

Stuxnet Malware

Official communication

presented at CIP Seminar 02-11-2010

by Thomas Brandstetter

Stuxnet Malware



What is the Stuxnet and what can it do?

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

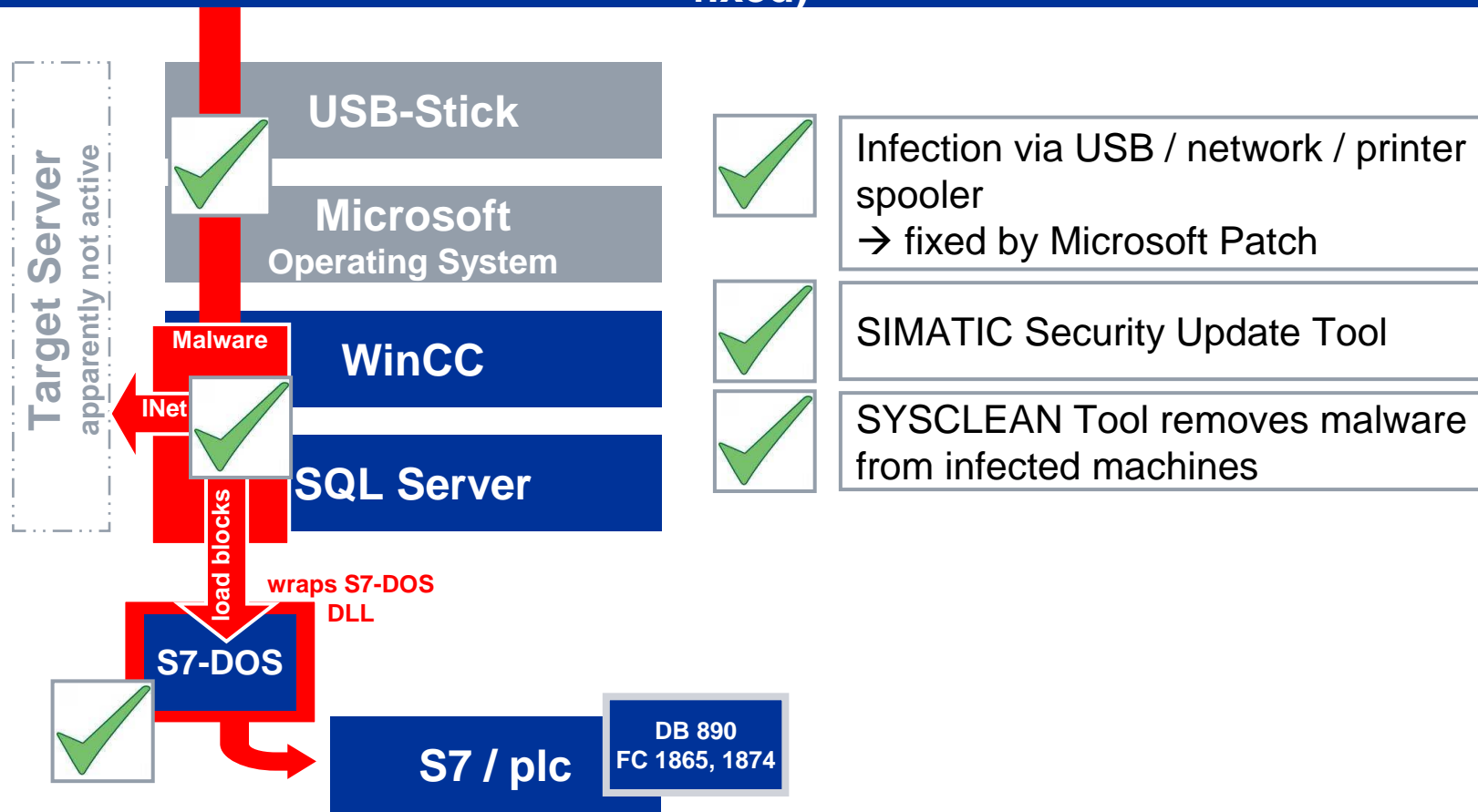
Potentially transfers data into and out of the system – but this has not yet been proven, especially as the target servers are down and not reachable

Stuxnet Malware

How will it affect a plant or system?



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



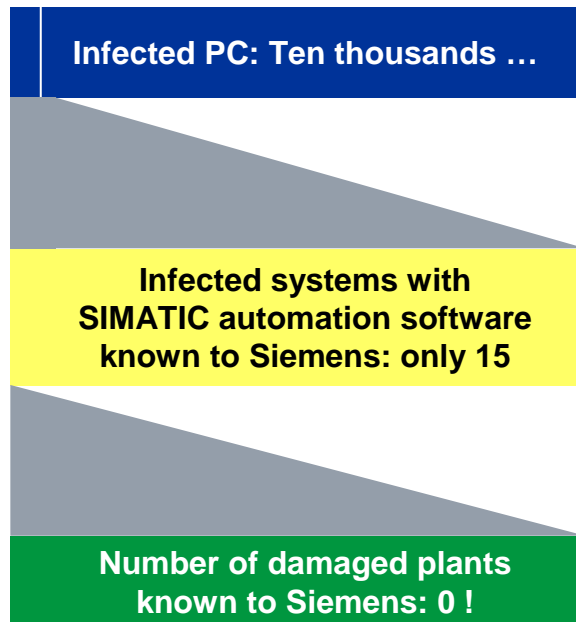
© Siemens AG 2010. All Rights Reserved.

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

Stuxnet Malware

Why is Siemens target of this malware?

Malware targets specific plant configuration



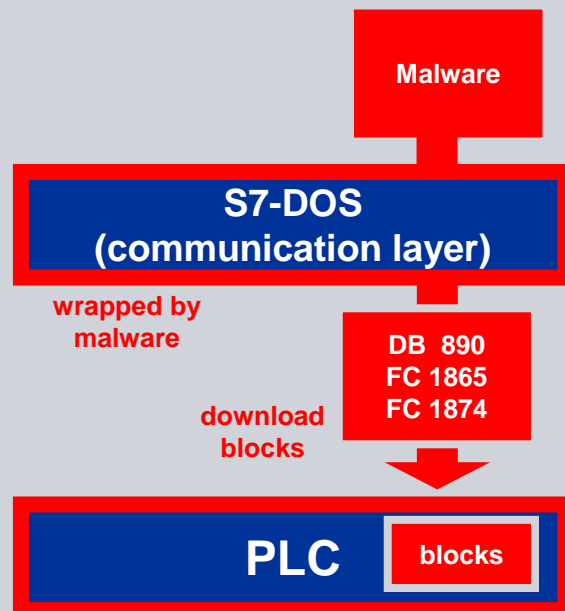
- Ten thousands of PC are infected, but ...
- Only a very small percentage is part of an automation environment
→ that explains the low number of known infected automation environments
- Malware is obviously **targetting a specific process or project** and not a particular brand or process technology
- 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?

Malware tries to download trojan plc code blocks

WinCC



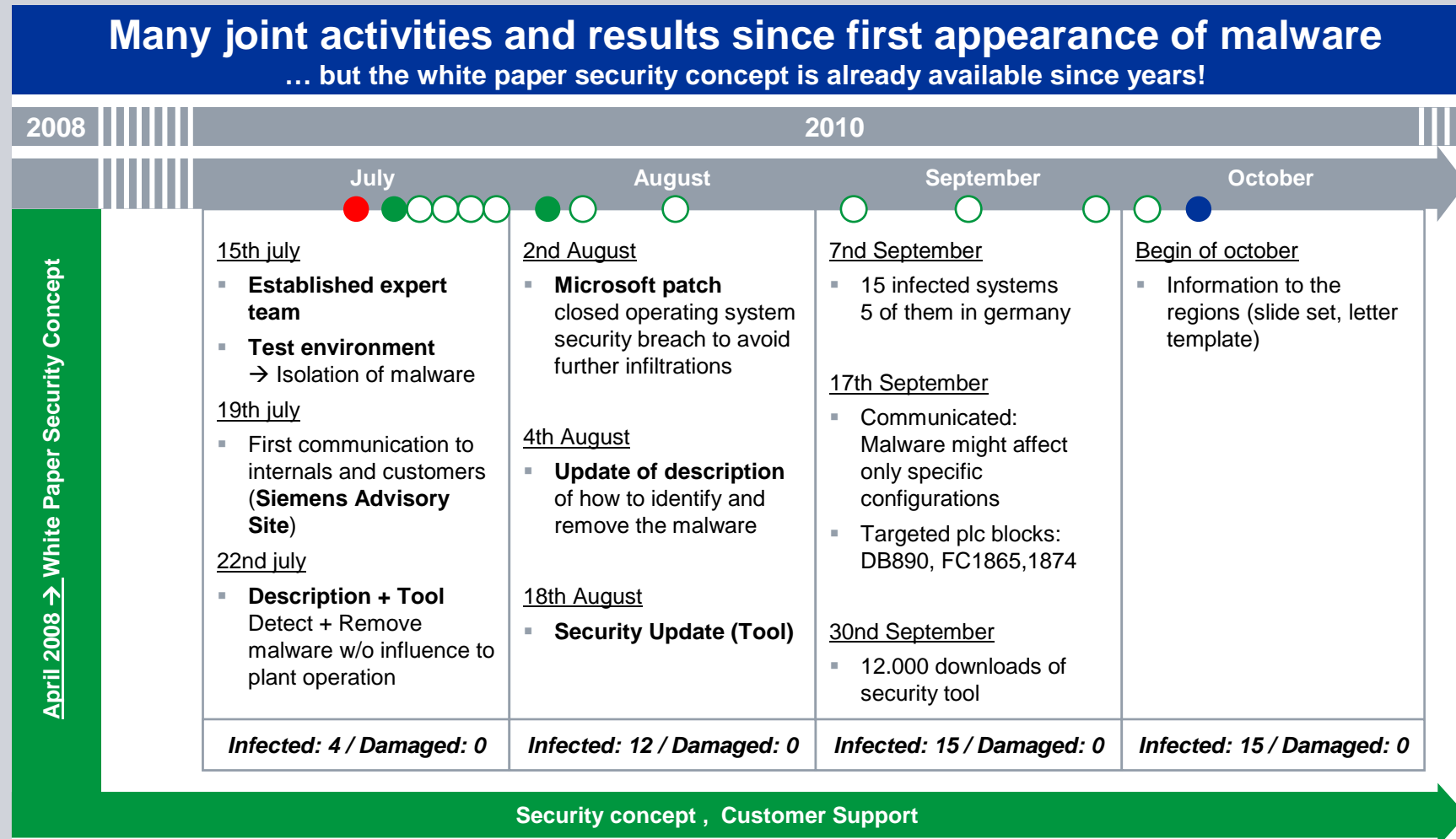
Details

- 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?



Stuxnet Malware



What has Siemens done against Stuxnet

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?



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

Security Concept

Product list Entry list

Filter settings:

Entry type: Manuals

Search term(s):

Title	Date
Manuals Detailed documents on the "Security concept PCS 7 and WinCC"	2009-09-22
- Manuals Security Concept PCS 7 & WinCC (Detail) Administration of Virus Scanners	2009-09-22 ID: 38625981
- Manuals SIMATIC Process Control system PCS 7, Virus scanners	2009-09-07
- Manuals, configurable SIMATIC Process Control System PCS 7 Trend Micro Office Scan configuration V7.3 including Patch 2	2009-09-07 ID: 38006161
- Manuals, configurable Trend Micro OfficeScan V8.0 Configuration	2009-09-07 ID: 38006929
- Manuals, configurable SIMATIC Process Control System PCS 7 Symantec AntiVirus V10.2 Configuration	2009-09-07 ID: 38006339
- Manuals, configurable SIMATIC Process Control System PCS 7 Symantec Endpoint Protection 11.0 Configuration	2009-09-07 ID: 38004630

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>

SIEMENS	
M o d e l l e n e	
SIMATIC	
Security concept PCS 7 and WinCC - Basic document	
Whitepaper	
Preface	1
Aim of the security concept	2
References	3
Definitions	4
Strategies of the security concept	5
Implementing the security strategies in security solutions	6
Appendix	7

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

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