Lab 12-04

Analyze the malware found in the file Lab12-04.exe.

Questions

1. What does the code at 0x401000 accomplish?

The subroutine at address 0x401000 is repeatedly called within a loop. Its function is to identify the winlogon.exe process by using the OpenProcess, EnumProcessModules, and GetModuleBaseNameA APIs.

If a match is found, the subroutine returns 1; otherwise, it returns 0. This allows the malware to determine whether it has located the correct process or if it should continue scanning other processes until the target is found.

2. Which process has code injected?

The targeted process at sub_401174 is winlogon.exe.

The injected code is intended to use SfcTerminateWatcherThread in order to disable WFP (Windows File Protection) until next system reboot.

3. What DLL is loaded using LoadLibraryA?

At 0x4013B4 the malware wants to load psapi.dll in order to make use of three functions: EnumProcessModules, GetModuleBaseNameA, EnumProcesses.

The usage of this library and its functions gives the malware knowledge about currently running processes on the OS. This way it can find the target it wants to inject to.

Another LoadLibraryA occurs at 0x4011A8 in order to load up sfc_os.dll SfcTerminateWatcherThread function which is intended to turn off Windows File Protection until next reboot, this way the malware can manipulate original files at system32 directory without being overwritten.

4. What is the fourth argument passed to the CreateRemoteThread call?

The fourth argument is a lpStartAddress which is an address of ordinal 2 of sfc_os.dll file, and that is SfcTerminateWatcherThread.

The internet explains that it is undocumented library and that SfcTerminateWatcherThread can be abused to disable Windows File Protection in order to make changes in the system32 directory until next reboot.

5. What malware is dropped by the main executable?

The malware moves original wupdmgr.exe to %temp% folder under name winup.exe then creates a new file under a name wupdmgr.exe at system32 directory, resolves the PE data from resources and writes it onto the newly created file and executes it using WinExec.

6. What is the purpose of this and the dropped malware?

In short words, the purpose of this malware is to access hxxp[://]www[.]practicalmalwareanalysis[.]com/updater[.]exe, download the file, save the downloaded bytes to a system32\\wupdmgrd.exe and execute it. It's a trojan and loader type of malware.

In more extended analysis, once executed, the malware performs lots of action to achieve its goal to download another malicious file and execute it while evading any suspicion.

Malware actions (in order of code flow):

1. Dynamically loads psapi.dll.
2. Retrieves all of the currently running processes using loaded psapi.dll library.
3. Searches for winlogon.exe process in the list.
4. Performs its own process privileges escalation of SeDebugPrivilege.
5. Dynamically loads sfc_os.dll and injects SfcTerminateWatcherThread function into winlogon.exe using CreateRemoteThread in order to disable Windows File Protection.
6. Moves original file system32\\wupdmgr.exe to %temp%\\winup.exe.
7. Resolves malicious PE file from its own resources and saves it at system32\\wupdmgr.exe and executes it.
8. The newly resolved executed file uses URLDownloadToFileA call to access http://www.practicalmalwareanalysis.com/updater.exe and save the bytes into a system32\\wupdmgrd.exe file and then execute it.