StuxNet Explained

Sandro Etalle

Technische Universiteit
Eindhoven
University of Technology

Where innovation starts

About the speaker

- **Sandro Etalle**
  - **Italian/Dutch (1965)**
  - **Full professor,**
    - **head of the Security Group at the TU/Eindhoven**
    - **member of the DIES group at the UTwente**
  - **Founder (& for the moment CEO) of the spin-off SecurityMatters. www.securitymatters.eu.**

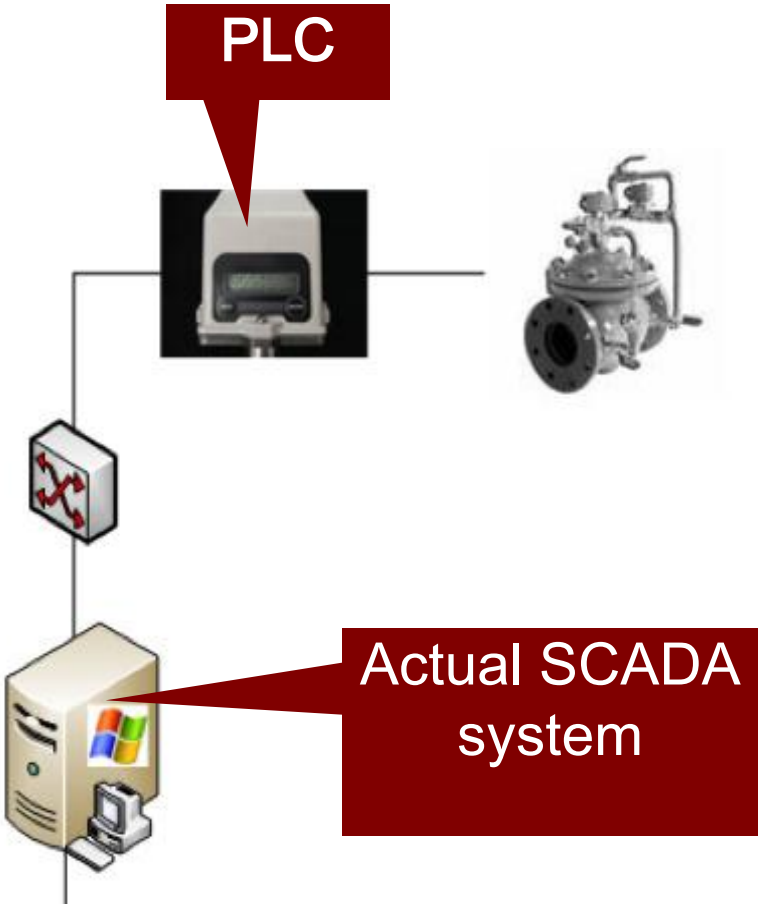
  - **Contact:**
    - **s.etalle@tue.nl**
    - **Or use LinkedIn**

What is SCADA

- **Supervisory control and data acquisition**
- **Modern infrastructures such as water, gas, electricity, etc. distributions are controlled by computers**
- **SCADA refers to the computer networks and systems plus the SW applications controlling critical infrastructures**

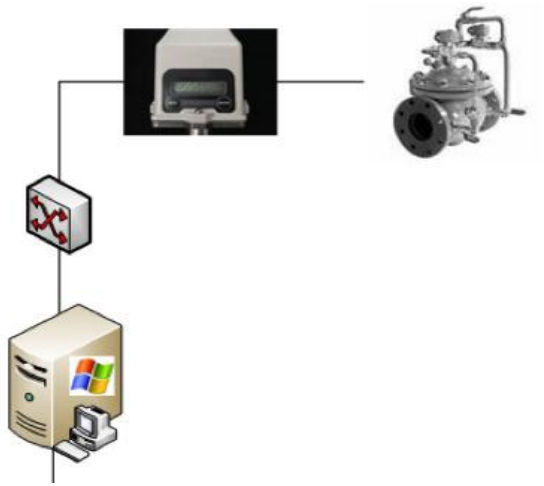
SCADA Essentials

- **PLC: programmable logic controller**
- **Connected to Sensors and Actuators.**
  - **switches,**
  - **temperature and pressure sensors**
  - **operate electric motors,**
  - **pneumatic or hydraulic cylinders**
  - **…**

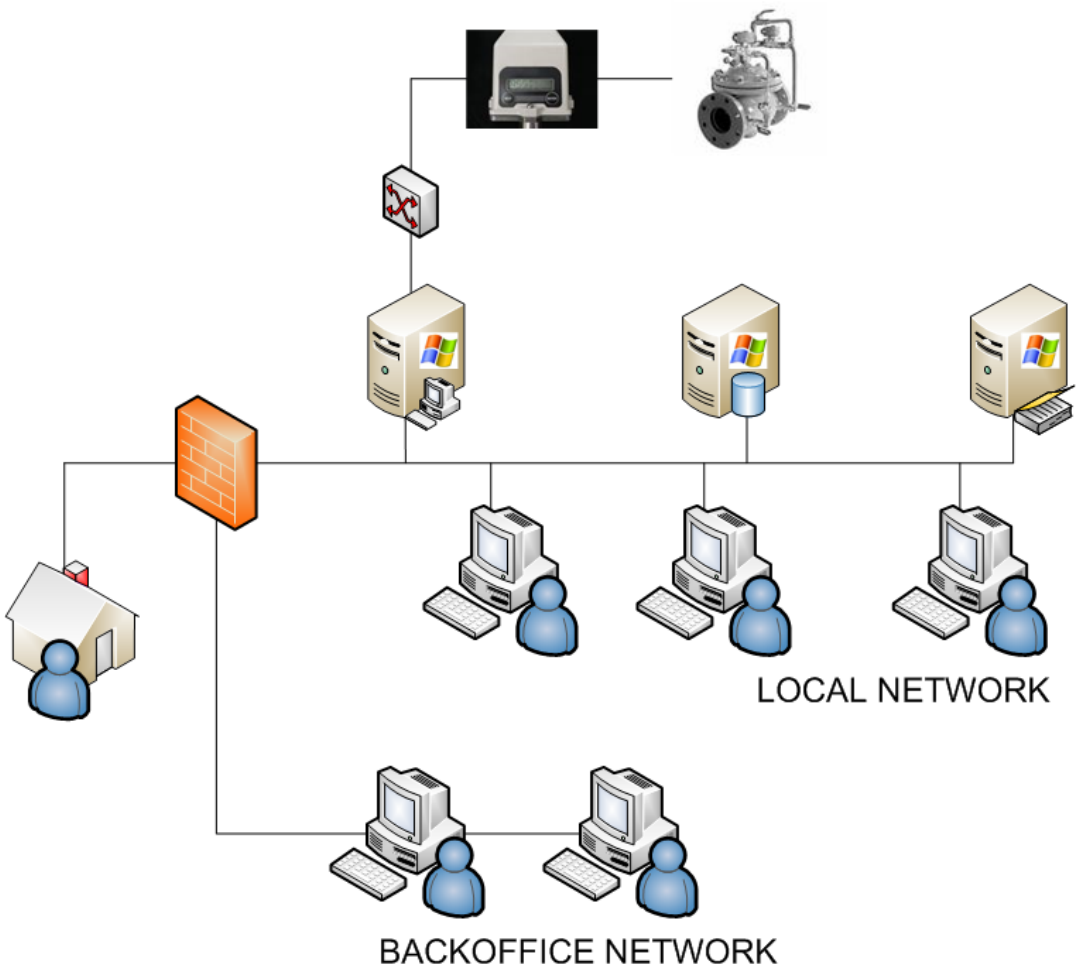


SCADA [20 years ago]

- isolated from public networks for long time
- security was provided by restricted physical access
- systems were proprietary and embedded
- 20 years ago there was no Internet



SCADA Today



The Trouble with SCADA

- **Non-standard, proprietary protocols**
  - **(or open protocols with proprietary extensions)**
  - **security trough obscurity**
- **Communication authenticated by means of MAC and IP addresses (user passwords are usually shared)**
  - **an attacker can easily fake MAC and IP addresses**
- **In general, IT security practices are not fully developed/implemented**
  - **e.g.: common intrusion detection systems (IDS) are signature-based, and a few signatures are available for SCADA**

How Bad is the situation

- **ARE THERE MANY ATTACKS ON SCADA NETWORKS?**
  - **There have never been that many attacks,**
  - **Nothing compared to the Internet**
  - **Though there has been a very significant one (discussed later)**
- **THIS IS ALSO WHY WHY SCADA SYSTEMS ARE SECURITY-WISE STILL SO LOUSY.**
  - **no network access control**
    - **“easily” misused**
  - **hardly resilient**
  - **difficult to protect**
    - **(were not designed with network security in mind)**

A bit on security through obscurity

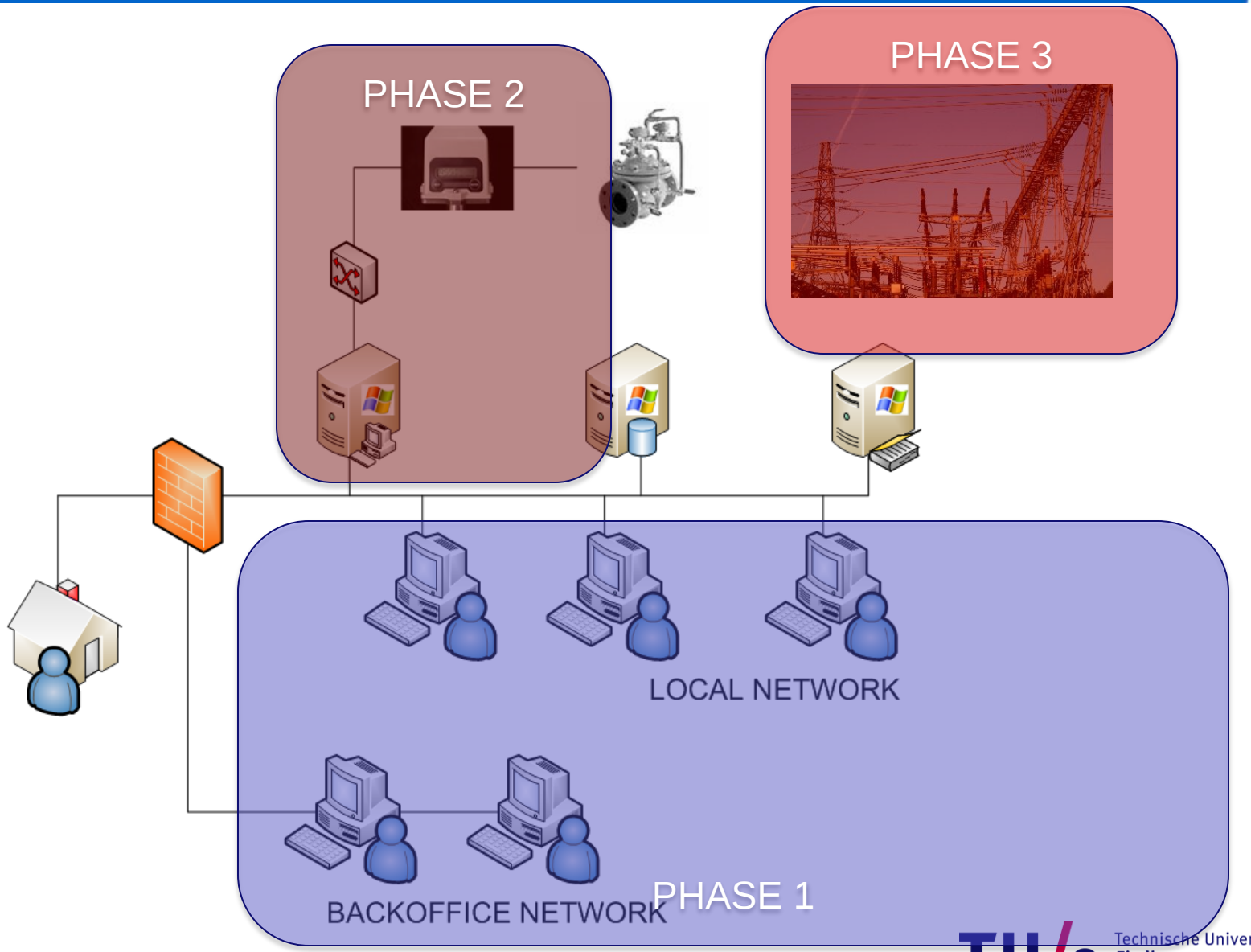
STUXNET

Stuxnet Identity Card

- **The next step in SCADA-based cyberwarfare**

- **Birth Date: Before June 2009**
- **Discovered: June 2010 by VirusBlokAda.**
- **Retirement Date (currently): June 24, 2012**
- **# of computers infected: >= 100.000**
  - **[Kas]: India: 86,000, Indonesia: 34,000, Iran:14,000**
  - **[Sym]: Iran: 60,000, Indonesia 12,000, India: 6,000**
    - **Very conservative**

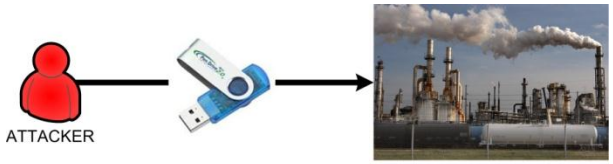
How Does it spread

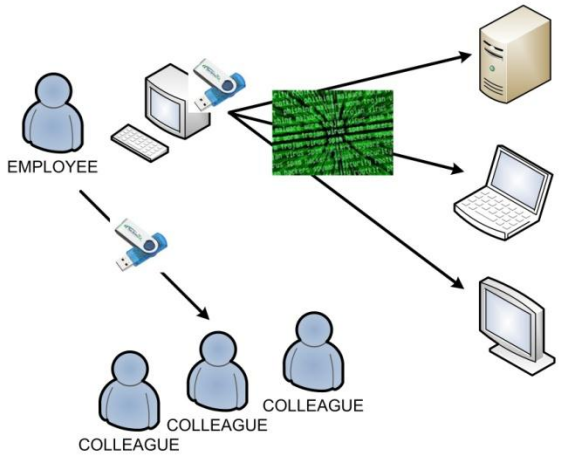


The attack phases

- **PHASE 1: an almost normal worm, amazingly smart**
  - **It spreads, hides, updates itself**
  - **It looks around**
    - **To duplicate itself**
    - **TO SEE IF IT CAN ENTER PHASE 2**
- **PHASE 2: attacking the Siemens + PLC systems**
  - **Infects the SIEMENS System**
  - **It modifies the PLC programming**
- **PHASE 3: sabotage**
  - **Check for a specific factory environment.**
  - **If it does not find it, it does nothing**
  - **If it finds it …. ????**

Phase 1: the Windows system



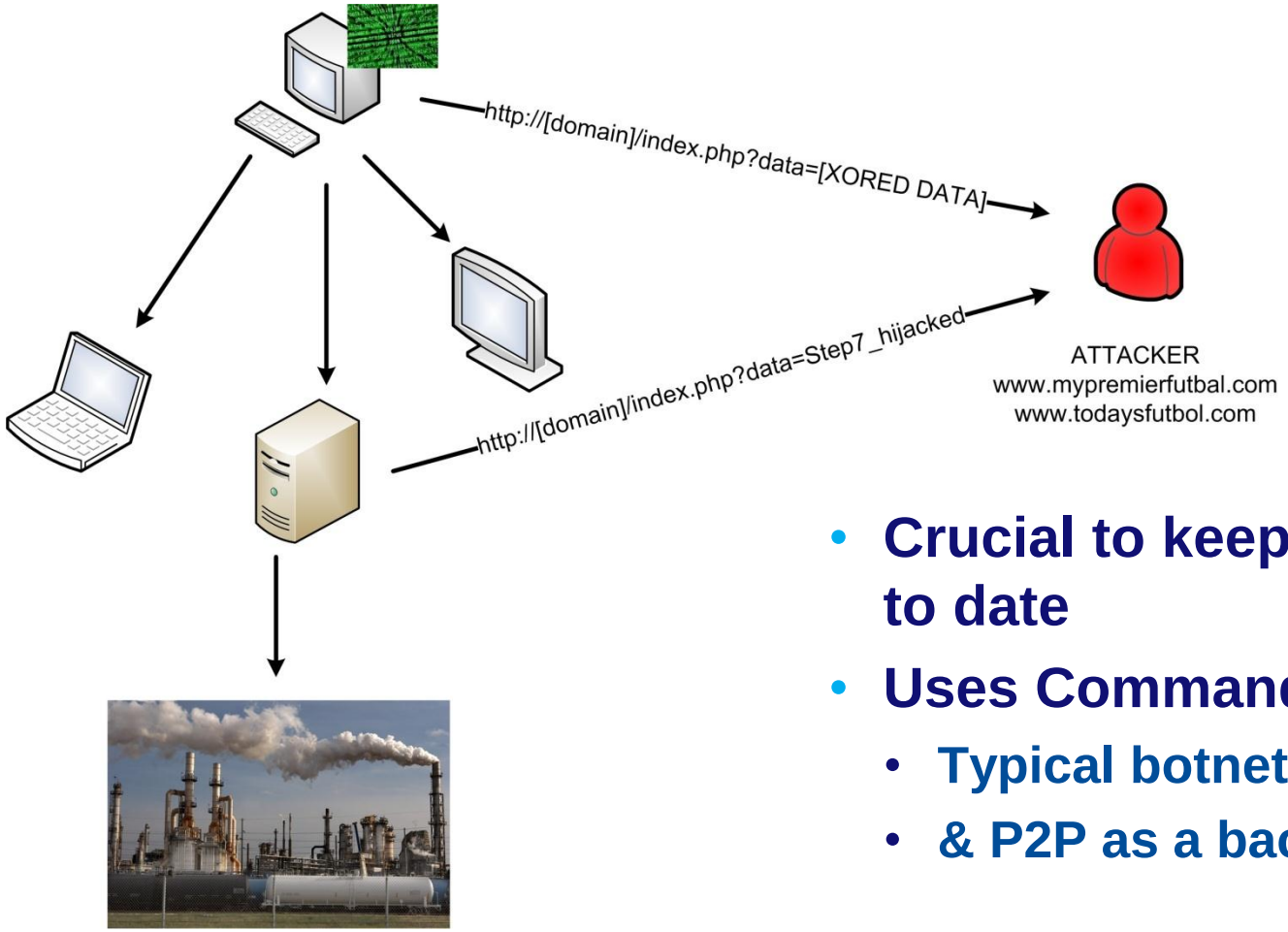


- A very elaborate standard worm
- To get inside the LAN: USB Sticks
- Within a LAN: USB Sticks + Print Spooler, Shared Folders etc
- 4 zero-days vulnerabilities
  - LNK (MS10-046) [patched]
  - Print Spooler (MS10-061) [patched]
  - Server Service (MS08-067) [patched]
  - Privilege escalation (2x, unpatched)
  - Siemens Step 7 project folders

Phase 1: hiding

- Installs a rootkit that makes it invisible.
- It uses drivers that are digitally signed to avoid suspects
  - Uses Realtek & JMicron (stolen) certificates
  - Works on all versions of Windows >= Windows 2K
  - Exits when it finds an “uninteresting” system (e.g. 64 bits)
- Smart injection techniques
  - first checks which antivirus is active
  - Then chooses the target executable accordingly.
  - Very smart way to avoid behaviour blocking when loading DLLs (loadlibrary calls)
  - Avoids double infections

Phase 1: updating the system



- **Crucial to keep the SW up to date**
- **Uses Command & Control**
  - **Typical botnet**
  - **& P2P as a backup**

Phase 1: complexity (part 1)

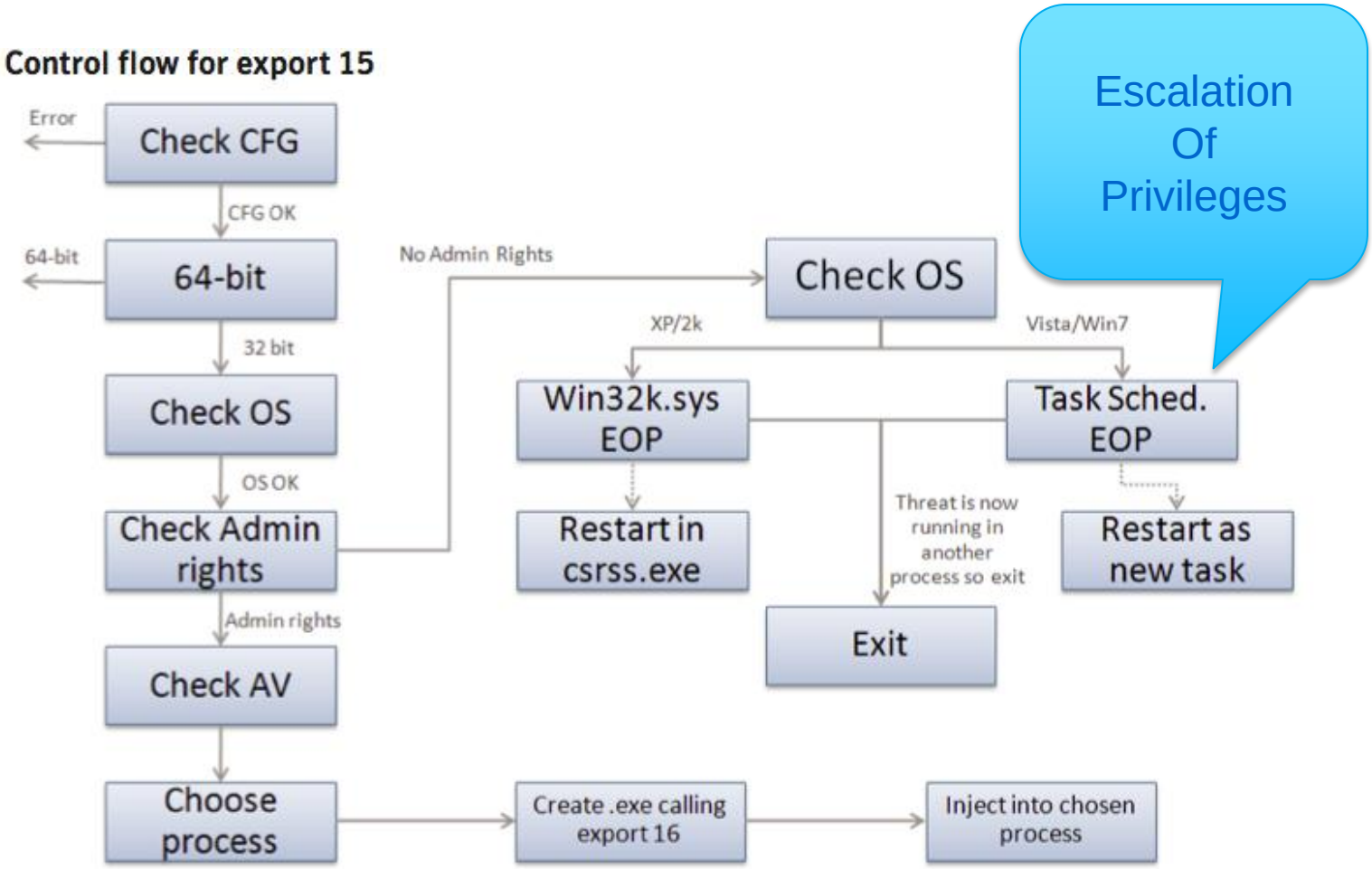
- 20 dll exports
- In the next slide:
  - flowchart of #15
- And this is the "easy part".

Table 2

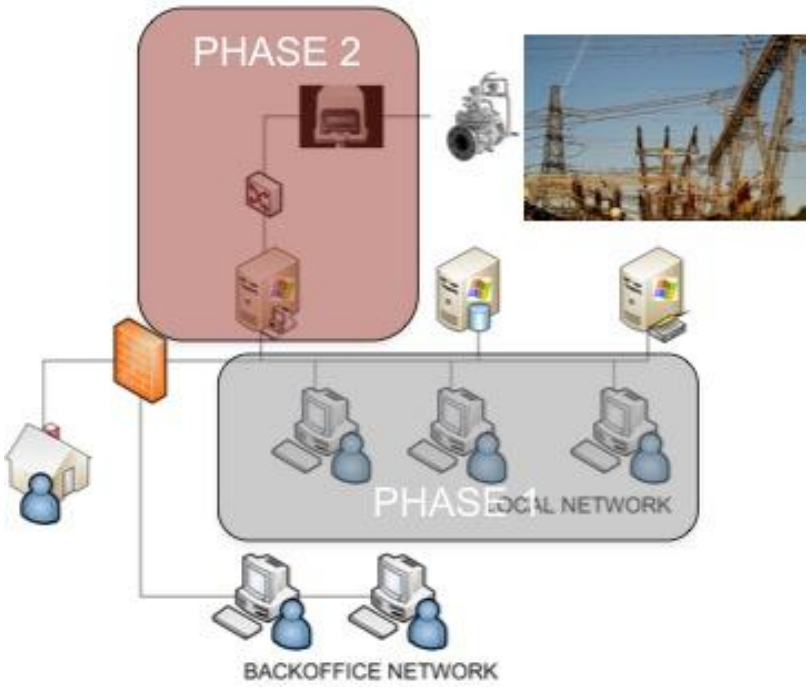
DLL Exports

Export #	Function
1	Infect connected removable drives, starts RPC server
2	Hooks APIs for Step 7 project file infections
4	Calls the removal routine (export 18)
5	Verifies if the threat is installed correctly
6	Verifies version information
7	Calls Export 6
9	Updates itself from infected Step 7 projects
10	Updates itself from infected Step 7 projects
14	Step 7 project file infection routine
15	Initial entry point
16	Main installation
17	Replaces Step 7 DLL
18	Uninstalls Stuxnet
19	Infects removable drives
22	Network propagation routines
24	Check Internet connection
27	RPC Server
28	Command and control routine
29	Command and control routine
31	Updates itself from infected Step 7 projects
32	Same as 1

Phase 1: complexity (part 2)



Phase 2: targeted attack

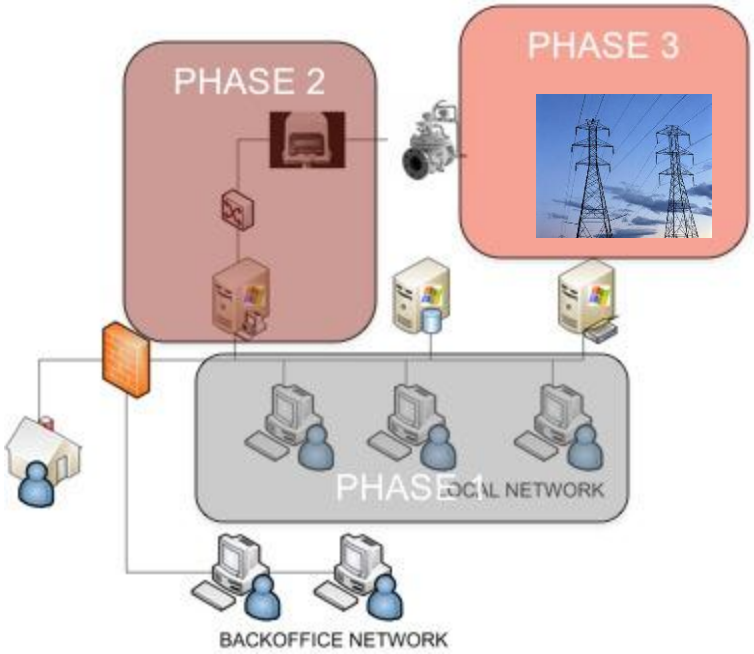


- Looks for systems running
  - WinCC and PCS 7 SCADA MANAGEMENT PROGRAMS
- Finds them even if disconnected (via USB sticks)
- It attacks them, exploiting
  - Hard-wired password (WinCC)
  - Uploads as stored procedure
  - Siemens Project 7 folder vulnerabilities

Phase 2: targeted attacks

- Hooks into specific Step 7 dll to communicate with the PLC
- It replaces the PLC Code
  - Makes a “massive reworking” of the PLC code
- Hides using Rootkit techniques
  - First PLC rootkit EVER
- Very high level PLC code

Phase 3: sabotage

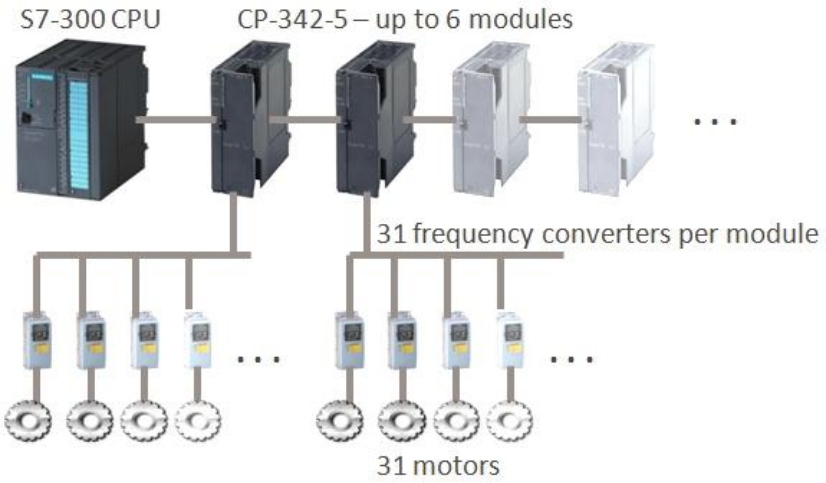


- It checks for a specific configuration.
- If not found: it does nothing
- If found: …

Phase 3: what do we know?

- http://www.symantec.com/connect/blogs/stuxnet-breakthrough

- **Hits frequency converters controlling speed of motors**



- **Stuxnet requires the industrial control system to have frequency converter drives from at least one of two specific vendors, one headquartered in Finland and the other in Tehran, Iran.**

Sabotage

- **Stuxnet requires the frequency converter drives to be operating at very high speeds, between 807 Hz and 1210 Hz. These speeds are used only in a limited number of applications.**

- **Stuxnet changes the output frequencies and thus the speed of the motors for short intervals over periods of months.**

- **The number of possible targets is limited**
- **It is designed to hit a specific plant**

Other features

- **>1.5 MB IN SIZE**
  - **Written in different languages, C, C++**
- **Cost? > 1M$**
- **Symantec (now): 30 people for months/years**
  - **With different expertise**
  - **+ a lab for testing**
  - **+ quality assurance**
    - **….**
  - **+ detailed info on the target system**
  - **+ insiders to steal the certificates**
- **This thing has been tested for months on a duplicate of the target SCADA system!**

About the Target

- **Likely target:**
  - **Natanz Uranium Enrichment Plant.**
  - **60% of the infections were in Iran (Symantec, Aug 2010)**
  - **IRAN acknowledged stuxnet has damaged the nuclear program**
    - **May have delayed the nuclear program**
- **That's why it targeter SIEMENS systems**
  - **The (specific) target plant uses Siemens PLCs**
  - **Could have been any other system**
    - **Siemens is no more vulnerable than other vendors**

Can we believe the media?

Zoekresultaten: stuxnet

Gisteren, 13:02 De hoogte en dieptepunten van 2010 (Podcast) nieuws 3
Deze week in de podcast de hoogte- en dieptepunten van 2010 op beveiligingsgebied. Eigenlijk staan twee...

Gisteren, 11:18 Vernietigde Stuxnet-worm 1000 Iraanse centrifuges? nieuws 2
De Stuxnet-worm heeft mogelijk duizend Iraanse centrifuges bedoeld voor de verrijking van Uranium vernietigd,...

Woensdag, 13:27 Wie heeft de macht op het internet ? forum 4
De laatste tijd is het heel onrustig geweest op het internet. Cybercriminelen hebben steeds...

Maandag, 16:33 Iraanse kernreactor ook doelwit Stuxnet 2 nieuws 8
De ontwikkeling van geavanceerde malware voor het platleggen van Iraanse kernreactoren stopte niet met de...

17-12-2010, 12:46 Stuxnet-worm net zo effectief als militaire aanval nieuws 2
De Stuxnet-worm was in het ontregelen van het Iraanse nucleaire programma net zo effectief als een militaire...

16-12-2010, 10:43 HP opslaghardware bevat backdoor nieuws 12
Eigenaren van een HP StorageWorks P2000 G3 opslagsysteem zijn gewaarschuwd voor een backdoor, waardoor...

15-12-2010, 15:14 "China ontwikkelde Stuxnet-worm" nieuws 5
De Stuxnet-worm die Iraanse kernreactoren ontregelde is niet door de VS of Israël gemaakt, maar door China....

15-12-2010, 12:38 Microsoft dicht 266 lekken in 2010 nieuws 1
Microsoft heeft op de laatste patchdinsdag van 2010 een recordaantal patches in één keer uitgebracht en ook...

13-12-2010, 17:46 "Iran heeft Stuxnet-worm niet onder controle" nieuws 13
Ondanks verklaringen van de Iraanse overheid, heeft het land de besmettingen van twee kernreactoren door de...

10-12-2010, 00:28 Microsoft sluit 2010 af met monsterpatch nieuws 6
Microsoft zal tijdens de laatste patchdinsdag van 2010 zeventien patches uitbrengen voor veertig...

08-12-2010, 10:33 Gevaarlijke rootkit besmet Windows 7 via Stuxnet-lek nieuws
Er is een nieuwe variant van de TDL4 rootkit ontdekt die systemen via het laatste ongepatchte "Stuxnet-lek"...

06-12-2010, 16:12 Arrestaties na aanslag op Iraanse Stuxnet-expert nieuws 6
De Iraanse autoriteiten zeggen dat ze de daders hebben gearresteerd die vorige week de belangrijkste Iraanse...

30-11-2010, 13:39 Autobom doodt Iraanse Stuxnet-expert nieuws 12
De Iraanse expert voor het bestrijden van de Stuxnet-worm is door een autobom om het leven gekomen. Een...

29-11-2010, 17:18 Iran bevestigt Stuxnet-aanval op uraniumverrijking nieuws 8
De Iraanse president Mahmoud Ahmadinejad heeft bevestigd dat de centrifuges voor uraniumverrijking in het...

29-11-2010, 17:11 Iran bevestigt cyberaanval op centrifuges forum
Edit: Nu ook bericht van de redactie: https://secure.security.nl/artikel/35282/1/ Niet echt Security, maar...

28-11-2010, 21:18 "Stuxnet-code niet in handen terroristen" nieuws 4
Afgelopen vrijdag verscheen [illegible] Stuxnetworm op de zwarte markt verkocht werd en...

Remarkable News (Security.nl)

- **12-2010, "China ontwikkelde Stuxnet-worm"**
  - **De Stuxnet-worm die Iraanse kernreactoren ontregelde is niet door de VS of Israël gemaakt, maar door China…**
- **12-2010, Arrestaties na aanslag op Iraanse Stuxnet-expert**
  - **De Iraanse minister Heidar Moslehi beweerde dat de Mossad, CIA en MI6 een rol bij de aanvallen op de Iraanse wetenschappers speelden**
- **30-11-2010, Autobom doodt Iraanse Stuxnet-expert**
  - **De Iraanse expert voor het bestrijden van de Stuxnet-worm is door een autobom om het leven gekomen. Een…**
- **29-11-2010, Iran bevestigt Stuxnet-aanval op uraniumverrijking**
  - **De Iraanse president Mahmoud Ahmadinejad heeft bevestigd dat de centrifuges voor uraniumverrijking in het...**
- **23-11-2010, Greenpeace achter Stuxnet-worm?**
  - **In bijna alle berichten en discussies over de Stuxnet-worm wordt er vanuit gegaan dat de malware een Iraanse...**
- **17-11-2010, "13% slachtoffers Stuxnet-worm in Nederland"**

Countermeasures?

- **Possibilities**
  - **Antivirus**
  - **Intrusion Detection**
  - **Whitelisting**

Antivirus

- **Work in theory, but not against something this elaborate.**

- **Stuxnet was devised to**
  - **Be invisible to signature-based systems**
  - **Avoid detection by behavior-based antivirus.**
    - **It stopped when it encountered an antivirus that could detect it.**
  - **And was thoroughly tested in the lab**

- **Reputation-based mechanisms should work in in theory**
  - **But need a sufficiently large number of peers**
  - **And an Internet connection for updates is needed**
  - **“Local” reputation-based will probably not work**
    - **SCADA systems are too heterogeneous (and not as many as “regular” clients)**

White-listing

- **“Not-so-common” technique in critical infrastructure, some hope.**
- **Most solutions available today might have blocked the execution through LNK and autorun**
  - **However, to allows flexibility for users, monitoring software is usually instructed to allow certain processes and users to execute any operations**
  - **The user SYSTEM is likely one of them**
- **Usability problem.**
- **Several solutions check also for DLL hijacking**
  - **Same limitations about usability apply**

Intrusion Detection?

- **Signature-based: hopeless**
  - **(should have detected the Conficker-like exploitation)**
  - **Basically hopeless in this situation (but extremely useful once the worm has bee identified)**

- **Signature-less: some hope**
  - **should have detected the network horizontal scan for the vulnerable services**
  - **possibly the P2P-like communication too, although it was carried on over standard RPC (common in SCADA)**

Is there hope? (a personal view)

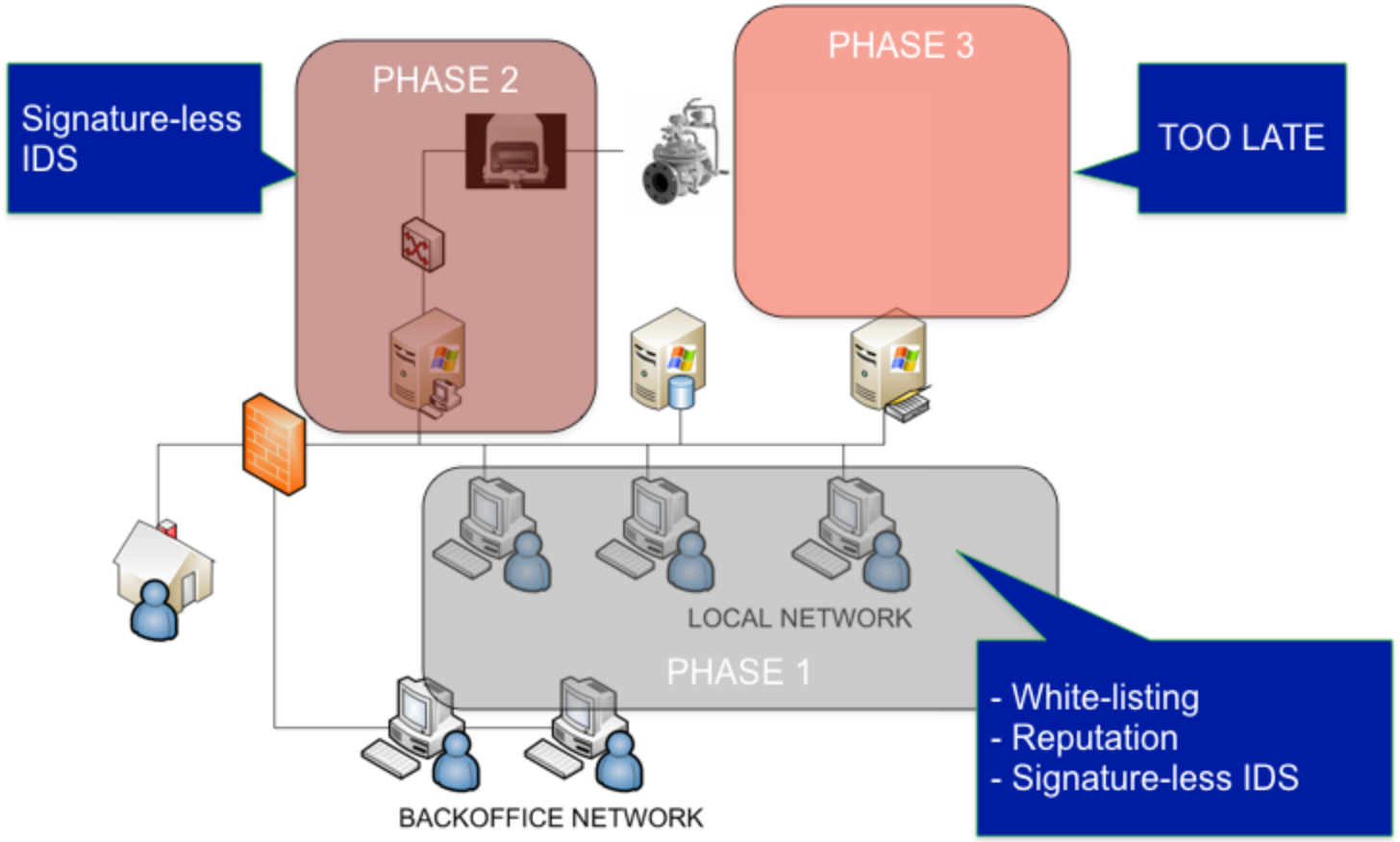
- **Enhanced signature-less intrusion detection**
  - **Combine protocol-awareness and anomaly detection**
  - **Payload-based**
  - **Detection models are tailored to the local traffic**

    Support basic data types and binary/complex data

- **Each network communication is validated**
  - **Syntactically, by the protocol parser**
  - **Semantically, by the anomaly detection engine**

- **We (UTwente + SecurityMatters) are developing a specific detection system for this kind of systems.**

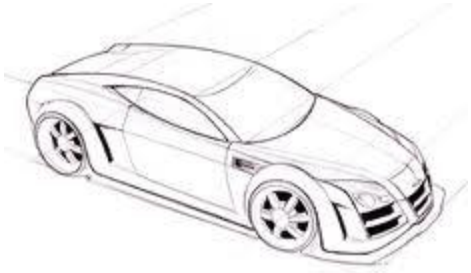
Possible countermeasures: a summary



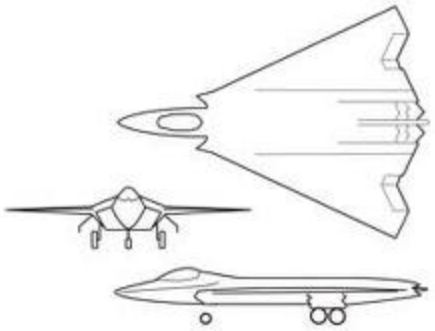
QUESTIONS?

- **Regular**

- **Elaborate**



- **Stuxnet**



Sources

- [F-SEC] F-secure
  - http://www.f-secure.com/weblog/archives/00002040.html
- [Kas] Kasperski labs
  - http://www.securelist.com/en/blog/325/Myrtus_and_Guava_the_epidemic_the_trends_the_numbers
- [Sym] Symantec. W32 Stuxnet Dossier
  - Version 1.0, September 2010
- http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_?taxonomyId=85&pageNumber=

Where?