BUNKER

CYBER SECURITY

Top 4 técnicas de

Movimentação Lateral

E-book contém um conjunto de técnicas de movimentação lateral comumente utilizadas por grupos criminosos e informações que vão ajudar as equipe de Blue Team a identificá-las e contextualizá-las: Análise de captura de rede, análise de telemetria de EDR, linhas de comando, dicas para investigação, etc

Dica: Siga a página da **Bunker Cyber Security no linkedin** para receber a segunda versão deste e-book com outras 6 técnicas adicionais que deverá ser lançado em Novembro/25.

Objetivo

Lateral Movement ou movimentação lateral é uma das piores fases de um ataque, pois o seu sucesso pode significar um incidente de grandes proporções, uma vez que permite um criminoso acessar ou manipular uma grande quantidade de computadores. Além disso, é difícil identificar uma ação legítima de uma ação manual, uma vez que ocorrem de forma muito similar. Lateral Movement aqui é uma forma de a partir de um hostA você conseguir executar um comando ou acessar informações em um host remoto.

O objetivo deste e-book é compartilhar conhecimento sobre os principais formas de movimentação lateral que observamos durante nossas atuações e também em leitura/estudos de relatórios de inteligência, incidentes, etc. Pretendemos apoiar os defensores a entender e simular as técnicas apropriadas em um ambiente controlado e para que possam se preparar para identificar este tipo de atividade em seu ambiente, antes que seja realizado por criminosos reais.

Disclaimer

A utilização das ferramentas mencionadas neste e-book é de total responsabilidade de quem as utilizar. Não nos responsabilizamos por inconvenientes que possam resultar através de ações em ambiente de produção utilizando as parte das orientações coletadas neste e-book. O conteúdo deste e-book não cobre toda e qualquer forma de movimentação lateral e existem formas de alterar o comportamento dos processos se realizados por criminosos mais habilidosos que podem “burlar” as dicas de investigação contidas neste e-book (i.e Customização de deployment do seviço do PSExec).

Outras formas de movimentação lateral (i.e paexec, services, scheduled task, dcom, etc) estão em fase de refinamento e o material será compartilhado com todos os seguidores da página da Bunker Cyber Security no linkedin.

Lista de Técnicas cobertas neste e-book:

Técnica 1 – RDP (i.e SharpRDP)

Técnica 2 – WMI over RPC/DCOM (i.e CrackMapExec)

Técnica 3 – WinRM (i.e PowerShell Remoting)

Técnica 4 – SMBv2 (i.e PSEXEC)

Técnica 1

BUNKER CYBER SECURITY

RDP

rdp

No.	Time	Source	Destination	Protocol	Lengtl	Info
1836	2025-10-08 18:16:18.665410	172.31.4.76	172.31.7.162	RDP	101	Cookie: mstshash=10BANK\al,
1873	2025-10-08 18:16:19.030587	172.31.7.162	172.31.4.76	RDP	73	Negotiate Response

```
> Frame 1836: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF_{D7F2A7
> Ethernet II, Src: 02:ab:bb:fc:77:95 (02:ab:bb:fc:77:95), Dst: 02:d1:6c:14:8a:05 (02:d1:6c:14:8a:05)
> Internet Protocol Version 4, Src: 172.31.4.76, Dst: 172.31.7.162
v Transmission Control Protocol, Src Port: 58954, Dst Port: 3389, Seq: 1, Ack: 1, Len: 47
    Source Port: 58954
    Destination Port: 3389

0000  02 d1
0010  00 57
0020  07 a2
0030  04 1a
0040  00 43
0050  68 3d
0060  00 0b
```

```
C:\Disk>SharpRDP.exe computername=ip-172-31-7-162.us-east-2.compute.internal command="tasklist" username=10bank\conector password=[redacted]
[+] Connected to          :  ip-172-31-7-162.us-east-2.compute.internal
[+] Execution priv type   :  non-elevated
[+] Executing tasklist
[+] Disconnecting from    :  ip-172-31-7-162.us-east-2.compute.internal
[+] Connection closed     :  ip-172-31-7-162.us-east-2.compute.internal
```

RDP (1) Overview

Mitre Technique T1021.001

Descrição
RDP é o método mais popular de administração de servidores Windows. Acessos RDP na maioria das vezes são legítimos, exceto, quando realizados por um grupo criminoso. Ferramentas de EDR ou Antivírus não conseguem diferenciar um acesso RDP legítimo de um acesso RDP suspeito, portanto, é uma das formas mais utilizadas por criminosos para realizar a movimentação lateral.

Ferramentas
As ferramentas mais utilizadas são o mstsc.exe (executável nativo do Windows) e o SharpRDP.exe (é uma forma de execução de código remoto – estilo psexec – geralmente utilizado para executar código em massa via RDP.

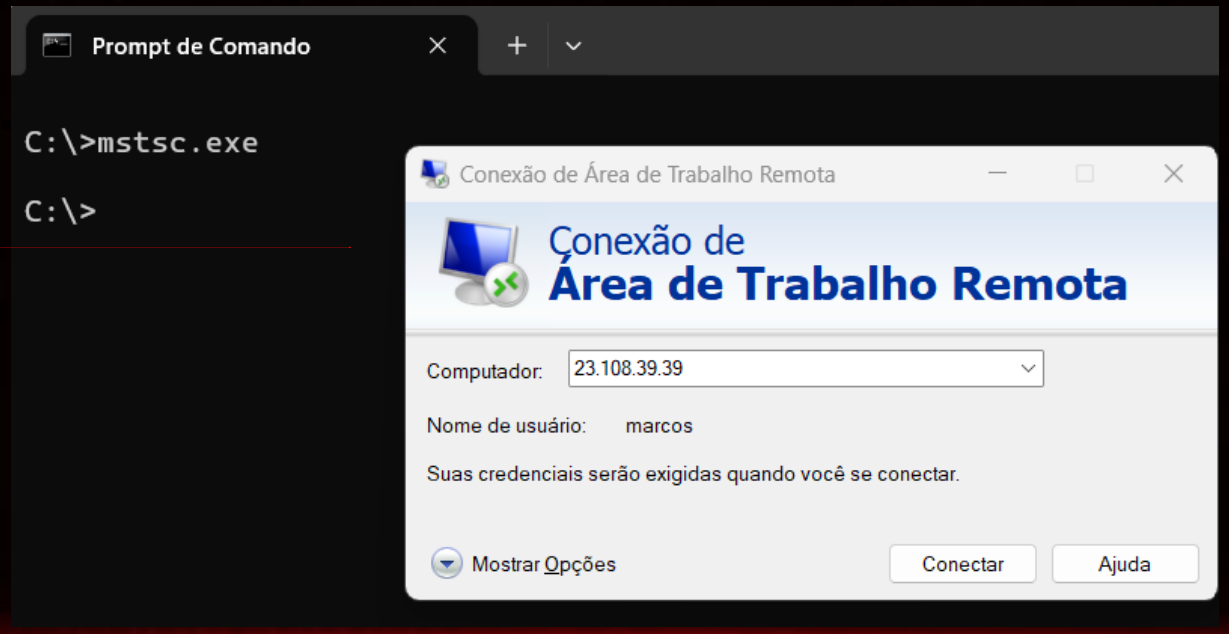
Portas utilizadas
A porta utilizada nos acessos RDP é a 3389. Sempre observe a direção da porta para identificar qual host está recebendo a conexão RDP (source port = 3389) e qual host está iniciando a sessão RDP (dst port = 3389).

Ferramentas

RDP (2)

MSTSC

Mstsc.exe /v:nome_do_host <ENTER>
Mstsc.exe <ENTER>



SharpRDP (execução de código em massa via RDP)

SharpRDP.exe computername=WORKSTATION400 command="tasklist" username=dominio\usuario password=123456 <ENTER>

```
C:\Disk>SharpRDP.exe computername=ip-172-31-7-162.us-east-2.compute.internal command="tasklist" username=10bank\conector password=[redacted]
[+] Connected to          :  ip-172-31-7-162.us-east-2.compute.internal
[+] Execution priv type   :  non-elevated
[+] Executing tasklist
[+] Disconnecting from    :  ip-172-31-7-162.us-east-2.compute.internal
[+] Connection closed     :  ip-172-31-7-162.us-east-2.compute.internal
```

RDP (3) Captura de rede

Ao analisar uma captura de rede (abaixo), é possível observar qual servidor foi acessado via RDP (172.31.7.162) e qual host acessou (172.31.4.76), através da identificação de onde está a porta 3389.

rdp

No.	Time	Source	Destination	Protocol	Length	Info
1836	2025-10-08 18:16:18.665410	172.31.4.76	172.31.7.162	RDP	101	Cookie: mstshash=10BANK\al,
1873	2025-10-08 18:16:19.030587	172.31.7.162	172.31.4.76	RDP	73	Negotiate Response

```
> Frame 1836: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF_{D7F2A7
> Ethernet II, Src: 02:ab:bb:fc:77:95 (02:ab:bb:fc:77:95), Dst: 02:d1:6c:14:8a:05 (02:d1:6c:14:8a:05)
> Internet Protocol Version 4, Src: 172.31.4.76, Dst: 172.31.7.162
v Transmission Control Protocol, Src Port: 58954, Dst Port: 3389, Seq: 1, Ack: 1, Len: 47
    Source Port: 58954
    Destination Port: 3389
```

```
0000  02 d1
0010  00 57
0020  07 a2
0030  04 1a
0040  00 43
0050  68 3d
0060  00 0b
```

RDP (4) Visibilidade em EDRs

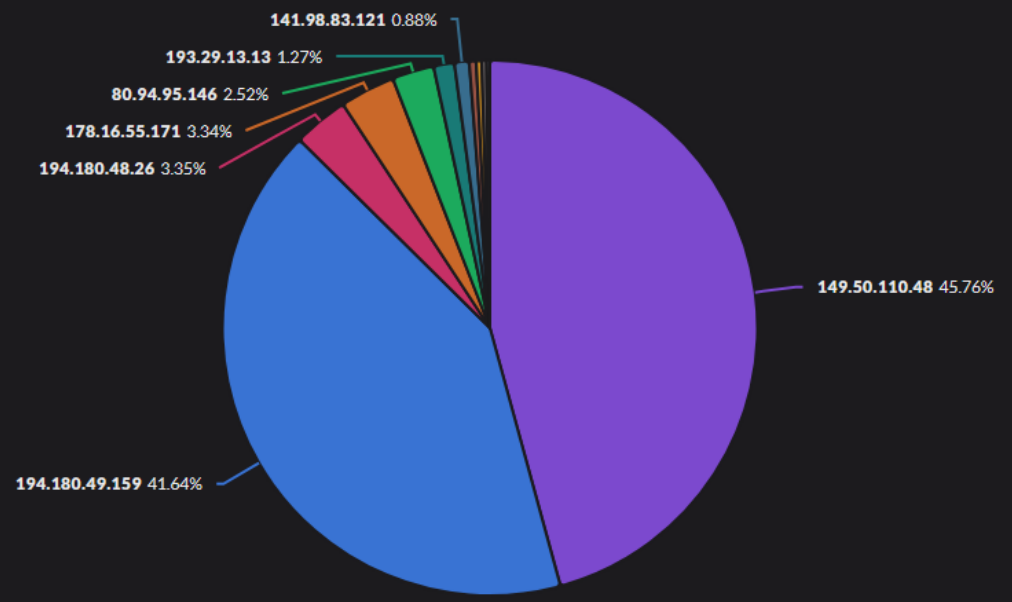
Query que mostra os hosts de origem que mais iniciaram sessões RDP:

All Data

```
event.type = 'IP Connect' and (dst.port.number = 3389) and src.ip.address != '127.0.0.1'
| columns event.time, endpoint.name, src.process.user, src.process.name, src.ip.address, src.port.number, dst.ip.address, dst.port.number
| group count() by src.ip.address
| sort -src.ip.address
```

columns filter group join inner join sql inner join left join sql left join outer join sql outer join let limit lookup parse sort transpose union

count() Sep



RDP (5) Visibilidade em EDRs

Query abaixo mostra quais processos foram utilizados para iniciar uma sessão RDP:

All Data

```
event.type = 'IP Connect' and (dst.port.number = 3389 OR src.port.number = 3389) and src.process.name != 'svchost.exe'
| columns event.time, endpoint.name, src.process.user, src.process.name, src.ip.address, src.port.number, dst.ip.address, dst.port.number
| group count() by src.process.name
```

columns filter group join inner join sql inner join left join sql left join outer join sql outer join let limit lookup parse sort transpose union

4 rows returned Sep 27, 2025 10:01 AM – Oct 11, 2025 10:01 AM UTC-3

src.process.name	count()
chrome.exe	523
mstsc.exe	9
Phoenix.Service.exe	3
SharpRDP.exe	1

Dica: Crie uma regra para alertar quando uma sessão RDP for iniciada por um processo desconhecido (i.e Processos diferentes dos mstsc.exe, chrome.exe, svchost.exe, etc).

RDP (6)

Identificando acessos RDP através do EventViewer

Acessos RDP no host que foi acessado podem ser identificados através do Event ID 4624 **Type 10** . Observe a direita, que neste evento temos 3 informações importantes:

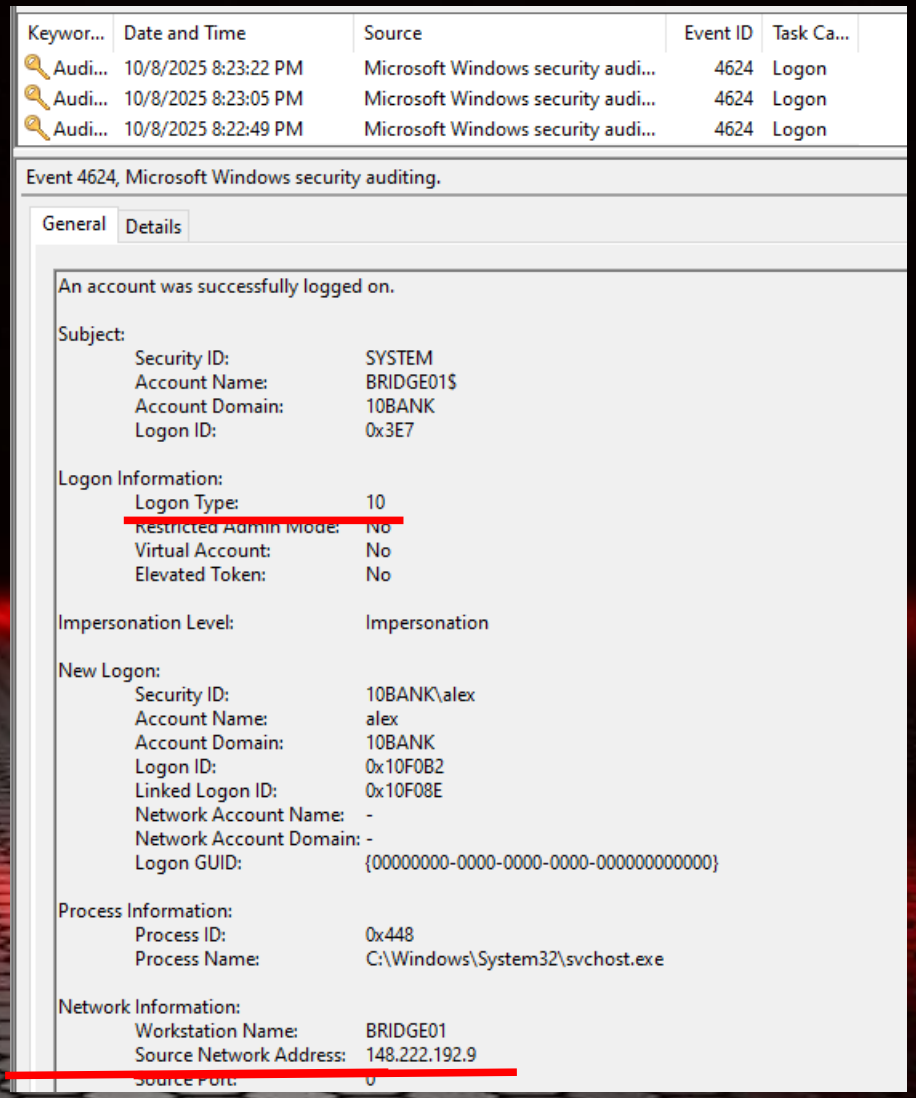
New Logon - Security ID – Conta de usuário que fez logon

Network Information - Workstation Name – Nome do host que foi acessado via RDP

Network Information - Source Network Address – Endereço do IP do host de origem, que iniciou o acesso RDP.

Outros Event Ids relacionados ao acesso RDP que também são úteis:

1149 – Remote Desktop Services User Authentication succeeded
21 – Remote Desktop Services Session Logon succeeded
4779 – A session was disconnected from a Windows Station
4778 – A session was reconnected to a Windows Station



Keywor...	Date and Time	Source	Event ID	Task Ca...
Audi...	10/8/2025 8:23:22 PM	Microsoft Windows security audi...	4624	Logon
Audi...	10/8/2025 8:23:05 PM	Microsoft Windows security audi...	4624	Logon
Audi...	10/8/2025 8:22:49 PM	Microsoft Windows security audi...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
Security ID: SYSTEM
Account Name: BRIDGE01$
Account Domain: 10BANK
Logon ID: 0x3E7

Logon Information:
Logon Type: 10
Restricted Admin Mode: No
Virtual Account: No
Elevated Token: No

Impersonation Level: Impersonation

New Logon:
Security ID: 10BANK\alex
Account Name: alex
Account Domain: 10BANK
Logon ID: 0x10F0B2
Linked Logon ID: 0x10F08E
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x448
Process Name: C:\Windows\System32\svchost.exe

Network Information:
Workstation Name: BRIDGE01
Source Network Address: 148.222.192.9
Source Port: 0

RDP (7) Dicas de investigação

Um acesso RDP legítimo não é muito diferente de um acesso RDP realizado por um criminoso. Para fazer o acesso RDP, o criminoso precisa ter:

a) Comunicação/conectividade com o servidor de destino na porta 3389.
b) Uma conta de usuário válida, que tenha direitos pelo menos de acesso remoto no servidor de destino.

Contra-medidas:

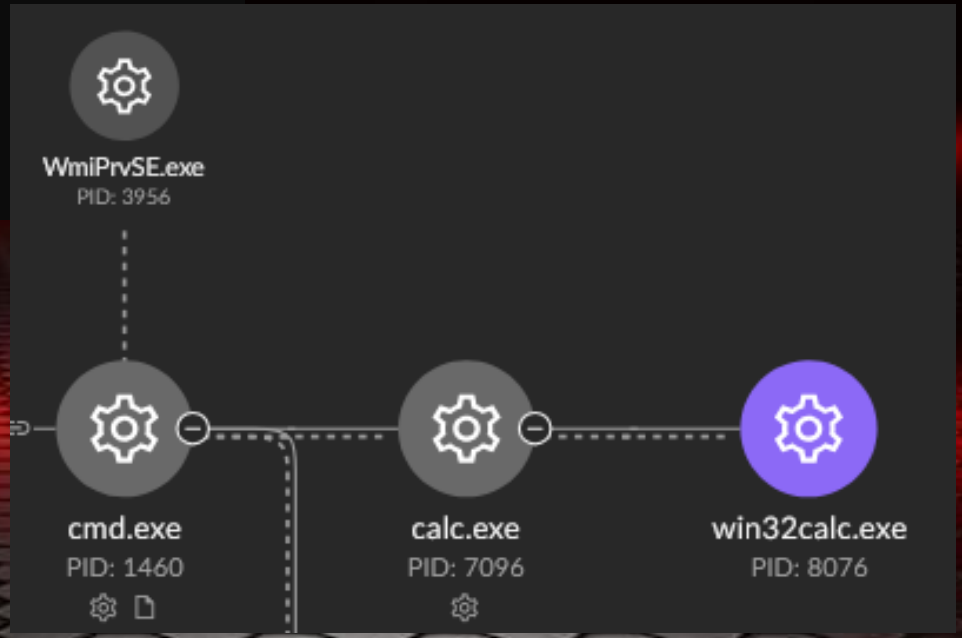
1) Implementar uma ferramenta de Cofre de Senhas ou PAM que centralize e controle todo o acesso RDP.
2) Garantir que todo acesso RDP só seja permito se a origem são os servidores do Cofre de Senhas ou "jump servers" autorizados.
3) Caso não exista Cofre de Senhas, garantir que todo acesso RDP para servidores seja realizado mediante aprovação de um mecanismo de duplo fator de autenticação.
4) Monitorar acessos RDP realizados a partir de origem desconhecido.
5) Monitorar ferramentas de acesso remoto (i.e mstsc) utilizadas por usuários que não precisam utilizá-as em seu dia a dia.
6) Monitorar processos incomuns iniciando sessões RDP.

Técnica 2

WMI over RPC/DCOM

```
C:\Disk>wmic /node:bridge01.10bank.com.br /user:conector process call create "notepad.exe"
Enter the password :***********

Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 7032;
        ReturnValue = 0;
};
```



WMI OVERVIEW

over RPC/DCOM (1)

Mitre Technique T1047

Descrição
WMI é uma funcionalidade no Windows que permite uma interface de gerenciamento de diversos componentes do Windows através da linha de comando. Esta interação pode ser local ou remoto.

Ferramentas
Wmic.exe é o processo nativo do windows que permite o gerenciamento do Windows via WMI. Execução de código via WMI usando DCOM utiliza a porta 135. WMI também pode ser usado através de WinRM, entretanto, WinRM será coberto na técnica 3 deste e-book.

Portas utilizadas
Remote WMI over RPC/DCOM utiliza inicialmente a porta 135. Após estabelecer a conexão via RPC, é estabelecido portas dinâmicas (entre 49152-65535) para a transmissão de dados entre os hosts.

WMI
over RPC/DCOM (2)

Ferramentas

WMIC.EXE

Wmic.exe é o processo nativo do windows que permite o gerenciamento de componentes do Windows via WMI, através da linha de comando, exemplo abaixo:

```
C:\Disk>wmic /node:bridge01.10bank.com.br /user:conector process call create "notepad.exe"
Enter the password :***********
```

Crackmapexec

Crackmapexec é uma ferramenta popular encontrada no Kali Linux e também pode ser instalada sob demanda em hosts Windows e Linux e tem várias funcionalidades de execução de código remoto, incluindo via WMI over RPC/DCOM:

```
root@ip-172-31-32-213:/home/ubuntu# crackmapexec wmi 172.31.7.162 -d 10bank.com.br -u conector -p [redacted] -x mspaint.exe
RPC         172.31.7.162    135    BRIDGE01         [*] Windows NT 10.0 Build 20348 (name:BRIDGE01) (domain:10bank.com.br)
WMI         172.31.7.162    135    BRIDGE01         [+] 10bank.com.br\conector:[redacted] (Pwn3d!)
```

WMI
over RPC/DCOM (3)

Captura de Rede

No.	Time	Source	Destination	Protocol	Length	Info
1155	8.804206	172.31.32.213	172.31.7.162	TCP	74	44250 → 135 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=3990238669 TSecr=0 WS=128
1156	8.804315	172.31.7.162	172.31.32.213	TCP	74	135 → 44250 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=8961 WS=256 SACK_PERM TSval=5138762 TSecr=3990238669
1157	8.804320	172.31.7.162	172.31.32.213	TCP	74	[TCP Retransmission] 135 → 44250 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=8961 WS=256 SACK_PERM TSval=5138762
1160	8.805544	172.31.32.213	172.31.7.162	TCP	66	44250 → 135 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=3990238670 TSecr=5138762
1161	8.805773	172.31.32.213	172.31.7.162	DCERPC	138	Bind: call_id: 1, Fragment: Single, 1 context items: EPMv4 V3.0 (32bit NDR)
1162	8.824321	172.31.7.162	172.31.32.213	TCP	66	135 → 44250 [ACK] Seq=1 Ack=73 Win=2102784 Len=0 TSval=5138782 TSecr=3990238671
1163	8.824328	172.31.7.162	172.31.32.213	TCP	66	[TCP Dup ACK 1162#1] 135 → 44250 [ACK] Seq=1 Ack=73 Win=2102784 Len=0 TSval=5138782 TSecr=3990238671
1169	8.891948	172.31.7.162	172.31.32.213	DCERPC	126	Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance
1170	8.891952	172.31.7.162	172.31.32.213	TCP	126	[TCP Retransmission] 135 → 44250 [PSH, ACK] Seq=1 Ack=73 Win=2102784 Len=60 TSval=5138849 TSecr=3990238671
1171	8.893180	172.31.32.213	172.31.7.162	TCP	66	44250 → 135 [ACK] Seq=73 Ack=61 Win=62848 Len=0 TSval=3990238758 TSecr=5138849
1172	8.894641	172.31.32.213	172.31.7.162	TCP	66	44250 → 135 [FIN, ACK] Seq=73 Ack=61 Win=62848 Len=0 TSval=3990238759 TSecr=5138849
1173	8.894667	172.31.7.162	172.31.32.213	TCP	66	135 → 44250 [ACK] Seq=61 Ack=74 Win=2102784 Len=0 TSval=5138853 TSecr=3990238759
1174	8.894670	172.31.7.162	172.31.32.213	TCP	66	[TCP Dup ACK 1173#1] 135 → 44250 [ACK] Seq=61 Ack=74 Win=2102784 Len=0 TSval=5138853 TSecr=3990238759
1175	8.894732	172.31.7.162	172.31.32.213	TCP	66	135 → 44250 [FIN, ACK] Seq=61 Ack=74 Win=2102784 Len=0 TSval=5138853 TSecr=3990238759
1176	8.894734	172.31.7.162	172.31.32.213	TCP	66	[TCP Retransmission] 135 → 44250 [FIN, ACK] Seq=61 Ack=74 Win=2102784 Len=0 TSval=5138853 TSecr=3990238759
1180	8.896075	172.31.32.213	172.31.7.162	TCP	66	44250 → 135 [ACK] Seq=74 Ack=62 Win=62848 Len=0 TSval=3990238761 TSecr=5138853

```
> Frame 1169: Packet, 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\N
> Ethernet II, Src: 02:d1:6c:14:8a:05 (02:d1:6c:14:8a:05), Dst: 02:9c:2e:de:4e:f7 (02:9c:2e:de:4e:f7)
> Internet Protocol Version 4, Src: 172.31.7.162, Dst: 172.31.32.213
> Transmission Control Protocol, Src Port: 135, Dst Port: 44250, Seq: 1, Ack: 73, Len: 60
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Bind_ack, Fragment: Single, FragLen:
```

```
0000  02 9c 2e de 4e f7 02 d1  6c 14 8a 05 08 00 45 00   ····N··· l·····E·
0010  00 70 13 3c 40 00 80 06  00 00 ac 1f 07 a2 ac 1f   ·p·<@··· ********
0020  20 d5 00 87 ac da 4f 37  3c 13 51 b1 e2 a4 80 18   ·····O7 <·Q·····
0030  20 16 81 18 00 00 01 01  08 0a 00 4e 69 a1 ed d6   ******** ···Ni···
0040  35 cf 05 00 0c 03 10 00  00 00 3c 00 00 00 01 00   5******· ··<·····
0050  00 00 b8 10 b8 10 2a 2b  00 00 04 00 31 33 35 00   *******+ ····135·
0060  00 00 01 00 00 00 00 00  00 00 04 5d 88 8a eb 1c   ******** ···]····
```

Acima está uma captura de rede no momento em que o crackmapexec foi utilizado a partir do host **172.31.32.213** para executar código remoto no host **172.31.7.162** via WMI (over RPC/DCOM). Observe a porta do primeiro pacote SYN (135) e uma vez que o 3-way handshake é estabelecido, incia-se a comunicação via DCERPC. Em seguida um conjunto de portas dinâmicas (entre 49152-65535) são utilizadas.

WMI
over RPC/DCOM (4)

Visibilidade via EDR

BUNKER CYBER SECURITY

All Data

```
event.type = 'Process Creation' AND osSrc.process.parent.name = 'WmiPrvSE.exe'
| columns event.time, event.type, endpoint.name, src.process.user, osSrc.process.parent.name, src.process.name, src.process.cmdline
| sort -event.time
```

Last 4 hours | Search

columns | filter | group | join | inner join | sql inner join | left join | sql left join | outer join | sql outer join | let | limit | lookup | parse | sort | transpose | union

Table

14 rows returned 8:41 AM – 12:41 PM UTC-3

Copy | Download

event.time	event.type	endpoint.name	src.process.user	osSrc.process.parent.name	src.process.name	src.process.cmdline
Oct 11 · 12:28:34.085 pm	Process Creation	BRIDGE01	10BANK\conector	WmiPrvSE.exe	cmd.exe	cmd.exe /Q /c notepad.exe 1> C:\windows\temp\bd587aae-f8d9-4554-9e4f-b920a7af92d \windows\temp\bd587aae-f8d9-4554-9e4f-b920a7af92df.txt C:\windows\temp\e741f8d3-e "usebackq" %G in ("C:\windows\temp\e741f8d3-eddc-4ad3-ace8-e4f1ac5f0dbd.txt") do 8eb41624-2d68-4c4f-bd36-0e054844d0d9 /t REG_SZ /d "%G" /f && del /q /f /s C:\windo C:\windows\temp\e741f8d3-eddc-4ad3-ace8-e4f1ac5f0dbd.txt
Oct 11 · 11:30:31.284 am	Process Creation	BRIDGE01	10BANK\conector	WmiPrvSE.exe	cmd.exe	cmd.exe /Q /c mspaint.exe 1> C:\windows\temp\e859c2d6-6b58-4b1e-bcaa-edc52e89b12

Acima, a visibilidade via EDR sobre os processos que foram executados via WMI nos hosts destino, incluindo qual conta foi utilizada para realizar estas execuções de código remoto via WMI (over RPC/DCOM).

WMI
over RPC/DCOM (5)

Visibilidade via EDR

BUNKER CYBER SECURITY

All Data

```
event.type='Behavioral Indicators' indicator.name='InterpreterFromWmiExecutedRemotely'
| columns event.time, endpoint.name, src.process.user, indicator.metadata
```

Last 1 hour

columns filter group join inner join sql inner join left join sql left join outer join sql outer join let limit lookup parse sort transpose union

1 row returned 10:15 PM – 11:15 PM UTC-3

Copy

event.time	endpoint.name	src.process.user	indicator.metadata
Oct 12 · 10:53:02.115 pm	BRIDGE01	10BANK\conector	Process[Name: "cmd.exe (CLI interpreter)", Pid: "1148", UID: "144931809A5150DC", StorylineID: "154931809A5150DC", IntegrityLevel: "High", RelationToSource: "Child"], Command Line: "cmd.exe /Q /c notepad.exe 1> C:\windows\temp\544478ca-faaf-4108-b09c-dac9cdb57bf4.txt 2>&1 && certutil -encodehex -f C:\windows\temp\544478ca-faaf-4108-b09c-dac9cdb57bf4.txt C:\windows\temp\b0d71106-4fe8-4b57-aff2-840a13d05f68.txt 0x40000001 && for /F "usebackq" %G in ("C:\windows\temp\b0d71106-4fe8-4b57-aff2-840a13d05f68.txt") do reg add HKLM\Software\Classes\HmIPer /v 844874f1-9fc9-49d5-9f8c-9cc03a3c5dd2 /t REG_SZ /d "%G" /f && del /q /f /s C:\windows\temp\544478ca-faaf-4108-b09c-dac9cdb57bf4.txt C:\windows\temp\b0d71106-4fe8-4b57-aff2-840a13d05f68.txt"

A query acima, utilizando o EDR da SeninelOne, buscamos especificamente pelo comportamento já identificado como “InterpreterFromWmiExecuteRemotely” e é possível revelar a execução de código via CrackMapExec.

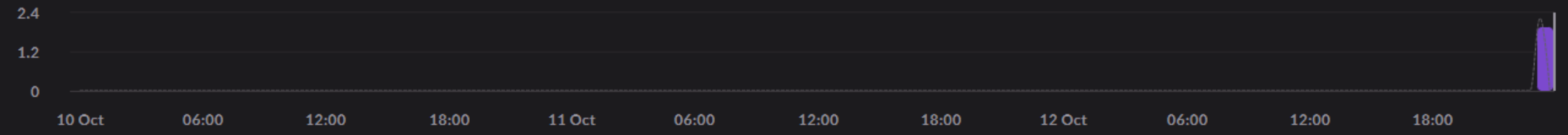
WMI
over RPC/DCOM (6)

Visibilidade via EDR

All Data | event.type = 'IP Connect' and src.process.name='WMIC.exe' | Last 72 hours | Search

2 matching records Oct 9, 2025 11:56 PM – Oct 12, 2025 11:56 PM [UTC-3] - 1 hour / bar

Show Graph



Actions | No Items selected | Jump to « Oldest Most Recent » | Most Recent First | Table | Settings | Export

event.time	src.ip.address	src.port.number	dst.ip.address	dst.port.number	src.process.cmdline
Oct 12, 2025 11:28:55 PM	172.31.7.162	54738	172.31.4.76	49667	wmic /node:workstation400 proces
Oct 12, 2025 11:22:05 PM	172.31.4.76	51027	172.31.7.162	49668	wmic /node:172.31.7.162 /user:cor

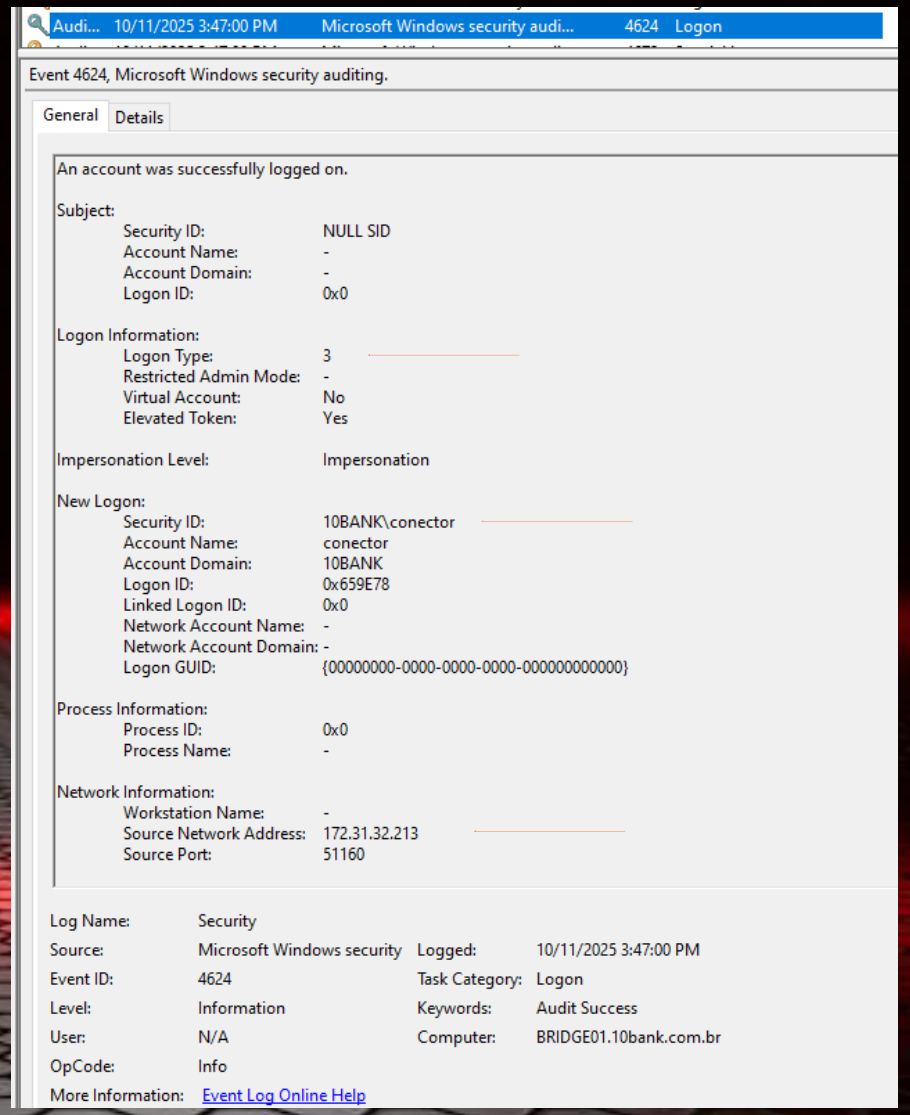
A query acima, mostra as conexões de rede realizadas pelo processo WMIC.exe, observe as portas de destino que batem com as portas dinâmicas que são automaticamente atribuídas após a primeira comunicação via 135.

WMI over DCOM (7)

Visibilidade no Event Viewer

O Event ID 4624, tipo 3, significa que aconteceu um logon através da rede. Ao executar código remoto através de Crackmac ou wmic, este evento é gerado e contém o host de origem (Source Network Address) e a conta utilizada (conector). Entretanto, existem outras situações de acesso a recursos na rede que o mesmo tipo de evento também é gerado. Não é do nosso conhecimento um event ID que consigamos “cravar” que a simples existência dele significa que houve execução de código remoto usando WMI over DCOM.

Os Event Ids 5861, 5857 e 5858, também podem ajudar atividade WMI, em busca de subscrições suspeitas utilizando WMI.



WMI
over RPC/DCOM (8)

Dicas de Investigação

1. Monitore a utilização do processo wmic.exe com o parâmetro /node. Se existem aplicações que normalmente utilizam este mecanismo para gerenciamento do ambiente, exclua estes padrões legítimos do seu monitoramento e configure alarmes caso veja isto acontecendo a partir de hosts ou contas incomuns.

2. A porta 135 utilizada por execução de código remoto via WMI over RPC/DCOM é normalmente utilizada por outras funcionalidades e serviços em um ambiente de rede MS Windows. Entretanto, alguns tipos de serviços (i.e servidor de banco de dados, servidor WEB, etc), não fazem sentido ter a porta 135 exposta ao resto da rede. Portanto, pode ser uma boa opção monitorar as conexões nesta porta para este tipo de servidor ou mesmo bloquear após validar que de fato esta porta não é utilizada neste ambiente.

3. Monitore os processos incomuns que iniciam as conexões de rede realizadas para a porta 135.

4. Monitore linhas de comando comumente utilizadas por ferramentas como o CrackMapExec, exemplo:

```
src.process.cmdline

cmd.exe /Q /c  notepad.exe 1> C:\windows\temp\bd587aae-f8d9-4554-9e4f-b920a7af92d
\windows\temp\bd587aae-f8d9-4554-9e4f-b920a7af92df.txt C:\windows\temp\e741f8d3-e
"usebackq" %G in ("C:\windows\temp\e741f8d3-eddc-4ad3-ace8-e4f1ac5f0dbd.txt") do
8eb41624-2d68-4c4f-bd36-0e054844d0d9 /t REG_SZ /d "%G" /f && del /q /f /s C:\wind
C:\windows\temp\e741f8d3-eddc-4ad3-ace8-e4f1ac5f0dbd.txt
```

Técnica 3 - WinRM

Select Command Prompt - powershell

```
PS C:\> enter-pssession

cmdlet Enter-PSSession at command pipeline position 1
Supply values for the following parameters:
ComputerName: bridge01.10bank.com.br
[bridge01.10bank.com.br]: PS C:\Users\conector\Documents>
[bridge01.10bank.com.br]: PS C:\Users\conector\Documents>
[bridge01.10bank.com.br]: PS C:\Users\conector\Documents> ipconfig

Windows IP Configuration
```

No.	Time	Source	Destination	Protocol	Length	Info
5373	2025-10-13 03:24:37.897588	172.31.4.76	172.31.13.48	TCP	66	61618 → 5985 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0 MSS=8961 WS=256 SACK_PERM
5374	2025-10-13 03:24:37.897593	172.31.4.76	172.31.13.48	TCP	66	[TCP Retransmission] 61618 → 5985 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0 MSS=8961 WS=256 SACK_PERM
5375	2025-10-13 03:24:37.898212	172.31.13.48	172.31.4.76	TCP	66	5985 → 61618 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=8961 WS=256 SACK_PERM
5376	2025-10-13 03:24:37.898257	172.31.4.76	172.31.13.48	TCP	54	61618 → 5985 [ACK] Seq=1 Ack=1 Win=268800 Len=0
5377	2025-10-13 03:24:37.898260	172.31.4.76	172.31.13.48	TCP	54	[TCP Dup ACK 5376#1] 61618 → 5985 [ACK] Seq=1 Ack=1 Win=268800 Len=0
5380	2025-10-13 03:24:37.898596	172.31.4.76	172.31.13.48	HTTP	4587	POST /wsman?PSVersion=5.1.20348.2849 HTTP/1.1
5381	2025-10-13 03:24:37.898607	172.31.4.76	172.31.13.48	TCP	4587	[TCP Retransmission] 61618 → 5985 [PSH, ACK] Seq=1 Ack=1 Win=268800 Len=4533
5382	2025-10-13 03:24:37.900491	172.31.13.48	172.31.4.76	HTTP	395	HTTP/1.1 200
5383	2025-10-13 03:24:37.901439	172.31.4.76	172.31.13.48	TCP	326	61618 → 5985 [PSH, ACK] Seq=4534 Ack=342 Win=268288 Len=272 [TCP PDU reassembled in 5385]
5384	2025-10-13 03:24:37.901443	172.31.4.76	172.31.13.48	TCP	326	[TCP Retransmission] 61618 → 5985 [PSH, ACK] Seq=4534 Ack=342 Win=268288 Len=272
5385	2025-10-13 03:24:37.901547	172.31.4.76	172.31.13.48	HTTP	8253	POST /wsman?PSVersion=5.1.20348.2849 HTTP/1.1 (application/http-kerberos-session-encrypted)
5386	2025-10-13 03:24:37.901561	172.31.4.76	172.31.13.48	TCP	8253	[TCP Retransmission] 61618 → 5985 [PSH, ACK] Seq=4806 Ack=342 Win=268288 Len=8199 [TCP PDU reassembled in 5385]
5387	2025-10-13 03:24:37.902453	172.31.13.48	172.31.4.76	TCP	54	5985 → 61618 [ACK] Seq=342 Ack=13005 Win=2141952 Len=0
5398	2025-10-13 03:24:38.162308	172.31.13.48	172.31.4.76	HTTP	2743	HTTP/1.1 200 (application/http-kerberos-session-encrypted)
5399	2025-10-13 03:24:38.176894	172.31.4.76	172.31.13.48	TCP	66	61619 → 5985 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0 MSS=8961 WS=256 SACK_PERM
5400	2025-10-13 03:24:38.176902	172.31.4.76	172.31.13.48	TCP	66	[TCP Retransmission] 61619 → 5985 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0 MSS=8961 WS=256 SACK_PERM
5401	2025-10-13 03:24:38.177277	172.31.13.48	172.31.4.76	TCP	66	5985 → 61619 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=8961 WS=256 SACK_PERM

```
> Frame 5382: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{D7F2A7DC-EA23-44EF-8EBE-84BAD862A
> Ethernet II, Src: 02:d4:9c:2b:4f:e9 (02:d4:9c:2b:4f:e9), Dst: 02:ab:bb:fc:77:95 (02:ab:bb:fc:77:95)
> Internet Protocol Version 4, Src: 172.31.13.48, Dst: 172.31.4.76
> Transmission Control Protocol, Src Port: 5985, Dst Port: 61618, Seq: 1, Ack: 4534, Len: 341
v Hypertext Transfer Protocol
  > HTTP/1.1 200 \r\n
  > WWW-Authenticate: Kerberos YIGYBgkqhkiG9xIBAgICAG+BiDCBhaADAgEFoQMCAQ+ieTB3oAMCARKicARu86fflW9noACv5EEcyViXKyfQhgadKd4KyE8UWVesQU1
    Server: Microsoft-HTTPAPI/2.0\r\n
    Date: Mon, 13 Oct 2025 03:24:37 GMT\r\n
  > Content-Length: 0\r\n
    \r\n
    [Request in frame: 5380]
    [Time since request: 0.001895000 seconds]
    [Request URI: /wsman?PSVersion=5.1.20348.2849]
    [Full request URI: http://srvdc002:5985/wsman?PSVersion=5.1.20348.2849]
```

```
0000  02 ab bb fc 77 95 02 d4  9c 2b 4f e9 08 00 45 02   ····w··· ·+O···E·
0010  01 7d 25 c3 40 00 80 06  69 fb ac 1f 0d 30 ac 1f   ·}%·@··· i····0··
0020  04 4c 17 61 f0 b2 83 78  97 97 b5 1f f5 ba 50 18   ·L·a···x ======P·
0030  20 d0 2c 50 00 00 48 54  54 50 2f 31 2e 31 20 32    ·,P··HT TP/1.1 2
0040  30 30 20 0d 0a 57 57 57  2d 41 75 74 68 65 6e 74   00 ··WWW -Authent
0050  69 63 61 74 65 3a 20 4b  65 72 62 65 72 6f 73 20   icate: K erberos
0060  59 49 47 59 42 67 6b 71  68 6b 69 47 39 78 49 42   YIGYBgkq hkiG9xIB
0070  41 67 49 43 41 47 2b 42  69 44 43 42 68 61 41 44   AgICAG+B iDCBhaAD
0080  41 67 45 46 6f 51 4d 43  41 51 2b 69 65 54 42 33   AgEFoQMC AQ+ieTB3
0090  6f 41 4d 43 41 52 4b 69  63 41 52 75 38 36 66 66   oAMCARKi cARu86ff
00a0  6c 57 39 6e 6f 41 43 76  35 45 45 63 79 56 69 58   lW9noACv 5EEcyViX
00b0  4b 79 66 51 68 67 61 64  4b 64 34 4b 79 45 38 55   KyfQhgad Kd4KyE8U
00c0  57 56 65 73 51 55 31 48  43 50 4d 53 7a 70 6d 78   WVesQU1H CPMSzpmx
00d0  41 61 64 75 45 6e 75 4e  6d 72 2f 77 45 77 53 71   AaduEnuN mr/wEwSq
00e0  2b 4b 4c 37 32 6a 30 35  63 6e 31 65 61 76 73 37   +KL72j05 cn1eavs7
00f0  44 72 64 4c 73 32 53 2f  67 62 4d 4b 53 4f 30 2f   DrdLs2S/ gbMKSO0/
0100  35 76 47 64 52 2f 4c 67  4a 64 34 59 7a 72 6c 76   5vGdR/Lg Jd4Yzrlv
```

WinRM (1) Overview

Mitre Technique T1021.006

Descrição
WinRM (Windows Remote Management) é uma funcionalidade que permite gerenciar hosts Windows através do protocolo WS-Management que usa SOAP e é baseado em XML. A comunicação do WinRM pode ser configurado para ser criptografado (HTTPS) ou sem criptografia (HTTP).

Ferramentas
Powershell Remoting é a principal ferramenta utilizada para execução de código remoto via WinRM.

Portas utilizadas
WMI over WinRM utiliza as portas 5985 (HTTP) e 5986 (HTTPS)

WinRM (2) Ferramentas

Método 1:
Powershell Remoting – Usando Enter-PSSession:

```
Select Command Prompt - powershell
PS C:\> enter-pssession

cmdlet Enter-PSSession at command pipeline position 1
Supply values for the following parameters:
ComputerName: bridge01.10bank.com.br
[bridge01.10bank.com.br]: PS C:\Users\conector\Documents>
[bridge01.10bank.com.br]: PS C:\Users\conector\Documents>
[bridge01.10bank.com.br]: PS C:\Users\conector\Documents> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : 10bank.com.br
   IPv4 Address. . . . . . . . . . . : 172.31.7.162
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.31.0.1
[bridge01.10bank.com.br]: PS C:\Users\conector\Documents> hostname
BRIDGE01
[bridge01.10bank.com.br]: PS C:\Users\conector\Documents> exit
PS C:\> _
```

Método 2:
Powershell Remoting – Usando Invoke-Command:

```
PS C:\Python313\Scripts> Invoke-Command -ComputerName srvdc002 -ScriptBlock { tasklist }

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        144 K
Registry                        68 Services                   0     67,716 K
smss.exe                       572 Services                   0        212 K
csrss.exe                      732 Services                   0      1.372 K
```

WinRM Captura de Rede

(3)

No.	Time	Source	Destination	Protocol	Length	Info
5373	2025-10-13 03:24:37.897588	172.31.4.76	172.31.13.48	TCP	66	61618 → 5985 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0 MSS=8961 WS=256 SACK_PERM
5374	2025-10-13 03:24:37.897593	172.31.4.76	172.31.13.48	TCP	66	[TCP Retransmission] 61618 → 5985 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0 MSS=8961 WS=256 SACK_PERM
5375	2025-10-13 03:24:37.898212	172.31.13.48	172.31.4.76	TCP	66	5985 → 61618 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=8961 WS=256 SACK_PERM
5376	2025-10-13 03:24:37.898257	172.31.4.76	172.31.13.48	TCP	54	61618 → 5985 [ACK] Seq=1 Ack=1 Win=268800 Len=0
5377	2025-10-13 03:24:37.898260	172.31.4.76	172.31.13.48	TCP	54	[TCP Dup ACK 5376#1] 61618 → 5985 [ACK] Seq=1 Ack=1 Win=268800 Len=0
5380	2025-10-13 03:24:37.898596	172.31.4.76	172.31.13.48	HTTP	4587	POST /wsman?PSVersion=5.1.20348.2849 HTTP/1.1
5381	2025-10-13 03:24:37.898607	172.31.4.76	172.31.13.48	TCP	4587	[TCP Retransmission] 61618 → 5985 [PSH, ACK] Seq=1 Ack=1 Win=268800 Len=4533
5382	2025-10-13 03:24:37.900491	172.31.13.48	172.31.4.76	HTTP	395	HTTP/1.1 200
5383	2025-10-13 03:24:37.901439	172.31.4.76	172.31.13.48	TCP	326	61618 → 5985 [PSH, ACK] Seq=4534 Ack=342 Win=268288 Len=272 [TCP PDU reassembled in 5385]
5384	2025-10-13 03:24:37.901443	172.31.4.76	172.31.13.48	TCP	326	[TCP Retransmission] 61618 → 5985 [PSH, ACK] Seq=4534 Ack=342 Win=268288 Len=272
5385	2025-10-13 03:24:37.901547	172.31.4.76	172.31.13.48	HTTP	8253	POST /wsman?PSVersion=5.1.20348.2849 HTTP/1.1 (application/http-kerberos-session-encrypted)
5386	2025-10-13 03:24:37.901561	172.31.4.76	172.31.13.48	TCP	8253	[TCP Retransmission] 61618 → 5985 [PSH, ACK] Seq=4806 Ack=342 Win=268288 Len=8199 [TCP PDU reassembled in 5385]
5387	2025-10-13 03:24:37.902453	172.31.13.48	172.31.4.76	TCP	54	5985 → 61618 [ACK] Seq=342 Ack=13005 Win=2141952 Len=0
5398	2025-10-13 03:24:38.162308	172.31.13.48	172.31.4.76	HTTP	2743	HTTP/1.1 200 (application/http-kerberos-session-encrypted)
5399	2025-10-13 03:24:38.176894	172.31.4.76	172.31.13.48	TCP	66	61619 → 5985 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0 MSS=8961 WS=256 SACK_PERM
5400	2025-10-13 03:24:38.176902	172.31.4.76	172.31.13.48	TCP	66	[TCP Retransmission] 61619 → 5985 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0 MSS=8961 WS=256 SACK_PERM
5401	2025-10-13 03:24:38.177277	172.31.13.48	172.31.4.76	TCP	66	5985 → 61619 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=8961 WS=256 SACK_PERM

```
> Frame 5382: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{D7F2A7DC-EA23-44EF-8EBE-84BAD862A
> Ethernet II, Src: 02:d4:9c:2b:4f:e9 (02:d4:9c:2b:4f:e9), Dst: 02:ab:bb:fc:77:95 (02:ab:bb:fc:77:95)
> Internet Protocol Version 4, Src: 172.31.13.48, Dst: 172.31.4.76
> Transmission Control Protocol, Src Port: 5985, Dst Port: 61618, Seq: 1, Ack: 4534, Len: 341
v Hypertext Transfer Protocol
  > HTTP/1.1 200 \r\n
  > WWW-Authenticate: Kerberos YIGYBgkqhkiG9xIBAgICAG+BiDCBhaADAgEFoQMCAQ+ieTB3oAMCARKicARu86fflW9noACv5EEcyViXKyfQhgadKd4KyE8UWVesQU1
    Server: Microsoft-HTTPAPI/2.0\r\n
    Date: Mon, 13 Oct 2025 03:24:37 GMT\r\n
  > Content-Length: 0\r\n
    \r\n
    [Request in frame: 5380]
    [Time since request: 0.001895000 seconds]
    [Request URI: /wsman?PSVersion=5.1.20348.2849]
    [Full request URI: http://srvdc002:5985/wsman?PSVersion=5.1.20348.2849]
```

```
0000  02 ab bb fc 77 95 02 d4  9c 2b 4f e9 08 00 45 02   ····w··· ·+O···E·
0010  01 7d 25 c3 40 00 80 06  69 fb ac 1f 0d 30 ac 1f   ·}%·@··· i····0··
0020  04 4c 17 61 f0 b2 83 78  97 97 b5 1f f5 ba 50 18   ·L·a···x ======P·
0030  20 d0 2c 50 00 00 48 54  54 50 2f 31 2e 31 20 32    ·,P··HT TP/1.1 2
0040  30 30 20 0d 0a 57 57 57  2d 41 75 74 68 65 6e 74   00 ··WWW -Authent
0050  69 63 61 74 65 3a 20 4b  65 72 62 65 72 6f 73 20   icate: K erberos
0060  59 49 47 59 42 67 6b 71  68 6b 69 47 39 78 49 42   YIGYBgkq hkiG9xIB
0070  41 67 49 43 41 47 2b 42  69 44 43 42 68 61 41 44   AgICAG+B iDCBhaAD
0080  41 67 45 46 6f 51 4d 43  41 51 2b 69 65 54 42 33   AgEFoQMC AQ+ieTB3
0090  6f 41 4d 43 41 52 4b 69  63 41 52 75 38 36 66 66   oAMCARKi cARu86ff
00a0  6c 57 39 6e 6f 41 43 76  35 45 45 63 79 56 69 58   lW9noACv 5EEcyViX
00b0  4b 79 66 51 68 67 61 64  4b 64 34 4b 79 45 38 55   KyfQhgad Kd4KyE8U
00c0  57 56 65 73 51 55 31 48  43 50 4d 53 7a 70 6d 78   WVesQU1H CPMSzpmx
00d0  41 61 64 75 45 6e 75 4e  6d 72 2f 77 45 77 53 71   AaduEnuN mr/wEwSq
00e0  2b 4b 4c 37 32 6a 30 35  63 6e 31 65 61 76 73 37   +KL72j05 cn1eavs7
00f0  44 72 64 4c 73 32 53 2f  67 62 4d 4b 53 4f 30 2f   DrdLs2S/ gbMKSO0/
0100  35 76 47 64 52 2f 4c 67  4a 64 34 59 7a 72 6c 76   5vGdR/Lg Jd4Yzrlv
```

Acima está uma captura de rede no momento em que uma execuçãod e código remoto via PowerShell Remoting foi realizada, a partir do host **172.31.4.76**. O host de destino onde o código remoto (comando tasklist) foi executado, foi o host **172.31.13.48**. Observe os endereços IPs na coluna Source e Destination.

WinRM Visibilidade via EDR

(4)

Uma forma de visualizar as execuções de código remoto via WinRM (Powershell Remoting), é buscar pelo tipo de evento “Process Creation” e filtrar onde o processo pai é o “wsmprovhost.exe”:

All Data

```
| filter (event.type='Process Creation' OR event.type=='Behavioral Indicators') AND src.process.parent.name == 'wsmprovhost.exe'
| columns event.time, event.type, endpoint.name, src.process.user, osSrc.process.parent.name, src.process.parent.name, src.process.name, src.process.cmdline
| sort -event.time
| limit 1000
```

Last 1 hour | Search

columns filter group join inner join sql inner join left join sql left join outer join sql outer join let limit lookup parse sort transpose union

Table

2 rows returned 10:51 PM – 11:51 PM UTC-3

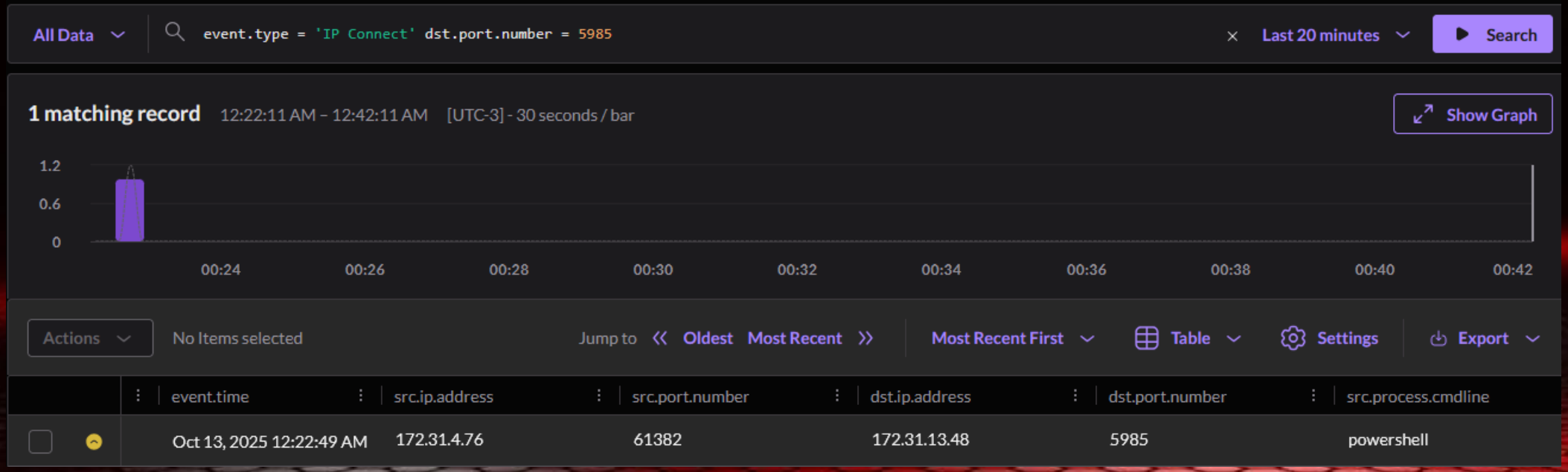
Copy | Download

event.time	event.type	endpoint.name	src.process.user	osSrc.process.parent.name	src.process.parent.name	src.process.name	src.process.cmdline
Oct 8 · 11:39:22.185 pm	Process Creation	BRIDGE01	10BANK\conector	null	wsmprovhost.exe	HOSTNAME.EXE	"C:\Windows\system32\HOSTNAME.EXE"
Oct 8 · 11:39:17.422 pm	Process Creation	BRIDGE01	10BANK\conector	null	wsmprovhost.exe	ipconfig.exe	"C:\Windows\system32\ipconfig.exe"

WinRM Visibilidade via EDR

(5)

Uma outra forma de visualizar as execuções de código remoto via WinRM (Powershell Remoting), é buscar pelo tipo de evento “IP Connect” e filtrar a porta 5985:



WinRM (6)

Visibilidade no Event Viewer

Ao monitorar o event viewer no host “alvo”, enquanto uma execução de código remoto é feita via WinRM, observamos a presença desta sequência de 3 eventos (ID 4624, 4799 e 4662):

Date and Time	Source	Event ID	Task Category
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4662	Other Object Access Events
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4634	Logoff
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4624	Logon
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4672	Special Logon
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4634	Logoff
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4634	Logoff
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4624	Logon
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4672	Special Logon
10/13/2025 12:20:16 PM	Microsoft Windows security auditing.	4634	Logoff
10/13/2025 12:20:14 PM	Microsoft Windows security auditing.	4624	Logon
10/13/2025 12:20:14 PM	Microsoft Windows security auditing.	4672	Special Logon
10/13/2025 12:20:11 PM	Microsoft Windows security auditing.	4624	Logon
10/13/2025 12:20:11 PM	Microsoft Windows security auditing.	4672	Special Logon
10/13/2025 12:20:11 PM	Microsoft Windows security auditing.	4624	Logon
10/13/2025 12:20:11 PM	Microsoft Windows security auditing.	4672	Special Logon
10/13/2025 12:20:10 PM	Microsoft Windows security auditing.	4799	Security Group Management
10/13/2025 12:20:10 PM	Microsoft Windows security auditing.	4634	Logoff
10/13/2025 12:20:10 PM	Microsoft Windows security auditing.	4624	Logon
10/13/2025 12:20:10 PM	Microsoft Windows security auditing.	4672	Special Logon
10/13/2025 12:19:59 PM	Eventlog	1102	Log clear

Event 4624, Microsoft Windows security auditing.

General | Details

An account was successfully logged on.

Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Information:
- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
- Security ID: 10BANK\alex
- Account Name: alex
- Account Domain: 10BANK.COM.BR
- Logon ID: 0x23CB87
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {66dbecf9-29ff-4110-34e2-7679894376a8}

Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name:
- Source Network Address: 172.31.4.76
- Source Port: 54656

Event 4799, Microsoft Windows security auditing.

General | Details

A security-enabled local group membership was enumerated.

Subject:
- Security ID: SYSTEM
- Account Name: BRIDGE01$
- Account Domain: 10BANK
- Logon ID: 0x3E7

Group:
- Security ID: BUILTIN\Administrators
- Group Name: Administrators
- Group Domain: Builtin

Process Information:
- Process ID: 0x4d4
- Process Name: C:\Windows\System32\svchost.exe

Event 4662, Microsoft Windows security auditing.

General | Details

An operation was performed on an object.

Subject :
- Security ID: LOCAL SERVICE
- Account Name: LOCAL SERVICE
- Account Domain: NT AUTHORITY
- Logon ID: 0x3E5

Object:
- Object Server: LSA
- Object Type: SecretObject
- Object Name: Policy\Secrets\$MACHINE.ACC
- Handle ID: 0x1b87f4e6470

Operation:
- Operation Type: Query
- Accesses: Query secret value

- Access Mask: 0x2
- Properties: -

WinRM (7) Dicas de Investigação

1. Monitore a utilização das diferentes formas de Powershell Remoting no ambiente. Se existem aplicações que normalmente utilizam este mecanismo para gerenciamento de ativos, exclua estes padrões legítimos do seu monitoramento e configure alarmes caso veja isto acontecendo a partir de hosts ou contas incomuns.

2. Monitore os hosts e que estão se conectando em hosts remotos na porta 5985 e 5986.

3. Monitore os processos que estão se comunicando com hosts remotos na porta 5985 e 5986.

4. Monitore processos anormais que são executados via WinRM. Faça um baseline de quais processos geralmente são usados na organização por aplicações via WinRM, através do monitoramento de processos executados pelo “wsmprovhost.exe”. Após isso, configure alertas em caso processos diferentes sejam executados pelo processo wsmprovhost.exe (via WinRM).

Técnica 4

PSEXEC

```
C:\Disk\pstools>PsExec.exe \\bridge01.10bank.com.br tasklist

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Image Name
==================
System Idle Proces
System
Registry
smss.exe
csrss.exe                    640 Services                   0      2,812 K
```

	Source	Destination	Protocol	Length	Info
13:03:51.282219	172.31.4.76	172.31.7.162	TCP	66	49226 → 445 [SYN, ECE, CWR] Seq=0 Win=62727 Len=0
13:03:51.282224	172.31.4.76	172.31.7.162	TCP	66	[TCP Retransmission] 49226 → 445 [SYN, ECE, CWR]
13:03:51.282938	172.31.7.162	172.31.4.76	TCP	66	445 → 49226 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535
13:03:51.282982	172.31.4.76	172.31.7.162	TCP	54	49226 → 445 [ACK] Seq=1 Ack=1 Win=268800 Len=0
13:03:51.282985	172.31.4.76	172.31.7.162	TCP	54	[TCP Dup ACK 555#1] 49226 → 445 [ACK] Seq=1 Ack=1
13:03:51.283647	172.31.4.76	172.31.7.162	SMB	127	Negotiate Protocol Request
13:03:51.283651	172.31.4.76	172.31.7.162	TCP	127	[TCP Retransmission] 49226 → 445 [PSH, ACK] Seq=1
13:03:51.284507	172.31.7.162	172.31.4.76	SMB2	306	Negotiate Protocol Response
13:03:51.284559	172.31.4.76	172.31.7.162	SMB2	358	Negotiate Protocol Request
13:03:51.284562	172.31.4.76	172.31.7.162	TCP	358	[TCP Retransmission] 49226 → 445 [PSH, ACK] Seq=7

PSEXEC (1) Overview

Mitre Technique T1021.002

PSEXEC é uma ferramenta da Microsoft que permite executar processos em computadores remoto. O PSEXEC utiliza o protocolo SMB2 para copiar um executável chamado **PSEXESVC.exe** no compartilhamento **admin$** do host remoto. Após isso, ele instala e inicia o serviço no host remoto chamado **PSEXESVC** .

A partir daí, é o processo c:\windows\psexesvc.exe responsável por executar os processos passados na linha de comando via psexec no host alvo.

Ferramentas

PSEXEC é uma das principais ferramentas utilizada para movimentação lateral através do protocolo SMBv2 e é comumente utilizada por grupos criminosos em suas operações.

Portas utilizadas

PSEXEC utiliza SMBv2 (porta 445), DCE/RPC (135) e SVCCTL (portas altas dinâmicas i.e 59794)

PSEXEC (2) Ferramentas

Linha de Comando:

```
C:\Disk\pstools>PsExec.exe \\bridge01.10bank.com.br tasklist

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com



Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0         76 K
Registry                        76 Services                   0     22,228 K
smss.exe                       492 Services                   0        252 K
csrss.exe                      640 Services                   0      2,812 K
```

PSEXEC (3) Captura de Rede

BUNKER CYBER SECURITY

	Source	Destination	Protocol	Lengtl	Info
13:03:51.284507	172.31.7.162	172.31.4.76	SMB2	306	Negotiate Protocol Response
13:03:51.284559	172.31.4.76	172.31.7.162	SMB2	358	Negotiate Protocol Request
13:03:51.285127	172.31.7.162	172.31.4.76	SMB2	430	Negotiate Protocol Response
13:03:51.294223	172.31.4.76	172.31.7.162	SMB2	2028	Session Setup Request
13:03:51.295557	172.31.7.162	172.31.4.76	SMB2	315	Session Setup Response
13:03:51.295837	172.31.4.76	172.31.7.162	SMB2	192	Tree Connect Request Tree: \\bridge01.10bank.com.br\ADMIN$
13:03:51.296674	172.31.7.162	172.31.4.76	SMB2	138	Tree Connect Response
13:03:51.296738	172.31.4.76	172.31.7.162	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
13:03:51.296852	172.31.4.76	172.31.7.162	SMB2	234	Create Request File:
13:03:51.297158	172.31.7.162	172.31.4.76	SMB2	322	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
13:03:51.297462	172.31.7.162	172.31.4.76	SMB2	298	Create Response File:
13:03:51.297657	172.31.4.76	172.31.7.162	SMB2	146	Close Request File:
13:03:51.297940	172.31.7.162	172.31.4.76	SMB2	182	Close Response
13:03:51.298079	172.31.4.76	172.31.7.162	SMB2	382	Create Request File: PSEXESVC.exe
13:03:51.298488	172.31.7.162	172.31.4.76	SMB2	130	Create Response, Error: STATUS_PENDING
13:03:51.298550	172.31.7.162	172.31.4.76	SMB2	130	Create Response, Error: STATUS_SHARING_VIOLATION
13:03:51.681880	172.31.4.76	172.31.7.162	SMB2	510	Create Request File: PSEXEC-WORKSTATION400-DE1B577C.key
13:03:51.682836	172.31.7.162	172.31.4.76	SMB2	410	Create Response File: PSEXEC-WORKSTATI
13:03:51.683524	172.31.4.76	172.31.7.162	SMB2	178	Write Request Len:8 Off:0 File: PSEXEC
13:03:51.683990	172.31.7.162	172.31.4.76	SMB2	138	Write Response
13:03:51.684118	172.31.4.76	172.31.7.162	SMB2	178	Write Request Len:8 Off:8 File: PSEXEC
13:03:51.684472	172.31.7.162	172.31.4.76	SMB2	138	Write Response
13:03:51.686221	172.31.4.76	172.31.7.162	SMB2	188	Tree Connect Request Tree: \\bridge01.
13:03:51.686984	172.31.7.162	172.31.4.76	SMB2	138	Tree Connect Response
13:03:51.687070	172.31.4.76	172.31.7.162	SMB2	194	Create Request File: PSEXESVC
13:03:51.687752	172.31.7.162	172.31.4.76	SMB2	210	Create Response File: PSEXESVC

No.	Time	Source	Destination	Protocol	Lengtl	Info
660	2025-10-13 13:03:51.600791	172.31.4.76	172.31.7.162	SVCCTL	226	OpenSCManager2 request
662	2025-10-13 13:03:51.601311	172.31.7.162	172.31.4.76	SVCCTL	194	OpenSCManager2 response
665	2025-10-13 13:03:51.647338	172.31.4.76	172.31.7.162	SVCCTL	370	CreateWowService request
667	2025-10-13 13:03:51.647956	172.31.7.162	172.31.4.76	SVCCTL	194	CreateWowService response
668	2025-10-13 13:03:51.648128	172.31.4.76	172.31.7.162	SVCCTL	226	OpenServiceW request
670	2025-10-13 13:03:51.648639	172.31.7.162	172.31.4.76	SVCCTL	194	OpenServiceW response
671	2025-10-13 13:03:51.650679	172.31.4.76	172.31.7.162	SVCCTL	194	StartServiceW request
673	2025-10-13 13:03:51.651311	172.31.7.162	172.31.4.76	SVCCTL	178	StartServiceW response
674	2025-10-13 13:03:51.653162	172.31.4.76	172.31.7.162	SVCCTL	194	QueryServiceStatus request
676	2025-10-13 13:03:51.654601	172.31.7.162	172.31.4.76	SVCCTL	194	QueryServiceStatus response
677	2025-10-13 13:03:51.654705	172.31.4.76	172.31.7.162	SVCCTL	194	CloseServiceHandle request
679	2025-10-13 13:03:51.655089	172.31.7.162	172.31.4.76	SVCCTL	194	CloseServiceHandle response
680	2025-10-13 13:03:51.655183	172.31.4.76	172.31.7.162	SVCCTL	194	CloseServiceHandle request
682	2025-10-13 13:03:51.655570	172.31.7.162	172.31.4.76	SVCCTL	194	CloseServiceHandle response

```
> Frame 671: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface \Device\NPF_{D7F2A7DC-EA23-44EF-8E
> Ethernet II, Src: 02:ab:bb:fc:77:95 (02:ab:bb:fc:77:95), Dst: 02:d1:6c:14:8a:05 (02:d1:6c:14:8a:05)
> Internet Protocol Version 4, Src: 172.31.4.76, Dst: 172.31.7.162
> Transmission Control Protocol, Src Port: 49229, Dst Port: 59794, Seq: 2870, Ack: 787, Len: 140
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLen: 140, Call: 5, Ct
v Service Control, StartServiceW
    Operation: StartServiceW (19)
    [Response in frame: 673]
```

Acima um trecho na captura que mostra a comunicação via SMBv2 (porta 445) durante a execução de código via PSEXEC.

Ao lado, após a cópia do PSEXESVC.EXE, utilizando DCE/RPC o serviço do PSEXEC é iniciado remotamente (usando portas altas - 59794)

PSEXEC (4) Visibilidade via EDR

A melhor forma de monitorar os processos executados via PSEXEC, é monitorar os processos executados pelo processo pai “PSEXESVC.exe”:

EDR

```
event.type = 'Behavioral Indicators' osSrc.process.parent.name = 'PSEXESVC.exe'
| columns event.time , endpoint.name , src.process.user , osSrc.process.parent.name, src.process.name , src.process.cmdline
```

columns filter group join inner join sql inner join left join sql left join outer join sql outer join let limit lookup parse sort transpose union

11 rows returned 9:29 AM – 11:29 AM UTC-3

Event Time	Endpoint Name	Source Process User	OS Source Process Parent Name	Source Process Name	Source Process Comma
Oct 13, 2025 9:51:45 AM	BRIDGE01	10BANK\alex	PSEXESVC.exe	notepad.exe	"notepad.exe"
Oct 13, 2025 11:11:03 AM	BRIDGE01	10BANK\alex	PSEXESVC.exe	tasklist.exe	"tasklist"

PSEXEC (5)

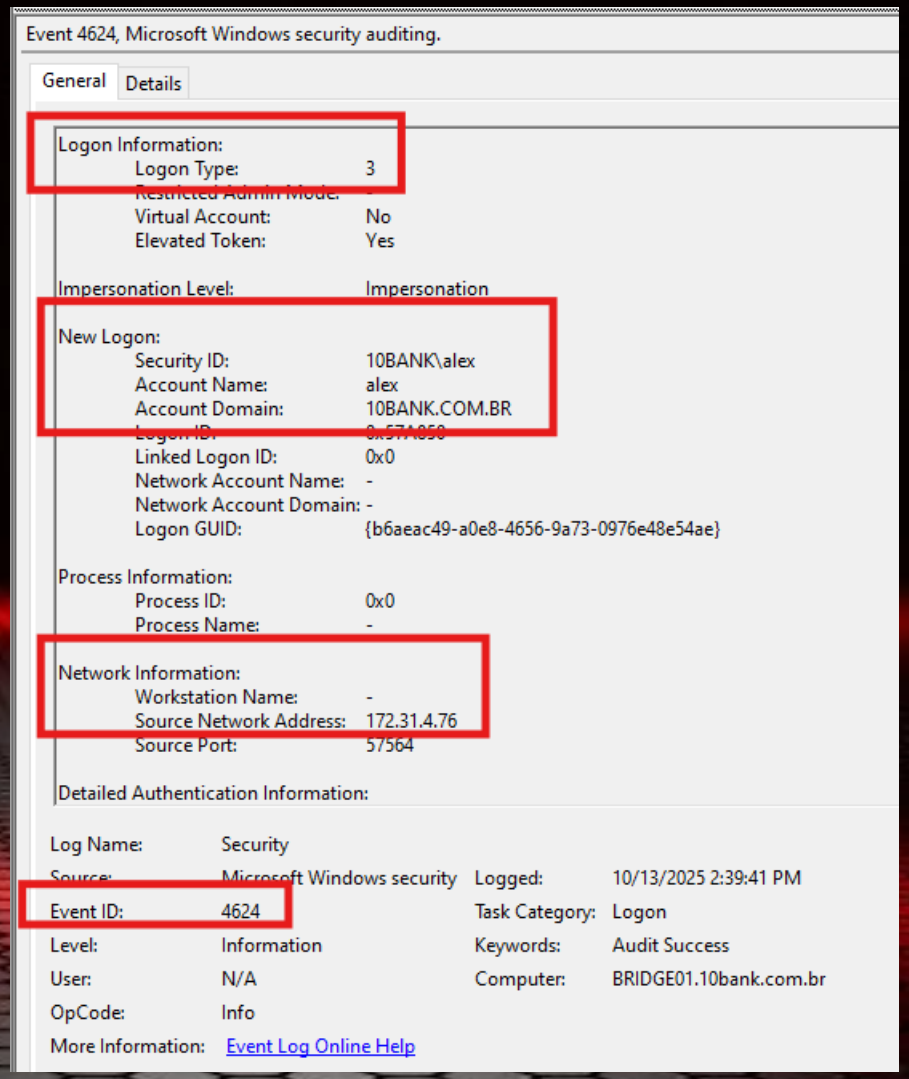
Visibilidade no Event Viewer

Ao monitorar o event viewer no host “alvo”, enquanto uma execução de código remoto é feita via PSEXEC, observamos eventos generalistas que também ocorrem quando outros tipos de acesso a rede acontecem.

Somente pelo event viewer, não identificamos uma forma precisa de confirmar a execução de código remoto via PSEXEC, exceto caso você tenha no event viewer logs de execuções de processo, aí basta monitorar as execuções via PSEXESVC.exe

Em alguns casos, o evento ID 7045 sobre a instalação de um novo serviço é evidenciado no event viewer, na seção System.

Observe que há formas diferentes de execução do PSEXEC, via binário da Microsoft, via Metasploit, CobaltStrike, etc. Padrões podem ser modificados.



PSEXEC (6) Dicas de Investigação

1. Monitore a execução do psexec nas máquinas de origem, através da monitoração do processo psexec.exe e psexec64.exe.

2. Monitore no host alvo, os processos executados onde o processo pai destes processos é o PSEXESVC.exe.

3. Monitore a instalação de um novo serviço (event id 7045) de forma remota e referencia ao nome PSEXESVC.

Soluções e Serviços que oferecemos:

BUNKER CYBER SECURITY

Soluções

- Anti-Ransomware (Security Snares)
- EDR / XDR
- PAM
  - Conexão Remota Privilegiada Segura
  - Gestão de privilégios humanos e não humanos
  - Privilégios temporários automatizados
  - Cofre de Senhas
- Cloud Security
- ITDR – Identity Threat Detection and Response
- CTEM - Continuous Threat Exposure Management
- BAS – Breach Attack Simulation
- Auditoria e Governança de acessos
- Network Security
  - Risk and Exposure Management
  - Threat Detection & Response
- Triagem Forense

Serviços

- Resiliência contra ataques de Ransomware
- Teste de ferramentas de segurança contra ataques de Ransomware
- Assessment de Hygiene de segurança de TI
- Compromise Assessment
- MSP
- MDR
- Assistência a deployments de soluções de segurança.
- Consultoria de melhores práticas.
- Treinamentos especializados.
- Simulação de Crise Cibernética (table top)
- Identity Risk Assessment.
- Resposta a incidentes.

Obrigado pela leitura!

Feedbacks com comentários e sugestões são bem vindos para:
alex@bunkercs.com.br

Para vídeos e mais informações sobre a Bunker, acesse
www.bunkercybersecurity.com.br .