ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 19

B-2026-09-10b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

September 10, 2026

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on September 10, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

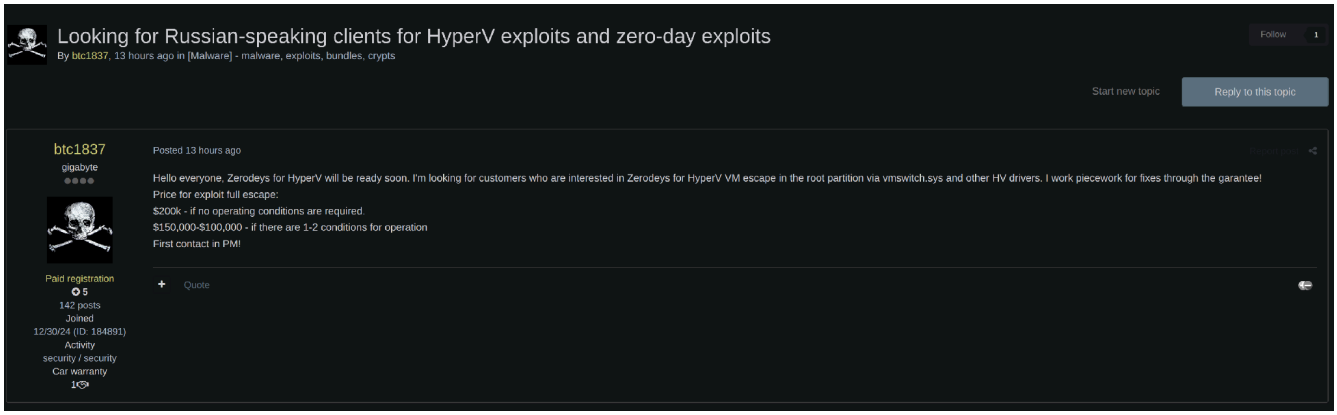
| Brief | The Underground Economist: Volume 6, Issue 19

| Alleged Virtual Machine Zero-Day for Sale

On September 8, 2026, untested Russian-language threat actor "btc1837" announced on the dark web forum Exploit that they are seeking Russian-speaking clients interested in Hyper-V and zero-day vulnerabilities that could enable Hyper-V virtual machine (VM) escape into the root partition through vmswitch.sys and other Hyper-V drivers. The actor claims that the advertised zero-day exploits will be ready and fully functional soon.

- Hyper-V is a native Microsoft hypervisor, which is used to create and manage VMs on Windows systems.
- The advertised price ranges from USD 100,000–200,000, depending on the operating conditions required for deployment.

The claimed capability is notable, as a functional Hyper-V VM escape would likely allow an attacker to move from a virtualized guest environment into the underlying host or root partition, increasing the likely impact of a successful compromise. The relatively high asking price also suggests the actor almost certainly considers the alleged exploit highly valuable. However, ZeroFox was unable to independently verify the existence, functionality, and exploitability of the claimed vulnerabilities.



btc1837's original Exploit post

Source: ZeroFox Intelligence

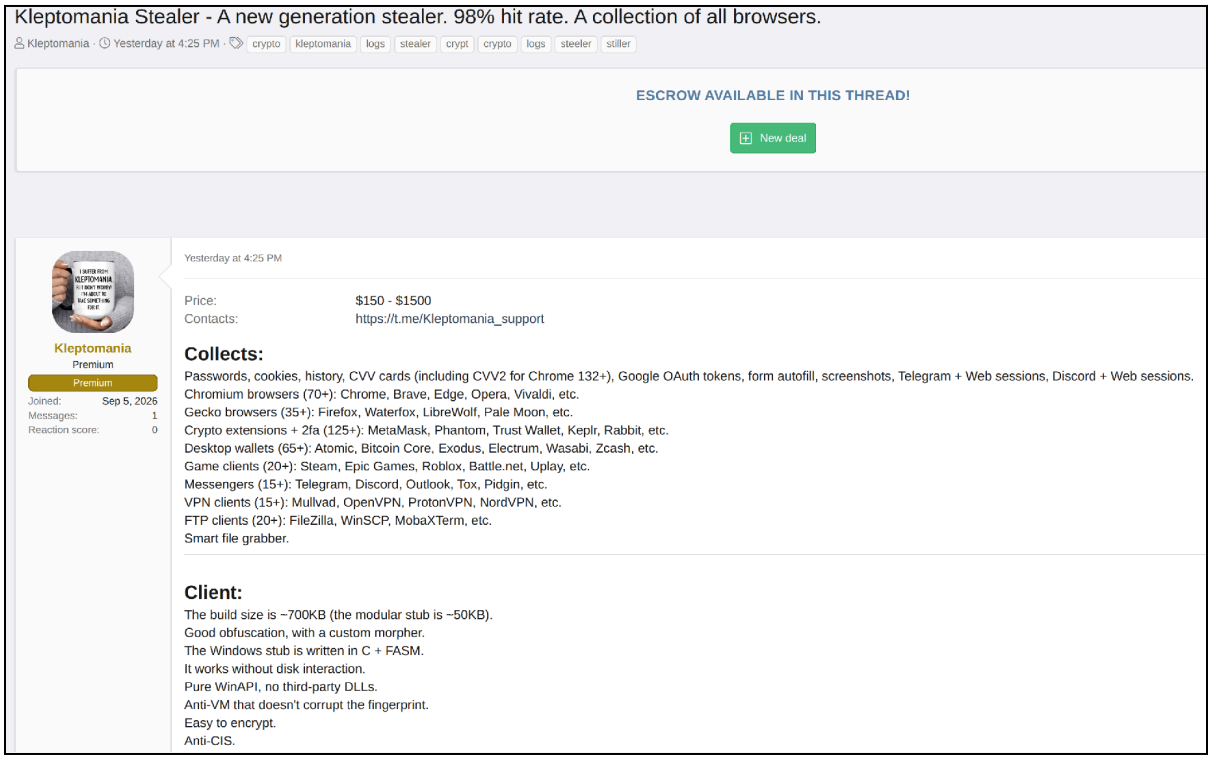
Kleptomania Infostealer Available on XSS

On September 7, 2026, untested threat actor "Kleptomania" posted on the dark web forum XSS announcing a "new generation infostealer" called "Kleptomania", advertised as a broad-spectrum credential and data theft malware targeting Windows users. According to the actor, the stealer can harvest:

- Passwords
- Cookies
- Browsing history
- Payment card data
- Google OAuth tokens
- Autofill data
- Screenshots
- Session data from Telegram, Discord, and other applications

Kleptomania reportedly supports more than 70 Chromium-based and 35 Gecko-based browsers, alongside numerous cryptocurrency wallets and extensions, desktop wallets, gaming platforms, messengers, and virtual private network (VPN) and file transfer protocol (FTP) clients. The malware is advertised as a roughly 700 KB modular Windows payload written in C/FASM, featuring custom obfuscation, anti-VM capabilities, diskless operation, and server-side decryption.

- The advertised service costs USD 150 per month, USD 400 for three months, or USD 1,500 annually. Additional capabilities—including wallet brute forcing, seed phrase scanning, a clipper, hidden virtual network computing (HVNC), and a macOS variant—are reportedly available or under development.



Kleptomania's post on XSS

Source: ZeroFox Intelligence

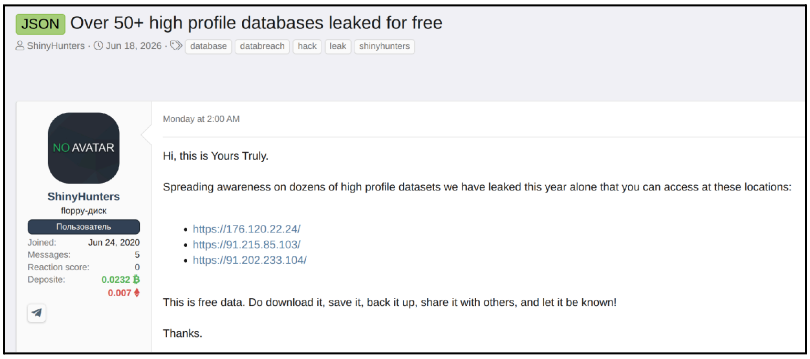
The breadth of supported browsers, applications, wallets, and session data makes it very likely that Kleptomania is a versatile credential and session theft tool rather than a narrowly focused infostealer. If the advertised capabilities are functional, the tool's ability to collect cookies, OAuth tokens, and application session data likely increases the risk of account takeover even when passwords are protected by multi-factor authentication (MFA).

The reported development of additional features such as wallet brute forcing, seed phrase scanning, a clipper, HVNC, and a macOS variant also suggests an expanding capability set and likely interest in supporting broader criminal use cases. ZeroFox was unable to verify the actor's claims regarding functionality and upcoming features.

ShinyHunters Reappears on XSS with Alleged Victim Data

On September 1, 2026, threat actor group ShinyHunters posted on the XSS forum and shared three IP address links to web servers allegedly hosting more than 5 TB of leaked data from the group's victims. The group stated that the leaked data was free to download, retain, or redistribute.

- According to the post, ShinyHunters compromised all of the affected victims in 2026 and stored their data on its infrastructure. The group allegedly published the data after the victims refused to pay ransom.
- This marks the reappearance of ShinyHunters on XSS. The group registered on the forum on June 24, 2020, but the profile remained largely dormant, with only five posts recorded over more than six years. This renewed activity raises questions about the group's current operational status and control of its previously established forum personas.



ShinyHunters' post on XSS

Source: ZeroFox Intelligence

In September 2025, a collective statement posted on dark web forum BreachForums claimed that 15 major ransomware and data extortion groups, including ShinyHunters, Scattered Spider, and Lapsus$, were permanently shutting down their operations. ShinyHunters's subsequent activity demonstrates that these claims did not represent a definitive end to the group's operations. ZeroFox noted similar previous announcements regarding the group's supposed retirement have also been followed by renewed activity.

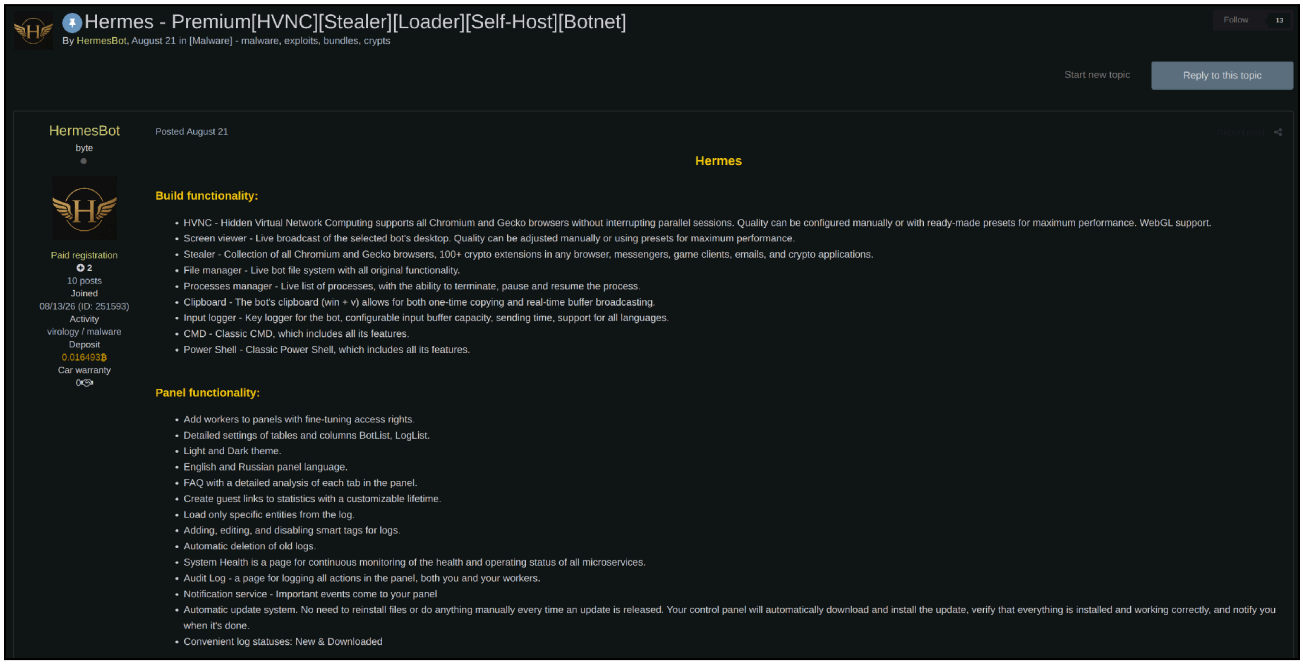
Several members or associates linked to the group, including an individual operating under the ShinyHunters alias on BreachForums, were arrested in 2025. However, the group's activities have historically involved multiple individuals, making it difficult to attribute control of its personas and infrastructure to a single actor.

ShinyHunters' renewed activity on XSS suggests that previously established forum accounts and infrastructure very likely remain accessible to members of the broader collective. The distribution of more than 5 TB of victim data also demonstrates that the group almost certainly retains, or has regained, the operational capacity to publicly distribute substantial volumes of stolen information.

New Malware-as-a-Service Platform "Hermes" Advertised

On August 21, 2026, untested threat actor "HermesBot" advertised a malware-as-a-service (MaaS) suite named "Hermes" on the Exploit forum, offering remote access, credential theft, and botnet capabilities under a tiered subscription model. ZeroFox has not identified any confirmed victims or incidents attributed to Hermes at this time.

- HermesBot has no independently verified forum history, reputation, or prior activity on Exploit. The advertised capabilities of the Hermes tool remain unconfirmed pending independent testing or observed victim reporting.
- The actor offered Hermes under a tiered subscription model ranging from USD 150 for 14-day access to USD 500 for 30-day premium access.



HermesBot's post on Exploit

Source: ZeroFox Intelligence

HermesBot claims the Hermes MaaS suite has the following capabilities:

- **Data theft:** Credentials and sessions from Chromium and Gecko browsers, 100+ cryptocurrency wallet extensions, and Discord and Steam tokens.
- **Remote access and control:** HVNC, live screen viewing of infected devices, keylogging and real-time clipboard capture, remote CMD/PowerShell execution, and remote file and process management.

The actor claims the malware suite provides a multi-user panel with tiered "worker" access built for team-based, scaled operations, which would likely increase adoption across multiple threat groups.

- If the claims are legitimate, Hermes is very likely to lower the technical barrier needed to conduct credential theft, cryptocurrency theft, and remote surveillance at scale. Additionally, features such as graphics processing unit (GPU)-accelerated encoding and low-latency screen viewing are likely to enable threat actors to scale operations with ease.

- HVNC provisioning is likely to help threat actors evade detection of malicious activity.

The developer's deliberate exclusion of the Commonwealth of Independent States (CIS) region very likely suggests they operate within or adjacent to the Russian-language cybercriminal ecosystem, where this is a well-established practice to avoid domestic law enforcement scrutiny.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant MFA, and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Appendix C: ZeroFox Intelligence Threat Actor Reputation Scale

Untested	Moderately Credible	Well-regarded	Prominent
Has garnered no reputation; credibility cannot be determined.	Has made up to 10 transactions; has been active on forum for at least three months.	Has at least 10 transactions; has been active on forum for three months to one year.	One of the most well-known and credible threat actors on the site; long-term, established presence on the forum of more than one year.