Michael Esposito
Network Defense 2

Homework #3

Table of Contents

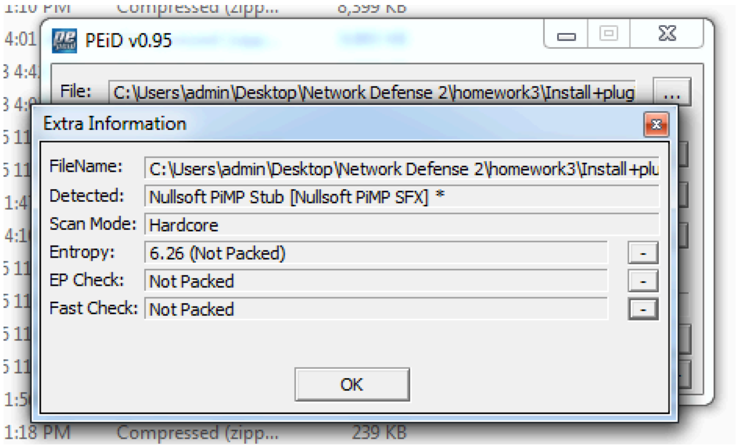
Static Analysis 2
PEiD 2
McAfee FileInsight 3
PEStudio 3
Dynamic Analysis 3
File System 3
Registry 4
Network Calls 4
Summary 4

Static Analysis

A static analysis on Install+plugin1.exe was performed. The executable file was analyzed with various tools before being installed on the host system.

PEiD

PEiD was initially performed to establish if the executable file in question was packed or not. The entropy level was 6.26, indicating that this malware file most likely was not packed.



File: C:\Users\admin\Desktop\Network Defense 2\homework3\Install+plug

FileName: C:\Users\admin\Desktop\Network Defense 2\homework3\Install+plu

Detected: Nullsoft PiMP Stub [Nullsoft PiMP SFX] *

Scan Mode: Hardcore

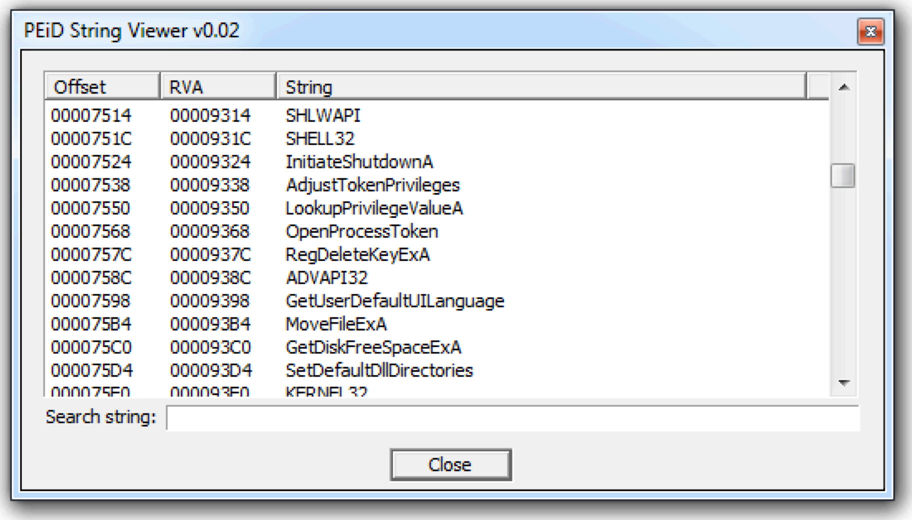
Entropy: 6.26 (Not Packed)

EP Check: Not Packed

Fast Check: Not Packed

Figure 1: Entropy level indicated that the installer is not packed

An analysis of the available strings from the malware bytecode was performed using PEiD. In the following screenshot, numerous values show this program might edit the registry, move files, open processes, edit directories and privileges and initiate a shutdown.



Offset	RVA	String
00007514	00009314	SHLWAPI
0000751C	0000931C	SHELL32
00007524	00009324	InitiateShutdownA
00007538	00009338	AdjustTokenPrivileges
00007550	00009350	LookupPrivilegeValueA
00007568	00009368	OpenProcessToken
0000757C	0000937C	RegDeleteKeyExA
0000758C	0000938C	ADVAPI32
00007598	00009398	GetUserDefaultUILanguage
000075B4	000093B4	MoveFileExA
000075C0	000093C0	GetDiskFreeSpaceExA
000075D4	000093D4	SetDefaultDllDirectories
000075E0	000093E0	KERNEL32

Figure 2: Strings analysis

McAfee FileInsight

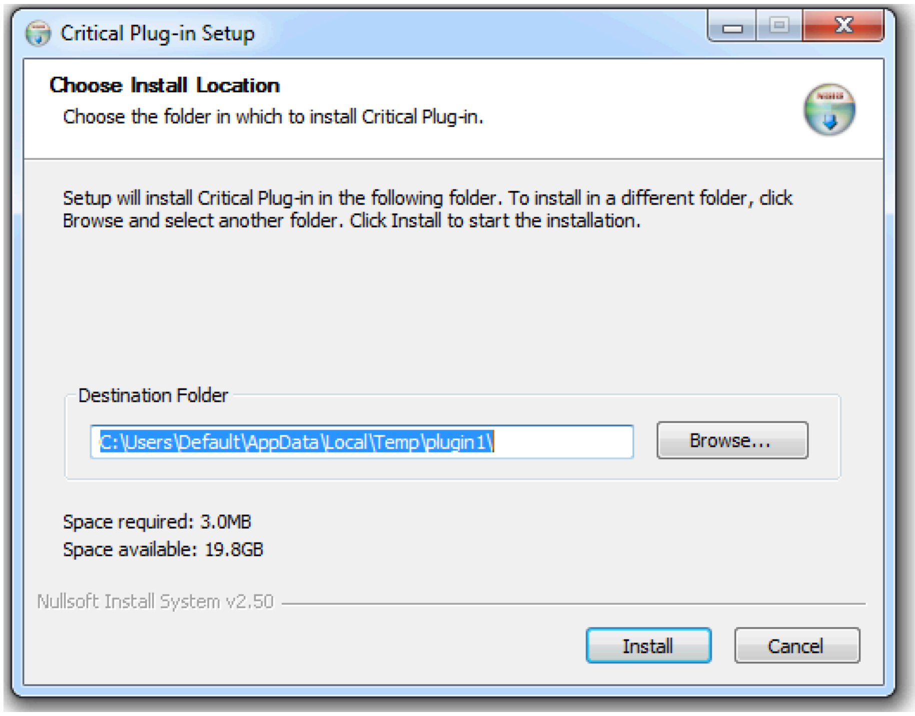
FileInsight showed a lot of features indicative of a python program. This file may be a python program compiled into a Windows executable file.

PEStudio

This malware was reported to be a Trojan by 10 different malware engines. PEStudio also expanded upon the initial strings analysis and discovered that these strings were related to imported symbols. 67 of these symbols were on PEStudio's blacklisted list.

Dynamic Analysis

Using Process Monitor, I was able to follow the events performed by Install+Plugin1.exe. This program created another executable, plugin1.exe, and saved it to disk. Wireshark was used to perform network monitoring during the execution of Install+plugin1.exe and plugin1.exe



Critical Plug-in Setup

Choose Install Location

Choose the folder in which to install Critical Plug-in.

Setup will install Critical Plug-in in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Users\Default\AppData\Local\Temp\plugin1\

Space required: 3.0MB
Space available: 19.8GB

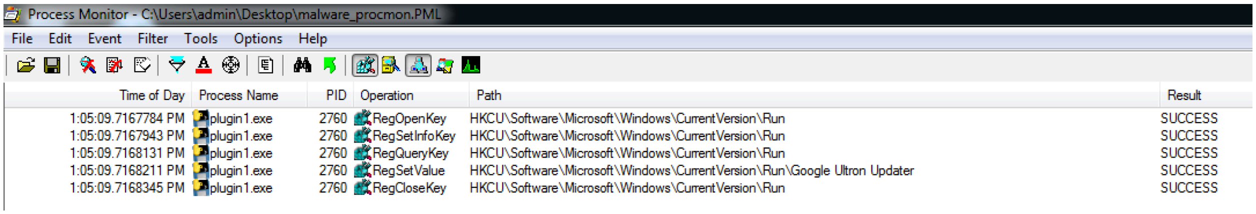
Figure 3: Installer completed

File System

Install+plugin.exe created another file, C:\Users\Default\AppData\Local\Temp\plugin1\plugin1.exe. plugin1.exe also created a number of files inside the directory C:\Users\admin\AppData\Local\Temp_MEI35762.

Registry

plugin1.exe set a value inside the registry in order to become persistent. The registry path was HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Google Ultron Updater, which means that this updater will run whenever the infected computer boots up.



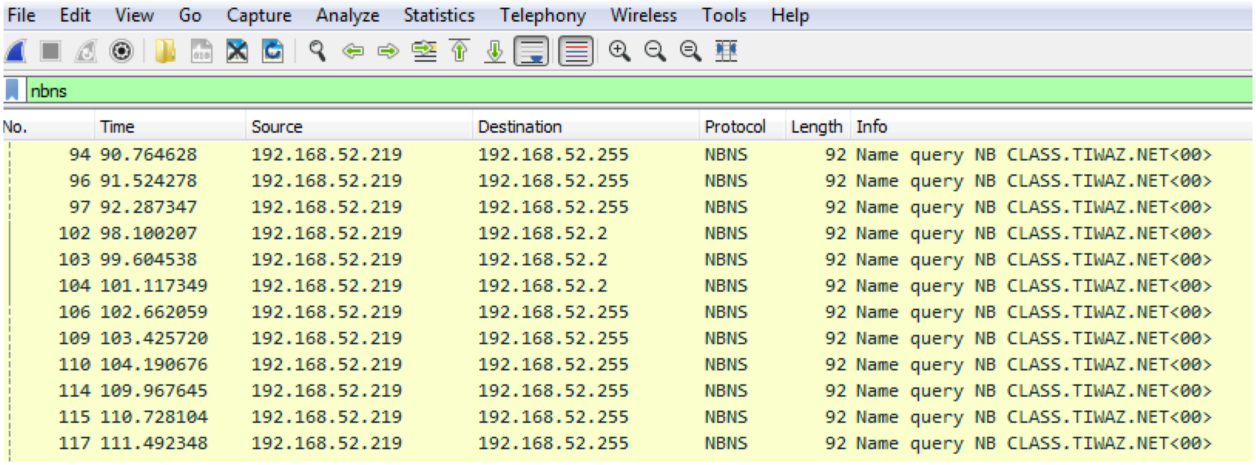
Process Monitor - C:\Users\admin\Desktop\malware_procmon.PML
File
Edit
Event
Filter
Tools
Options
Help

Time of Day	Process Name	PID	Operation	Path	Result
1:05:09.7167784 PM	plugin1.exe	2760	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS
1:05:09.7167943 PM	plugin1.exe	2760	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS
1:05:09.7168131 PM	plugin1.exe	2760	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS
1:05:09.7168211 PM	plugin1.exe	2760	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Google Ultron Updater	SUCCESS
1:05:09.7168345 PM	plugin1.exe	2760	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS

Figure 4: Registry entries edited by plugin1.exe

Network Calls

Wireshark was used to capture network traffic initiated by the malware samples. Plugin1.exe periodically performed NetBIOS Name Service (NBNS) queries to CLASS.TIWAZ.NET.



nbns

No.	Time	Source	Destination	Protocol	Length	Info
94	90.764628	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
96	91.524278	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
97	92.287347	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
102	98.100207	192.168.52.219	192.168.52.2	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
103	99.604538	192.168.52.219	192.168.52.2	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
104	101.117349	192.168.52.219	192.168.52.2	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
106	102.662059	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
109	103.425720	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
110	104.190676	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
114	109.967645	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
115	110.728104	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>
117	111.492348	192.168.52.219	192.168.52.255	NBNS	92	Name query NB CLASS.TIWAZ.NET<00>

Figure 5: Wireshark packet capture of malware traffic

Summary

Install+plugin1.exe installed plugin1.exe. This plugin modified the registry in order to create persistence and allow the program to execute after the victim computer reboots. In order to detect this malware, one can look for the identified registry value and executable file dropped into the temp directory.