Author: Jack Fitzgerald


# Official Incident Report

**Date:** Mar, 13, 2025, 09:44 AM

**Event ID:** 316

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

# Table of Contents

# Alert Details

**Severity:** Critical

**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.

Based on the information provided in the alert, it appears that a **phishing email** containing malware was sent to a LetsDefend user. The alert is triggered by rule SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing.

Overall, it appears that the alert may be **suspicious**, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

# Detection

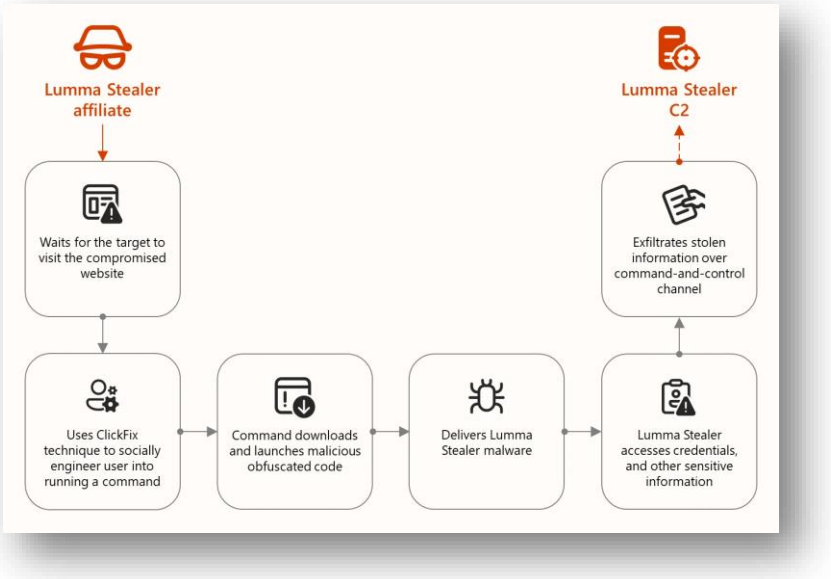
## Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to investigate the Lumma Stealer distribution.

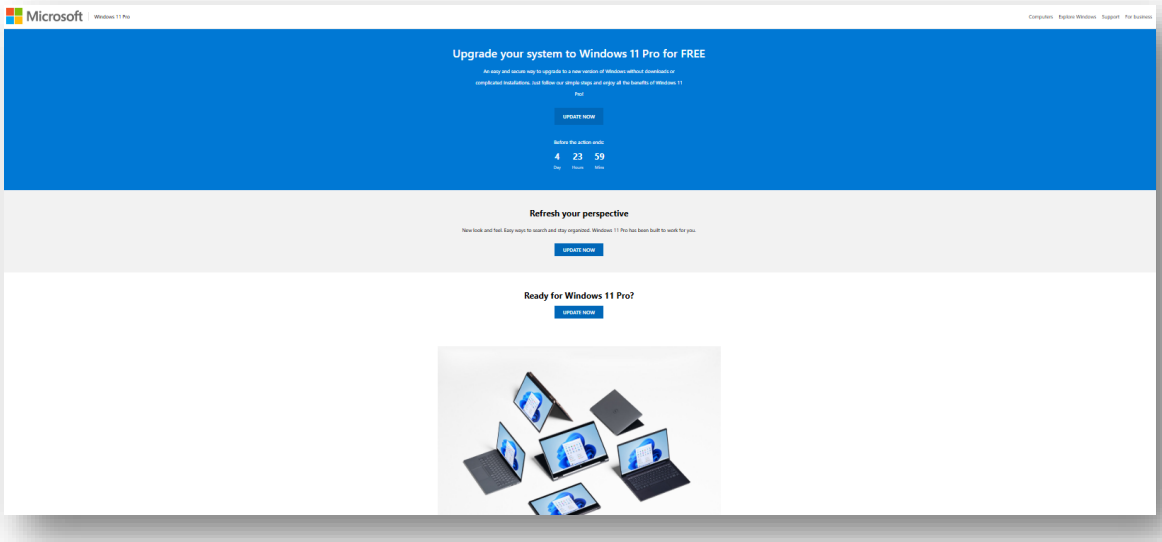
According to Microsoft's Security Blog, Lumma Stealer (also known as LummaC2) is a malware as a service (MaaS) offering that is capable of stealing data from various browsers and applications such as cryptocurrency wallets and installing other malware.

Lumma Stealer emails impersonate known brands and services to deliver links or attachments. The emails lead victims to cloned websites or malicious servers that deploy the Lumma payload to the targets' environment.

A particularly deceptive method involves fake CAPTCHA pages, commonly observed in the ClickFix ecosystem. Targets are instructed to copy malicious commands into their system's Run utility under the pretense of passing a verification check. These commands often download and execute Lumma directly in memory, using Base64 encoding and stealthy delivery chains.



The next step is to identify the email that was sent from **update@windows-update.site** to **dylan@letsdefend.io**.



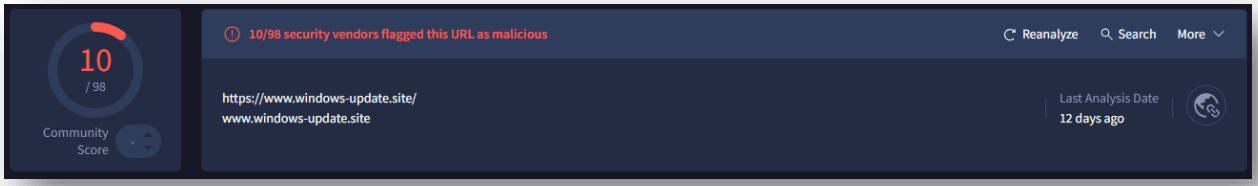

The identified email contains a legitimate-looking Microsoft page with links to upgrade to **Windows 11 Pro for FREE**. This combined with the **countdown of 5 days** creates a sense of **urgency for the user**, a key indicator of phishing emails.

The ‘UPDATE NOW’ buttons redirect the user to **https://www.windows-update.site/**. This site acts as an impersonating site for Microsoft’s Windows updater.

# Analysis

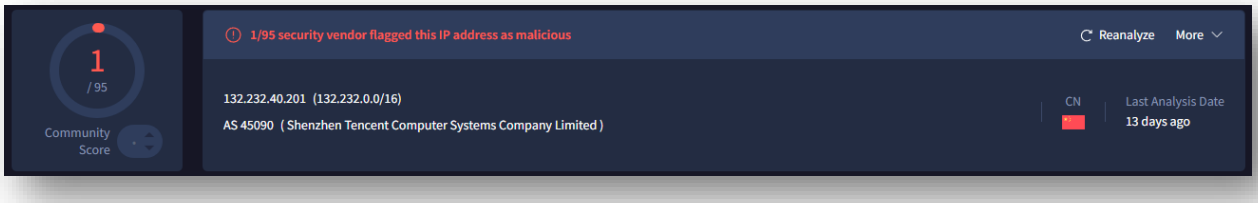
Now that we have detected the alert and its details, we can start by analyzing the URL found in the email.

https://www.virustotal.com/gui/url/278608290e63c5aedbc707bf513ae455300d26da180a329a9cc88798f43454d9

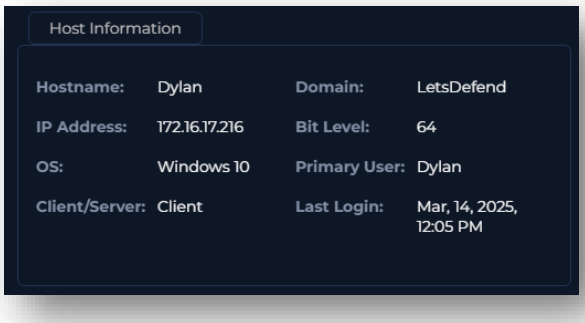



Next, we should analyse the SMTP address 132.232.40.201 that the email was sent from.

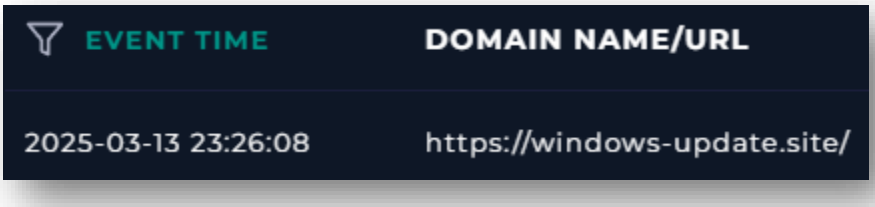
https://www.virustotal.com/gui/ip-address/132.232.40.201



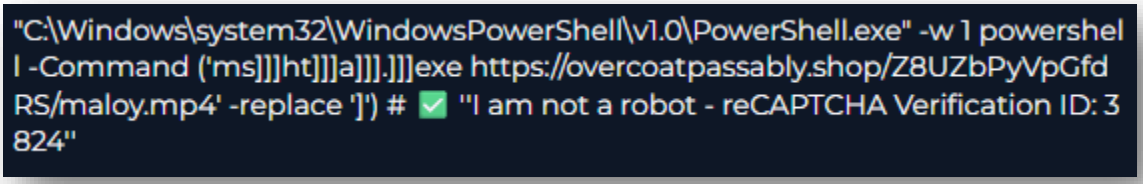

These analyses show indicators of malicious intent; therefore, we will investigate Endpoint Security of Dylan for further information.



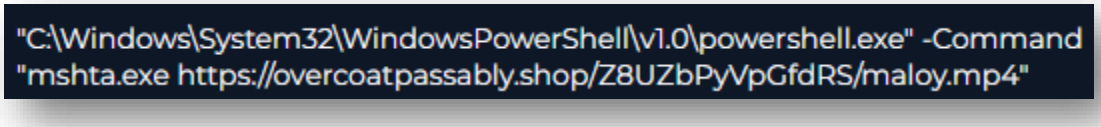
Investigating Dylan's Browser History shows access to **https://windows-update.site/** on the date of the alert.




Investigating Dylan's Terminal History shows indicators of compromise following the Lumma Stealer distribution behaviour. Specifically, identifying that Dylan fell victim to fake CAPTCHA pages, where the user was **instructed to copy malicious commands into their system's Run utility under the pretense of passing a verification check**. These commands often download and execute Lumma directly in memory, using Base64 encoding and stealthy delivery chains.

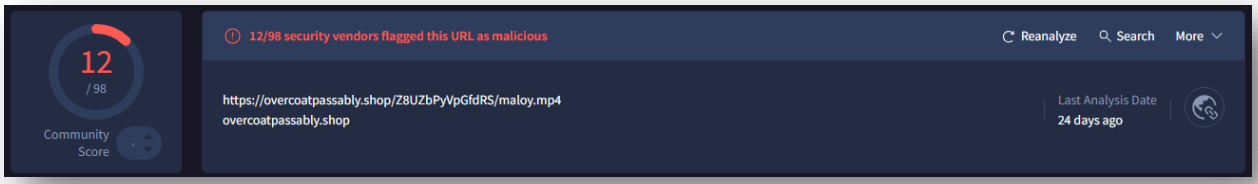



Copying these malicious commands from the websites fake CAPTCHA resulted in using **mshta.exe** to launch **maloy.mp4**.




Investigating the website **https://overcoastpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4** found that it was malicious.

https://www.virustotal.com/gui/url/4167df1da641f6816c4c880e32fa28e169fed728b8e310a0517dd73316b223e5




After investigating Dylan's machine Processes, we found the MD5 hash

**fa93130bcd584f7349fb6399b2092b0f** for maloy.mp4.

We found a previous analysis performed on the maloy.mp4 file hash.

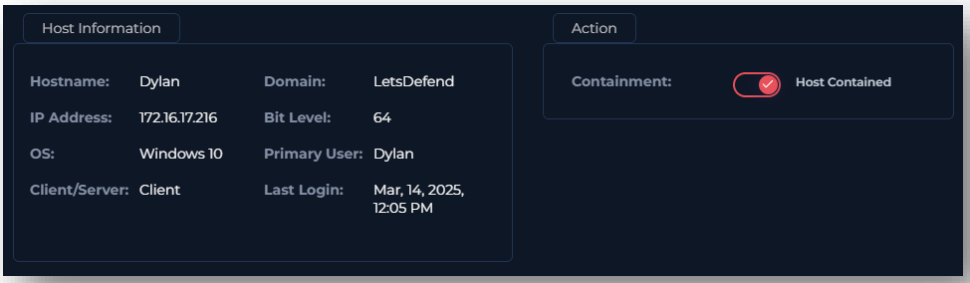
https://hybrid-analysis.com/sample/15c80b5be235bf2a8c38291eb697a702c07dde087eb459e9ea46a2bee17c5f03/67dfd9cc239b6ef9880498ce

Next, we will investigate Log Management to find any further details of the alert. There were 14 events (before Mar, 13, 2025, 11:26 PM UTC), with 2 events that were related to this incident.

These events showcased Dylan clicking on the link from the malicious email, redirecting the user to https://windows-update.site/ with IP **132.232.40.201** and https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4 with IP **172.67.139.19**.

# Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



# Summary

The incident involves a compromised system named **Dylan** with an IP address of **172.16.17.216**. The alert was triggered by the identification of a click fix phishing email containing malware following the behaviour of the Lumma Stealer distribution, based on the rule SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing.

The identified email contained a legitimate-looking Microsoft page with links to upgrade to **Windows 11 Pro for FREE**. This combined with the **countdown of 5 days** creates a sense of **urgency for the user**, a key indicator of phishing emails.

The 'UPDATE NOW' buttons redirect the user to **https://www.windows-update.site/**. This site acts as an impersonating site for Microsoft's Windows updater.

Investigating Dylan's Terminal History shows indicators of compromise following the Lumma Stealer distribution behaviour. Specifically, identifying that Dylan fell victim to fake CAPTCHA pages, where the user was **instructed to copy malicious commands into their system's Run utility under the pretense of passing a verification check**. These commands often download and execute Lumma directly in memory, using Base64 encoding and stealthy delivery chains.

Copying these malicious commands from the websites fake CAPTCHA resulted in using **mshta.exe** to launch **maloy.mp4**.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

## Lessons Learned

- The ‘ClickFix’ social engineering technique, often combined with DLL side-loading, relies heavily on user manipulation to bypass traditional security controls
- Human behavior is the primary vulnerability in this attack chain, necessitating a multi-layered defense strategy focused on user education and endpoint security controls
- Threat actors impersonate legitimate brands to reduce suspicion and increase the likelihood of compliance

## Remediation Actions

- Require multifactor authentication (MFA)
- Leverage phishing-resistant authentication methods such as FIDO Tokens
- Enable Local Security Authority (LSA) protection to block credential stealing from the Windows local security authority subsystem

# Appendix

## MITRE ATT&CK

| MITRE Tactics | MITRE Techniques |
|---|---|
| Initial Access | T1566.002 - Phishing: Spearphishing Link |
| Execution | T1059.001 - Command and Scripting Interpreter: PowerShell |
| Execution | T1204.004 - User Execution: Malicious Copy and Paste |
| Defense Evasion | T1656 - Impersonation |
| Defense Evasion | T1027 - Obfuscated Files or Information |

## Artifacts

| Value | Comment | Type |
|---|---|---|
| https://windows-update.site/ | Lumma Stealer IoC email link | URL Address |
| https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4 | Redirected link from windows-update | URL Address |
| update@windows-update.site | Email sender | E-mail Sender |
| windows-update.site | Illegitimate Microsoft domain | E-mail Domain |
| 132.232.40.201 | SMTP Address | IP Address |
| 172.67.139.19 | https://overcoatpassably.shop/ | IP Address |
| fa93130bcd584f7349fb6399b2092b0f | maloy.mp4 | MD5 Hash |

## LetsDefend Playbook

LetsDefend Event ID: 316