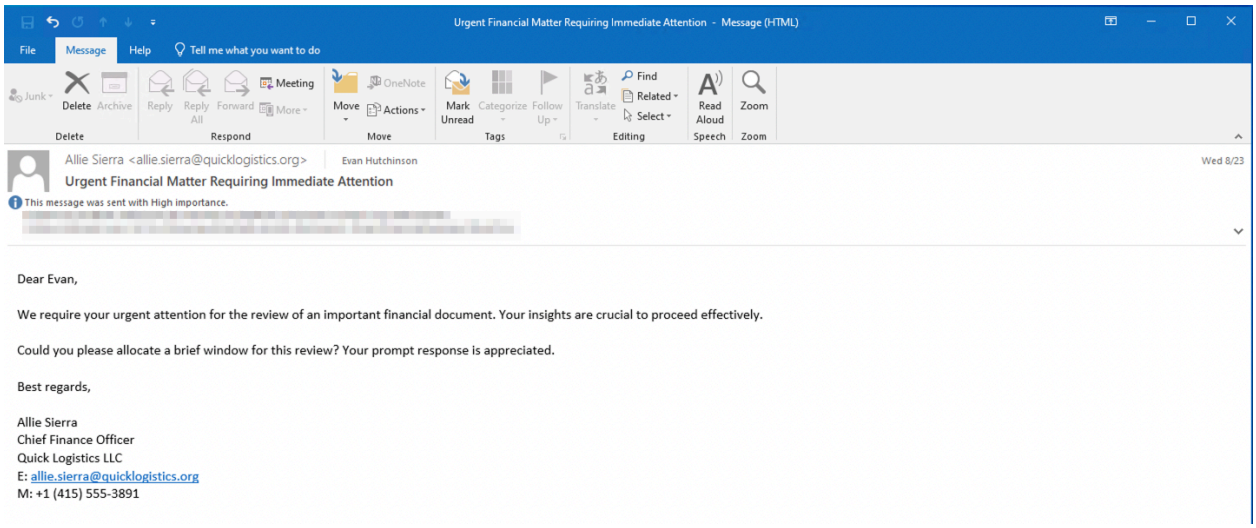
Lurking in the Dark

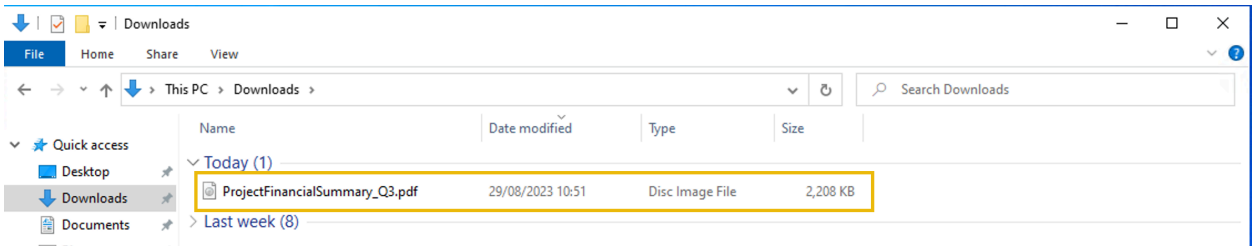
Without tripping any security defences of Quick Logistics LLC, the Boogeyman was able to compromise one of the employees and stayed in the dark, waiting for the right moment to continue the attack. Using this initial email access, the threat actors attempted to expand the impact by targeting the CEO,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



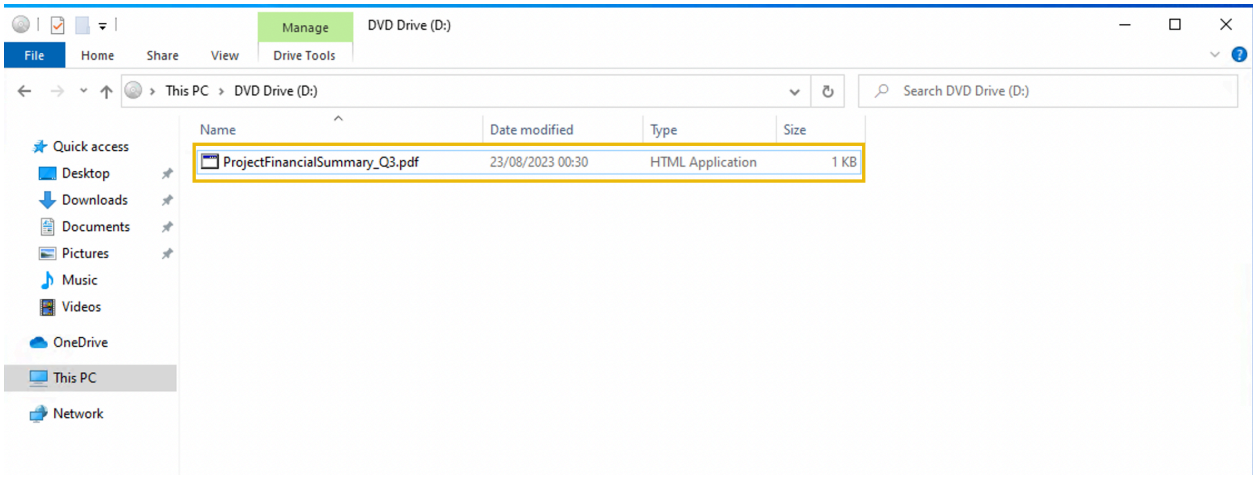
The email appeared questionable, but Evan still opened the attachment despite the scepticism. After opening the attached document and seeing that nothing happened, Evan reported the phishing email to the security team.

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.

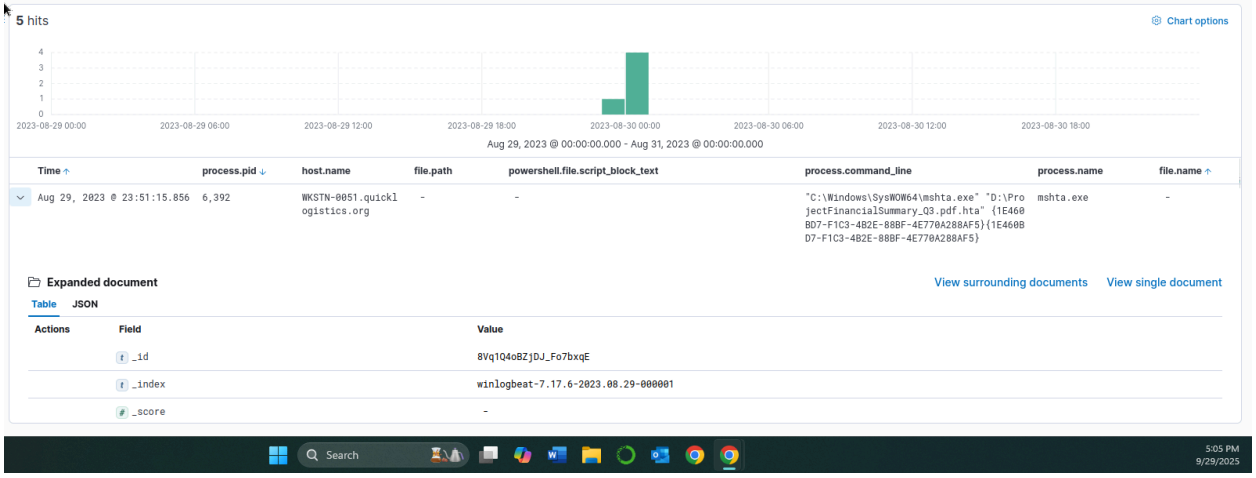


Lastly, it was presumed by the security team that the incident occurred between **August 29 and August 30, 2023**.

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

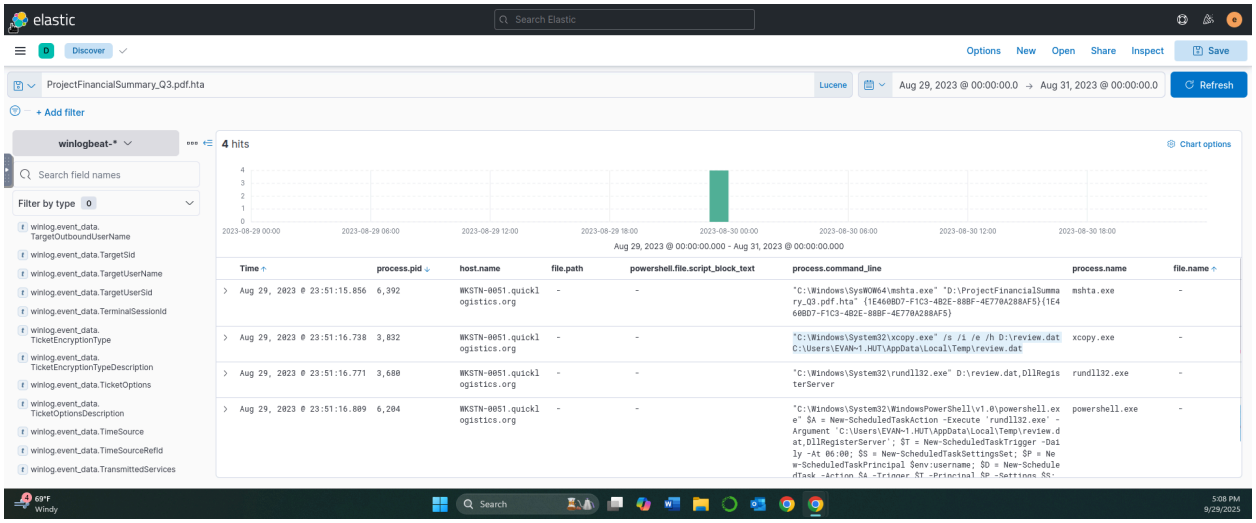
What is the PID of the process that executed the initial stage 1 payload?

So we know that the file downloaded was an html file, so I filtered for html files in Elastic. The answer popped up right at the top: 6392



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

So we know that the malicious file is “ProjectFinancialSummary_Q3.pdf.hta”, so I went ahead and filtered for the file. We could then see the stage 1 payload attempt to implant a file to another location under the command-line value: "C:\Windows\System32\xcopy.exe" /s /i /e /h D:\review.dat C:\Users\EVAN~1.HUT\AppData\Local\Temp\review.dat

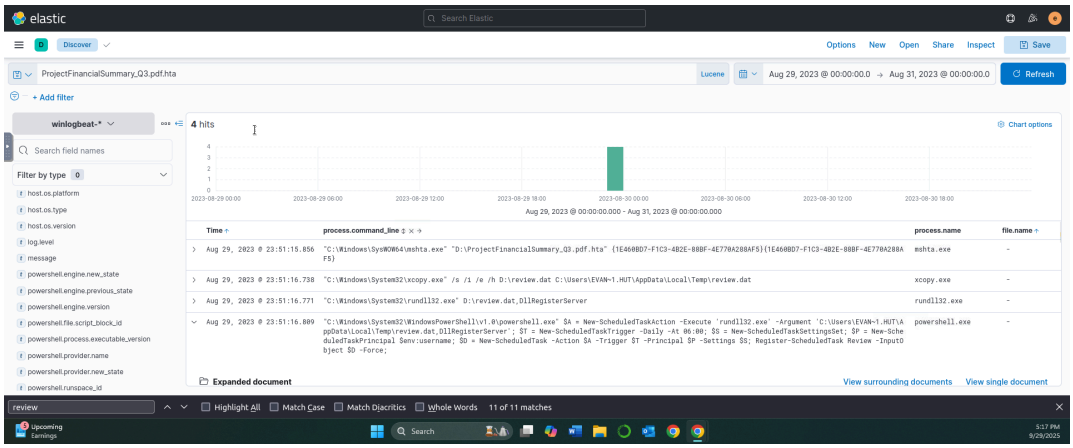


The implanted file was eventually used and executed by the stage 1 payload. What is the full command-line value of this execution?

Using the screenshot above, we get the answer right below the command ran in the last question: "C:\Windows\System32\rundll32.exe" D:\review.dat,DllRegisterServer

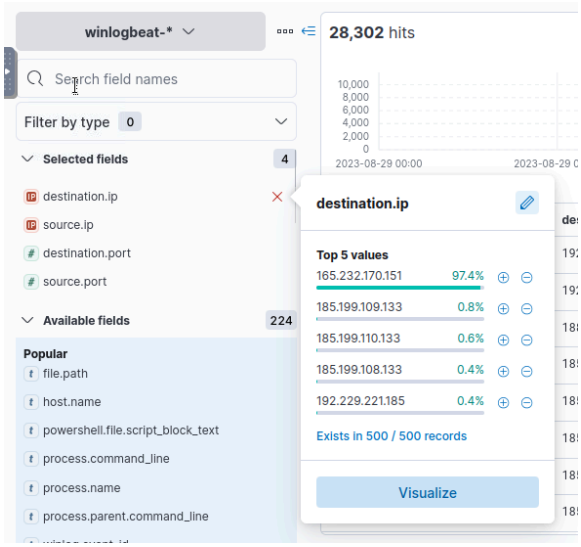
The stage 1 payload established a persistence mechanism. What is the name of the scheduled task created by the malicious script?

Still under the same filter for the malicious file, we can see that the new scheduled task created by the malicious script is “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)

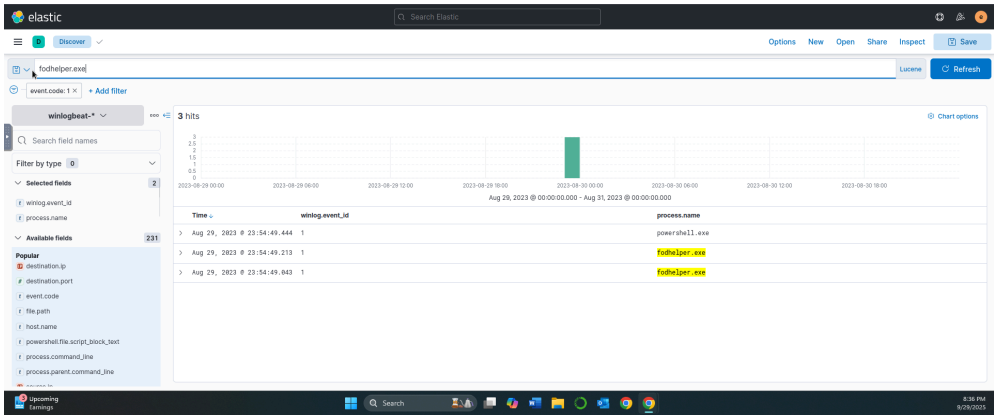
I went ahead and looked at the destination ip filter and it was clear that a C2 connection was established with 97.4% of destination ip addresses being: 162.232.170.151. We can then click and see that the port 80 is being used by this C2 connection.



Aug 30, 2023 @ 02:13:42.377	165.232.170.151	10.10.155.159	80
Aug 30, 2023 @ 02:10:20.014	165.232.170.151	10.10.155.159	80
Aug 30, 2023 @ 02:08:49.615	165.232.170.151	10.10.155.159	80
Aug 30, 2023 @ 02:08:44.095	165.232.170.151	10.10.155.159	80
Aug 30, 2023 @ 02:08:38.645	165.232.170.151	10.10.155.159	80
Aug 30, 2023 @ 02:08:33.198	165.232.170.151	10.10.155.159	80
Aug 30, 2023 @ 02:08:27.755	165.232.170.151	10.10.155.159	80
Aug 30, 2023 @ 02:08:22.298	165.232.170.151	10.10.155.159	80

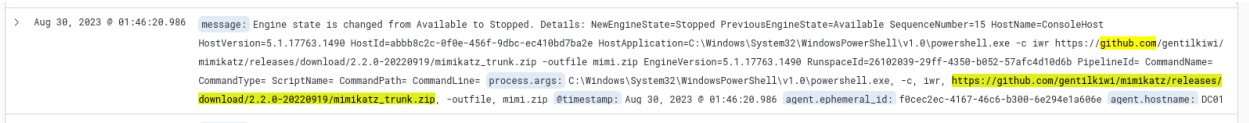
The attacker has discovered that the current access is a local administrator. What is the name of the process used by the attacker to execute a UAC bypass?

I did some research here on common UAC bypass techniques and filtered in the search bar for “fodhelper.exe”. It came across and per inspection, I was able to determine that the attacker used this technique for exploitation.



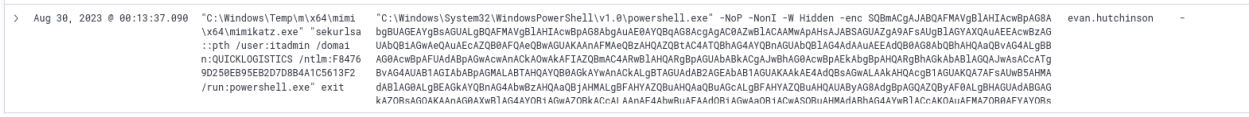
Having a high privilege machine access, the attacker attempted to dump the credentials inside the machine. What is the GitHub link used by the attacker to download a tool for credential dumping?

So I went ahead and filtered for *github* in the search bar since we know the attacker used a github link to download the tool. I scrolled through the results and saw that the attacker downloaded a link containing mimikatz, a known post exploitation tool that extracts windows credentials.



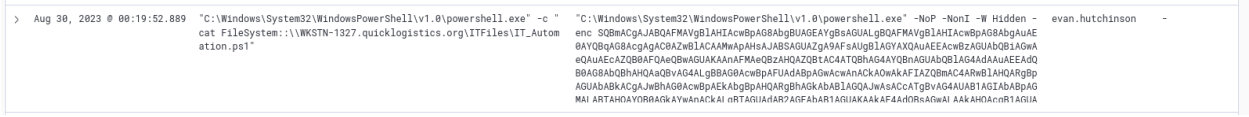
After successfully dumping the credentials inside the machine, the attacker used the credentials to gain access to another machine. What is the username and hash of the new credential pair? (format: username:hash)

Filtering for mimikatz in the search bar, we can follow the attacker's chain of attacks and we see the attacker use the itadmin username to gain access to another machine



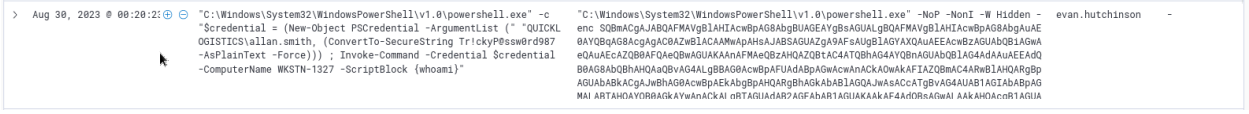
Using the new credentials, the attacker attempted to enumerate accessible file shares. What is the name of the file accessed by the attacker from a remote share?

Following the chronological order of events and when the attacker used the new credentials, we can see that right after using them, the user accesses the file "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)

Continuing following the attacker's events in chronological order under the "mimi" filter, we can see that the attacker discovered the following credentials after getting the contents of the remote file: QUICKLOGISTICS\allan.smith:Tr!ckyP@ssw0rd987

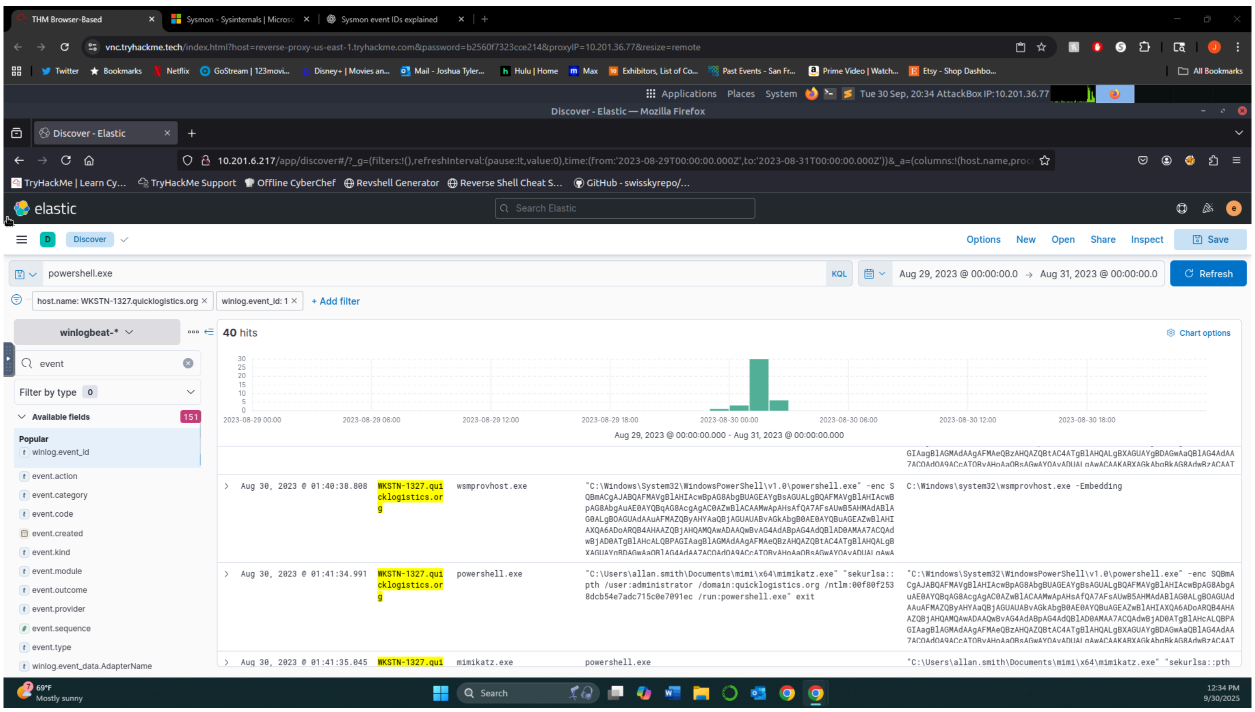


What is the hostname of the attacker's target machine for its lateral movement attempt?

We can get this answer from the previous question / screenshot, where we see the hostname of the machine is WKSTN-1327.

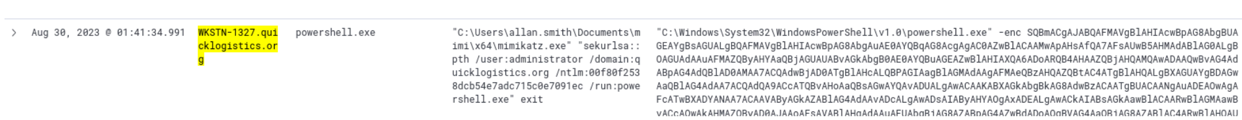
Using the malicious command executed by the attacker from the first machine to move laterally, what is the parent process name of the malicious command executed on the second compromised machine?

For this question, I filtered for the new machine we saw the attacker target in the prior question, and then based on the command executed by the attacker on the first machine, I filtered for powershell.exe and Sysmon event ID 1. From here I was able to quickly find my 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)

Knowing that the attacker is on the WKSTN-1327 machine, we can filter for this, and then “mimi” to locate the answer: administrator:00f80f2538dcb54e7adc715c0e7091ec

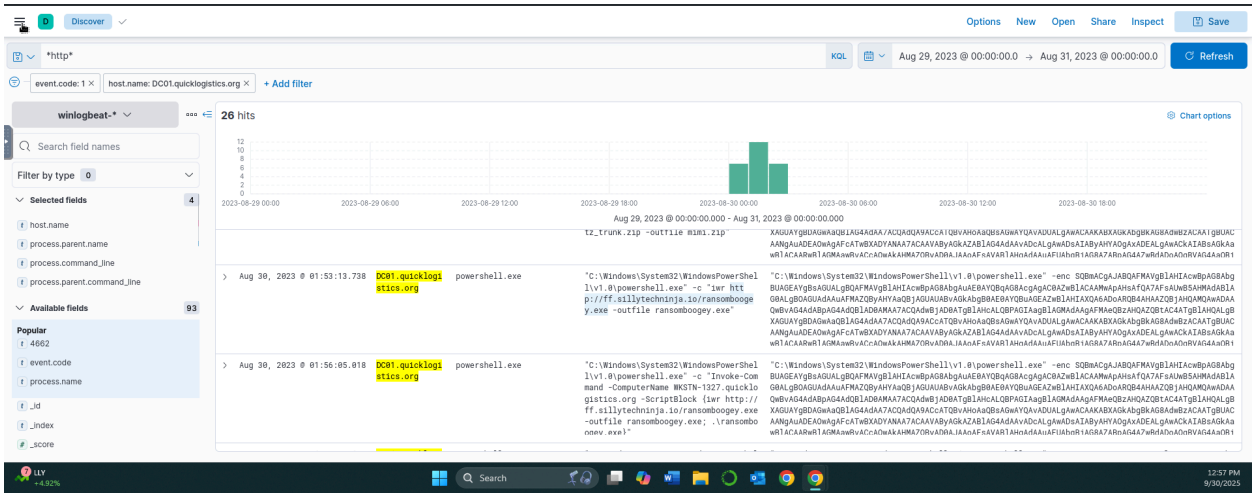


After gaining access to the domain controller, the attacker attempted to dump the hashes via a DCSync attack. Aside from the administrator account, what account did the attacker dump?

I filtered for DCsync in the search bar for this one, and a few records popped up around the administrator account the attacker dumped, and I was then able to see that the attacker also dumped the “backupda” account.

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?

Based on what we know, I filtered for the host name used in the prior question, filtered for Sysmon event ID 1, and filtered for *http*. From here, I was able to look chronologically after the user dumped the hashes, and found the answer: http://ff.sillytechninja.io/ransomboogey.exe



Conclusion:
This was a great lab to wrap up the SOC Level 1 course and complete the Boogeyman capstone challenges. It was a great refresher on using Elastic and evaluating SIEM logs, and was very interesting to see the attacker execute the full cyber kill chain, and see all of the steps the attacker took each step of the way, including initial compromise, persistence, privilege escalation, credential theft, lateral movement, domain compromise, and attempted ransomware. It shows just how quickly stolen credentials rapidly expand the attacker’s access.