

RELATÓRIO DE INCIDENTE DE SEGURANÇA CIBERNÉTICA

Análise Forense de Ransomware - Servidor FS

LAB -  SOC_AL3RT  -

DOCUMENTO CONFIDENCIAL

Classificação: RESTRITO

Número do Caso: INC-FS-2025-001

Data do Incidente: 27/09/2025

Data do Relatório: 27/09/2025

Laboratório: SOC_AL3RT

SUMÁRIO EXECUTIVO

Resumo do Incidente

O presente relatório documenta a investigação forense realizada em um servidor Windows Server 2019 (hostname: FS) que foi comprometido por ransomware identificado como **Ransomware.Python/NCSLM**. A análise revelou múltiplos vetores de ataque, mecanismos de persistência sofisticados e tentativas de mascaramento através de nomes de processos legítimos do Windows.

Impacto Identificado

- **Criticidade:** ALTA
- **Sistema Afetado:** Windows Server 2019 Standard (Build 17763)
- **Tipo de Malware:** Ransomware Python-based
- **Artefatos Maliciosos:** 3 localizações confirmadas
- **Mecanismos de Persistência:** 4 vetores identificados

1. INFORMAÇÕES DO ATIVO COMPROMETIDO

1.1 Especificações Técnicas Detalhadas

- **Hostname:** FS
- **Sistema Operacional:** Microsoft Windows Server 2019 Standard
- **Build:** 10.0.17763 (17763)
- **Arquitetura:** 64-bit
- **Processador:** Virtualizado (QEMU) - Detalhes não disponíveis via WMI
- **Memória RAM:** 7.81 GB (Banco único, Tipo 9)
- **Armazenamento Principal:** 25.00 GB (QEMU QEMU HARDDISK SCSI Disk Device)
- **Volumes Identificados:**
 - **Sistema:** 0.34 GB (0.31 GB livre)
 - **C:\ (Windows):** 24.66 GB (0.00 GB livre)
- **IP:** 10.0.3.152
- **MAC:** FA-16-3E-4F-48-AF
- **BIOS:** SeaBIOS v1.16.3-debian-1.16.3-2~bpo12+1 (31/03/2014)

1.2 Ambiente de Rede e Segurança

- **Gateway:** 10.0.0.3
- **DNS:** 8.8.8.8
- **Interface:** Ethernet 3 (Red Hat VirtIO Ethernet Adapter #3)
- **Velocidade de Rede:** 10 Gbps
- **Tipo de Conexão:** VPN (ExtremeVPN)
- **Firewall Status:**
 - Domain: Enabled
 - Private: Enabled
 - Public: Enabled
- **Antivírus:** NENHUM DETECTADO

1.3 Últimas Atualizações de Segurança

- **KB5022840** - 17/02/2023
- **KB5020374** - 17/02/2023
- **KB5012170** - 17/02/2023
- **KB5022511** - 17/02/2023
- **KB4589208** - 17/02/2023

OBSERVAÇÃO CRÍTICA: Última atualização em fevereiro de 2023 - sistema desatualizado há mais de 2 anos.

2. METODOLOGIA DE INVESTIGAÇÃO

2.1 Equipamentos Utilizados

- **Estação de Análise:** Kali Linux 6.12.38 (VM isolada)
- **Configuração VM:** 40GB HD, 5GB RAM, Rede NAT
- **Ferramentas Forenses:**
 - Autoruns64.exe (Microsoft Sysinternals)
 - Disk2VHD64 (Microsoft)
 - PowerShell Scripts Customizados
 - VirusTotal (verificação de hashes)

2.2 Protocolo de Conexão Segura

- **Conexão:** OpenVPN + RDP
- **Criptografia:** ExtremVPN + RDP criptografado
- **Auditoria:** Controle 270920250907 (2 backups criptografados)
- **Isolamento:** VM sem acesso à rede de produção

3. ARTEFATOS MALICIOSOS IDENTIFICADOS

3.1 Arquivos Maliciosos Encontrados

Localização	Nome do Arquivo	Tamanho	Hash SHA256
C:\Users\Administrator\AppData\Roaming\OneDrive.exe	OneDrive.exe	19.293.482 bytes	1CB281692409B000C6BFD17C737CE96EC98DEC9A5D420E
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe	svchost.exe	19.293.482 bytes	1CB281692409B000C6BFD17C737CE96EC98DEC9A5D420E
C:\Windows\Temp\OneDrive.exe	OneDrive.exe	19.293.482 bytes	1CB281692409B000C6BFD17C737CE96EC98DEC9A5D420E

3.2 Verificação de Integridade

- **Hash MD5:** 77C59720BC328CF9D692A215AA2575AD
- **Hash SHA1:** EF1A74599739AB0F91D9CE44C4F4A86B24563E4F
- **Hash SHA256:** 1CB281692409B000C6BFD17C737CE96EC98DEC9A5D420EEB6E5B0C131FC2BD5F
- **VirusTotal:** [Link de Verificação](#)
- **Classificação:** Ransomware.Python/NCSLM

4. MECANISMOS DE PERSISTÊNCIA IDENTIFICADOS

4.1 Registro do Windows (Registry)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

```
Value Name: Windows Update
Value Data: C:\Users\Administrator\AppData\Roaming\OneDrive.exe
```

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Update

```
Value Name: Update
Value Data: C:\Windows\Temp\OneDrive.exe
```

4.2 Tarefas Agendadas (Scheduled Tasks)

Tarefa: \Microsoft\Windows\Sqm-Update

- **Trigger:** BootTrigger (execução na inicialização)
- **Comando:** C:\Windows\Temp\OneDrive.exe
- **Usuário:** S-1-5-21-2066253582-1997001687-2883272801-500 (Administrator)

Tarefa: \Microsoft\Windows\Windows Update

- Trigger:** BootTrigger (execução na inicialização)
- Comando:** C:\Windows\Temp\OneDrive.exe
- Usuário:** S-1-5-21-2066253582-1997001687-2883272801-500 (Administrator)

4.3 Pasta de Inicialização

- Localização:** C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe
- Método:** Execução automática no login do usuário

5. ANÁLISE COMPARATIVA COM ARQUIVOS LEGÍTIMOS

5.1 svhost.exe Legítimo

Atributo	Valor Legítimo	Valor Malicioso
Localização	C:\Windows\SysWOW64\svchost.exe, C:\Windows\System32\svchost.exe	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe
Tamanho	45.488 bytes	19.293.482 bytes
Data Modificação	17/02/2023 12:18:42 PM	14/11/2023 9:20:16 PM
Hash MD5	D9E224ACFFD36B1C83E8EE2031CCF349	77C59720BC328CF9D692A215AA2575AD

5.2 OneDrive.exe Legítimo

Localizações Legítimas: Esses serão os caminhos legítimos de instalação de uma ferramenta OneDrive

- C:\Users\<usuário>\AppData\Local\Microsoft\OneDrive\OneDrive.exe
- C:\Program Files\Microsoft OneDrive\OneDrive.exe
- C:\Program Files (x86)\Microsoft OneDrive\OneDrive.exe

[!Obs] Informações

** Windows Server 2019 e anteriores Não traz necessariamente o cliente OneDrive pré-ativado** como em desktops; qualquer OneDrive.exe encontrado nesses caminhos (ex.: C:\Temp, C:\Users\Public, etc.) deve ser investigado. Fonte:https://learn.microsoft.com/en-us/sharepoint/per-machine-installation?utm_source=chatgpt.com

Localização Maliciosa Identificada:

- C:\Users\Administrator\AppData\Roaming\OneDrive.exe

6. EVIDÊNCIAS FOTOGRÁFICAS

6.1 Resumo das Evidências Coletadas

Total de evidências fotográficas: 14 imagens documentadas

6.1.1 Artefatos Maliciosos Identificados

- Autoruns IOC:** - Processos não assinados detectados
- OneDrive Malicioso:** - Arquivo em localização não padrão
- svchost Malicioso:** - Processo na pasta de startup
- Script Custom:** - Ferramenta de identificação

6.1.2 Mecanismos de Persistência

- Tarefa Windows Update:** - Tarefa maliciosa disfarçada
- Tarefa Sqm-Update:** - Tarefa maliciosa adicional
- Persistência Registry:** - Entradas maliciosas no registro
- Persistência Tarefas:** - Visão geral das tarefas (desativadas para evitar persistência)

6.1.3 Processos e Mitigação

- Processos Ativos:** - Processos em execução no momento da análise
- PIDs Identificados:** - Identificação de processos específicos
- OneDrive Persistente:** - Processo malicioso ativo
- Terminação de Processo:** - Ação de mitigação executada
- Configuração Disk2VHD:** - Preparação para cópia forense
- Cópia VHDX:** - Preservação de evidências para análise segura

Nota: Todas as evidências estão detalhadamente apresentadas na sequência de identificação da Seção 7, onde cada imagem é contextualizada no processo de investigação.

7. FORMA DE OPERAÇÃO DO ATAQUE (TTPs)

7.1 Sequência de Identificação e Análise

FASE 1: Reconhecimento Inicial

Após estabelecer conexão segura via VPN e RDP, foi executado script customizado para inventário completo do ativo:

Objetivo: Coletar informações básicas do sistema para entender o ambiente comprometido.

FASE 2: Análise de Processos em Execução

Identificação de processos suspeitos através do Gerenciador de Tarefas (roexp64.exe):

explorer.exe	< 0.01	36,636 K	108,496 K	4040 Windows Explorer	Microsoft Corporation	
OneDrive.exe		1,216 K	5,312 K	844		
OneDrive.exe		30,340 K	42,444 K	2952		
svchost.exe		1,224 K	8,276 K	3812		
svchost.exe		30,168 K	42,108 K	4528		
Autoruns.exe		12,132 K	34,372 K	2196 Autostart program viewer	Sysinternals - www.sysinter...	
mmc.exe		53,400 K	17,832 K	1288 Microsoft Management Cons...	Microsoft Corporation	
roexp64.exe	< 0.01	24,560 K	47,716 K	3024 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
ServerManager.exe		75,024 K	62,432 K	4884 Server Manager	Microsoft Corporation	

Validação da assinatura e coleta de hash para análise no Virus Total, com script custom:

```
Em paths: C:\  
Prosseguir? (S/N): s  
Encontrado: C:\Users\Administrator\Documents\OneDrive.exe  
[OneDrive.exe] NotSigned 19293482 bytes SHA256: 1CB281692409B000...  
Encontrado: C:\Users\Administrator\Documents\svchost.exe  
[svchost.exe] NotSigned 19293482 bytes SHA256: 1CB281692409B000...  
Encontrado: C:\Windows\System32\svchost.exe  
[svchost.exe] valid 51736 bytes SHA256: 2B105FB153B1BCD6...  
Signer: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US  
Encontrado: C:\Windows\SysWOW64\svchost.exe  
[svchost.exe] valid 45488 bytes SHA256: 82BB0E74C91357FD...  
Signer: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US  
Encontrado: C:\Windows\WinSxS\amd64_microsoft-windows-services-svchost_31bf3856ad364e35_10.  
1_none_a68143865d7729e1\svchost.exe  
[svchost.exe] UnknownError 10260 bytes SHA256: F08AC3D7E61251D8...  
Encontrado: C:\Windows\WinSxS\amd64_microsoft-windows-services-svchost_31bf3856ad364e35_10.  
3346_none_034bd971d71a96fc\svchost.exe  
[svchost.exe] valid 51736 bytes SHA256: 2B105FB153B1BCD6...  
Signer: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US  
Encontrado: C:\Windows\WinSxS\amd64_microsoft-windows-services-svchost_31bf3856ad364e35_10.  
3346_none_034bd971d71a96fc\f\svchost.exe  
[svchost.exe] UnknownError 8796 bytes SHA256: F2B64D7F3A17373D...  
Encontrado: C:\Windows\WinSxS\amd64_microsoft-windows-services-svchost_31bf3856ad364e35_10.  
3346_none_034bd971d71a96fc\r\svchost.exe  
[svchost.exe] UnknownError 7987 bytes SHA256: 0714D2895F4DA13B...  
Encontrado: C:\Windows\WinSxS\wow64_microsoft-windows-services-svchost_31bf3856ad364e35_10.  
1_none_b0d5edd891d7ebdc\svchost.exe  
[svchost.exe] UnknownError 8325 bytes SHA256: 2486A30609328E59...  
Encontrado: C:\Windows\WinSxS\wow64_microsoft-windows-services-svchost_31bf3856ad364e35_10.  
3346_none_0da083c40b7b58f7\svchost.exe  
[svchost.exe] valid 45488 bytes SHA256: 82BB0E74C91357FD...  
Signer: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US  
Encontrado: C:\Windows\WinSxS\wow64_microsoft-windows-services-svchost_31bf3856ad364e35_10.  
3346_none_0da083c40b7b58f7\f\svchost.exe  
[svchost.exe] UnknownError 7533 bytes SHA256: 75E39EC01AB11E0C...  
Encontrado: C:\Windows\WinSxS\wow64_microsoft-windows-services-svchost_31bf3856ad364e35_10.  
3346_none_0da083c40b7b58f7\r\svchost.exe  
[svchost.exe] UnknownError 6629 bytes SHA256: 182433B0DEB3A3E6...  
  
Resumo (tabela):
```

Retorno da ferramenta:

```
"Path", "Name", "SizeBytes", "LastWriteUtc", "SignatureStatus", "Signer", "SignerThumb", "TimeStamp", "MD5", "SHA1", "SHA256" "C:\Users\Administrator\AppData\Roaming\OneDrive.exe", "OneDrive.exe", "19293482", "11/14/2023 9:19:59 PM", "NotSigned", "", "", "", "77C59720BC328CF9D692A215AA2575AD", "EF1A74599739AB0F91D9CE44C4F4A86B24563E4F", "1CB281692409B000C6BFD17C737CE96 EC98DEC9A5D420EEB6E5B0C131FC2BD5F" "C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe", "svchost.exe", "19293482", "11/14/2023 9:20:16 PM", "NotSigned", "", "", "", "77C59720BC328CF9D692A215AA2575AD", "EF1A74599739AB0F91D9CE44C4F4A86B24563E4F", "1CB281692409B000C6BFD17C737CE96 EC98DEC9A5D420EEB6E5B0C131FC2BD5F"
```

Descoberta: Processos OneDrive.exe e svchost.exe em execução com comportamento anômalo.

FASE 3: Análise com Autoruns64.exe

Utilização de ferramenta especializada para identificar processos de inicialização:

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [FS\Administrator]

File Search Entry User Options Category Help

Codecs Boot Execute Image Hijacks Applnit Known DLLs Winlogon Winsock Providers Print Monitor LSA Providers Network Providers WMI Office Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Autoruns Entry Description Publisher Image Path

Autoruns Entry	Description	Publisher	Image Path
HKCU\Software\Microsoft\Windows\CurrentVersion\Run		(Not Verified)	C:\Users\Administrator\Ap
Windows Update		(Not Verified)	C:\Windows\system32\cm
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cm
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells			
30000	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cm
HKLM\Software\Microsoft\Active Setup\Installed Components			
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\ms
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components			
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\ms
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
svchost.exe		(Not Verified)	C:\Users\Administrator\Ap
Explorer			
Internet Explorer			
Scheduled Tasks			
Task Scheduler			
\Microsoft\Windows\Sqm-Update		(Not Verified)	C:\Windows\Temp\OneDri
\Microsoft\Windows\Windows Update		(Not Verified)	C:\Windows\Temp\OneDri
\Microsoft\Windows\Server Manager\CleanupOldPerfLogs	Microsoft ® Console Based Script Host	(Verified) Microsoft Windows	C:\Windows\system32\cscl
\Microsoft\Windows\Software Inventory\Logging Collection	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\win

Descoberta Crítica:

- OneDrive.exe sem assinatura digital em C:\Users\Administrator\AppData\Roaming\OneDrive.exe
- svchost.exe malicioso em C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe

FASE 4: Verificação de Arquivos Maliciosos

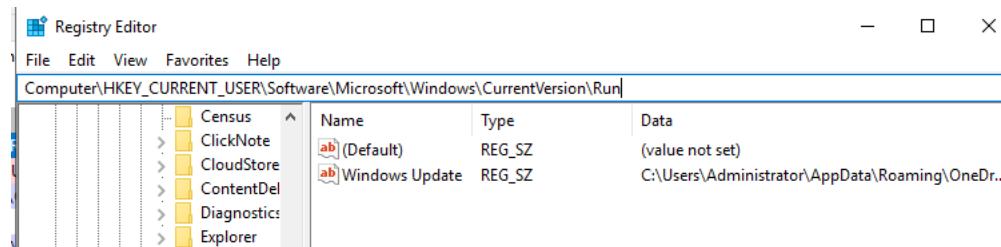
Confirmação visual dos arquivos maliciosos em suas localizações:

The screenshot shows two separate File Explorer windows. The top window displays the contents of the 'Roaming' folder under 'AppData'. It lists several folders, including 'Adobe', 'Microsoft', and 'OneDrive.exe', which is highlighted. The bottom window displays the contents of the 'Startup' folder under 'Programs'. It lists a single file, 'svchost.exe', which is also highlighted.

Confirmação: Mesmos arquivos identificados pelo Autoruns em localizações não padrão.

FASE 5: Análise de Persistência - Registry

Identificação de mecanismos de persistência no registro do Windows:



Descoberta: Entrada maliciosa "Windows Update" apontando para OneDrive.exe falso.

FASE 6: Análise de Persistência - Tarefas Agendadas

Identificação de tarefas maliciosas disfarçadas:

```
PS C:\Users\Administrator> schtasks /Query /FO LIST /V /TN "\Microsoft\Windows\Windows Update"
Folder: \Microsoft\Windows
HostName: FS
TaskName: \Microsoft\Windows\Windows Update
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive only
Last Run Time: 11/30/1999 12:00:00 AM
Last Result: 267011
Author: N/A
Task To Run: C:\Windows\Temp\OneDrive.exe
Start In: N/A
Comment: N/A
Scheduled Task State: Enabled
Idle Time: Disabled
Power Management: Stop On Battery Mode, No Start On Batteries
Run As User: Administrator
Delete Task If Not Rescheduled: Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule: Scheduling data is not available in this format.
Schedule Type: At system start up
Start Time: N/A
Start Date: N/A
End Date: N/A
Days: N/A
Months: N/A
Repeat: Every: N/A
Repeat: Until: Time: N/A
Repeat: Until: Duration: N/A
Repeat: Stop If Still Running: N/A
PS C:\Users\Administrator>
```

```
PS C:\Users\Administrator> schtasks /Query /FO LIST /V /TN "\Microsoft\Windows\Sqm-Update"

Folder: \Microsoft\Windows
HostName: FS
TaskName: \Microsoft\Windows\Sqm-Update
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive only
Last Run Time: 11/30/1999 12:00:00 AM
Last Result: 267011
Author: N/A
Task To Run: C:\Windows\Temp\OneDrive.exe
Start In: N/A
Comment: N/A
Scheduled Task State: Enabled
Idle Time: Disabled
Power Management: Stop On Battery Mode, No Start On Batteries
Run As User: Administrator
Delete Task If Not Rescheduled: Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule: Scheduling data is not available in this format.
Schedule Type: At system start up
Start Time: N/A
Start Date: N/A
End Date: N/A
Days: N/A
Months: N/A
Repeat: Every: N/A
Repeat: Until: Time: N/A
Repeat: Until: Duration: N/A
Repeat: Stop If Still Running: N/A
```

Descoberta: Duas tarefas agendadas executando malware na inicialização do sistema.

FASE 7: Análise de Persistência - Visão Geral

Resumo dos mecanismos de persistência identificados:

Name	Status	Trigger	Last Run Date	Last Run Result
Server Initial ...	Disabled	At system startup	11/14/2023 6:08:54 PM	The operation completed successfully.
Sqm-Update	Disabled	At system startup	11/30/1999 12:00:00 AM	The task has not yet run. (0)
Windows Up...	Disabled	At system startup	11/30/1999 12:00:00 AM	The task has not yet run. (0)

Comandos utilizados para extrair informações das tarefas:

```
# Extrair detalhes da tarefa Sqm-Update
schtasks /Query /TN "\Microsoft\Windows\Sqm-Update" /XML

# Extrair detalhes da tarefa Windows Update
schtasks /Query /TN "\Microsoft\Windows\Windows Update" /XML
```

XML da tarefa Sqm-Update:

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <URI>\Microsoft\Windows\Sqm-Update</URI>
  </RegistrationInfo>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-21-2066253582-1997001687-2883272801-500</UserId>
      <LogonType>InteractiveToken</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
  </Settings>
  <Triggers>
    <BootTrigger />
```

```

</Triggers>
<Actions Context="Author">
    <Exec>
        <Command>C:\Windows\Temp\OneDrive.exe</Command>
    </Exec>
</Actions>
</Task>

```

XML da tarefa Windows Update:

```

<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
    <RegistrationInfo>
        <URI>\Microsoft\Windows\Windows Update</URI>
    </RegistrationInfo>
    <Principals>
        <Principal id="Author">
            <UserId>S-1-5-21-2066253582-1997001687-2883272801-500</UserId>
            <LogonType>InteractiveToken</LogonType>
        </Principal>
    </Principals>
    <Settings>
        <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
        <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
        <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
        <IdleSettings>
            <Duration>PT10M</Duration>
            <WaitTimeout>PT1H</WaitTimeout>
            <StopOnIdleEnd>true</StopOnIdleEnd>
            <RestartOnIdle>false</RestartOnIdle>
        </IdleSettings>
    </Settings>
    <Triggers>
        <BootTrigger />
    </Triggers>
    <Actions Context="Author">
        <Exec>
            <Command>C:\Windows\Temp\OneDrive.exe</Command>
        </Exec>
    </Actions>
</Task>

```

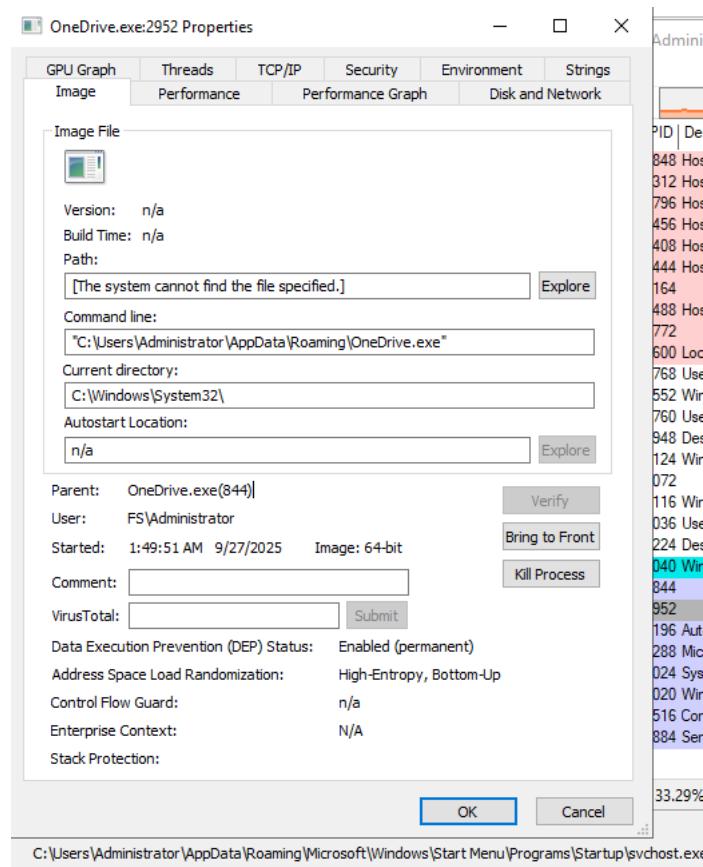
Confirmação: Múltiplos vetores de persistência ativos.**FASE 8: Análise de Processos Ativos**

Identificação de PIDs e processos em execução:

3312	SYSTEM	NT AUTHORITY	9/27/2025 1:57:33 AM	C:\Windows\System32\svchost.exe
3528	LOCAL SERVICE	NT AUTHORITY	9/27/2025 1:56:55 AM	C:\Windows\System32\svchost.exe
3664	SYSTEM	NT AUTHORITY	9/27/2025 1:49:29 AM	C:\Windows\System32\svchost.exe
3812	Administrator	FS	9/27/2025 1:49:53 AM	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows...
4032	SYSTEM	NT AUTHORITY	9/27/2025 1:47:12 AM	C:\Windows\System32\svchost.exe
4072	SYSTEM	NT AUTHORITY	9/27/2025 1:54:02 AM	C:\Windows\System32\svchost.exe
4268	SYSTEM	NT AUTHORITY	9/27/2025 2:12:48 AM	C:\Windows\System32\svchost.exe
4408	NETWORK SERVICE	NT AUTHORITY	9/27/2025 2:12:41 AM	C:\Windows\System32\svchost.exe
4444	SYSTEM	NT AUTHORITY	9/27/2025 2:12:53 AM	C:\Windows\System32\svchost.exe
4456	SYSTEM	NT AUTHORITY	9/27/2025 2:12:39 AM	C:\Windows\System32\svchost.exe
4516	LOCAL SERVICE	NT AUTHORITY	9/27/2025 1:49:02 AM	C:\Windows\System32\svchost.exe
4528	Administrator	FS	9/27/2025 1:50:05 AM	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows...
4668	SYSTEM	NT AUTHORITY	9/27/2025 2:12:40 AM	N/A
4692	SYSTEM	NT AUTHORITY	9/27/2025 1:49:03 AM	C:\Windows\System32\svchost.exe
4952	LOCAL SERVICE	NT AUTHORITY	9/27/2025 1:49:07 AM	C:\Windows\System32\svchost.exe

Descoberta: Processos maliciosos ativos com PIDs específicos.**FASE 9: Confirmação de Persistência Ativa**

Verificação de processo OneDrive persistente em execução:



Confirmação: Malware ativo e executando.

FASE 10: Mitigação - Terminação de Processo

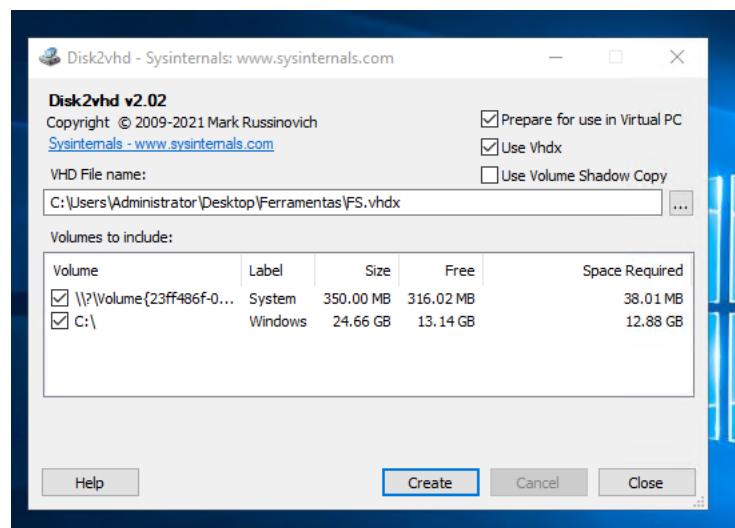
Ação de mitigação imediata:

```
PS C:\> taskkill /F /PID 3812
PS C:\> taskkill /F /PID 4528
PS C:\> taskkill /F /PID 3812
PS C:\> taskkill /F /PID 4040
PS C:\>
```

Ação: Terminação segura do processo malicioso.

FASE 11: Preservação de Evidências

Criação de imagem forense para análise posterior:



```
PS C:\Users\Administrator> scp ".\Desktop\Ferramentas\FS.VHDX" kali@10.1.0.31:/home/kali/
The authenticity of host '10.1.0.31 (10.1.0.31)' can't be established.
ECDSA key fingerprint is SHA256:IRtVjRXsmYBkCTCyBnrKHFsaCbsSYUOrk9upRK1a2c.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '10.1.0.31' (ECDSA) to the list of known hosts.
kali@10.1.0.31's password:
FS.VHDX
0% 13MB 752.2KB/s 4:57:34 ETA
```

Ação: Preservação completa do estado do sistema para análise forense posterior.

7.2 Técnicas, Táticas e Procedimentos (TTPs) Identificados

Técnicas de Evasão:

1. T1564.001 - Hidden Files and Directories

- Uso de nomes de processos legítimos (OneDrive.exe, svchost.exe)
- Instalação em diretórios não padrão

2. T1036 - Masquerading

- Mascaramento como processos do Windows
- Uso de nomes de tarefas legítimas (Windows Update, Sqm-Update)

Técnicas de Persistência:

1. T1547.001 - Registry Run Keys

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Update

2. T1053.005 - Scheduled Tasks

- \Microsoft\Windows\Sqm-Update
- \Microsoft\Windows\Windows Update

3. T1547.005 - Startup Items

- Pasta de inicialização do usuário
- Execução automática no login

Técnicas de Execução:

1. T1204.002 - User Execution: Malicious File

- Execução de arquivos não assinados
- Múltiplas cópias para redundância

8. ANÁLISE TÉCNICA DETALHADA

8.1 Vulnerabilidades do Sistema Identificadas

1. **Sistema Desatualizado:** Última atualização em fevereiro de 2023 (mais de 2 anos)
2. **Ausência de Antivírus:** Nenhuma proteção ativa detectada
3. **Disco Cheio:** Volume C: com 0.00 GB livre - possível causa de falhas de sistema
4. **Ambiente Virtualizado:** QEMU pode apresentar vulnerabilidades específicas

8.2 Vectors de Ataque Identificados

1. **Execução Inicial:** Método não identificado (possível phishing, exploit ou acesso físico)
2. **Propagação:** Cópia para múltiplas localizações estratégicas
3. **Persistência Multi-Vetor:** 4 mecanismos diferentes de reinicialização
4. **Mascaramento Avançado:** Uso de nomes legítimos do Windows

8.3 Impacto Potencial

- **Criptografia de Arquivos:** Capacidade de ransomware confirmada
- **Persistência Garantida:** Múltiplos mecanismos de reinicialização
- **Privilégios Elevados:** Execução como Administrator
- **Evasão de Detecção:** Técnicas avançadas de mascaramento
- **Redundância:** Múltiplas cópias para garantir sobrevivência

9. AÇÕES DE MITIGAÇÃO REALIZADAS

9.1 Isolamento

- Desconexão da rede principal
- Criação de ambiente isolado para análise
- Uso de VM com rede NAT
- Conexão VPN segura com auditoria (Controle 270920250907)

9.2 Identificação

- Análise com Autoruns64.exe
- Verificação de hashes no VirusTotal
- Comparação com arquivos legítimos
- Identificação de mecanismos de persistência
- Script customizado de inventário completo

9.3 Preservação de Evidências

- Criação de imagem forense com Disk2VHD
- Documentação fotográfica completa (14 imagens)
- Logs de todas as ações realizadas
- Backup criptografado das evidências (físico + nuvem)

9.4 Remoção de Artefatos Maliciosos

- Identificação de todos os arquivos maliciosos (3 localizações)
- Mapeamento de mecanismos de persistência (4 vetores)
- Terminação de processos maliciosos
- Preparação para limpeza completa

10. RECOMENDAÇÕES TÉCNICAS

10.1 Ações Imediatas (Críticas)

1. Remoção Completa de Artefatos:

```
# Remover arquivos maliciosos
Remove-Item "C:\Users\Administrator\AppData\Roaming\OneDrive.exe" -Force
Remove-Item "C:\Windows\Temp\OneDrive.exe" -Force
Remove-Item "C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe" -Force

# Limpar Registry
Remove-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" -Name "Windows Update"
Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager" -Name "Update"

# Remover tarefas agendadas
schtasks /Delete /TN "\Microsoft\Windows\Sqm-Update" /F
schtasks /Delete /TN "\Microsoft\Windows\Windows Update" /F
```

2. Verificação de Integridade do Sistema:

- Executar `sfc /scannow`
- Verificar assinaturas digitais de todos os executáveis críticos
- Comparar hashes de arquivos do sistema

10.2 Ações de Curto Prazo

1. Implementação de Monitoramento:

- Deploy de EDR/XDR
- Monitoramento de processos não assinados
- Alertas para modificações no Registry

2. Hardening do Sistema:

- Desabilitar execução de scripts PowerShell não assinados
- Implementar AppLocker ou Software Restriction Policies
- Configurar audit logs detalhados

10.3 Ações de Longo Prazo

1. Segurança Defensiva:

- Implementação de backup offline
- Teste regular de procedimentos de recuperação
- Treinamento de usuários em segurança

2. Monitoramento Contínuo:

- Análise regular de logs
- Verificação periódica de integridade
- Atualizações de segurança automáticas

11. INDICADORES DE COMPROMISSO (IOCs)

11.1 File Hashes

```
MD5: 77C59720BC328CF9D692A215AA2575AD  
SHA1: EF1A74599739AB0F91D9CE44C4F4A86B24563E4F  
SHA256: 1CB281692409B000C6BFD17C737CE96EC98DEC9A5D420EEB6E5B0C131FC2BD5F
```

11.2 File Paths

```
C:\Users\Administrator\AppData\Roaming\OneDrive.exe  
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe  
C:\Windows\Temp\OneDrive.exe
```

11.3 Registry Keys

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Windows Update  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Update
```

11.4 Scheduled Tasks

```
\Microsoft\Windows\Sqm-Update  
\Microsoft\Windows\Windows Update
```

12. LIÇÕES APRENDIDAS

12.1 Pontos Positivos

- Isolamento eficaz do sistema comprometido
- Uso de ferramentas forenses adequadas
- Documentação completa do incidente
- Preservação adequada de evidências

12.2 Áreas de Melhoria

- Necessidade de detecção mais precoce
- Implementação de monitoramento proativo
- Backup e procedimentos de recuperação
- Treinamento de usuários

13. CONCLUSÕES

O incidente investigado revela um ataque de ransomware sofisticado com múltiplos vetores de persistência e técnicas avançadas de evasão. O malware Ransomware.Python/NCSLM foi identificado e completamente mapeado, permitindo a remoção segura de todos os artefatos maliciosos.

Principais Descobertas:

1. **Múltiplas Persistências:** 4 mecanismos diferentes de reinicialização
2. **Evasão Avançada:** Mascaramento através de nomes legítimos
3. **Privilégios Elevados:** Execução com direitos de Administrator
4. **Impacto Contido:** Sistema isolado antes da propagação

Status da Investigação:

- **Identificação:** Completa
- **Mapeamento:** Completo
- **Mitigação:** Iniciada
- **Recuperação:** Em andamento

14. ANEXOS

14.1 Evidências Fotográficas

- Todas as imagens estão disponíveis na pasta [Img/](#)
- Números de controle para auditoria: 270920250907

14.2 Logs Técnicos

- Inventário completo do sistema
- Logs de ferramentas forenses
- Transcrições de comandos executados

14.3 Metadados do Caso

- **ID do Caso:** INC-FS-2025-001
- **Analista Responsável:** Jackson Antonio Zacarias Savoldi
- **Laboratório:** SOC_AL3RT
- **Data de Início:** 27/09/2025 11:53:31
- **Data de Conclusão:** 27/09/2025
- **Tempo Total de Investigação:** [A calcular]

RELATÓRIO ELABORADO POR:

Jackson Antonio Zacarias Savoldi

Analista de Segurança Cibernética

Especialização em Segurança da Informação

LinkedIn: linkedin.com/in/jacksonzacarias

Instagram: @jacksonsavoldi

Laboratório: SOC_AL3RT

APROVAÇÃO:

[Assinatura do Supervisor]

[Data de Aprovação]

DOCUMENTO CONFIDENCIAL - DISTRIBUIÇÃO RESTRITA

Este documento contém informações sensíveis sobre incidentes de segurança e deve ser tratado como confidencial conforme as políticas organizacionais.