INDUSTRIAL DEFENDER®

Industrial Defender, Inc.
16 Chestnut Street · Suite 300
Foxborough · MA · USA · 02035
T: +1·508·718·6700
F: +1·508·718·6701

The Stuxnet Worm and Options for Remediation

Andrew Ginter, Chief Security Officer, Industrial Defender

Last updated: August 6, 2010

Table of Contents

1: Introduction 2
2: Variants and Naming 3
3: LNK Vulnerability 3
4: Stuxnet Propagation 4
5: Evidence of Compromise 5
6: Signed Code 6
7: Network Operations 6
8: Stuxnet Targets Siemens PCS 7 Systems 7
9: Geographic Distribution 9
10: Remediations 13
10.1: Microsoft Patch for LNK Vulnerability 15
10.2: Microsoft Tool to Disable Display of File Shortcuts 15
10.3: Siemens / TrendMicro Remediation Tool 15
10.4: Siemens Update 16
10.5: Third Party LNK Vulnerability Avoidance Tools 16
10.6: Anti-Virus Tools 16
10.7: Whitelisting / Host Intrusion Prevention Systems 17
10.8: Host Intrusion Detection Systems 18
10.9: Disabling USB Keys 19
10.10: Strict Firewall Egress Filtering 20
10.11: Other Topics 20
11: Conclusions 21
12: Links 21

1: Introduction

On June 17, 2010, the makers of the VirusBlokAda anti-virus product in Belarus identified a new worm. The worm was significant in that it propagated via a previously unknown vulnerability in the method that all versions of Microsoft Windows operating systems, since at least Windows NT, handled file shortcut or ".LNK" files. Further, the malware was signed by a RealTek certificate. On July 14, Frank Boldewin, a security expert in Germany, investigated the worm further and discovered that the worm targeted Siemens WinCC control system components, part of the Siemens PCS 7 control system solution.

This combination of characteristics:

- Using an unknown and un-patched vulnerability to compromise machines,
- Being signed with a certificate from a well-known vendor, presumably stolen, and
- A sophisticated attack on industrial control systems components,

made the worm very unusual. This paper summarizes what is known about the worm at the time of writing, and describes ways to protect industrial control systems from the worm.

2: Variants and Naming

The VirusBlokAda paper used a number of terms to refer to the worm. Components of the worm were identified as "Rootkit.TmpHider" and "Rootkit.TmpHider.2," presumably because the worm was embedded in ".tmp" files. By the time Microsoft published their advisory, a majority of labs with signatures published for the worm had dubbed it "Stuxnet." Microsoft identified the "TmpHider" and "TmpHider.2" components of the worm as "Stuxnet.A" and "Stuxnet.B".

This first Stuxnet.A/B variant of the worm was signed with a RealTek certificate. On July 17, ESET labs announced that they had found a second variant of the worm, signed with a JMicron certificate. On July 23, Kaspersky labs reported that their anti-virus products were reporting over 40,000 computers infected with Stuxnet.A/B, but only two machines infected with the JMicron-signed variant. Little has been published about the variant and differing naming conventions for the variant exist.

Symantec reports that it has analyzed some four variants of the Stuxnet worm. The first three differed only in "junk" bytes added to or removed from the Stuxnet installer file to change checksums and file sizes. The fourth variant appears to be a much older version of Stuxnet dating from June of 2009. That variant does not yet use the LNK vulnerability to propagate, but still targets Siemens control systems.

Most of the information in this report relates to the Stuxnet.A/B variant in all its slightly different packagings.

3: LNK Vulnerability

The Microsoft Windows LNK vulnerability appears evident in all versions of Windows operating systems, back to at least Windows NT 4.0. The vulnerability is related to the rendering of icons in the Windows Explorer "shell" for certain file shortcuts. It seems that when the shell renders icons for certain shortcuts, the shell activates code in the files to which the shortcuts refer. Stuxnet code is initially activated this way.

The Stuxnet worm propagates via USB mass storage media, such as USB flash sticks. The Stuxnet code is activated by viewing the Stuxnet shortcuts in Windows Explorer. On the surface, this sounds similar to many other worms which propagate via USB sticks. Those worms use the

"autorun.inf" file to trigger execution of the malware; a common protection against such worms is to instruct Windows not to run the autorun files when media is attached to USB ports or even CD drives. This autorun.inf protection does not prevent Stuxnet from running – you activate the Stuxnet code by having Windows Explorer display the Stuxnet shortcut icons.

The same vulnerability can be triggered anywhere that file shortcut icons are displayed – on the hard disk, on network shares and on WebDAV shares. More recently, there are reports that the vulnerability can be triggered by file shortcuts embedded in Microsoft Office documents, other kinds of files and even electronic mail. Other kinds of malware have also started using the LNK vulnerability to propagate.

Note: The ICS-CERT and Microsoft advisories on the LNK vulnerability are easy to misinterpret. Neither list Windows NT, Windows 2000 or Windows XP SP2 as affected by the vulnerability. The reason for the omission is that these platforms are out of support by Microsoft. The platforms are in fact affected by the vulnerability, and are still widely used in industrial control systems.

Note: The Microsoft advisory indicates that "program information files" (PIF) can be abused to trigger the execution of malware, in much the same way as LNK files can be abused. PIF files however, are not used by Stuxnet to propagate, and so are not treated in depth in this discussion of Stuxnet.

4: Stuxnet Propagation

Stuxnet moves between computers on USB sticks and via network shares. If you look at an infected USB stick on a Linux machine, or a Windows machine protected to the point where it cannot run the software on the USB stick, you will see files:

Copy of Copy of Copy of Copy of Shortcut to.lnk

Copy of Copy of Copy of Shortcut to.lnk

Copy of Copy of Shortcut to.lnk

Copy of Shortcut to.lnk

~wtr4132.tmp

~wtr4141.tmp

The LNK files are the malicious file shortcuts, all referring to "~wtr4132.tmp." The TMP files contain the code of the worm. If you attach another USB stick to a compromised machine, these files are usually copied to the stick. The version of Stuxnet Industrial Defender tested would not create these files on an empty USB stick, but would create them if the stick contained a number of other files.

Note*:* The "does not write to empty USB sticks" is not behavior you should rely on.

Once a machine is compromised, the Stuxnet worm renders the TMP and LNK files on the USB stick invisible to Windows Explorer. If you watch closely while Stuxnet compromises a machine, you may see the files briefly displayed in Windows Explorer, and then disappear a number of seconds later.

Symantec reports that Stuxnet also propagates via network shares to which the compromised machine has permission to write to. The worm is said to store a file named:

DEFRAG[random number].tmp

in the root folder of any “Admin$” share the worm finds. These shares are invisible administrative shares created by default on many file servers. To activate the TMP file on that share, the worm contacts the share server over the network and schedules execution of the TMP file, making remote use of the Windows task scheduler.

5: Evidence of Compromise

When the Stuxnet worm compromises a Windows machine, it does many things, including creating files, creating and starting services, and hiding code inside of apparently benign processes in memory. The easiest changes to identify are the creation of files:

%SystemRoot%\system32\drivers\mrxcls.sys

%SystemRoot%\system32\drivers\mrxnet.sys

%SystemRoot%\inf\oem6c.pnf

%SystemRoot%\inf\oem7a.pnf

Unlike the masked LNK and TMP files on USB sticks, these files are visible to Windows Explorer. The worm also creates two services:

MRXCLS

MRXNET

and creates a number of registry keys in:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCLS

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNET

The services, however, are not visible in the Control Panel / Administrative Tools / Services tool.

In addition, there are indications in the worm code that the worm checks for the presence of anti-virus systems on compromised equipment and may disable those systems. If a system has been compromised and owners are removing the worm, owners should check that any anti-virus protections which should be active on the machine are still working.

6: Signed Code

The mrxcls and mrxnet drivers are signed because Windows Vista prompts you if drivers you are installing are not signed with a trusted certificate, and Windows 7 refuses to install drivers which are not signed this way. Most of the Stuxnet worms circulating are signed with a RealTek certificate. Verisign has confirmed that the certificates were legitimate – they were legitimately issued to representatives of RealTek and JMicron. Both certificates have been revoked, but this only means that no new code can be signed with them, not that signatures on existing code have become invalid.

No one knows for sure how the malware came to be signed with certificates legitimately issued to these firms. There is speculation that since the firms have offices close to each other in an industrial park in Taiwan, that the theft might have been by a corporate insider in that geography. Other speculation is that the firms may have been compromised by malware of some sort which steals certificates. For example, the Zeus botnet is known to steal website certificates, but is not known to steal other kinds of certificates.

7: Network Operations

Symantec reports that once the worm has compromised a machine, it contacts a command and control (C&C) server on port 80 at DNS addresses:

www . mypremierfutbol . com

www . todaysfutbol . com

Some variants of the worm also contain hard-coded IP addresses which are identical to the IP addresses these DNS entries once resolved to. The two IP addresses involved identified two C&C servers – one in Malaysia and one in Denmark. Symantec reports that it worked with agencies to get the C&C DNS entries redirected to benign IP addresses. The benign addresses are now being used to count infected machines and to work with authorities in different countries to assist in cleaning up the infection.

Note: Symantec cautions that the Stuxnet worm is easily reconfigured to use different IP addresses and DNS entries to contact its C&C servers. No such variants have yet been identified. However, users should not be complacent because the existing versions of the worm have been frustrated in their attempts to contact a C&C server.

Symantec further reports that the worm sends basic information about the compromised host to the C&C server, including:

- Windows version information,
- Computer name,
- Network group name,
- A flag as to whether the WinCC software is installed or not, and
- IP addresses of all network interfaces.

The information is sent encrypted to the URL:

http://<C&C server address>/index.php?data=<encrypted data>

The server responds with either a command to execute a remote procedure call on the compromised host, or with a download of a new DLL for the worm to download and execute. The remote procedure calls include:

- Read a file
- Write to a file
- Delete a file
- Create a process
- Inject a .dll into lsass.exe
- Load an additional .dll file
- Inject code into other processes
- Update the configuration data for the worm

No information has been published as to whether any of these RPCs were activated on compromised hosts, or whether additional dll files have been discovered to have been downloaded to those hosts.

8: Stuxnet Targets Siemens PCS 7 Systems

Stuxnet targets Siemens WinCC components of PCS 7 control systems. Little has been published regarding what effect the worm has on such control systems.. However, a good deal has been published regarding the technologies built into the worm. In examining these technologies it becomes clear what the current version of the worm could do, even without downloading additional dll files.

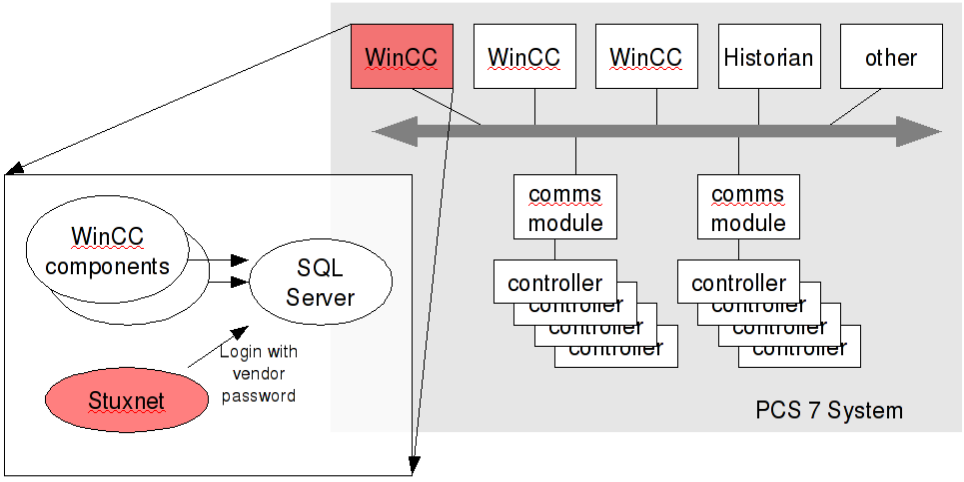

Figure 1: Siemens PCS 7 System Structure

Stuxnet targets computers running the WinCC Human / Machine Interface (HMI) components of a Siemens PCS 7 control system. In process control systems, HMIs display graphic analogues of the physical process to a plant operator, animating the graphics with the latest real-time data acquired from Programmable Logic Controllers (PLCs). The sensors and controllers in the physical process are wired into the PLCs. In addition, operators can manipulate the graphic user interface to change the physical process, for example: start pumps, close valves, increase pressures, and so on. The HMI translates those graphic manipulations into low-level commands and sends those commands to the PLCs. Note that PLCs are generally not Windows computers and so are not of themselves vulnerable to direct compromise by the Stuxnet worm.

Every WinCC component uses the Microsoft SQLServer database to store information. The database runs on the same machine as the WinCC software. The WinCC software uses a hard-coded password to access the SQLServer database. Users are not able to change this “vendor password,” since the password is embedded in the WinCC product. If users were to change the password in the SQLServer database, the WinCC components would malfunction, as they would no longer be able to contact the database.

When Stuxnet takes over a machine, it checks to see if the machine is running WinCC software. If so, the worm opens a connection to the SQLServer database on the machine using the vendor password. Frank Boldewin, the security researcher who first published that the worm targets Siemens control systems, has published SQL queries embedded in the worm. His analysis is that if those embedded queries execute, they will extract IP addresses and port numbers of other WinCC machines that are connected up in the PCS 7 system. The SQLServer database on WinCC hosts can by default accept connections from other hosts on the same network using the vendor password. There is no indication that the worm uses this capability.

Symantec has published an analysis of the worm's capabilities as well. Symantec reports that the worm contains a wrapper for the Siemens “s7otbxdx.dll”. This dll is used by WinCC to communicate with PLCs. The wrapper exports exactly as many functions as the real dll. Some of these functions simply pass control directly into the real dll without changing any data, and other functions either manipulate inputs before passing them on to the real dll, or manipulate the outputs of the real dll. The set of functions which manipulate inputs or outputs is listed below:

- s7_event
- s7ag_bub_cycl_read_create
- s7ag_bub_read_var
- s7ag_bub_write_var
- s7ag_link_in
- s7ag_read_szl
- s7ag_test
- s7blk_delete
- s7blk_findfirst
- s7blk_findnext
- s7blk_read
- s7blk_write
- s7db_close
- s7db_open
- s7ag_bub_read_var_seg
- s7ag_bub_write_var_seg

These functions are related to PLC programming. With these function wrappers, Symantec has identified Stuxnet as “the first known rootkit for SCADA devices.” Symantec and other researchers report that if a PLC program has been modified in a certain way, these wrappers act to hide the modification from users trying to examine the PLC program from a compromised Windows host. Any user looking at the PLC from a programming tool on the compromised WinCC host makes request to see the list of function blocks in the PLC, using the wrapped functions above. If the programming tool requests all the function blocks for display, but the return values from the library are modified by the wrapper to exclude the malicious function blocks, those blocks are invisible to the programming tool, and so are invisible to the user using the programming tool.

To date there have been no reports of PLC programs compromised in this way.

9: Geographic Distribution

On July 15, Kaspersky Labs, the Russian anti-virus vendor, reported over 5,000 compromised machines with a geographic distribution as follows:

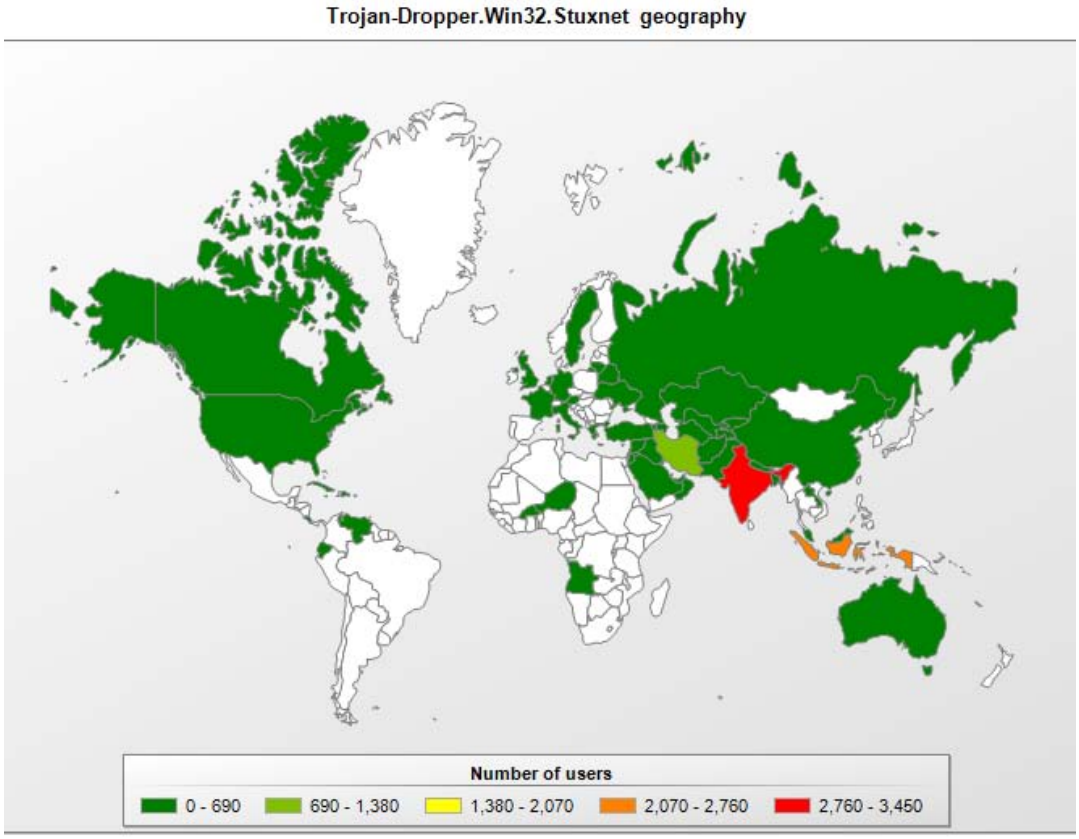

Figure 2: July 15 Kaspersky Labs Infection Data

On July 16, the Microsoft Protection Center reported detecting and rejecting infection attempts at some 1000 machines per day. Less than .02% of all machines globally, which Microsoft monitors, report infection attempts daily. Microsoft reports a significant rate of infection attempts in the USA, but when you normalize the infection attempts by the number of monitored machines in each geography, Microsoft reports infection attempts as follows:

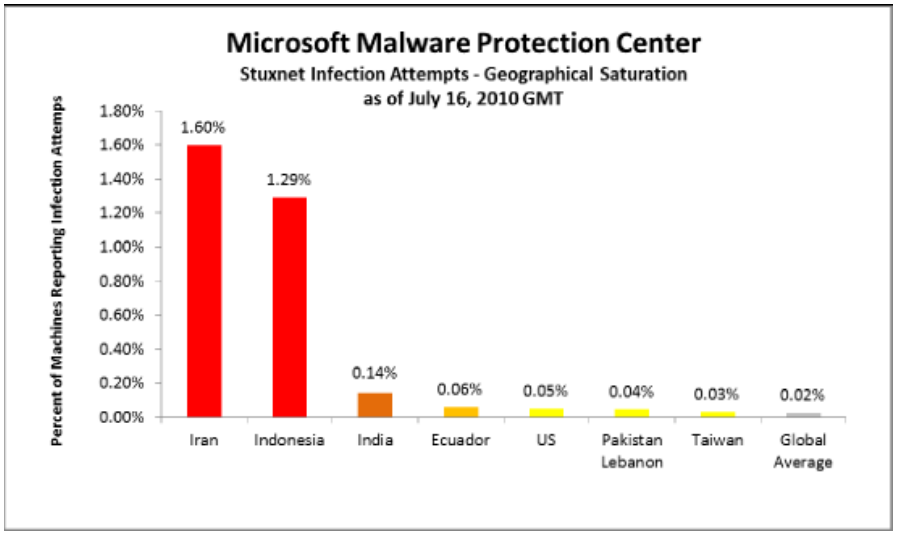

Figure 3: July 16 Microsoft Infection Attempt Data

On July 17, ESET, the French anti-virus vendor reported infections distributed geographically as follows:

United States	57.71%
Iran	30.00%
Russia	4.09%
Indonesia	3.04%
Faroe Islands	1.22%
United Kingdom	0.77%
Turkey	0.49%
Spain	0.44%
India	0.29%
Rest of the world	1.73%

Figure 4: July 18 ESET Infection Data

ESET published only these percentages, not a total count of infected machines.

On July 22, Symantec reported over 14,000 distinct IP addresses harvested from the benign IP addresses which were substituted for the real C&C servers. The geographic distribution of those addresses was as follows:

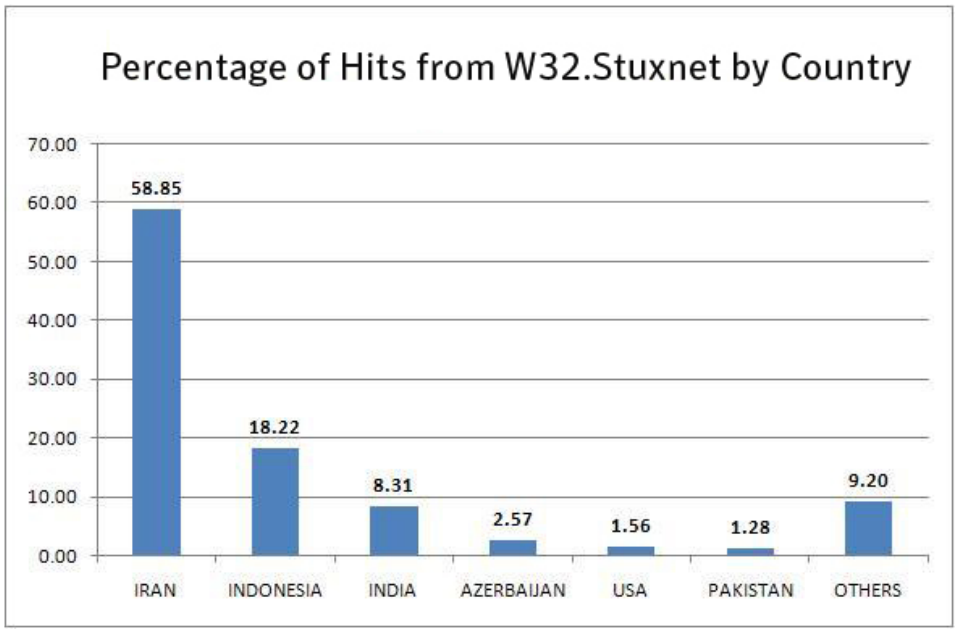

Figure 5: July 22 Symantec Compromised Host IP Address Data

The IP address data can be misleading. A compromised host can contact a C&C server only if it is on a network with connectivity to the open internet.

On July 23, Kaspersky Labs reported over 45,000 infected machines, with about 1,000 new machines being infected per day:

⊞india	18307
⊞indonesia	14010
⊞iran, islamic republic of	11952
⊞afghanistan	1592
⊞azerbaijan	1372
⊞russian federation	773
⊞uzbekistan	763
⊞malaysia	717
⊞pakistan	613
⊞tajikistan	572
⊞turkmenistan	569
⊞syrian arab republic	496
⊞kyrgyzstan	467
⊞united arab emirates	345
⊞united states	319
⊞iraq	312
⊞armenia	190
⊞kazakhstan	177
⊞saudi arabia	170
⊞germany	157

Figure 6: July 23 Kaspersky Labs Infection Data

These reports do not agree particularly well. It may be that some of the reported “infection” data was in fact “infection attempt” data. It may also be that some of the anti-virus vendors have limited installed bases in some geographies, thus skewing their statistics. To the extent that they agree, it is clear that the most-impacted countries are India, Indonesia and Iran. There is disagreement as to what extent computers in the USA were affected.

10: Remediations

Whenever the Stuxnet worm is discussed, the question “What can I do about it?” arises. For end users on home computers, the answer is simple:

- Don't worry about Stuxnet – there are so few infections in the world you are unlikely to encounter one.
- Do worry about other more widespread malware taking advantage of the LNK and PIF vulnerabilities. Make sure you have an anti-virus system installed. All credible anti-virus vendors now have signatures for the LNK and PIF vulnerabilities and many have signatures for the Stuxnet worm.
- A Microsoft patch for the LNK and PIF vulnerabilities has been available since August 2, install the patch and you should be well-protected.

For corporate networks the answer is similar, though it may take corporate IT teams a little longer to test and distribute the Microsoft patch.

For sites running industrial control systems, the question is quite a bit more involved. What you should do depends very much on how vulnerable your control systems are, how stringent your safety and availability requirements are, and what your existing security program looks like.

There is an incredible variety among control system security postures. Some systems are more or less managed like corporate IT systems – well patched, protected by anti-virus and other modern protections, with signatures updated regularly. Such systems will be protected as soon as the new anti-virus signatures make it through their site's change control processes. Other sites are running old versions of operating systems without anti-virus, and cannot patch those systems

due to the risk of causing a malfunction, or because the sites will breach the terms of their vendor support contracts. Still others run anti-virus on their older systems but do not update the signatures because they do not have a change control process in place capable of testing new signatures enough to ensure continued correct operation of the control system with new signatures in place.

Some control systems have very stringent safety and availability requirements – think nuclear sites, refineries and electric power systems. If things go catastrophically wrong at one of these sites there are significant impacts on the public at large. Such sites have very tight change control systems. Every change, however small, must be evaluated as to the risk the change poses to the correct operation of the physical process. Yes, the overall control system has many layers of redundant safety systems, and the HMI is only one of these layers, but nobody should use that as a reason to be complacent about changes to the HMI workstations.

And finally, different sites have different degrees of security programs. Some sites have programs which are well thought through, comprehensive, regularly assessed for compliance to the site security policy, and reviewed and updated as the threat environment, or available security approaches change. Other sites may have much less well thought-through programs, and unfortunately there are still some industries where control system security is still very much an afterthought, especially smaller sites.

The short story as to what industrial sites should do in light of the Stuxnet threat is easy: re-evaluate your security posture in light of this new threat. If a site does not have the expertise in-house to do this, they will need to bring in a qualified outside party. Depending on the existing security posture, sites should expect the re-evaluation to result in recommendations ranging from “don't worry, you're good already” to “you need significant improvements to your security program.” Industry experts are nearly unanimous in agreeing that the right security posture for industrial sites is a “defense-in-depth” posture, with layers of defenses including policies, procedures, training, physical security, computer security, personnel screening and many other elements. A detailed description of a defense-in-depth security program is beyond the scope of this report. Interested readers are referred to any of:

- NIST 800-82: Guide to Industrial Control Systems (ICS) Security
- ISA SP-99 Security for Industrial Automation and Control Systems – Part 1: Terminology, Concepts and Models
- Department of Homeland Security: Catalog of Control Systems Security: Recommendations for Standards Developers

In the course of re-evaluating their security posture, industrial sites may wish to consider the following remediations. Note that while the focus of this report has been the Stuxnet worm and some of the remediations below are specific to the worm, sites should consider that the worm is only one example – the first example – of an advanced threat to control systems. Industrial sites are at risk from all kinds of malware, not only Stuxnet. Even if most other kinds of malware do not target control systems specifically, such systems will still be affected by any malware which takes over a machine, affected in ways that are difficult to predict. If a site is poorly protected against run-of-the-mill malware, the site should strengthen those protections, as well as considering specific protections against the Stuxnet worm.

The following sections discuss specific remediation options.

10.1: Microsoft Patch for LNK Vulnerability

Microsoft has released a patch for the LNK and PIF vulnerabilities. Only newer versions of Windows operating systems are supported by the patch. In particular, the Windows 2000 and Windows XP SP2 versions of the operating system used heavily in industrial control systems, are

not supported. In addition, many control systems have no effective patch program or are constrained in what patches they can apply by support contracts with their control system vendors.

Sites which can apply the patch should expect to be protected against any exploit of the LNK and PIF vulnerabilities by the patch. A strong patch program generally should protect a site against much malware. Exceptions to the protections patches offer include zero-day threats, insider attacks and threats like trojans which persuade authorized users to download and run them.

10.2: Microsoft Tool to Disable Display of File Shortcuts

Microsoft has released a tool at:

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

Which disables the display of file shortcuts, thus preventing the exploit of the LNK and PIF file vulnerability. Users who have tried the tool are unanimous in their rejection of it – the tool makes Windows operating systems extremely difficult to use.

10.3: Siemens / TrendMicro Remediation Tool

Siemens has published instructions on how to use the TrendMicro “Sysclean” tool to remove the Stuxnet worm from compromised systems:

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

Note: Siemens recommends that users contact their specific support organizations before using the remediation tool. Control systems generally, PCS 7 included, tend to be highly customized. Siemens, like most responsible control systems vendors, cannot recommend that any specific change be made safely to a highly customized control system. It is only the technical people familiar with a particular customization who have the test bed and procedures to test if it is safe to apply the Siemens tool on a particular control system.

Use of the remediation tool does not protect a site from compromise by the Stuxnet worm. The tool is designed to remove the worm from a compromised machine. There are no reports yet as to the effectiveness of the tool.

10.4: Siemens Update

Siemens has issued an update to their WinCC software which:

- Modifies registry settings according to the Microsoft security advisory for the LNK and PIF vulnerabilities, and
- Tightens up SQLServer security settings, especially for client authentication.

Note: Applying this Siemens update will disable viewing of file shortcut icons just as the Microsoft tool does. This may make control system user interfaces on affected machines much harder to use.

10.5: Third Party LNK Vulnerability Avoidance Tools

Sophos and Surfright have released tools to prevent exploitation of the vulnerability without disabling most Windows icons:

http://www.sophos.com/shortcut

http://hitmanpro.wordpress.com/2010/07/30/hitman-pro-lnk-exploit-protection-released/

Feedback on the Sophos tool is that it protects against LNK exploits only when both the shortcut file and the file target are on external media. Neither tool protects against the PIF vulnerability.

10.6: Anti-Virus Tools

Control systems with anti-virus products installed and virus signatures current should already be protected against malicious shortcut files and the Stuxnet worm. Sites with anti-virus products installed but without current signatures should have a comparatively easy time of acquiring some degree of protection. New signatures need to be run through the change control system, reviewed, tested, and applied.

Sites with existing control systems lacking installed anti-virus products may not find anti-virus technology to be their best option to retrofit protection. Sites must first determine if their vendors recommend or support running their versions of control systems with anti-virus products. If the vendors support the products, the sites will need to apply a reasonably rigorous testing process to ensure that the operation of the anti-virus products does not impair the operation of their production control systems. Indiscriminate application of anti-virus products to existing control systems has historically resulted in component malfunctions and control systems failures.

Anti-virus tools will protect against Stuxnet and other known threats and vulnerabilities. However, anti-virus vendors generally do not produce signatures for a threat until between five hundred and five thousands instances of the threat are observed world-wide. Further, anti-virus vendors can only produce signatures for known threats. Thus, anti-virus tools provide good general protection, but cannot protect against previously unknown, or low-volume threats such as attacks targeted at a specific site.

10.7: Whitelisting / Host Intrusion Prevention Systems

Whitelisting or host intrusion prevention system (HIPS) products calculate a cryptographic hash for all approved executables in the filesystem on a machine. Whenever the operating system tries to load an executable file, including DLL libraries and other kinds of executables, the hash is recalculated and compared to the list of approved hashes. If there is no entry for the hash, it means the file being loaded is either not approved to execute, or has been tampered with. HIPS systems are generally configured either to issue a warning in this case and continue execution, or to block execution of the unauthorized software.

HIPS products are comparatively new technologies and a good fit for control systems. The products themselves change very slowly, unlike anti-virus systems which issue new signatures as often as several times per day. As a result, HIPS products put less of a change management burden on industrial sites. Further, HIPS products protect against even low-volume and zero-day attacks, because malware software is never on the approved list of cryptographic hashes for a protected machine.

For example: Industrial Defender labs have tested the Industrial Defender HIPS product with a live copy of the Stuxnet worm and confirmed that the HIPS product prevented compromise of the protected machine.

Timestamp	Source	Target	Description
010-08-04 13:56:20	...\~WTR4141.tmp	xp-a	Execute file denied

Figure 7: Industrial Defender HIDS Results for Stuxnet Worm

The HIPS system simply reports blocking the execution of the file "~wtr4132.tmp" every time a Windows Explorer renders icons on a compromised USB stick.

HIPS products have been criticized in enterprise applications because of the extra work required to keep the approved application list current as new patches and new software are frequently installed. This concern does not apply to most control systems. HIPS products check executables when they are loaded from disk and not all threats come from disk – threats may come from networks with buffer overflow attacks for example. HIPS products deal with such threats in part by observing that most network-based malware uses the network shell code only to pull much larger executable files on to the machine and execute them. Execution of this second stage of the malware is then blocked by the HIPS. Further, most HIPS products have one form or another of memory protection, either periodically or in real-time scanning memory for suspicious executables that did not come from disk.

Retrofitting HIPS protections onto an existing control system should be done cautiously, within the confines of a strong change control program. However, customers will likely find the slow pace of change of HIPS products to be a better fit for existing control systems than would be an anti-virus system retrofit on to those systems.

10.8: Host Intrusion Detection Systems

If a control system has host intrusion detection systems (HIDS) installed, those systems should be sufficient to alert the site to a compromise by the Stuxnet worm. Industrial sites may use HIDS as part of a defense-in-depth strategy to find out whether anything got past their other protections, or they might use HIDS on very sensitive equipment where more intrusive HIPS or anti-virus products are considered a poor fit.

Industrial Defender tested our own HIDS agents with a live Stuxnet worm and saw a burst of some 20 alerts describing unexpected changes to the control system host:

Dashboard | Incidents | System Monitor | Reports | Admin

Timestamp	Source	Target	Description
2010-05-01 14:38:27	...m32/CatRoot2/{F750E6C3-38EE-11D1-85E5...	xp-a	Modification Time
2010-05-01 14:38:26	C:/WINDOWS/system32/CatRoot2/edb.chk	xp-a	Modification Time
2010-05-01 14:37:56	[illegible]	xp-a	Process terminated
2010-05-01 14:[illegible]34	C:/WINDOWS/system32/drivers/mrxcls.sys	xp-a	File Added
2010-05-01 14[illegible]37:33	C:/WINDOWS/system32/drivers/mrxnet.sys	[illegible]p-a	File Added
2010-05-01 14:37:26	C:/WINDOWS/system32/drivers	xp-a	Modification Time
2010-05-01 14:36:57	lsass.exe	xp-a	Process started

Figure 8: Industrial Defender HIDS Results for Stuxnet Worm

The most obvious indication of Stuxnet compromise were the alerts reporting new mrxnet.sys and mrxcls.sys drivers in the system32/drivers folder, as well as the alerts reporting the creation of two new services.

HIDS products come in many shapes and sizes. Some install agents on the monitored hosts and others monitor hosts remotely. The former tend to be more powerful, since Windows facilities for remote monitoring are not as feature-rich as the on-host Windows programming environment. Further, some agents are designed to be non-intrusive, strictly throttling resource usage and running entirely in user space, while others are more profligate of machine resources and come with new kernel drivers and introduce new execution paths to all monitored software. Retrofitting HIDS on to an existing control system may be easier with remote monitoring, since even though the remote monitoring does introduce new execution paths into software on the control system host, those new paths may not be as significant as new paths introduced by host agents.

In terms of effectiveness, most modern HIDS systems should be powerful enough to detect, but not prevent, compromise by Stuxnet.

10.9: Disabling USB Keys

Many HIPS products include options to entirely disable the use of removable storage, such as USB flash sticks. Whether or not they use such technology, sites should strongly consider a policy forbidding the use of removable storage on production control system components. There is too much malware which propagates via removable storage and this makes it too easy for errors and omissions to change software on production hosts in violation of change management policies.

In addition, customers with Windows control system hosts can use Windows Software Restriction Policies (SRP) to prohibit the execution of software loaded directly from network shares or USB keys. Simply create a policy which says that software may only be loaded for execution from the machine's hard drives, and that direct execution of software from any other media is prohibited.

Such SRPs can often be retrofitted into existing control systems comparatively cheaply. They protect against malware propagating via network shares, USB flash sticks, USB hard drives and even CD/RW media. SRPs are enough to protect against propagation of the Stuxnet worm. However, SRPs do not protect against many other kinds of malware.

10.10: Strict Firewall Egress Filtering

Egress filtering is the filtering of outbound connections from a more trusted to a less trusted network. Such filtering is useful against Stuxnet and in fact against many kinds of malware, because the most powerful modern malware tends to work closely with instructions from a command and control (C&C) server. In order to contact the server, the malware must connect to an IP address on the open internet from the trusted network. If the firewall prohibits connections to random IP addresses from the trusted network, the malware does compromise the machine, but cannot receive new instructions or software updates from the C&C server. Further, if the firewall logs such communications attempts and site personnel review the logs, those personnel will be alerted to suspicious communications attempts from trusted IP addresses and can investigate those hosts for possible compromise.

Egress filtering does not prevent compromise by Stuxnet or by any malware. Egress filtering prevents malware on compromised machines from doing any more than their hard-coded instructions. Malware without contact with a C&C server cannot start doing more things or worse things to your control system than was originally programmed in the malware. Monitoring egress filtering logs provides a kind of intrusion detection as well, which can be one layer in a defense-in-depth posture.

10.11: Other Topics

There are many aspects to a strong security program. Sites re-evaluating their security posture generally, rather than specifically for this one kind of threat, may want to consider in addition measures like the following:

- Keeping a site compliant with a mature security program can add up to enough effort to keep one or more full-time security personnel busy. Consider managing or reducing those costs with a compliance management system. Such systems help a site reduce costs while still keeping their security posture strong.
- Develop, document and test a strong incident response plan. Even some of the best-protected sites will be compromised from time to time. When a site is compromised, it is important to respond quickly and correctly. Such response is only possible if it has been thought through and practiced in advance.
- Consider strong protections for control systems hosts – host hardening, patch programs, and regular vulnerability assessments.
- Consider strengthening physical security and personnel security measures at industrial sites. The authors of this malware have been refining it for some time.
- Outsource the most complex or the most time-consuming security functions to experts focused on industrial security. This lets a site's personnel remain focused on the challenging skill-set which is continued correct operation of the control system, while still supporting a strong security posture.
- And in the long term, work with control systems vendors to make clear to them what security measures will be expected in all new control systems products.

11: Conclusions

The Stuxnet worm is very unusual. It is a sophisticated piece of malware that clearly targets industrial control systems in a way that no other malware before it has. The ability of the worm to intercept, change, and hide PLC programs is of great concern, as, such changes undetected, could easily disrupt important civilian infrastructure. The best defense against threats lof this type is a strong industrial security program, which includes a defense-in-depth security posture.

Industrial Defender provides many of the technologies and services described in the "Remediations" section of this report, in an easy-to-use, integrated solution designed specifically for industrial control systems. Customers with industrial sites should never hesitate to call upon Industrial Defender to understand how we might help to improve a security program, now or in the future.

12: Links

Siemens Advisory	http://support.automation.siemens.com/WW/view/en/43876783
Hitman Pro LNK Exploit Protection	http://hitmanpro.wordpress.com/2010/07/30/hitman-pro-lnk-exploit-protection-released/
Mandiant Analysis	http://blog.mandiant.com/archives/1236
ESET Analysis	http://blog.eset.com/2010/07/19/win32stuxnet-signed-binaries
	http://blog.eset.com/2010/07/17/windows-shellshocked-or-why-win32stuxnet-sux
Microsoft Analysis and Security Update	http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx
	http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan%3AWinNT%2FStuxnet.B
	http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx
Symantec Analysis	https://www-secure.symantec.com/connect/blog-tags/w32stuxnet
Kaspersky Lab Analysis	http://www.securelist.com/en/blog?topic=199380300
Wilders Security	http://www.wilderssecurity.com/showthread.php?t=276994
Frank Boldewin	http://www.reconstructer.org/main.html
Industrial Defender Blog	http://www.findingsfromthefield.com
ICS-CERT Advisory	http://www.us-cert.gov/control_systems/pdf/ICSA-10-201-01 – USB Malware Targeting Siemens Control Software.pdf
VirusBlokAda Analysis	http://www.f-secure.com/weblog/archives/new_rootkit_en.pdf