Increase in Lumma Stealer Activity Coincides with Use of Adaptive Browser Fingerprinting Tactics

Published: 2025-11-13 · Archived: 2026-04-05 13:42:46 UTC

Malware

In this blog entry, Trend™ Research analyses the layered command-and-control approaches that Lumma Stealer uses to maintain its ongoing operations while enhancing collection of victim-environment data.

By: Junestherry Dela Cruz, Sarah Pearl Camiling Nov 13, 2025 Read time: 6 min (1698 words)

Key takeaways

- The doxxing of Lumma Stealer's alleged core members initially led to a decline in activity, but Trend™ Research observed an increase in Lumma Stealer-related activity (which Trend Micro tracks as Water Kurita) since the week of October 20, as well as new behaviors and C&C techniques.
- Lumma Stealer now uses browser fingerprinting as part of its command-and-control (C&C) tactics, supplementing traditional C&C protocols. The fingerprinting technique involves collecting and exfiltrating system, network, hardware, and browser data using JavaScript payloads and stealthy HTTP communications with Lumma Stealer's C&C server.
- These newly observed behaviors enable Lumma Stealer to maintain operational continuity, assess victim environments to guide follow-on actions, and evade detection.
- Trend Vision One™ detects and blocks the specific indicators of compromise (IoCs) mentioned in this blog, and offers customers access to hunting queries, threat insights, and intelligence reports related to Lumma Stealer.

In the wake of a targeted doxxing campaign last month that exposed the alleged core members of Lumma Stealer (which Trend Micro tracks as Water Kurita), the underground infostealer landscape experienced a significant upheaval. As detailed in Trend™ Research's previous reportopen on a new tab, this exposure led to a marked decline in Lumma Stealer's activity, with many of its customers migrating to rival platforms such as Vidaropen on a new tab and StealC. However, recent observations from our telemetry indicate a resurgence in Lumma Stealer activity, accompanied by notable changes in its command-and-control (C&C) behaviors, particularly the introduction of browser fingerprinting techniques.

Detailed analysis

Starting the week of October 20, 2025, Trend's telemetry began to detect a notable uptick in activity associated with Lumma Stealer, revealing a shift in its targeting strategy as new endpoints emerged as prime targets (Figure 1). A key development in this resurgence is the implementation of browser fingerprinting techniques by the malware, representing a significant evolution in its C&C infrastructure while maintaining core communication protocols consistent with previous versions.

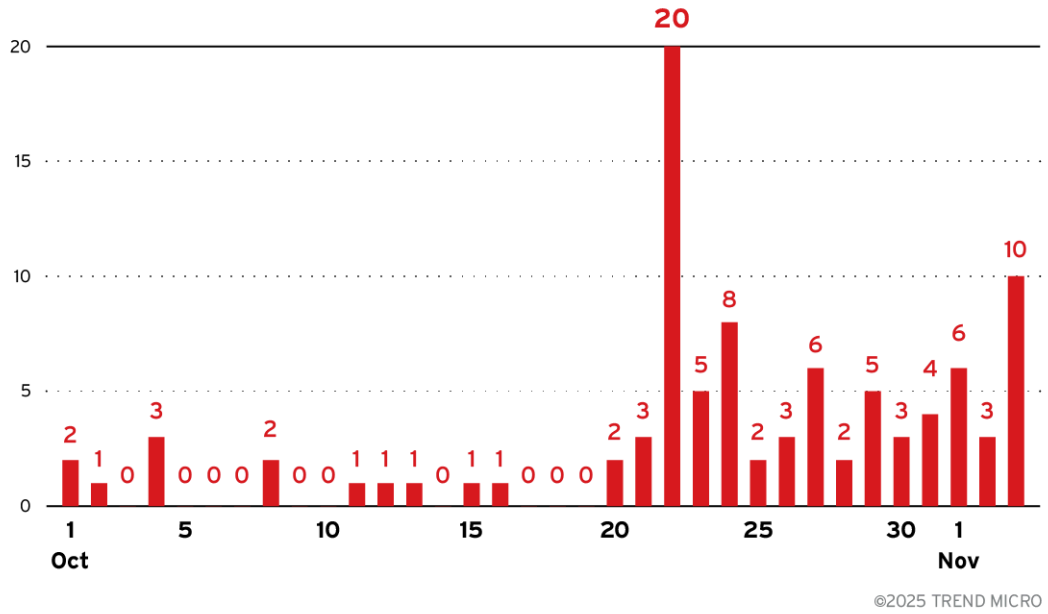

Figure 1. Endpoints targeted by Lumma Stealer from October 1 to November 3, 2025

Process injection and browser hijacking

The analyzed samples demonstrate Lumma Stealer's use of process injection techniques, specifically employing remote thread injection from MicrosoftEdgeUpdate.exe into legitimate Chrome browser processes (chrome.exe), as seen in Figure 2. This technique allows the malware to execute within the context of a trusted browser process, effectively bypassing many security controls and appearing as legitimate browser traffic to network monitoring systems.

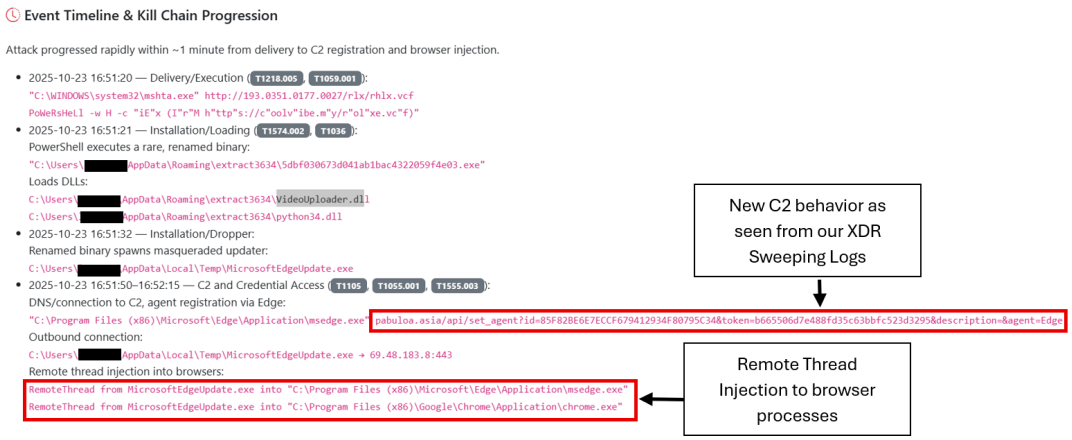

Figure 2. New Lumma Stealer browser fingerprinting behavior as seen from Trend's XDR logs

Network traffic analysis

Network capture analysis reveals the malware's communication patterns with the C&C infrastructure. The initial connection to the fingerprinting endpoint at *<c2 domain>/api/set_agent* is clearly visible in the network traffic, showing the HTTP GET request with the associated parameters including the unique identifier and authentication token (Figure 3). This traffic pattern represents a new addition to Lumma Stealer's communication repertoire, occurring alongside its traditional C&C protocols.

Figure 3. Browser fingerprinting behavior

New C&C endpoint: Browser fingerprinting infrastructure

The malware now communicates with a dedicated fingerprinting endpoint at */api/set_agent* on the C&C domain (*jamelik[.]asia* in this case). The initial GET request includes several parameters:

- **id** - A unique 32-character hexadecimal identifier
- **token** - A session token for authentication
- **agent** - Browser identification (Chrome in this case)

Despite the introduction of browser fingerprinting capabilities, our analysis confirms that Lumma Stealer maintains its core C&C communication structure as previously documented in Microsoft's researchopen on a new tab (Figure 4). Debug analysis reveals the malware continues to transmit traditional C&C parameters (Figure 5), including:

- **uid** - The unique identifier for the Lumma Stealer client/operator and campaign (updated from 'lid' in version 6)
- **cid** - Optional field identifying additional Lumma Stealer features (updated from 'j' in version 6)

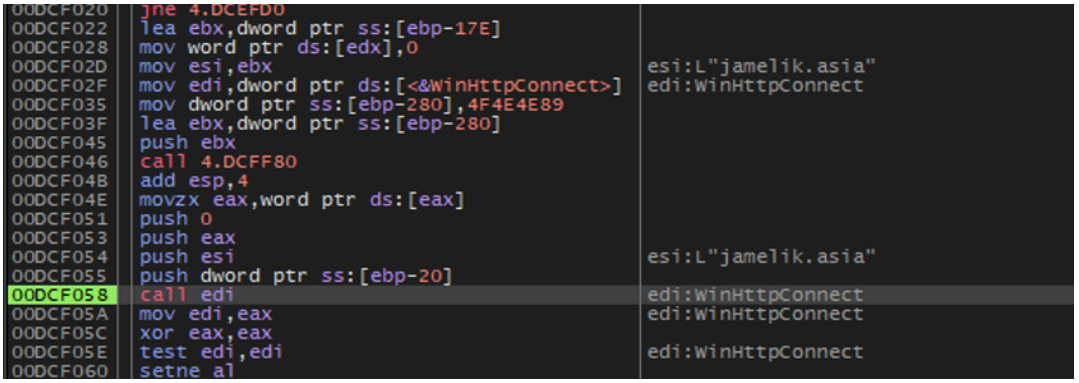

Figure 4. Using WinHTTP APIs, the malware establishes an outbound connection to its C&C server, enabling remote operators to issue commands, exfiltrate data, or deploy additional payloads

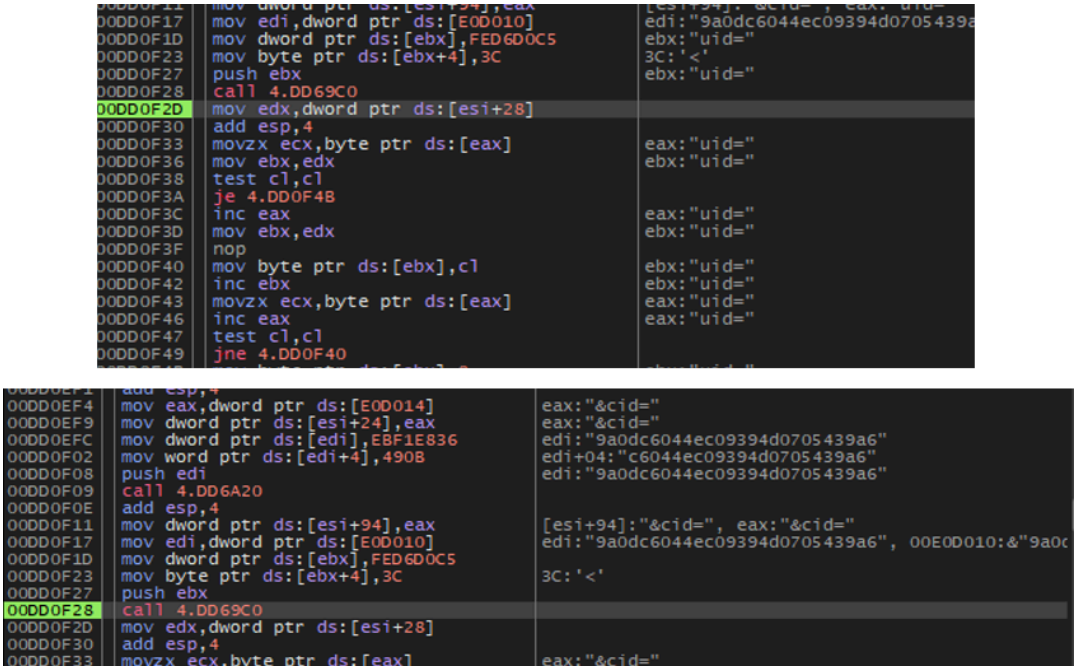

Figure 5. URL parameters uid and cid are transmitted to Lumma Stealer C&C for operators to track campaigns

This consistency indicates that the fingerprinting functionality represents an augmentation rather than a replacement of existing C&C infrastructure, suggesting the operators are layering new capabilities onto proven communication frameworks.

Configuration management

Analysis of the downloaded configuration data (Figure 6) reveals how the malware orchestrates both traditional data exfiltration and the new fingerprinting operations. The configuration maintains the established structure for managing C&C domains, command parameters, and operational directives while incorporating new directives for browser profiling activities.

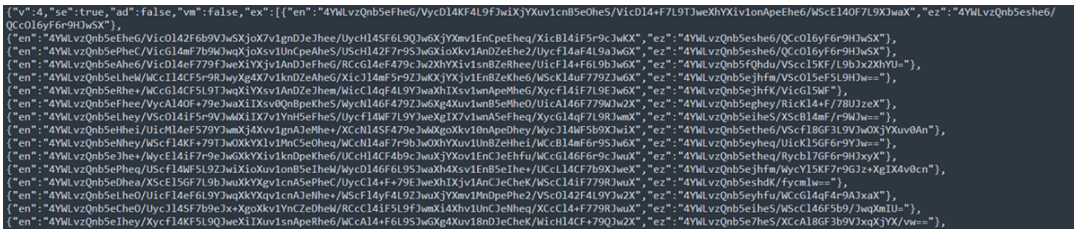

Figure 6. Downloaded configuration from C&C server

Browser fingerprinting payload

Upon accessing the fingerprinting endpoint, the C&C server responds with JavaScript code designed to collect an extensive array of system and browser characteristics. The fingerprinting script gathers the following information:

System information

- Platform details, user agent strings, and language preferences
- Hardware specifications including CPU cores, device memory, and touch capabilities
- Browser vendor information and application metadata

Browser profiling

- ***WebGL fingerprinting*** - Extracts graphics card vendor, renderer information, and supported extensions
- ***Canvas fingerprinting*** - Generates unique visual signatures by rendering text and shapes
- ***Audio context analysis*** - Captures audio system capabilities including sample rates and channel configurations.
- ***WebRTC information*** - Collects network interface details through Interactive Connectivity Establishment (ICE) candidates and Session Description Protocol (SDP) data

Network and hardware characteristics

- Connection type, effective bandwidth, and round-trip time measurements
- Screen resolution, color depth, and orientation data
- Available fonts and browser plugin information

Data exfiltration mechanism

After collecting the comprehensive fingerprint data, the script serializes all information into JSON format and transmits it back to the C&C server via a POST request to the same endpoint with an additional *act=log* parameter. The data is sent using URL-encoded form data, and upon completion, the browser is redirected to *about:blank* to minimize user awareness.

Tactical implications

This hybrid approach – combining established C&C protocols with new fingerprinting capabilities – serves multiple strategic purposes for Lumma Stealer operators:

- ***Enhanced evasion*** - The detailed system profiling allows the malware to identify virtual machines, sandboxes, and analysis environments
- ***Improved targeting*** - Operators can selectively deploy payloads based on victim profiles and system capabilities
- ***Operational continuity*** - Maintaining proven C&C parameters ensures compatibility with existing infrastructure and tools
- ***Detection avoidance*** - The use of legitimate browser processes and standard HTTP traffic patterns makes detection significantly more challenging

This fingerprinting implementation, combined with the retention of established C&C protocols, indicates that Lumma Stealer developers have strategically enhanced their capabilities without abandoning proven operational methods.

Water Kurita (Lumma Stealer) threat landscape assessment

Underground forum monitoring reveals a notable decline in Lumma Stealer threat actors' presence across cybercriminal communities, though marketplace activity continues with ongoing buying and selling of Lumma Stealer logs. The threat landscape has been further disrupted by multiple fraudulent Telegram accounts impersonating legitimate Lumma Stealer channels, potentially creating confusion within the threat actor community and fragmenting the user base. This operational disruption suggests the Lumma Stealer ecosystem is facing significant challenges in maintaining its previous level of coordination and communication.

Despite reduced underground visibility, Lumma Stealer remains an active threat with continued endpoint targeting and the documented deployment of GhostSocks as a secondary payload. However, operational degradation is evident in the threat actors' infrastructure management practices. New binary samples now contain outdated C&C domains – including Microsoft-sinkholed infrastructure – alongside single active C&C servers, contrasting sharply with previous comprehensive domain rotation practices that demonstrated more sophisticated operational security.

We assess with medium confidence that Lumma Stealer operators are keeping a low profile to avoid attracting attention from law enforcement and competitors. The threat actors appear to be deliberately reducing their visibility while maintaining

basic operations, likely waiting for the right opportunity to resume full-scale activities. This suggests they are still in business but operating more cautiously rather than shutting down completely.

Security recommendations

To help organizations effectively defend against the evolving tactics of Lumma Stealer, users and defenders can apply security best practices such as:

- Strengthen email security awareness. Train employees to identify and report phishing emails, particularly those impersonating legitimate software updates, shipping notifications, or urgent security alerts that trick users into downloading malicious attachments or clicking suspicious links
- Exercise caution with online advertisements. Be wary of clicking on advertisements, especially those offering free software downloads, urgent security warnings, or "too good to be true" deals, as cybercriminals use malicious ads to distribute malware through compromised websites
- Enforce software installation controls. Restrict user permissions to install software and establish approved software repositories, as malware often spreads through fake software installers, cracked applications, and malicious browser extensions downloaded from unofficial sources
- Be suspicious of unusual CAPTCHA requests. Question CAPTCHA prompts that ask you to copy and paste commands, run PowerShell scripts, or perform actions beyond simple image verification, as cybercriminals use fake CAPTCHA pages to trick users into executing malicious code that downloads malware
- Implement multi-factor authentication (MFA) on your accounts: Even though advanced attacks like adversary-in-the-middle (AiTM) phishing can try to get around it, MFA is still a crucial security measure that blocks many types of account compromise.

Hunting Queries

Trend Vision One Search App

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

Detection of Suspicious File Movement Involving .mid and .mid.bat Files
eventSubId: 2 AND objectCmd: /move.*\w+.mid(.bat)?/

Detection of Lumma Stealer Browser Fingerprinting Activity
eventSubId: 701 AND objectCmd: "*//api//set_agent?*&id*&token*&description*"

More hunting queries are available for Trend Vision One customers with Threat Insights entitlement enabledopen on a new tab.

Indicators of Compromise (IoCs)

File

Indicator	Detection name
516cd47d091622b3eb256d25b984a5ede0d5dd9540e342a28e199082395e65e5	TrojanSpy.Win64.LUMMASTEALER.THKAAI

URLs

Indicator	Description
pabuloa[.]asia	C&C server

jamelik[.]asia	C&C server

Tags
