Michael Esposito

Network Defense 2

Homework #3

Table of Contents

[Static Analysis 2](#_Toc507673478)

[PEiD 2](#_Toc507673479)

[McAfee FileInsight 3](#_Toc507673480)

[PEStudio 3](#_Toc507673481)

[Dynamic Analysis 3](#_Toc507673482)

[File System 3](#_Toc507673483)

[Registry 4](#_Toc507673484)

[Network Calls 4](#_Toc507673485)

[Summary 4](#_Toc507673486)

# 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.

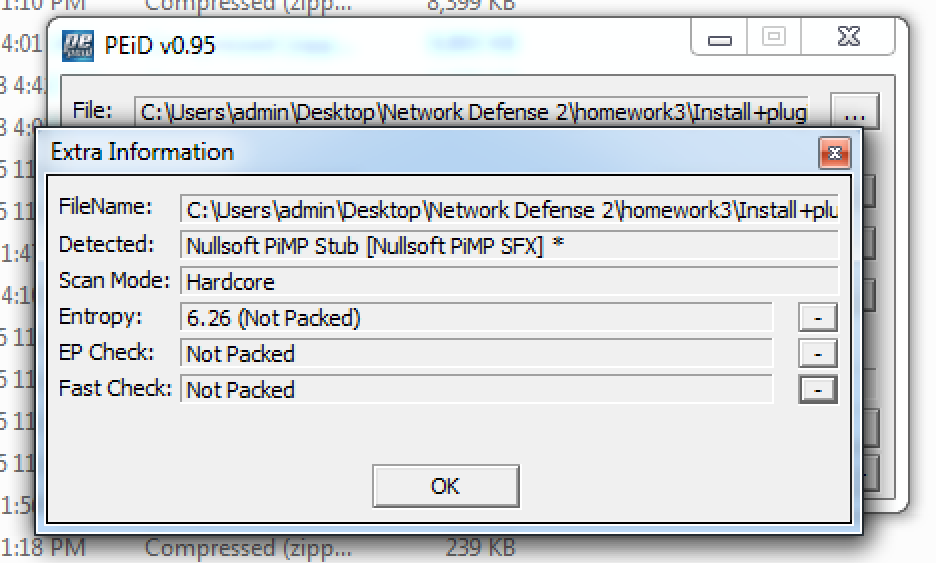


Figure 1: Entropy level indicated that the installer is not packed

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.

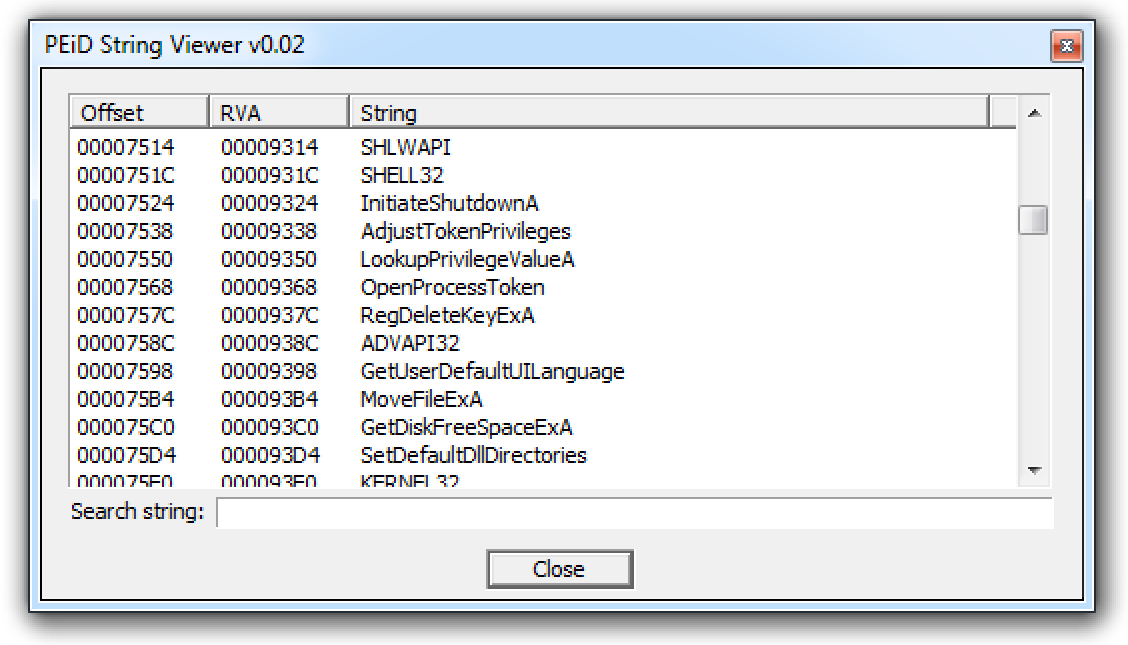


Figure 2: Strings analysis

## 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

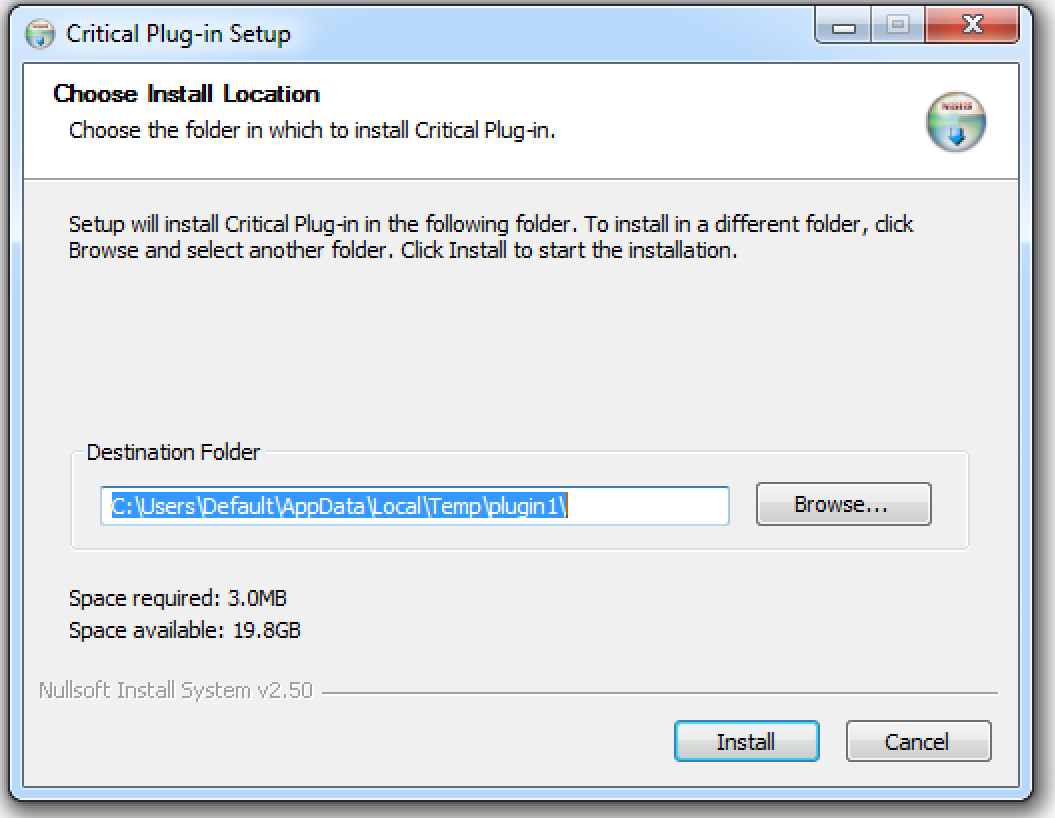


Figure 3: Installer completed

## 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.

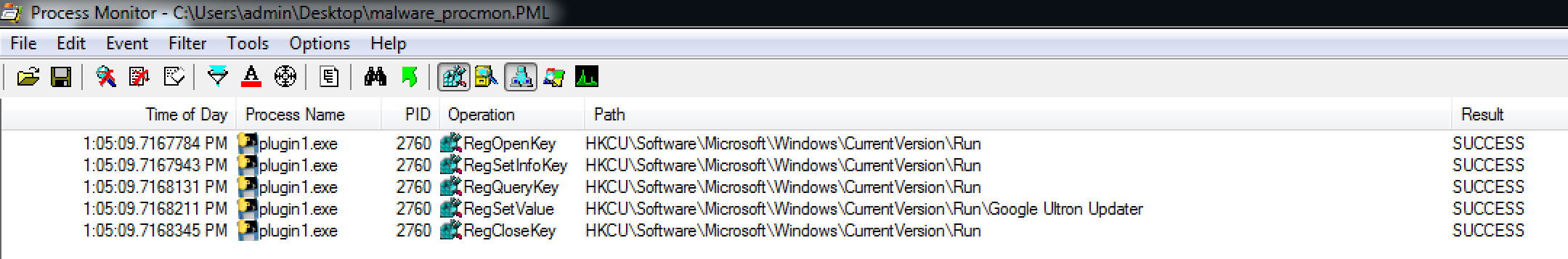


Figure 4: Registry entries edited by plugin1.exe

## 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.

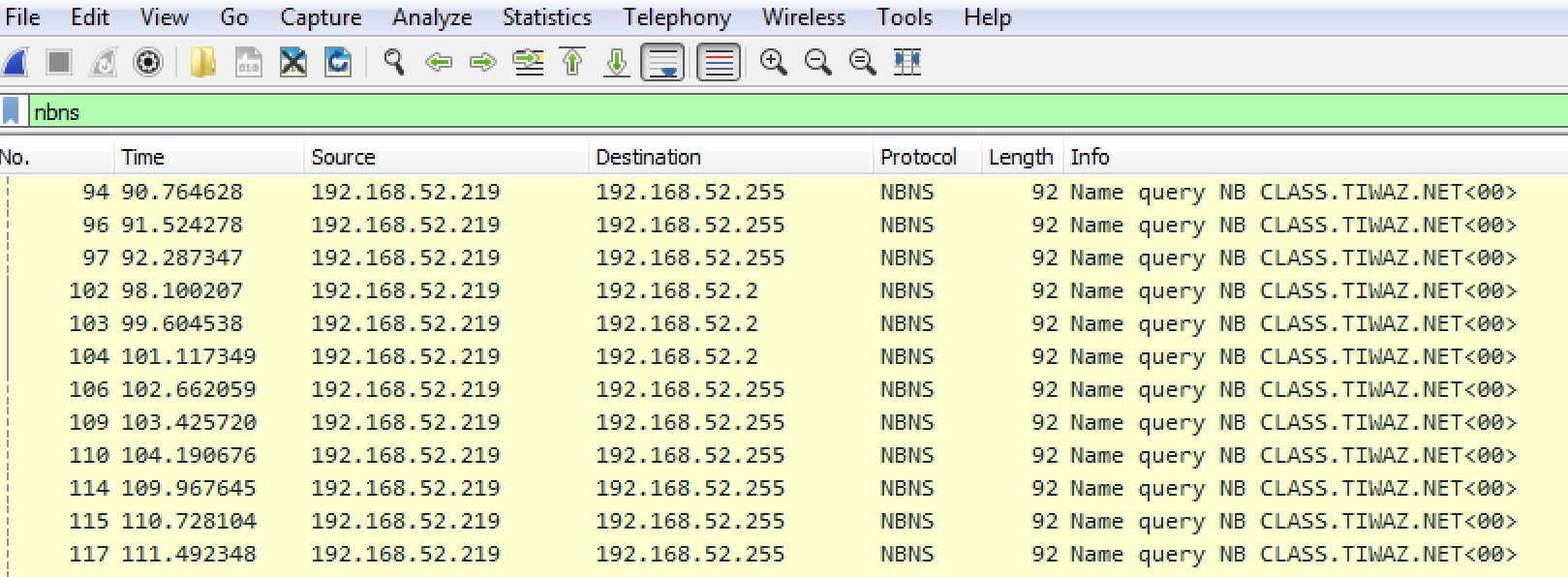


Figure 5: Wireshark packet capture of malware traffic

# 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.