Boogeyman 3

Task 1: Introduction

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.

In this room, you will be tasked to analyse the new tactics, techniques, and procedures (TTPs) of the threat group named Boogeyman.

Prerequisites

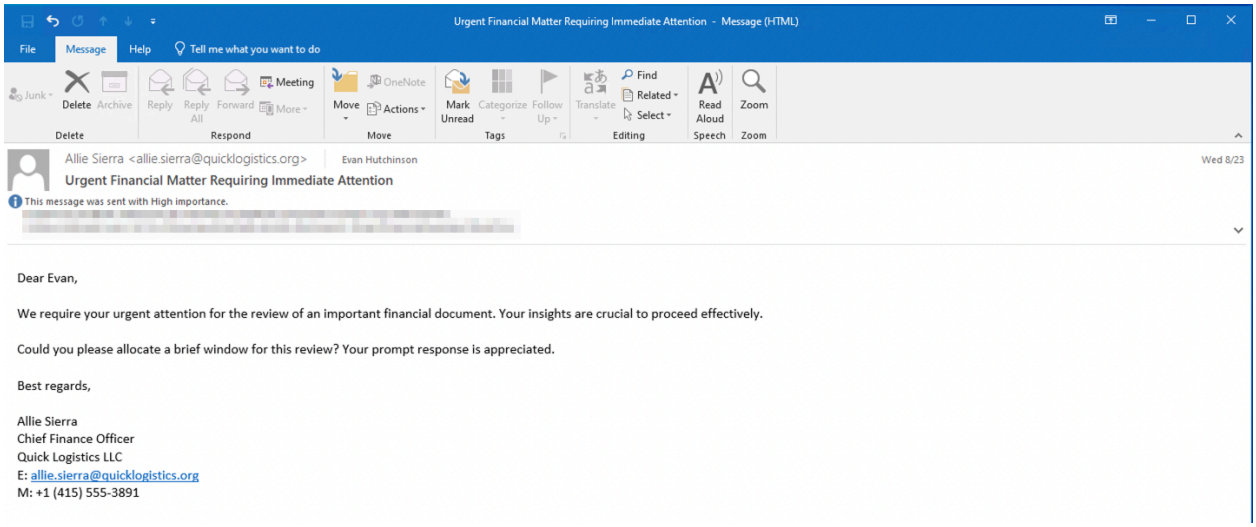
This room may require the combined knowledge gained from the SOC L1 Path. We recommend going through the following rooms before attempting this challenge.

- Sysmon
- ItsyBitsy
- Investigating with ELK
- Boogeyman 1
- Boogeyman 2

Task 2: The Chaos Inside

Lurking in the Dark

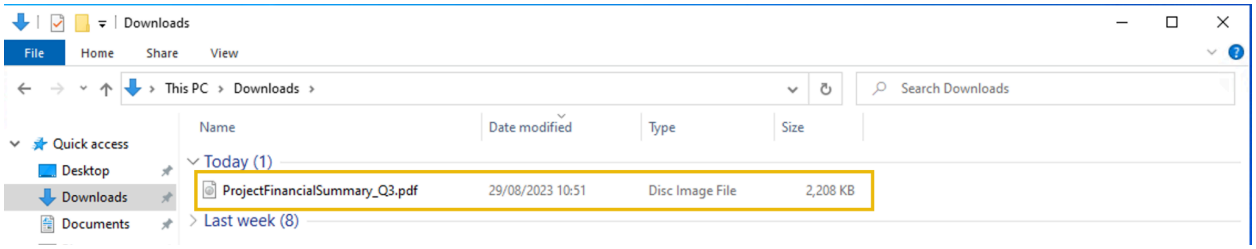
Without tripping any security defences of Quick Logistics LLC, the Boogeyman was able to compromise one of the employees and stayed in the dark, waiting for the right moment to continue the attack. Using this initial email access, the threat actors attempted to expand the impact by targeting the CEO,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



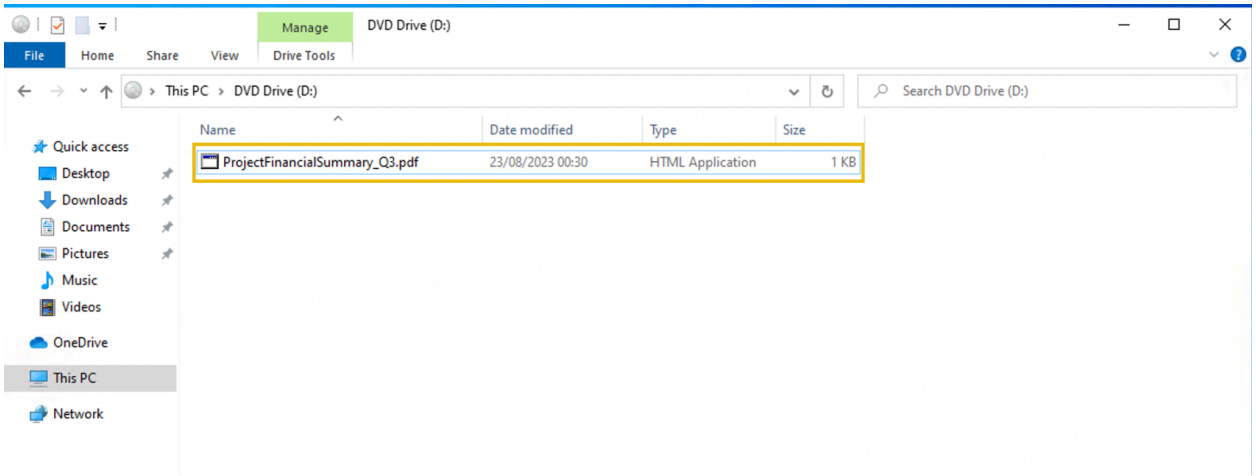
The email appeared questionable, but Evan still opened the attachment despite the scepticism. After opening the attached document and seeing that nothing happened, Evan reported the phishing email to the security team.

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.



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



Lastly, it was presumed by the security team that the incident occurred between **August 29 and August 30, 2023.**

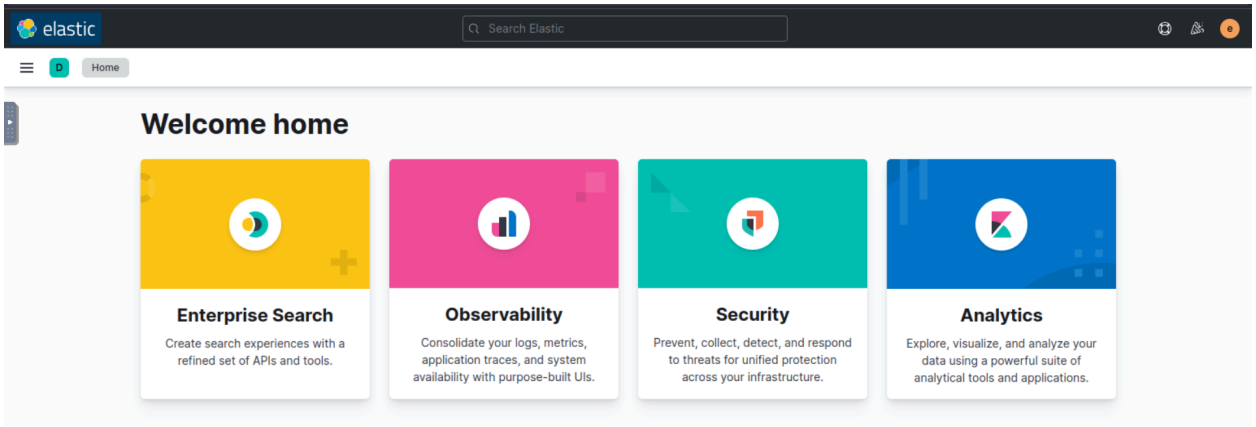
Given the initial findings, you are tasked to analyse and assess the impact of the compromise.

****

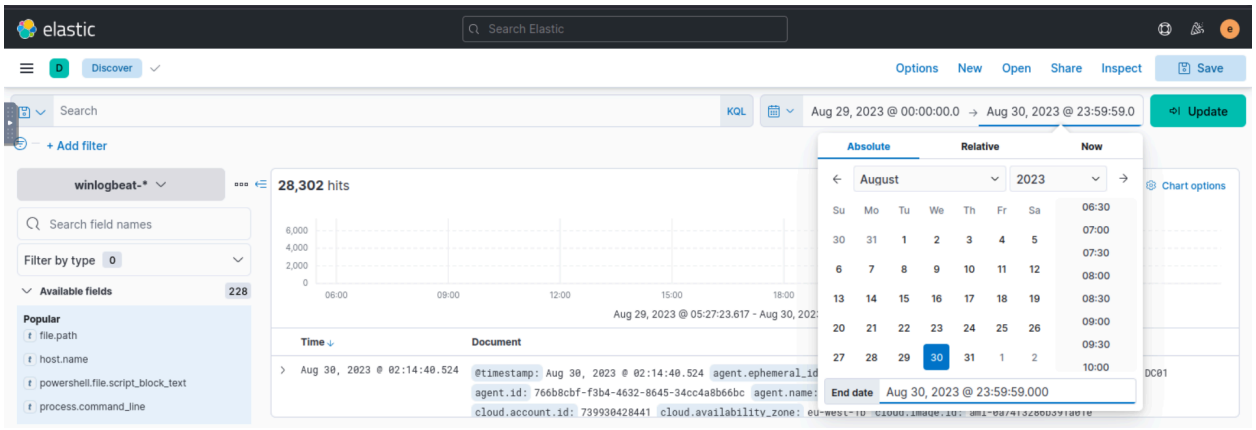
Answer the questions below:

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

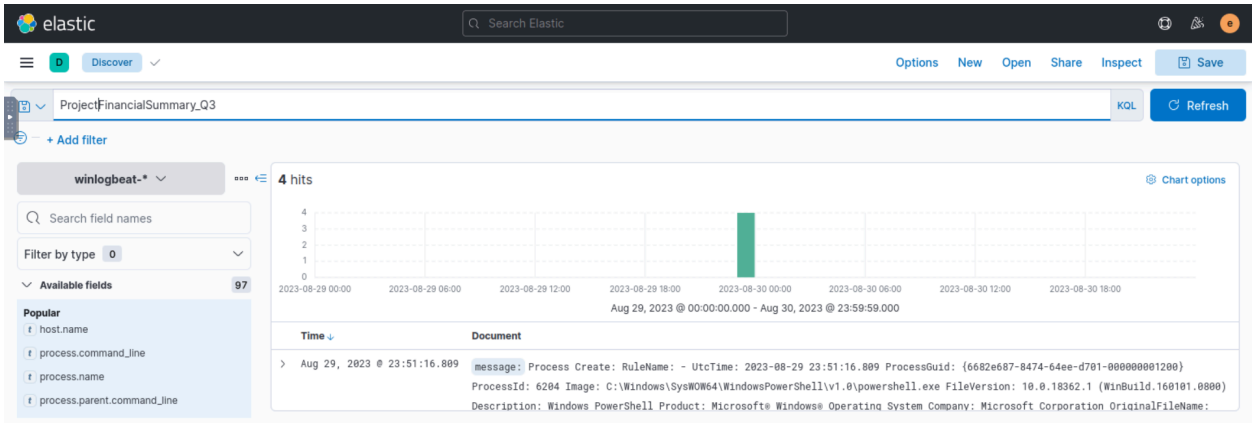
Start by logging into the Elastic instance for this room. To do this connect to the IP address of the machine instance and enter “elastic” for both the username and password.



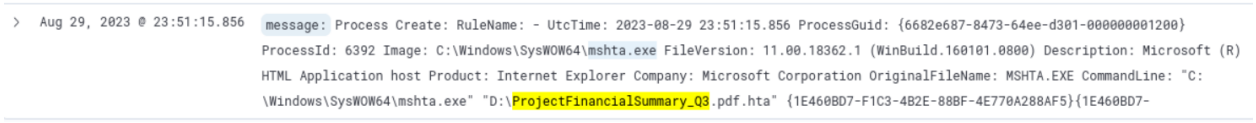
Go to the discover tab and update the time filter to be from August 29th 2023 to August 30th 2023. This will show us all the logs for the incident in question.



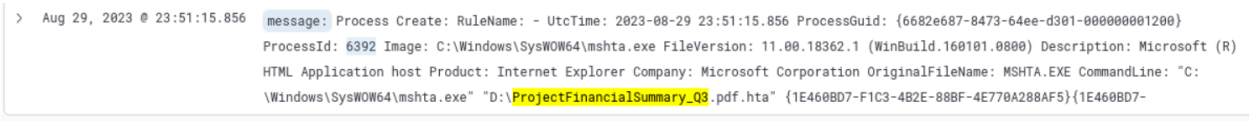
To begin I simply started by searching for the malicious document found in the email.



This resulted in four hits. Starting at the oldest entry we see that the malicious file spawns mshta.exe, this is a native Windows binary that is used to run .HTA HTML files, and when we look at the information given to us earlier in the task we see that the ProjectFinancialSummary_Q3.pdf file was saved as an HTML file.



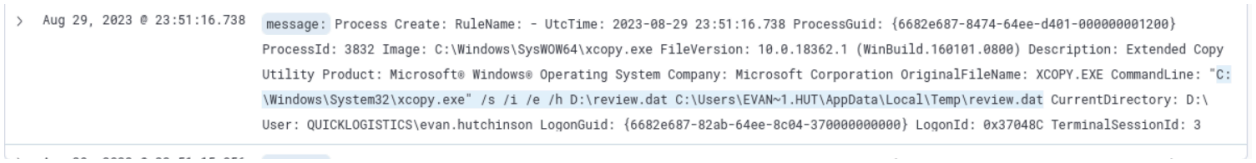
The PID is also found in that same output.



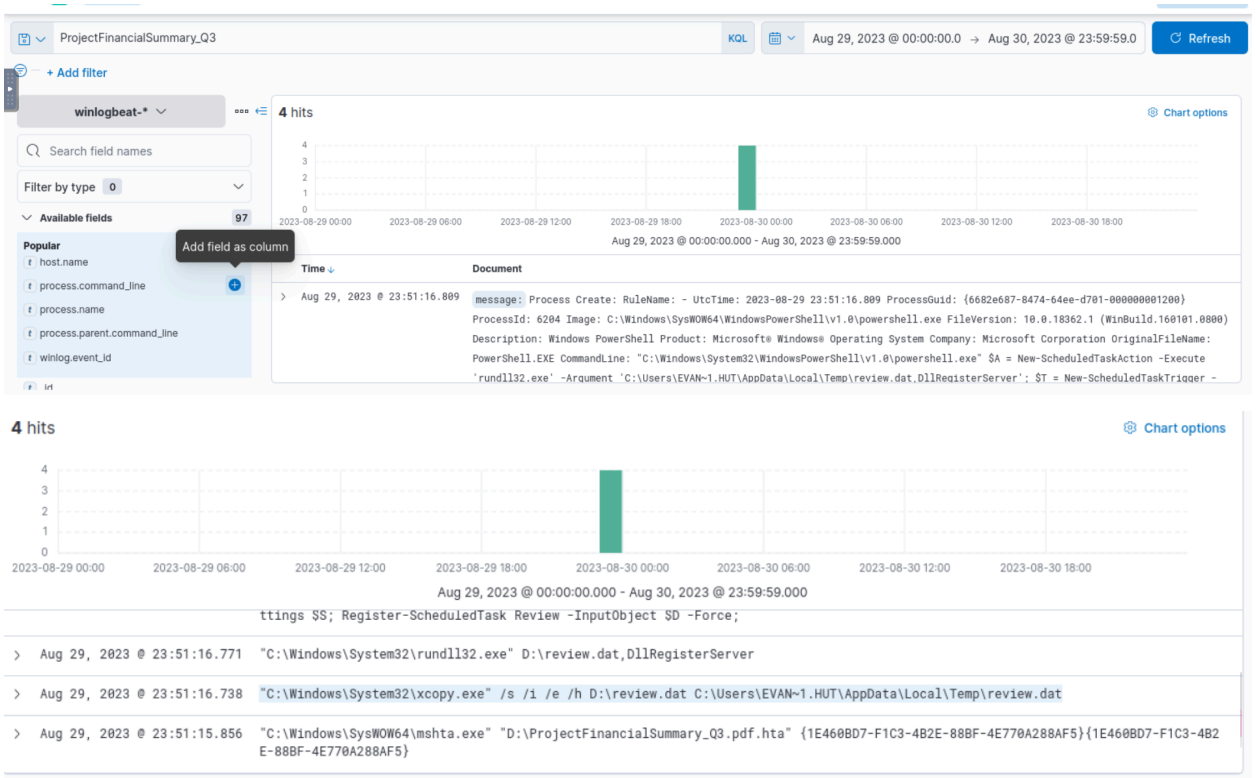
Answer: 6392

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

Moving to the next log we see that the file used xcopy to write a file to the temp directory on the CEO's machine.



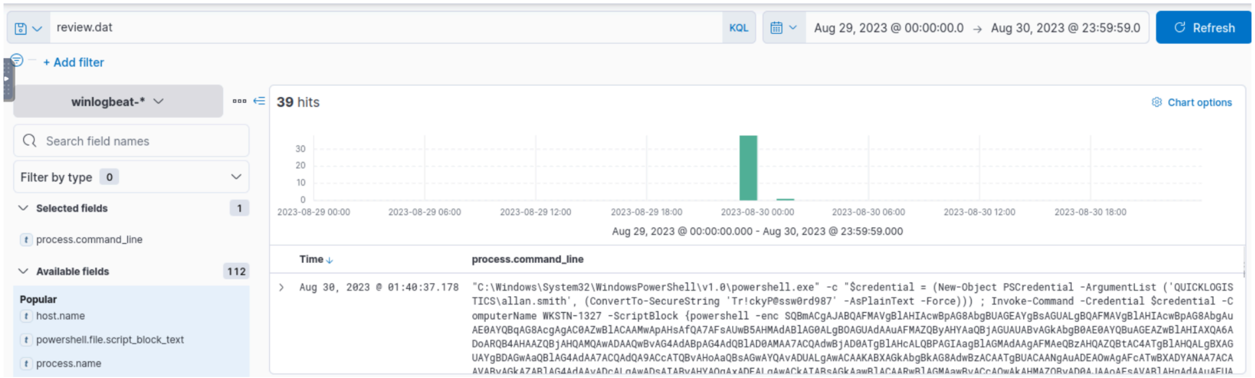
Since we're looking for a command-line input we can make this information easier to find at a glance by adding a column for the process.command_line field.



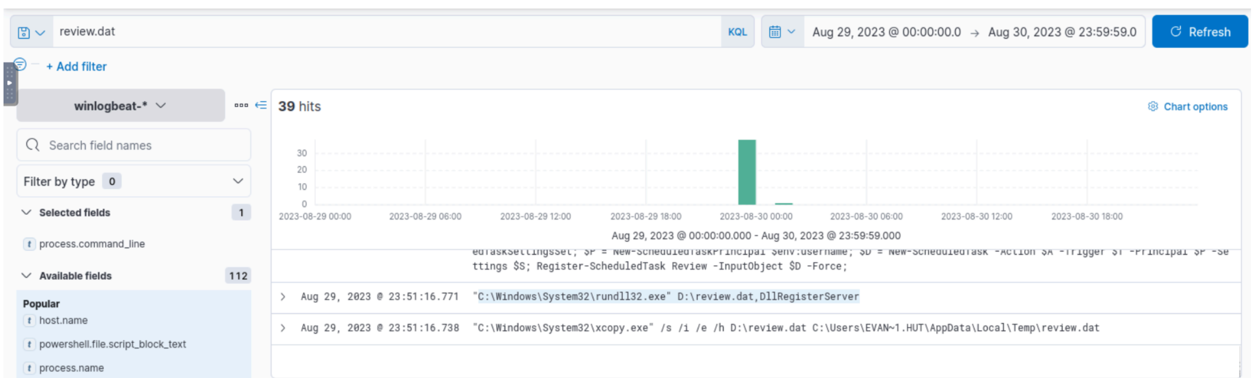
Answer: "C:\Windows\System32\xcopy.exe" /s /i /e /h D:\review.dat C:\Users\EVAN~1.HUT\AppData\Local\Temp\review.dat

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

Since we're looking for the execution of the implanted file I started by changing the search to "review.dat." This resulted in a total of 39 hits.



Again, we're looking for the full command-line value so I kept the same process.command_line column from the last question and started at the oldest of the logs.

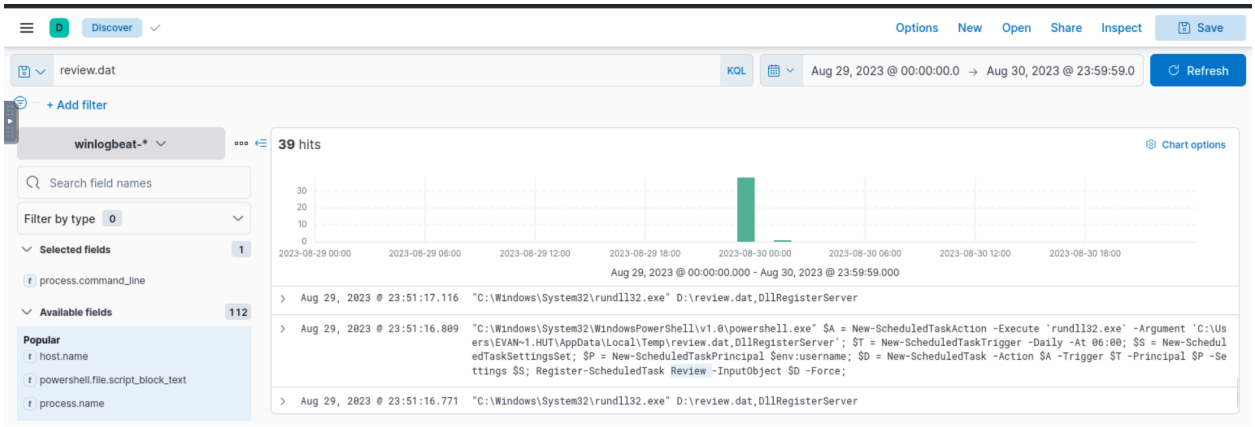


We see that rundll32.exe is being run by the implanted file.

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

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

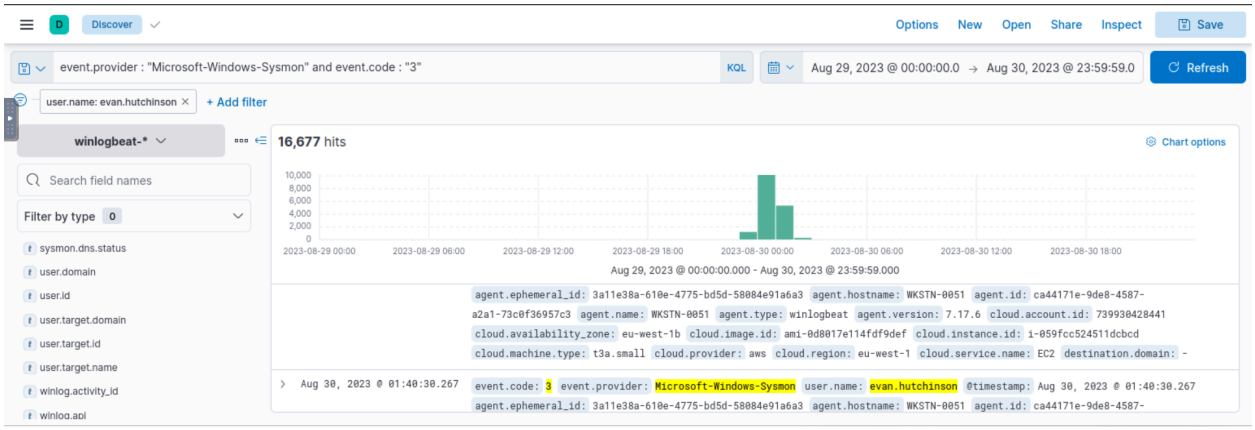
The next log shows the creation of a scheduled task that runs rundll32.exe with an argument of "C:\Windows\System32\rundll32.exe" D:\review.dat,DllRegisterServer" everyday at 6:00am, with a name of "Review."



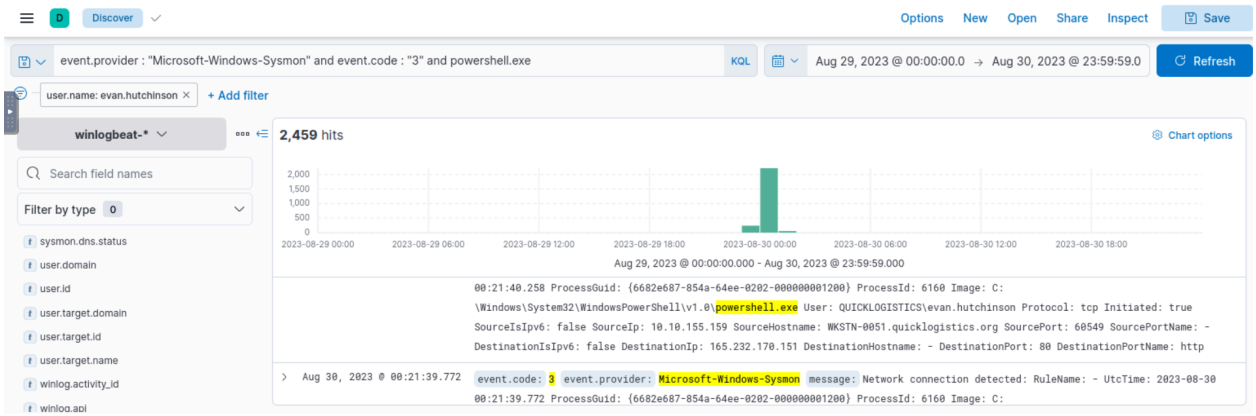
Answer: Review

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)

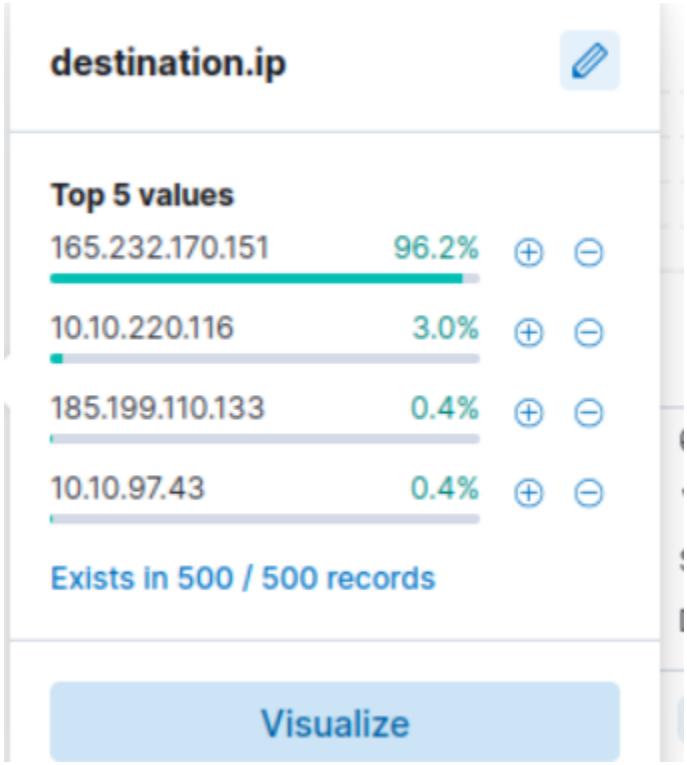
This one took me a minute to figure out where to start. I couldn't figure out a way to show network connections based on the Available Fields. Looking back through the information given by the room it says that Quick Logistics LLC uses Sysmon, and I know Sysmon EventID=3 is for network connections so I searched for that!



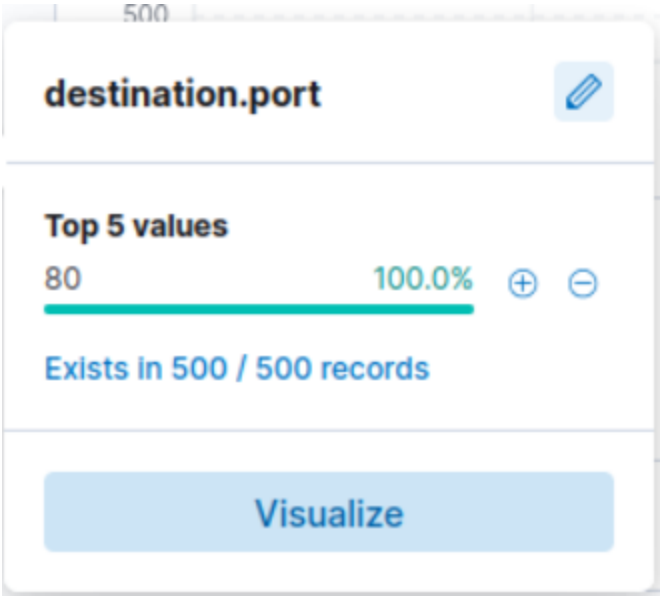
This left me with over 16,000 logs even after filtering for just the CEO's computer. Since the malicious file uses PowerShell I filtered down further with that too.



This brought the results down to 2,459 logs. From here we can use the destination.ip field name to see the top 5 destination IPs.

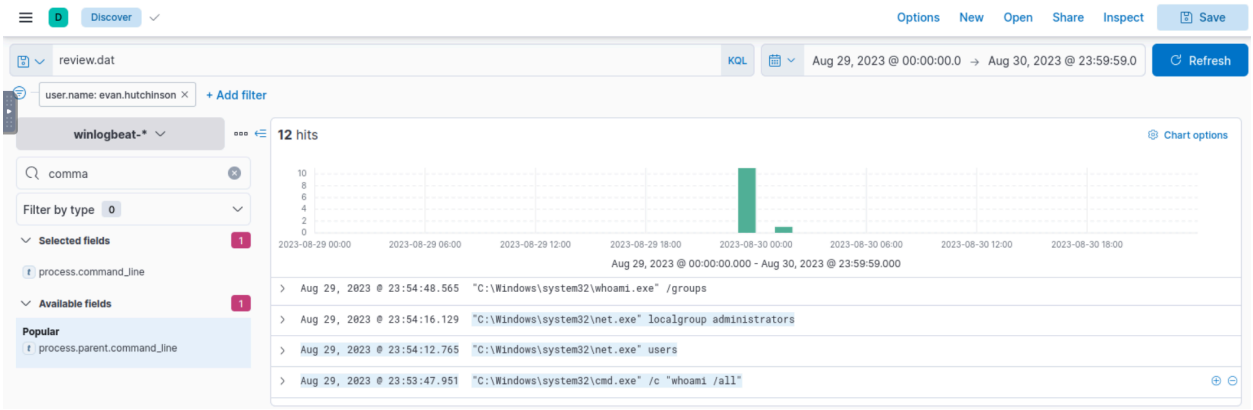


165.232.170.151 is by far the most accessed IP by PowerShell and since it is suspicious for PowerShell to be connecting to an external IP this is most likely our C2 server's IP address! We still need to find the port number and this can be done in the same way by looking at the destination.port field after filtering to just 165.232.170.151.

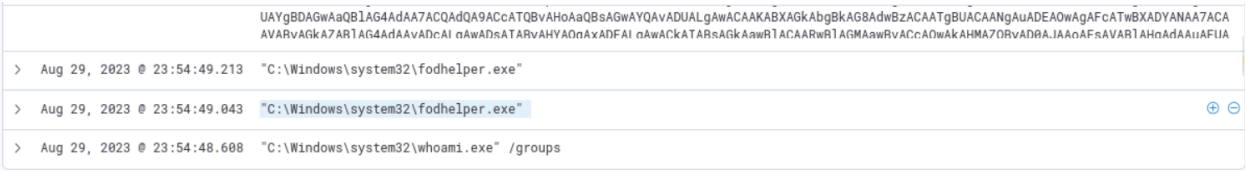


And here we have it! 100% of the time our potential C2 server was accessed it was accessed over HTTP using port 80.
Answer: 165.232.170.151:80

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?
The attacker bypassed User Access Controls(UAC) to escalate their privilege. The hint for this question tells us to “search for common UAC bypass techniques and follow the trail of events” and a common way attackers bypass UAC is through DLL hijacking. Starting with looking back at review.dat to see what other commands were executed with it.



We see that the attacker did some reconnaissance with the whoami command and net.exe to see who the local admins are. Scrolling through the logs I see a suspicious process called fodhelper.exe.

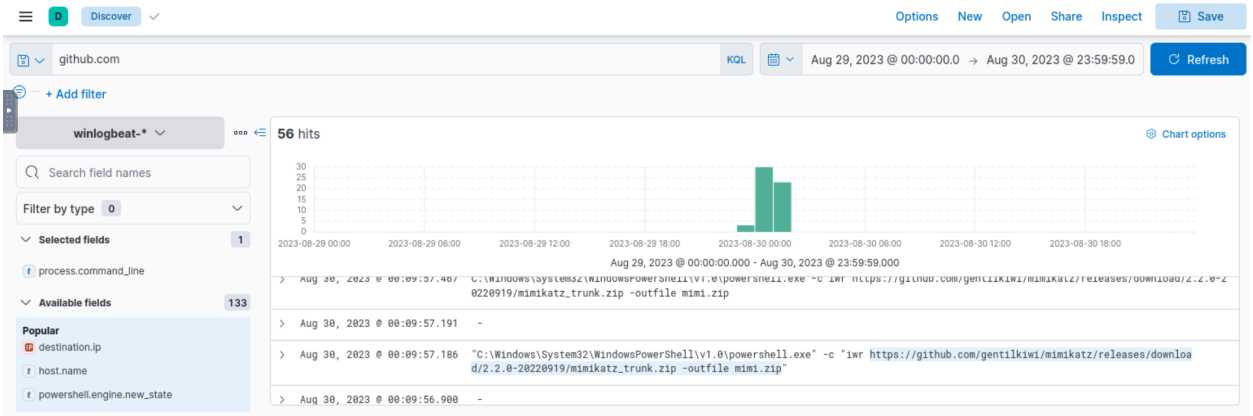


I wasn't sure what fodhelper did so I googled it and almost every result was how it can be used to bypass UAC. I still wanted to learn what it did though and after a little digging I found a blog post that says "Fodhelper is a trusted binary in Windows operating systems, which allows elevation without requiring a UAC prompt with most UAC settings."

Answer: fodhelper.exe

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?

For this one I just searched for "github.com" and filtered for the CEO's username and the process.command_line field.

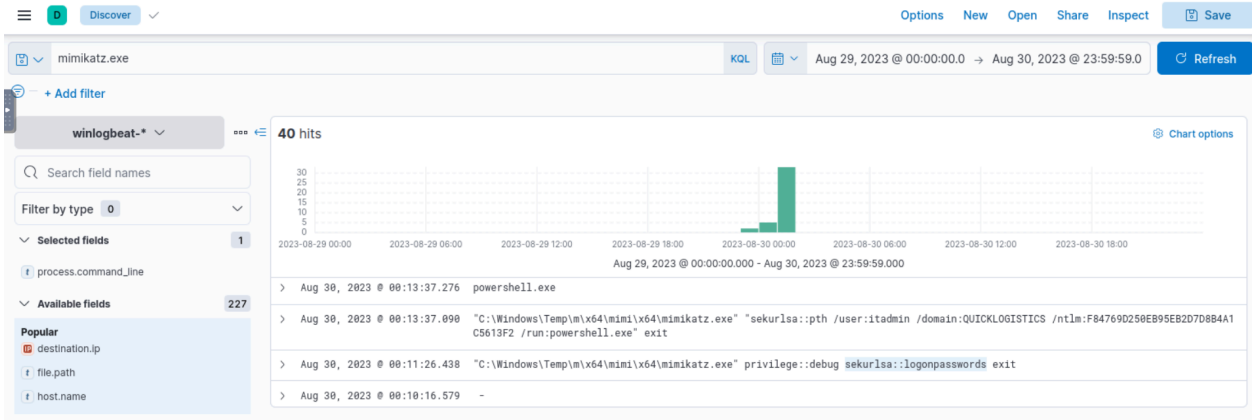


Here we see the attacker downloaded Mimikatz, a well known credential dumping tool.

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

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)

Searching for Mimikatz.exe we see that the attacker gets the username and plaintext password of a user recently logged onto this computer, sekurlsa::logonpasswords.

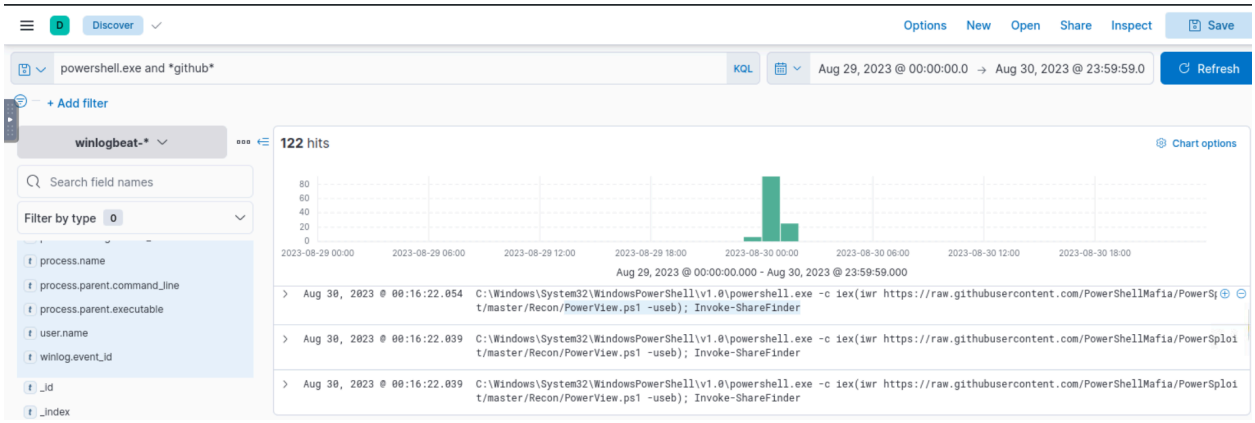


Using that new found information the user then logs as that user and uses a Pass the Hash attack to get access to the itadmin account.

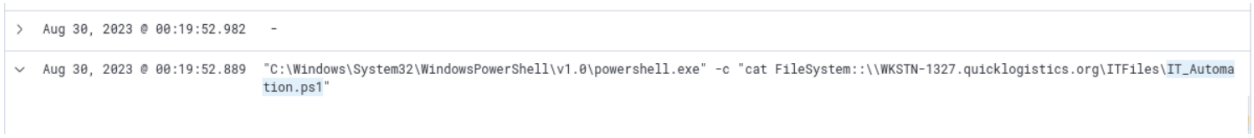
Answer: itadmin:F84769D250EB95EB2D7D8B4A1C5613F2

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?

Again, I wasn't quite sure how to start with this one. So after trying a few things and getting nowhere I turned to google to see if I could get an idea of where to start. A walkthrough for this room(Thank you Drew Arpino!) said that based on the TTPs of the attacker it's likely that they'd use PowerShell to download more tools from GitHub. Searching for "powershell.exe and *github*" this led to 122 results compared to the 56 when searching for "github.com." After scrolling past the Mimikatz download I found earlier I found some commands to download PowerView.ps1 and the Invoke-ShareFinder script. PowerView according to the GitHub is, "a PowerShell tool to gain network situational awareness on Windows domains," and the Invoke-ShareFinder is a script to find "non-standard shares on a host in the local domain."



Searching for all PowerShell commands issued by the workstation the attacker compromised, WKSTN-0051.quicklogistics.org, I found the answer after some digging.



Answer: IT_Automation.ps1

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)

Searching through the logs for the previous question I found the answer to this one.

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

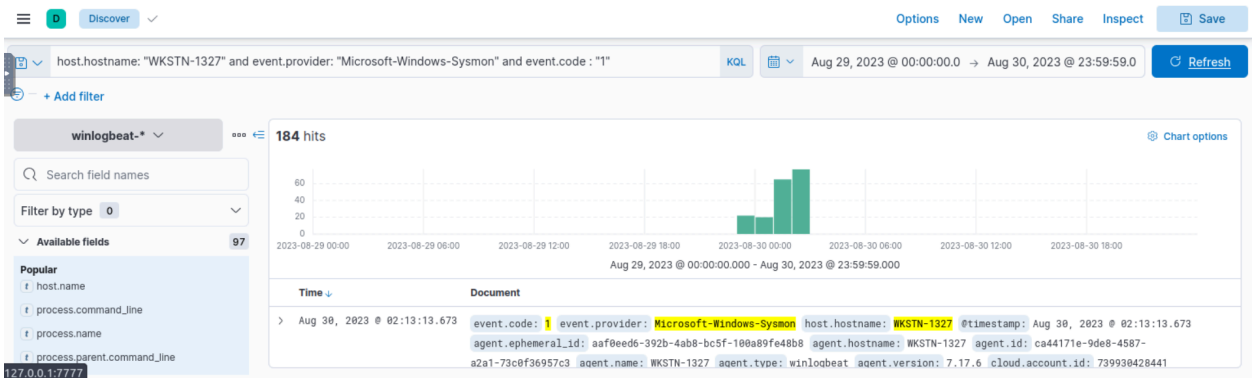
What is the hostname of the attacker's target machine for its lateral movement attempt?

The answer to this is found in the same command as the last answer.

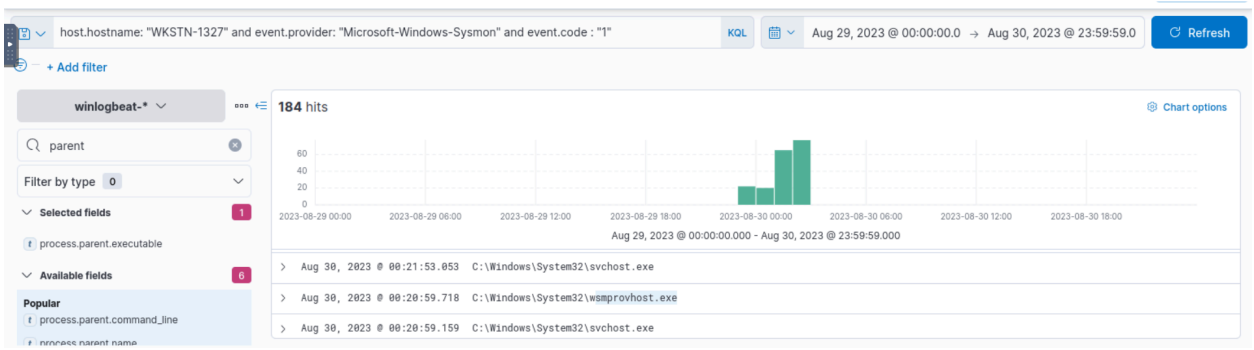
Answer: **WKSTN-1327**

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?

Knowing that we're on WKSTN-1327 now and that we're looking for process creation I'll filter for Sysmon EventID=1.

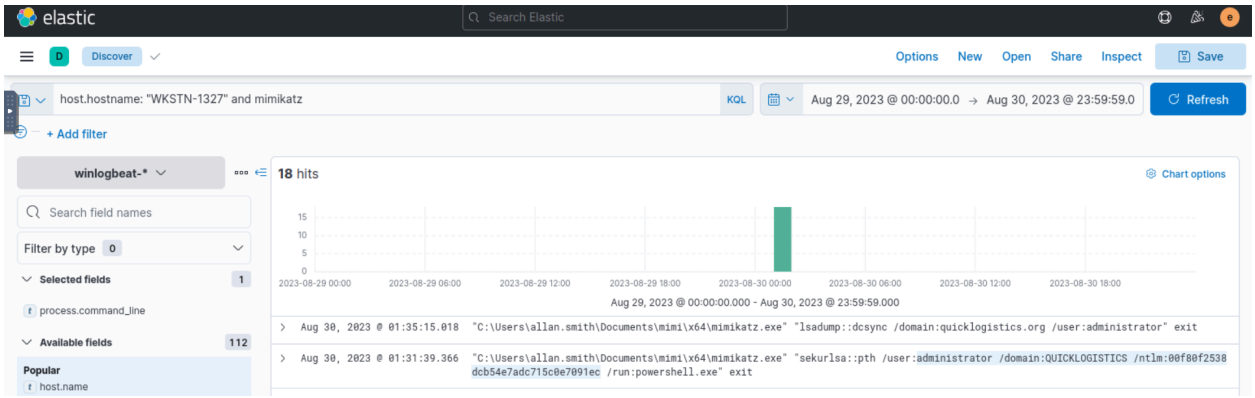


Filtering for parent.process.executable we see “wsmprovhost.exe” which is a process used for hosting remote sessions on a target.



Answer: wsmprovhost.exe

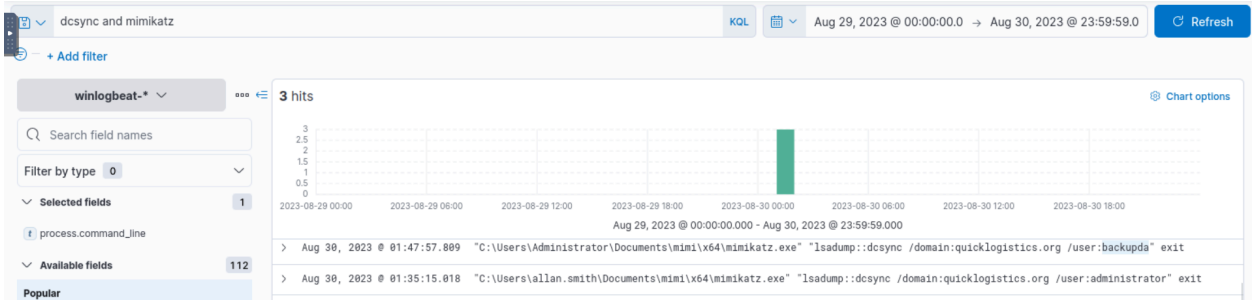
The attacker then dumped the hashes in this second machine. What is the username and hash of the newly dumped credentials? (format: username:hash)
Much like question 8 for this I searched for Mimikatz but still filtered for WKSTN-1327.



Answer: administrator:00f80f2538dcb54e7adc715c0e7091ec

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?

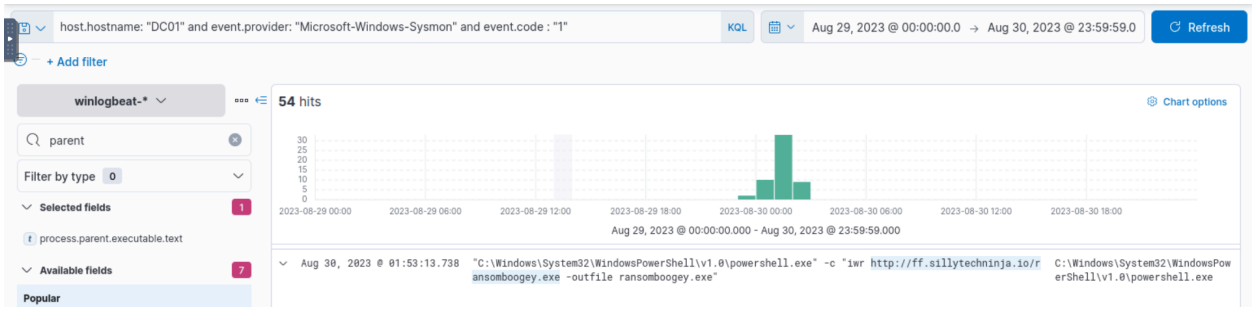
In the last question I noticed that the log above the one that had the answer showed the DCSync attack against the administrator account. So for this question I just searched for “dcsync and mimikatz” and got the answer.



Answer: backupda

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?

We know that the attacker got access to the Domain Controller and we know that the attacker uses PowerShell to download files so I searched for that but had too many results. From here I switched to filtering for Sysmon EventID=1 on the domain controller and got the answer. I had seen “ransomboogey.exe” multiple times throughout this room so I knew it was going to come back at the end.



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

Conclusion:

Overall this was an enjoyable challenge. There was only one question I needed outside help to figure out. I feel like these final capstone challenge rooms were a good sampler of different types of assignments I’d get as a SOC Level 1 analyst and I look forward to diving deeper and getting more experience with harder challenge rooms and the SOC Level 2 learning path.