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?

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)

- USB-Stick
- Microsoft Operating System
- WinCC
- SQL Server
- S7 / plc

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

Target Server
apparently not active

Malware
INet
load blocks
wraps S7-DOS DLL

Infection via USB / network / printer spooler → fixed by Microsoft Patch

SIMATIC Security Update Tool
SYSCLEAN Tool removes malware from infected machines

DB 890 FC 1865, 1874
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 targeting 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?

Many joint activities and results since first appearance of malware
... but the white paper security concept is already available since years!

<table>
<thead>
<tr>
<th>2008</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>July</td>
<td></td>
</tr>
<tr>
<td>15th July</td>
<td></td>
</tr>
<tr>
<td>Established expert team</td>
<td></td>
</tr>
<tr>
<td>Test environment → Isolation of malware</td>
<td></td>
</tr>
<tr>
<td>19th July</td>
<td></td>
</tr>
<tr>
<td>First communication to internals and customers (Siemens Advisory Site)</td>
<td></td>
</tr>
<tr>
<td>22nd July</td>
<td></td>
</tr>
<tr>
<td>Description + Tool</td>
<td></td>
</tr>
<tr>
<td>Detect + Remove malware w/o influence to plant operation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>August</td>
<td></td>
</tr>
<tr>
<td>2nd August</td>
<td></td>
</tr>
<tr>
<td>Microsoft patch</td>
<td></td>
</tr>
<tr>
<td>closed operating system security breach to avoid further infiltrations</td>
<td></td>
</tr>
<tr>
<td>4th August</td>
<td></td>
</tr>
<tr>
<td>Update of description</td>
<td></td>
</tr>
<tr>
<td>of how to identify and remove the malware</td>
<td></td>
</tr>
<tr>
<td>18th August</td>
<td></td>
</tr>
<tr>
<td>Security Update (Tool)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>September</td>
<td></td>
</tr>
<tr>
<td>7th September</td>
<td></td>
</tr>
<tr>
<td>15 infected systems</td>
<td></td>
</tr>
<tr>
<td>5 of them in Germany</td>
<td></td>
</tr>
<tr>
<td>17th September</td>
<td></td>
</tr>
<tr>
<td>Communicated: Malware might affect only specific configurations</td>
<td></td>
</tr>
<tr>
<td>Targeted plc blocks: DB890, FC1865, 1874</td>
<td></td>
</tr>
<tr>
<td>30th September</td>
<td></td>
</tr>
<tr>
<td>12,000 downloads of security tool</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>October</td>
<td></td>
</tr>
<tr>
<td>Begin of October</td>
<td></td>
</tr>
<tr>
<td>Information to the regions (slide set, letter template)</td>
<td></td>
</tr>
</tbody>
</table>

Infected: 4 / Damaged: 0
Infected: 12 / Damaged: 0
Infected: 15 / Damaged: 0
Infected: 15 / Damaged: 0
# 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

### 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

---

Has also the customer done all he can?
Stuxnet Malware
Will this happen again in the future?

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

Stuxnet specific
• Siemens Advisory Site
• Contact Support
• Security Tool to clean infected PC


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


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