CyberDefenders: PhishStrike Lab

The following writeup is for PhishStrike Lab on CyberDefenders, it involves analysing a phishing email using a series of tools, including VirusTotal, Sublime Text, URLHaus, Hybrid Analysis, and more. This lab is not necessarily difficult; it just involves a lot of rabbit holes to find what you are looking for. Keep in mind that this is a threat intelligence-based lab, whereby you will need to utilise a series of threat intelligence tools in order to find the answer.

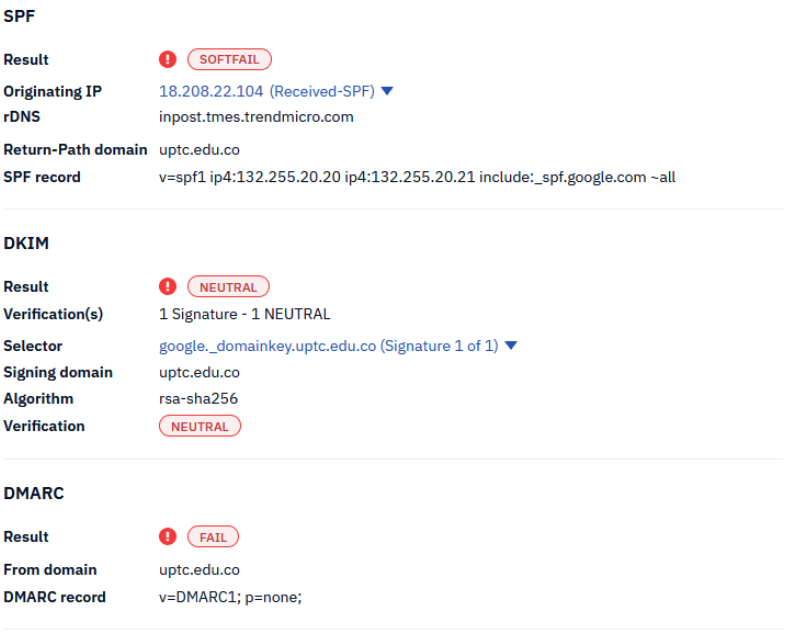
Scenario: As a cybersecurity analyst at an educational institution, you receive an alert about a phishing email targeting faculty members. The email appears to be from a trusted contact and claims a $625,000 purchase, providing a link to download an invoice.
Your task is to investigate the email using Threat Intel tools. Analyze the email headers and inspect the link for malicious content. Identify any Indicators of Compromise (IOCs) and document your findings to prevent potential fraud and educate faculty on phishing recognition.

Identifying the sender's IP address with specific SPF and DKIM values helps trace the source of the phishing email. What is the sender's IP address that has an SPF value of softfail and a DKIM value of fail?

When analysing emails manually, I enjoy using sublime text with the email header syntax created by 13Cubed.

```
Authentication-Results: spf=softfail (sender IP is 18.208.22.104)
 smtp.mailfrom=uptc.edu.co; dkim=fail (no key for signature)
 header.d=uptc.edu.co;dmarc=none action=none
 header.from=uptc.edu.co;compauth=softpass reason=201
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 uptc.edu.co discourages use of 18.208.22.104 as permitted sender)
```

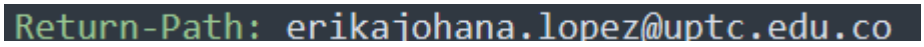
Alternatively, you can create a free account with PhishTool, which is an incredible email analysis tool that does all the heavy lifting for you:



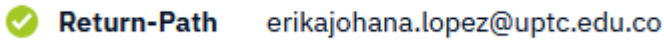
Answer: 18.208.22.104

Understanding the return path of an email is essential for tracing its origin. What is the return path specified in this email?

The return path is an email header that tells the SMTP server where bounced emails should be sent. You can find this manually:



Or by using PhishTool:



Answer: erikajohana.lopez@uptc.edu.co

Identifying the source of malware is critical for effective threat mitigation and response. What is the IP address of the server hosting the malicious file related to malware distribution?

This question is simply referring to the URL contained within the email that points to the URI loader/install.exe:

```
--------_=_NextPart_001_98774E78.6EF8C317
Content-Type: text/plain;
    charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

COMMERCIAL PURCHASE RECEIPT

Your purchase Ref. 00034959 for the amount of $625

VIEW INVOICE DOCUMENT HERE
<http://107.175.247.199/loader/install.exe>
ACCESS CODE: 8657

Erika Johana López Valiente
Magister in Education, Research Mode.
LEB Teacher - FESAD.
```

You can also see this URL under the Message URLs tab in PhishTool:

IP	107.175.247.199
Path	/loader/install.exe
Scheme	HTTP
Port	80

Answer: 107.175.247.199

Identifying malware that exploits system resources for cryptocurrency mining is critical for prioritizing threat mitigation efforts. The malicious URL can deliver several malware types. Which malware family is responsible for cryptocurrency mining?

I first tried to determine the malware family by searching for the IP on VirusTotal and Cisco Talos, although this didn't result in anything of use. Based on the hint, I then used URLhaus, which is a platform from abuse.ch and Spamhaus that shares malicious URLs being used for malware distribution. It enables you to search the database like as follows:

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2025-04-04 08:59:32	http://107.175.247.199//loader//install.exe	Offline		kynhvc
2022-10-22 12:39:04	http://107.175.247.199/loader/install.exe	Offline	AsyncRAT bitrat CoinMiner	abuse_ch
2022-10-22 06:36:06	http://107.175.247.199/loader/Rckjlz.exe	Offline	exe PureCrypter	abuse_ch
2022-10-22 06:35:08	http://107.175.247.199/loader/server.exe	Offline	bitrat exe	abuse_ch

As you can see, this URL is associated/tagged with CoinMiner.

Answer: CoinMiner

Identifying the specific URLs malware requests is key to disrupting its communication channels and reducing its impact. Based on the previous analysis of the cryptocurrency malware sample, what does this malware request the URL?

If you click on the Malware URL that is given the CoinMiner tag on URLHaus, you will be provided with more information about the entry, along with payloads that URLhaus has retrieved from this URL:

Firstseen	Filename	File Type	Payload (SHA256)	VT	Bazaar	Signature
2022-10-26	n/a	exe	bf7628695c2df7a3020034a065397592a1f8850e59f9a448b555bc1c8c639539	n/a		BitRAT
2022-10-25	n/a	exe	5ca468704e7ccb8e1b37c0f7595c54df4e2f4035345b6e442e8bd4e11c58f791	n/a		AsyncRAT
2022-10-22	n/a	exe	453fb1c4b3b48361fa8a67dcedf1eaec39449cb5a146a7770c63d1dc0d7562f0	n/a		CoinMiner

We are concerned with the SHA256 hash of the payload that has the CoinMiner signature. If you chuck this hash into VirusTotal and go to the Relations tabs, you can see that it has contacted two URLs:

Contacted URLs (2)

Scanned	Detections	Status	URL
2025-04-08	11 / 97	-	http://ripley.studio/loader/uploads/Qanjttrbv.jpeg
2025-01-23	9 / 96	200	http://107.175.247.199/loader/server.exe

Answer: http://ripley.studio/loader/uploads/Qanjttrbv.jpeg

Understanding the registry entries added to the auto-run key by malware is crucial for identifying its persistence mechanisms. Based on the BitRAT malware sample analysis, what is the executable's name in the first value added to the registry auto-run key?

Following the same process as the previous question, we can see that the binary does create a Run key for persistence:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Jzwvix
```

You can find this in the Behaviour tab under the Registry Keys Set heading.

Answer: Jzwvix.exe

Identifying the SHA-256 hash of files downloaded from a malicious URL is essential for tracking and analyzing malware activity. Based on the BitRAT analysis, what is the SHA-256 hash of the file previously downloaded and added to the autorun keys?

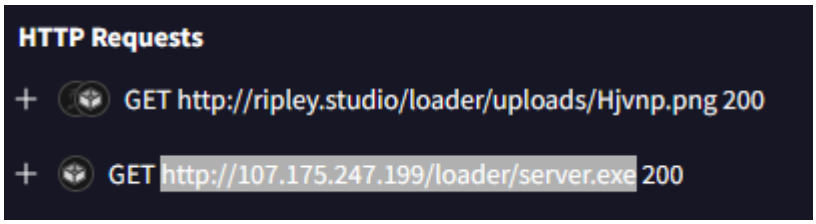
I was able to find the SHA256 hash of the Jzwvix.exe binary by taking a look at one of the report URLs given in the community section on VirutsTotal.

Also Known As	C:\Users\RDhJ0CNFevzX\AppData\Roaming\Ozndcoodb\Jzwvix.exe (Accessed File, Dropped File)
MIME Type	application/vnd.microsoft.portable-executable
File Size	24.00 KB
MD5	86c57967785fe8dbcdf209fb564f9a85
SHA1	c388ca38a675e0709f3d62ae985d6b74f195123f
SHA256	bf7628695c2df7a3020034a065397592a1f8850e59f9a448b555bc1c8c639539
SSDeep	384:V2PLnw7jjye7nw60flGC4600dc+kMEe5QRBCslwSbmy/uLPxBnptYcFmVc03K:8wueTwpMdnWHbbmv7ptYcFmVc6K
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744

Answer: bf7628695c2df7a3020034a065397592a1f8850e59f9a448b555bc1c8c639539

Analyzing the HTTP requests made by malware helps in identifying its communication patterns. What is the URL in the HTTP request used by the loader to retrieve the BitRAT malware?

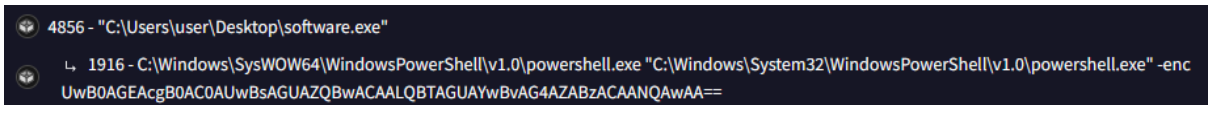
First, we need to take the hash from the previous question and enter that into VirusTotal. You can then navigate to the Behaviour tab and look at the HTTP Requests:



Answer: http://107.175.247.199/loader/server.exe

Introducing a delay in malware execution can help evade detection mechanisms. What is the delay (in seconds) caused by the PowerShell command according to the BitRAT analysis?

Using the same hash as the previous question, navigate to Behaviour > Process Tree section. Here we can see an encoded PowerShell command that is spawned from the server.exe file (BitRAT malware):



You can decode this base64 string in many ways, I chose to do it through the terminal:

```
timba@TimsPC:/mnt/c/Windows/system32$ echo "UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAwAA==" | base64 -d; echo
Start-Sleep -Seconds 50
```

As you can see, it sleeps for 50 seconds.

Answer: 50

Tracking the command and control (C2) domains used by malware is essential for detecting and blocking malicious activities. What is the C2 domain used by the BitRAT malware?

If you check out the Community tab in VirusTotal, we can find the C2 domain:

Answer: gh9st.mywire.org

Understanding how malware exfiltrates data is essential for detecting and preventing data breaches. According to the AsyncRAT analysis, what is the Telegram Bot ID used by this malware?

Similar to one of the previous questions, seeing as we don't have the malware sample handy, we need to look at sandbox reports from other users. You can often find links to these reports in the Community tab. In my case, I used the following report:

- https://tria.ge/221025-m4mhxscdep/behavioral2

Within this report is a Network section that contains the network requests that were made by the sample:

DNS	api.telegram.org	
GET	https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offset=-5	
GET	https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offset=-5	
GET	https://api.telegram.org/bot5610920260:AAHF8huJMzSwUso7E5WSzQW0Bzo4GdubP4k/getUpdates?offset=-5	

Here you can find the Telegram Bot ID used by this malware sample.

Answer: bot5610920260