Tofino Security

White Paper

Version 3.1
Published October 14, 2010

Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Industrial Control System Professionals

Contents

Authors

Eric Byres, P. Eng.
CTO, Byres Security Inc.
eric@byressecurity.com
www.tofinosecurity.com

Scott Howard
Technical Services Manager, Byres Security Inc.
scott@byressecurity.com
www.tofinosecurity.com

Executive Summary

Stuxnet is a computer worm designed to take advantage of a number of previously unknown vulnerabilities present in the Windows operating system and Siemens SIMATIC WinCC, PCS7 and S7 product lines.

Of concern to the SCADA and industrial control systems (ICS) community is the fact that Stuxnet was designed to target one or more industrial systems that use Siemens PLCs. The objective of the malware appears to be to reprogram and sabotage these industrial processes. It is also one of the most complex and carefully engineered worms ever seen. It takes advantage of at least four zero-day vulnerabilities[i], has seven different propagation processes and shows considerable sophistication in its exploitation of Siemens systems.

This White Paper summarizes the current known facts about the Stuxnet worm. It also summarizes the actions that operators of SCADA and ICS systems can take to protect critical operations.

What's New in this Version

This document was previously titled "*Analysis of Siemens WinCC / PCS7 Malware Attacks*". It has been changed to "*Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Industrial Control System Professionals*".

The following are the key changes in this version of the White Paper:

- Sections on what Stuxnet is, what it does and what the consequences are of being infected have been completely rewritten in light of new information released by Ralph Langner, Symantec and others.
- Information on the spread of the malware has been updated.
- Vulnerable systems are revised to include unsupported and current versions of Windows including Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 and Windows 7.
- Analysis of the available Detection and Removal tools has been expanded.
- Patches for most (but not all) versions of the Windows operating system are available from Microsoft for three of the vulnerabilities exploited by Stuxnet (MS08-067, MS10-046 and MS10-061). Two other vulnerabilities that allow escalation of privilege on Windows systems were not patched at the time this White Paper was published.
- Workarounds for operating systems where no patches are available has been integrated into a Prevention/Mitigation section that covers both patchable and non-patchable systems.
- References to Siemens, US-CERT, Symantec and Microsoft have been updated

[i] See the Frequently Asked Questions section for an explanation of zero-day vulnerabilities.

Threat Details

What is it?

Stuxnet is a computer worm designed to take advantage of a number of security vulnerabilities present in the Windows operating system and Siemens SIMATIC WinCC, PCS7 and S7 product lines. It is capable of infecting both unsupported and current versions of Windows including Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 and Windows 7. It also infects the Siemens STEP 7 project files in such a way that it automatically executes when the STEP 7 project is loaded by an uninfected Siemens system.

Stuxnet appears to be a targeted worm, designed to reprogram and sabotage one or more very specific industrial processes. While there has been rampant speculation on Stuxnet's intended target, no definitive victim has been identified.

What does it do?

Stuxnet is one of the most complex and well-engineered worms ever seen. It takes advantage of at least four zero-day vulnerabilities and shows considerable sophistication in its exploitation of Siemens systems.

When installed on a computer, Stuxnet attempts to locate Siemens STEP 7 programming stations and infect these. If it succeeds, it replaces the STEP 7 DLL routines, so that any person viewing a PLC's logic would not see any changes Stuxnet later makes to the PLC(s).

Stuxnet then looks for specific models of Siemens PLCs (6ES7-315-2 and 6ES7-417). If it is able to connect to one of these two models, it "finger-prints" the PLC by checking for the existence of process configurations and certain strings in the PLC.

If Stuxnet finds what it is looking for in the PLC, it starts one of three sequences to inject STEP 7 code into the PLC. The PLC's PROFIBUS driver is replaced and the main PLC program block (Organizational Block 1) and the primary watchdog block (Organizational Block 35) are significantly modified. As well, depending on which sequence is selected, between 17 and 32 additional function blocks and data blocks are injected into the PLC.

The infected PLC now appears to wait for a specific event to occur, which it detects by monitoring a variable. If that variable matches a specific value (0xDEADF007), then it significantly changes the executing process logic and prevents the original logic in the watchdog block from executing. How this change in logic impacts the actual industrial process is unknown.

What are the potential consequences to SCADA and control systems?

The objective of the malware appears to be to reprogram and sabotage one or more very specific industrial systems. How it impacts the target industrial process is unknown, but it is probably significant and destructive.

For Siemens-based SCADA or ICS systems that are not the target system, the impact is less severe, but not insignificant. Several Siemens users reported the virus would modify the communication configuration for the PLC's Ethernet ports or processors in offline project files. This could potentially cause loss of communications for the control system should these files be downloaded to the PLCs in the field.

Stuxnet will not modify PLC logic where there is no Siemens product present. However it is important to note that any Windows-based system can be infected by this malware, regardless of whether or not Siemens software is used.

How does it spread?

Of particular concern to the operators of ICS and SCADA system is the fact that Stuxnet infects its victims using any one of three different propagation pathways:

1. Via infected Removable USB Drives;

2. Via Local Area Network communications and
3. Via infected Siemens project files

Within these pathways, it takes advantage of seven independent mechanisms to spread to other computers. This complicates any attempts to control the spread of Stuxnet and requires a multi-tiered approach if security is to be effective.

Removable USB Drives Propagation:

1. Infects computers via removable USB drives (even when AutoRun is disabled) via a previously undiscovered shortcut (i.e. *.lnk file) vulnerability (MS10-046).
2. Versions of Stuxnet created prior to March 2010 did not use the *.lnk file exploit, but instead spread via removable USB drives using an AutoRun-based exploit.

Local Area Network Propagation:

3. Spreads over local area networks to computers with network shares by enumerating all user accounts of the computer and the domain. It then tries all available network resources in order to copy and execute on the remote share, thereby infecting the remote computer.
4. Spreads over local area networks to computers offering print sharing via a Windows Print Spooler zero-day vulnerability (MS10-061).
5. Spreads over local area networks via the Server Service Vulnerability (MS08-067).
6. Infects computers running Siemens WinCC database software by using Siemens "internal" system passwords (that cannot be changed) to log into the SQL server, transfer a version of Stuxnet and execute it locally.

Siemens Project File Propagation:

7. Propagates by copying itself to any discovered Siemens STEP 7 projects (*.S7P, *.MCP and *.TMP files) and then auto-executes whenever the user opens the infected project.

Stuxnet also has a separate P2P (peer-to-peer) networking system to automatically update all installations of the Stuxnet worm in the wild, even if they cannot connect back to the Internet.

WARNING: Disabling AutoRun DOES NOT prevent infection! Simply viewing an infected USB drive using Windows Explorer will infect your computer.

This diversity of propagation mechanisms means that "single-answer" security solutions will not prevent the worm from spreading. A multi-tier/multi-step "defense-in-depth" solution is needed in order to provide effective security. This is discussed further in the Prevention/Mitigation section.

How common is this malware?

This malware is in the "wild" and probably has been for at least 20 months. According to analysts at Microsoft, versions of the Stuxnet were first detected in March of 2009. Since then the worm has been under continued development, as the authors added additional components, encryption and exploits. It only came to public attention in late July 2010.

Analyzing the various malware tracking services such as Symantec and the Microsoft Malware Protection Center, it appears that there are approximately 100,000 infected hosts as of late September, 2010. Symantec states that approximately 60% of the infected hosts are located in Iran. They also report that 67% of the infected systems with Siemens STEP 7 software installed are located in Iran.

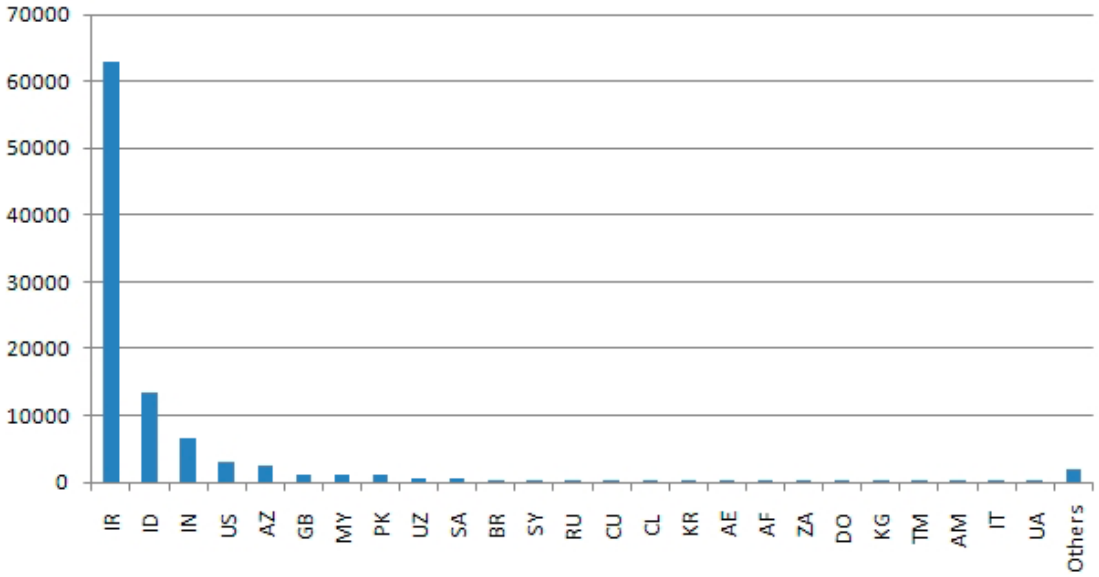

Figure : Infected Hosts by Country (Courtesy of Symantec)

According to the Siemens website, there are 15 known control systems that have been infected by the Stuxnet malware. Based on reports from clients, and the Symantec data, we believe there are a number of other control systems that have been infected, but are either not aware of the infection or are not reporting the infection to Siemens.

Affected Systems

What operating systems are affected?

Based on our analysis, we believe that statements such as "*The virus affects operating systems from XP and higher*" are incorrect.

Our list of vulnerable systems has been expanded to include all unsupported and current versions of Windows including Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 and Windows 7. Of particular importance are the Windows 2000 systems, as there are no patches for these systems.

It appears that Stuxnet will infect Windows NT machines, but will then abort.

What Control/SCADA Systems are affected?

The following control and SCADA systems are believed to be directly affected by this malware:

- All Siemens HMI, SCADA or PCS7 systems based on the WinCC platform
- All Siemens systems using the STEP 7 programming software, particularly S7-300 or s7-400 PLC products

Please note that Stuxnet will infect Windows-based computers on any control and SCADA system, regardless of whether or not it is a Siemens system; however, the malware will not attempt to make modifications to controllers that are not S7-300 or s7-400 PLCs.

Detection and Removal

Anti-virus products

All major anti-virus vendors have released signatures to detect the presence of Stuxnet. Make certain that you are using signatures from July 25, 2010 or later.

US-CERT primary Stuxnet indicators:

The ICS-CERT has released an advisory listing primary Stuxnet indicators. Six are files that may be present in infected machines regardless of whether Siemens WinCC/STEP 7 software is installed. Another three are files that are changed in Siemens WinCC/STEP 7 system and project folders. Details can be found at: http://www.us-cert.gov/control_systems/pdf/ICSA-10-272-01.pdf

Siemens solutions

Siemens is offering Sysclean, a tool from TrendMicro for detecting and removing the virus, for downloading. It is available at: http://support.automation.siemens.com/WW/view/en/43876783

According to the ICS-CERT, the SysClean tool removes multiple malware components and restores the affected DLL file necessary for the STEP 7 software to run. However our tests indicated that Sysclean did not clear infected STEP 7 project files, making it possible that the malware could re-infect a cleaned system when an infected project file was accessed.

That said, Siemens also offers a SIMATIC Security Update (updated 18th August 2010) which performs the following actions:

1. Closes the Microsoft security hole by disabling icons if the Microsoft Security Update for the *.lnk file vulnerability has not been installed.
2. Enforces stricter SQL Server authentication settings.
3. Scans WinCC and STEP 7 project data for Stuxnet infection.

It appears the combination of these two tools might remove all active instances of Stuxnet from a computer but this has not been confirmed.

Note 1: None of these tools remove from PLCs the function blocks which Stuxnet inserted into those PLCs.

Note 2: Siemens also makes the following statement on its web site:

> *"The malware carries its own blocks (for example, DB890, FC1865, 1874) and tries to load them into the CPU and integrate them into the program sequence. If the above-mentioned blocks are already present, the malware does not infiltrate the user program."*

We do not believe that checking for these blocks is a reliable test, as Stuxnet loads fake DLLs into the Siemens programming stations, specifically to hide the existence of these blocks. Thus while the existence of these blocks in a PLC indicates infection, the opposite does not hold true.

Available Patches or Updates

As of Friday, October 8, 2010, patches for most (but not all) versions of the Windows operating system are available from Microsoft for three of the vulnerabilities exploited by Stuxnet (MS08-067, MS10-046 and MS10-061). Two other vulnerabilities that allow escalation of privilege on Windows systems were not patched at this time.

Patches to address the three above noted vulnerabilities are available from Microsoft for the following operating systems:

- Windows XP Service Pack 3
- Windows XP Professional x64 Edition Service Pack 2

- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 1 and Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems
- Windows 7 for x64-based Systems
- Windows Server 2008 R2 for x64-based Systems
- Windows Server 2008 R2 for Itanium-based Systems

These patches can be downloaded from:

http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx

http://www.microsoft.com/technet/security/bulletin/MS10-061.mspx

We are unaware of any patches to address the Siemens STEP 7 project file exploits or to change the default WinCC SQL server passwords. However, the SIMATIC Security Update (updated 18th August 2010) does enforce stricter SQL Server authentication settings.

For those operating systems where no patches exist, there are a number of workarounds that we describe in the section below.

Prevention/Mitigation

As noted earlier, Stuxnet is a complex worm with no single solution. As a result, this section is divided into subsections dedicated to addressing each of the possible propagation vectors. Within each subsection is guidance for both supported systems (i.e. those that are patchable) and unsupported systems (i.e. those that are not patchable). The latter solutions are known as "Workarounds" and are configuration changes that will not correct the underlying issue, but will help block known attack vectors for systems where no patch is available.

General Infection Prevention:

1. Anti-Virus / White List Installation

Applicability: All Windows Operating Systems

We recommend that that either anti-virus or white listing software be installed on all potentially vulnerable computers. Current versions of this type of software will prevent Stuxnet infection and these tools work across most propagation methods.

Impact: Some anti-virus or white listing products may be incompatible with control system products. Check with your PCS vendor as to whether such tools will cause malfunction of your control products or affect your support status.

Removable USB Drive Propagation:

The following patches, mitigations and workarounds help protect computers from infection via removable USB drives (includes *.lnk file vulnerability (MS10-046) and AutoRun-based exploits).

2. **Avoid using USB Drives in Control Systems**

   Applicability: All Windows Operating Systems

   If possible, we recommend not installing any USB drives into any Windows systems, regardless of OS patch level or whether AutoRun has been disabled or not.

3. **Prequalify all USB Drives**

   Applicability: All Windows Operating Systems

   If USB drives must be used, prequalify them by first installing them in an isolated computer that is fully patched and is running antivirus detection software with signatures capable of detecting Stuxnet.

4. **Disable Autorun for all USB Drives**

   Applicability: All Windows Operating Systems

   Early versions of Stuxnet exploited the Autorun functionality to load from USB drives. To prevent this possibility, disable Autorun functionality as described in Microsoft document "*How to disable the Autorun functionality in Windows*" (http://support.microsoft.com/kb/967715).

5. **Install Windows Patch for *.lnk file vulnerability**

   Applicability: Windows XP SP3, Windows Server 2003, Windows Vista, Windows Server 2008 and Windows 7

   Install patch for the vulnerability as described in Microsoft Security Bulletin MS10-046 – Critical (http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx).

6. **Disable the displaying of icons for shortcuts**

   Applicability: Windows 2000, Windows XP SP2 or older and Windows Server 2003 SP1 or older

   The Stuxnet *.lnk exploit will only execute if the .lnk files icons are displayed in a file browser. Thus disabling the display of icons for shortcuts will reduce the chance of infection. To manually disable the displaying of icons for shortcuts see Microsoft Support Knowledgebase Article 2286198 (http://support.microsoft.com/kb/2286198). A Fixit tool to do this automatically is also available on this site.

   Impact of workaround: When this workaround is implemented, shortcut files and Internet Explorer shortcuts will no longer have an icon displayed. This may make viewing the Windows system difficult.

7. **Disable the WebClient service**

   Applicability: Windows 2000, Windows XP SP2 or older and Windows Server 2003 SP1 or older

   While Stuxnet does not use this vector, disabling the WebClient service helps protect affected systems from other attempts to exploit this vulnerability. It does this by blocking a possible remote attack vector through the Web Distributed Authoring and Versioning (WebDAV) client service. After applying this workaround, it will still be possible for remote attackers who successfully exploited this vulnerability to cause Microsoft Outlook to run programs located on the targeted user's computer or the Local Area Network (LAN), but users will be prompted for confirmation before opening arbitrary programs from the Internet.

To disable the WebClient Service see Microsoft Support Knowledgebase Article 2286198 (http://support.microsoft.com/kb/2286198).

Impact of workaround: When the WebClient service is disabled, Web Distributed Authoring and Versioning (WebDAV) requests are not transmitted. In addition, any services that explicitly depend on the Web Client service will not start, and an error message will be logged in the System log. For example, WebDAV shares will be inaccessible from the client computer. For most industrial control systems, this will have little affect on operations.

Local Area Network Propagation:

The following patches, mitigations and workarounds help protect computers from infection over the local area network via various network services vulnerabilities (Print Spooler Service vulnerability (MS10-061) and MS08-067 Windows Server Service vulnerability (MS08-067)).

8. Use a Firewall to block all TCP and UDP ports associated with RPC

Applicability: All Windows Operating Systems

Install a zone firewall between sub-systems to block UDP ports 135, 137, 138, and 445, and TCP ports 135, 139, 445, and 593 and all ports above 1024 that are not specifically needed for control system operations.

Impact of workaround: The Print Spooler Service uses the Remote Procedure Call (RPC) protocol, which is the same underlying protocol as OPC Classic (a popular SCADA integration protocol). Thus this workaround can negatively impact critical OPC communications. Use of an appropriate OPC-aware industrial firewall to block all non-OPC RPC traffic will prevent this problem from occurring.

9. Install Windows Patch for Print Spooler Service vulnerability

Applicability: Windows XP SP3, Windows Server 2003, Windows Vista, Windows Server 2008 and Windows 7

Install patch for the vulnerability as described in Microsoft Security Bulletin MS10-061 – Critical http://www.microsoft.com/technet/security/bulletin/MS10-061.mspx

10. Disable printer sharing

Applicability: Windows 2000, Windows XP SP2 or older and Windows Server 2003 SP1 or older

To disable printer sharing on Windows 2000, Windows XP and Windows 2003 systems, perform the following actions:

i. Click **Start**, and then click **Printer and Faxes**.

ii. Right-click the printer icon and select **Sharing**.

iii. Select **Do Not Share This Printer**, and then click **OK**.

iv. Repeat this process for each printer shared on the system.

Impact of workaround: By disabling this feature, remote users will not be able to print to the shared printer.

11. Disable the Guest Account

Applicability: Windows 2000 and Windows XP systems

On Windows 2000 and XP, the guest account is enabled by default, which allows anonymous users to access printer shares. On Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, an attacker must be authenticated in order to exploit this vulnerability, unless password-based sharing is disabled. Note: If password-based sharing is disabled, attackers could exploit these systems without authentication.

Impact of workaround: Minimal for most industrial control systems

12. **Install Windows Patch for Server Services vulnerability**

    Applicability: Windows 2000 SP4, Windows XP (all Versions), Windows Server 2003 (SP1 and SP2), Windows Vista, Windows Server 2008

    Install patch for vulnerability as described in Microsoft Security Bulletin MS08-067 – Critical
    http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

The reader will note that not all Stuxnet propagation methods have been addressed by the above Prevention/Mitigation steps. In particular, solutions to address the Siemens WinCC SQL database propagation, the Siemens S7 project file propagation and the P2P (peer-to-peer) networking system are still under investigation. As well, the two reported Escalation of Privilege exploits are still unpatchable and there is no known workaround.

Actions Not Recommended

WARNING: While it might seem that one reasonable solution is to change the default passwords for the WINCCConnect account, this would impede communication between WinCC and the database and is therefore not recommended.

Frequently Asked Questions

What is a shortcut?

A shortcut is a link to a file or program, represented by an icon. If you double-click a shortcut, the file or program opens. The shortcut is a mechanism often used to keep frequently used files in a single, easily accessed location, such as a folder or the desktop. Shortcuts are implemented as files with the *.lnk* extension.

What is Siemens WinCC/STEP 7/PCS7?

Siemens WinCC is a Human Machine Interface (HMI) application for the visualization and supervision of process control and SCADA systems.

Siemens STEP 7 is a family of software tools for configuration and programming of Siemens automation systems.

Siemens PCS7 is an integrated distributed control system comprised of various operator systems (WinCC), automation systems (S7-400 PLC), engineering systems (STEP 7) and other components.

What is a zero-day vulnerability?

Zero-day vulnerabilities are those that are unpatched by the affected software's manufacturer. The "days" start counting once a patch is released.

I don't use the versions of Windows listed on the Siemens and Microsoft sites – do I still need to be concerned?

Absolutely – all versions of Microsoft Windows newer than Windows NT 4.0 can be infected.

I don't use Siemens products – do I still need to be concerned?

Yes – computers can still be infected by the Stuxnet, regardless of whether Siemens products are present.

I have disabled AutoRun on my system- am I safe?

No – Stuxnet takes advantage of a new vulnerability that does not require AutoRun to be active. That said, it is still a good idea to disable AutoRun.

Can this malware only be distributed by USB drives?

Stuxnet is most likely to be introduced through removable USB drives. However, the malware can also be distributed over network shares or remote WebDAV shares or through a variety of SQL, print server and Windows Server Service vulnerabilities. It can also be distributed through WinCC database connections and infected STEP 7 project files.

References

For more information about this issue, see the following references:

Microsoft Security Bulletins

http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx

http://www.microsoft.com/technet/security/bulletin/MS10-061.mspx

Microsoft Security Advisory (2286198)

http://www.microsoft.com/technet/security/advisory/2286198.mspx

http://support.microsoft.com/kb/2286198

http://support.microsoft.com/kb/2347290

Microsoft Malware Protection Center

http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx

http://blogs.technet.com/b/mmpc/archive/2010/07/30/stuxnet-malicious-lnks-and-then-there-was-sality.aspx

Siemens Automation

http://support.automation.siemens.com/WW/view/en/43876783

US-CERT

http://www.us-cert.gov/control_systems/pdf/ICSA-10-201-01C%20-%20USB%20Malware%20Targeting%20Siemens%20Control%20Software%20-%20Update%20C.pdf

http://www.us-cert.gov/control_systems/pdf/ICSA-10-272-01.pdf

http://www.us-cert.gov/control_systems/pdf/ICSA-10-238-01B%20-%20Stuxnet%20Mitigation.pdf

Symantec Security Focus

http://www.securityfocus.com/bid/31874/

http://www.securityfocus.com/bid/41732

http://www.securityfocus.com/bid/43073

CVE References

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2729

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2772

Some SCADA/ICS-related blog posts on Stuxnet:

http://www.tofinosecurity.com/blog/stuxnet-mystery-continues

http://www.tofinosecurity.com/blog/amazing-mr-stuxnet

http://www.tofinosecurity.com/blog/stuxnet-i-was-wrong

http://www.tofinosecurity.com/blog/why-stuxnet-affects-all-windows-systems

http://www.tofinosecurity.com/blog/why-another-security-blog-stuxnet-shows-why

http://findingsfromthefield.com/?p=555

http://controlsystemsecurity.blogspot.com/2010/10/symantec-stuxnet-dossier.html

Detailed discussion on the malware and how it works:

http://www.langner.com/en/

http://www.symantec.com/connect/blogs/w32stuxnet-dossier

http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf