

# 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.

Current Search Parameters:  
Exclude Hidden Offenses (Clear Filter)

#	ID	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start Date
1	25	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.11.11	10	192.168.11.11	192.168.11.11	Multiple (2)	Multiple (2)	50	0	Nov 8, 2020, 11
2	25	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.10.15	10	192.168.10.15	192.168.10.15	None	Multiple (2)	97	0	Nov 8, 2020, 10
3	24	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.13.12	10	192.168.13.12	192.168.13.12	Administrator	Multiple (2)	23	0	Nov 8, 2020, 9:2
4	23	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.10.29	10	192.168.10.29	192.168.10.29	Multiple (2)	Multiple (2)	85	0	Nov 8, 2020, 9:1
5	22	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.12.12	10	192.168.12.12	192.168.12.12	None	Multiple (2)	172	0	Nov 8, 2020, 4:2
6	21	Exploit Followed by Suspicious Host Activity - Channel containing Module Logging: Command invocation	Source IP	192.168.20.26	10	192.168.20.26	192.168.20.26	Multiple (2)	Multiple (2)	166	0	Nov 8, 2020, 2:1
7	20	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.11.11	10	192.168.11.11	192.168.11.11	Multiple (2)	Multiple (2)	37	0	Nov 8, 2020, 11
8	19	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.12.11	10	192.168.12.11	192.168.12.11	Multiple (3)	Multiple (2)	267	0	Nov 4, 2020, 11
9	17	Login Failures Followed By Success from the same Username preceded by Multiple Login Failures for the	Username	qradarcollector	10	Multiple (5)	Local (6)	qradarcollector	Multiple (7)	8,441	0	Nov 4, 2020, 11
10	18	Exploit Followed by Suspicious Host Activity - Channel containing Module Logging: Command invocation	Source IP	192.168.20.20	10	192.168.20.20	192.168.20.20	Multiple (4)	Multiple (2)	233	0	Nov 4, 2020, 11
11	18	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.10.15	10	192.168.10.15	192.168.10.15	Multiple (2)	Multiple (2)	112	0	Nov 4, 2020, 9:4
12	15	Multiple Login Failures for the Same User containing Failure Audit: An account failed to log on	Username	Guest	10	192.168.11.11	192.168.11.11	Guest	Multiple (2)	11	0	Nov 4, 2020, 7:3
13	14	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.11.11	10	192.168.11.11	192.168.11.11	Multiple (2)	Multiple (2)	33	0	Nov 4, 2020, 5:1
14	13	Exploit Followed by Suspicious Host Activity - Channel containing Module Logging: Command invocation	Source IP	192.168.20.20	10	192.168.20.20	192.168.20.20	Multiple (4)	Multiple (2)	240	0	Nov 3, 2020, 11
15	12	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.10.15	10	192.168.10.15	192.168.10.15	Multiple (2)	Multiple (2)	180	0	Nov 3, 2020, 10
16	13	General Authentication Successful and Admin Login Successful and User Login Failure and User Login Su	Username	qradarcollector	10	Multiple (4)	Local (4)	qradarcollector	Multiple (4)	9,160	0	Nov 3, 2020, 9:1
17	11	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.11.13	10	192.168.11.13	192.168.11.13	Multiple (5)	Multiple (2)	248	0	Nov 3, 2020, 9:1
18	9	Login Failures Followed By Success from the same Username preceded by Multiple Login Failures for the	Username	qradarcollector	10	Multiple (5)	Local (6)	qradarcollector	Multiple (7)	48,892	0	Nov 3, 2020, 8:1
19	8	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.10.15	10	192.168.10.15	192.168.10.15	Multiple (5)	Multiple (2)	1,421	0	Nov 2, 2020, 8:1
20	7	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.12.12	10	192.168.12.12	192.168.12.12	None	Multiple (2)	5	0	Nov 1, 2020, 4:4
21	8	Exploit Followed by Suspicious Host Activity - Channel containing Success Audit: Successful login with ad...	Source IP	192.168.12.11	10	192.168.12.11	192.168.12.11	Multiple (5)	Multiple (2)	274	0	Oct 28, 2020, 1
22	5	Multiple Login Failures for the Same User containing Failure Audit: An account failed to log on	Username	Guest	10	192.168.10.19	192.168.10.19	Guest	Multiple (2)	15	0	Oct 28, 2020, 2
23	4	Exploit Followed by Suspicious Host Activity - Channel containing Script Block: Executed/Compiled	Source IP	192.168.20.26	10	192.168.20.26	192.168.20.26	Administrator	Multiple (2)	23	0	Oct 27, 2020, 4
24	3	Excessive Firewall Denies Between Hosts containing Firewall - Deny	Source IP	192.20.80.25	10	192.20.80.25	Local (253)	None	Multiple (2)	1,671	0	Oct 23, 2020, 4
25	2	Exploit Followed by Suspicious Host Activity - Channel containing The Group Policy settings for the user u	Source IP	192.168.10.11	10	192.168.10.11	192.168.10.11	Multiple (5)	Multiple (2)	405	0	Oct 18, 2020, 6
26	1	Flow Source/Interface Stopped Sending Flows	Rule	Flow Source Stopper	10	192.168.28.21	192.168.28.21	None	Custom Rule Engine	2	0	Oct 17, 2020, 11

Fig 1 — Offenses

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

Start Time: 11/8/2020 10:00 PM End Time: 11/10/2020 3:00 PM Update

View: Select An Option Display: Default (Normalized) Results Limit: 10

\* Current Statistics

Total Results	72,957 (32.8MB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	436ms
Data Files Searched	3,258 (7.6MB Total)	Index File Count	0 (0B Total)	More Details	

Fig 2— Log Activity

## How many log sources available?

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



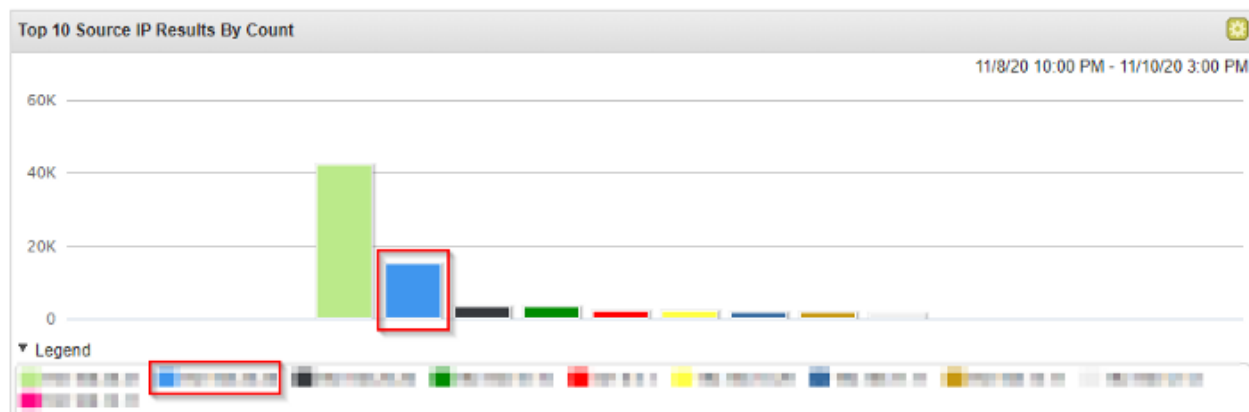


Fig 5 — Ip .20

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

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

Add Filter

Parameter:  Operator:  Value:

Fig 6 — sid

We will find 110 logs from SO-Suricata where 72

Event Information			
Event Name	NIDS Alert		
Low Level Category	Custom Policy High		
Event Description			
Magnitude	<div><div></div></div>		(9) Relevance 10
Username	N/A		
Start Time	Nov 8, 2020, 10:23:03 PM	Storage Time	Nov 8, 2020, 10:23:03 PM
Alert Category (custom)	Potentially Bad Traffic		
Event Type (custom)	alert		
RULE SID (custom)	<div><div></div></div>		
Rule Name (custom)	ET INFO Observed DNS Query to .cloud TLD		
orig_bytes (custom)	N/A		
resp_bytes (custom)	N/A		
resp_ip_bytes (custom)	N/A		
suricata_rule (custom)	alert dns \$HOME_NET any -> any (msg:"ET INFO Observed DNS Query to .cloud TLD"; dns.query; content:".cloud"; nocase; ends with; reference:url,www.spamf2019_08_13_deployment Perimeter, former_category INFO, signature_severity Major, updated_at 2020_09_17.)		
Domain	Default Domain		

Fig 7— RULE SID

**What is the attacker's IP address?**

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



Endpoint Firewall												
Source IP is 192.168.13.15 (Clear Filter)												
Y Current Statistics												
Total Results		3,188 (2,166) Total Subsearch (No Data Files)		Compressed Data Files (Standard Index File Count)		Subsearch (No Compressed Data Files)		Download (No Index Files)		30 Days		
Data Files Selected		Subsearch (No Data Files)				Subsearch (No Index Files)		Download (No Index Files)				
Event Name	Event Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Message	Severity	
Success Audit: Group membership information	FD-HM-FR-03	1	Nov 6, 2020, 12:23:38 PM	Information	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: Successful login with administrative or special privileges	FD-HM-FR-03	1	Nov 6, 2020, 10:20:28 PM	Admin Login Successful	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: Group membership information	FD-HM-FR-03	2	Nov 6, 2020, 12:21:38 PM	Information	192.168.13.15	0	192.168.13.15	0	SA		High	
Process Create	FD-HM-FR-03	6	Nov 6, 2020, 12:21:38 PM	Process Creation Success	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: An account was successfully logged on	FD-HM-FR-03	2	Nov 6, 2020, 12:21:38 PM	User Login Success	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: Successful login with administrative or special privileges	FD-HM-FR-03	2	Nov 6, 2020, 12:21:38 PM	Admin Login Successful	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: Group Membership Enumeration	FD-HM-FR-03	2	Nov 6, 2020, 12:21:38 PM	Information	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: Group Membership Enumeration	FD-HM-FR-03	1	Nov 6, 2020, 12:21:49 PM	Network Scan	192.168.13.15	60726	192.168.20.21	514	SA		High	
Success Audit: Group Membership Enumeration	FD-HM-FR-03	1	Nov 6, 2020, 12:22:23 PM	Information	192.168.13.15	0	192.168.13.15	0	SA		High	
Connection Record	FD-HM-FR-03	1	Nov 6, 2020, 10:22:48 PM	Network Scan	192.168.13.15	48760	239.255.255.250	1600	SA		High	
Connection Record	FD-HM-FR-03	1	Nov 6, 2020, 12:23:38 PM	Network Scan	192.168.13.15	61640	192.168.20.21	514	SA		High	
Microsoft Windows Security Event Log Message	FD-HM-FR-03	1	Nov 6, 2020, 12:24:25 PM	Skipped	192.168.13.15	0	192.168.13.15	0	SA		High	
2545 Query	FD-HM-FR-03	1	Nov 6, 2020, 12:24:47 PM	Disk in Progress	192.168.13.15	0	192.168.13.15	0	SA		High	
2545 Query	FD-HM-FR-03	1	Nov 6, 2020, 12:24:47 PM	Disk in Progress	192.168.13.15	0	192.168.13.15	0	SA		High	
Information	FD-HM-FR-03	1	Nov 6, 2020, 12:24:47 PM	System Status	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: Group membership information	FD-HM-FR-03	1	Nov 6, 2020, 12:24:47 PM	Information	192.168.13.15	0	192.168.13.15	0	SA		High	
Process Create	FD-HM-FR-03	2	Nov 6, 2020, 12:24:47 PM	Process Creation Success	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: Successful login with administrative or special privileges	FD-HM-FR-03	8	Nov 6, 2020, 12:24:47 PM	Admin Login Successful	192.168.13.15	0	192.168.13.15	0	SA		High	
Success Audit: An account was successfully logged on	FD-HM-FR-03	6	Nov 6, 2020, 12:24:47 PM	User Login Success	192.168.13.15	0	192.168.13.15	0	SA		High	
Connection Record	FD-HM-FR-03	1	Nov 6, 2020, 12:24:48 PM	Network Scan	192.168.13.15	49556	192.168.20.21	442	SA		High	
Connection Record	FD-HM-FR-03	1	Nov 6, 2020, 12:24:48 PM	Network Scan	192.168.13.15	49560	192.168.20.21	442	SA		High	
Success Audit: An account was successfully logged on	DC	2	Nov 6, 2020, 12:24:48 PM	User Login Success	192.168.13.15	0	192.168.20.20	0	SA		High	
Success Audit: An account was successfully logged on	DC	2	Nov 6, 2020, 12:24:48 PM	User Login Success	192.168.13.15	0	192.168.20.20	0	SA		High	
Success Audit: An account was successfully logged on	DC	1	Nov 6, 2020, 12:24:48 PM	User Login Success	192.168.13.15	0	192.168.20.20	0	SA		High	
Success Audit: An account was successfully logged on	DC	1	Nov 6, 2020, 12:24:48 PM	User Login Success	192.168.13.15	0	192.168.20.20	0	SA		High	
Success Audit: An account was successfully logged on	DC	1	Nov 6, 2020, 12:24:48 PM	User Login Success	19							

**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.

<b>Current Filter:</b>										
(Username is any of root)	(Clear Filter)									
<b>* Current Statistics</b>										
Total Events	139 (133 FWS Total)		Compressed Data Files Generated	Subsource (No Compressed Data File)		Duration	26mins			
Data Files Generated	Subsource (No Data File)		Index File Count	Subsource (No Subsource File)		Max Size				
Event Name	Log Source	Event Count	Time *	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	
Success Audit: An account was successfully logged on	DC	2	Nov 8, 2020 10:24:40 PM	User Logon Success	192.168.16.15	48878	192.168.29.20	0	nroot	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020 10:24:40 PM	User Logon Success	192.168.29.20	48871	192.168.29.20	0	nroot	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020 10:24:40 PM	Host Logon	192.168.29.20	0	192.168.29.20	0	nroot	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020 10:24:40 PM	User Logon Success	192.168.16.15	48872	192.168.29.20	0	nroot	
Success Audit: A host-based service failed to start	DC	1	Nov 8, 2020 10:24:40 PM	Windows Service Control	192.168.16.15	48874	192.168.29.20	0	nroot	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020 10:24:40 PM	User Logon Success	192.168.16.15	48877	192.168.29.20	0	nroot	
Success Audit: An account was logged off	DC	1	Nov 8, 2020 10:24:40 PM	Host Logout	192.168.29.20	0	192.168.29.20	0	nroot	
Success Audit: An account was logged off	DC	1	Nov 8, 2020 10:24:40 PM	Host Logout	192.168.29.20	0	192.168.29.20	0	nroot	
Success Audit: An account was successfully logged on	DC	2	Nov 8, 2020 10:24:50 PM	User Logon Success	192.168.16.15	48881	192.168.29.20	0	nroot	
Success Audit: An account was logged off	DC	2	Nov 8, 2020 10:24:50 PM	Host Logout	192.168.29.20	0	192.168.29.20	0	nroot	
Success Audit: An account was successfully logged on	DC	8	Nov 8, 2020 10:25:21 PM	User Logon Success	192.168.29.20	0	192.168.29.20	0	nroot	
Success Audit: An account was successfully logged on	DC	8	Nov 8, 2020 10:25:21 PM	User Logon Success	192.168.16.15	48813	192.168.29.20	0	nroot	
Success Audit: An account was logged off	DC	1	Nov 8, 2020 10:26:43 PM	Host Logout	192.168.29.20	0	192.168.29.20	0	nroot	
Success Audit: An account was logged off	DC	1	Nov 8, 2020 10:26:43 PM	Host Logout	192.168.29.20	0	192.168.29.20	0	nroot	
Success Audit: An account was logged off	DC	1	Nov 8, 2020 10:33:13 PM	Host Logout	192.168.29.20	0	192.168.29.20	0	nroot	
Success Audit: An account was successfully logged on	DC	1	Nov 8, 2020 10:33:13 PM	User Logon Success	192.168.16.15	19324	192.168.29.20	0	nroot	
Microsoft Windows Started	HD-PHV-03	1	Nov 8, 2020 10:38:15 PM	Information	192.168.16.15	0	192.168.16.15	0	nroot	
SFC scanning finished started	HD-PHV-03	1	Nov 8, 2020 10:38:25 PM	Information	192.168.16.15	0	192.168.16.15	0	nroot	
Mediafire Console Ready	HD-PHV-03	1	Nov 8, 2020 10:38:25 PM	Information	192.168.16.15	0	192.168.16.15	0	nroot	
Medium Logging Command Invocation	HD-PHV-03	1	Nov 8, 2020 10:38:30 PM	Command Execution	192.168.16.15	0	192.168.16.15	0	nroot	
Medium Logging Command Invocation	HD-PHV-03	1	Nov 8, 2020 10:38:30 PM	Command Execution	192.168.16.15	0	192.168.16.15	0	nroot	

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.

**Current Filters:**

Quick Filter is del (Clear Filter)

**Current Statistics**

Total Results 2 (2.8KB Total)

**Fig 14— Second System**

The screenshot displays the 'Payload Information' tab for a specific system. The main area contains a table of events with columns for ID, Name, Type, Category, Record Number, Time Generated, Time Received, Level, Info, Remarks, and Keywords. The first event is highlighted, showing details such as AgentID=0000000000000000, EventID=0000000000000000, EventType=0000000000000000, and Description: Windows Command Processor Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFilename: cmd.exe CommandLine: cmd.exe /q /c del \*.txt

By looking up persistence techniques in [mitre](#), we can search for logs about which techniques the attacker may have used.

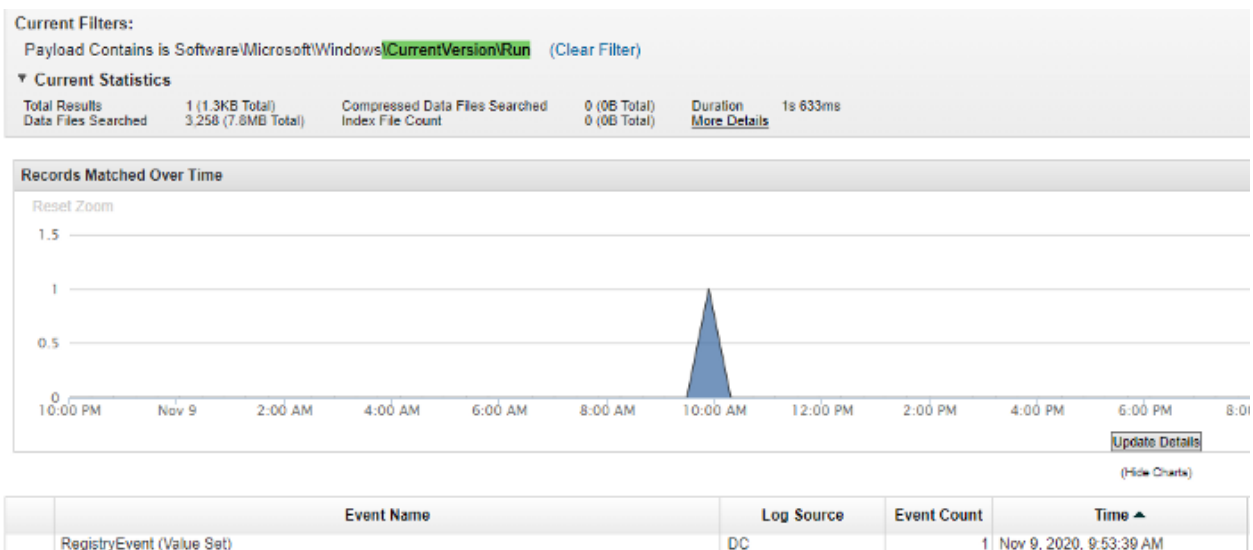


Fig 19 — Run

ID: T1562.004

Sub-technique of: T1487

*i* **Tactics:** Persistence, Privilege Escalation

*i* **Platforms:** Windows

*i* **Permissions**  
Required: Administrator, User

*i* **CAPEC ID:** CAPEC-270

Contributors: Oddvar Moe,  
@oddvarmoe

Version: 1.1

Created: 23 January 2020

Last Modified: 06 January 2021

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.

Current Filters:

Source IP is 192.168.10.15 (Clear Filter) Log Source is Zeek\_conn (Clear Filter)

Current Statistics

Total Results	1,615 (1 MB Total)	Compressed Data File Searched	Subsearch (No Compressed Data Files)	Duration	20ms
Data File Searched	Subsearch (No Data File)	Index File Count	Subsearch (No Index File)	Match Status	

Event Name	Log Source	Event Count	Time	Low-Level Category	Source IP	Source Port	Destination IP	Destination Port
connection record	Zeek_conn	1	Nov 8, 2020, 10:48:12 PM	Network Record	192.168.10.15	0	192.168.221.248	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:04:03 PM	Network Record	192.168.10.15	0	192.168.10.1	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:05:18 PM	Network Record	192.168.10.15	0	192.168.10.209	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:25 PM	Network Record	192.168.10.15	0	192.168.10.8	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:25 PM	Network Record	192.168.10.15	0	192.168.10.8	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:26 PM	Network Record	192.168.10.15	0	192.168.10.16	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:33 PM	Network Record	192.168.10.15	0	192.168.10.8	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:37 PM	Network Record	192.168.10.15	0	192.168.10.8	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:41 PM	Network Record	192.168.10.15	0	192.168.10.8	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:45 PM	Network Record	192.168.10.15	0	192.168.10.8	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:49 PM	Network Record	192.168.10.15	0	192.168.10.8	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:53 PM	Network Record	192.168.10.15	0	192.168.10.8	0
connection record	Zeek_conn	1	Nov 8, 2020, 11:06:57 PM	Network Record	192.168.10.15	0	192.168.10.8	0

### Fig 21—Protocol

**Payload information**

att: true, name: name04

Wrap text

```
{(3)ver:08,20:13:06,13:06,28,26,C0G5TASH;[{"2020-11-08T20:13:06.795Z","H00micr":{"ts":"2020-11-08T20:13:06.490456Z","c":"C0P0K0X0Y0","l":"152.168.10.15","id_resp_0":"152.168.10.1","id_resp_1":"","proto":,"duration":0.00021902774056303,"orig_bytes":32,"resp_bytes":32,"conn_state":"OTH","local_orig":true,"local_resp":true,"missed_bytes":0,"orig_pkts":1,"orig_ip_bytes":80,"resp_pkts":1,"resp_ip_bytes":68,"community_id":""}]}#E9D900X0p+IdkQ0R0nd=}
```

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.info> 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.

[illegible]

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...**





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.

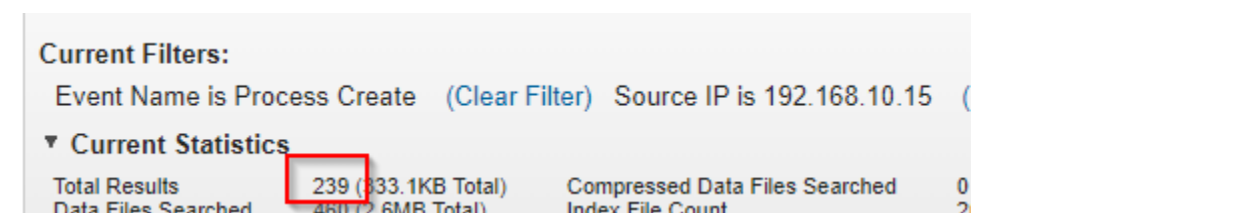


Fig 26—PID filter

Event Name	Log Source	Event Count	Time	Low Level Category
Process Create	HD-FIN-03	4	Nov 8, 2020, 10:21:30 PM	Process Creation Success
Process Create	HD-FIN-03	2	Nov 8, 2020, 10:24:47 PM	Process Creation Success
Process Create	HD-FIN-03	1	Nov 8, 2020, 10:25:29 PM	Process Creation Success
Process Create	HD-FIN-03	7	Nov 8, 2020, 10:25:50 PM	Process Creation Success
Process Create	HD-FIN-03	1	Nov 8, 2020, 10:26:43 PM	Process Creation Success
Process Create	HD-FIN-03	1	Nov 8, 2020, 10:26:54 PM	Process Creation Success
Process Create	HD-FIN-03	1	Nov 8, 2020, 10:30:03 PM	Process Creation Success
Process Create	HD-FIN-03	1	Nov 8, 2020, 10:31:02 PM	Process Creation Success
Process Create	HD-FIN-03	1	Nov 8, 2020, 10:32:44 PM	Process Creation Success
Process Create	HD-FIN-03	2	Nov 8, 2020, 10:33:45 PM	Process Creation Success
Process Create	HD-FIN-03	1	Nov 8, 2020, 10:33:56 PM	Process Creation Success
Process Create	HD-FIN-03	2	Nov 8, 2020, 10:35:17 PM	Process Creation Success

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>



