

The dark side of ICT

Gian Piero Siroli, Physics & Astronomy Dept. Univ. of Bologna & CERN

CERN Academic Training, Geneva, January 2016

What a cyber-weapon can look like: Stuxnet

- 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 cyber-weapon, deployed to seek and damage a real world physical target, operating the machinery outside its safe/usual performance envelope. Heavy insider knowledge, combination of cyber-war and intelligence
- Disruption of Iran's nuclear program by damaging centrifuges at uranium enrichment facility in Natanz
- Worm analyzed in public conferences, papers from various authors, probably the best studied piece of malware in history. Executable code available on the network

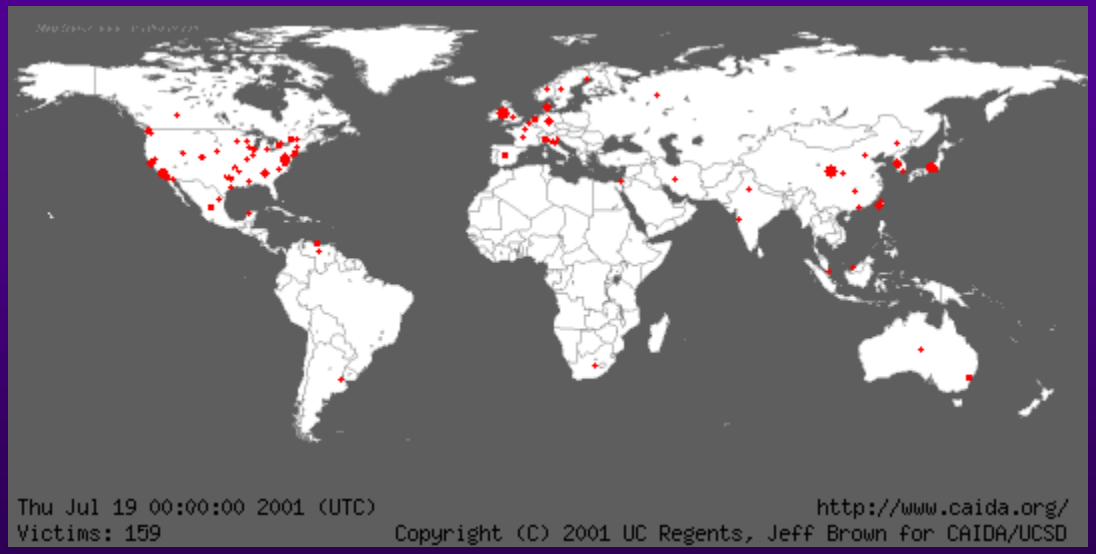
What is Stuxnet?

- **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**

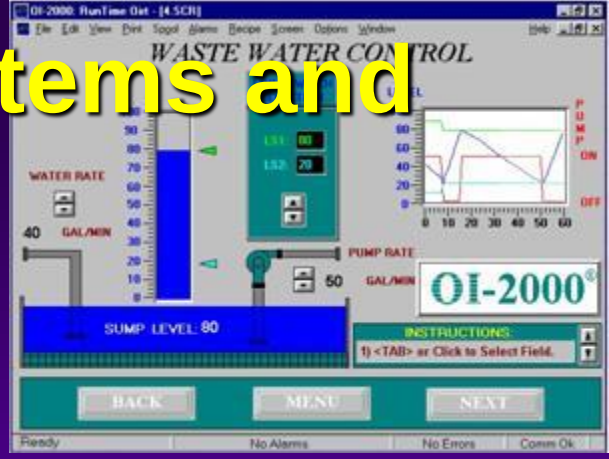
What is a worm

- 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

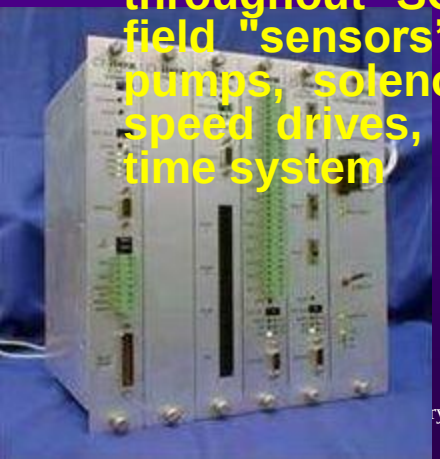
Code Red worm propagation during 24h following release (2001)



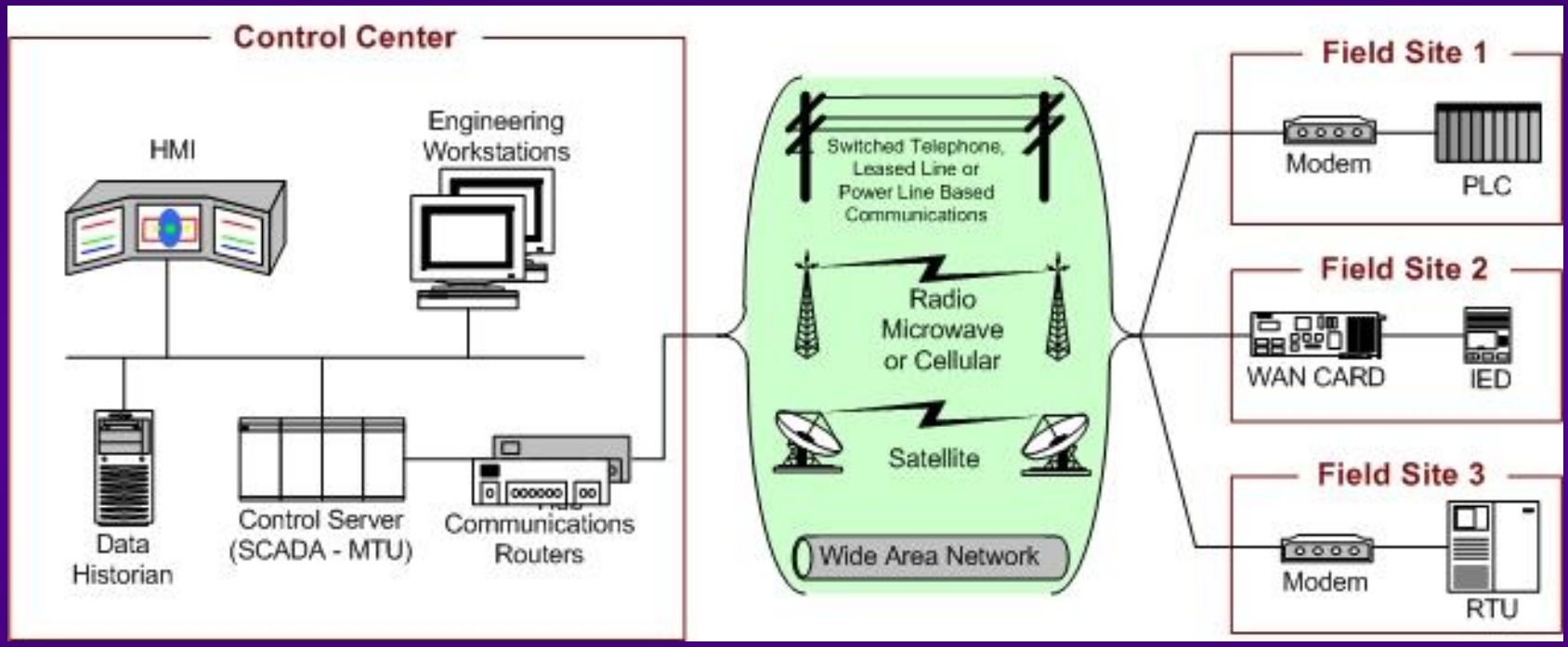
Industrial Control Systems and SCADA



- 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
- 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

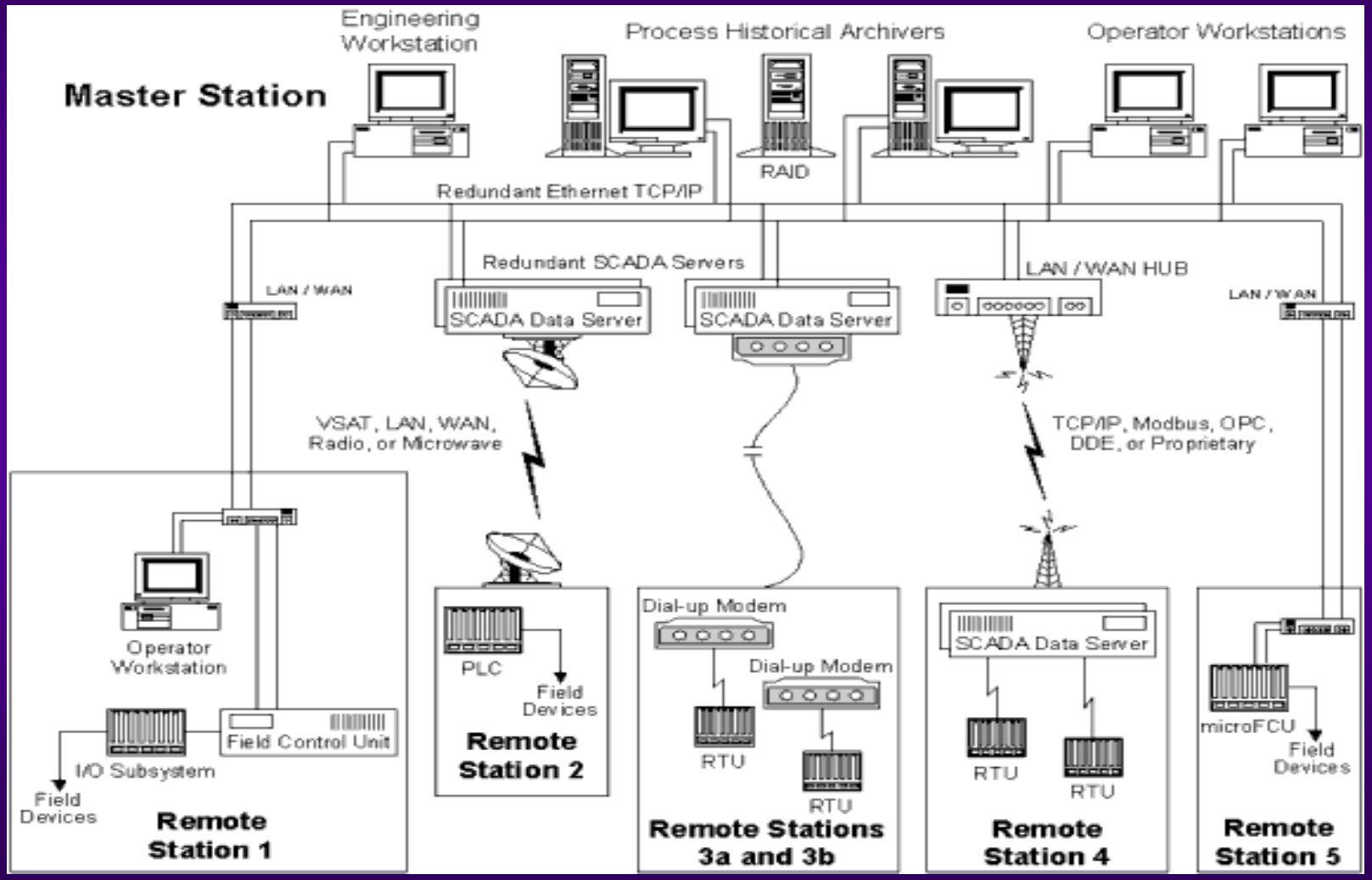


SCADA general architecture



Network components: fieldbus network, control network, communication routers, firewalls, modems, remote access points

Many intrusion vectors and open doors



SCADA & ICT

Historically SCADA systems have been closed/isolated environments built around custom made & proprietary protocols and systems

- **Control networks converging with corporate networks (business requirements, decision support systems, cost reduction). Standardization of SCADA components…**
  - **Proprietary field busses replaced by Ethernet LAN & TCP/IP**
  - **Field devices connect through Ethernet & TCP/IP**
  - **VPN connections from outside world onto the control networks for remote maintenance**
- **…and extensive use of ICT protocols & applications**
  - **HTTP (WWW), FTP, Telnet, SMTP, SNMP…**
  - **Wireless LAN, Notebooks, USB sticks…**
- **Poorly secured systems: communications with no authentication (spoofing), very little encryption, unrestricted access**
  - **Internet Worms spreading within seconds**
  - **Unpatched operating systems and applications**
  - **Missing anti-virus software or old virus signature files**
- **Zero Day Exploits: security holes without patches**
  - **Break-ins occur before patches are available or deployed (and immediately after)**

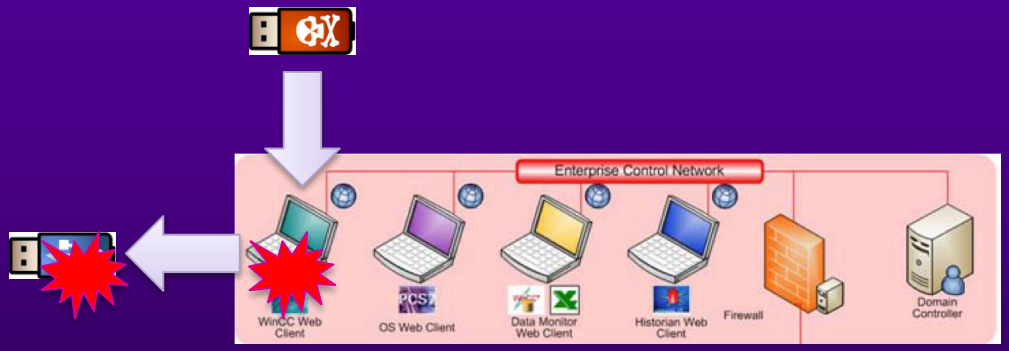
Critical infrastructures strongly dependent on ICT, intrinsically unsafe and vulnerable

- Security flaws inherent in Internet Protocol suite (TCP/IP, most widely used communication standard on the Internet). Security not was not a primary design consideration. Many attacks are “legal” actions according to protocols
- Faulty implementation of protocols and improper configuration
- Bugs in s/w code, flaws in architecture & design
- Security often not (properly) implemented
- Vulnerabilities of ICT underlying layer projected onto critical infrastructures

Vulnerabilities available on the net

First Infection: Enterprise Computer

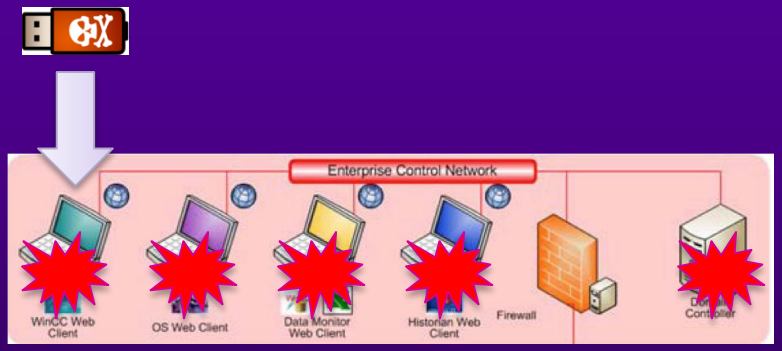
- Infected USB drive infiltrated into the plant and inserted into computer (employees laptop infected off-site, infected project files from contractor). Malicious act or through social engineering. “Air-gap” overcome
- Stuxnet successfully installs even though computer is fully patched and up to date 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



(animation from E.Byres, Tofino Security)

Propagation on Enterprise Network

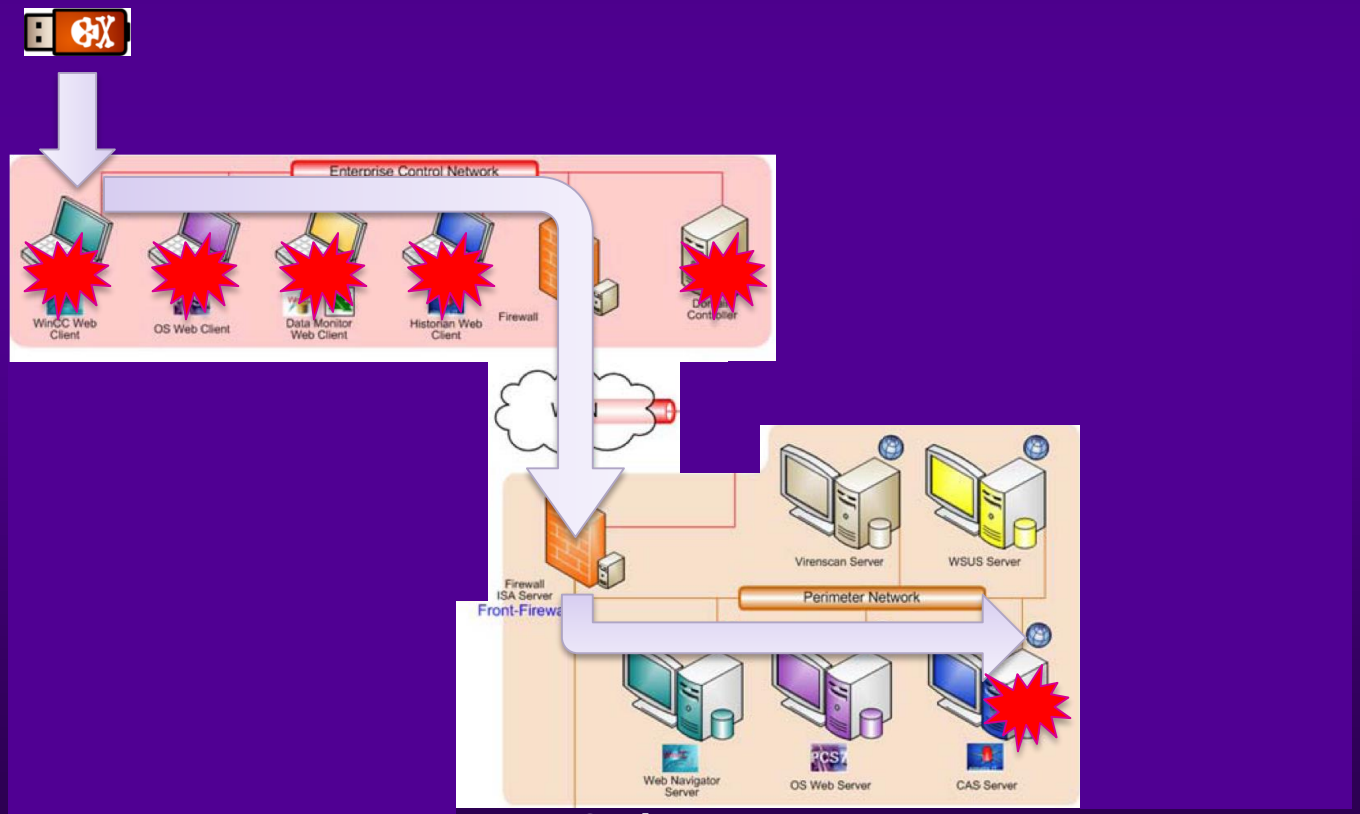
- Rapidly spreads to Print Servers and File Servers within hours of initial infection
- Establishes P2P network and access to C&C server (but the worm is autonomous, no remote control, “Launch and Forget”)
- Infects any new USB Flash drive inserted into any computer



(animation from E.Byres, Tofino Security)

Penetrating Perimeter Network

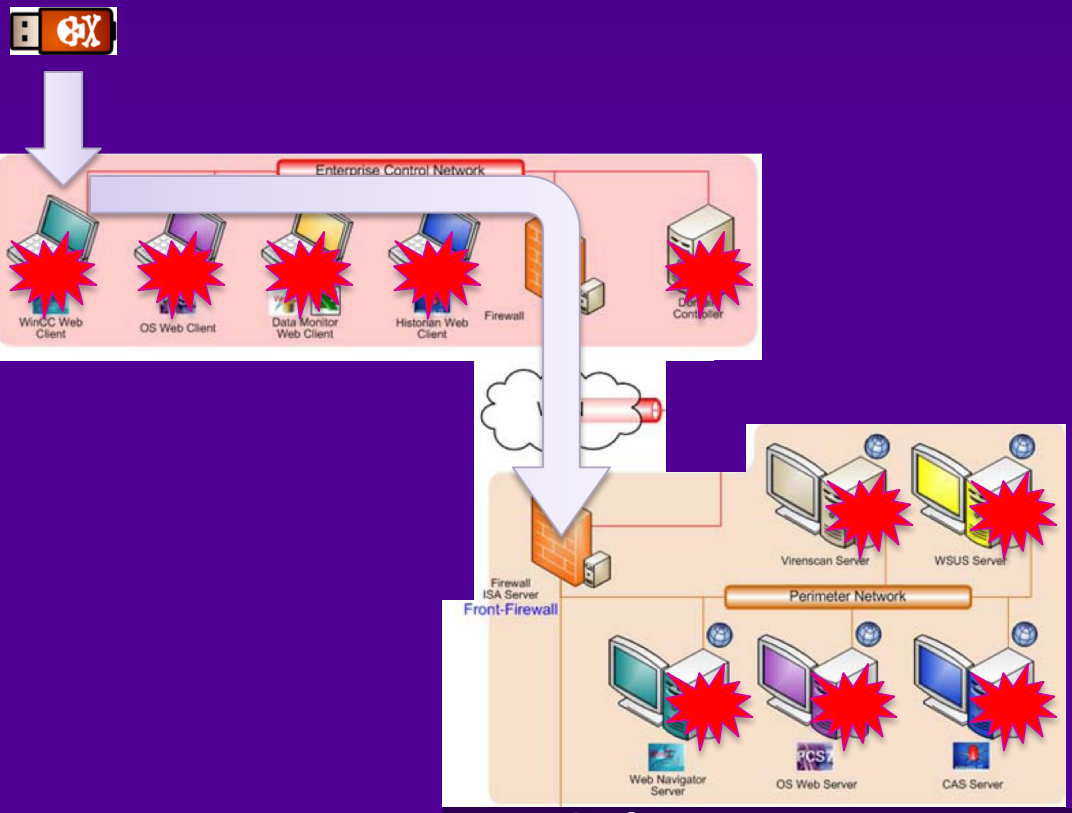
- System Admin (Historian) becomes infected through network printer and file shares
- System Admin connects via VPN to Perimeter Network and infects the CAS Server and its WinCC SQL Server database



(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

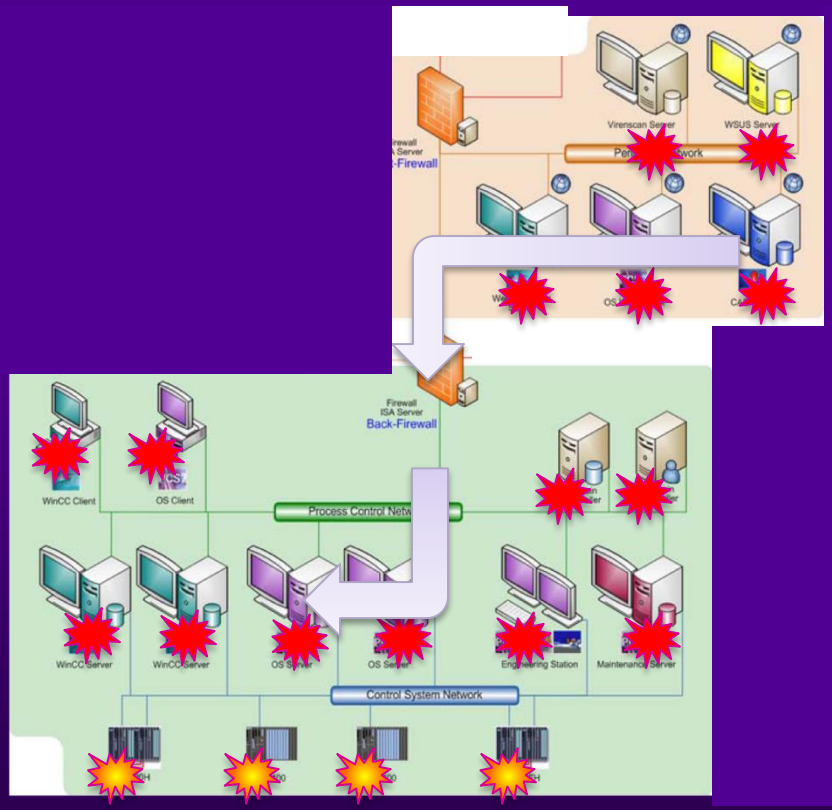


(animation from E.Byres, Tofino Security)

Propagation to Control Networks

- Leverages network connections between Perimeter and Process Control Network
- Exploits database connections between CAS Server (Perimeter) and Operator Station Server (PCN)
- Infects other hosts on PCN via Shares, WinCC or STEP7 methods

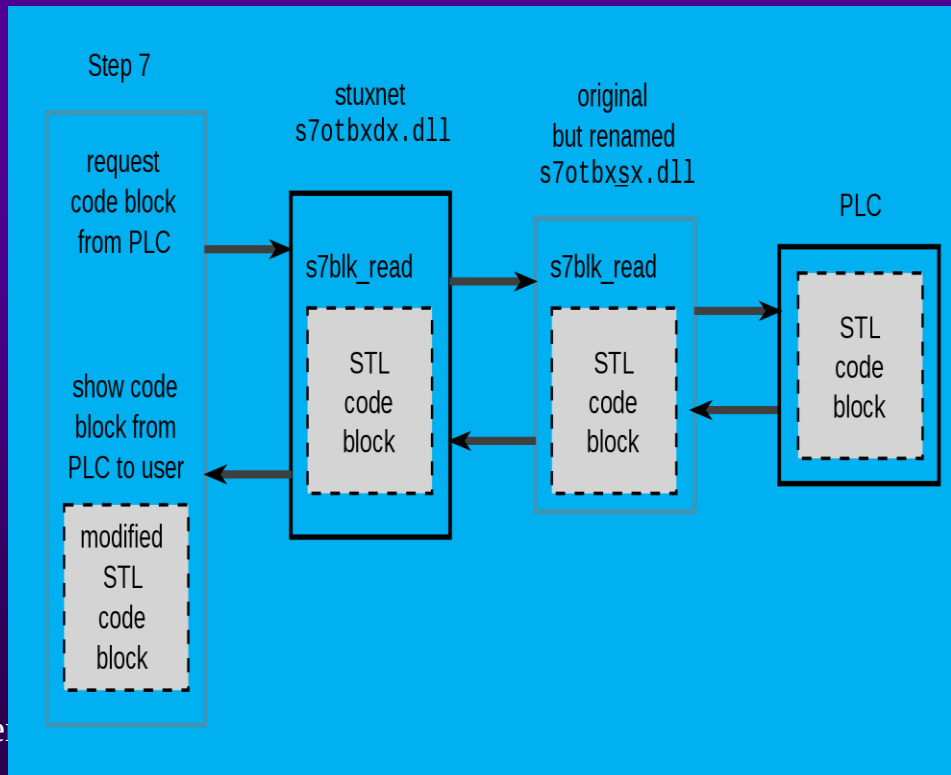
- …until it gets at the interface of the PLC level, and propagates further crossing it…



(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

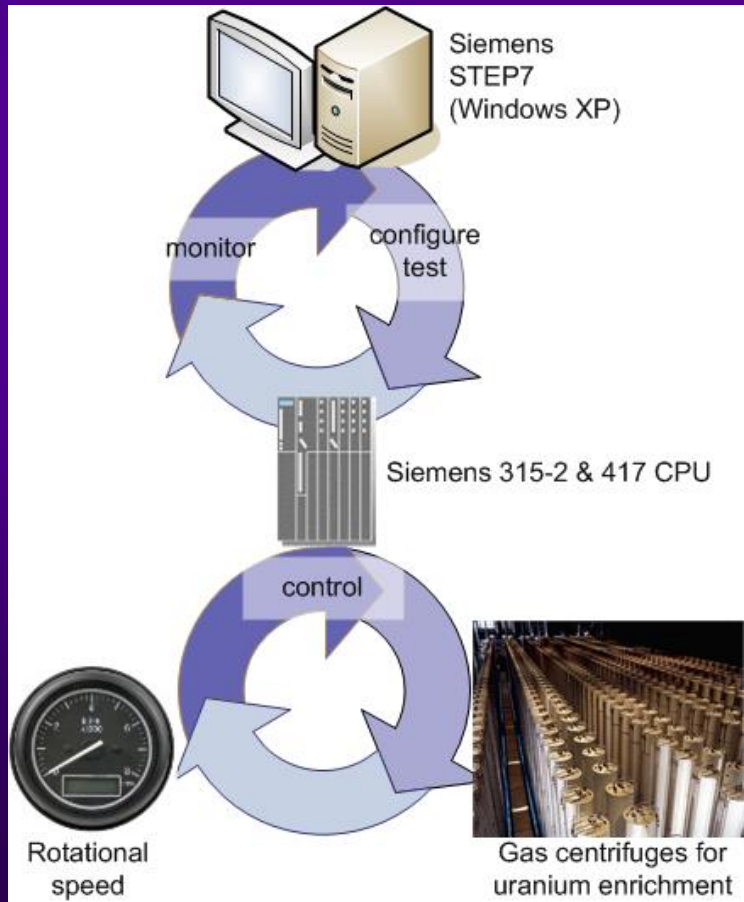
- Stuxnet downloads and replaces code and data to alter PLC behavior controlling the communication between PLC & control system. It intercepts the input values from sensors and give fake data to legitimate programs

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

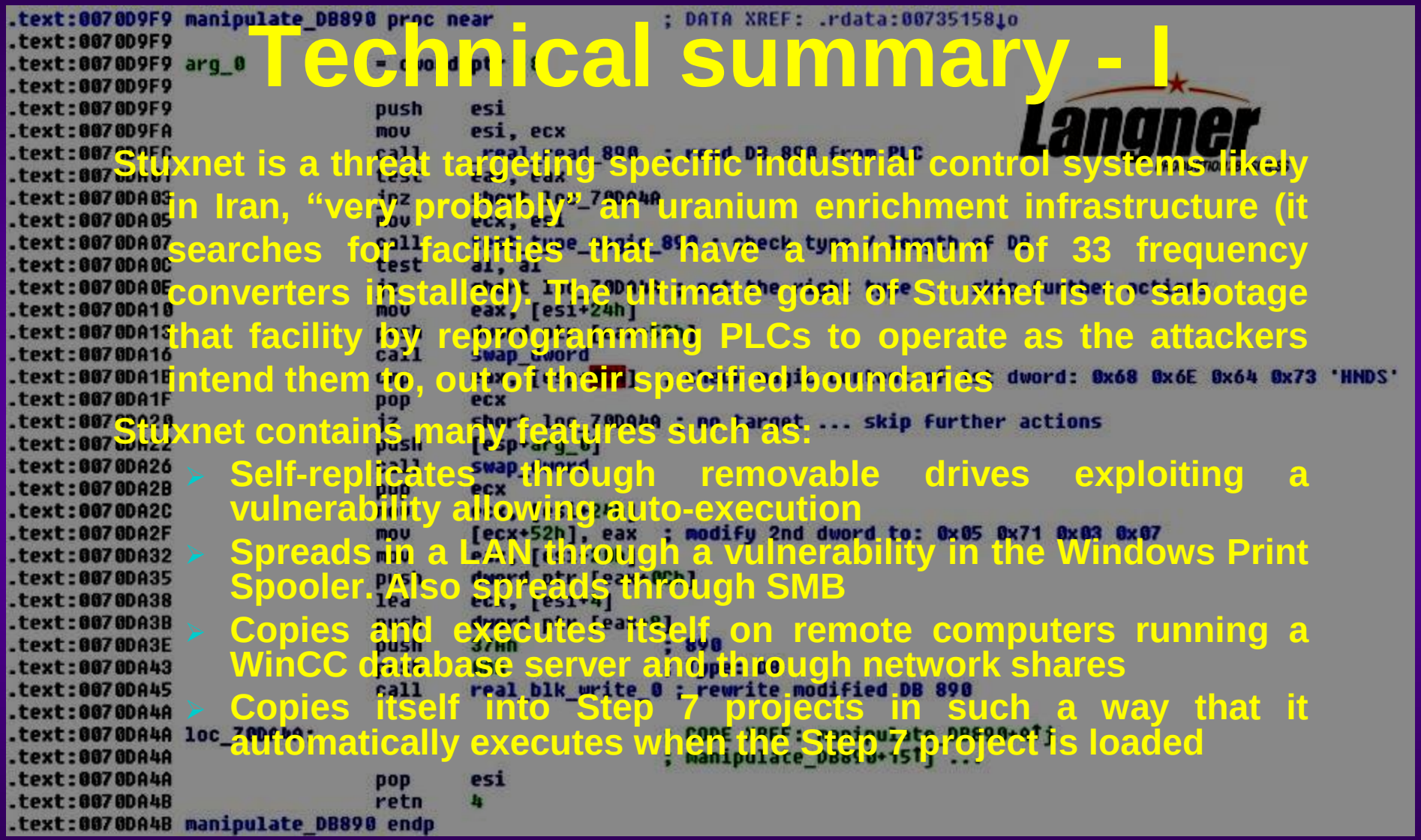
wearing them out by slowly cracking centrifuge rotors and inhibiting uranium enrichment

…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, out of their specified boundaries

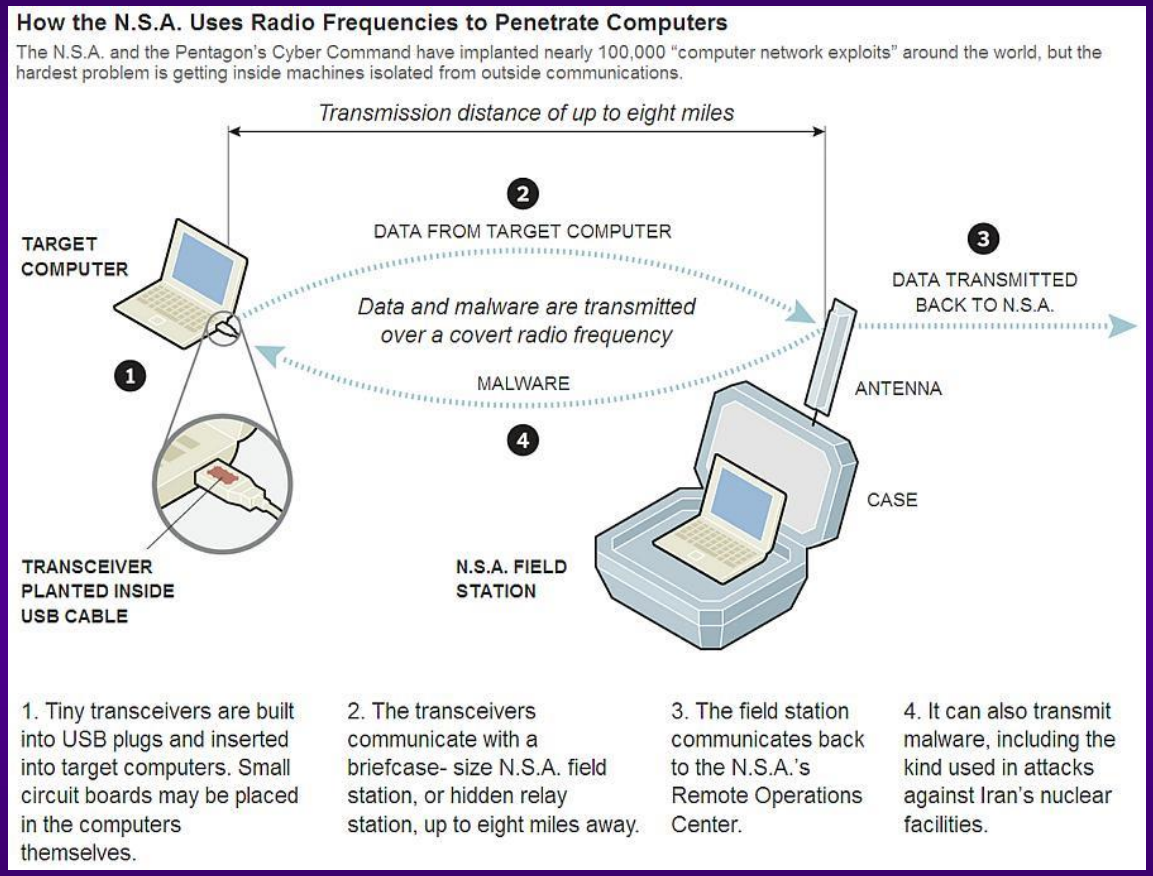
Stuxnet contains many features such as:

- 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. Autonomous cyber weapon system
- 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
- Many different versions starting 6/2009
- Sophisticated techniques to limit/avoid reverse engineering of the code (encryption, anti-anti debug)
- One of the most complex and carefully engineered worms ever seen. Science-fiction code

Air gap penetration example



Ultrasonic (inaudible) sounds to bridge air-gapped computers?! (BadBIOS??)

Comments

- Stuxnet code is sophisticated, very large (about 0.5MB). 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(?)
- Model for simple, destructive SCADA worms. It exploits inherent PLC design issues
- The attack involves heavy insider knowledge. Combination of cyber-war and intelligence
- Stuxnet, targeting a specific industrial control system, is responsible for the disruption of Iran's nuclear program by damaging centrifuges at uranium enrichment facility in Natanz (no other targets). Iranian President acknowledged the damage by the worm (distribution of infected hosts: 59% Iran, 18% Indonesia, 8% India)

ICS vulnerabilities: back to this society…??

…basic infrastructures, almost ICT / ICS independent…

More cyberweapons

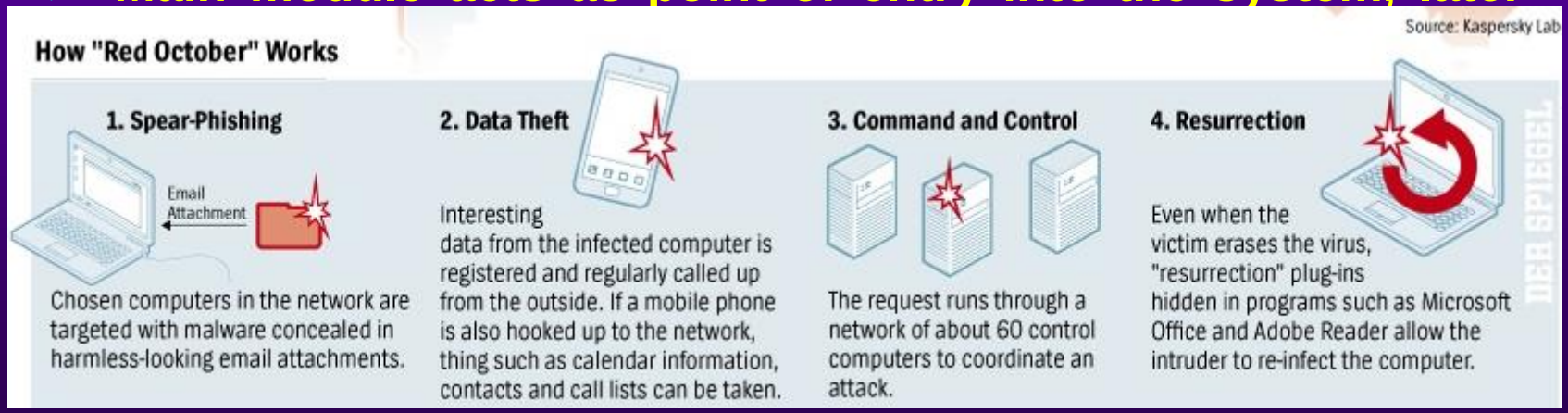
- **Duqu (2011, Remote Access Trojan, not self-replicating, missing component?). Very similar to Stuxnet, targeting computers rather than ICS. Probably built for information gathering (back door, recording keystrokes and system information). Cyber-reconnaissance? Precursor of next Stuxnet-like attack?? Limited targets. Designed to last 36 days. Duqu2.0**
- **Flame (June 2012 reported in Iran). Optimized for espionage, at least two years old, mainly confined in Iran and Middle East. Large and complex, impressive espionage capabilities: recording voice and skype conversations, screenshots, keyboard activity, network traffic. No automatic replication/propagation (stealthier and better targeting). "Self destruct" module to eliminate traces and avoid code analysis. Connection to Stuxnet, commissioned by the same nations?**
- **Gauss (summer 2012) - Nation-state sponsored banking Trojan for info stealing, monitor bank accounts & money flow. Similarities with Flame. Distributed mainly in Lebanon, Israel, Palestine. Mysterious encrypted payload surgically targeted**
- **Shamoon (summer 2012) - cyber-sabotage in oil & energy sectors (Saudi company Aramco). Similarities with Flame**
- **Red October (January 2013) - advanced cyber espionage network targeting diplomatic/governmental agencies and scientific research organizations attacking computers, mobile phones, network equipment**

…and more to come…

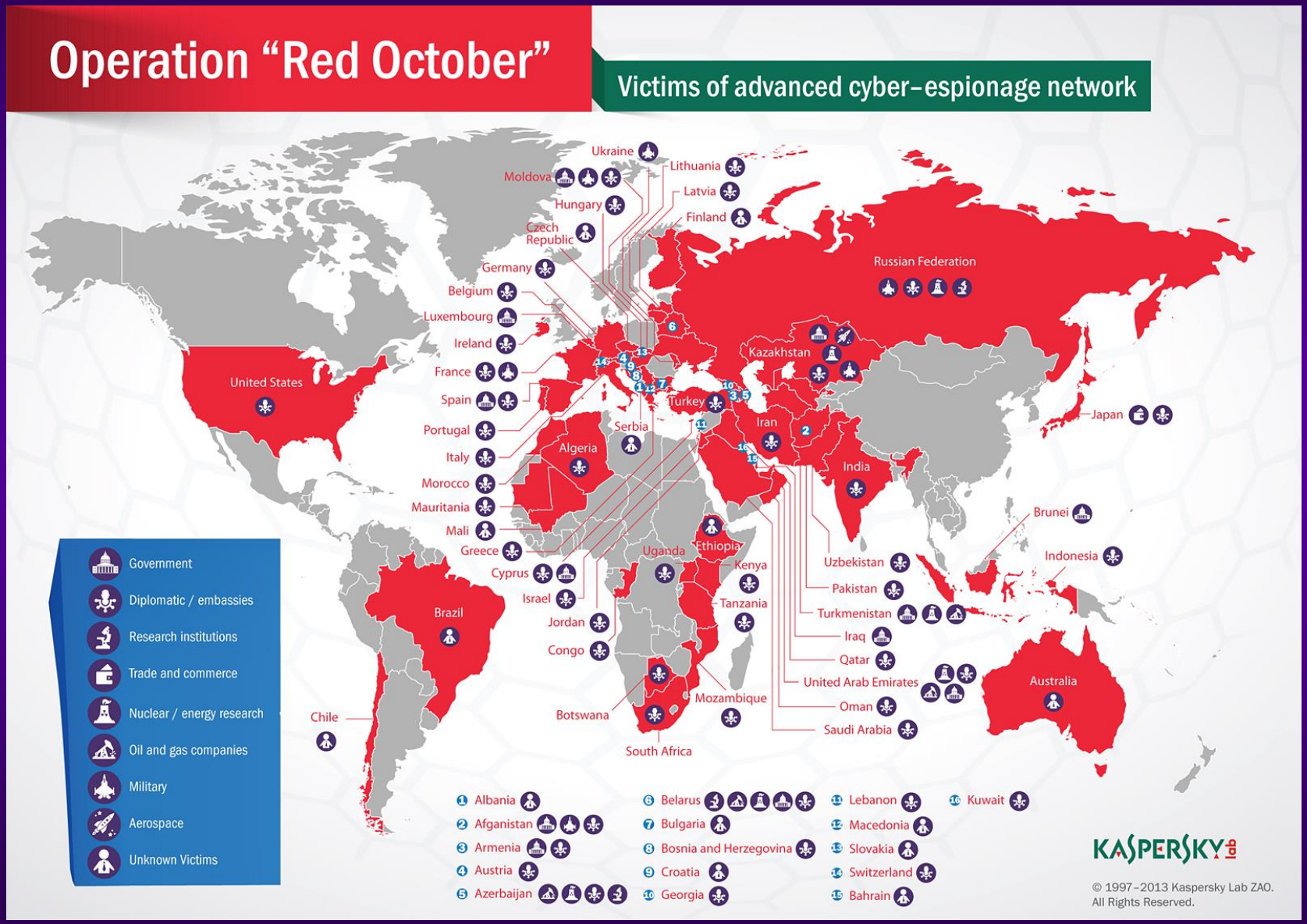
the next one might already be on your desktop, laptop, smartphone

Red October

- 1,000+ modules allowing to craft highly advanced infections tailored to unique configurations of infected nodes & user profiles. Most of the tasks as one-time events: DLL code received from an attacker server, executed in memory & immediately discarded. Social engineering component: targeted email phishing. Active since 2007, undetected for more than 5 years. Hijack WinUpdate mechanism. Different exploits: Excel(2009) & Word(2010, 2012) via email, malicious web pages(2011), relying on Java exploit for infection
- Main module acts as point of entry into the system, later

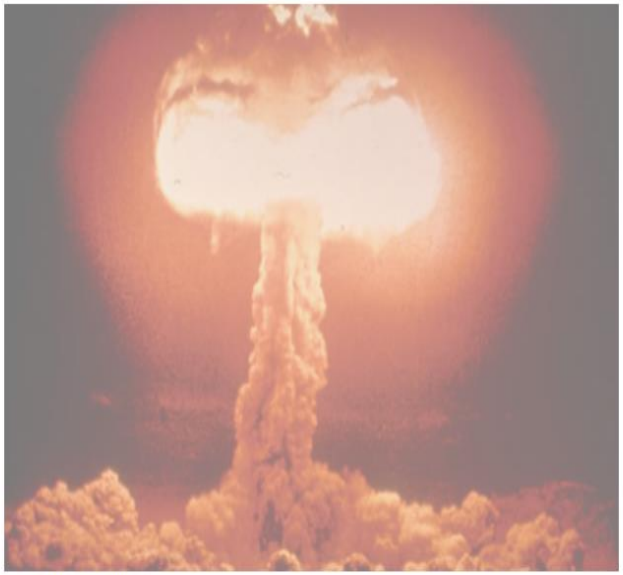


Red October


Operation "Red October"
Victims of advanced cyber-espionage network
Ukraine
Moldova
Lithuania
Latvia
Hungary
Finland
Czech Republic
Germany
Belgium
Luxembourg
Ireland
France
Spain
Portugal
Italy
Morocco
Mauritania
Mali
Greece
Cyprus
Israel
Jordan
Congo
Botswana
South Africa
Chile
Brazil
United States
Russian Federation
Kazakhstan
Turkey
Serbia
Algeria
Iran
India
Japan
Brunei
Indonesia
Uzbekistan
Pakistan
Turkmenistan
Iraq
Qatar
United Arab Emirates
Oman
Saudi Arabia
Uganda
Ethiopia
Kenya
Tanzania
Mozambique
Australia
Government
Diplomatic / embassies
Research institutions
Trade and commerce
Nuclear / energy research
Oil and gas companies
Military
Aerospace
Unknown Victims
1 Albania
2 Afganistan
3 Armenia
4 Austria
5 Azerbaijan
6 Belarus
7 Bulgaria
8 Bosnia and Herzegovina
9 Croatia
10 Georgia
11 Lebanon
12 Macedonia
13 Slovakia
14 Switzerland
15 Bahrain
16 Kuwait
KASPERSKY lab
© 1997-2013 Kaspersky Lab ZAO.
All Rights Reserved.

MORE

Ways $460 million military contract for cyber bombs could attack targets



Credit: FEMA News Photo

Defense contractors will compete for a $460 million contract to develop critical infrastructure cyber bombs. The CEO of Indegy provided insight into potential ways cyber weapons could attack targets as well as what can be done to protect against them.

Computerworld | Nov 25, 2015 5:00 AM PT

RELATED TOPICS

- Cybercrime & Hacking
- Infrastructure Management
- IT Management

For years, the U.S. has expressed concerns about potentially tainted supply chains. Some of the tech contained 'trapdoors' for espionage. Yet according to Fidelis Cybersecurity CSO Justin Harvey, Chinese state-sponsored attackers, in recent times have been "leaving behind something much more sinister: logic-bombs. The theory is that these logic-bombs are being left behind so that in the event of a military strike, China would have the capability to render its foes incapacitated."

MORE LIKE THIS


Forecast 2016: Security takes center stage


Review: Password managers help keep hackers at bay

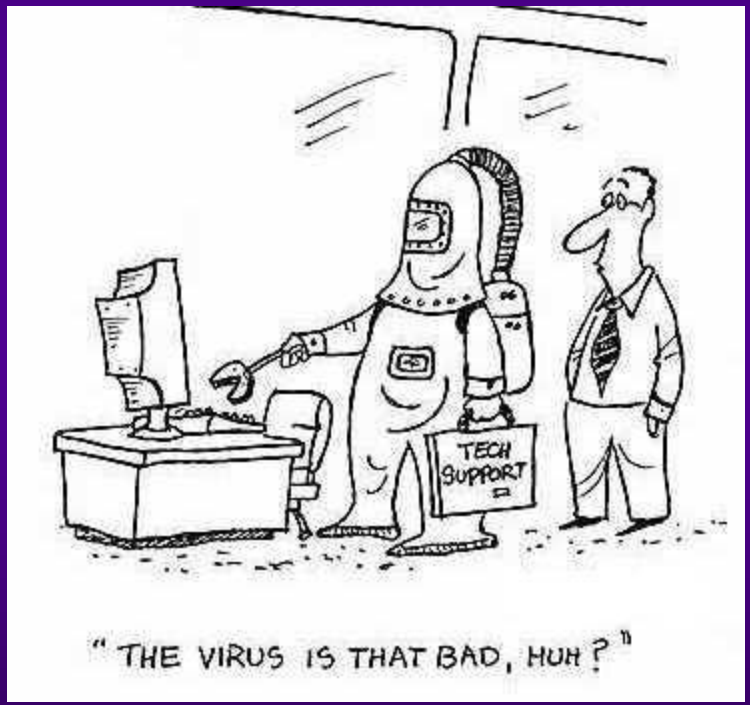

This is why tech toys are dangerous

on IDG Answers
If I buy a Chromebook and can't get to grips with OS can I convert to windows?

?? more ??

- **January 2016: report from SANS about the possible Russian attack on the electric power grid in Ukraine causing a black out**
  - **"Ukrainian power outage is more likely to have been caused by a cyber attack than previously thought. Early reporting was not conclusive but a sample of malware taken from the network bolsters the claims. The unique nature of the malware indicate some level of targeting may be possible but much more information is needed to confirm that targeting of ICS or this specific facility was intended" (SANS)**
- **2014: German Steel Mill Meltdown**
  - **Attacked an unnamed steel mill in Germany. Manipulating and disruption of control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive" (unspecified) damage (German Federal Office for Information Security)**
- **2008: Mysterious Turkey Pipeline Blast**
  - **The Turkish government publicly blamed a malfunction (3 weeks to recover)…For western intelligence agencies, the blowout was a watershed event. Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line**

The end
(part I)



World Wild Web

Gian Piero Siroli

World Wild Web

The end

(part I)

Gian Piero Siroli