

Lunex Uses BYOVD to Disable Security Monitoring and Deploy Persistent Stealer

Threat Bulletin

September 29 2026



HIGH



INFOSTEALER

Regions Targeted:

Ukraine

EXECUTIVE SUMMARY:

Lunex Malware-as-a-Service (MaaS) platform uses a fake CAPTCHA lure to deliver a loader, abuse a vulnerable AMD driver, and deploy the LunexStealer credential-stealing and C2 agent. The campaign is notable for using PDB-guided Bring Your Own Vulnerable Driver (BYOVD) techniques to identify and zero kernel callbacks associated with endpoint security products before executing the final payload. LunexStealer subsequently steals browser credentials, authentication data, and cryptocurrency wallets while establishing multiple persistence mechanisms, including a Chrome and Microsoft Edge Native Messaging Host capable of persistent remote filesystem access

KEY TAKEAWAYS

- LunexLoader abuses AMD's PDFWKRN.sys driver, affected by CVE-2023-20598, and uses exposed IOCTL functionality to read and write kernel memory.
- The loader retrieves kernel debugging symbols from Microsoft's Symbol Server to dynamically resolve security-related kernel structures for the victim's specific Windows build.
- LunexStealer targets seven Chromium-based browsers and multiple desktop and browser-extension cryptocurrency wallets while supporting continued C2 tasking.
- A Native Messaging Host registered as com.lunex.explorer provides filesystem and execution capabilities that can remain available even after the primary stealer executable is removed.

What is Lunex?

The Lunex [campaign](#) documented by Ontinue begins with a Ukrainian-language fake CAPTCHA page hosted on uasputnik[.]com. Victims are instructed to execute an msixexec command that silently downloads and installs a malicious MSI package. The installer operates from a per-user location under %LOCALAPPDATA%, does not initially require administrator privileges, suppresses the normal Windows Installer interface, and automatically launches LunexLoader.

LunexLoader is a 64-bit executable compiled with MinGW-w64 that disguises itself as an "Update Manager" from Canonical Ltd. Operational strings, including API names, registry paths, process names, C2 URLs, WMI queries, and kernel symbols, are encrypted with AES-256-CTR and decrypted at runtime. The loader also performs virtual machine and sandbox detection and checks running processes and kernel modules against an encrypted security-product blocklist. Before loading its vulnerable driver, LunexLoader performs a multi-step elevation chain. It modifies its Process Environment Block to appear as a trusted Windows binary, invokes the auto-elevating CMSTPLUA COM object, obtains administrator privileges without displaying a UAC prompt, enables SeLoadDriverPrivilege, and installs the vulnerable driver as a service.

PDB-Guided BYOVD

LunexLoader's implementation of BYOVD distinguishes the campaign from more conventional information-stealer operations. The loader reads the victim's `ntoskrnl.exe` and extracts the PDB GUID corresponding to the system's specific Windows kernel build. It then uses `curl.exe` to retrieve matching debugging symbols from Microsoft's legitimate Symbol Server and parses the PDB to locate kernel structures associated with process, thread, image-load, and other callback mechanisms. According to Ontinue, this makes the technique version-agnostic across Windows 10 and Windows 11 because the resulting offsets correspond to the running kernel. The malware then deploys AMD's `PDFWKRN.L.sys`, a driver affected by [CVE-2023-20598](#). LunexLoader uses IOCTL functionality exposed by the driver to read kernel callback table contents and write zeroes to selected entries.

LunexLoader determines which kernel modules own individual callback entries, compares those modules against a 20-entry security-product blocklist, and zeroes matching callbacks. Products and components represented in the list include Microsoft Defender, Kaspersky, Dr.Web, ESET, Elastic, Sysmon, CrowdStrike, SentinelOne, and Windows Filter Manager. Ontinue notes that targeting Windows Filter Manager could disable minifilter-based security products simultaneously rather than targeting a single vendor. Unlike EDR-killer malware that simply terminates security processes, this technique can leave security products running while disrupting their visibility into subsequent malicious activity. Ontinue also reported that validated testing found neither HVCI nor the then-current Microsoft Vulnerable Driver Blocklist prevented the specific `PDFWKRN.L.sys` variant used in the analyzed attack chain from loading.

LunexStealer and Persistent Access

After manipulating the kernel callbacks, LunexLoader downloads LunexStealer, which functions as both an information stealer and a persistent C2 agent. LunexStealer targets Google Chrome, Microsoft Edge, Brave, Yandex Browser, Opera, Opera GX, and Vivaldi. It collects credentials, cookies, authentication tokens, credit card information, and autofill data. Ontinue found support for Chrome encryption versions 10, 11, and 20, including App-Bound Encryption and the newer ChaCha20-Poly1305 format. The malware also targets Bitcoin Core, Litecoin, Exodus, Atomic Wallet, Electrum, MetaMask, OKX Wallet, and SafePal Wallet.

LunexStealer establishes persistence through a registry Run key, a hidden scheduled task named `psychedelicloveUtils`, and Chrome and Edge Native Messaging Host registrations. The Native Messaging Host is particularly significant. Registered as `com.lunex.explorer`, an embedded PowerShell component can enumerate drives, list directories, read and write files, download files from the compromised host, and execute arbitrary programs. Ontinue found that this mechanism can survive deletion of the LunexStealer executable, system reboots, and browser restarts.

Campaign Attribution

Ontinue identified 28 Lunex panels across 13 countries, compared with six panels across five countries identified by BlueTeamCoolTeam in June 2026. Multiple stealer codebases connecting to the same panel architecture, combined with self-registration functionality, support Ontinue's assessment that Lunex operates as a MaaS platform sold to multiple independent criminal operators rather than representing a single campaign or malware codebase.

Ontinue assesses with confidence that the activity analyzed in this campaign originates from a financially motivated, CIS-aligned threat actor operating through the Lunex platform. Separately, Ontinue assesses that the Lunex platform itself is developed by a Russian-speaking developer or development team and sold to independent criminal operators.

The platform contains more than 150 Russian-language interface strings, uses Russian as its default locale, and includes other Russian-language development artifacts. The specific operator analyzed by Ontinue used the configuration tag "Psychedelic" and targeted Ukrainian-speaking users. Separate Lunex infrastructure

has also been associated with phishing domains impersonating Western and Middle Eastern brands, demonstrating that different operators use the platform for different campaigns and targeting.

Analyst Commentary

Lunex demonstrates why defenders cannot assume that a running endpoint security product is necessarily a functioning one. Rather than simply terminating EDR or antivirus processes and creating an obvious indication that defensive tooling has been disrupted, LunexLoader uses a vulnerable signed driver and build-specific kernel information to interfere with security callbacks before deploying its final payload. The security product may remain present while losing visibility into activity occurring on the compromised system.

This makes the earlier stages of the infection chain particularly important. Lunex must perform multiple observable actions before it can interfere with endpoint monitoring, including delivery of the MSI and loader, privilege elevation, retrieval of Windows kernel symbols, deployment of PDFWKRNL.sys, and creation of a service to load the driver. Each stage creates an opportunity to identify and disrupt the attack before the final payload executes under degraded security visibility.

The campaign also illustrates the risk of treating removal of the primary malware executable as equivalent to complete remediation. LunexStealer establishes multiple persistence mechanisms, including a Native Messaging Host capable of filesystem access and program execution that Ontinue found can survive deletion of the stealer binary, system reboots, and browser restarts. Incident responders should therefore evaluate the complete attack chain and persistence footprint rather than focusing exclusively on the final-stage payload.

This is where a crowdsourced, multi-engine approach to malware detection provides significant defensive value. PolySwarm enables security teams to submit suspicious files and obtain verdicts from a diverse marketplace of independent malware detection engines, reducing dependence on the visibility or conclusions of any single security product. In a campaign specifically designed to undermine endpoint security controls, the ability to independently analyze artifacts such as malicious installers, loaders, vulnerable drivers, and final-stage payloads provides defenders with an additional layer of intelligence outside the compromised endpoint's own detection stack.

Organizations can use PolySwarm to enrich suspicious-file investigations, compare detection coverage across multiple engines, and identify malicious artifacts that individual products may classify differently or fail to detect. PolySwarm's threat intelligence capabilities can also help security teams pivot from identified artifacts and incorporate resulting intelligence into hunting, triage, and incident-response workflows.

Lunex reinforces the value of defense in depth. Endpoint security remains critical, but no individual defensive layer should represent the final authority on whether an artifact is malicious. PolySwarm provides organizations with access to a broad ecosystem of malware detection engines and threat intelligence that can complement existing EDR and antivirus deployments, strengthen malware triage, and provide additional visibility when attackers deliberately target the security controls defenders normally rely upon.

IOCs

PolySwarm has multiple samples associated with this activity.

bf14cd6c3328ebd08e940478b5d1da04e9e5aa576d045d41950bf4f1e2456dd8
6e8b49cf70bf854e8c59c7d27cefa89406caf8978461190dabb86dafcd8554e1
06f434695f93d7fd11eeff71358ff69fed79d310a66d993bbcc4ff979c117c90

