### **SOC338 — Lumma Stealer — DLL Side-Loading via Click Fix Phishing**

### **Event Summary**

**Alert ID —**SOC338

**Event ID —**316

**Detection Rule —**Lumma Stealer — DLL Side-Loading via Click Fix Phishing

**Event Time (UTC) —**2025–05–21 06:33:00

**Source Email —**update@windows-update.site

**Target Email —**dylan@letsdefend.io

**Email Subject —**Upgrade your system to Windows 11 Pro for FREE

**Device Action —**Allowed (Email delivered)

**Trigger Reason —**Redirected site contains a click-fix script used in Lumma Stealer delivery

### **Threat Intelligence**

**Threat Name —**Lumma Stealer

**Category —** Info stealer

**First Seen —**August 2022

**Written In —**C Language

**Delivery Model —**Malware-as-a-Service (MaaS) on Russian forums

#### **Tactics Used by Lumma Stealer:**

* Phishing emails
* Drive-by downloads (posing as browser updates)
* Fake CAPTCHA pages
* Masquerading as AI tools or software

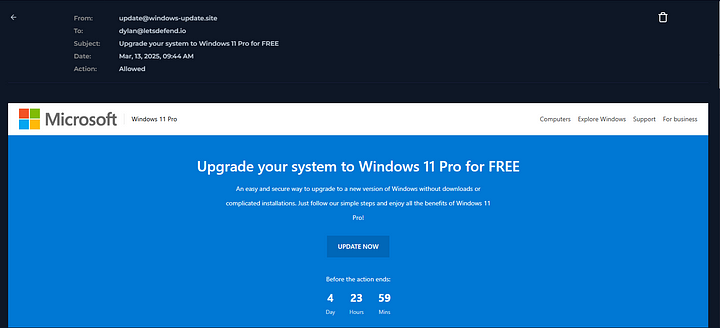
#### **Common Loaders Used:**

* ArechClient2 / SectopRAT
* Emmenhtal
* SmartLoader
* HijackLoader / IDAT Loader

**Source:** Malpedia — Lumma Stealer

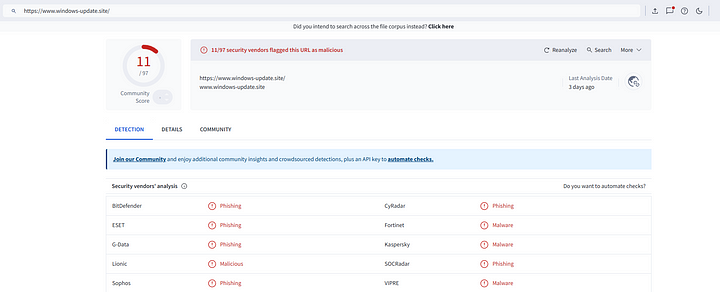
### **Initial Triage and Analysis**

#### **Email Analysis:**

****

* The phishing email impersonated a legitimate Windows Update notification.
* Included urgency via a visual **countdown timer** and social engineering to trick the user into clicking.
* Contained a **malicious link** redirecting to a **click-fix style loader site**.

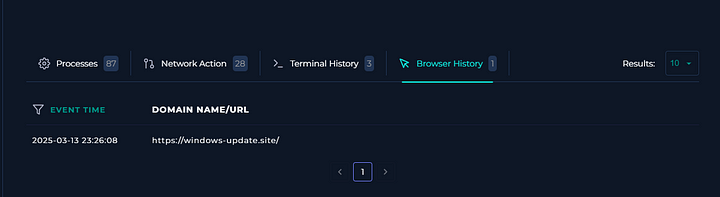
#### **URL Analysis:**

****

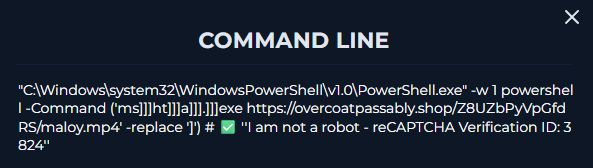
* Link extracted from email and submitted to VirusTotal.
* Flagged as **malicious** by multiple engines.
* Hosted a script tied to Lumma Stealer delivery.

#### **Victim Behavior:**

* Email was delivered (Device Action: Allowed).
* Victim (dylan@letsdefend.io) **visited the URL** shortly after receiving the email.
* **Browser history confirms** access to the malicious domain.



* **PowerShell commands executed** moments after the visit — consistent with payload delivery via script-based loaders.



### **Action Taken**

* **Isolated the victim’s endpoint** (dylan@letsdefend.io) from the network.
* **Escalated alert** to Tier 2 SOC for memory, file, and network forensic investigation.

