ICS-CERT ADVISORY

ICSA-10-238-01B—STUXNET MALWARE MITIGATION

UPDATE B

September 15, 2010

OVERVIEW

In July, ICS-CERT published an advisory and a series of updates regarding the Stuxnet malware entitled "ICSA-10-201—USB Malware Targeting Siemens Control Software."[a] Since then, ICS-CERT has continued analysis of the Stuxnet malware in an effort to determine more about its capabilities and intent. As the analysis has progressed, understanding of the malware sophistication has continued to increase.

Stuxnet makes use of a digitally signed kernel-mode rootkit. There have been two digital certificates used to sign this rootkit. The original certificate was revoked. Subsequently, a second variant was discovered in which the same rootkit was signed with a different key, which has also been revoked. With approximately 4,000 functions, Stuxnet contains as much code as some commercial software products. The complex code is object oriented and employs many programming techniques that demonstrate advanced knowledge in many areas, including the Windows operating system, Microsoft SQL Server, Siemens software, and Siemens PLCs. The malware also employs many advanced anti-analysis techniques that make reverse engineering difficult and time consuming.

ICS-CERT has identified that while USB drives appear to be a primary infection mechanism, Stuxnet can also infect systems through network shares and SQL databases. The Stuxnet malware stores dropped files in many locations on a target system. The infection mechanism is complex, and the exact files that may be dropped will vary depending on the system it is infecting. After infecting a system, the malware gathers extensive data from MS SQL server, Windows registry, and application software.

Once the malware has installed itself on a system, it employs many evasive techniques, including bypassing antivirus software, advanced process injection, hooking useful functions by kernel-mode rootkits, and the quick removal of temporary files. ICS-CERT is continuing to reverse engineer and analyze this malware. Because of the malware's complexity, this work is expected to take some time.

a. ICS-CERT Advisory, http://www.us-cert.gov/control_systems/pdf/ICSA-10-201-01C - USB Malware Targeting Siemens Control Software - Update C.pdf, website last accessed August 24, 2010.

MITIGATION

--------- Begin Update B ----------

According to reports and analysis, Stuxnet uses a total of five vulnerabilities; one previously patched (MS08-067) and four zero-days. Two of the four zero-day vulnerabilities have been patched since Stuxnet's discovery.

The first zero-day was addressed in MS10-046[b] on August 24th, 2010. The second and most recent zero-day vulnerability was addressed in MS10-061[c]: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290), released on Sept 14th, 2010. According to Microsoft, "This vulnerability in the Print Spooler Service is rated Critical for Windows XP and Important on all other affected platforms and is used by Stuxnet to spread to systems inside the network where the Print Spooler service is exposed without authentication."

The other two vulnerabilities are local escalation of privilege vulnerabilities that enable an attacker to gain full control of an affected system. According to an MSRC[d] post, one the vulnerabilities affects Windows XP and the other affects Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2. Microsoft is evaluating these vulnerabilities and will be releasing updates in future bulletins.

ICS-CERT recommends that control system owners and operators review system upgrades and consider applying available patches to mitigate the risks for Stuxnet infection. As with all system changes, administrators should consult their control systems vendor prior to making any system changes.

On Sept 7th, Siemens also updated their support site to indicate that they were aware of 15 infections worldwide. According to Siemens, in none of the cases did the infection cause an adverse impact to the automation system.

---------- End Update B ----------

Implementing security measures and properly cleaning an infected system will help to mitigate the effects of the malware and overall risk of a successful Stuxnet infection. The following sections provide guidance that can be used by owners and operators to prevent or identify and remove the Stuxnet malware.

PREVENTING INFECTION

MICROSOFT WINDOWS UPDATES

[b] http://www.microsoft.com/technet/security/Bulletin/MS10-046.mspx
[c] http://www.microsoft.com/technet/security/bulletin/ms10-061.mspx
[d] http://blogs.technet.com/b/msrc/

Organizations affected by Stuxnet and running Siemens WinCC or Step7 software should follow Siemens recommendations[e] for applying the Microsoft updates.

Stuxnet malware also references a Microsoft vulnerability that was addressed in MS08-067[f], although it is not yet clear how this vulnerability is used. ICS-CERT recommends that control system owners and operators review system upgrades and consider applying this patch if it has not already been applied. As with all system changes, administrators should consult their control systems vendor prior to making any system changes.

USB POLICY AND USAGE

Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. This convenience also poses a security concern. Stuxnet and other malware take advantage of USB drives to propagate. Organizations are encouraged to review internal company policies and establish protective technical measures to disable USB drives. ICS-CERT recommends reviewing the Control Systems Analysis Report "USB Drives Commonly Used As an Attack Vector against Critical Infrastructure"[g] for additional information on removable media and best practices.

IDENTIFYING AND REMOVING THE STUXNET MALWARE

The overall sophistication of the Stuxnet malware cannot be overstated. Because of this complexity, cleanup procedures will vary. Some infections will be simple, while others involving Siemens products may be significantly more complex. Below are mitigation recommendations for two different system types:

1. Systems running Siemens software
2. Standard systems that are not running Siemens software.

Control system owners and operators should exercise caution and consult their control systems vendor prior to making any changes or using antivirus software. In addition, proper impact analysis and testing should always be conducted prior to making any changes to control systems.

With this caveat in mind, if current antivirus software identifies a system as being infected with Stuxnet malware, the following guidelines will aid in malware mitigation.

INFECTION OF SYSTEMS RUNNING SIEMENS SOFTWARE

e. Siemens Product Support, http://support.automation.siemens.com/WW/view/en/43876783, website last accessed August 23, 2010.
f. Microsoft Security Bulletin, http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx, website last visited August 25, 2010.
g. ICS-CERT, http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-USB%20USAGE.pdf, website last accessed August 24, 2010.

If Siemens SIMATIC WinCC or STEP 7 software is running on an infected system, then Siemens Customer Support and ICS-CERT should be contacted. Siemens recommends installing the Microsoft Patch,[h] running the SysClean tool,[i] and installing the SIMATIC Security Update.[i] The details of the Siemens procedure are listed on the Siemens Product Support website:

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

NOTE: The SysClean tool removes multiple malware components (including the malicious DLL) and ICS-CERT has independently verified that the SIMATIC Security Update restores the affected DLL file necessary for the STEP 7 software to run.

A Stuxnet infection can be complicated and involve many changes to the infected system and possibly to attached PLC hardware. Control system owners and operators should be aware that although SysClean does remove a number of files, remnant artifacts may be left on a system after cleaning. Remnants can include new files, modified files (including WinCC project files), registry changes, and new or modified database tables.

SysClean appears to stop the malware from infecting USB drives. However, because of the complexity of this malware, it is not yet understood if these remnants could pose future problems.

ICS-CERT recommends working closely with Siemens Customer Support to determine whether to completely rebuild a compromised system or to clean it through manual and/or automated means.

ICS-CERT will also provide support to organizations requesting additional guidance or analysis including onsite support where appropriate. ICS-CERT is continuing to collaborate with Siemens on this malware.

INFECTION OF STANDARD SYSTEMS (NOT RUNNING SIEMENS SOFTWARE)

If a standard computer system (a system not running Siemens software) is found to be infected, then ICS-CERT recommends following the direction of your antivirus vendor to clean the Stuxnet malware. Because Stuxnet specifically targets Siemens' systems, it will behave very differently on standard systems than it does on systems running Siemens software. Current analysis indicates that cleanup of standard systems will be less complicated than on a system with Siemens' software installed.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585

h. Microsoft, http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx, website last accessed August 23, 2010.
i, Siemens Product Support, http://support.automation.siemens.com/WW/view/en/43876783, website last accessed August 23, 2010.

For Control System Security Program Information and Incident Reporting:
www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

Can I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public Web sites. All comments or questions related to this document should be directed to the ICS-CERT at ics-cert@dhs.gov.