Shifts in the Underground: The Impact of Water Kurita's (Lumma Stealer) Doxxing

By By: Junestherry Dela Cruz Oct 16, 2025 Read time: 5 min (1254 words)

Published: 2025-10-16 · Archived: 2026-04-02 11:14:41 UTC

Key Takeaways

- A targeted underground exposure campaign leaked sensitive details of alleged core members of Lumma Stealer (tracked by Trend Micro as Water Kurita) , coinciding with a sharp decline in observed activity.
- This exposure, along with the compromise of the threat actor's Telegram accounts, caused a drop in Lumma Stealer activity for both new sample detections and C&C operations.
- Customers of Lumma Stealer's operators have been migrating to alternative infostealer Malware-as-a-Service (MaaS) platforms, mainly Vidar and StealC, and related services like Amadey saw reduced activity.
- This downshift in volume sparked aggressive competition among malware authors, possibly leading to new innovations and the rise of new infostealer variants in underground markets.

Introduction

In September 2025, we noted a striking decline in new command and control infrastructure activity associated with Lummastealer (which Trend Micro tracks as Water Kurita), as well as a significant reduction in the number of endpoints targeted by this notorious malware. This sudden drop appears to align with a targeted underground exposure campaign that has put the spotlight on individuals allegedly linked to the Lummastealer operation. Allegedly driven by competitors, this campaign has unveiled personal and operational details of several supposed core members, leading to significant changes in Lummastealer's infrastructure and communications.

This development is pivotal, marking a substantial shake-up in one of the most prominent information stealer malware operations of the year. While previous law enforcement interventions have played a critical role in combating cybercrime, this situation seems to have originated from internal cybercriminal rivalries and reputational attacks. The exposure of operator identities and infrastructure details, regardless of their accuracy, could have lasting repercussions on Lummastealer's viability, customer trust, and the broader underground ecosystem.

Lumma Stealer's decline

Lumma Stealer's growth and wide adoption was due to its efficiency, support, and frequent updates. However, its dominance in the underground market made it a key target for international law enforcement, culminating in a coordinated takedown attempt in May 2025. Despite this, Lumma Stealer quickly resurfaced, along with its operators, restoring infrastructure and reengaging with customers. Beginning in June, activity levels remained high, with fresh samples continuing to appear in the wild, indicating both operator resilience and strong demand within the cybercrime ecosystem.

However, this period of stability was disrupted in September 2025, when we began to observe a steady decline in both sample detections and C&C activity. This drop coincided with an aggressive underground exposure campaign targeting the individuals allegedly behind Lumma Stealer, resulting in significant operational setbacks for the malware's operators.

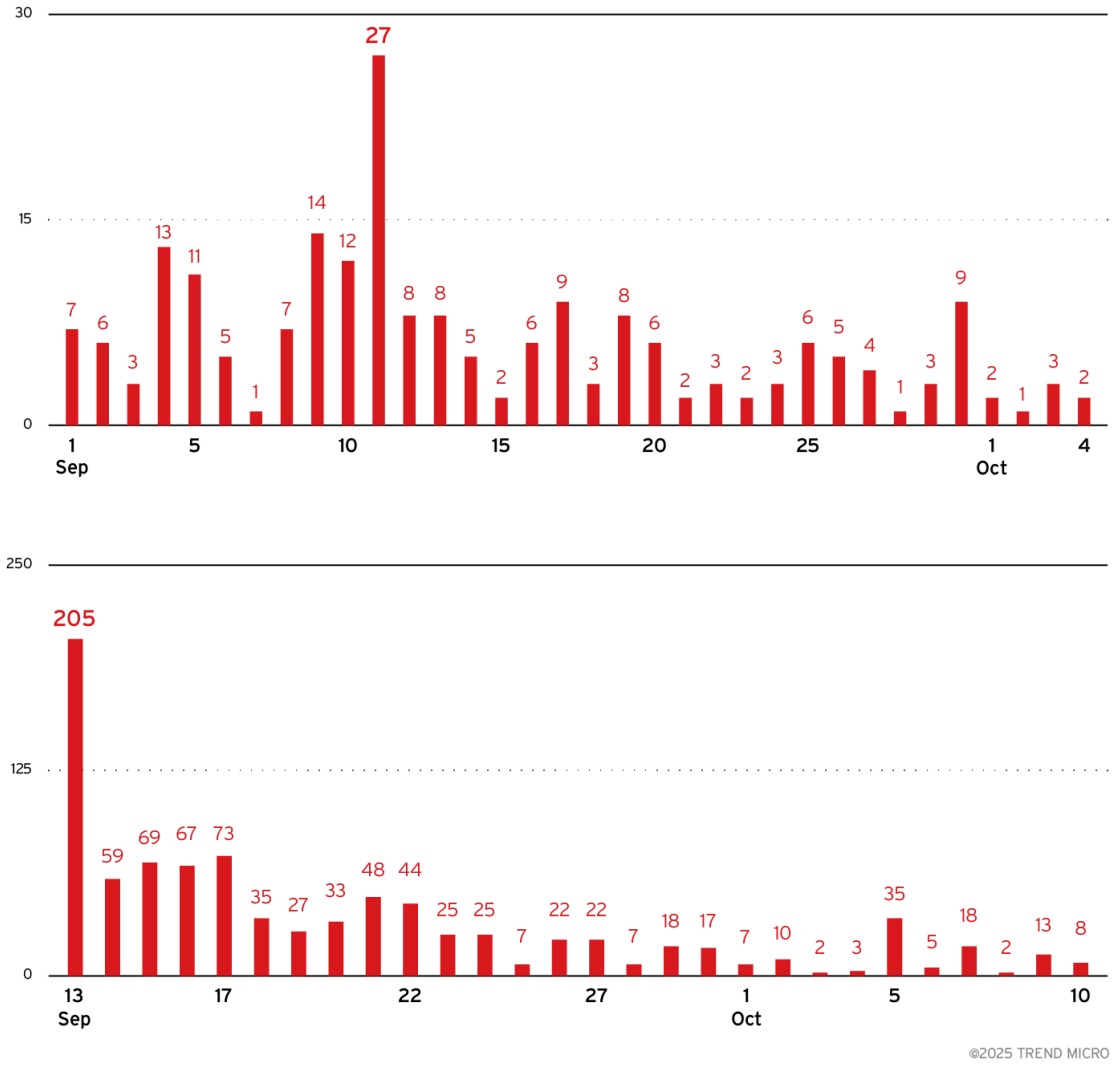

Figure 1. Lumma Stealer's downward trend in the number of targeted endpoints (top) and network infrastructure sourcing activity (bottom) from early September to early October 2025.

Timeline

The following sequence of events outlines the unraveling of Lumma Stealer's operations during late 2025, based on public sources and internal telemetry:

- Early September, 2025: Trend telemetry began to register a steady decline in Lumma Stealer sample detections and C&C activity.
- September 17, 2025: Lumma Stealer's official Telegram accounts were reportedly compromised or stolen.
- Late August to October 2025: A doxxing campaign published extensive personal and operational details of five individuals allegedly connected to the Lumma Stealer operation.

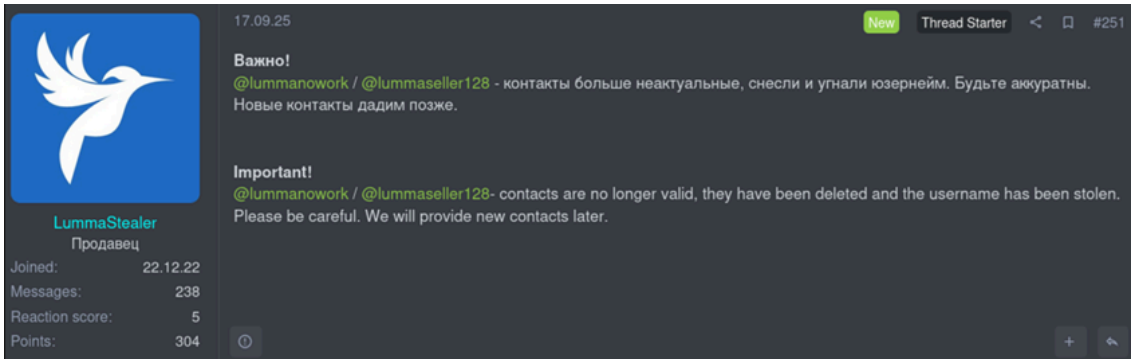

Figure 2. A representative of Water Kurita/Lumma Stealer posting in an underground forum regarding their Telegram accounts being stolen

Incident details

The decline in Lumma Stealer activity coincides with an aggressive underground exposure campaign targeting individuals allegedly affiliated with the malware's development and administration. The campaign, which began in late August and continued through early October, systematically released personally identifiable information (PII), financial records, passwords, and social media profiles of five purported Lumma Stealer operators, which were shown in a website called "*Lumma Rats*".

Based on the disclosed information, these were the roles of these individuals:

1. Administration/management: Responsible for operational oversight.
2. Development/technical: Focused on crypter development for malware obfuscation.
3. Unknown roles: Three additional members whose specific functions were not disclosed but were significant enough to warrant extensive doxxing.

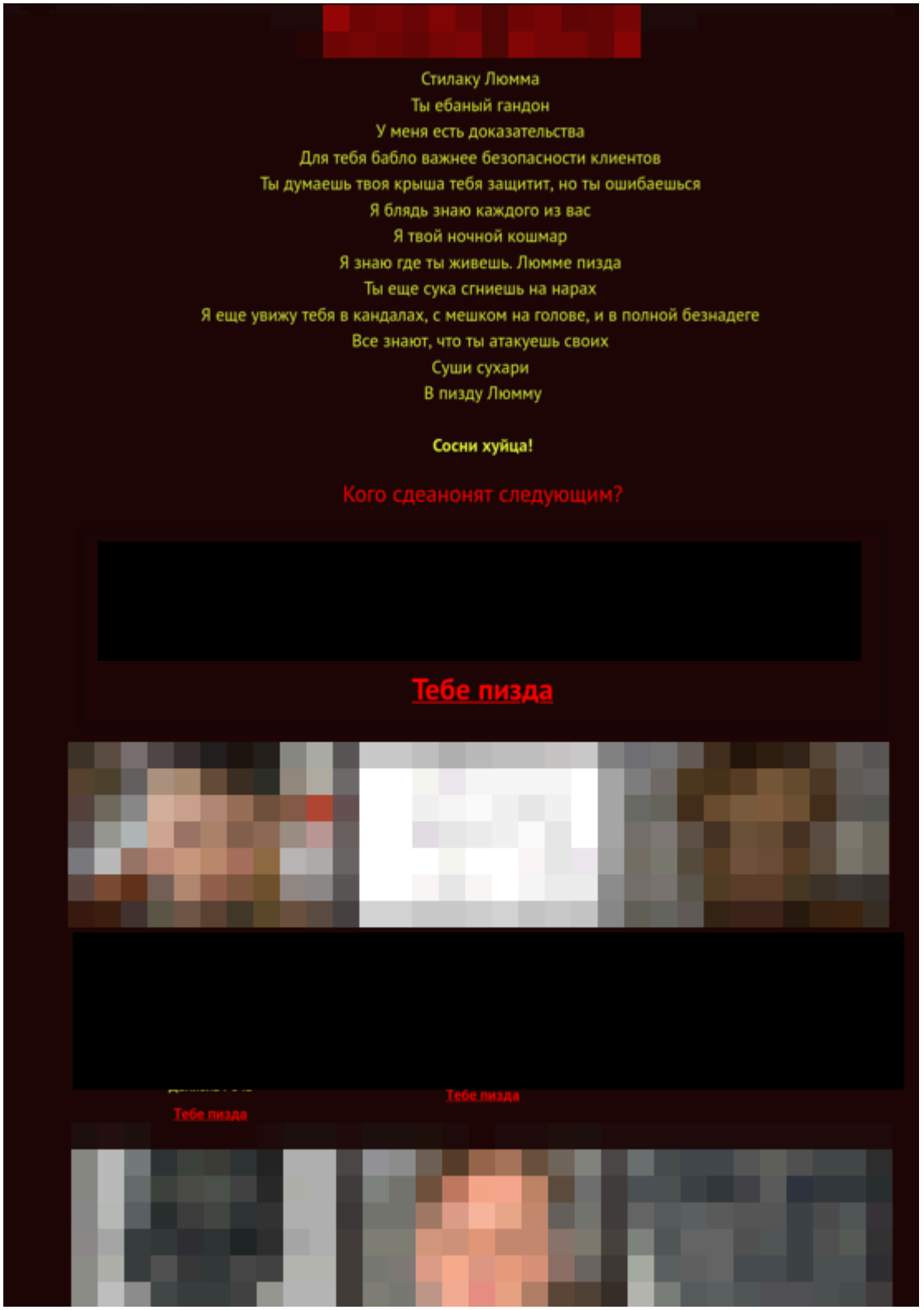

Figure 3. Alleged Lumma Stealer threat actors were doxed in a website called "Lumma Rats"

The disclosures included highly sensitive details such as passport numbers, bank account information, email addresses, and links to various online profiles. The exposure campaign was accompanied by threats, accusations of betrayal within the cybercriminal community, and claims that the Lumma Stealer team had prioritized profit over the operational security of their clients. The campaign’s consistency and depth suggest insider knowledge or access to compromised accounts and databases.

Following these disclosures, Lumma Stealer's Telegram accounts were reportedly compromised on September 17, further disrupting their ability to communicate with customers and coordinate operations. This has led to the previously mentioned reduction in new Lumma Stealer samples and observable C&C infrastructure, indicating that the operation has been severely affected—whether through loss of key personnel, erosion of trust, or fear of further exposure.

It is important to note that the accuracy of the doxed information and the actual involvement of the named individuals have not been independently verified. The campaign may also be motivated by personal or competitive grudges, and attribution should be treated with caution.

Response in the underground ecosystem

The attempt by unknown threat actors to undermine the operation of Lumma Stealer has triggered notable shifts in the underground malware-as-a-service (MaaS) landscape. Customers who previously relied on Lumma Stealer have been observed actively discussing alternative information stealer solutions on forums and Telegram channels. Vidar and StealCnews article have emerged as the primary replacement options, with many users reporting migrations to these platforms due to Lumma Stealer's instability and loss of support.

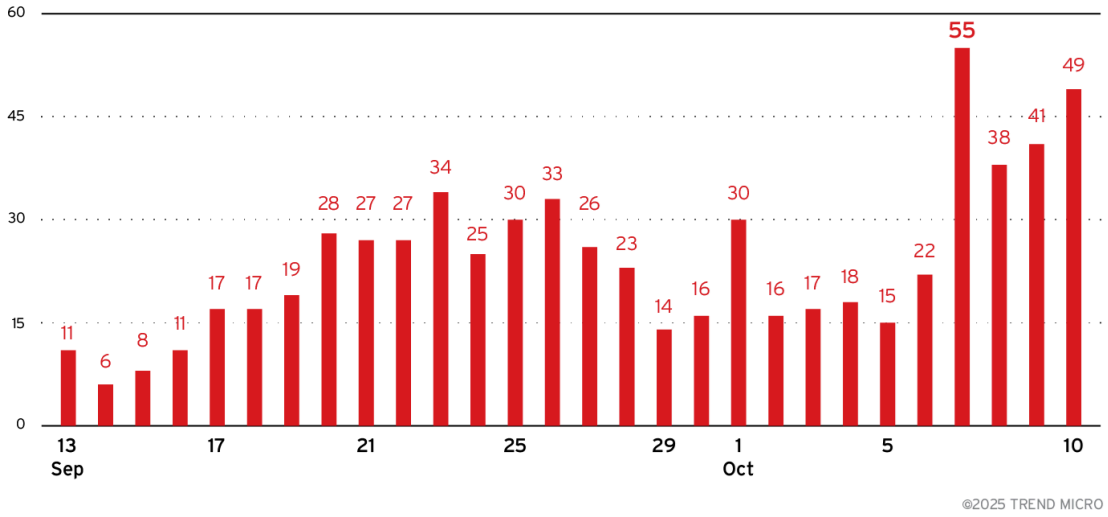

Figure 4. Vidar's upward trend in file sourcing activity since September (based on Trend telemetry data from September 13 to October 9, 2025)

This transition is also affecting the broader ecosystem, including pay-per-install (PPI) services such as Amadey, which have been widely used to deliver infostealer payloads. As Lumma Stealer's volume has decreased, Amadey has experienced a parallel drop in activity, suggesting reduced demand for its services in connection with infostealer distribution.

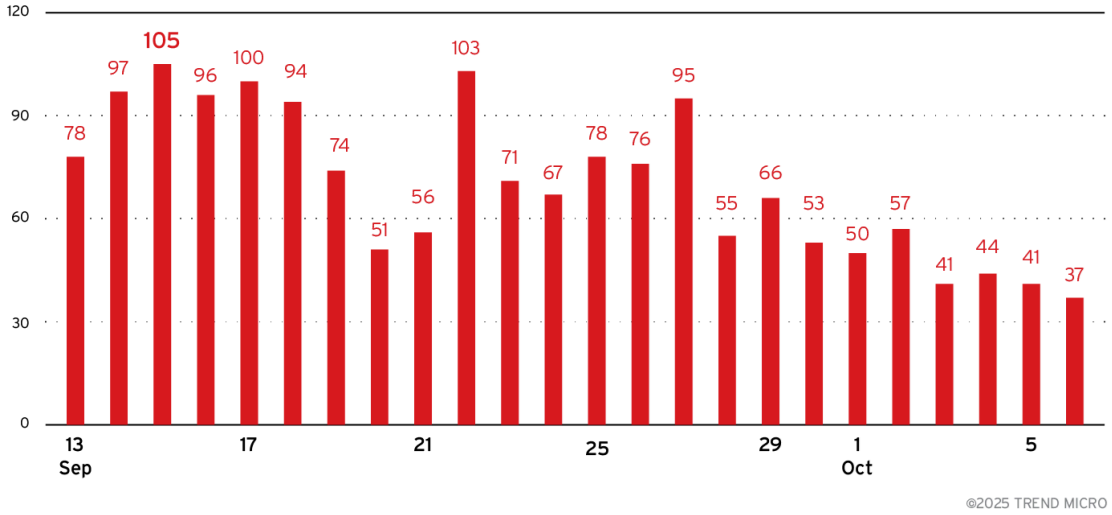

Figure 5. Amadey's downward trend in file sourcing activity suggests a reduced demand in services due to the decline in infostealer distribution (based on Trend telemetry data from September 13 to October 6, 2025)

Meanwhile, other malware authors are capitalizing on the situation by aggressively marketing their own alternative offerings, with the goal of attracting former Lumma Stealer customers. This opportunistic promotion is fueling rapid innovation and intensifying competition among MaaS providers, raising the likelihood of new, stealthier infostealer variants entering the market.

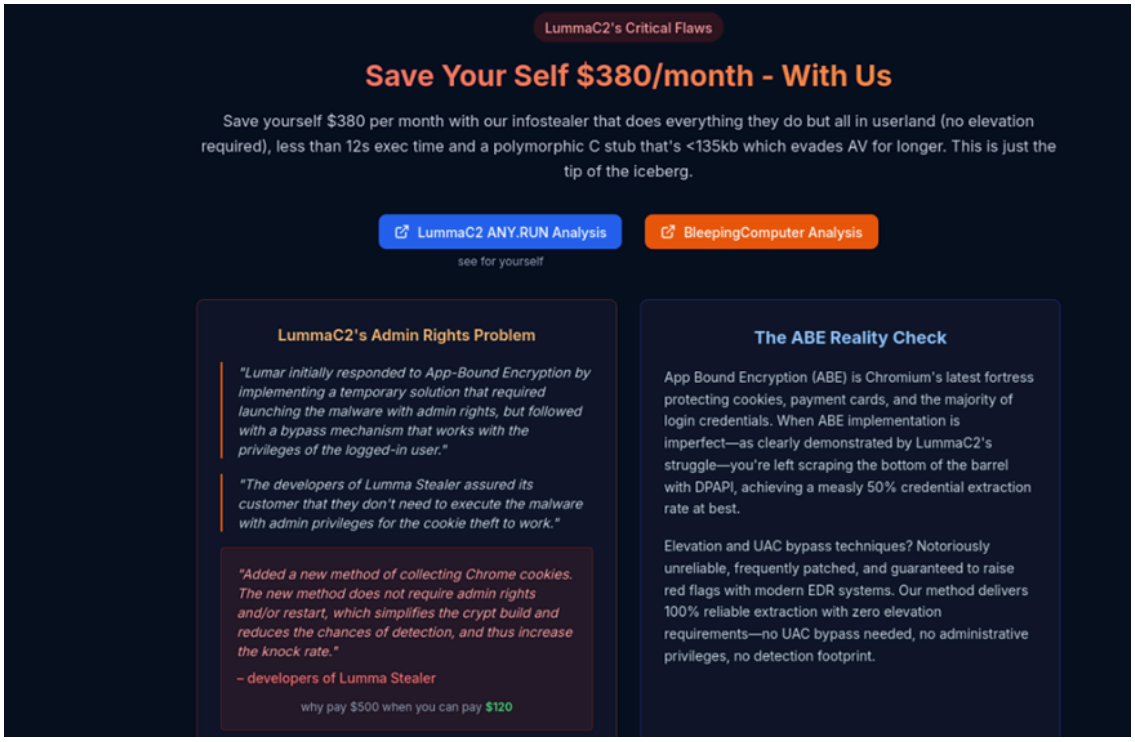

Figure 6. New infostealer ad comparing its services to Lumma Stealer and pointing out its flaws

Conclusion

The recent decline in Lumma Stealer activity demonstrates the volatile nature of the cybercriminal ecosystem, where even the most dominant malware families are vulnerable to both external law enforcement pressure and internal rivalries. As Lumma Stealer's position at the top made it a prime target for takedown operations and underground exposure campaigns, its disruption has prompted shifts in the threat landscape, with competitors eager to fill the void and attract former customers. This situation illustrates an important point: in the world of infostealers (and in the cybercriminal underground in general), being number one means facing scrutiny and attacks from both defenders and competitors alike.

Recommendations

Given the rapid migration away from Lumma Stealer, defenders should closely monitor the following:

- **Old MaaS like Vidar and StealC:** Continue monitoring for new campaigns, infrastructure, and samples associated with these increasingly popular alternatives.
- **Emerging MaaS Platforms:** Track newly promoted infostealers and pay attention to underground discourse indicating shifts in customer preference.

Tags
