Kaizen Solutions Software

Date: September 04th, 2018.

Description

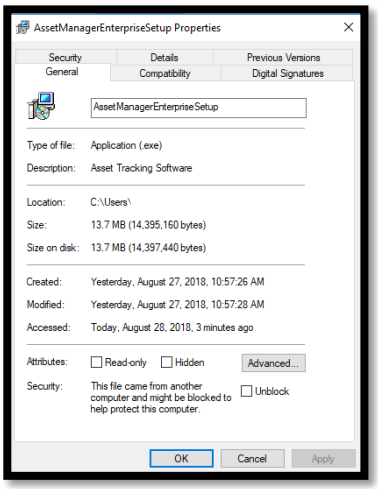
Two solutions were verified in this assessment: 1) the Asset Manager (Enterprise Edition) and 2) the Training Manager (Enterprise Edition). The first is used to control and monitor fixed assets such as computers and equipment. The second is used to track employee training records.

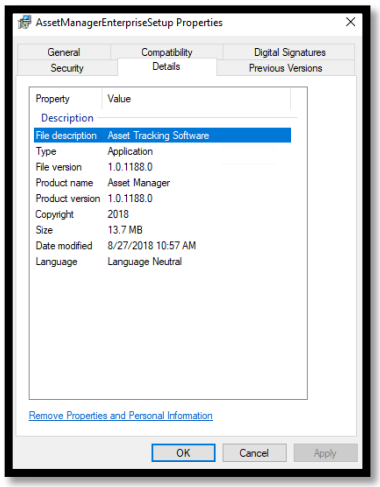
Both software presented some vulnerabilities including remote access and persistence. The main causes of those vulnerabilities were related to specific files such as: “isxdl.dll”, “996E.temp”, “profinder.vshost.exe”, “AssetManager.exe” and “TrainingManager.exe”.

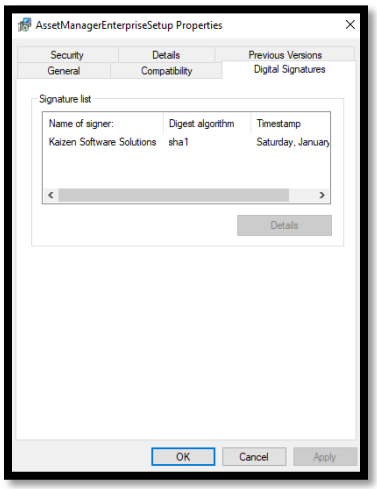
Currently, there are several documented techniques that could be used to exploit those vulnerabilities.

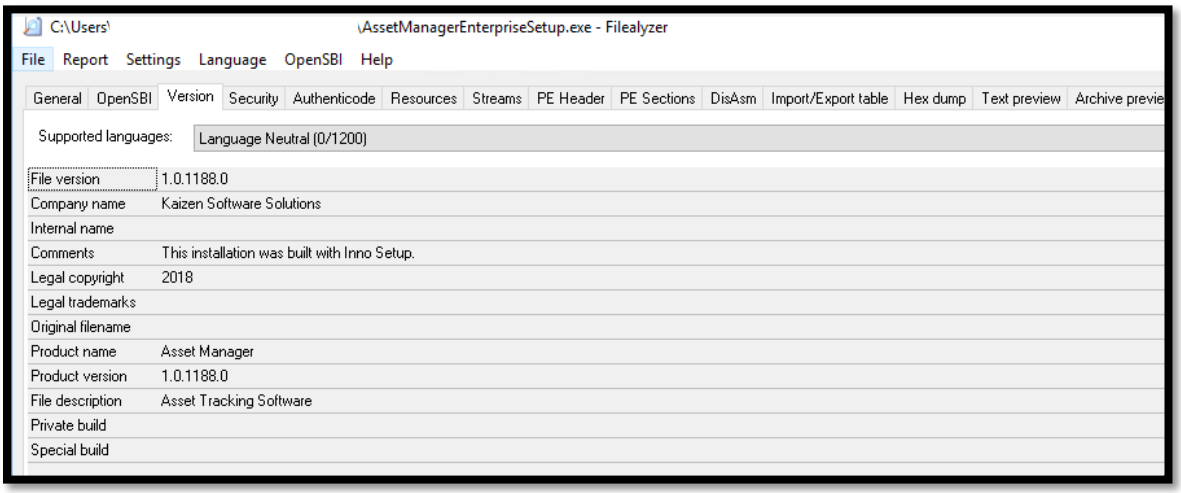
File Analysis

This is the Asset Manager software:

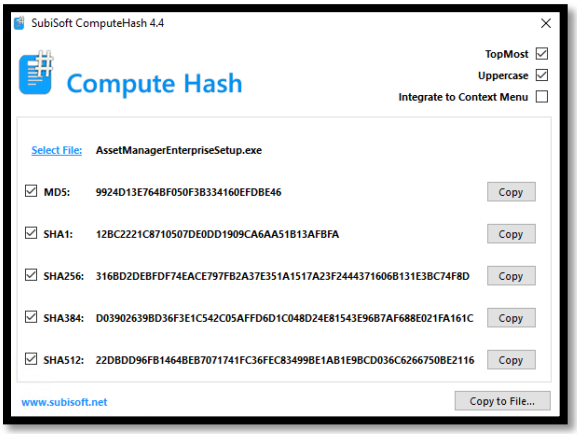






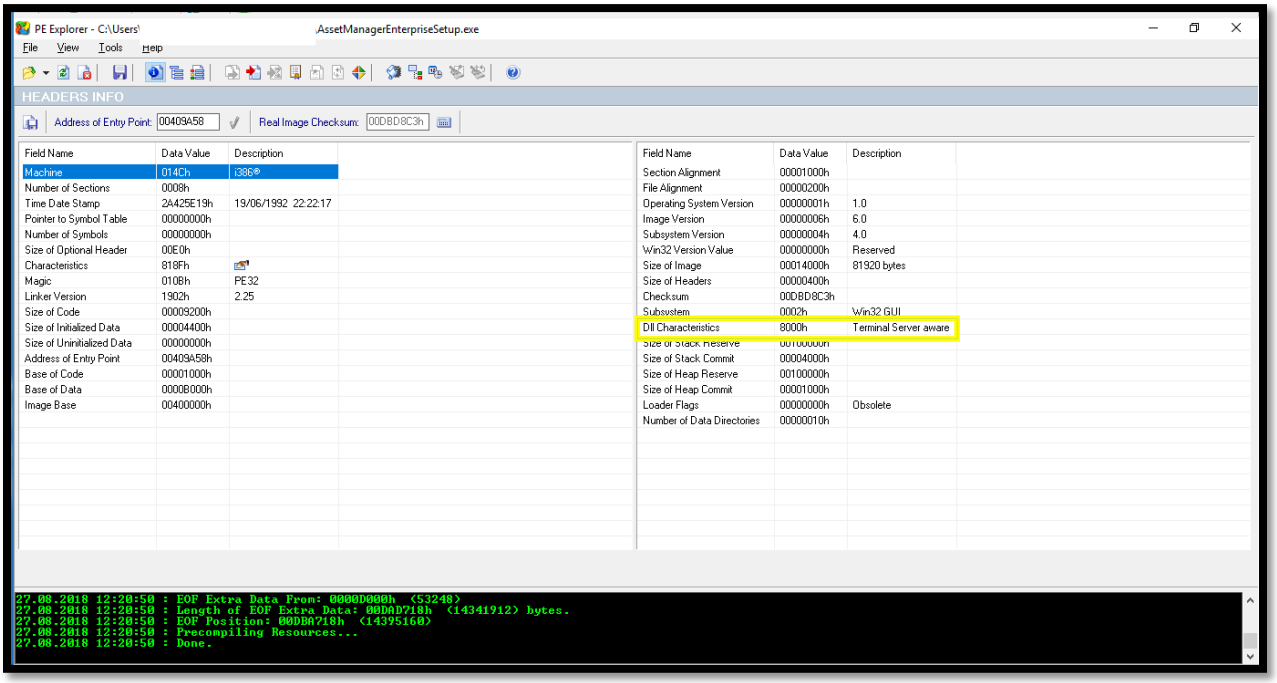


Calculate the Hash:



Red Flags

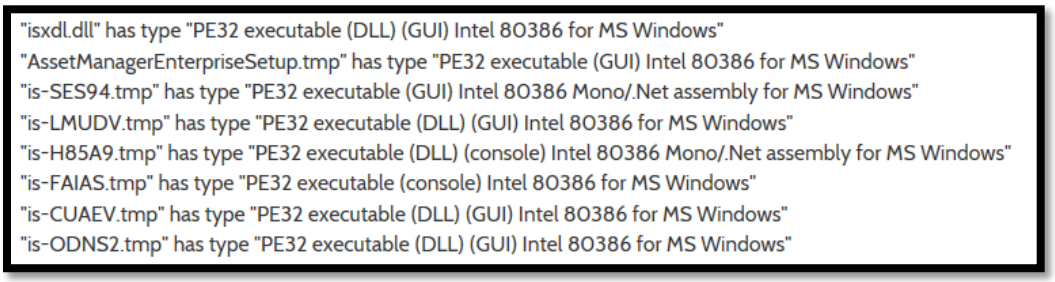
We can identify a Terminal Server aware feature:



Terminal Server can create a virtual Windows folder instead of using the system's Windows directory. This gives users access to their own INI files. If an application is Terminal Server aware, it must neither rely on INI files nor write to the HKEY_CURRENT_USER registry during setup. In general this characteristics is not valid for drivers, VxDs, or DLLs[1].

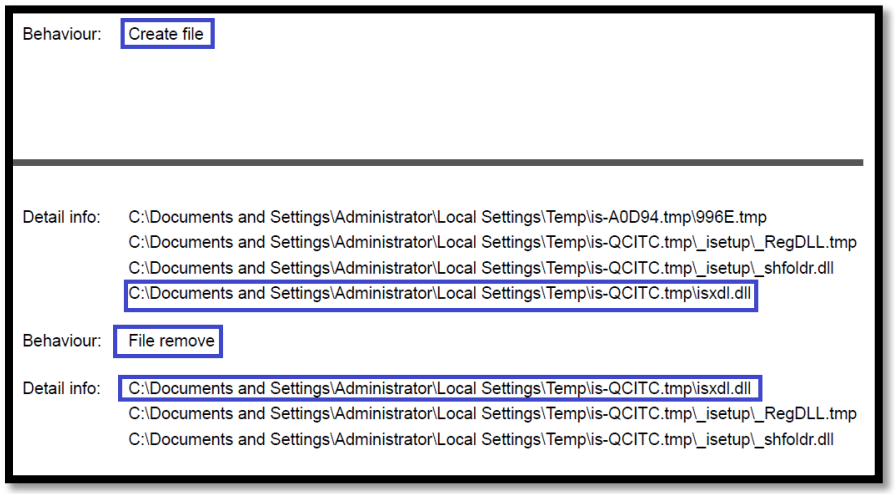
Persistence

The persistence can be associated with several executable files.

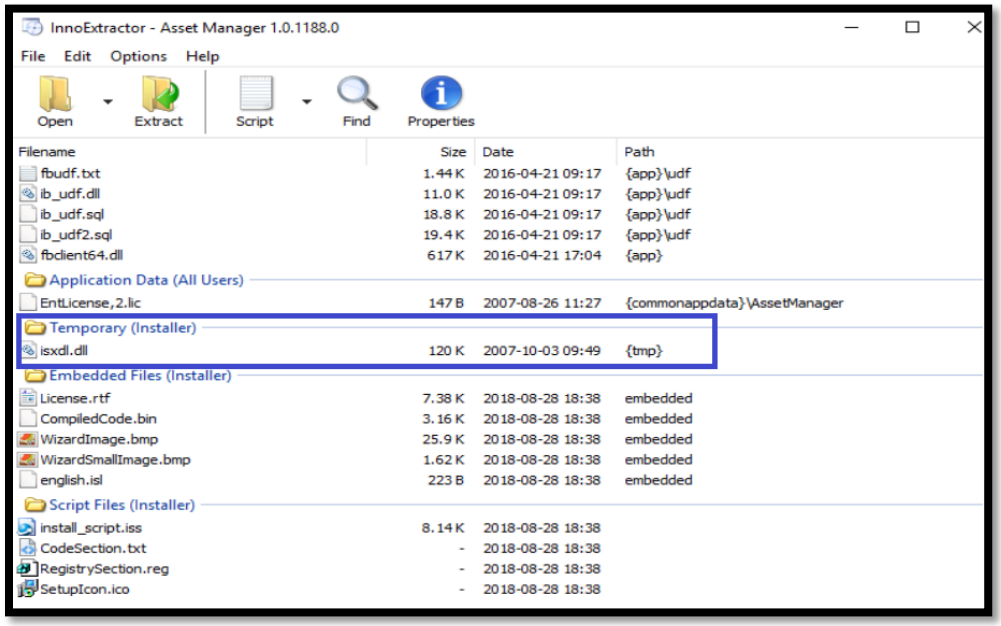


[1] https://docs.microsoft.com/en-us/cpp/build/reference/tsaware-create-terminal-server-aware-application

In specific, the file isxdl.dll[2] has the property to create and remove itself.

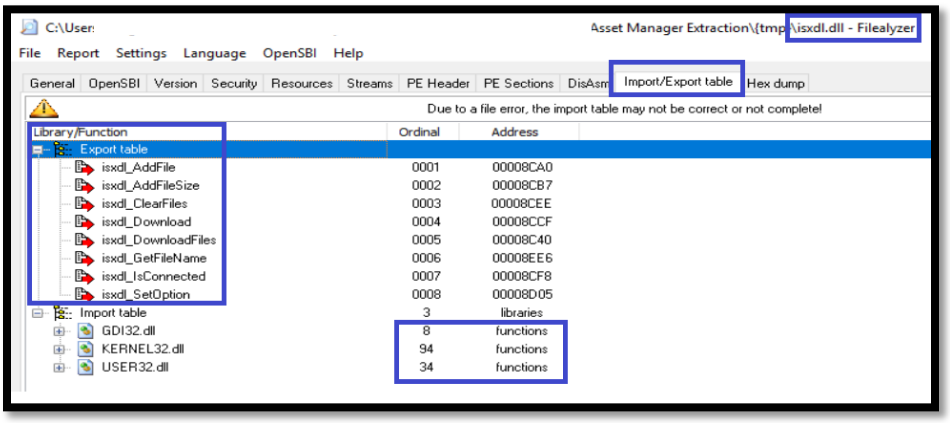


The software has some compressed data. A more detailed information was found after an extraction in the file:

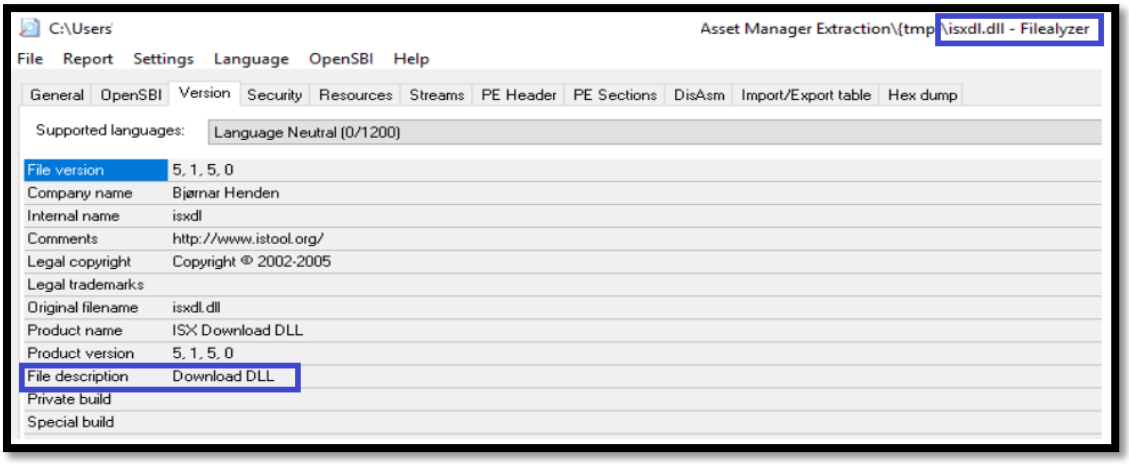


[2] https://www.virustotal.com/#/file/316bd2debfdf74eace797fb2a37e351a1517a23f2444371606b131e3bc74f8dc/behavior

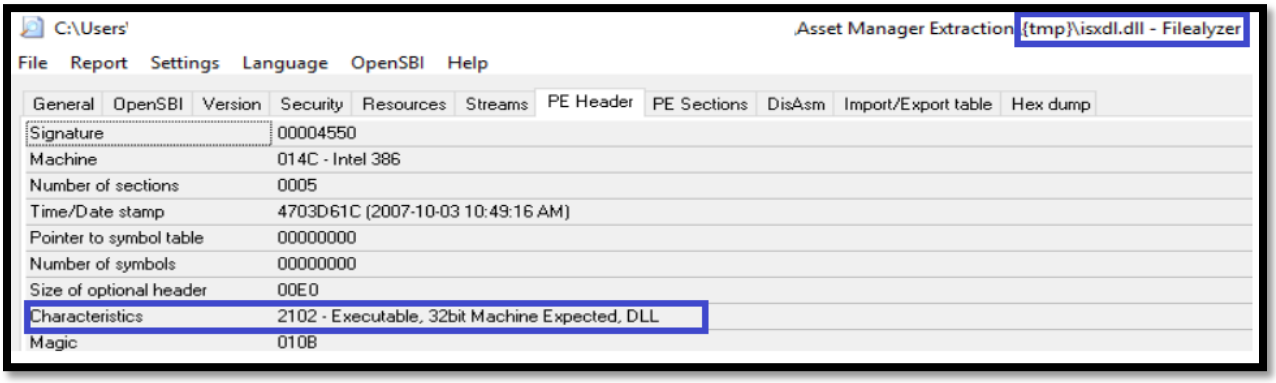
This is the attributes of the file, once the software is installed:



Note the capacity to download other dll:



It is possible to confirm the initial characteristics:

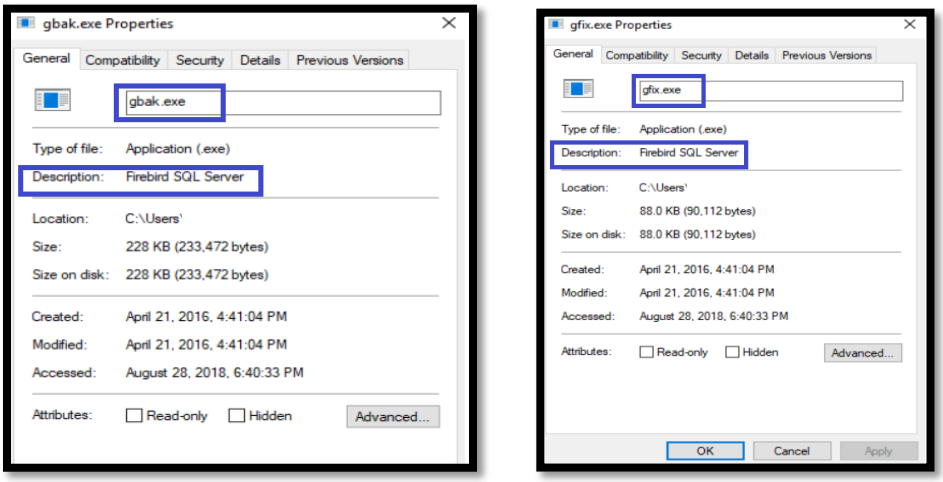


Suspicious File

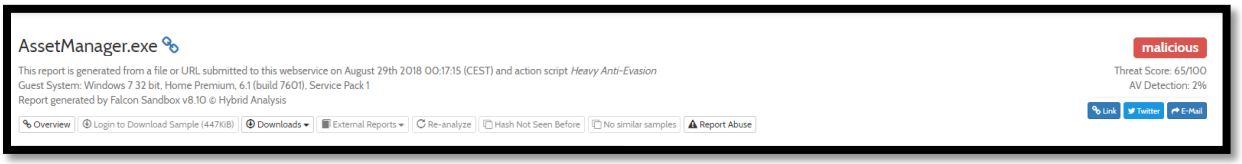
The file 996E.temp seems like a temporary file, but it is in fact an executable file, and possibly not a good one[3].

Executable files found after the extraction:

[3] http://www.exefilesupport.com/easy-guide-to-remove-996e-exe-from-pc

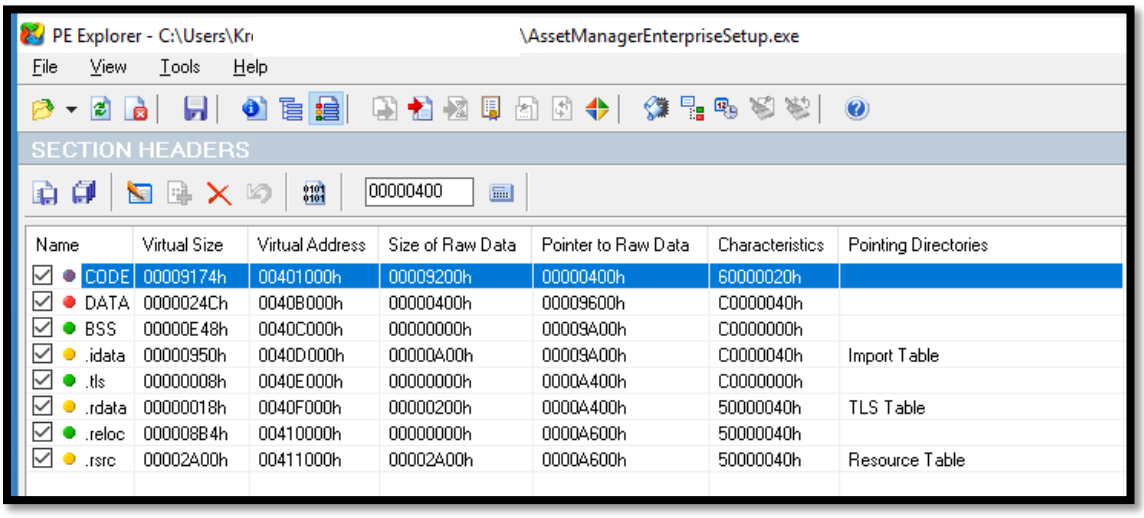


The "gfix.exe" and "gbak.exe" offers SQL capability and the AssetManager.exe was considered malicious[4]:

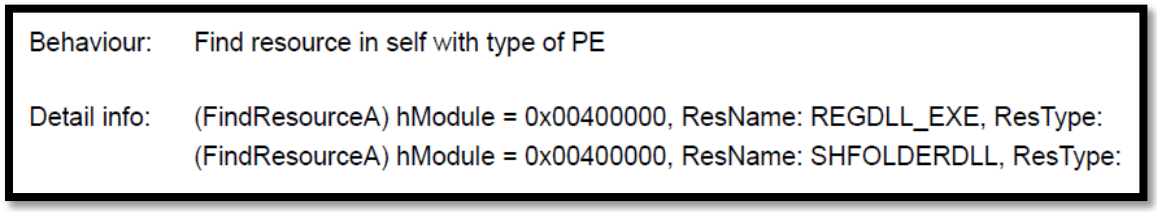


Pointing Directories

Since the software can point resources in to itself through the resource table, it is possible to identify two files with portable executable characteristics.



[4] https://www.hybrid-analysis.com/sample/b64187b4dc9b0ae5cd558a400af82675c93dcd8ea148c6785c668ebd112c0343/5b85d8fe7ca3e16eee36b374

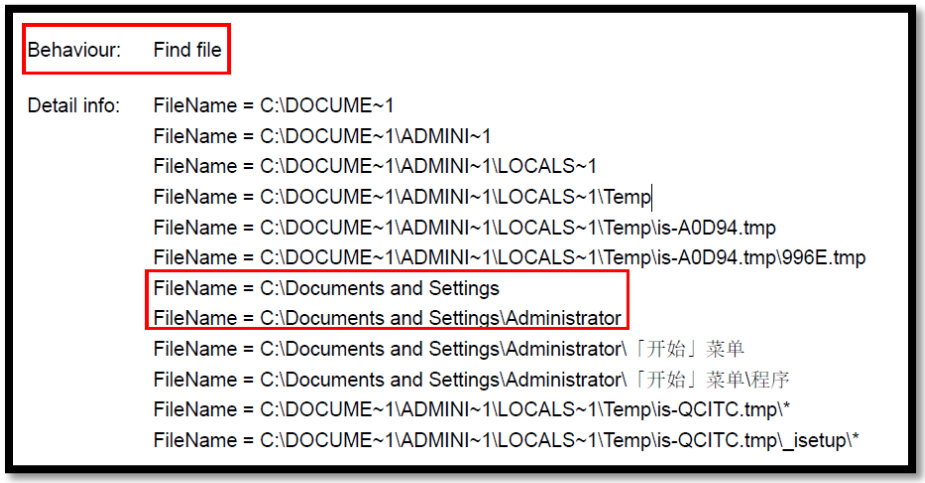


It is possible to note also the use of a TLS table[5]. Which can be used by the executable code to get the address of the TLS data area for the given program and module.

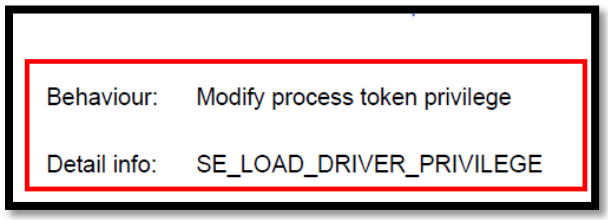
Suspicious Behaviours

Admin privilege

A tentative to identify administrator details.



Which can be useful if someone need to install new drivers:

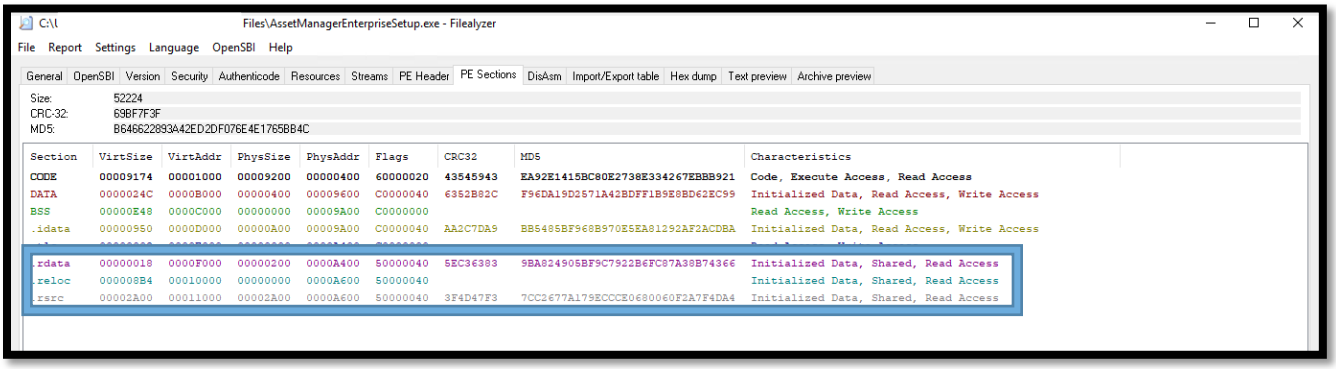


[5] https://docs.microsoft.com/en-us/windows/desktop/Debug/pe-format#the-tls-section

The software can create mutex functions to manage the shared resource from simultaneous access by multiple threads or processes[6]:

Behaviour:	Create mutex
Detail info:	CTF.LBES.MutexDefaultS-*
	CTF.Compart.MutexDefaultS-*
	CTF.Asm.MutexDefaultS-*
	CTF.Layouts.MutexDefaultS-*
	CTF.TMD.MutexDefaultS-*
	CTF.TimListCache.FMPDefaultS-*MUTEX.DefaultS-*
	MSCTF.Shared.MUTEX.EBH
	MSCTF.Shared.MUTEX.AFK

It is possible that the shared mutex might be related to data stored in the .rdata, .reloc, .rsrc:

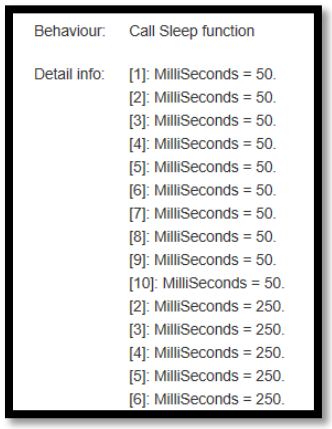


And the software has anti-debugging functions[7]:

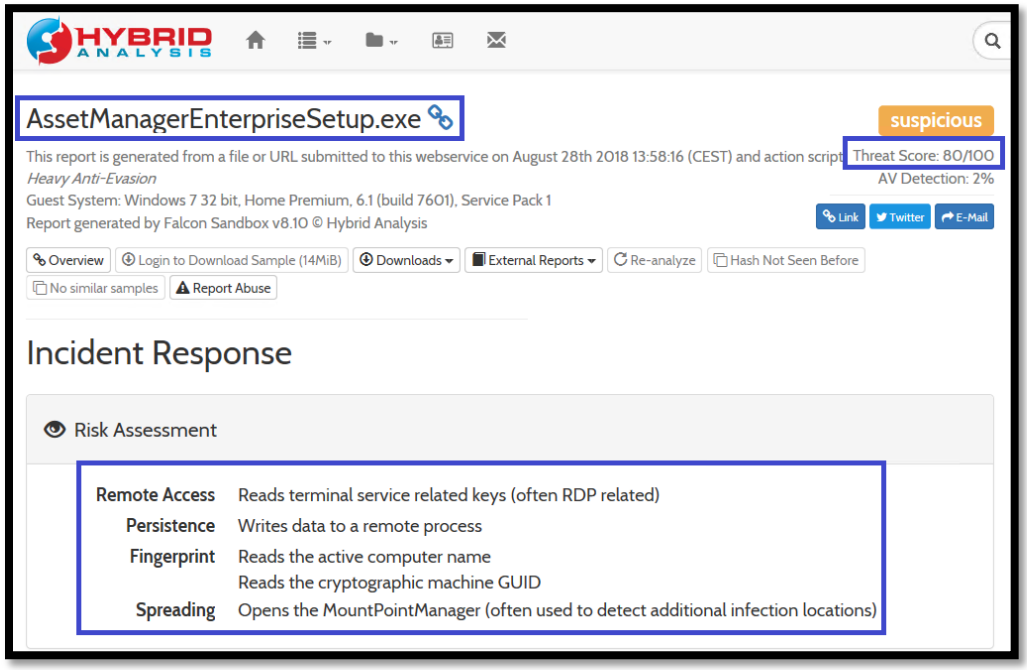
Behaviour:	Open event
Detail info:	HookSwitchHookEnabledEvent
	Global\crypt32LogoffEvent
	_fCanRegisterWithShellService
	CTF.ThreadMIConnectionEvent.00000714.00000000.00000012
	CTF.ThreadMarshalInterfaceEvent.00000714.00000000.00000013
	CTF.ThreadMIConnectionEvent.00000714.00000000.00000013
	MSCTF.SendReceiveConection.Event.EBH.IC
	MSCTF.SendReceive.Event.EBH.IC

[6] https://docs.microsoft.com/en-us/windows/desktop/sync/using-mutex-objects
[7] https://www.veracode.com/blog/2009/02/anti-debugging-series-part-iv

A possible evasion technique could be in place using a sleep technique:

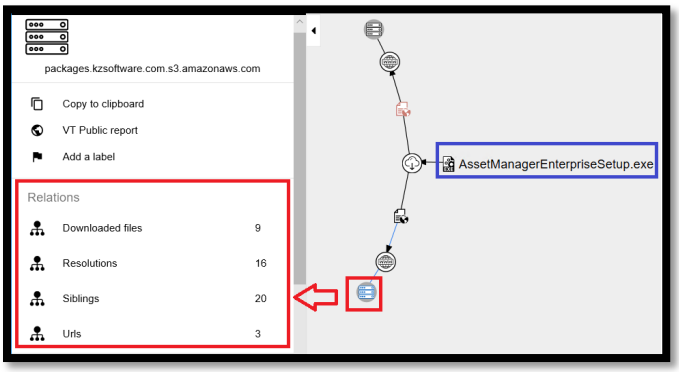


Identified Risks[8]



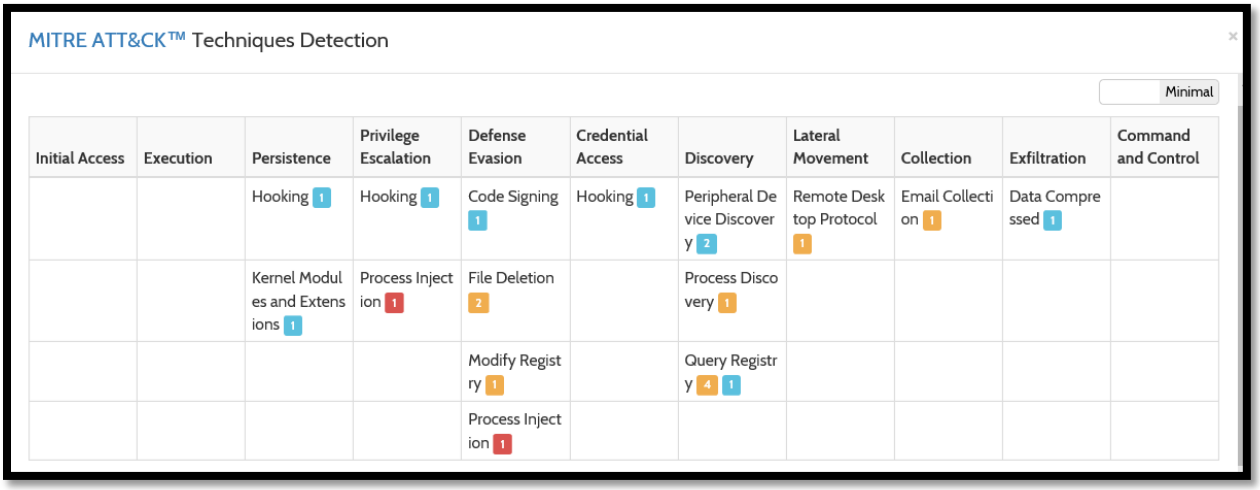
[8] https://www.hybrid-analysis.com/sample/316bd2debfdf74eace797fb2a37e351a1517a23f2444371606b131e3bc74f8dc?environmentId=100

Final Map



Attacks

The types of attacks can be selected from documented techniques[9].

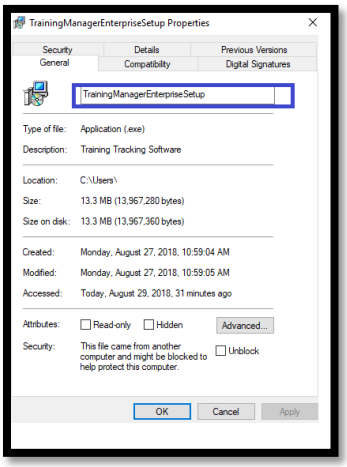


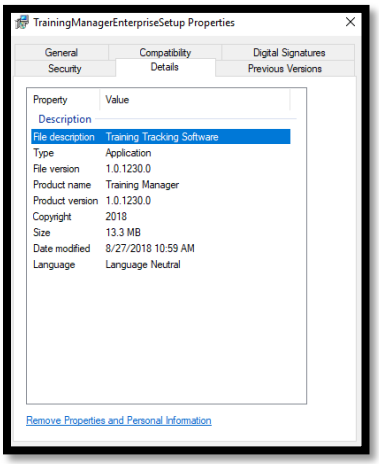
[9] https://www.hybrid-analysis.com/sample/316bd2debfdf74eace797fb2a37e351a1517a23f2444371606b131e3bc74f8dc

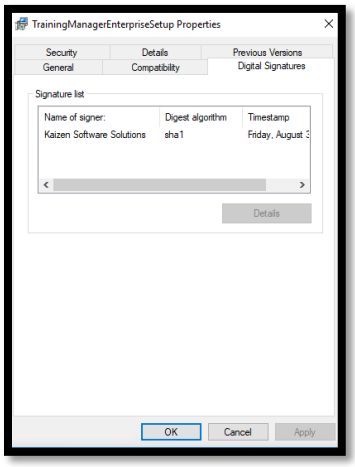
Replicated Approach (Training Manager)

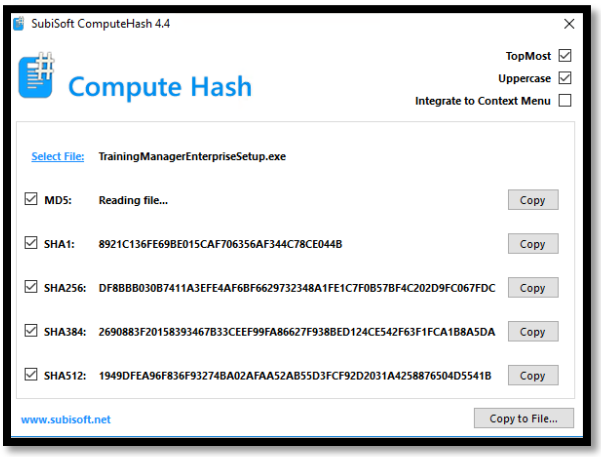
The Training Manager software share similar file structure and similar findings described in the Asset Manager.

File Analysis



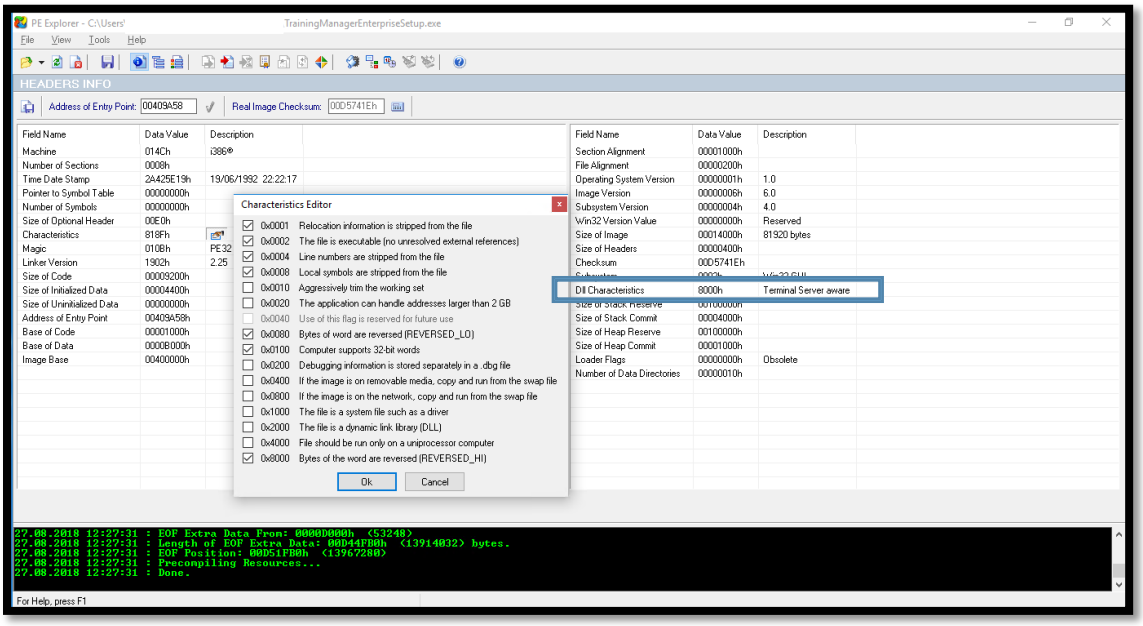




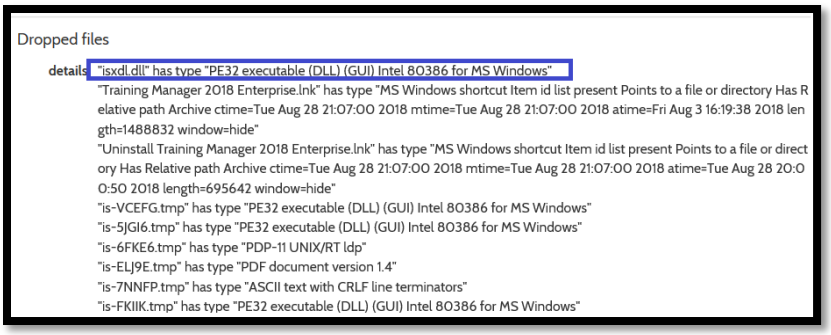


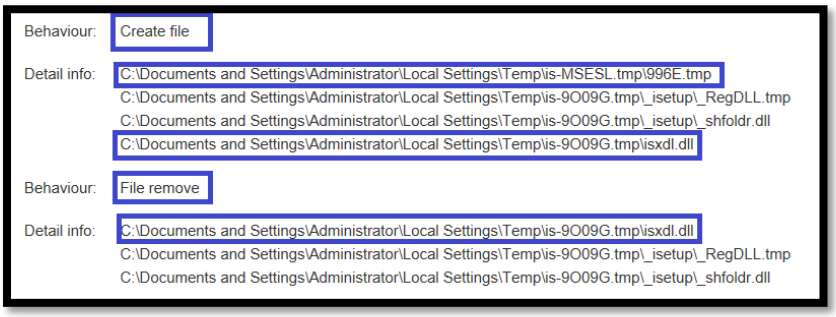
Red Flags

Terminal Server



Use the isxdl.dll and the 996E.tmp files[10] previously discussed.





[10]https://www.virustotal.com/#/file/df8bbb030b7411a3efe4af6bf6629732348a1fe1c7f0b57bf4c202d9fc067fdc/behavior

Behaviour:	Load addtional file
Detail info:	Image: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-9O09G.tmp\isxdl.dll.

Process And Service Actions

Permissions Requested

SE_LOAD_DRIVER_PRIVILEGE

Processes Terminated

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-MSESL.tmp\996E.tmp
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-HSJHD.tmp\996E.tmp

As the Asset Manager, the Training Manager also make changes in the Windows Directory

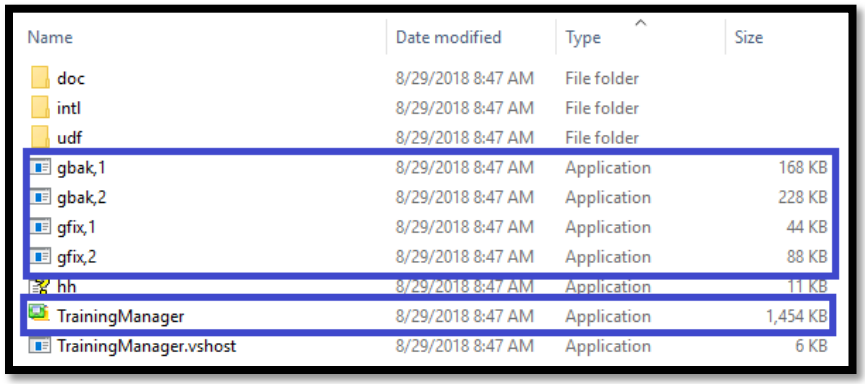
Touches files in the Windows directory

details "<Input Sample>" touched file "C:\Windows\AppPatch\sysmain.sdb"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\Fonts\StaticCache.dat"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\user32.dll.mui"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\Globalization\Sorting\SortDefault.nls"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\msctf.dll.mui"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\KernelBase.dll.mui"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\netmsg.dll"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\netmsg.dll.mui"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\shfolder.dll"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\imageres.dll"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\imageres.dll.mui"
"AssetManagerEnterpriseSetup.tmp" touched file "%APPDATA%\Microsoft\Windows\Start Menu"
"AssetManagerEnterpriseSetup.tmp" touched file "C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs"

Touches files in the Windows directory

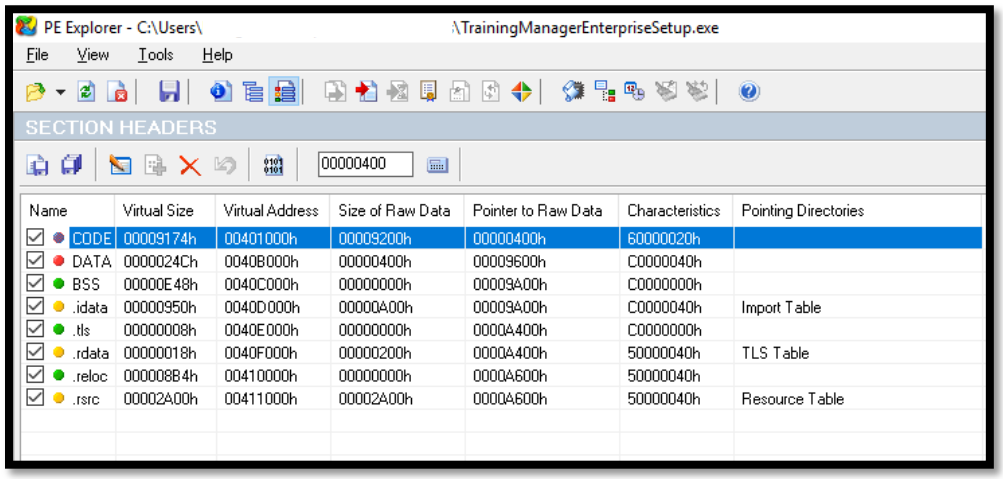
details "<Input Sample>" touched file "C:\Windows\System32\en-US\KernelBase.dll.mui"
"<Input Sample>" touched file "C:\Windows\System32\netmsg.dll"
"<Input Sample>" touched file "C:\Windows\System32\en-US\netmsg.dll.mui"
"<Input Sample>" touched file "C:\Windows\Globalization\Sorting\SortDefault.nls"
"<Input Sample>" touched file "C:\Windows\AppPatch\sysmain.sdb"
"TrainingManagerEnterpriseSetup.tmp" touched file "C:\Windows\Fonts\StaticCache.dat"
"TrainingManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\user32.dll.mui"
"TrainingManagerEnterpriseSetup.tmp" touched file "C:\Windows\Globalization\Sorting\SortDefault.nls"
"TrainingManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\msctf.dll.mui"
"TrainingManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\KernelBase.dll.mui"
"TrainingManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\netmsg.dll"
"TrainingManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\en-US\netmsg.dll.mui"
"TrainingManagerEnterpriseSetup.tmp" touched file "C:\Windows\System32\shfolder.dll"

After extraction similar files such as “gfix.exe” and “gbak.exe” were found:

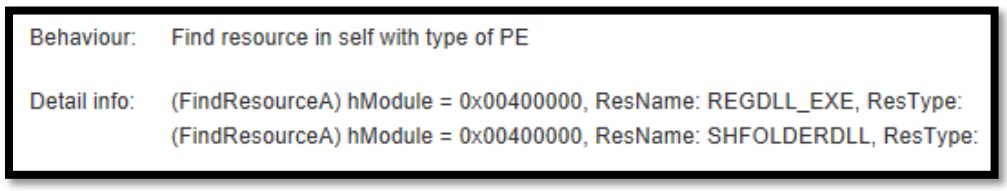


The Training Manager was considered malicious[11].

Similar Pointing Directories



Similar resources as executable files:



[11] https://www.hybrid-analysis.com/sample/c9a5607f8b33472ef60f1e3647d7863bcd6a28ad299f693bd44cea092e5bf176

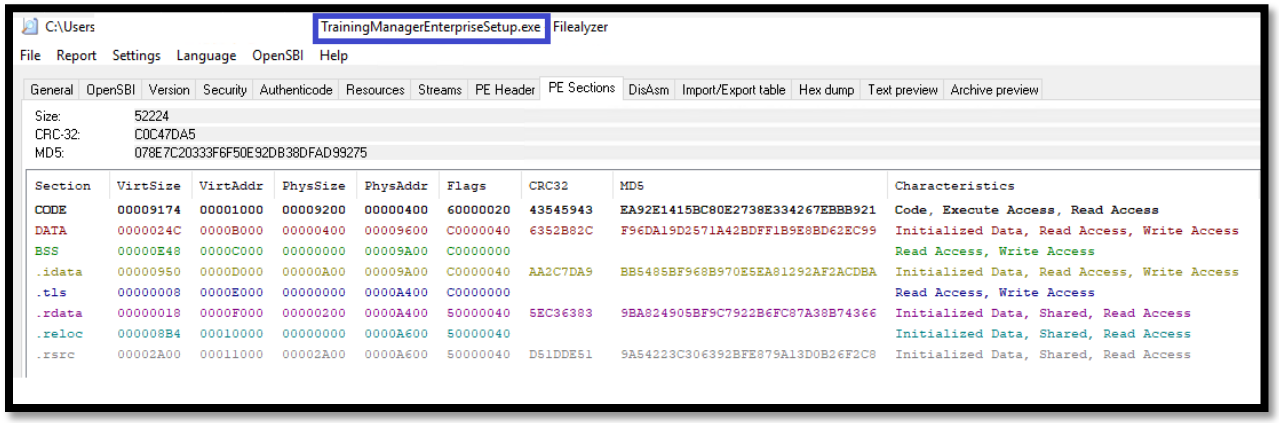
Similar identification of admin privileges:

Behaviour:	Find file
Detail info:	FileName = C:\DOCUME~1 FileName = C:\DOCUME~1\ADMINI~1 FileName = C:\DOCUME~1\ADMINI~1\LOCALS~1 FileName = C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp FileName = C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-MSESL.tmp FileName = C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-MSESL.tmp\996E.tmp FileName = C:\Documents and Settings FileName = C:\Documents and Settings\Administrator FileName = C:\Documents and Settings\Administrator\「开始」菜单 FileName = C:\Documents and Settings\Administrator\「开始」菜单\程序 FileName = C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-9O09G.tmp* FileName = C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-9O09G.tmp_isetup*

Use of Mutex

Behaviour:	Create mutex
Detail info:	CTF.LBES.MutexDefaultS-* CTF.Compart.MutexDefaultS-* CTF.Asm.MutexDefaultS-* CTF.Layouts.MutexDefaultS-* CTF.TMD.MutexDefaultS-* CTF.TimListCache.FMPDefaultS-*MUTEX.DefaultS-* MSCTF.Shared.MUTEX.EBH MSCTF.Shared.MUTEX.MEK

These are similar characteristics observed in each section:



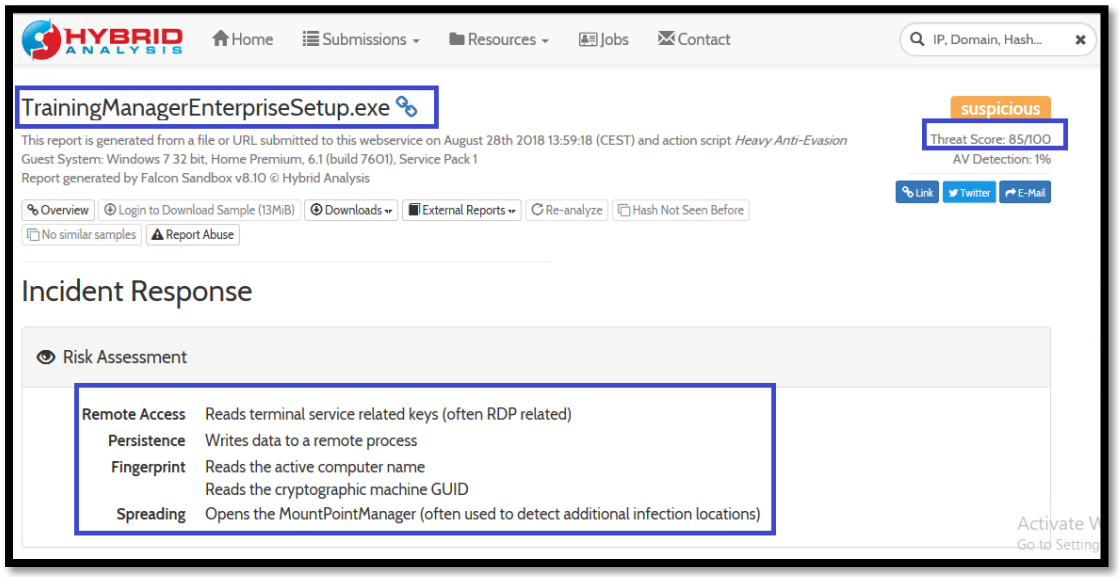
Aspects of anti-debugging functions:

Behaviour:	Open event
Detail info:	HookSwitchHookEnabledEvent Global\crypt32LogoffEvent _fCanRegisterWithShellService CTF.ThreadMIConnectionEvent.00000714.00000000.00000013 CTF.ThreadMarshalInterfaceEvent.00000714.00000000.00000014 CTF.ThreadMIConnectionEvent.00000714.00000000.00000014 MSCTF.SendReceiveConection.Event.EBH.IC MSCTF.SendReceive.Event.EBH.IC

Use of sleep function:

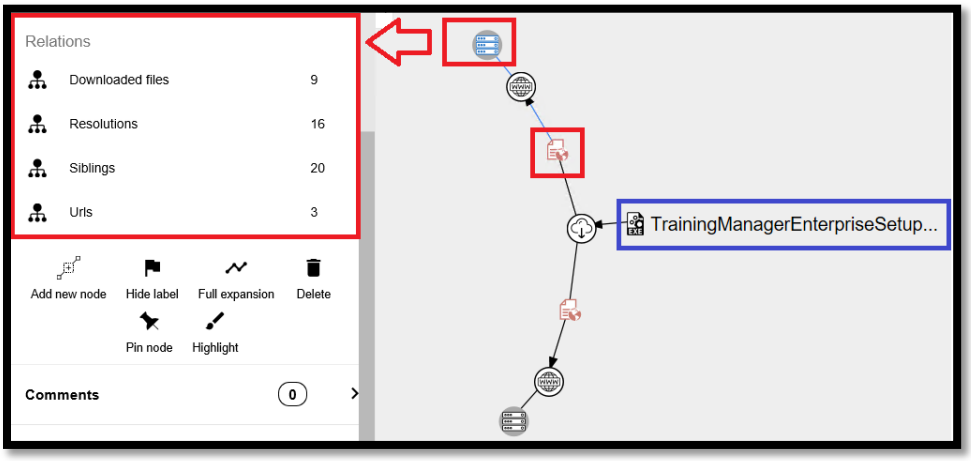
Behaviour:	Call Sleep function
Detail info:	[1]: MilliSeconds = 50. [2]: MilliSeconds = 50. [3]: MilliSeconds = 50. [4]: MilliSeconds = 50. [5]: MilliSeconds = 50. [6]: MilliSeconds = 50. [7]: MilliSeconds = 50. [8]: MilliSeconds = 50. [9]: MilliSeconds = 50. [10]: MilliSeconds = 50. [2]: MilliSeconds = 250. [3]: MilliSeconds = 250. [4]: MilliSeconds = 250. [5]: MilliSeconds = 250. [6]: MilliSeconds = 250.

Identified Risks[12]



[12] https://www.hybrid-analysis.com/sample/df8bbb030b7411a3efe4af6bf6629732348a1fe1c7f0b57bf4c202d9fc067fdc?environmentId=100

Final Map



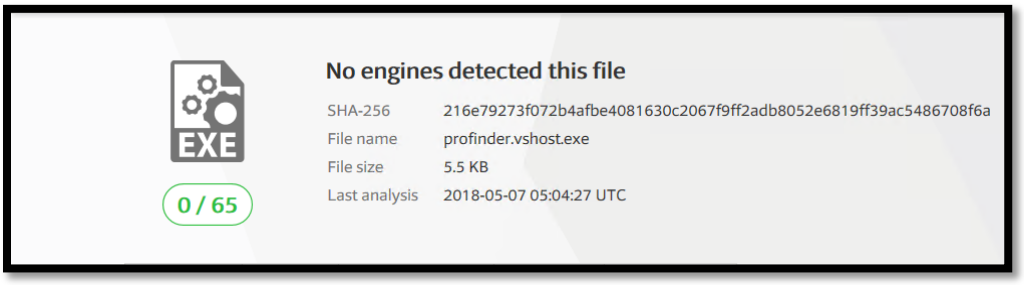
Possible Attacks

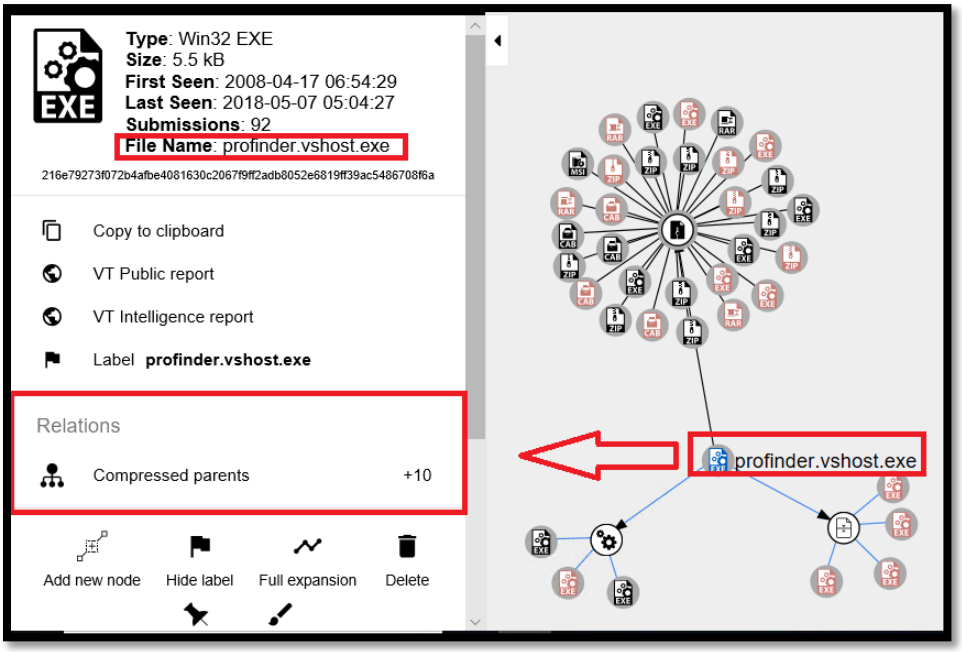
MITRE ATT&CK™ Techniques Detection

Minimal

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Hooking 1	Hooking 1	Code Signing 1	Hooking 1	Network Service Scanning 1	Remote Desktop Protocol 1		Data Compressed 1	
		Kernel Modules and Extensions 1	Process Injection 1	File Deletion 2		Peripheral Device Discovery 2				
				Modify Registry 1		Process Discovery 1				
				Process Injection 1		Query Registry 4 1				

Finally, an additional suspicious file was found in both software under the names of AssetManager.vshost and TrainingManager.vshost called "profinder.vshost.exe". In general, hosting process files (vshost.exe) are to be use by Microsoft Visual Studio and should not be run directly or deployed with an application[13].





Attack Techniques

Overall the vulnerabilities in both software are similar. A few differences were found in the Discovery section that in the Training Manager an attacker could use a Network Service Scanning technique and in the Asset Manager an Email Collection technique would be an additional attack alternative.

[13] https://msdn.microsoft.com/en-us/library/ms185331.aspx