Anaisy Garcia

5734454

Lab 7-1

Analyze the malware found in the file Lab07-01.exe.

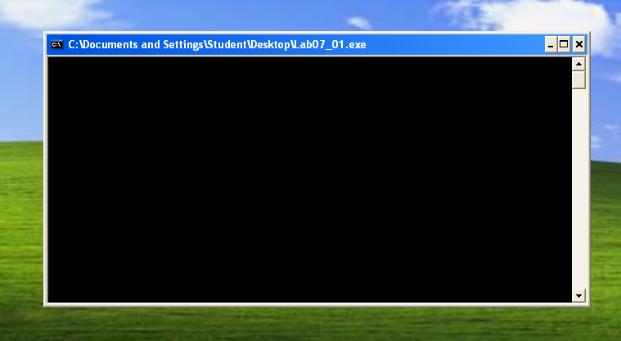
Questions

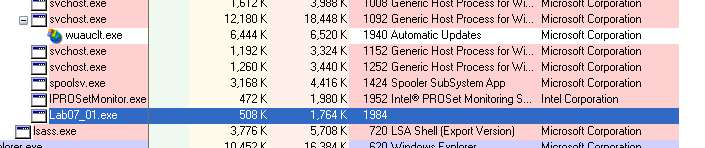
1. How does this program ensure that it continues running (achieves persistence) when the computer is restarted?

The program creates a service called MalService which makes sure it’s always running.



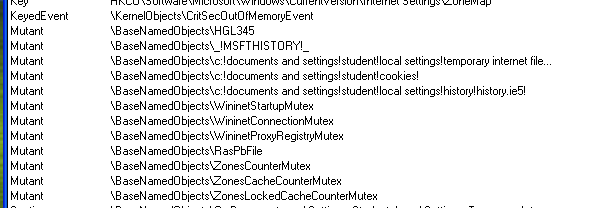
When the program is run a command prompt that stays open and when the computer is restarted the program can still be seen active in process explorer under svhost.exe.



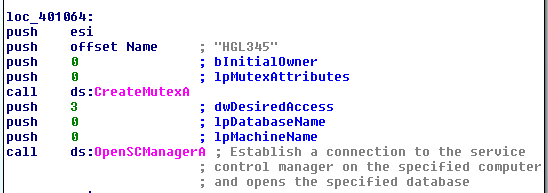
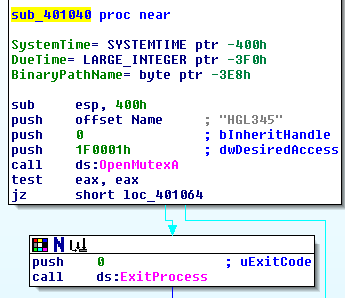


1. Why does this program use a mutex?

A mutex is used for the program to make sure its only running once. This can be seen working in process explorer where we see mutants come up called StartupMutex, CounterMutex, and LockedCacheCounterMutex.



Using IDA pro, it can be seen that this program creates a mutex named HGL345 then the program calls OpenMutexA. If it is called it continues the program if not is exits.



1. What is a good host-based signature to use for detecting this program?

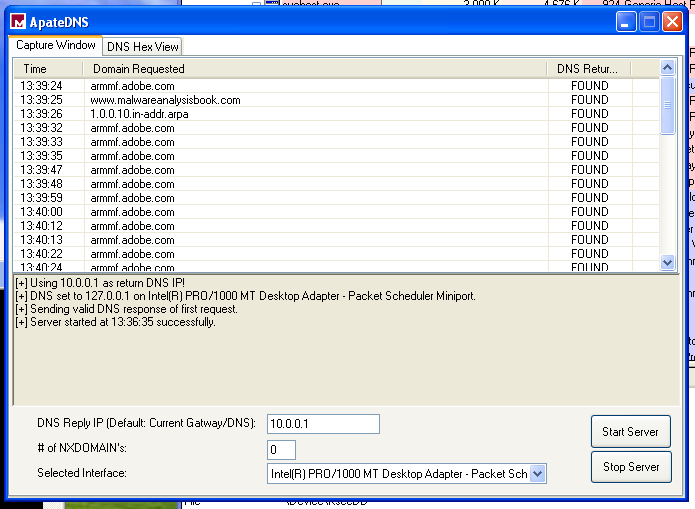
Since it is running on the computer, we can use process monitor or process explorer and search for either a mutant named HGL345 or the service Malservice because this is what it uses constantly.

1. What is a good network-based signature for detecting this malware?

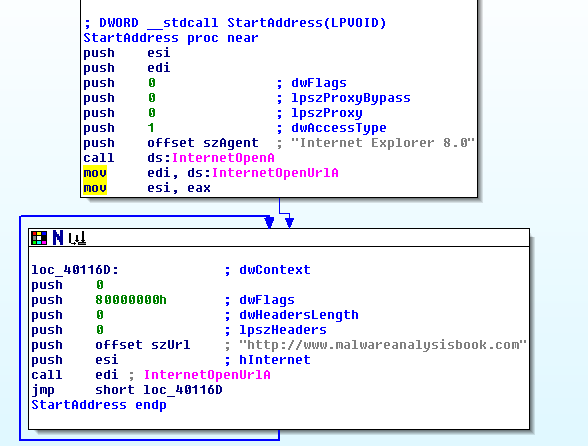
The imports in PEiew shows us that this program uses WINNET.dll and the imports InternetOpenURL and InternetOpen. This means the program communicates with a url at some point.



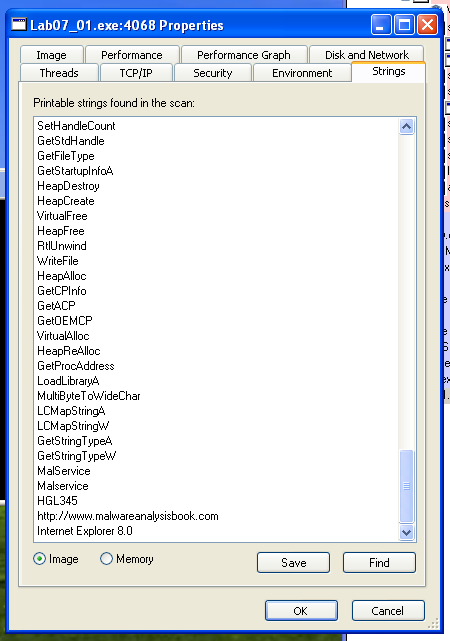
Using ApateDNs we can see that the program requests the website “www.malwareanalysisbook.com”.



This is made further certain using IDA pro. This is where it is seen the malware uses “Internet Explorer 8.0” and accesses “http:/ www.malwareanalysisbook.com”.

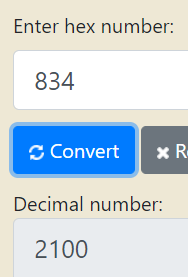
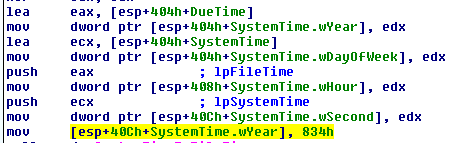


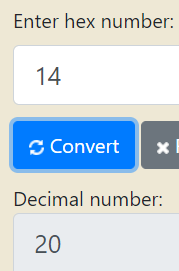
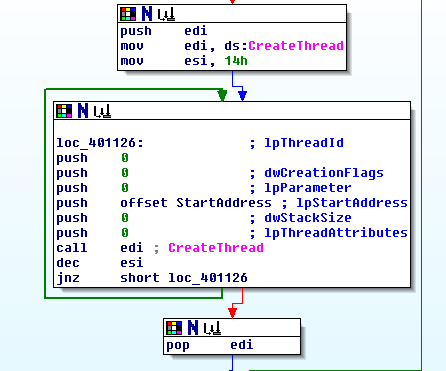
Process explorer helps us confirm this using the string tab.



1. What is the purpose of this program?

From IDA pro we can tell this program sleeps until the year 2100 then once it is that year the program creates 20 threads and makes multiple requests to http:/www.malwareanalysisbook.com. This would most likely be used to flood the site with requests to attack.





1. When will this program finish executing?

The program never ends it runs forever once executed and once it reaches year 2100 it continues to flood the website.