CyberDefenders Qradar101 Write-up

This write-up is based on Cyberdefenders Qradar101 challenge from *Andrew Sefin*

First of all, let's start looking for offenses.

We can see 26 offenses between Oct 17 and Nov 8 of 2020.

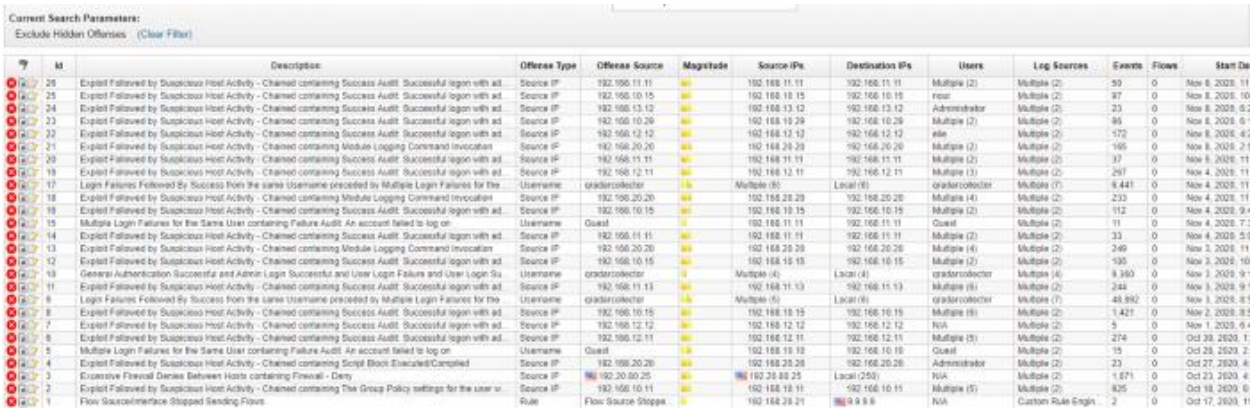

Fig 1 — Offenses

Despite this, the logs are between 10/11/2020 10:00 PM and 10/11/2020 3:00 PM

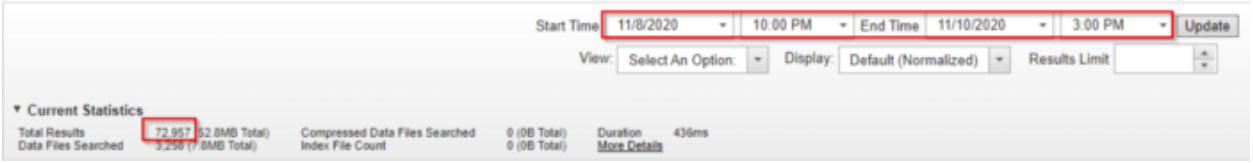

Fig 2— Log Activity

How many log sources available?

We can find this information going to Admin > Log Sources.

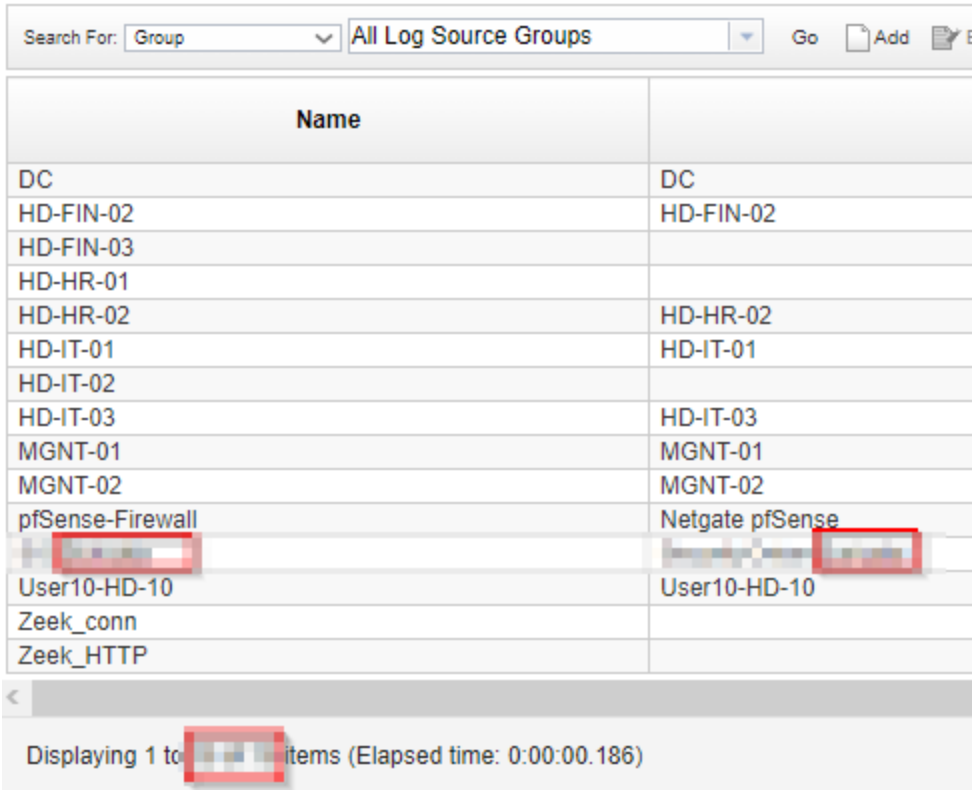

Fig 3 — Log Sources

What is the IDS software used to monitor the network?

We can see in figure 3 the IDS is one of the log sources.

What is the domain name used in the network?

We can find this information looking for payload events related to hosts as an example: Success Audit: A Kerberos service ticket was granted.

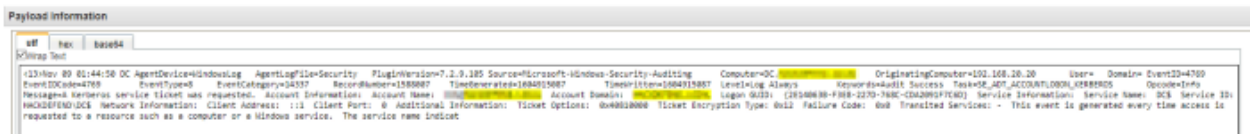

Fig 4 — Domain Payload

Multiple IPs were communicating with the malicious server. One of them ends with “20”. Provide the full IP.

We can display log Activity by Source IP to see what IPs generated more communication.

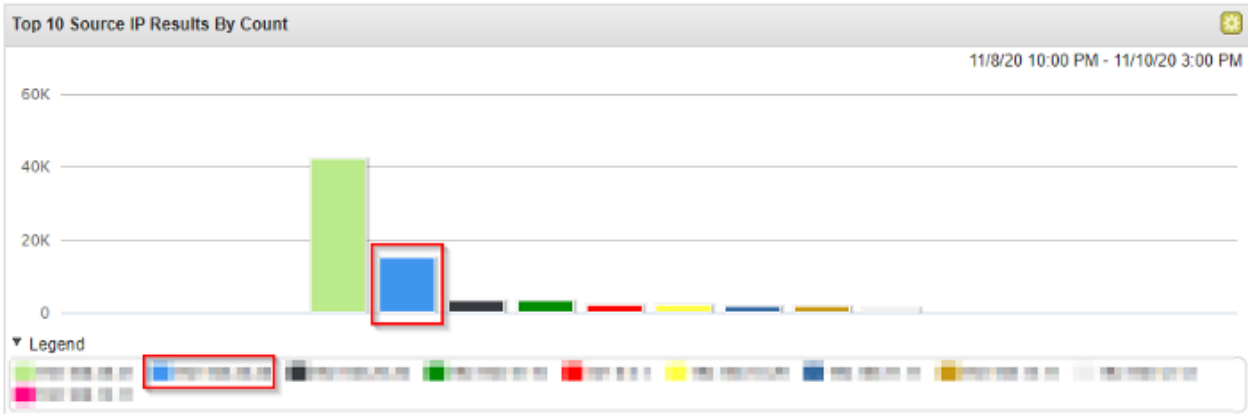

Fig 5 — Ip .20

What is the SID of the most frequent alert rule in the dataset?

We can look for sid: in the payload with regular expression.

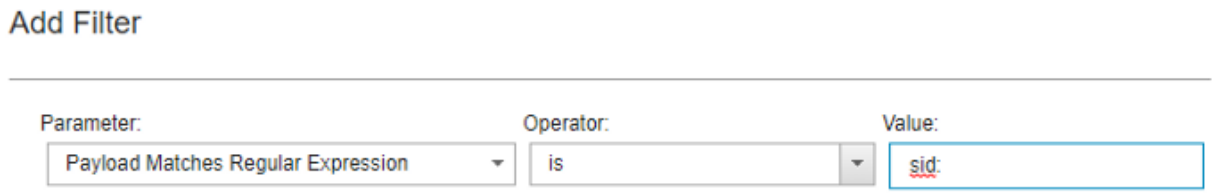

Fig 6 — sid

We will find 110 logs from SO-Suricata where 72

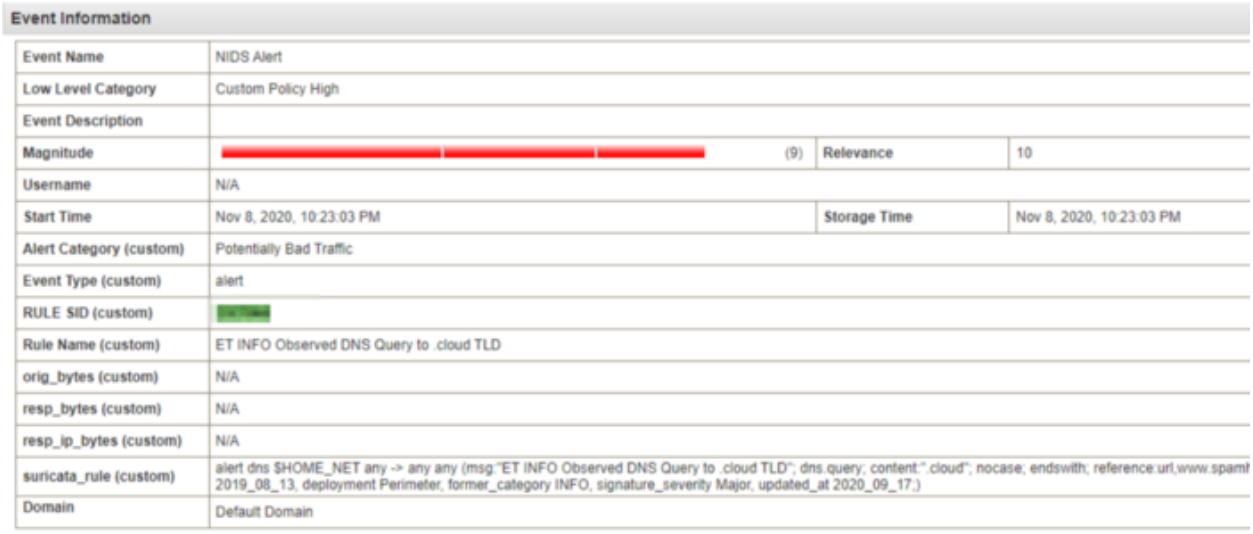

Fig 7— RULE SID

What is the attacker's IP address?

In closed offenses, we can see a suspicious public IP.

Fig 8— Attacker IP

The attacker was searching for data belonging to one of the company's projects, can you find the name of the project?

We can search for project with regular expression.

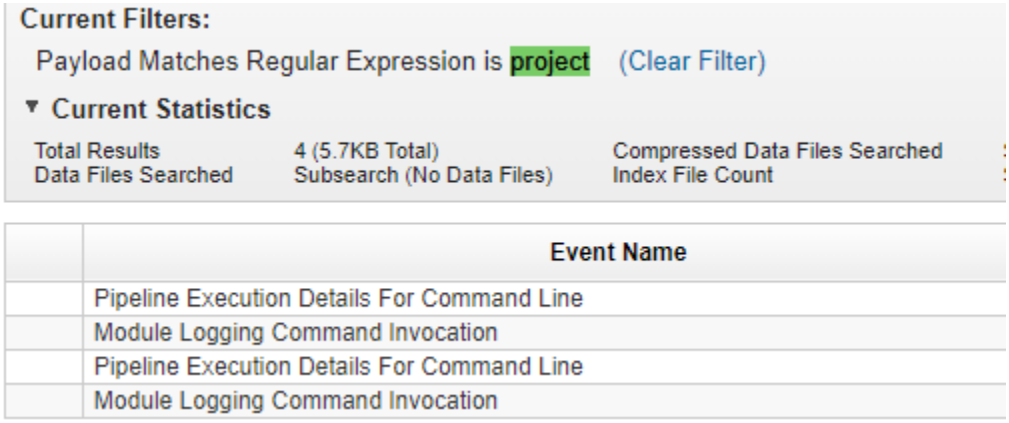

Fig 9—Project

We will find 4 events, then we will read the payload.

Fig 10— Project.xlsx

What is the IP address of the first infected machine?

We can order the events by increasing time. We can see a suspicious event.

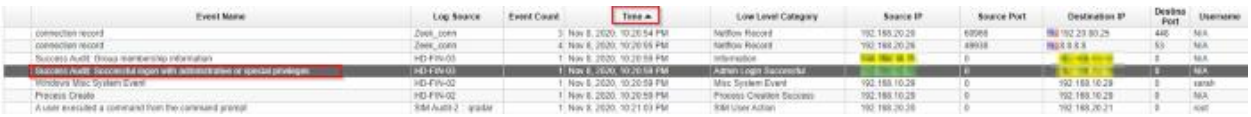

Fig 11 — First Infected

What is the username of the infected employee using 192.168.10.15?

Adding a filter where Source IP is 192.168.10.15 we can find the first username that logged in.

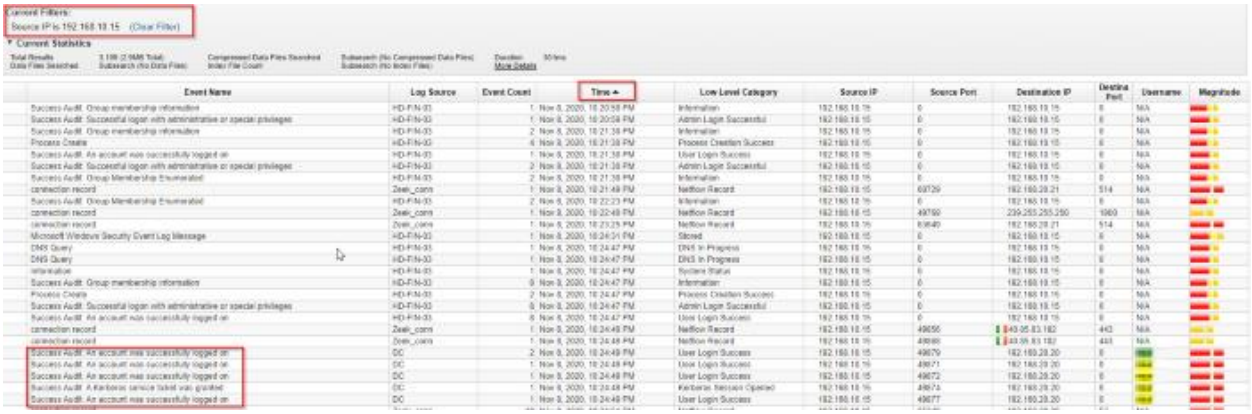

Fig 12 — Infected employee

Hackers do not like logging, what logging was the attacker checking to see if enabled?

Let's look for the first events that the attacker generated. We can observe a tool widely used in attacks.

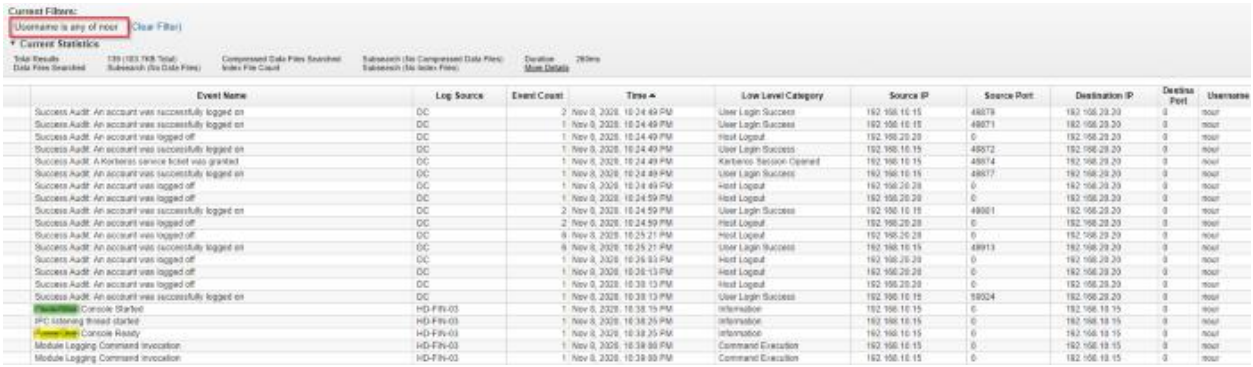

Fig 13— Infected employee

We can also see that the attacker is using PowerShell to find project48.

Name of the second system the attacker targeted to cover up the employee?

We can search for deleted files.

Fig 14— Second System

Fig 15 — Del

When was the first malicious connection to the domain controller (log start time — hh:mm:ss)?

We can look for detected network connections by looking at the payloads, we can see that the first event is for a connection to the attacker's server 192.20.80.25. And by a process that should not be making this connection.

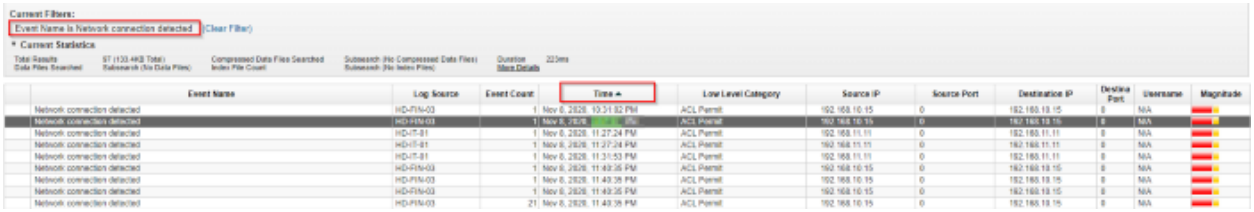

Fig 16 — Connection

What is the md5 hash of the malicious file?

Filtering by hash, we find 10 events, when we look at the first one from the infected machine 192.168.10.15 we can find the .docx file with malicious hash.

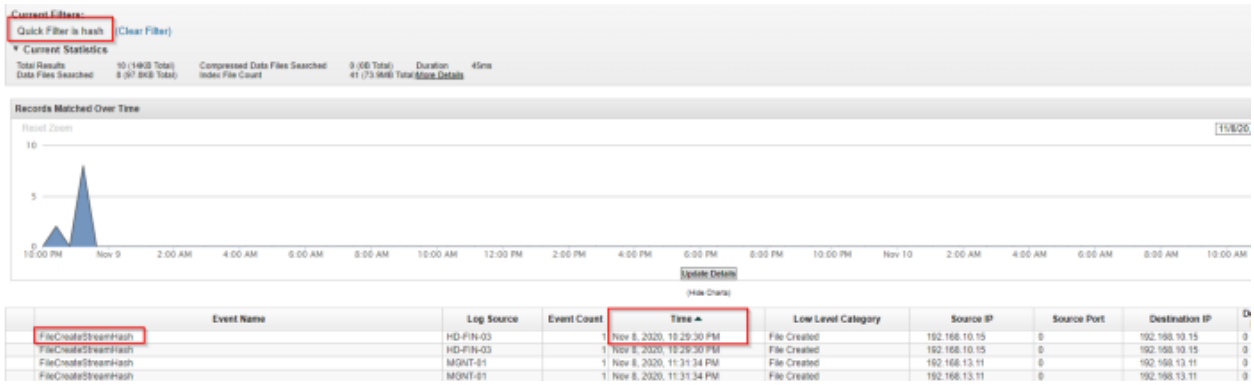

Fig 17 — Hash

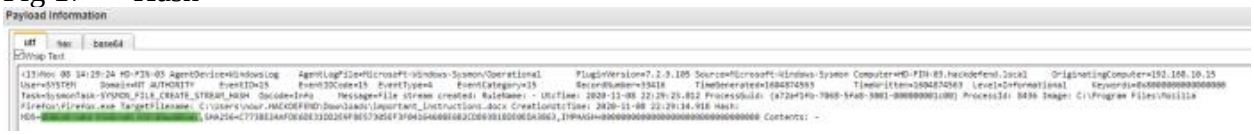

Fig 18 — Hash Payload

What is the MITRE persistence technique ID used by the attacker?

By looking up persistence techniques in ***mitre***, we can search for logs about which techniques the attacker may have used.

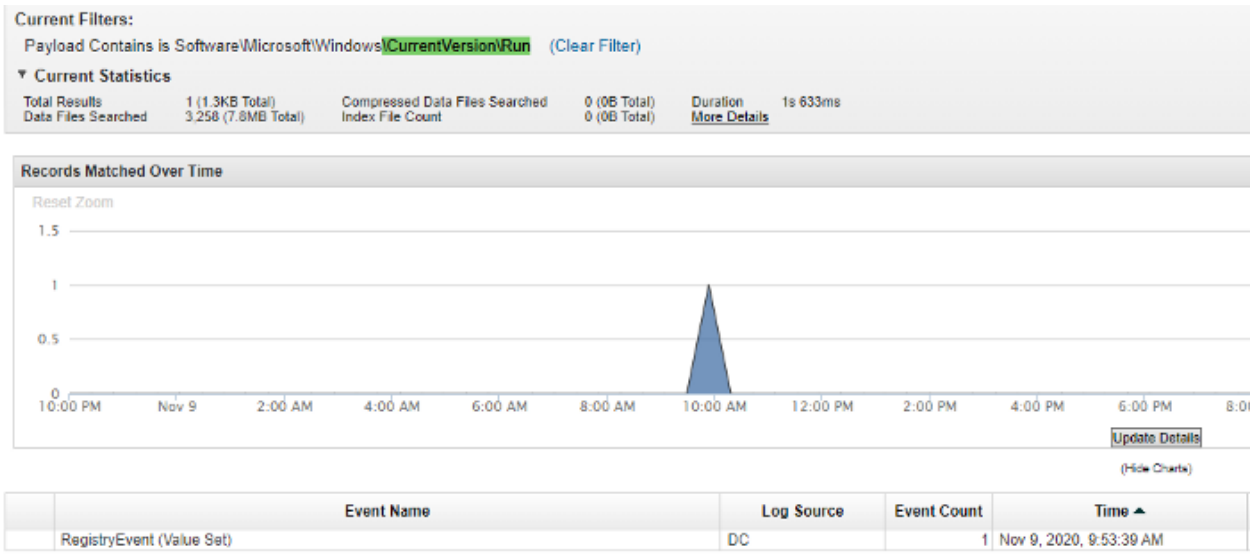

Fig 19 — Run

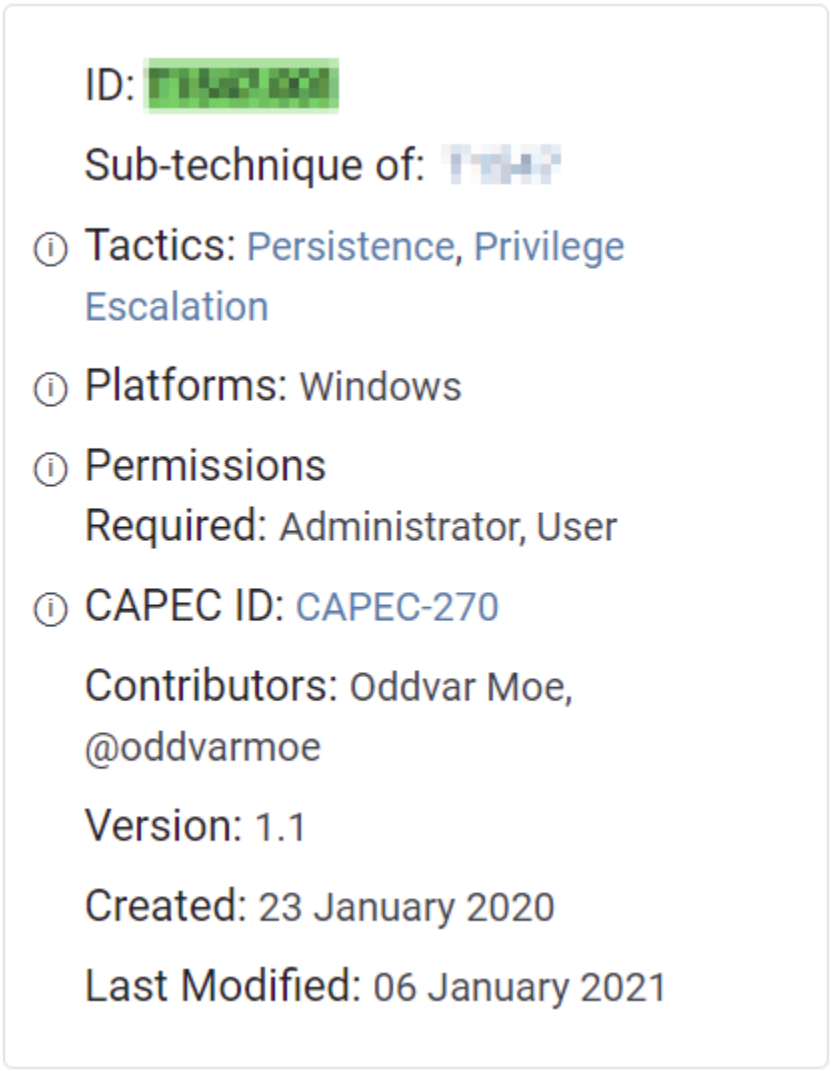

Fig 20— Persistence

What protocol is used to perform host discovery?

We can discover this information by analyzing the outgoing traffic from the first compromised host.

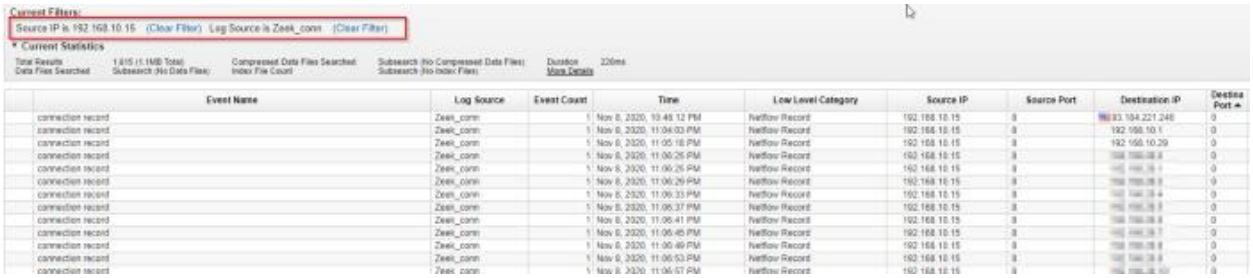

Fig 21— Protocol

Fig 22 — Protocol payload

What is the email service used by the company?(one word)

We can look for traffic directed to the standard ports of the IP's services, in this case, we had no success so let's look at HTTPS traffic port 443 We checked on https://viewdns.inf that most IP's belong to Microsoft and so we found our answer.

What is the name of the malicious file used for the initial infection?

We found the file with the md5 hash.

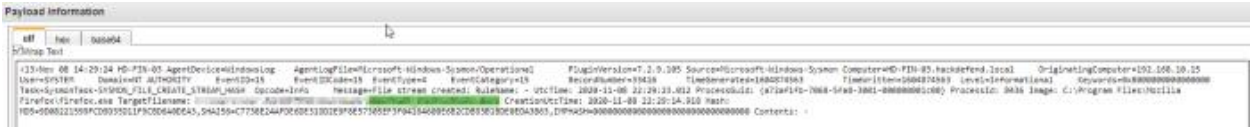

Fig 23 — File

What is the name of the new account added by the attacker?

We can search for Event id 4720 A user account was created.

Windows Security Log Event ID 4720 - A user account was created

4720: A user account was created On this page The user identified by Subject: created the user identified by New…

www.ultimatewindowssecurity.com

Fig 24–4720

Fig 25–4720 payload

What is the PID of the process that performed injection?

We can look for process creation on the infected host.

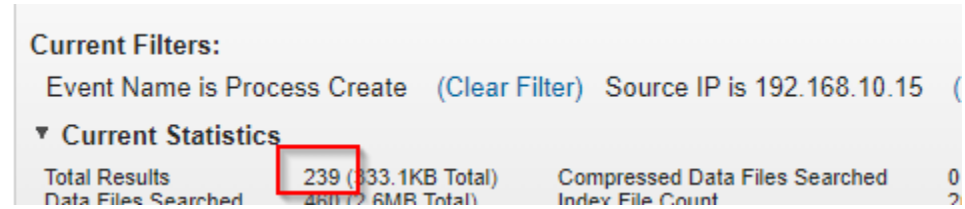

Fig 26— PID filter

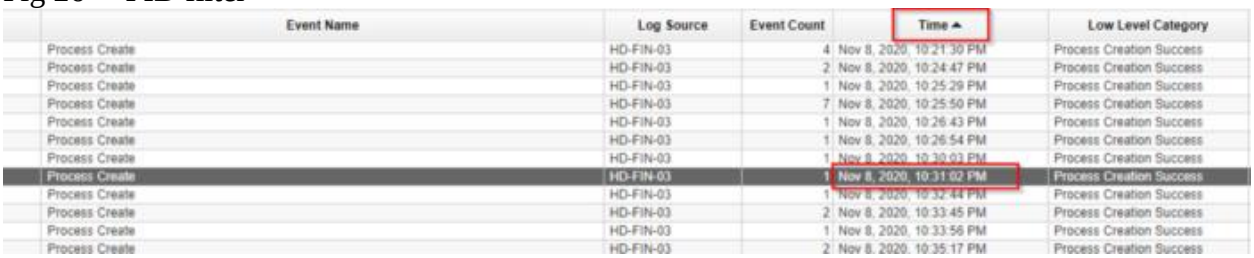

Fig 27 — PID event

Fig 28 — PID payload

What is the name of the tool used for lateral movement?

I didn't know about this tool and couldn't find anything in the logs, I needed to use the tip, so searching on google I found https://github.com/SecureAuthCorp/impacket

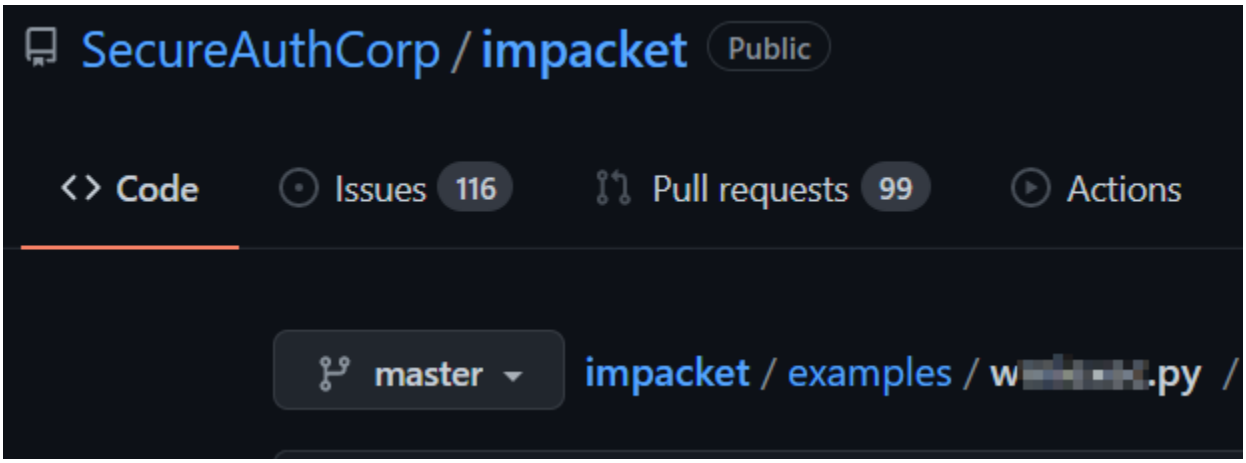

Fig 29 — Impacket

Attacker exfiltrated one file, what is the name of the tool used for exfiltration?

Searching for the events where there was communication with the attacker.

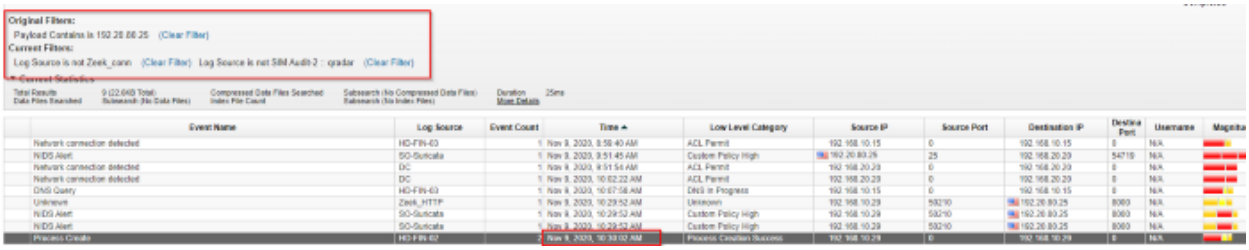
Fig 30— Exfiltration

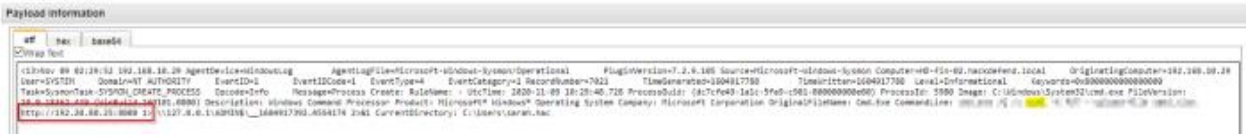
Fig 31— Exfiltration payload

Who is the other legitimate domain admin other than the administrator?

We can see a list of users grouped by username and search for event ***4672*****.**

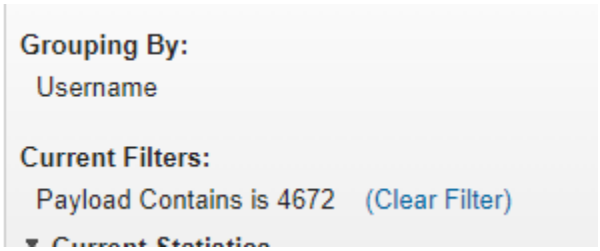

Fig 32–4672

Username	Source IP (Unique Count)
rambo	192.168.20.20
[redacted]	192.168.11.11
admin	Multiple (2)
LOCAL SERVICE	Multiple (5)
[redacted]	Multiple (2)
DWM-1	Multiple (5)
Administrator	Multiple (4)
N/A	Multiple (9)

Displaying 1 to 8 of 8 items (Elapsed time: 0:00:00.148)

Fig 33— Admin

The attacker used the host discovery technique to know how many hosts available in a certain network, what is the network the hacker scanned from the host IP 1 to 30?

We can check if the first compromised machine scanned the network.

Original Filters:

Source IP is 192.168.10.15 (Clear Filter), Log Source is Zeek_conn (Clear Filter)

Current Filters:

Destination Port is 0 (Clear Filter)

Fig 34 — Scan

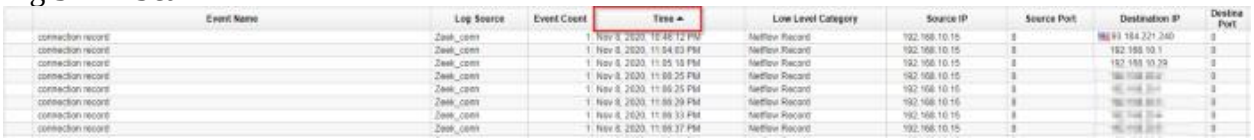

Fig 35 — Scan network

What is the name of the employee who hired the attacker?

While searching for which tool the attacker was performing data exfiltration we noticed a suspicious .xlsx spreadsheet.

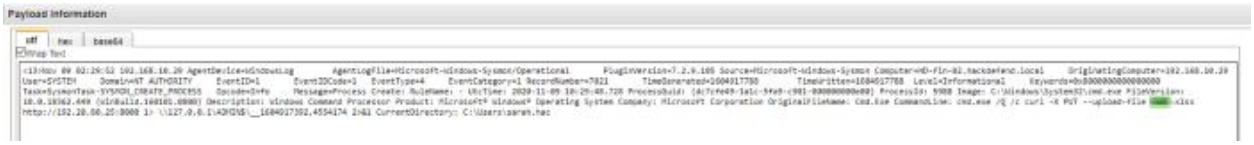

Fig 36 —Employee