Antiy Labs

Report on the Worm Stuxnet's Attack

Antiy CERT

Antiy Labs

(October 2010)

Contents

Background of the Attack

Recently, numerous news media have reported incidence about Stuxnet worm. Described as "super weapon", "Pandora's Box", it has attacked the SIMATIC WinCC SCADA system of Siemens.

The Stuxnet worm erupted in July this year. It utilizes at least four vulnerabilities of Microsoft operating system, including three new zero-day vulnerabilities; uses digital signature for its generated drivers; breaks through the physical limitations of industry-specific LAN(local area network) through various ways of invasion for mass spread out; and carries out a devastating attack by exploiting two vulnerabilities in WinCC system. It is the first malicious code that damages the industrial infrastructures directly. According to Symantec's statistics, about 45,000 networks around the world have been infected with the worm so far, and 60% of the victim hosts are in Iran. Iranian government has confirmed that the country's Bushehr nuclear power plant has been attacked by Stuxnet.

On July 15, Antiy labs captured the first variant of the Stuxnet worm and conducted an immediate analysis, publishing the corresponding report and preventive proposal instantly as well as keep tracking on them. By now, Antiy Labs has captured 13 variations, and 600+ samples with different hash values.

Behavior Analysis

Running Environment

Stuxnet can be activated in the following operating systems:

- Windows 2000、Windows Server 2000
- Windows XP、Windows Server 2003
- Windows Vista
- Windows 7、Windows Server 2008

Stuxnet exits immediately if the current operating environment is not the Windows NT families.

The attacked software targets include:

- SIMATIC WinCC 7.0
- SIMATIC WinCC 6.2

However, it doesn't mean that other versions of the WinCC can be ruled out from the target.

Local Behavior

When the sample is activated, its running process is shown in Figure 1.

First of all, the sample gets the version of current OS. It will exit when detecting itself running on Windows 9X/ME.

Next, the sample will load a DLL module, in which most codes to be executed are included. In order to prevent being scanned or killed, the sample copies the DLL module into memory directly and simulates the regular DLL loading style, rather than dumps the DLL module into a file and loads it.

In fact, the sample allocates enough memory space, and then hooks six system-level APIs which exported from the ntdll.dll:

- ZwMapViewOfSection
- ZwCreateSection
- ZwOpenFile
- ZwClose
- ZwQueryAttributesFile
- ZwQuerySection

In order to hook them, the sample modifies the security parameters of PE header from ntdll.dll module into its process's memory space, and then moves the valid data at offset 0x40b into jump code.

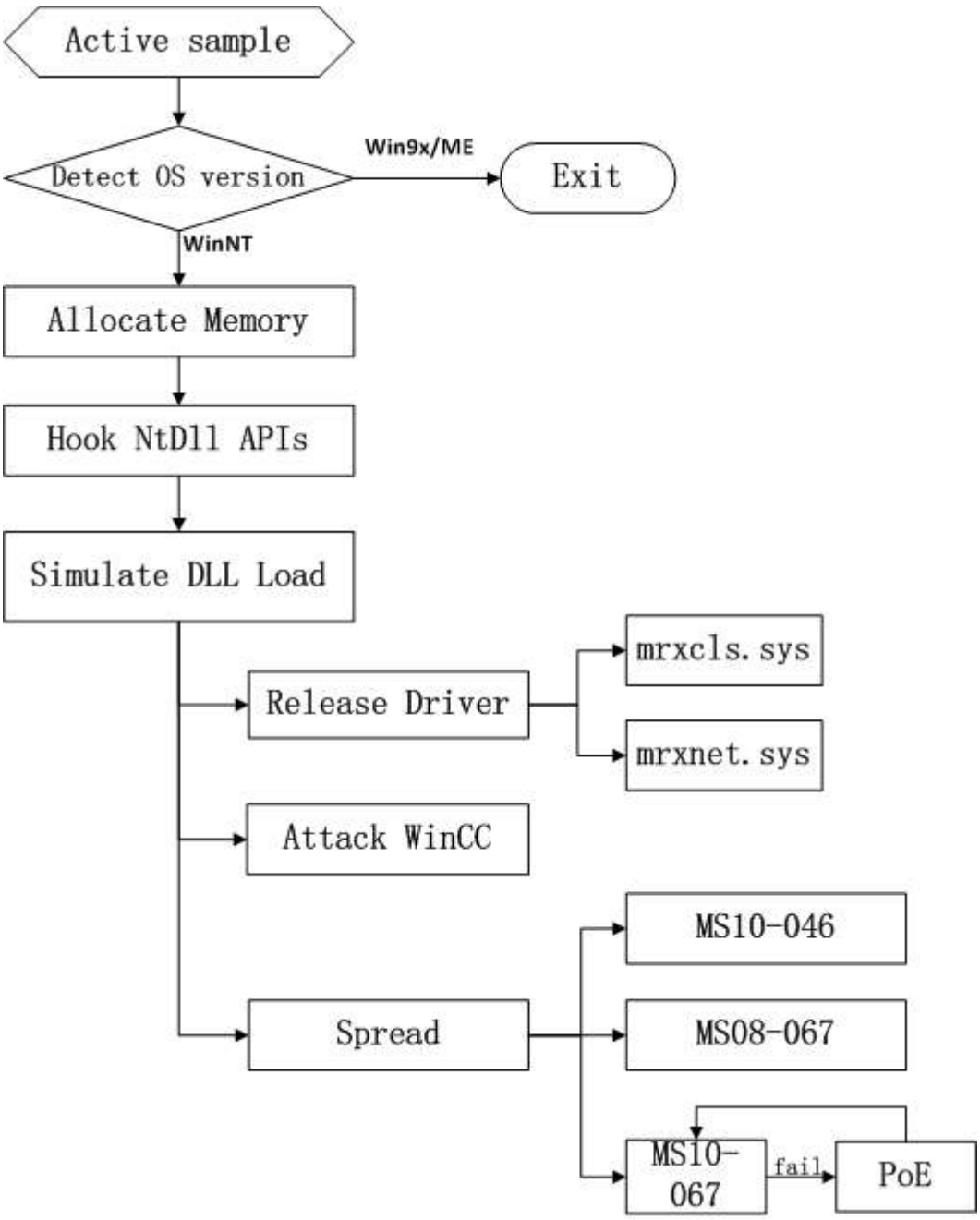

Figure 1 Sample's typical running process

Then, the sample will create a new PE section in memory space through modified API ZwCreateSection, and copies the DLL module into it. Finally, it gets the module handle through LoadLibraryW API.

Thereafter, the sample jumps into loaded DLL to execute, and generates the following files:

- %System32%\drivers\mrxcls.sys
- %System32%\drivers\mrxnet.sys

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

In addition, the two drivers of mrxcls.sys and mrxnet.sys are registeredd as two system services with the name of MRXCLS and MRXNET, to make sure the attack payload could start with the system startups. Both of two drivers use Rootkit technology, and rogue digital signatures.

The former one attacks WinCC system, and the other one hides some critical files in the kernel-level, such as some LNK files and DLL files which are copied into flash disks.

The driver mrxcls.sys will check if host has been installed WinCC system. In fact, it could monitor almost all of the processes environments, and then inject a module stored in %Windir\inf\oem7A.PNF into three processes: services.exe, S7tgtopx.exe, and CCProjectMgr.exe. As approved, S7tgtopx.exe and CCProjectMgr.exe are belongs to WinCC system natively.

In other way, the driver mrxnet.sys will try to hide .lnk files and DLL files which could be copied to flash disk by modifying some kernel-mode system calls. (See Figure 2)

```
loc_11703:                              ; CODE XREF: sub_11688+6A↑j
cmp     esi, 4
jle     short loc_1171D
push    4
lea     eax, [ebx+esi*2-8]
push    eax
mov     eax, offset a_lnk       ; ".LNK"
call    sub_114DA
test    al, al
jnz     short loc_1172F
```

Figure 2 The driver will hide some lnk files

Spread Method

The target of Stuxnet worms is the SIMATIC WinCC software, which is mainly used in the data acquisition and monitoring inindustrial control system. It is usually installed in special Intranet, which is isolated physically from the Internet. In order to begin the attack, Stuxnet uses various methods to start its penetration and spread out, shown in Figure 3.

Firstly, Stuxnet infects the external host. Secondly, it infects flash disk, and then penetrates into the Intranet by exploiting shortcut (".lnk") file parsing vulnerability (MS10-046). If succeeded, it attempts to infect more hosts by exploiting the shortcut file parsing vulnerability (MS10-046), RPC remote execution vulnerability (MS10-061), and the print spooler service vulnerability (MS10-061). Finally, it reaches the hosts which is suitable and confirmed to install the WinCC system and then attack them.

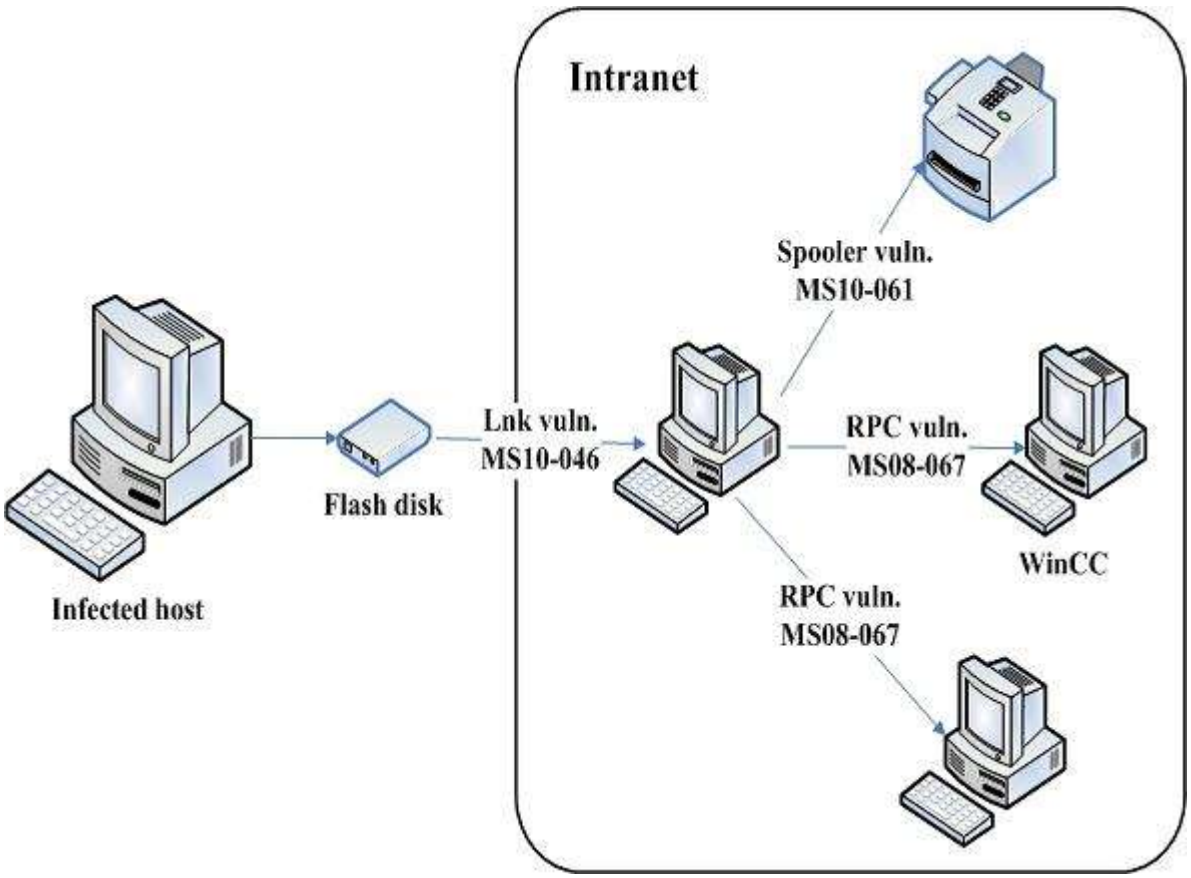

Figure 3 Stuxnet's spread method

Shortcut File Parsing Vulnerability (MS10-046)

Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer, as demonstrated in the wild in July 2010, and originally reported for malware that leverages CVE-2010-2772 in Siemens WinCC SCADA systems.

This vulnerability can be exploited through removable drives with a malicious shortcut file and an associated malicious binary. It can also be exploited by placing the malicious components in a malicious website or a remote network share.

If activated, it will automatically search the needed icon resource according to the file structure and be presented as the icon. If the icon resource is packaged into a DLL file, the system will load this DLL file. Therefore, an attacker can build a malicious shortcut file which could get the system to load the specified DLL files. And then the malicious code can be executed. Because the display of a shortcut file is executed by the system automatically, with no any interaction with users, the damage of exploits is bigger than others.

Stuxnet searches the removable storage devices in the computer (shown as Figure 4). While finding the device, it will copy the shortcut file and DLL files into it (as shown in Figure 5). If the user uses this device in the internal network, the related vulnerability is triggered, and then it makes the attack so-called "ferry" real, that is, successfully penetrate into the physically isolated network with the help of the dangerous removable storage devices.

```
MOV EBX,Region00.10061B30   {53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
PUSH Region00.10061A80      storage#volume#
MOV EDI,Region00.10061A0C   \\.\
MOV EBP,Region00.10061BCC   %s%s%s#%s
PUSH Region00.10061AA0      storage#volume#1&19f7e59c&0&
PUSH Region00.10061A4C      storage#removablemedia#8&
MOV EBP,Region00.10061BE0   %s%s%x&0&rm#%s
PUSH Region00.10061A18      storage#removablemedia#7&
```

Figure 4 Figure 4 Search flash disk

There are two DLL files copied to flash disk: ~wtr4132.tmp and ~wtr4141.tmp (Figure 5). The last one hooks some APIs in kernel32.dll and ntdll.dll as follow:

- FindFirstFileW
- FindNextFileW
- FindFirstFileExW
- NtQueryDirectoryFile
- ZwQueryDirectoryFile

It hooks these APIs in order to hide the LNK files and DLL files in flash disk. Now we can conclude that Stuxnet using two ways to hide flash disk files. The one is using kernel mode driver, the other one is hook APIs in user mode.

```
PUSH Region00.100618A4      copy of shortcut to.lnk
PUSH Region00.100618D4      copy of
PUSH Region00.100618E8      ~wtr4141.tmp
PUSH Region00.10061904      ~wtr4132.tmp
PUSH Region00.1005CD1C      *
PUSH Region00.100618E8      ~wtr4141.tmp
PUSH Region00.10061904      ~wtr4132.tmp
PUSH Region00.1005CD20      global\wkssvcshutdownevent2
PUSH Region00.100618E8      ~wtr4141.tmp
PUSH Reqion00.10061904      ~wtr4132.tmp
```

Figure 5 Copy files to flash disk

RPC remote execution vulnerability (MS08-067), and privilege escalation vulnerability

This is the most critical vulnerability of Microsoft operating system in 2008, featured with these followed: simple, widely spread, highly damaged, etc.

```
PUSH Region00.10061C74          ncalrpc:[%s]
PUSH Region00.10061CE0          ncacn_ip_tcp:%s[%u]
PUSH Region00.10061C10          ntsvcs
MOV EBX,Region00.10061C00       browser
PUSH Region00.10061D30          ncacn_ip_tcp
PUSH Region00.10061D08          ncacn_ip_tcp:%s[%s]
PUSH Region00.1005C3FA          h
PUSH Region00.1005C422          h
PUSH Region00.1005C462          h
PUSH Region00.1005C490          h
PUSH Region00.1005C4BE          h
PUSH Region00.1005C5B0          h
PUSH Region00.10061C90          ncacn_np:%s[\\pipe\\%s]
PUSH Region00.10061CC0          ncacn_ip_tcp:%s
```

Figure 6 Start RPC exploit

Specifically, it is possible to allow remote code execution when the system with this vulnerability receives the constructed RPC requests. In Windows 2000, Windows XP and Windows Server 2003, the attacker could attack directly through build a malicious network packet to exploit this vulnerability, execute the attack load with no any authentications, and then get the root access. Therefore, the vulnerability is most probably used by typical worms for the large-scale spread of and attacks.

Stuxnet worms spread into the Intranet by exploiting this vulnerability (Figure 6). With help of this vulnerability, it fails just because the privilege is not sufficient, it will use an unknown and unpatched privilege escalation vulnerability (Figure 1), and then try to attack again. By now, Microsoft has not offered any solution to this vulnerability.

Print Spooler Service Vulnerability (MS10-061)

It is a critical vulnerability in the Windows Print Spooler service on Windows 2008/7/Vista/2003/XP computers, which allows arbitrary code to be remotely executed in the vulnerable computer.

If exploited successfully, MS10-061 allows hackers to gain remote control of the affected computer with the same privileges as the logged on user. If this user had administrator rights, the hacker could take complete control of the system: create, modify or delete files, install programs, create new user accounts, etc.

This vulnerability is usually exploited by sending a specially crafted print request to a vulnerable system that has a print spooler interface exposed over RPC.

Windows print spooler does not set user privileges reasonably. An attacker can submit a crafted print request to send the file to %System32% directory of the hosts which expose the print spooler interface. Arbitrary code can be executed successfully with system privileges exploiting this vulnerability, in order to achieve spread and attacks.

Stuxnet worms use this vulnerability to achieve the spread in Intranet. As shown in Figure 7, it sends two files to target host: winsta.exe and sysnullevnt.mof. The sysnullevnt.mof is a Managed Object Format file of Microsoft. It will execute winsta.exe when some events occur. Otherwise, winsta.exe is just the Stuxnet worm itself.

```
MOV EAX,DWORD PTR SS:[EBP+C]
MOV ECX,DWORD PTR SS:[EBP+10]
MOV DWORD PTR DS:[EBX+4],EAX
MOV DWORD PTR DS:[EBX+8],222———?1001681C     winsta.exe
MOV DWORD PTR DS:[EBX+C],ECX
MOV DWORD PTR DS:[EBX+14],222———?100177A8
MOV DWORD PTR DS:[EBX+18],222———?10016834    wbem\mof\sysnullevnt.mof
MOV DWORD PTR DS:[EBX+1C],63A
CALL 222———?10006070
```

Figure 7 Exploit print spooler vulnerability

Attack Behavior

Stuxnet query two registry key values to check whether the targeted hosts have installed WinCC system or not (Figure 8):

- HKLM\SOFTWARE\SIEMENS\WinCC\Setup
- HKLM\SOFTWARE\SIEMENS\STEP7

```
53 00 4F 00 46 00 54 00 57 00 41 00 52 00 45 00 S.O.F.T.W.A.R.E.
5C 00 53 00 49 00 45 00 4D 00 45 00 4E 00 53 00 \.S.I.E.M.E.N.S.
5C 00 57 00 69 00 6E 00 43 00 43 00 5C 00 53 00 \.W.i.n.C.C.\.S.
65 00 74 00 75 00 70 00 00 00 00 00 53 00 54 00 e.t.u.p.....S.T.
45 00 50 00 37 00 5F 00 56 00 65 00 72 00 73 00 E.P.7._.V.e.r.s.
69 00 6F 00 6E 00 00 00 53 00 4F 00 46 00 54 00 i.o.n...S.O.F.T.
57 00 41 00 52 00 45 00 5C 00 53 00 49 00 45 00 W.A.R.E.\.S.I.E.
4D 00 45 00 4E 00 53 00 5C 00 53 00 54 00 45 00 M.E.N.S.\.S.T.E.
50 00 37 00 00 00 00 00 00 00 00 00 53 00 4F 00 P.7.........S.O.
```

Figure 8 Query registry for WinCC

Stuxnet uses two vulnerabilities in the WinCC system.

The first one is a hard-coded problem in WinCC system, which saves a default account and password to access the database. Stuxnet uses this vulnerability to access the SQL database of the system (as shown in Figure 9).

The other one is a bug on the DLL loading strategy when opening the project file in the Step7 project which WinCC needs to use. The bug can result in an exploiting pattern similar with "DLL pre-loaded attack". Finally, Stuxnet achieves to hook some query functions and reading function by replacing a DLL file in Step7 software.

```
declare @t varchar(4000), @e int, @f int if exists (select text from dbo
declare @t varchar(4000), @e int, @f int if exists (select * from dbo.sy
use master
.mdf
select name from master..sysdatabases where filename like n'%s'
.mdf
.ldf
exec master..sp_attach_db 'wincc_svr',n'%s',n'%s'
exec master..sp_detach_db 'wincc_svr'
use wincc_svr
exec master..sp_detach_db 'wincc_svr'
.mdf
.ldf
 ((select top 1 1 from mcpvreadvarpercon)='1') --cc-sp
x
0
.mdf
.mdf
vector<t> too long
2wsxcder
winccconnect
master
.\wincc
sqloledb
provider='%s';data source=%s;initial catalog='%s';user id='%s';password=
```

Figure 9 Query WinCC database

Generation Relationship

As mentioned above, many worm variants have been captured. What are the general and specific characters of them in copying, distributing, attacking and derived files?

As Figure 10 shows, there are several possible sources of the samples.

The original samples or the samples which were exploiting the RPC vulnerability or the print spooler services vulnerability are all exe files. They load a module in their own .stud section invisibly, named "kernel32.dll.aslr.<random number>.dll".

Other samples, which are spreaded through flash disk, have been exploiting the vulnerability as soon as the system displays the shortcut file. As a result, ~wtr4141.tmp file is loaded. The tmp file loads a file named "shell32.dll.aslr.< random number >.dll" module. This module will load another file ~ wtr4132.tmp as "kernel32.dll.aslr.<random number>.dll".

The module "kernel32.dll.aslr.<random number>.dll" will start up to finish the following operations. It exports 22 functions to complete the main function about malicious code. Its resource section contains a bunch of files to be derived, which are stored in encrypted form.

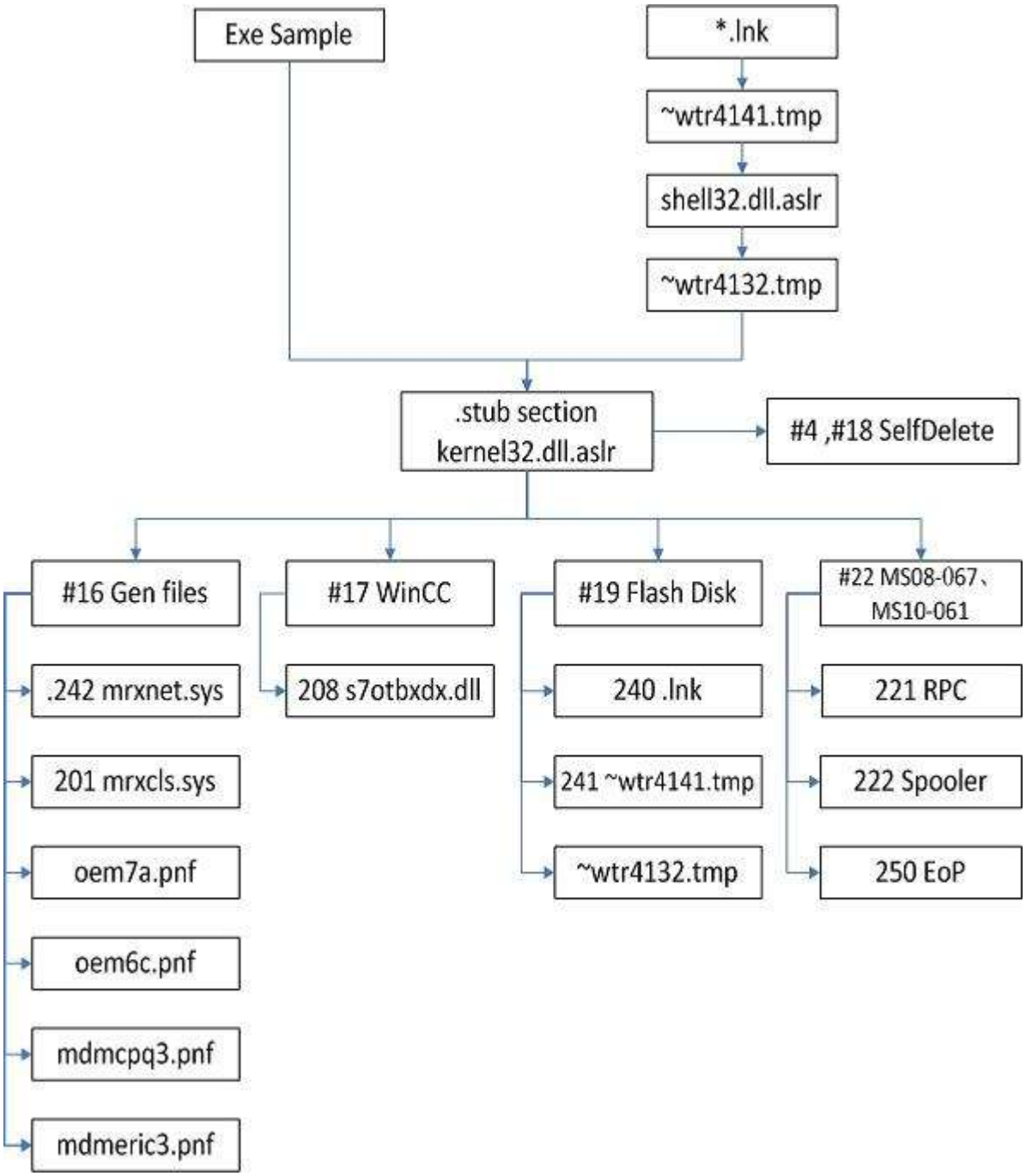

Figure 10 Generation Relationship

As shown, the No.16 exported function is used for the derivative of local files, including resources No.201 mrxcls.sys and No.242 mrxnet.sys drivers, and four .pnf files.

No. 17 exported function is used to attack the second vulnerability of WinCC system, it releases s7otbxdx.dll, the same name files in the WinCC system are modified to s7otbxsx.dll, and derived functions of this document are to be conducted a package, in order to hook APIs.

No.19 exported function is used to spread by the shortcut file parsing vulnerability. It generates some .lnk files and two .tmp files.

No.22 derived function is responsible for RPC vulnerability and print spooler service vulnerability to spread. Among the files it generates, resources No.221 is used to exploit RPC vulnerability, resources No.222 is used to attack print spooler service, and resources No.250 is used to escalate privilege.

Solutions and Proposals

Attack Prevention

Siemens has offered normal solution on this attack. The URL is given in Appendix section. We have provided the following removal solutions according to our analysis.

Scan and Kill Stuxnet by Relevant Tools or Manually

Steps of killing this worm manually are as follow:

1. Use the Antiy Atool to terminate all of lsass.exe process whose parent process is not winlogon.exe;
2. Delete the following derivative files forcibly:
   - %System32%\drivers\mrxcls.sys
   - %System32%\drivers\mrxnet.sys
   - %Windir%\inf\oem7A.PNF
   - %Windir%\inf\mdmeric3.PNF
   - %Windir%\inf\mdmcpq3.PNF
   - %Windir%\inf\oem6C.PNF
3. Delete the following registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNET

Install the following patches provided by Microsoft:

- RPC remote execution vulnerability (MS08-067)
- Shortcut file parsing vulnerability (MS10-046)
- Print spooler service vulnerability (MS10-061)

In addition, users should pay attention to the unpatched privilege escalation vulnerability, and another similar vulnerability found by Microsoft recently. Users should always keep the latest security events informed.

Install the Software Patches

Install the latest WinCC patches released by Siemens, please see the appendix part.

Proposals on Security

This significant attack has taught us that:

- It could be hacked even the targeted network are totally physical-isolated;
- The private software systems could most likely be attacked, including industrial control systems as the next upcoming targets.

Therefore, some proposals are offered to the relevant departments and enterprises as following:

- Strengthening hosts' defense (in particular the host in the Intranet) by updating the operating system patches wherever the computers are located in public area or fully physically isolated.
- Firewall and antivirus software best practices and standard default security configurations could help protecting network resources from attacks that originate outside the network perimeter.
- Build software security awareness, keep tracking of the software security issues of the critical computers and keep the software updated always;
- Best practices recommend that the internal posts exposed to Internet should be in controlled in a minimal number.
- Do NOT make weak passwords or default passwords enabled in ALL of the software and network services;
- Seriously manage the removable storage devices; Stop autorun mode; Scan viruses before using mobile devices.

New Characteristics of the Attack

As compared with the previous security incidents, this Stuxnet's attack showed us a number of innovative and impressive attack methods and features.

Attack the Industrial System

The direct target of the Stuxnet worms is Siemens SIMATIC WinCC system. This is a Supervisory Control and Data Acquisition systems (SCADA), it has been widely used in steel, automobiles, electric power, transportation, water conservancy, chemicals, oil and other critical industries, esp. the national-level projects. It runs on Windows platform, and often deployed in the private LAN which is fully physically isolated from Internet.

Normally, the value of worm is broad range of communication, and the universality of target. But this attack is diametrically opposed to principles，its ultimate goal is neither the opened host nor the common software. Whether it is to penetrate to the internal network, or mining the vulnerabilities of large proprietary software, it is rare to find it from usual attackers. It also shows that the intention of attack is clear with sophisticated planning.

Exploit Multiple Zero-day vulnerabilities

Stuxnet exploits Microsoft operating system with the vulnerabilities as follows:

1. RPC remote execution vulnerability(MS08-067)
2. shortcut fileparsing vulnerability(MS10-046）
3. Printer Spooler Service Vulnerability(MS10-061)
4. an unpublicized elevated privileges Vulnerability

The last three vulnerabilities above are firstly used in the Stuxnet，which are the real zero-day flaws. Such a large scale use of multiple zero-day flaws is rare to see before.

These vulnerabilities are not randomly selected. From the point of analyzing worm propagation, each vulnerability has acted an unique role. For example，autorun function has been denied by most of the antivirus software，shortcut file parsing vulnerability could probably be used as the bridging and middle tunnel.

On the other hand，the timestamps of some samples which are captured by Antiy labs are March this year. It means as earlier in March, the zero-day vulnerabilities have been exploited by the attacker, which does not begin to massive outbreak in July, and the vulnerability has not been disclosed before. During this period of time, the vulnerabilities are not widely exploited; it contributes to difficulties suffered from antivirus companies to identify this threat earlier.

Use Digital Signatures

After Stuxnet running, two driver files are released:

- %System32%\drivers\mrxcls.sys
- %System32%\drivers\mrxnet.sys

The two driver files use RealTek's digital signature to avoid being killed by the anti-virus software. At present, the signature has been issued by the agency revoked, and it is no longer valid. However, most of the current anti-virus products use the static method to indentify whether the executable file has a digital signature, so it is likely to be deceived.

Definite Purposes

According to Symantec，Stuxnet infected hosts in Iran was only 25% of total in July despite of a rapid growth to 60% by this September.

WinCC is widely used in the basic defense facilities in Iran. At Sep. 27, Iran's state news agency confirmed that the country's first nuclear power plant "the Bushehr nuclear power plant" has been under attack. It is known that the nuclear power plant was originally scheduled to begin official operation in August this year. Therefore, the attack has definite purposes.

Comprehensive Evaluation

The Industry is facing serious security challenges

In every country in the world, WinCC has been widely used in many important industries. If it is attacked, the operation of facilities related to the enterprise may be abnormal, and even result in the theft of commercial information, production downtime and other serious accidents.

We did not feel very surprised on the emergence of Stuxnet. As early as last year, submitted by user, Antiy Labs has researched on the security of the instrument of chemical industry, and the situation was not optimistic.

Industrial control network, including industrial Ethernet, and FieldBus control system have been already used in industrial enterprises for many years, currently in power, steel, chemicals and other large enterprises in the Large-scale heavy and chemical

industries, industrial Ethernet, DCS (Distributed Control System), FieldBus and other technologies have already penetrated into every aspect of the control system. Now the core of the industrial control networks is industrial control PC, and most of them are based the same Windows-Intel platforms. There are not essential differences between industrial Ethernet and civil Ethernet on technology, and the FieldBus technology applies the microcontroller or embedded system to the every control instruments. In addition to the same attacks as in civilian/commercial network, such as spreading malicious code through the LAN, industrial control network may be attacked by targeted and custom-made means for the FieldBus, which should not be underestimated.

Currently, the economic interests are the main target of most attacks on civilian/commercialcomputer and network. However,special attack against industrial control network and FieldBus, could destroy the companies' critical infrastructures and equipments and the natural tracking and command of those equipments. The consequence and impact could be catastrophic. Taking the chemical industry as an example, the specialized attacks against industrial control network may destroy the natural temperature or pressure tracking of reactors. The reactor will be at over-temperature or over-pressure state. It results in the catastrophic accidents, such as fire alarm or explosion, it probably causes the secondary or even lives loss. As a result, this kind of attacks, which aims at the industrial network, always has the characteristic of information weapons. It aims at the interference or fatal destroying of natural production in those important industrial enterprises. The initiator is generally not an individual or some underground hacker organization

At present, the industrial Ethernet and FieldBus are public standards, and there is no high technical threshold to develop targeted malicious code for programmers who are familiar with the industrial control system. Therefore, it is necessary to enhance and protect the following potential weak points of industrial network security:

- The industrial PC and industrial Ethernet based on the Windows-Intel platform, also may suffer the same attacks as civilian/commercial PC and network, such as spreading malicious code and network worms through the U disk, Stuxnet worm is a typical example.
- At present, products of configuration software in DCS and FieldBus control system (the core of monitoring software), are monopolized by a few companies, especially industry products, such as Siemens SIMATIC WinCC, commonly used in power industry, SUPCON, commonly used in the petrochemical industry, and so on. The attack aiming at configuration software would fundamentally undermine the monitoring system, and the target of Stuxnet is just the WinCC system.
- The safety of FieldBus is relatively good, which based on RS-485 bus and fiber optic physical layer, such as PROFIBUS and RS-485/MODBUS; while the safety of short-range wireless networks is poorer, especially the one that uses

short-range wireless communication measurement and control instruments (Instruments of Measurement) with user-defined special protocol, rather than use general short-range wireless protocol such as Zigbee (with a certain degree of security). Especially, there is hardly any security in the instruments of measurement, which are made in some domestic small enterprises, such as "wireless sensor", and take general 2.4GHz short-range wireless communication chip as its wireless communication part, even without any basic encrypted communications. The instruments of measurement is vulnerable to be eavesdropped and attacked, and will be weak points in FieldBus if used. Therefore, please type the text or Web address, or upload documents.

Industrial control networks are often independent network, whose transmission data is relatively small compared to civil/commercial networks, but the requirements of real-time and reliability are higher, which results in a very serious consequences of having problems.

Compared with information network, the security of traditional industrial network neglects prevention, and always depend on Intranet isolation. Thus, it is extremely urgent to check security and reinforce prevent for industrial systems.

Observation and Thinking

On the tendency and background, which the traditional industry and information technology mix together gradually, and the safety core in traditional industrial system transfers from physical safety to information safety, the Stuxnet attack incident is worthy of further thinking for us.

This is a very unusual attack, specifically reflects in:

- Traditionally, the malicious code is set for widely spreaded and effected, but this attack is highly intentional;
- Traditionally, the attacks were launched by the bug of common software. However, this attack is purposed for the special software in some certain fields.
- This attack was launched by several newly exploited zero-day vulnerabilities generally; it is really hard to see for the traditional attack.
- This attack successfully penetrates internal private network through the appropriate vulnerability, which is the traditional weaknesses of the attack;
- In the ways of time, technology, means, purpose, aggressive behavior, we cannot believe that the attack was launched by a general attack or organization.

Thereby, the new vulnerabilities and spread method adopted by the attack will bring the direct motivation to the new attack in a comparative long time. There are two new attack trends at least worthy of special attention as follows:

- Vulnerability discovery and attacks aiming at industry-specific software, especially attracts on the key industries and sensitive sectors concerning to national strategic. It is clearly pointed out that: "The current point of vulnerability discovery has begun to spread widely rather than focused on the mainstream manufacturers", in *The Analysis Report on the Event that Numbers of Enterprise Network Intruded by Homologous Trojan Samples* by Antiy Labs earlier this year. On the other hand, it is not necessary for attacks on software to exploit the software defects itself, because security is a full range of issues, and the attack may come from everywhere.
- The attacks are aiming at enterprise internal network, especially at the internal specified network with physical isolation. Such networks possess higher security requirements as well as higher aggressive value. Generally the methods to permeate such network include infecting, deceiving, Autorun.inf, and so on, through flash disk and other removable storage devices. Now, the appearance of using shortcut file display vulnerability provides a more effective method. Besides, the internal network will be paid attention and researched by attackers because of the attack, and it is possible to appear some new attacks.

Among the various predictions of the future virus, the most frightening one is not the influence to computer node data of itself, but the associated influence to the related links, such as the illegal control of weapons systems and so on. Unfortunately, the Stuxnet attack proves that: the prophecy will come true if there is no effective prevention.

The first progress of electronic system of industrial is the combination of analog electronic technology and manufacturing technology. Since then, with the continuous introduction of digital technology, it completes the second jump relying on SMC (Single Chip Microcontroller), embedded programs and early digital industrial control protocol. At this time, industrial control systems and office information networks are heteroid and separated, and its security should be mainly in physical security.

With the decreasing cost of PC environment and the Internet, more and more industrial systems, and other information systems begin to move towards a standard x86 environment, meanwhile, more and more control signal and the collection transmission begin to use TCP / IP protocol standards, or even to use public network transmission, which allows vast x86 virus with more possible deadly threats to new target. Therefore, it can NOT absolutely guarantee security to use data exchange even based on the traditional physical isolation. In this case, the threat is highlighted, which comes from non-real time transmission such as flash disk. On the other hand, older

versions of OS are often used in industrial systems based on the intranet isolation and stability, without effective patches, which exacerbates the security risk.

The designers and users of traditional industrial system have made a lot of consideration in the physical security. Industrial system is ensured to operate normally by a sufficient number of sensors, a large number of processes, documents and people's active efforts. However, in this case, system developers try to make the user name connected to the database and password to be the hard code, not with the program content which can be configured independently. This is a low-level mistake in the software development, but they may be prevalent in the current special software system. We can see that, in terms of security, the every detour through which the traditional PC developers went. And the pictures will be repeated in industrial control system. We could foresee that, in the next 20 years, the core of security in the industrial system is no longer an isolated issue only for physics and physical security and the security problems of information system undeniably impacts on the entire operation. Be frank, this issue has been present in Internet, which is regarded as the human's future development and direction.

Security vendors have not considered as one of the requirements in traditional industrial security system. Therefore, in the beginning of this event security vendors and the attackers were not located at the same position of asymmetric information. Attackers make a complete analysis and preparation for the target industrial system, and then launched the attack; when the security vendors faced the unexpected emergencies, they could not replicate the problem as quickly as possible so as to follow up and analyze, as the emergence of vulnerability in common software or internet software, but they must wait for the cooperation of related software developers. From this perspective, commonly transmitted by PC environment, and then launched the attack to the relatively closed industrial system or other specific system, got the time of attack by making use of information asymmetry between the manufactures and security vendors, this will become a new attack vector with challenge and great irony. Therefore, the misconception that the special system independent of security threats finally results in shutting doors to the security vendors but opening the loopholes to the attackers.

As a professional security engineer, we will take greater and heavier responsibility initiatively. We could prove that our research and analysis work is not only to protect a virtual world but also the world we live in.

Appendix Timeline of Antiy's Emergency Response

Jul 15th, 2010 Antiy captured the first variation of Stuxnet and updated the virus database of AVL SDK immediately, so that the virus can be scanned and killed.

Jul 20th, 2010 Analyzed the Stuxnet sample file and shortcut file parsing Vulnerability .

Jul 23rd, 2010 Completed the elementary analysis report.

Aug 18th, 2010 Officially issued the analysis report and preventive measures.

Jul 15th to Sep 28th, 2010 Continually captured the samples and followed the event.

Sep 27th, 2010 Release this report for the 1st version.

Sep 28th, 2010 Release this report for the 2nd and 3nd version.

Sep 29th, 2010 Modified 3nd version, release this report for English version.

Referred Links

1. Siemens has offered the regular solution:

http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objid=43876783

2. Microsoft links are followed about vulnerabilities:

RPC remote execute （MS08-067）

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

Shortcut file analyze （MS10-046）

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

Printer backstage program service (MS10-061)

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

3. WinCC Patch released by Siemens

http://support.automation.siemens.com/WW/llisapi.dll/csfetch/43876783/SIMATIC_Security_Update_V1_0_0_11.exe?func=cslib.csFetch&nodeid=44473682

4. Download Antiy Atool:

http://www.antiyfx.com/download/atool.zip

About Antiy Labs

Antiy Labs is an antivirus vendor which makes advanced research and technology contributions to the field. Currently, there are tens of thousands of firewalls, UTM and security devices deployed with our antivirus engine. More information is available at www.antiy.net.

Antiy Labs