The Stuxnet Worm; Retrospective and Future Scenarios

AF Security Seminar, UiO

Geir Mork, Norman ASA

About the presenter

- Principal Software Strategist in Norman
  - Network security as main working area
- Total 8 years with Norman, different positions within R&D
- About 20 years within network and information security

About Norman

- Established 1984
- Anti-malware since 1989
- Short interesting facts:

About Norman

- Established 1984
- Anti-malware since 1989
- Short interesting facts:
  - 1990: Approx. 59 known malware

About Norman

- Established 1984
- Anti-malware since 1989
- Short interesting facts:
  - 1990: Approx. 59 known malware
  - 2011: Approx. +45 million known malware

Agenda

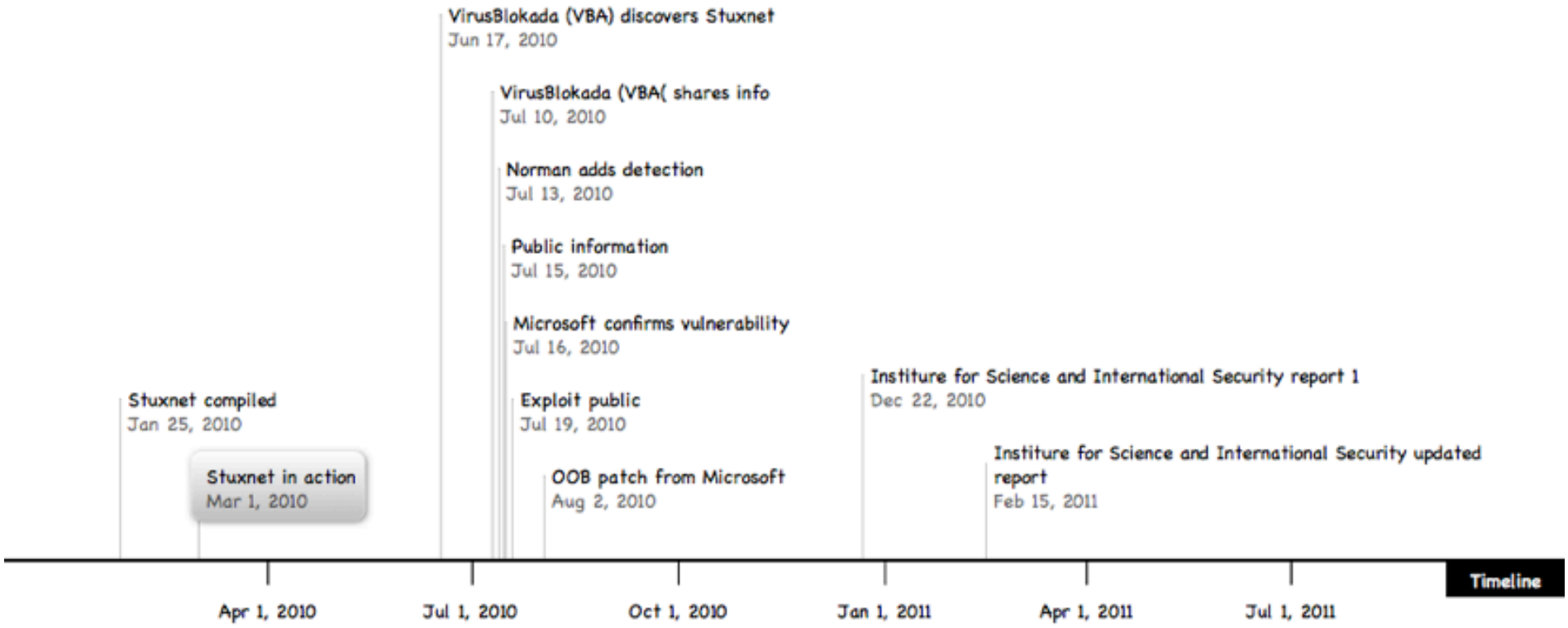
- Stuxnet - what really happened?
  - ⋆ Retrospective
  - ⋆ Consequences
    - Other known security incidents
- Future scenarios
- Discussion

Stuxnet - short facts

- First observert by VirusBlokada in June 2010
- Most complex and sophisticated malware ever seen
- Attempts to exploit several vulnerabilities in Windows
  - Most were unknown by Microsoft
- Used valid certificates for root kit drivers
- Custom made for Siemens SCADA systems

- Challenge for malware writers: Target is closed and isolated networks

Stuxnet - timeline



Stuxnet components

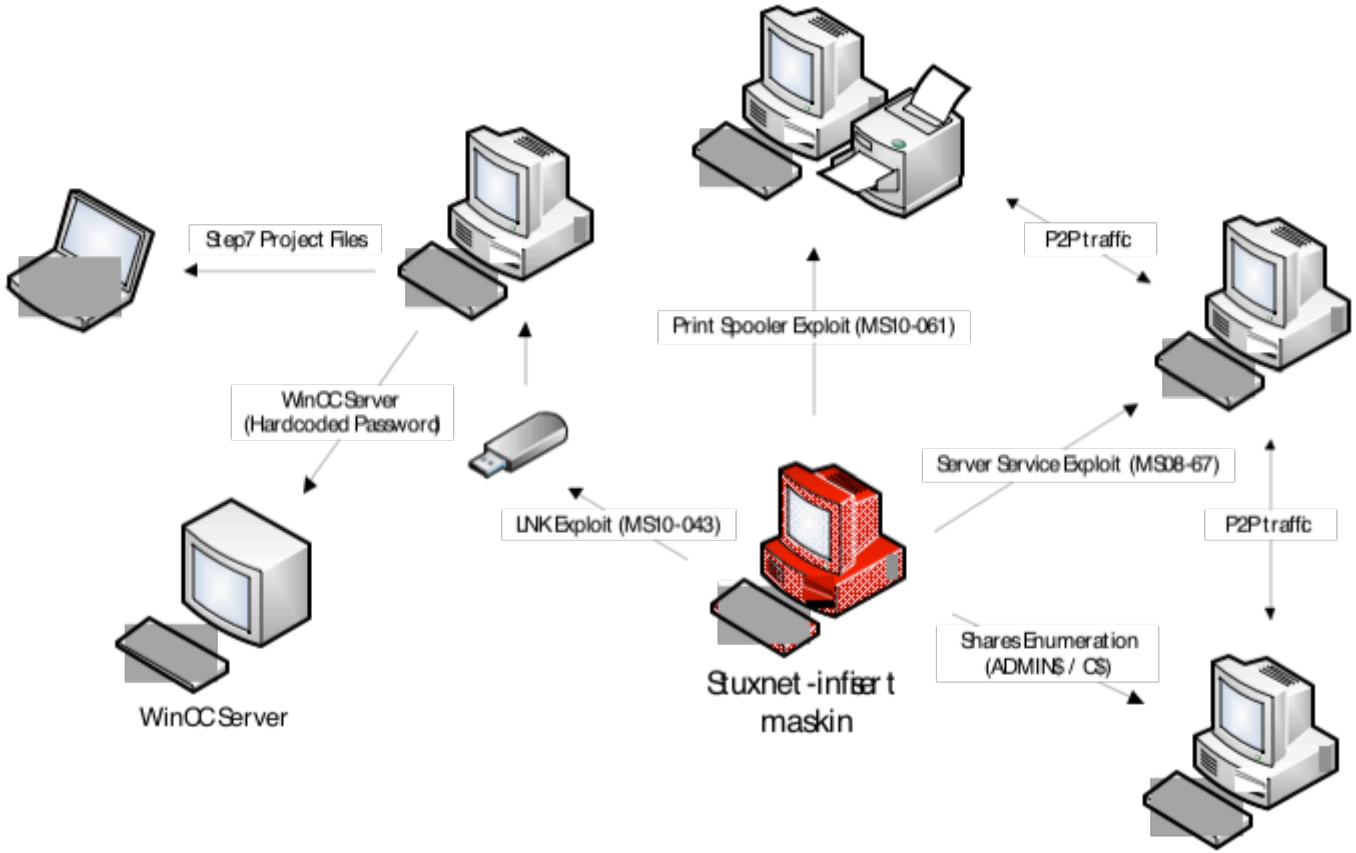
- Stuxnet was made up of several components that was used as needed

  ✓ Spreading vectors / exploits
  ✓ Peer-to-peer communication (in LAN)
  ✓ Windows rootkit
  ✓ PLC rootkit (SCADA)
  ✓ Command and control interface

Spreading mechanisms / proliferation

- Stuxnet attempts to spread through the following methods and vulnerabilities:
  - ✓ Through storage media (USB) (MS10-046)
  - ✓ Exploit of print spooler vulnerability (MS10-061)
  - ✓ Exploit of server service vulnerability (MS08-067)
  - ✓ Copying to Windows shares
  - ✓ Compromising of Siemens WinCC databases
  - ✓ Injection in Siemens Step7 project files
  - ✓ Update through own P2P client/server application through RPC

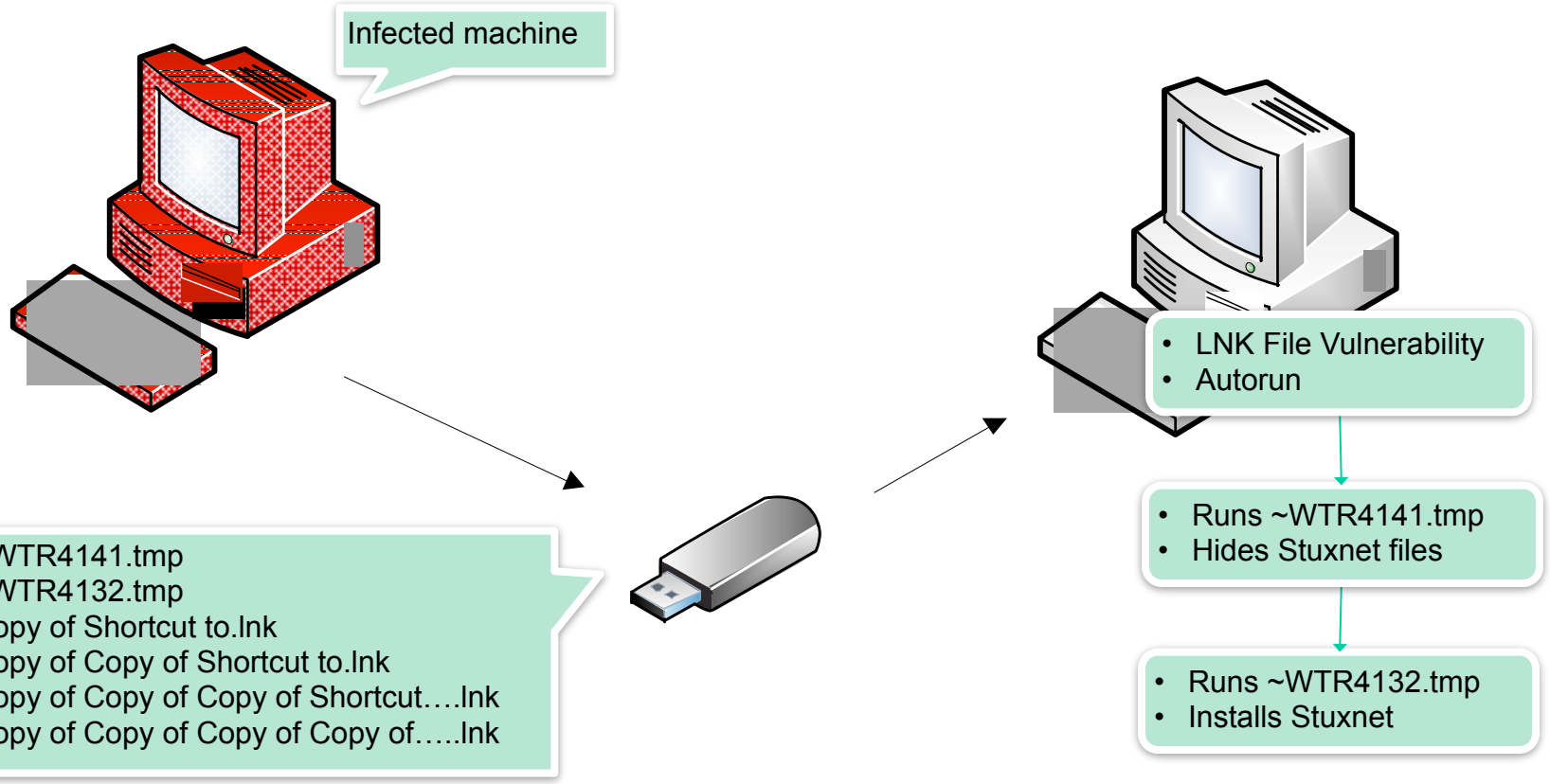
Spreading/proliferation mechanisms



Spreading through USB storage media (1)

- Most important spreading vector used by Stuxnet
  - Used to infiltrate closed networks (ICS/SCADA)
- Stuxnet copies itself to USB storage
  - Creates the files ~WTR4132.tmp and ~WTR4141.tmp
- Attempts to execute these when USB storage is inserted to other systems
  - Attempts to exploit the LNK vulnerability (CVE-2010-2568)

Spreading through USB storage media (2)

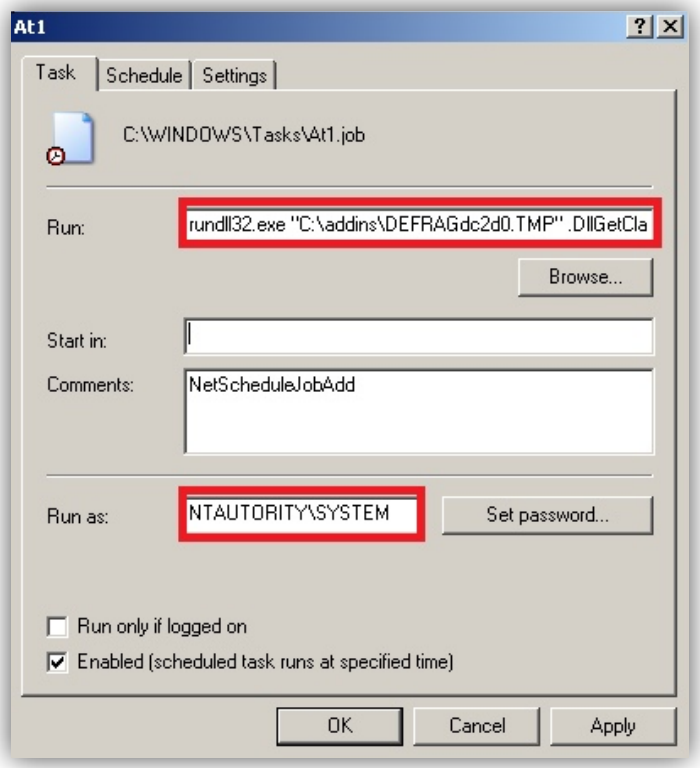


CVE-2010-2568 (LNK File Vulnerability)

- Allows loading of arbitrary DLL through specially crafted Windows shortcuts, or .LNK files
  - The DLL-file can reside on a USB stick or on a remote share (WebDAV)
- Erroneous handling of resource files in the Control Panel icon.
- Typical example of a design flaw
  - Often takes time to correct
- Fixed in MS10-046 (Aug 2010)

Proliferation through Windows Shares

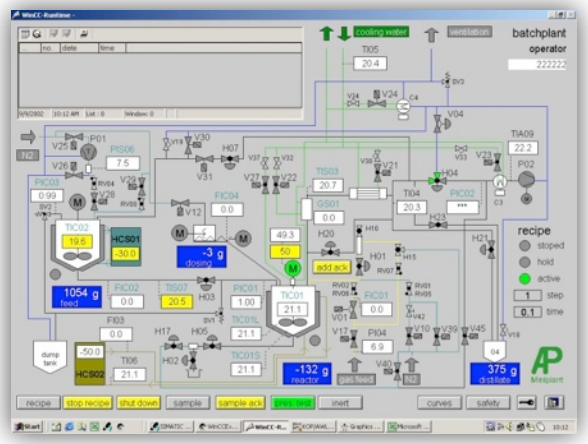
- Stuxnet enumerates servers and shared resources in the local network
  - Attempts to access ADMIN$ and C$ by using the local logged in user
  - Copies main module to the shared resource
  - Creates a remote scheduled task via *NetScheduleJobAdd* to execute the module
  - Attempts to use WMI also

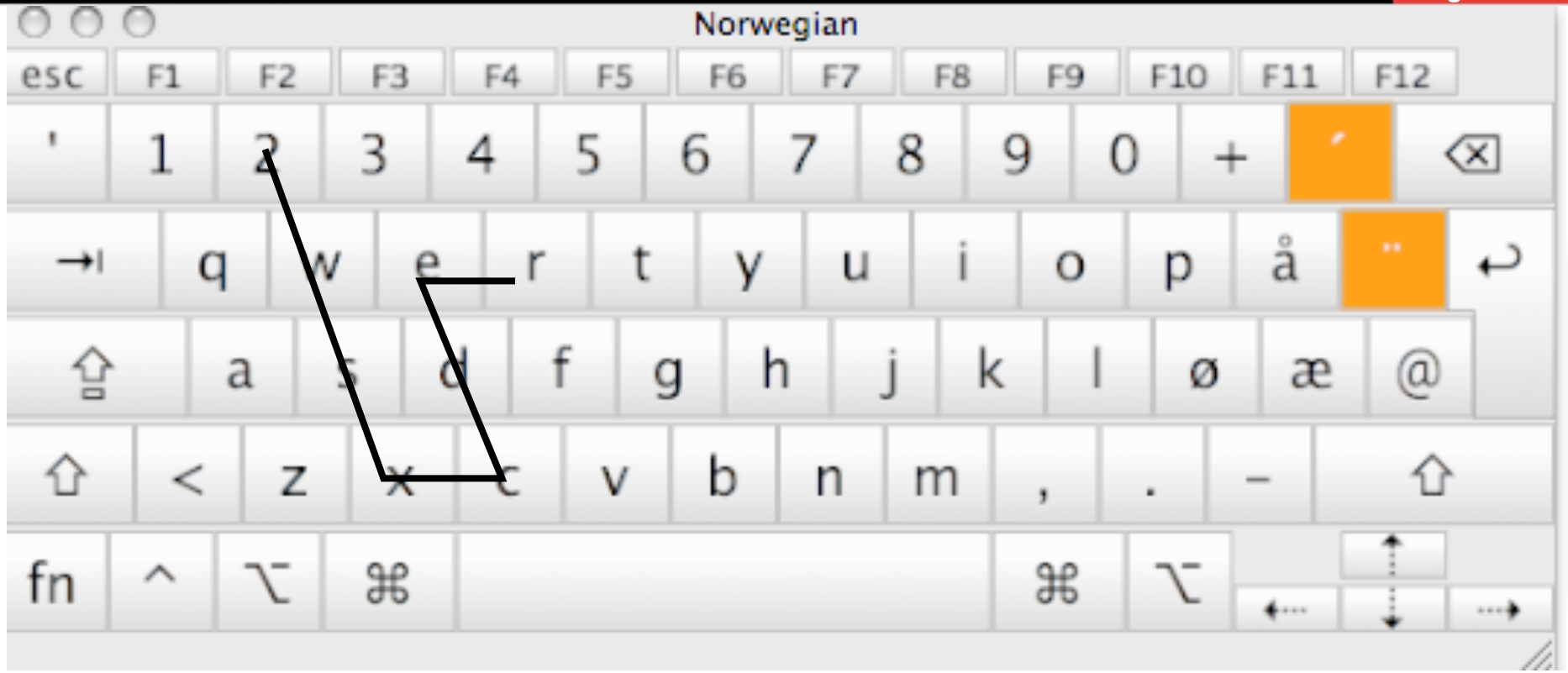


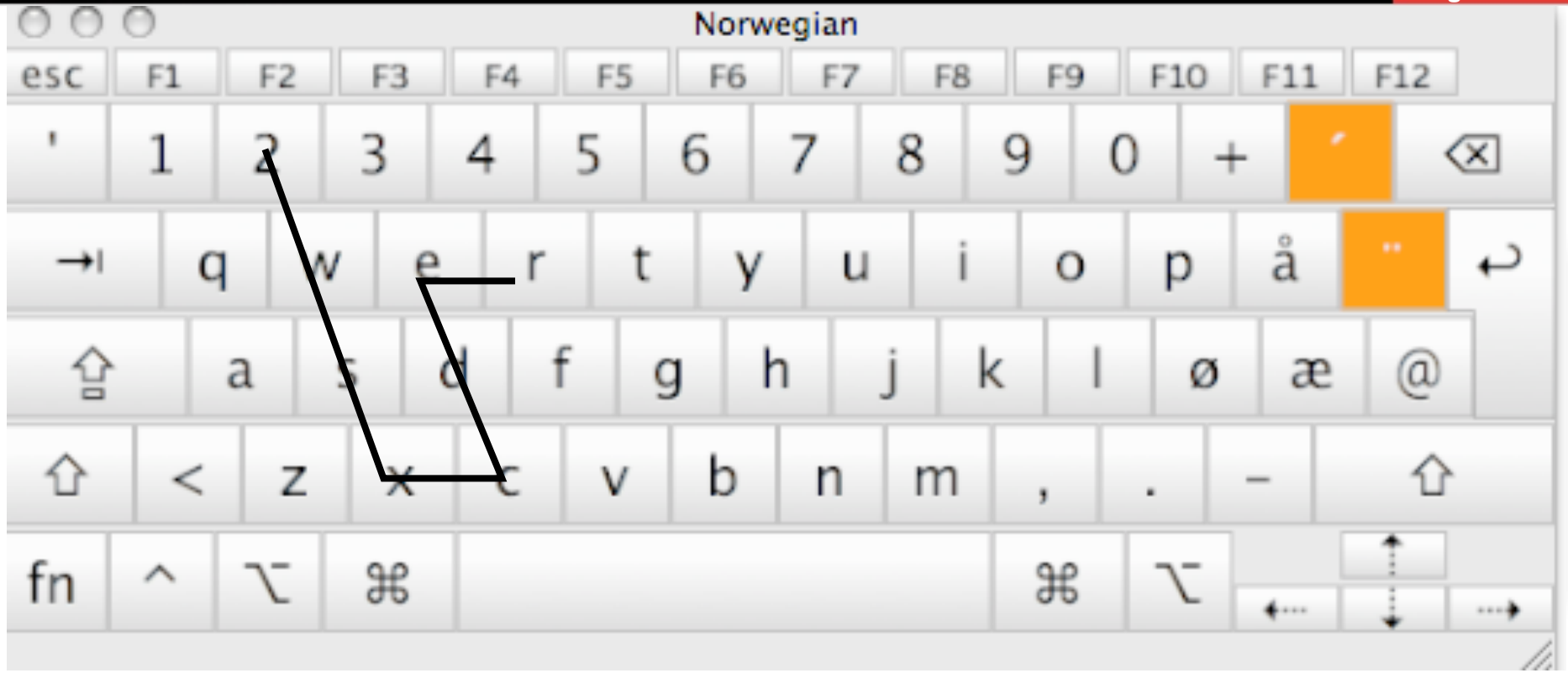
Credit: Stuxnet Under the Microscope (ESET)

Spreading through WinCC

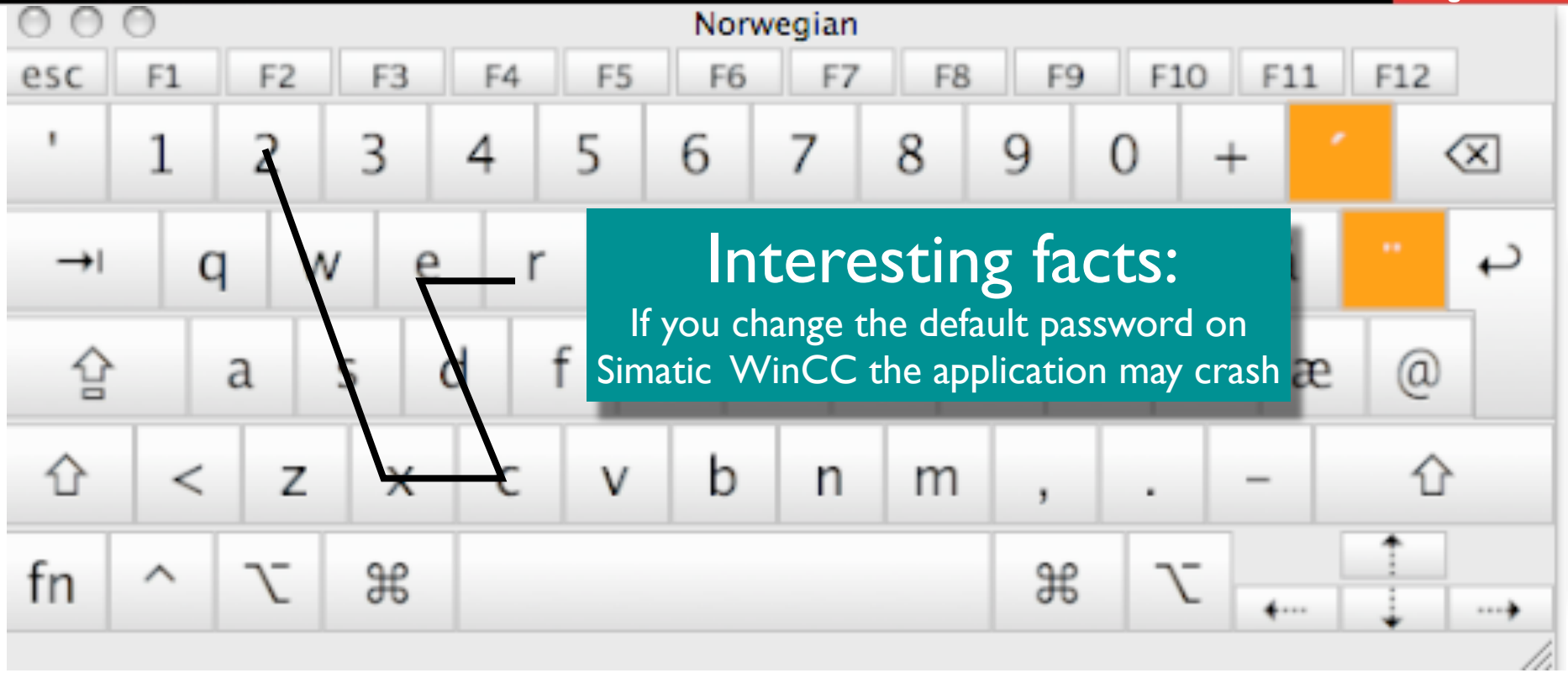
- Stuxnet attempts to log in to the SIMATIC WinCC servers by using the application´s hardcoded password
  - Sends SQL queries that allow transfer and execution of the Stuxnet module.




Norwegian
esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12
' 1 2 3 4 5 6 7 8 9 0 + ´
q w e r t y u i o p å ¨
a s d f g h j k l ø æ @
< z x c v b n m , . -
fn ^ ⌥ ⌘ ⌘ ⌥



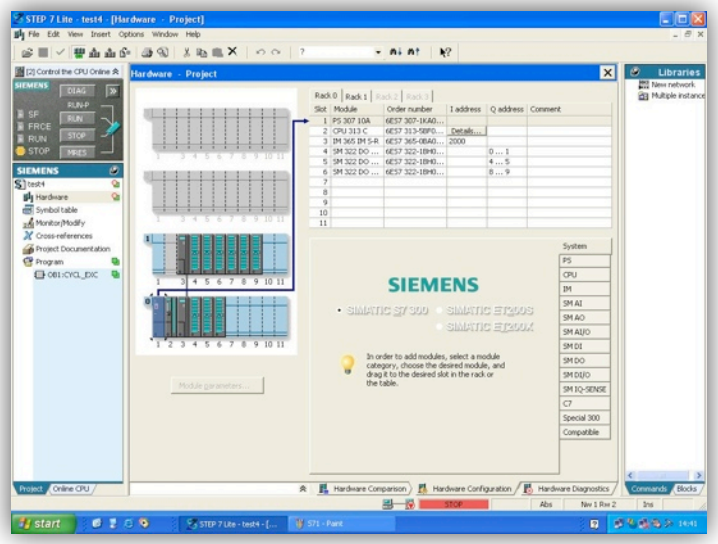
– "Server=.\WinCC; uid=WinCCConnect;pwd=2WSXcder"



– "Server=.\WinCC; uid=WinCCConnect;pwd=2WSXcder"

Spreading through Step7 projects

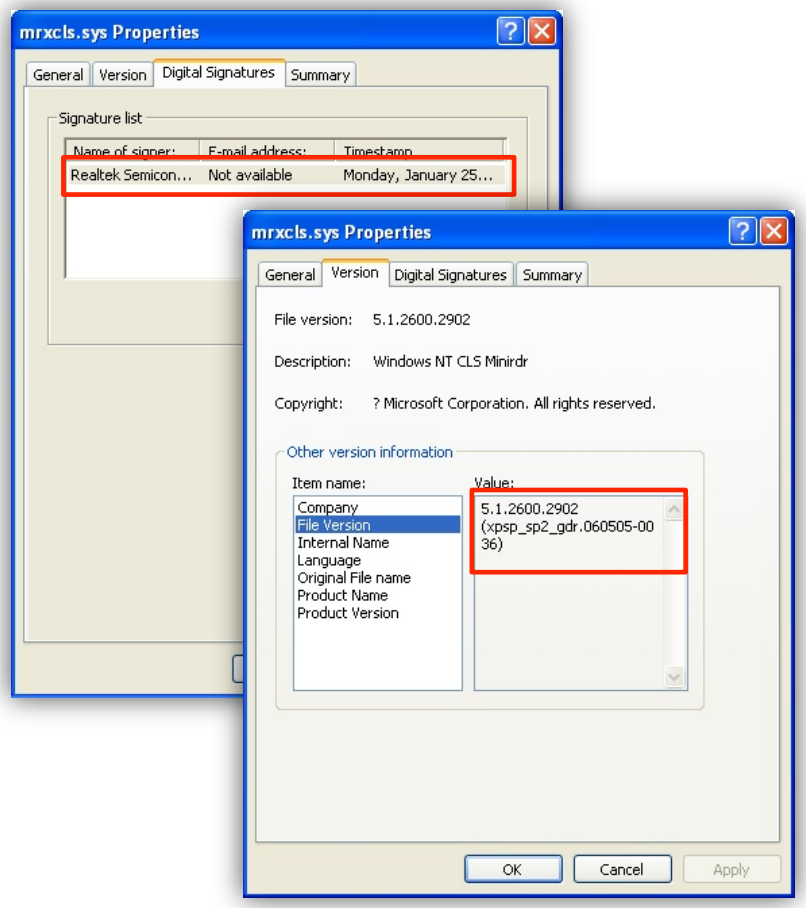
- Stuxnet attempts to “infect” Step7 project-files
  - .S7P og .MCP
- Uses DLL LoadLibrary injection («binary planting»)
  - Copies Stuxnet module to all folders with Step7 projects
  - Same filename as legitimate application module
  - When these load the application can attempt to load the DLL file in the folder

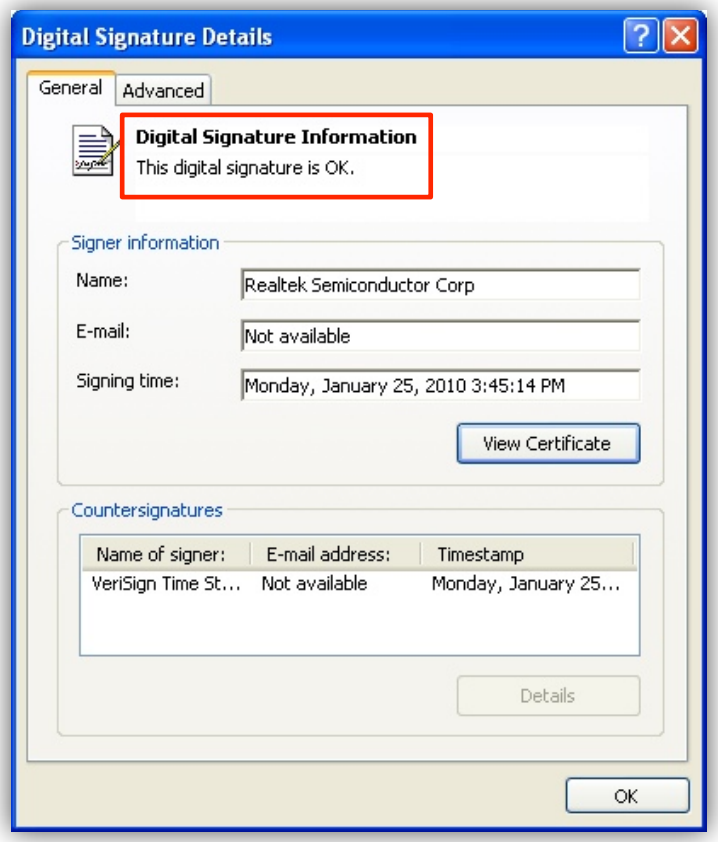


Spreading through Peer-to-Peer updates (1)

- Stuxnet can update already infected hosts within a local network through its own peer-to-peer protocol
  - Communicates over RPC
- Infected hosts can act as both server and client
  - Can ask or send info about updated versions of Stuxnet
- Used to stay in control of amchines that can't communicate with the outside world

Rootkit drivers signed with Realtek certificates





So how does it work, what does it do?

Stuxnet doesn't activate its payload before the "correct" equipment is available:

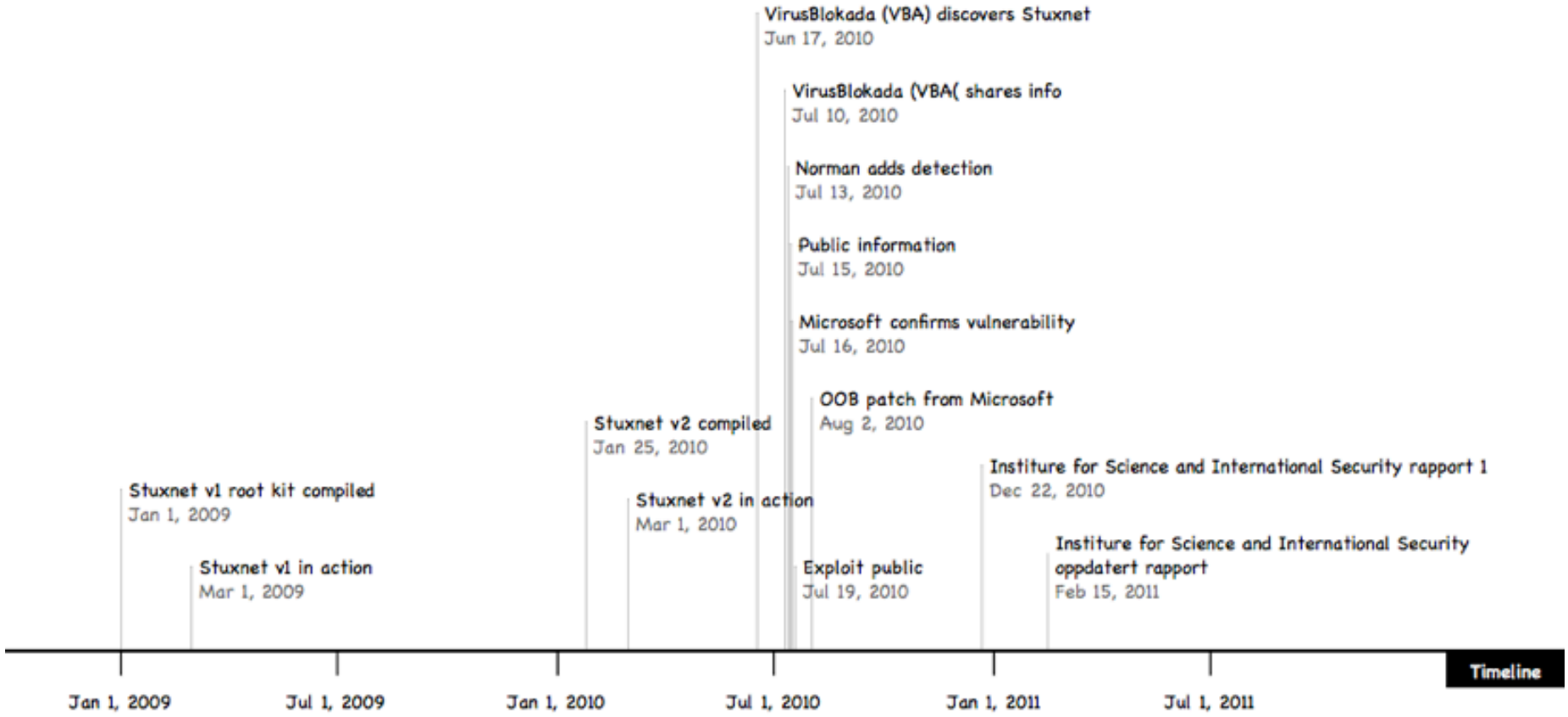
- When Stuxnet has infected a computer it will look for PLC's of the type S7-315 and S7-417 using specific CPU's of type 6ES7-315-2x and 6ES7-417x
- It will the replace the Step 7 DLL to filtrate and block data
- Data to/from the PLC will be filtrated so operators can not discover the infection, and Stuxnet can add the destructive code to the existing PLC code

So how does it work, what does it do?

- From forensic evidence it's believed that Stuxnet tried to manipulate or/and destroy special turbines used by the Fuel Enrichment Plant (FEP) at Natanz.

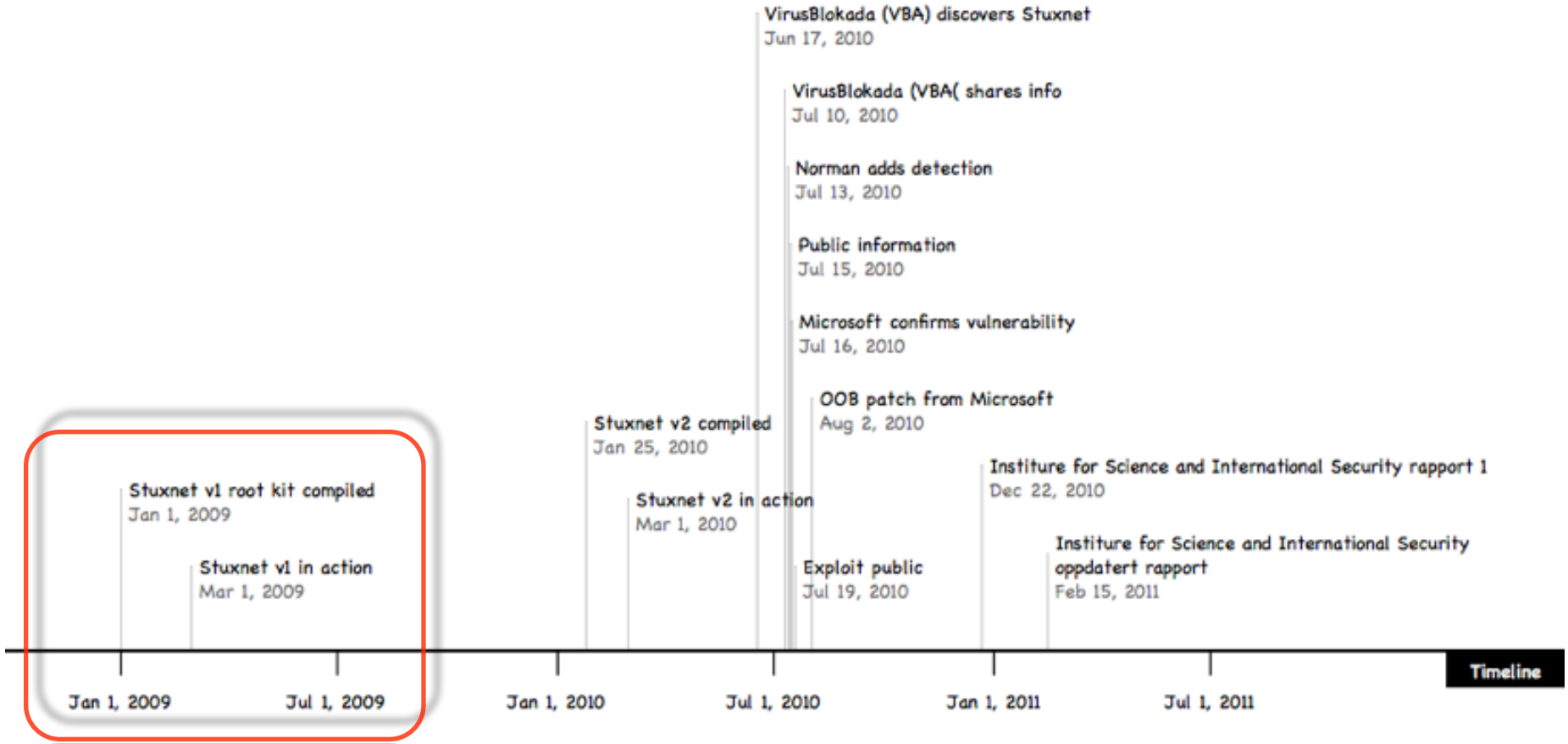
So what really happened?

- Remember the timeline? It's not entirely correct..



So what really happened?

- Remember the timeline? It's not entirely correct..



So what really happened? (2)

- The facility in Natanz was most probably hit already in late 2009 or early 2010, destroying about 1000 IR-1 centrifuges of about 9000 deployed at the site
- Part of the code uses Profibus to communicate with frequency converters from both Vacom from Finland and Fararo Paya from Iran
- Iranians did not understand what caused this at the time
- The code for S7-417 PLCs seems not to be finished and would probably not run as intended

So what really happened? (3)

- The world´s most advanced publicly known targeted attack
- So who wrote this extremely complex code?
  - Speculators point to military intelligence branches in US and Israel
- At least we know that writing Stuxnet require thorough knowledge of several different disciplines and we believe that a team of 10-15 people were involved
- Required a lot of funding

What was the consequences of Stuxnet?

- Delay in Iran´s nuclear program

Consequences of other attacks/mishaps

Nuclear reactor (US, name not disclosed)

- Reactor network slows down and the security and monitoring systems stay off-line for almost 5 hours.
- Cause: Malware infected systems through a consulting company's private T1 line that circumvented the network firewall
- Cost: $600.000

Australian Railway

- 300.000 commuters in greater Sydney area without transportation an entire day
- Cause: Malware compromises the signal and control systems
- Cost: Unknown, but estimated in the millions

Daimler Chrysler (US)

- 13 production plants shut down for over 1 hour. Up to 50.000 workers without anything to do..
- Cause: Malware compromised un-patched Windows 2000 systems
- Cost: $14 mill. (estimated)

What to expect in the Future?

- Trend is that targeted attacks increase compared to “common unique” malware
- What constitutes a successful targeted attack?
  - No publicity, under the radar
  - Victim not aware of compromised or lost information

- APT (Advanced Persistent Threat) will increase
  - State or organization endorsed or supported cyber attacks may increase
- “Hacktivism” may gain even more momentum
  - Polarization of cultures and politics add fuel to activists
  - The “Anonymous” group is a good example

What to expect in the Future?

- We will see that military conflicts will involve more digital warfare as part of states weapon arsenal

- **Stuxnet is a pioneer and "role model" of how to attack physical installations like power plants, nuclear reactors etc.**

References

- ESET – Stuxnet Under the Microscope
  - http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
- Symantec – W32.Stuxnet Dossier
  - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- Norman – W32/Stuxnet
- Norman - Teknisk gjennomgang av Stuxnet
- ISIS - Stuxnet Malware and Natantz (updated report from Feb 15th)
  - http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/