### **Investigating Windows 2.0 — TryHackMe**

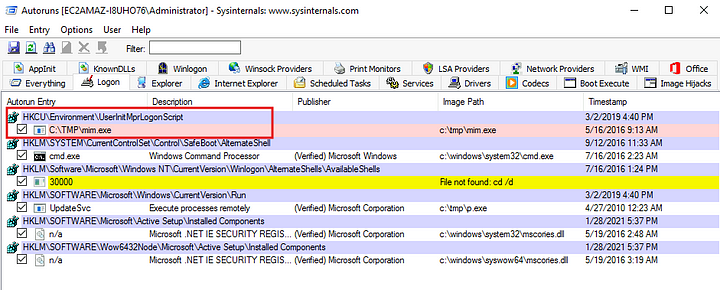
In the previous challenge you performed a brief analysis. Within this challenge, you will take a deeper dive into the attack.

**1.What registry key contains the same command that is executed within a scheduled task?**

We can check the task sceduler to check for any suspicious scheduled processes.



We can see a process named GameOver, which runs an executable file from the TMP directory. Now let us use autoruns tool to look at this closely. This tool is part of the sysinternals suite of tools which is used to view, analyze, and disable programs that automatically run at Windows startup.

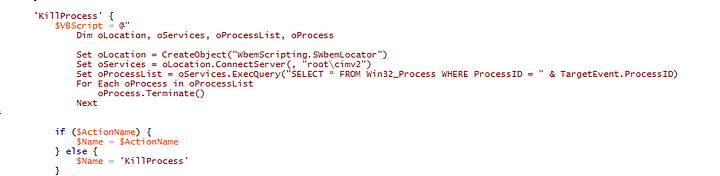


We can see refence to the same executable which we saw in the task scheduler.

Answer: HKCU\Environment\UserInitMprLogonScript

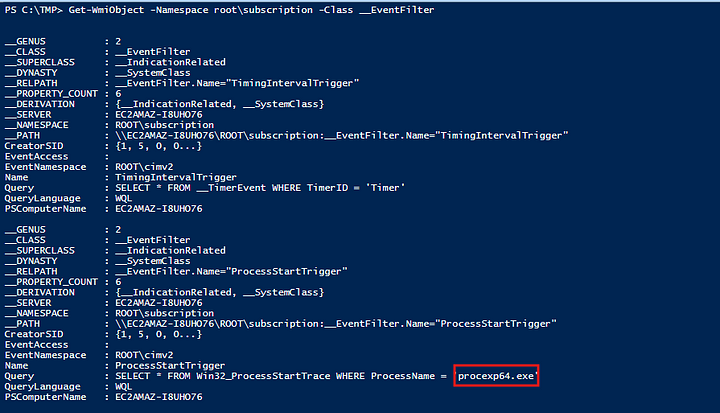
**2. What analysis tool will immediately close if/when you attempt to launch it?**

While analyzing the WMI backdoor I found that the attacker used WMI-based persistence, which hides in the system without creating visible files or services. I also found that it created a WMI object which will kill a specific process when triggered.



To find the exact process that is specified as a trigger I queried the ROOT\subscription namespace and found \_\_EventFilter objects that define when malicious actions should run

Get-WmiObject -Namespace ROOT\cimv2 -Class \_\_EventFilter



Answer: procexp64.exe

**3. What is the full WQL Query associated with this script?**

This is seen in the above screenshot



**Answer:** SELECT \* FROM Win32\_ProcessStartTrace WHERE ProcessName = ‘procexp64.exe’

**4. What is the script language?**

This is very clear from the syntax but, we can also confirm by the explicit definition of the interpreter to be used to run the script.



**Answer:** VBScript

**5. What is the name of the other script?**

In the above script I found another WMI ActiveScriptEventConsumer named LaunchBeaconingBackdoor that contains a **malicious VBScript** designed to beacon to a remote command-and-control server and execute instructions. This the answer to this question.

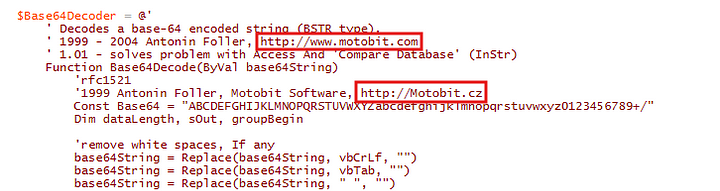
**Answer:** LaunchBeaconingBackdoor

**6. What is the name of the software company visible within the script?**

****

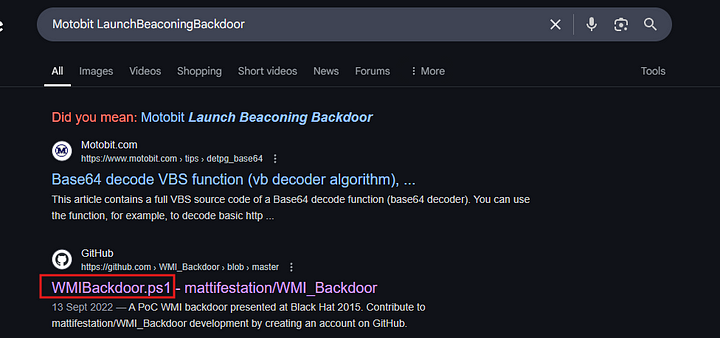
**Answer:** **Motobit Software**

**7. What 2 websites are associated with this software company? (answer, answer)**

****

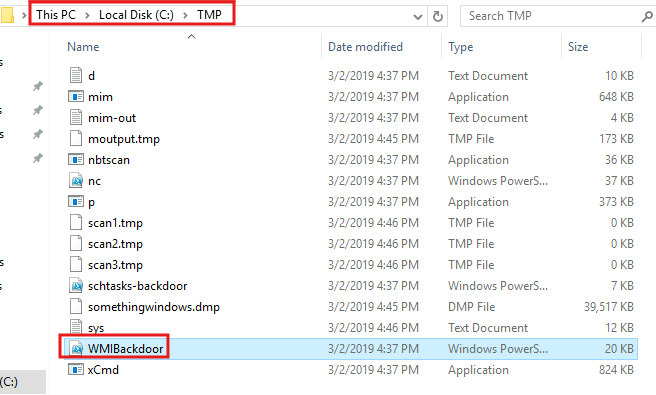
**Answer:** http://www.motobit.com,<http://motobit.cz>

**8. Search online for the name of the script from Q5 and one of the websites from the previous answer. What attack script comes up in your search?**

****

**Answer:** WMIBackdoor.ps1

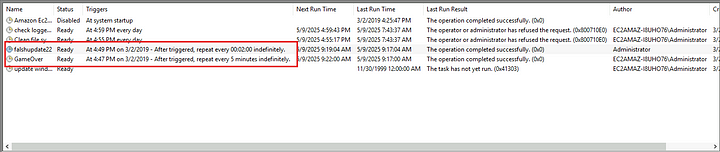
**9. What is the location of this file within the local machine?**

****

**Answer:** C:\TMP

**10. Which 2 processes open and close very quickly every few minutes? (answer, answer)**

In task sceduler we can see that there are only two tasks that are scheduled to run in regular intervals Flashupdate22 and GameOver.



And these are launcing powershell.exe and mim.exe respectively.

**Answer:** mim.exe, PowerShell.exe

**11. What is the parent process for these 2 processes?**

When we filter for powershell.exe and mim.exe in procmon64 we can find the Parent process Id is 924.

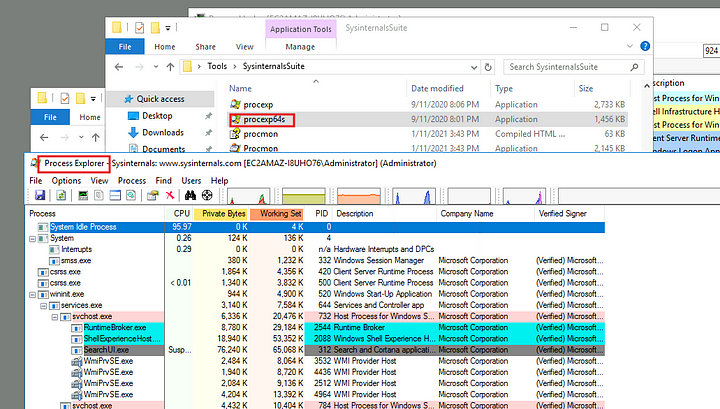


Now we can use Processhacker to find the proces related to this PID.



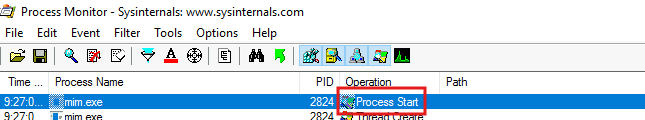
This is the parent process for these two processes.

We can also launch the process explorer by bypassing the script. We can bypass this by just reaming the process to a different name than procexp64. I renamed it to procexp64s and it launched without any problems.



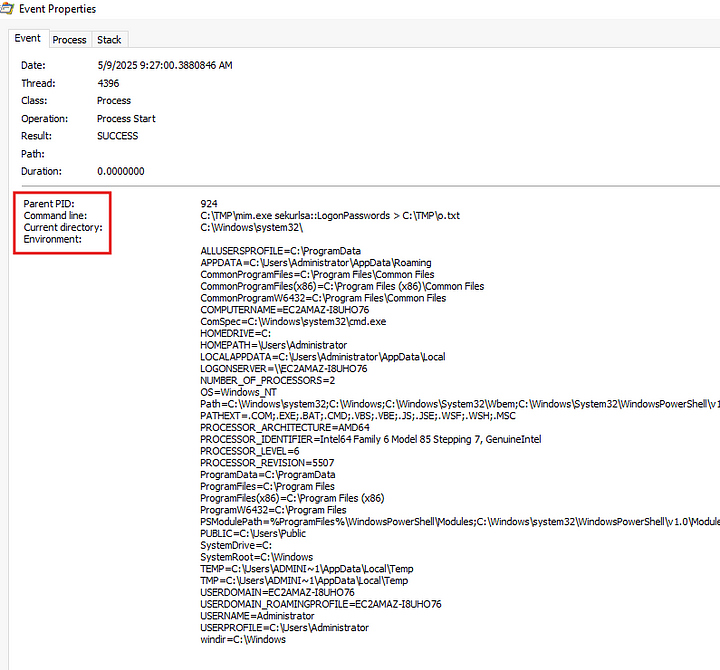
**Answer:** svchost.exe

**12. What is the first operation for the first of the 2 processes?**

****

Answer: Process create

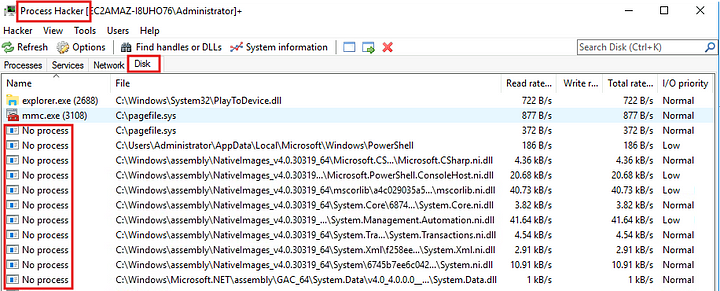
**13. Inspect the properties for the 1st occurrence of this process. In the Event tab what are the 4 pieces of information displayed? (answer, answer, answer, answer)**

****

**Answer:** Parent PID, Command line, Current directory, Environment

**14. Inspect the disk operations, what is the name of the unusual process?**

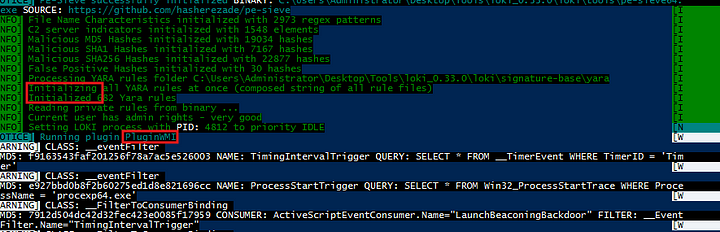
In process hacker, check the disk tab. There is a process called no process.



**Answer:** No Process

**15. Run Loki. Inspect the output. What is the name of the module after `Init`?**

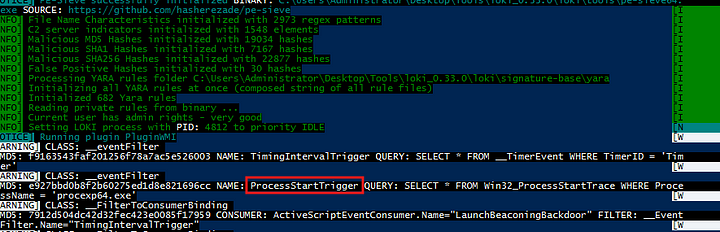
.\loki.exe -l output\_file



So as we can see above immediately after initialization loki is running a WMIScan

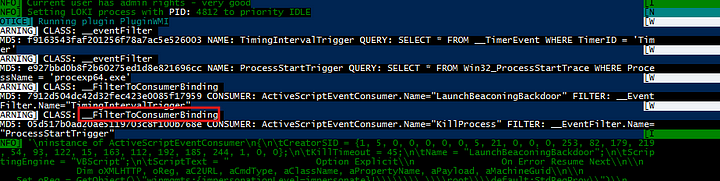
**Answer:** WMIScan

**16 .Regarding the 2nd warning, what is the name of the eventFilter?**

****

**Answer:** ProcessStartTrigger

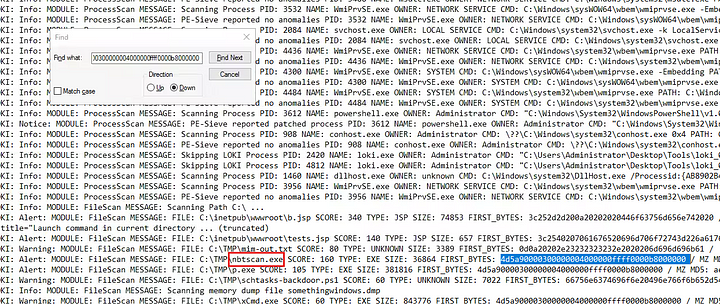
**17. For the 4th warning, what is the class name?**

****

**Answer:** \_\_FilterToConsumerBinding

**18. What binary alert has the following 4d5a90000300000004000000ffff0000b8000000 as FIRST\_BYTES?**

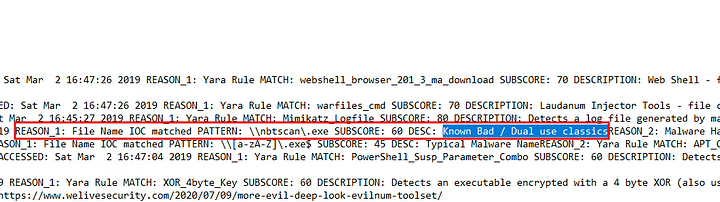
Open the output file of the loki scan and search for the given bytes.



**Answer:** nbtscan.exe

**19. According to the results, what is the description listed for reason 1?**

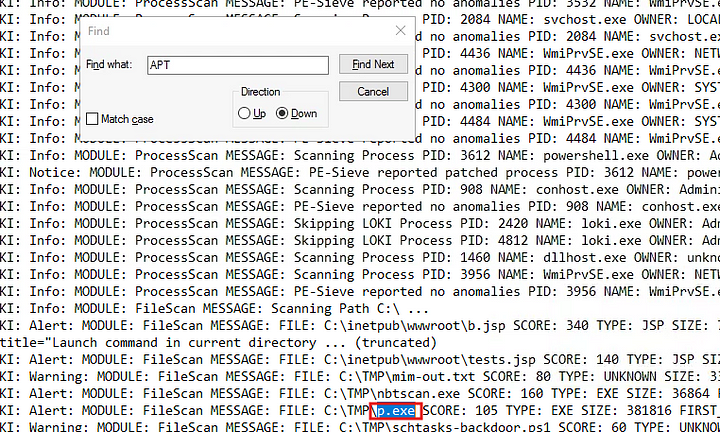
On the same line to the right there are reasons specified for why this file was flagged.



**Answer:** Known Bad / Dual use classics

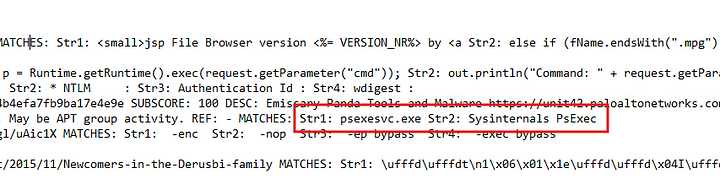
**20. Which binary alert is marked as APT Cloaked?**

Search for APT in the loki output file.



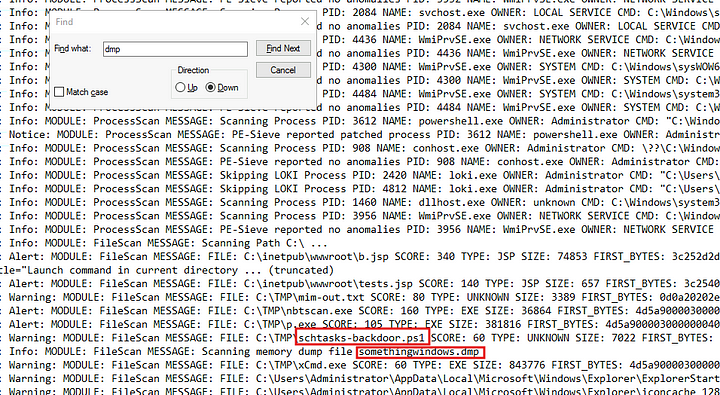
**Answer:** p.exe

**21. What are the matches? (str1, str2)**

****

**Answer:** psexesvc.exe, Sysinternals PsExec

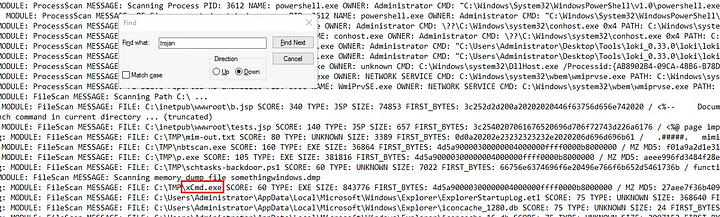
**22. Which binary alert is associated with somethingwindows.dmp found in C:\TMP?**

****

**Answer:** schtasks-backdoor.ps1

**23. Which binary is encrypted that is similar to a trojan?**

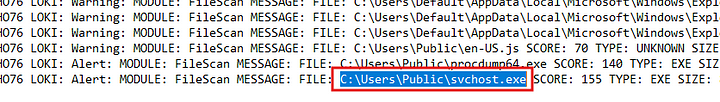
Search for trojan and on the found line scroll to the beginning of the line.



**Answer:** xCmd.exe

**24. There is a binary that can masquerade itself as a legitimate core Windows process/image. What is the full path of this binary?**

Earlier we identified that svchost.exe is the parent process for the two malicious processes. The path to svchost.exe is the answer to this.



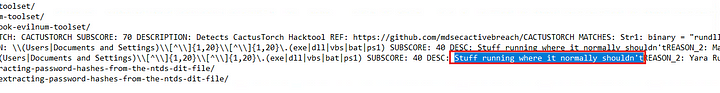
**Answer:** C:\Users\Public\svchost.exe

**25. What is the full path location for the legitimate version?**

The original path to svchost.exe is C:\Windows\System32\svchost.exe

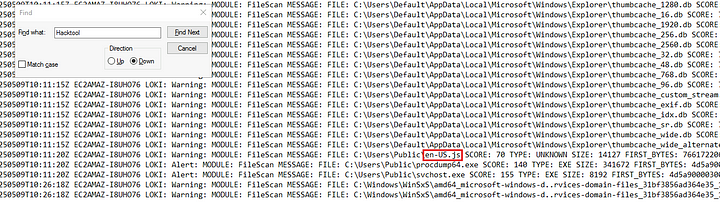
**Answer:** C:\Windows\System32\

**26. What is the description listed for reason 1?**

****

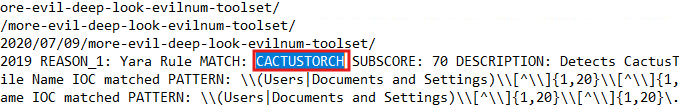
**Answer:** Stuff running where it normally shouldn’t

**27. There is a file in the same folder location that is labeled as a hacktool. What is the name of the file?**

****

**Answer:** en-US.js

**28. What is the name of the Yara Rule MATCH?**

****

**Answer:** CACTUSTORCH

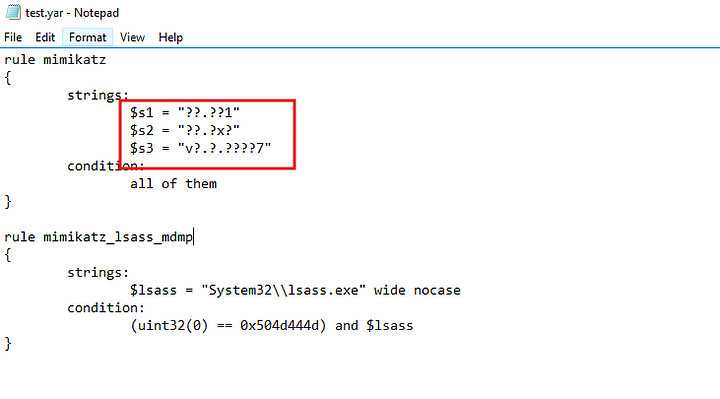
**29. Which binary didn’t show in the Loki results?**

mim.exe file is not detected in this scan. This means that the YARA rules does not contain the IOC’s regarding this file.

**Answer:** mim.exe

30. Complete the yar rule file located within the Tools folder on the Desktop. What are 3 strings to complete the rule in order to detect the binary Loki didn’t hit on? (answer, answer, answer)

First we will extract the strings from the mim.exe into a file called strings.txt. Now open the test.yar file

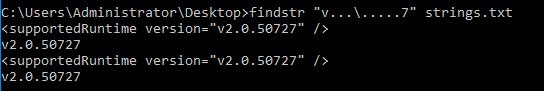
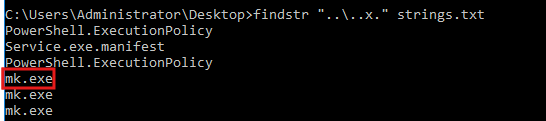
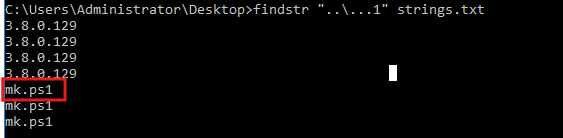


We can see that there are three strings, we need to pattern match with the extracted strings to find the exact strings that would match the mim.exe file. So we run three commands

findstr "..\...1" strings.txt

findstr "..\..x." strings.txt

findstr "v...\.....7" strings.txt



**Answer:** mk.ps1, mk.exe, v2.0.50727