Analysis of Siemens WinCC/PCS7 Malware Attacks
Executive Summary

Stuxnet (also known as W32.Temphid and as Rootkit.TmpHider) is a computer worm designed to take advantage of a previously unknown vulnerability present in all supported versions of the Windows operating system. It is spread via infected USB drives. It can also be propagated via network shares from other infected computers.

As of Tuesday, August 3, 2010, patches for most (but not all) versions of Windows are available from Microsoft for the vulnerability. There are also a number of workarounds for systems where no patches are available. Please note that standard mitigation for USB-based threats, such as disabling AutoRun, are not effective against this malware.

Of interest to the SCADA and process control community is that Stuxnet is designed to target any system using the Siemens WinCC Platform. The objective of the malware appears to be industrial espionage; i.e., to steal intellectual property from SCADA and process control systems. It may also have other SCADA-related targets and objectives.

What’s New in this Version

The following are the key changes in version 2.0 of this white paper:

- Patches for most (but not all) versions of the Windows operating system are available from Microsoft for the vulnerability.
- Information on the spread of the malware has been expanded.
- Workarounds for operating systems where no patches are available have been expanded.
- Sources for Detection and Removal tools have been expanded.
- References to Siemens, US-CERT, Symantec and Microsoft have been updated.

Threat Details

What is it?


It appears to be designed to attack and steal critical information from SCADA and Process Control HMI systems. It may also have other objectives.

As of Tuesday, August 3, 2010, patches for most (but not all) versions of Windows are available from Microsoft. For those operating systems where no patches exist, there are several temporary workarounds that we will describe later in this white paper.

What does it do?

Stuxnet takes advantage of a vulnerability in Windows’ handling of short cut files (known as .lnk files) found on an infected USB drive. It automatically executes the malware when the .lnk file is read by the operating system, typically when the USB drive is browsed using Windows Explorer. It then installs additional malware components onto the compromised computer:

- A backdoor (Worm:Win32/Stuxnet.A) to allow the malware developer to remote access the infected computer.
- A device driver (Trojan:WinNT/Stuxnet.A) to hide the presence of the .lnk files.
A second device driver (Trojan:WinNT/Stuxnet.B) to inject previously encrypted “data blobs” into memory, each of which appear to serve different purposes for the attacker.

It then proceeds to execute a number of tasks, only one of which has been analyzed. This task appears to:

- Search for any Siemens SCADA, HMI and PCS7 products on the computer using the WinCC platform and Microsoft SQL Server 2005 or later.
- Attempt to log into MSSQL using the Siemens default account of “WinCCConnect” and the default password “2WSXcder”.
- Collect a list of all variables in the database used by WinCC, such as descriptions of controller variables.
- Select the variables out of the database and place them into a large text field, possibly to write to a file.
- Execute a number of other procedures, one of which appears to be loading and executing another file into the database. The purpose of this file is not known.

(Our thanks to Frank Boldewin for his excellent decode and posting and to Steve Kirby at Tikor Consulting for this excellent analysis)

What are the potential consequences to SCADA and control systems?

The objective of the malware appears to be industrial espionage; i.e. to steal intellectual property from SCADA and process control systems.

Specifically, the malware uses the Siemens default password of the MSSQL account WinCCConnect to log into the PCS7/WinCC database and extract process data and possibly HMI screens. This information is then forwarded to servers in Malaysia and Denmark.

That said, any Windows system can be infected by this malware regardless of whether or not Siemens software is present.

How does it spread?

The Stuxnet malware is spread via USB key. It can be also be propagated via network shares from other infected computers.

As noted above, Stuxnet uses a specially crafted Windows shortcut placed on USB key drives to automatically execute malware as soon as the .lnk file is read by the operating system. In other words, simply browsing to the USB drive using an application that displays shortcut icons (like Windows Explorer) runs the malware without any additional user interaction.

Once the computer is infected, it will attempt to infect any other USB drive inserted into it.

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

How common is this malware?

This malware is in the “wild” and probably has been since at least early June 2010. According to analysts at Symantec, the development of the malware targeted at Siemens systems dates back to June of 2009. The threat has been under continued development as the authors added additional components, encryption and exploits. It was only come 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 approximately 5,000 new machines are reporting and blocking the attack each day. On July 22, Symantec reported that 14,000 unique IP addresses had been infected with Stuxnet and were attempting to contact the attacker’s command and control servers.
Most of the reports have been coming from the Indonesia, India, Iran and the US, but the percentage of attacked machines in Iran and Indonesia as compared to the number of reporting machines in these countries is at least two orders of magnitude higher. Brazil is starting to be a dominant source of reports as well, but this appears to be from malware that utilizes the same vulnerability, but is not SCADA related.

According to ISSSource as of August 3, there are six known control system victims of the malware attack, all in Europe. Based on the fact that the distribution of infection signatures are predominately from outside Europe, we believe there are a number of other control systems that have been infected, but are not aware of the infection.

**Affected Systems**

**What operating systems are affected**

Based on our analysis, we believe that statements that “The virus affects operating systems from XP and higher” are incorrect.

Our list of vulnerable systems has been expanded to include all obsolete and current versions of Windows including Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 and Windows 7.

**Control/SCADA Systems Affected**

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

- All Siemens HMI, SCADA and PCS7 systems based on the WinCC platform

Please note that any control and SCADA systems can be infected by the Stuxnet, regardless of whether WinCC is present or not.

**Detection and Removal**

All major anti-virus vendors have released signatures for Stuxnet. Make certain that you are using signatures from July 25, 2010 or later. Below is a brief list of download sites:

**Microsoft Security Essentials:**


**TrendMicro:**


**Symantec:**


**Computer Associates:**


**Sophos:**


**Siemens:**

Siemens is offering Sysclean, a tool from TrendMicro for detecting and removing the virus, for downloading. It is available at:

Available Patches or Updates

As of August 3, 2010, patches to address the vulnerability were 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 x64-based Systems and Windows Server 2008 for x64-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/MS10-046.mspx

Workarounds

Workarounds are configuration changes that will not correct the underlying issue, but will help block known attack vectors for systems where no patch is available. For the systems noted above with an available patch, we recommend only using workaround 1 and 2.

1. Avoid using USB Keys in Control Systems

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

2. Prequalify all USB keys

If USB keys 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.

The following two workarounds are courtesy of Microsoft Support Knowledgebase Article 2286198.

3. Disable the displaying of icons for shortcuts

The Stuxnet 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. A Fixit tool to do this automatically is available from Microsoft at http://support.microsoft.com/kb/2286198
To manually disable the displaying of icons for shortcuts:

1. Click **Start**, click **Run**, type `regedit` in the **Open** box, and then click **OK**.
2. Locate and then select the following registry key:
   
   HKEY_CLASSES_ROOT\lnkfile\shellex\IconHandler

3. Click the **File** menu, and then click **Export**.
4. In the **Export Registry File** dialog box, type `LNK_Icon_Backup.reg` and then click **Save**.
   
   **Note**: This step creates a backup of this registry key in the My Documents folder by default.

5. Select the value (Default) on the right pane in Registry Editor. Press ENTER to edit the value of the key. Delete the value so that the value is blank, and then press ENTER.
6. Locate and then select the following registry key:
   
   HKEY_CLASSES_ROOT\piffile\shellex\IconHandler

7. Click the **File** menu, and then click **Export**.
8. In the **Export Registry File** dialog box, type `PIF_Icon_Backup.reg`, and then click **Save**.
   
   **Note**: This step creates a backup of this registry key in the My Documents folder by default.

9. Select the value (Default) on the right pane in Registry Editor. Press ENTER to edit the value of the key. Delete the value so that the value is blank, and then press ENTER.

**Impact of workaround**: Disabling icons for shortcuts from being displayed prevents the issue from being exploited on affected systems. When this workaround is implemented, shortcut files and Internet Explorer shortcuts will no longer have an icon displayed.

**Disable the WebClient service**

Disabling the WebClient service helps protect affected systems from attempts to exploit this vulnerability by blocking the most likely 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, follow these steps:

1. Click **Start**, click **Run**, type `Services.msc` and then click **OK**.
2. Right-click **WebClient** service and select **Properties**.
3. Change the Startup type to **Disabled**. If the service is running, click **Stop**.
4. Click **OK** and exit the management application.

**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.

**Actions Not Recommended**

**WARNING**: While it might seem that a 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?
Siemens WinCC is a Human Machine Interface (HMI) application for the visualization and supervision of process control and SCADA systems.

I don't use the Versions of Windows listed on the Siemens and Microsoft sites – do I still need to be concerned?
Yes – all versions of Microsoft Windows can be infected.

I don't use Siemens WinCC – do I still need to be concerned?
Yes – computers can still be infected by the Stuxnet, regardless of whether WinCC is present or not.

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 drive?
This vulnerability is most likely to be exploited through removable USB drives. However, malware shortcuts can also be distributed over network shares or remote WebDAV shares.

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

Microsoft Security Bulletin (MS10-046)
http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx

Microsoft Security Advisory (2286198)
http://www.microsoft.com/technet/security/advisory/2286198.mspx
http://support.microsoft.com/kb/2286198

Microsoft Malware Protection Center

Siemens Automation

US-CERT
CVE Reference (CVE-2010-2568)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568

Detailed discussion on the malware and how it works:
http://www.symantec.com/connect/blogs/w32stuxnet-installation-details
http://www.symantec.com/connect/blogs/distilling-w32stuxnet-components
http://www.symantec.com/connect/blogs/w32stuxnet-network-operations