SIEMENS

Stuxnet Malware

Official communication

presented at SANS SCADA Summit 12-10-2010

by Thomas Brandstetter

Stuxnet Malware

What is the Stuxnet and what can it do?

SIEMENS

Stuxnet is a high sophisticated malware that targets very specific configurations

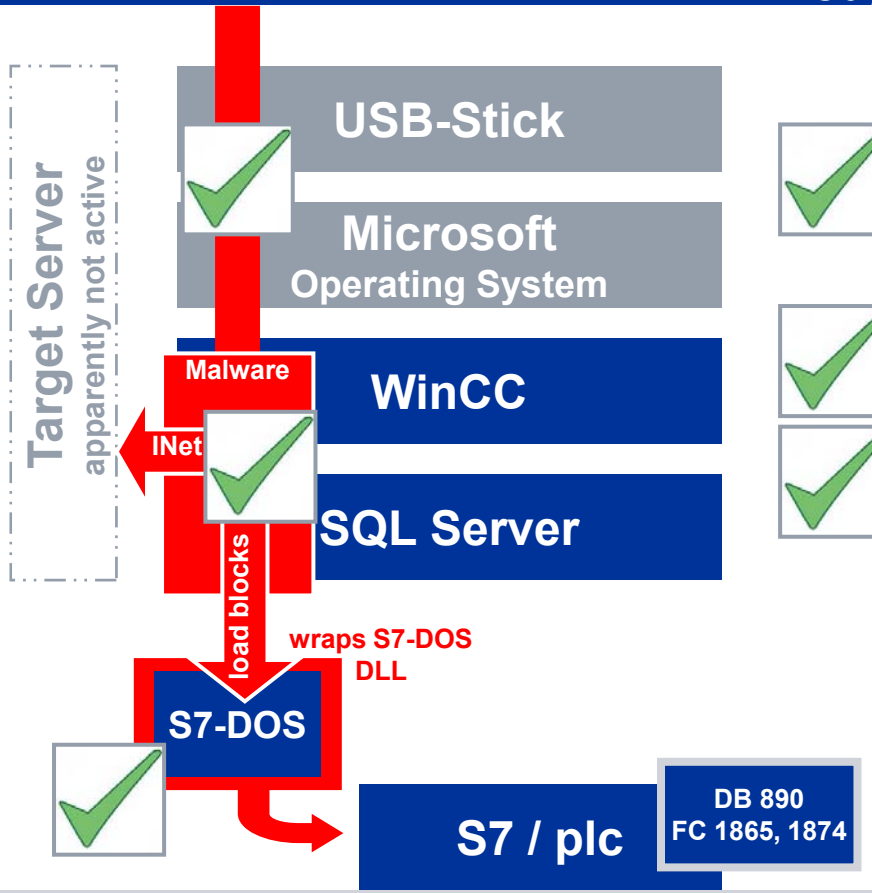
Affected system types	**Stuxnet could infect systems with** **• Windows operation systems (Windows XP and higher)** **• SIMATIC automation software WinCC SCADA or PCS 7 and S7-plc** **→ No damage to production or failed processes known so far** **→ Up-to-date virus scanner reliably detect and eliminate the malware** **→ Malware has been removed in all infected systems known to Siemens**
Highly sophisticated	**The highly sophisticated malware Stuxnet was probably developed by a "team of experts", because of the required knowhow about IT, industrial controllers, engineering skills and details about a specific project configuration**
Specific plant configuration	**Stuxnet requires a very specific environment (certain plc blocks):** **• Under certain conditions, it might influence the processing of operations** **• But: The behaviour has not yet been verified in test environments or real plants**
Malware outside communication	**Potentially transfers data into and out of the system – but this has not yet been proven, especially as the target servers are down and not reachable**

Stuxnet Malware

How will it affect a plant or system?

SIEMENS

Malware gets into the system via various Microsoft vulnerabilities (now fixed)



- Infection via USB / network / printer spooler
  → fixed by Microsoft Patch
- SIMATIC Security Update Tool
- SYSCLEAN Tool removes malware from infected machines

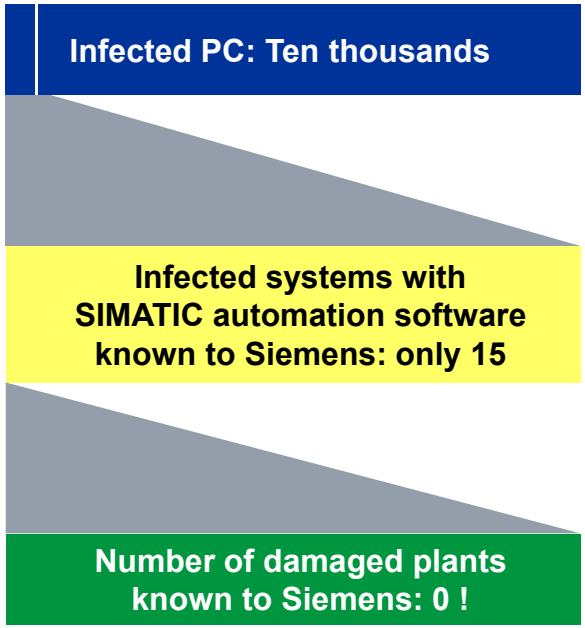
If the blocks are already present, the malware does not infiltrate the plc

Stuxnet Malware

Why is Siemens target of this malware?

SIEMENS

Malware targets specific plant configuration



- Ten thousands of PC are infected, but
- Only a very small percentage is part of an automation environment
  → that explains the low number of known infected automation environments
- Malware is obviously **targetting a specific process or project** and not a particular brand or process technology
- All known infected systems
  - ☑ have been cleaned
  - ☑ malware was not activated
- **Future infections unlikely** because malware pattern is being detected by up-to-date virus scanners.

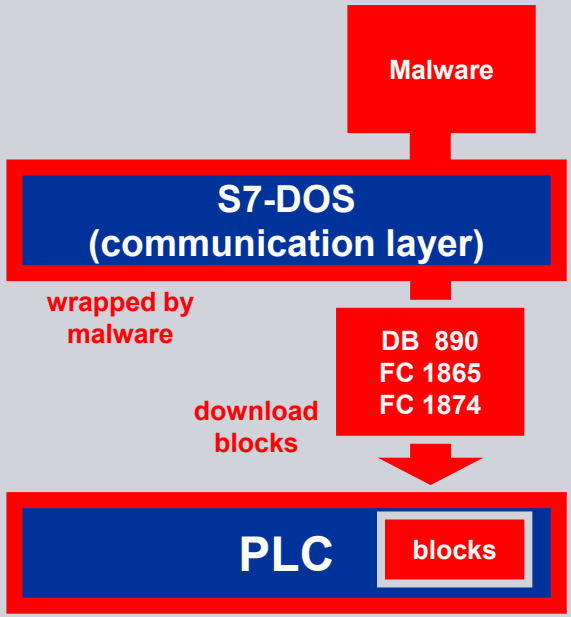
Stuxnet Malware

How are my SIMATIC S7 controllers affected?

SIEMENS

Malware tries to download trojan plc code blocks

WinCC



Details

- Malware carries own block (DB 890, FC 1865, FC 1874) and checks whether they are available in the target plc. If they already available, the malware does nothing
- If the blocks are not available, the malware downloads this blocks to the plc and links them into the program sequence
- If you identify those blocks in your plc but did not have them before in your project, Siemens urgently recommends restoring the plant control system to its original state.

Stuxnet Malware

What has Siemens done to reduce the risk to plants?

SIEMENS

Many joint activities and results since first appearance of malware

but the white paper security concept is already available since years!

2008 | 2010

July | August | September | October

April 2008 → White Paper Security Concept

15th july

- **Established expert team**
- **Test environment** → Isolation of malware

19th july

- First communication to internals and customers (**Siemens Advisory Site**)

22nd july

- **Description + Tool** Detect + Remove malware w/o influence to plant operation

Infected: 4 / Damaged: 0

2nd August

- **Microsoft patch** closed operating system security breach to avoid further infiltrations

4th August

- **Update of description** of how to identify and remove the malware

18th August

- **Security Update (Tool)**

Infected: 12 / Damaged: 0

7nd September

- 15 infected systems 5 of them in germany

17th September

- Communicated: Malware might affect only specific configurations
- Targeted plc blocks: DB890, FC1865,1874

30nd September

- 12.000 downloads of security tool

Infected: 15 / Damaged: 0

Begin of october

- Information to the regions (slide set, letter template)

Infected: 15 / Damaged: 0

Security concept , Customer Support

Stuxnet came up | Major steps | Updates | Today

Stuxnet Malware

What has Siemens done against Stuxnet

SIEMENS

Siemens is dealing very seriously with this issue

Internal

- Since years Siemens runs a **security lab** as part of system test
- **Established technical team** of experts
  - Isolation of malware
  - Forcing activation of malware
- Joint activities with **Siemens CERT**
- **Informed regional and head quarters** sales force via webinars, newsletter, mails, phone,)
- Close Attention of Top Management

Has also the customer done all he can?

External

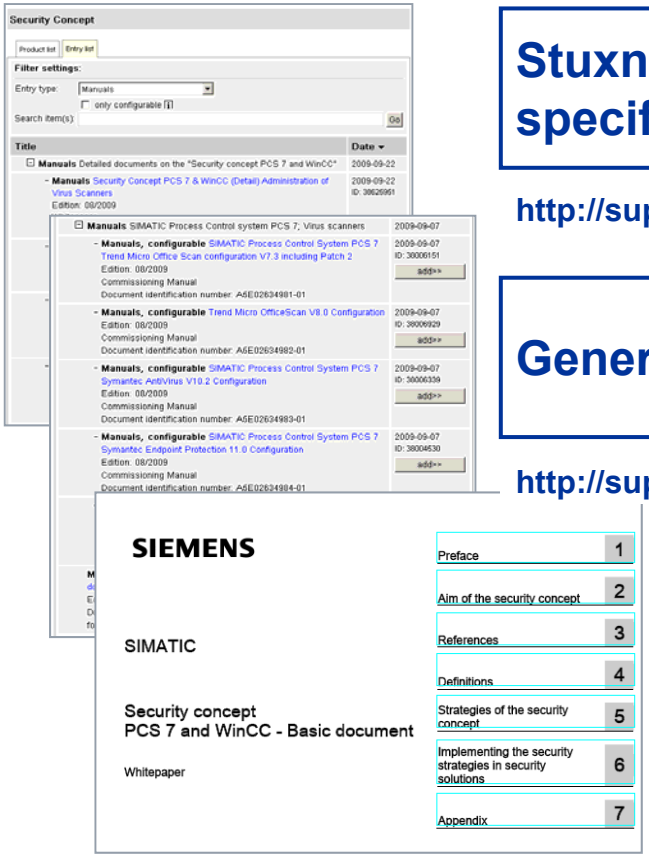
- **Siemens Advisory Site**
- **Security White Paper** for PCS 7 and WinCC available since years
- Used connections to **Microsoft** to get a „out-of-band patch“
- Joint activities with **Anti-Virus-Tool suppliers**: Symantec,TrendMicro,McAfee
- **Pro-Active communication** from the very beginning related to malware
- **Interview** with magazines
- **Informed** all known **infected projects pro-actively** about updates

Stuxnet Malware

Will this happen again in the future?

SIEMENS

You can rise the security barrier, but not to 100%



Stuxnet specific

- Siemens Advisory Site
- Contact Support
- Security Tool to clean infected PC

http://support.automation.siemens.com/WW/view/en/38616083/133300

General

Siemens offers a comprehensive White Paper / Security Concept for PCS 7 and WinCC

http://support.automation.siemens.com/WW/view/en/26462131

Future infections unlikely because malware pattern is being detected by up-to-date virus scanners, but:

Security is a joint continuous activity of system suppliers and customers

SIEMENS

Thank you for your attention!

Siemens AG

Gleiwitzer Str. 555
90475 Nuremberg

Speaker contact:
Thomas Brandstetter
Program Manager Hack-Proof Products
Siemens CERT
thomas.brandstetter@siemens.com