W32.Stuxnet

Discovered: July 13, 2010
Updated: September 26, 2017 12:07:03 PM
Also Known As: Troj/Stuxnet-A [Sophos], W32/Stuxnet-B [Sophos], W32.Temphid [Symantec], WORM_STUXNET.A [Trend], Win32/Stuxnet.B [Computer Associates], Trojan-Dropper:W32/Stuxnet [F-Secure], Stuxnet [McAfee], W32/Stuxnet.A [Norman], Rootkit.Win32.Stuxnet.b [Kaspersky], Rootkit.Win32.Stuxnet.a [Kaspersky]
Type: Worm
Infection Length: Varies
Systems Affected: Windows
CVE References: CVE-2010-2568

SUMMARY

W32.Stuxnet was first categorized in July of 2010. Originally Symantec named the detection W32.Temphid based upon the information originally received but later renamed it Stuxnet to bring our naming convention in line with other vendors, and therefore virus definitions dated July 19, 2010 or earlier may detect this threat as W32.Temphid.

It targets industrial control systems in order to take control of industrial facilities, such as power plants. While the attacker's exact motives for doing so are unclear, it has been speculated that it could be for any number of reasons with the most probable intent being industrial espionage. The identities of the attackers are also unknown but there seems little doubt that regardless of their identities, they are skilled and well resourced; this wasn't something that was put together in a short period of time.

Incredibly, Stuxnet exploits four zero-day vulnerabilities, which is unprecedented.

October, 2011 - W32.Duqu, a new beginning?
Symantec received reports of a new threat (W32.Duqu) that was created from the same code base as Stuxnet. Whilst the code base was near identical, and the methods around the attacks are similar, the purpose of the new threat appears to be completely different from Stuxnet. Stuxnet was primarily designed to sabotage industrial machinery whereas Duqu appears to be designed for information theft, particularly information related to industrial systems and other secrets. This activity could be carried out with a goal to use the stolen information to plan and mount future attacks of a similar nature to those made by Stuxnet.

Symantec have analyzed this threat in detail and have made our analysis available in a report.
W32.Duqu: The precursor to the next Stuxnet

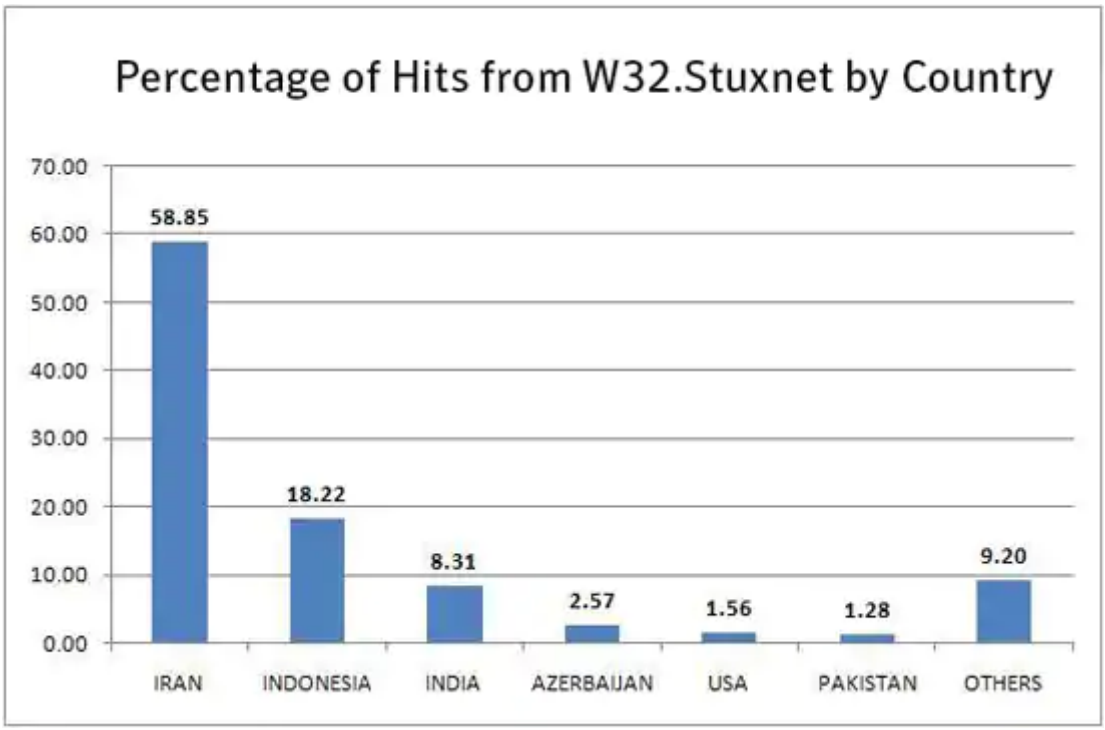
Infection
Stuxnet was the first piece of malware to exploit the Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732) in order to spread. The worm drops a copy of itself as well as a link to that copy on a removable drive. When a removable drive is attached to a system and browsed with an application that can display icons, such as Windows Explorer, the link file runs the copy of the worm. Due to a design flaw in Windows, applications that can display icons can also inadvertently run code, and in Stuxnet's case, code in the .lnk file points to a copy of the worm on the same removable drive.

Furthermore, Stuxnet also exploits the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874), which was notably used incredibly successfully by W32.Downadup (a.k.a Conficker), as well as the Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073).

The worm also attempts to spread by copying itself to network shares protected by weak passwords.

Functionality
The primary purpose of the Stuxnet worm is to take control of industrial facilities. Interestingly, one would expect the malware authors to design malware that would target only computers running the software that controls these facilities. However, like any other garden variety worm, it spreads indiscriminately using the vulnerability mentioned above.

Historic data from the early days of the Stuxnet worm attack showed that Iran, Indonesia and India accounted for the bulk of the countries where computers were targeted.



To achieve this goal, it firstly uses two different and most importantly legitimate certificates signed by well-known companies to avoid detection by antivirus applications. Once it finds its way onto a computer and exploits the .lnk vulnerability to run, it then installs a rootkit in order to hide itself on the system.

Stuxnet searches for industrial control systems, often generically (but incorrectly) known as SCADA systems, and if it finds these systems on the compromised computer, it attempts to steal code and design projects. It may also take advantage of the programming software interface to also upload its own code to the Programmable Logic Controllers (PLC), which are 'mini-computers', in an industrial control system that is typically monitored by SCADA systems. Stuxnet then hides this code, so when a programmer using a compromised computer tries to view all of the code on a PLC, they will not see the code injected by Stuxnet.

Thus, Stuxnet isn't just a rootkit that hides itself on Windows, but is the first publicly known rootkit that is able to hide injected code located on a PLC.

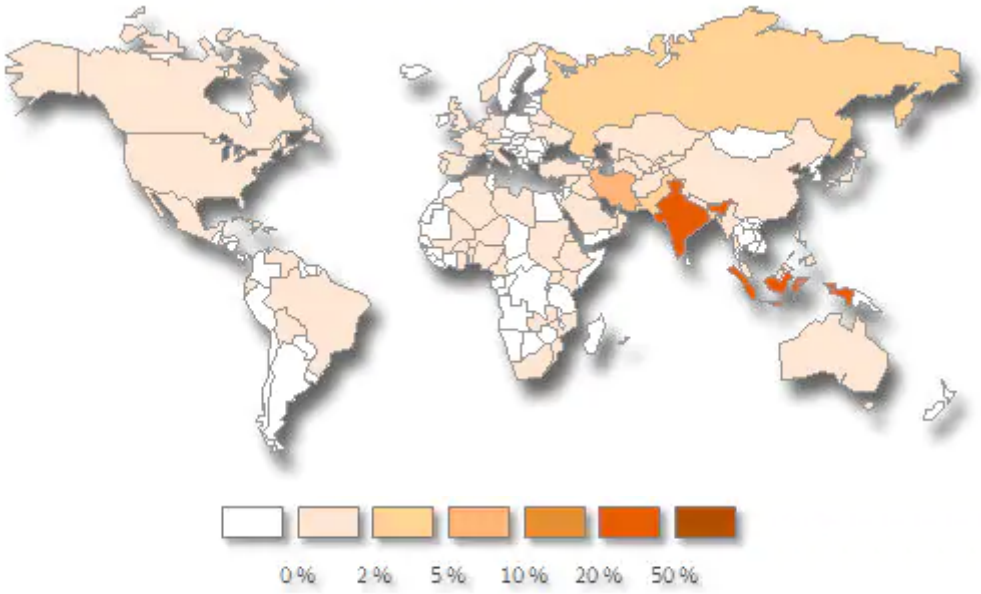
Symantec Endpoint Protection – Application and Device Control
Symantec Security Response has developed an Application and Device Control (ADC) policy for Symantec Endpoint Protection to protect against the activities associated with this threat. ADC policies are useful for reducing the risk of a threat infecting a computer, preventing the unintentional removal of data, and restricting the programs that are run on a computer.

This particular ADC policy can be used to help combat an outbreak of this threat by slowing down or eliminating its ability to spread from one computer to another. If you are experiencing an outbreak of this threat in your network, please download the policy .

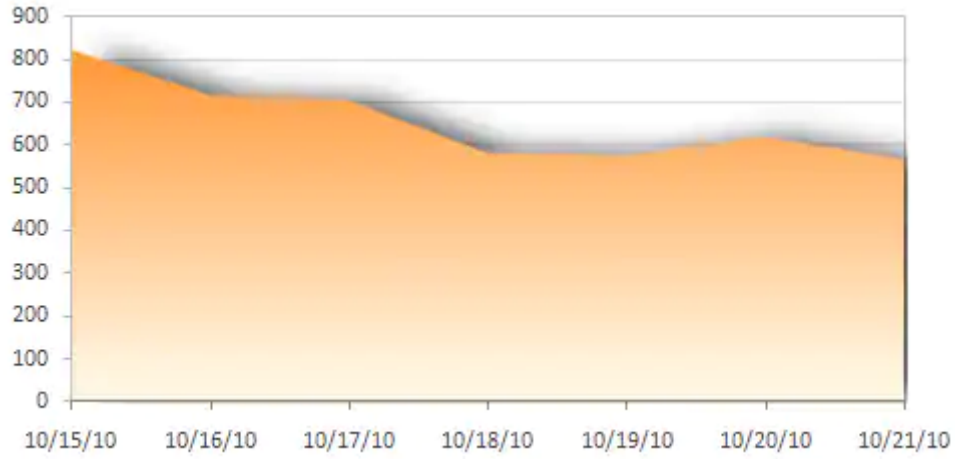
Please visit our support site for more information on ADC policies and how to manage and deploy them throughout your organization.

Note: The ADC policies developed by Security Response are recommended for use in outbreak situations. While useful in such situations, due to their restrictive nature they may cause disruptions to normal business activities.

GEOGRAPHICAL DISTRIBUTION
Symantec has observed the following geographic distribution of this threat.



PREVALENCE
Symantec has observed the following infection levels of this threat worldwide.



SYMANTEC PROTECTION SUMMARY
The following content is provided by Symantec to protect against this threat family.

Antivirus signatures
W32.Stuxnet

Antivirus (heuristic/generic)
W32.Stuxnet!lnk

Intrusion Prevention System

- HTTP W32 Stuxnet CC Activity
- HTTP W32 Stuxnet CC Activity 1

Antivirus Protection Dates

- **Initial Rapid Release version** July 13, 2010 revision 038
- **Latest Rapid Release version** August 17, 2018 revision 006
- **Initial Daily Certified version** July 13, 2010 revision 040
- **Latest Daily Certified version** August 17, 2018 revision 008
- **Initial Weekly Certified release date** July 14, 2010

Writeup By: Jarrad Shearer

TECHNICAL DESCRIPTION

1. PREVENTION AND AVOIDANCE

The following actions can be taken to avoid or minimize the risk from this threat.

1.1 User behavior and precautions

As Stuxnet spreads through removable drives, users are advised to take caution when connecting a removable drive to their computer. While this threat does not use the AutoRun feature in Windows to spread, it is a good security practice to disable this feature so that removable devices do not execute when they are inserted into a computer. It should be noted that the AutoRun feature is disabled by default for non-optical removable drives in recent versions of Windows and on systems with certain updates applied.

Removable drives should also be disconnected when not required and if write access is not required, enable the read-only mode if the option is available on the drive.

1.2 Patch operating system and software

Users are advised to ensure that their operating systems and any installed software are fully patched, and that antivirus and firewall software is up to date and operational. Users should turn on automatic updates if available, so that their computers can receive the latest patches and updates when they are made available.

This threat is known to be spread by exploiting certain vulnerabilities. Installation of the following patches will reduce the risk to your computer.

- Microsoft Security Bulletin MS10-046
- Microsoft Security Bulletin MS08-067
- Microsoft Security Bulletin MS10-061

1.3 Address blocking

Block access to the following addresses using a firewall, router, or add entries to the local hosts file to redirect the following addresses to 127.0.0.1:

- www.mypremierfutbol.com
- www.todaysfutbol.com

1.4 Network Shares and Removable Drives

This threat is also known to spread by copying itself to removable drives and inside large network by using shares, the following steps can help protect your computer against this threat.

- Users are advised to ensure that all network shares are only opened when they are necessary for use.

- Use a strong password to guard any shared folders or accounts. A strong password is a password that is of sufficient length of 8 or more characters. The password should also use a combination of numeric, capital, lowercase characters and symbols. Commonly used words from everyday language should not be used as they may easily be defeated by a dictionary attack. This blog provides some ideas on how to construct a strong yet memorable password.
- Its worth noting that while disabling the AutoRun feature will not prevent the threat from running in this case, it is good security practice to prevent dropped files from running automatically when a network drive is opened.
- Other mitigation strategies such as enabling read only or not leaving unused USB keys plugged in.

2. INFECTION METHOD

2.1 Remotely exploitable vulnerabilities

Stuxnet was the first worm to exploit the Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732) in order to spread; in fact when Stuxnet was first discovered, this vulnerability was an unknown, or zero-day, vulnerability and it wasn't until Stuxnet was analyzed that we discovered this vulnerability. Normally when one thinks of a vulnerability in software, one would think of a coding error that an attacker discovers and then exploits. However, while this does indeed fit the definition of a vulnerability, specifically it is a design flaw as Windows is doing exactly what it was designed to do.

The worm copies itself to removable drives as the following files:

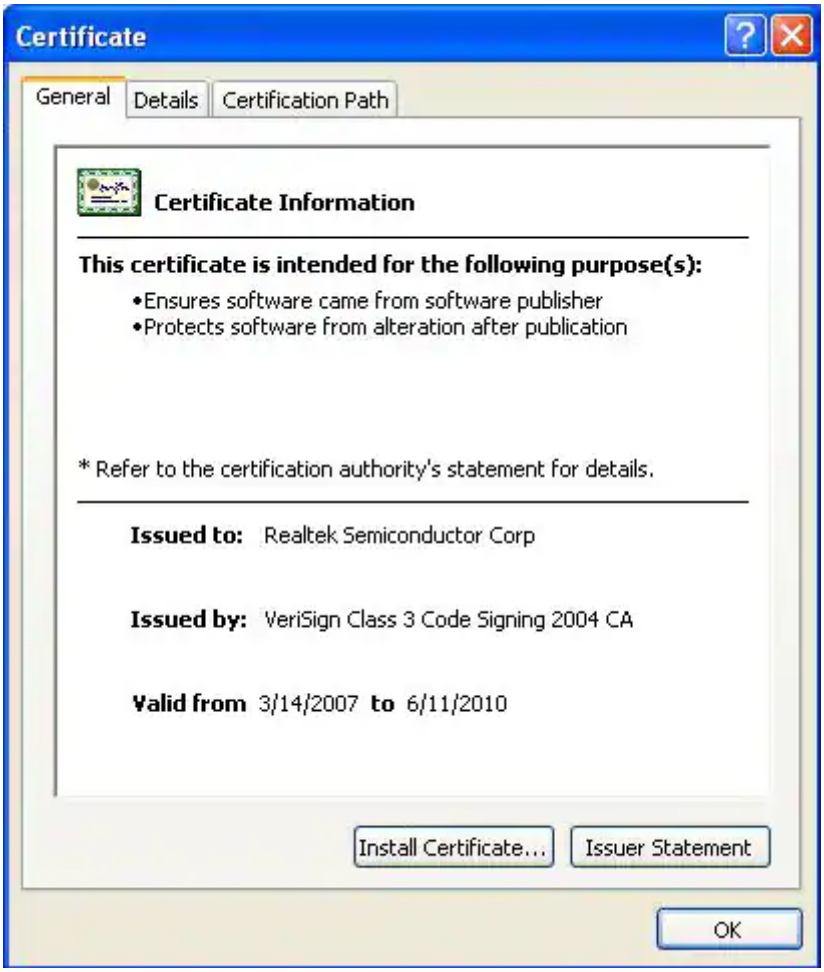
- %DriveLetter%\~WTR4132.tmp
- %DriveLetter%\~WTR4141.tmp

Note: Both file names are hardcoded and they are actually .dll files.

It also copies the following files to the above drives:

- %DriveLetter%\Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Copy of Shortcut to.lnk

When the drive is accessed by an application that can display icons, such as Windows Explorer, instead of displaying the icon for the .lnk files, it runs code that executes the file %DriveLetter%\~WTR4132.tmp. This file's main purpose is to execute the other file that is copied to the removable drive, DriveLetter%\~WTR4141.tmp, which is then loaded into memory. Its worth noting that this file has a valid signature issued to and signed by well-known companies.



It also uses a remote procedure call (RPC) exploit to spread. This exploit is only effective against computers that have not applied the patch for the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874).

Furthermore, it exploits the Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073) to copy itself from one compromised computer to another. The vulnerability allows for a file to be written to the %System% directory of a vulnerable computer. Stuxnet first uses this vulnerability to plant a copy of itself on a vulnerable machine and later it uses a feature of WBEM to achieve execution of that file on the remote computer.

2.2 Network Shares

Stuxnet also attempts to spread via network shares by copying itself to network shares as the following file: %DriveLetter%\ “DEFRAG[RANDOM NUMBER].tmp

Note: This file is in fact a .dll file.

It then attempts to create a job to run the .dll file.

3. FUNCTIONALITY

3.1 System modifications

File creation

The following file(s) may be seen on the compromised computer.

- %System%\drivers\mrxcls.sys
- %System%\drivers\mrxnet.sys
- %DriveLetter%\~WTR4132.tmp
- %DriveLetter%\~WTR4141.tmp
- %DriveLetter%\Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Shortcut to.lnk

- %DriveLetter%\Copy of Copy of Copy of Shortcut to.lnk
- %DriveLetter%\Copy of Copy of Copy of Copy of Shortcut to.lnk
- %Windir%\inf\oem6C.PNF
- %Windir%\inf\oem7A.PNF
- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\mdmeric3.PNF

File deletion
None

File modification
None

Registry entries created

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\"ImagePath" = "%System%\drivers\mrxcls.sys"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\"ImagePath" = "%System%\drivers\mrxnet.sys"

Registry subkeys/entries deleted
None

Registry subkeys/entries modified (final values given)
None

Processes

- iexplorer.exe (injection)
- lsass.exe (injection)

Installation
Once an infected removable drive is attached to a clean computer, the worm copies itself to the clean computer as the following files:
%System%\drivers\mrxcls.sys
%System%\drivers\mrxnet.sys

Next, the worm registers the file mrxcls.sys as a service with the following characteristics:
Display Name: MRXCLS
Startup Type: Automatic
Image Path: %System%\drivers\mrxcls.sys

The worm creates the following registry entry for the above service:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\"ImagePath" = "%System%\drivers\mrxcls.sys"

It also registers the file mrxnet.sys as a service with the following characteristics:
Display Name: MRXNET
Startup Type: Automatic
Image Path: %System%\drivers\mrxnet.sys

The worm creates the following registry entry for the above service:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\"ImagePath" = "%System%\drivers\mrxnet.sys"

It also creates the following files, which are encrypted copies of the worm:

- %Windir%\inf\oem6C.PNF
- %Windir%\inf\oem7A.PNF
- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\mdmeric3.PNF

The file %System%\drivers\mrxcls.sys decrypts these files to reinfect the compromised computer if attempts are made to remove the worm.

3.2 Network activity

The threat may perform the following network activities.

Downloading

The worm is able to download a payload executable on to the compromised computer from the C&C server and execute it.

Uploading

The worm sends an HTTP request to the server containing information about the compromised computer. This information is sent by making a request to the following URL:
http://[C&C SERVER ADDRESS]/index.php?data=[DATA]

Note: DATA represents the system information that has been gathered.

Other network activity

The worm contacts the following URLs through port 80, which are the worm's C&C servers, to test Internet connectivity:

- www.mypremierfutbol.com
- www.todaysfutbol.com

The data is not sent in plain text though; instead it is encrypted with XOR using a 31-byte key. The data section also contains several fields describing the data. The response received back from the C&C server is also encrypted using XOR but using a different 31-byte key. Both of these keys are contained in the malicious .dll file on the compromised computer and can be used to decipher network traffic to and from the C&C server.

The data sent from the compromised computer to the C&C server contains the following information:

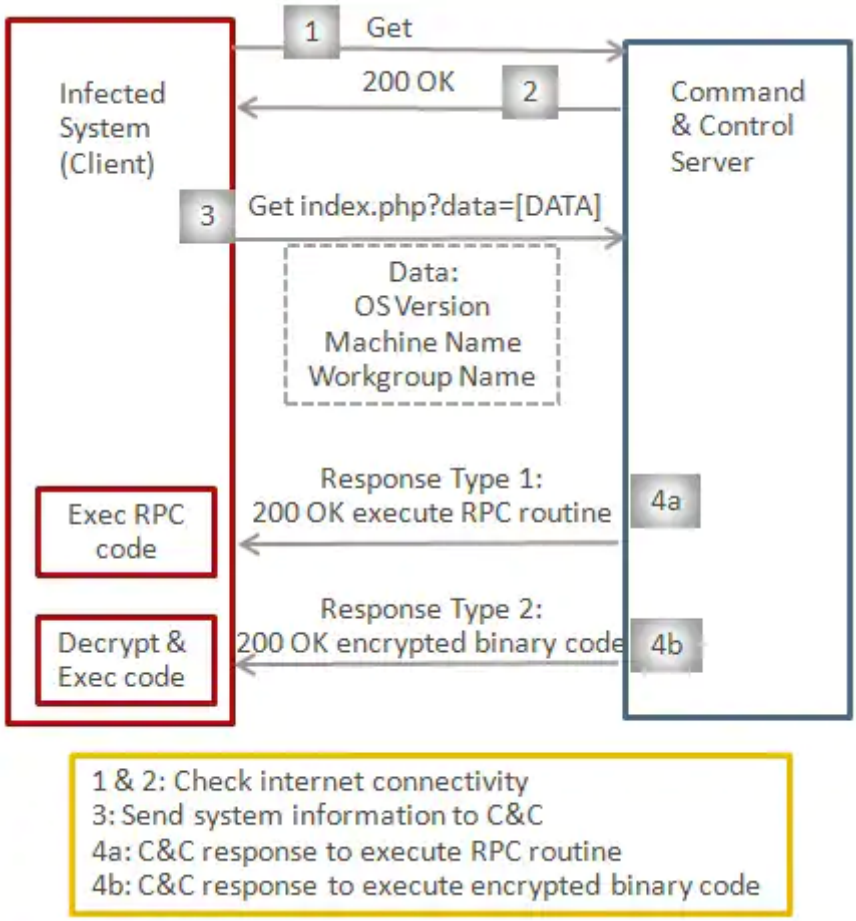
- The Windows version information
- The computer name
- The network group name
- Flag for whether SCADA software was installed or not
- IP addresses of all network interfaces

When the C&C receives this information it can reply with 2 types of responses. The first type of response instructs the threat to execute one of the procedures already existing within the threats code. In fact the data from this type of response is forwarded to various RPC routines within the main .dll file. The second type of response delivers an additional .dll file to the client in the response and instructs the client to load that .dll file and call an ordinal one from within the downloaded .dll file.

The first type of response acts as a wrapper for RPCs that will be forwarded to the local machine. The RPC calls implemented on the client side can perform the following actions:

- Read a file
- Write to a file
- Delete a file
- Create a process
- Inject a .dll into lsass.exe
- Load an additional .dll file and executed export 1
- Extract resource 210 from the main .dll file (this resource is used to inject into other processes)
- Update the configuration data for the threat

The parameters for these RPC calls are passed to the client via response type 1. For example, the .dll file to be injected into lsass.exe is passed to the client from the server inside response type 1.



3.3 Targetting SCADA software
Stuxnet is specifically targeting systems with supervisory control and data acquisition (SCADA) software installed. The threat performs many database queries on the database used by the Siemens Step 7 software and interacts with the .dll files belonging to that product. It tries to extract specific data from the database. For example, it tries to access files with the following characteristics, created by the Step 7 software:

- GracS\cc_tag.sav
- GracS\cc_alg.sav
- GracS\db_log.sav
- GracS\cc_tlg7.sav
- *.S7P
- *.MCP
- *.LDF

By accessing these files, Stuxnet steals code and design projects.

Industrial control systems consist of Programmable Logic Controllers (PLCs), which can be thought of as mini-computers that can be programmed from a Windows system. These PLCs contain special code that controls the automation of industrial processes. Programmers use software (e.g., on a Windows PC) to create code and then upload their code to the PLCs.

Stuxnet has the ability to take advantage of the programming software to also upload its own code to the PLC in an industrial control system that is typically monitored by SCADA systems. In addition, Stuxnet then hides these code blocks, so when a programmer using an infected machine tries to view all of the code blocks on a PLC, they will not see the code injected by Stuxnet. Thus, Stuxnet isn't just a rootkit that hides itself on Windows, but is the first publicly known rootkit that is able to hide injected code located on a PLC.

In particular, Stuxnet hooks the programming software, which means that when someone uses the software to view code blocks on the PLC, the injected blocks are nowhere to be found. This is done by hooking enumeration, read, and write functions so that you can't accidentally overwrite the hidden blocks as well. Thus Stuxnet introduces the first known rootkit for industrial control systems.

By writing code to the PLC, Stuxnet can potentially control or alter how the system operates. To date, no industrial facility has been knowingly compromised. What any attacker hopes to achieve by compromising an industrial facility is not known, but one thing is for sure: nothing good can come from a facility being

compromised.

3.4 Rootkit functionality
In an attempt to avoid detection the file %DriveLetter%\~WTR4132.tmp hides threat related files by hooking the following APIs from kernel32.dll and Ntdll.dll:
From Kernel32.dll

- FindFirstFileW
- FindNextFileW
- FindFirstFileExW

From Ntdll.dll

- NtQueryDirectoryFile
- ZwQueryDirectoryFile

It replaces the original code for these functions with code that checks for files with the following properties:

- File names ending with ".lnk"
- File names beginning with "~WTR" and ending in ".tmp" (which explains why the file names on the removable drive are hardcoded and cannot change significantly)

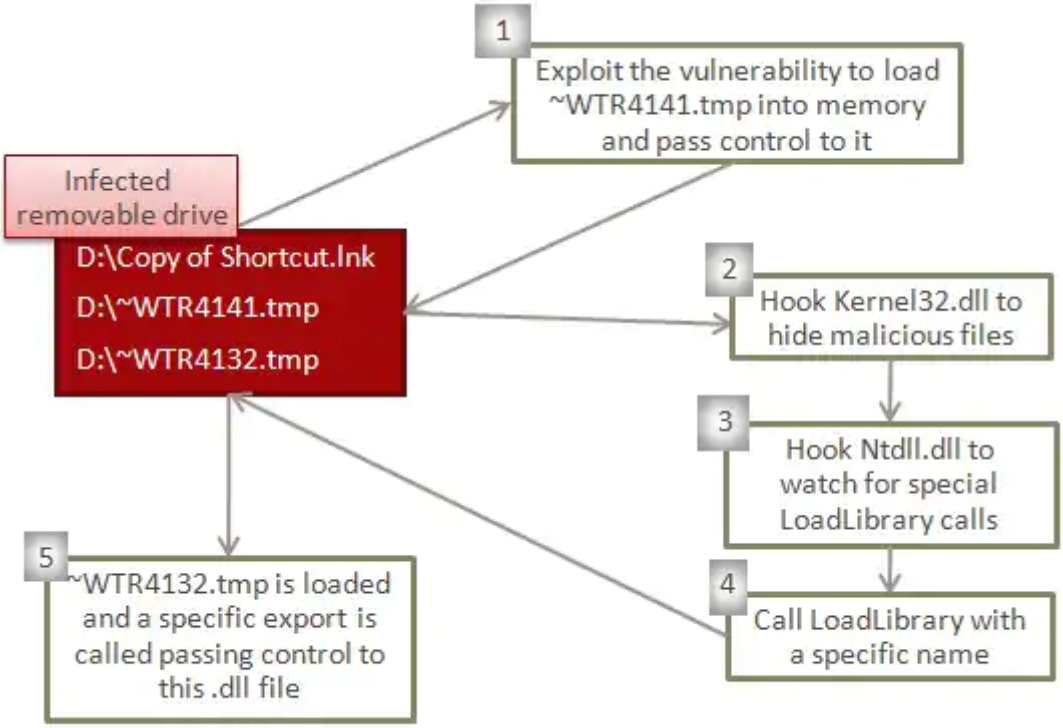
If a request is made to list a file with the above properties, the response from these APIs is altered to state that the file does not exist, thereby hiding all files with those properties.

After the kernel32.dll APIs are hooked, the file %DriveLetter%\~WTR4132.tmp loads the other .dll file, %DriveLetter%\~WTR4141.tmp. However, to achieve this Stuxnet uses a different approach from what one would normally expect. Rather than calling the "LoadLibrary" API to load a .dll file into memory, which is what one would normally expect, Stuxnet hooks certain Ntdll.dll functions, then calls the “LoadLibrary” with a specially crafted file name. The file requested to be loaded does not exist on disk, therefore normally LoadLibrary would fail. However, W32.Stuxnet has hooked Ntdll.dll to monitor for requests to load specially crafted file names. If a specially crafted file name is encountered, the hooked ntdll.dll functions know to load a .dll file from another location instead; a location specified by Stuxnet and that location is generally an area in memory where a .dll file has been decrypted and stored by the threat previously.

The functions hooked for this purpose in Ntdll.dll are:

- ZwMapViewOfSection
- ZwCreateSection
- ZwOpenFile
- ZwCloseFile
- ZwQueryAttributesFile
- ZwQuerySection

Once a .dll file has been loaded, GetProcAddress is used to find the address of a specific export from the .dll file and that export is called, handing control to that new .dll file.



3.5 Additional functionality

Lowering security settings
It injects its code into iexplorer.exe in order to bypass firewalls.

Next, it ends the following security-related processes:

- vp.exe
- Mcshield.exe
- avguard.exe
- bdagent.exe
- UmxCfg.exe
- fsdfwd.exe,
- rtvscan.exe
- ccSvcHst.exe
- ekrn.exe
- tmpproxy.exe

4. ADDITIONAL INFORMATION
For more information relating to this threat family, please see the following resource:
Blog entries on W32.Stuxnet
W32.Stuxnet Dossier (White paper - September, 2010)
W32.Stuxnet Timeline (Infographic - June, 2011)
Stuxnet 0.5 – The Missing Link (Video - February, 2013)
Stuxnet 0.5: The Missing Link (White paper - February, 2013)

Recommendations

Writeup By: Jarrad Shearer

REMOVAL

You may have arrived at this page either because you have been alerted by your Symantec product about this risk, or you are concerned that your computer has been affected by this risk.

Before proceeding further we recommend that you run a full system scan . If that does not resolve the problem you can try one of the options available below.

FOR NORTON USERS
If you are a Norton product user, we recommend you try the following resources to remove this risk.

Removal Tool

- Run Norton Power Eraser (NPE)
- Norton Power Eraser did not remove this risk

If you have an infected Windows system file, you may need to replace them using from the Windows installation CD .

How to reduce the risk of infection
The following resources provide further information and best practices to help reduce the risk of infection.

- Operating system updates to fix vulnerabilities
- File sharing protection
- Disable Autorun (CD/USB)
- Best practices for instant messaging
- Best practices for browsing the Web
- Best practices for email

FOR BUSINESS USERS
If you are a Symantec business product user, we recommend you try the following resources to remove this risk.

Identifying and submitting suspect files
Submitting suspicious files to Symantec allows us to ensure that our protection capabilities keep up with the ever-changing threat landscape. Submitted files are analyzed by Symantec Security Response and, where necessary, updated definitions are immediately distributed through LiveUpdate™ to all Symantec end points. This ensures that other computers nearby are protected from attack. The following resources may help in identifying suspicious files for submission to Symantec.

- Locate a sample of a threat
- Submit a suspicious file to Symantec

Removal Tool

- Run Symantec Power Eraser in Symantec Help (SymHelp)
- About Symantec Power Eraser
- Symantec Power Eraser User Guide

If you have an infected Windows system file, you may need to replace them using from the Windows installation CD .

How to reduce the risk of infection
The following resource provides further information and best practices to help reduce the risk of infection.
Protecting your business network

Use SEP's Application and Device Control (ADC) feature to block Stuxnet infections
SEP's ADC can help to prevent the spread of Stuxnet. A policy file is available which will block actions carried out by the threat.

Specifically, the policy will monitor for access to .lnk files by all processes in the following locations:

- Removable drives
- CD/DVD drive
- Network drives
- RAM drives

Note: Create/write/delete operations are allowed but logged.

The following process is permitted to read .lnk files:

- rtvscan.exe

Whenever a process action is blocked by this policy, the user is alerted with the following message:
See 'Vulnerability in Windows Shell Could Allow Remote Code Execution' (see Microsoft Security Advisory 2286198 for further information).

MANUAL REMOVAL
The following instructions pertain to all current Symantec antivirus products.

1. Performing a full system scan
How to run a full system scan using your Symantec product

2. Restoring settings in the registry
Many risks make modifications to the registry, which could impact the functionality or performance of the compromised computer. While many of these modifications can be restored through various Windows components, it may be necessary to edit the registry. See in the Technical Details of this writeup for information about which registry keys were created or modified. Delete registry subkeys and entries created by the risk and return all modified registry entries to their previous values.

Writeup By: Jarrad Shearer