hw5

dj$_{\text{dvorak}}$

April 24, 2020

Contents

1 Lab 7 Analyzing Malicious Windows Programs

2 Lab 07-01

2.1 Achieving Persistence

This file achieves persistence by creating a service called `MalService`.

2.2 Mutex Purpose

This program uses a mutex called `HGL345` to make sure their is only one instance of the original program running.

2.3 Good Host-based signature

You can check for the creation of a process called `Malware Service` or the name of the strange mutex `HGL345`. The service is automatically tied to the binary's path and filename.

2.4 Good Network-based signature

Any traffic to the site `practicalmalwareanalysis.com` with `Internet Explorer 8.0`.

2.5 Purpose

Seems to be a DDOS attcker? 20 threads are spawned starting in the year 2100.

2.6 Duration of Execution

Seems each thread will sleep for `0xffffff` milliseconds. But the attacks do not stop otherwise.

3 Lab 07-02

3.1 Persistence

It doesn't look like this program is persistent.

3.2 Purpose

The purpose seems to be open an ad with Internet Explorer, then exits. This software does so by using the OLE `CoCreateInstance` call which uses COM objects to open programs. The CLSID key is the key to opening IE.
`http://practicalmalwareanalysis.com/ad.html`.

3.3 Duration of Execution

Seems to run and then quits if anything fails (after the ad is opened).

4 Lab 07-03

4.1 How Does this Program Achieve Persistence

The original exe file copies the dll file into a fake windows dll under the path of `C:\windows\system32\kerne132.dll` . Note the 1 instead of the l.

4.2 Two good host-based indicators

Well, there is this string that says `THIS WILL DESTROY YOUR COMPUTERT`. Also, we see that mutex is created by the dll with the name `SADFHUHF`. An IP address is listed here 127.26.152.13 (seemingly changed for safety purposes). Additionally, it looks like it is listening for commands such as "exec", "sleep" and "q" from this external IP.

4.3 The purpose

The purpose is to inject their bogus .dll file into scan the possibly change any system calls to point to their bogus kerne132.dll . . . This also runs some back door serivce which allows for the arbitrary execution of commands and processes! Looks deadly.

4.4 How to remove this malware after Installation

Well, the damage is pretty bad since it modifies all system files. Better to just restore a backup image!