NetWitness Community

community.rsa.com/thread/185437

January 22, 2016

Information

Malware Family/Aliases: Sykipot

Malware Type: Trojan/Backdoor:Win32

Platform: Windows

MD5: 4f90ffbdf64fd1b2b96324378007aa8c
SHA1: 736537d5c264e5a784d3fda128d9d8e7f88f8274
SHA256: c13eb82839e133da2c8881c6690c91f3e20e145050b8b58ffef206335fd38e77

MD5: 1747e47baee61e06d1ee0e4d1c3649bf
SHA1: 06bb28927fe12aeb5e70d2e518abf5b9796cda9d
SHA256: 5ce4a75d368a337cfbd16c8eab3b8fbd0fb99d1d7d3d27636a9b36e9fa0e4859

Discovery Date: 2007

Summary

Sykipot is an APT malware family that is around since 2007 and is used as a backdoor to fully control the victim's machine. Once the machine is infected, the backdoor communicates with the C&C server to execute several kinds of commands on the affected system. Sykipot APT malware family has been used by cybercriminals on targeted attacks in order to steal sensitive information from key industries.

Notable features of this malware family are the ability to execute both command prompt and backdoor commands sent by the C&C server on the affected system, so that it can be able to retrieve system and network information, reboot the system, manage processes (list, execute, kill and etc.), manage files (list, read, delete, copy and etc.), uninstall itself from the system and so on. This malware family is also able to send and receive files to and from the C&C server and to configure a delay timer for the next communication time with the C&C server.

Malware Installation

[c13eb82839e133da2c8881c6690c91f3e20e145050b8b58ffef206335fd38e77]

This malware sample is an executable file that pretends to be a Merry Christmas image file. When the executable file is executed, the image is extracted and displayed to the user:

Right after that, the malware creates an msrt.exe file in temp folder:

%Temp%\msrt.exe

The malware then installs a fake Help and Support Center service that pretends to be original's Windows Help and Support service:

This is done by calling Windows APIs to install the new service and by adding and setting the following Registry entries:

HKLM\SYSTEM\ControlSet001\Services\helpsvcc\ImagePath: "C:\WINDOWS\system32\msrt.exe"

HKLM\SYSTEM\ControlSet001\Services\helpsvcc\DisplayName: "Help and Support Center"

HKLM\SYSTEM\ControlSet001\Services\helpsvcc\Description: "Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKLM\SYSTEM\CurrentControlSet\Services\helpsvcc\ImagePath: "C:\WINDOWS\system32\msrt.exe"

HKLM\SYSTEM\CurrentControlSet\Services\helpsvcc\DisplayName: "Help and Support Center"

HKLM\SYSTEM\CurrentControlSet\Services\helpsvcc\Description: "Enables Help and Support Center to run on this computer. If this service is stopped, Help and Support Center will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

Next, the malware persists itself at

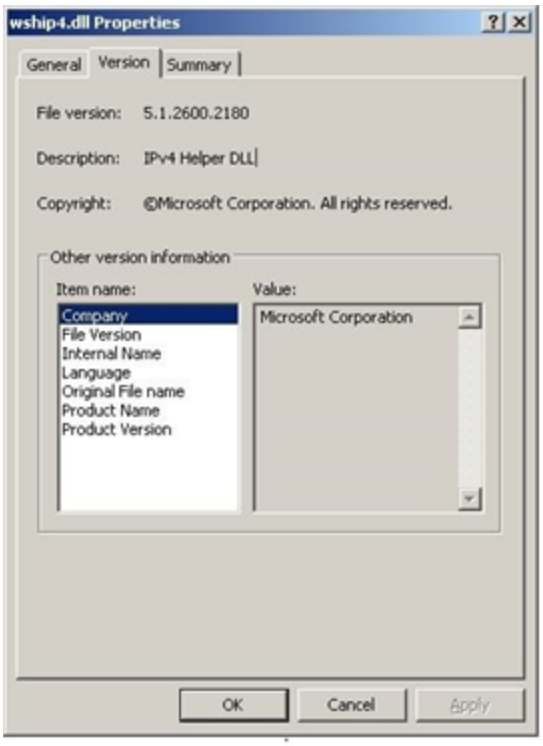
%WINDIR%\system32\msrt.exe

Deletes itself from

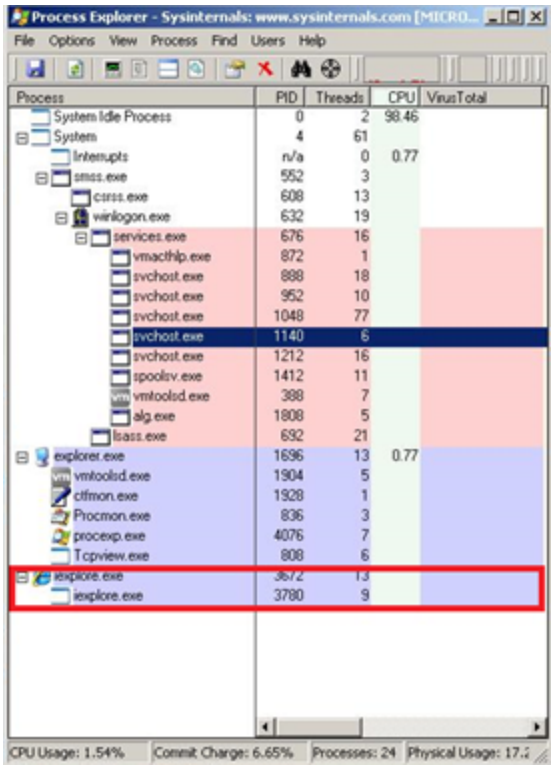
%Temp%\msrt.exe

And start the newly created Help and Support Center service, which points to %WINDIR%\system32\msrt.exe.

This instance of the malware will extract malicious code and write file %WINDIR%\system32\wship4.dll, which pretends to be an IPv4 Helper DLL from Microsoft Corporation:



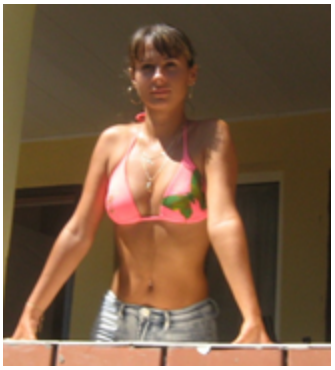
The malware creates a hidden instance of Internet Explorer browser and makes it use %WINDIR%\system32\wship4.dll to serve as backdoor to communicate with the C&C server and execute commands on the affected machine:



Finally, after the backdoor is running, the malware stops newly created Help and Support Center service.

[5ce4a75d368a337cfbd16c8eab3b8fbd0fb99d1d7d3d27636a9b36e9fa0e4859]

This malware sample is an executable file that pretends to be a girl image file. When the executable file is executed, the image is extracted and displayed to the user:



Right after that, the malware creates a siop.exe file in temp folder:

%Temp%\siop.exe

Exactly as the previous sample, the malware extracts malicious code and write file %Temp%\rsm.dll, which also pretends to be an IPv4 Helper DLL from Microsoft Corporation. The malware then creates a hidden instance of Internet Explorer browser and makes it use %Temp%\rsm.dll to serve as backdoor to communicate with the C&C server and execute commands on the affected machine.

Malware Protective Mechanisms

[c13eb82839e133da2c8881c6690c91f3e20e145050b8b58ffef206335fd38e77]

To protect the dropped files, the malware clones all date timestamp file properties from original's system file svchost.exe to dropped files msrt.exe and wship4.dll, making them look authentic.

The malware also creates and runs a hidden instance of Internet Explorer browser with current user's credentials by using current user's token, which is retrieved by looping through the list of processes and retrieving Windows Explorer current user's token.

[5ce4a75d368a337cfbd16c8eab3b8fbd0fb99d1d7d3d27636a9b36e9fa0e4859]

Exactly as the previous sample, the malware also creates and runs a hidden instance of Internet Explorer browser with current user's credentials by using current user's token, which is retrieved by looping through the list of processes and retrieving Windows Explorer current user's token.

Malware Persistency Techniques

[c13eb82839e133da2c8881c6690c91f3e20e145050b8b58ffef206335fd38e77]

As mentioned before, the malware installs it as a Windows service and is configured to automatically start during Windows startup (start type equals to "2"):

HKLM\SYSTEM\ControlSet001\Services\helpsvcc\Start: 0x00000002

HKLM\SYSTEM\CurrentControlSet\Services\helpsvcc\Start: 0x00000002

[5ce4a75d368a337cfbd16c8eab3b8fbd0fb99d1d7d3d27636a9b36e9fa0e4859]

To make itself persistent, the malware configures itself to be run during Windows startup. It does this by adding the following registry key.

RegKey:

HKU\Software\Microsoft\Windows\CurrentVersion\Run\start:

Value:

start

Data:

"%Temp%\siop.exe -install"

Network Behavior

Some of the malware samples try to connect to the following domains:

- motor.hyundei-motor.com
- onesfocus.com
- strongtable.3322.org
- notes.topix21century.com
- map.kortimes.com
- chosunkor.com
- racingfax.com
- news.marinetimemac.com
- hotgreenlight.com
- sports.hotgreenlight.com
- mysundayparty.com
- news.mysundayparty.com
- movieshowgirl.com
- moto.sourceinsightonline.com
- happybehere.com
- music.defense-association.com
- altchksrv.hostdefence.net

Once the backdoor is active, the malware communicates with the C&C server from time to time and can execute commands on the affected machine.

The malware pings the C&C by using a GET request that follows the pattern:

http://[C&C_Domain]/asp/kys_allow_get.asp?name=getkys.[jpg|dat|kys]&hostname=[Computer_Name]-[IP_Address]-[Unique_Identifier]

Some versions of the malware have the ability to read a delay timer information from the configuration file retrieved from the C&C server. This will be used to configure the time interval of the communication between the malware and the C&C server. The purpose of this feature is to make it hard to be detected by analysis tools.

Security Analytics Solution

The following query can be used to detect Sykipot network activity using RSA Security Analytics:

action = 'get' && filename = 'kys_allow_get.asp' && query begins 'name='

More details can be found here.

Researcher

Norton Santos