



| Brief |

The Underground Economist: Volume 6, Issue 20

B-2026-09-24b

Classification: TLP:CLEAR

Criticality: LOW

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

September 24, 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 24, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 6, Issue 20

| Alleged Windows ALPC Privilege Escalation Exploit Advertised

On September 23, 2026, moderately credible threat actor "QatarRat" advertised an alleged privilege escalation exploit for CVE-2026-85880 on the predominantly Russian-language dark web forum Exploit. CVE-2026-85880 is a heap-based buffer overflow vulnerability in the Windows Advanced Local Procedure Call (ALPC) subsystem, a native Windows inter-process communication mechanism.

- The threat actor claims the exploit grants SYSTEM-level privileges via a single executable that auto-detects the target Windows build—including Windows 10, Windows 11, and Windows 11 25H2 build 26200—locates the kernel, calculates the required offsets, and steals a SYSTEM token without further user interaction.
- QatarRat states the package includes an exploit framework, a dropper, and Windows Management Instrumentation (WMI)-based propagation functionality and claims that once SYSTEM access is achieved, an operator can install a backdoor, move laterally, and copy the tool to other machines.
- The actor claims the exploit was tested on a live system running Windows 10 and Windows 11 25H2 build 26200—returning process, token, and link values (pid=0x1d0, token=0x2f8, links=0x1d8)—and states the trigger correctly identified a patched build and exited cleanly without causing a Blue Screen of Death (BSOD).

- The exploit is priced at USD 20,000; QatarRat has stated deals are conducted through the forum's guarantor service and instructed interested parties to make contact via Telegram.

A functional SYSTEM-level ALPC exploit is notable, as SYSTEM access would very likely give an operator full administrative control over a compromised host, enabling backdoor deployment, credential theft, and lateral movement with minimal additional tooling. The actor's reported inclusion of WMI-based propagation and a dropper suggests the package is likely intended to support post-exploitation and spread beyond an initial foothold rather than function as a standalone proof of concept.

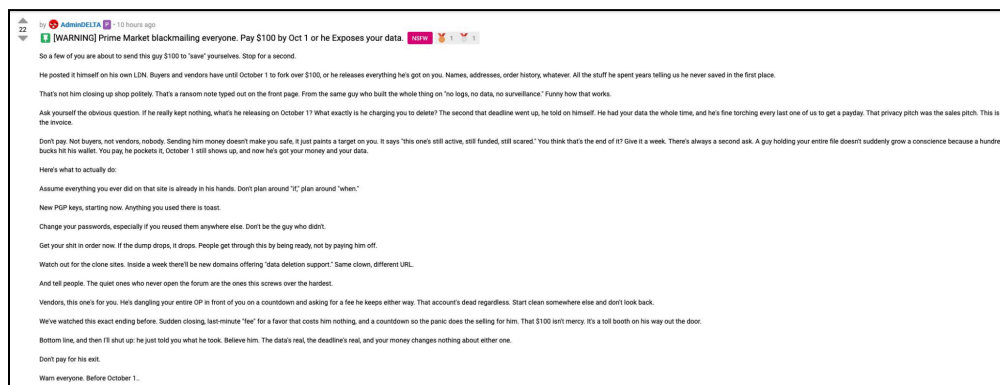
- CVE-2026-85880 is a confirmed vulnerability; Microsoft patched it as part of the September 8, 2026, Patch Tuesday release after confirming it had already been exploited in the wild, and the Cybersecurity and Infrastructure Security Agency (CISA) added it to its Known Exploited Vulnerabilities (KEV) catalog the same day, with a September 22 remediation deadline for federal civilian agencies.

| Prime Market Admin Extorting Users

On September 21, 2026, an administrator of the dark web marketplace Prime Market posted a message blackmailing users of the site. The admin has demanded each user pay USD 100 before October 1, 2026, or all of the data retained by Prime Market will be released.

- User data held by Prime Market likely includes translation logs, order history, and cryptocurrency wallet information.
- There is a roughly even chance the admin also has names and addresses of Prime Market users and vendors.

Later the same day, Prime Market user "AdminDelta" posted advice for other marketplace users. In that post, AdminDelta called out the extortionist and predicted that no data was actually available, as the site advertises that it retains no user data. AdminDelta posited that Prime Market's admin is attempting to extort users and make as much money as possible before shutting the site down. Finally, AdminDelta warned users not to pay and to prepare themselves and their businesses for the data dump.



Source: ZeroFox Intelligence

In March 2024, admins on another dark web marketplace, Incognito Market, issued similar threats after the owner of Incognito executed an exit scam and shut down the site. In that case, Incognito Market admins demanded USD 100–20,000 from vendors to avoid having their data leaked. The price demanded was dependent on the size of the vendor's business.

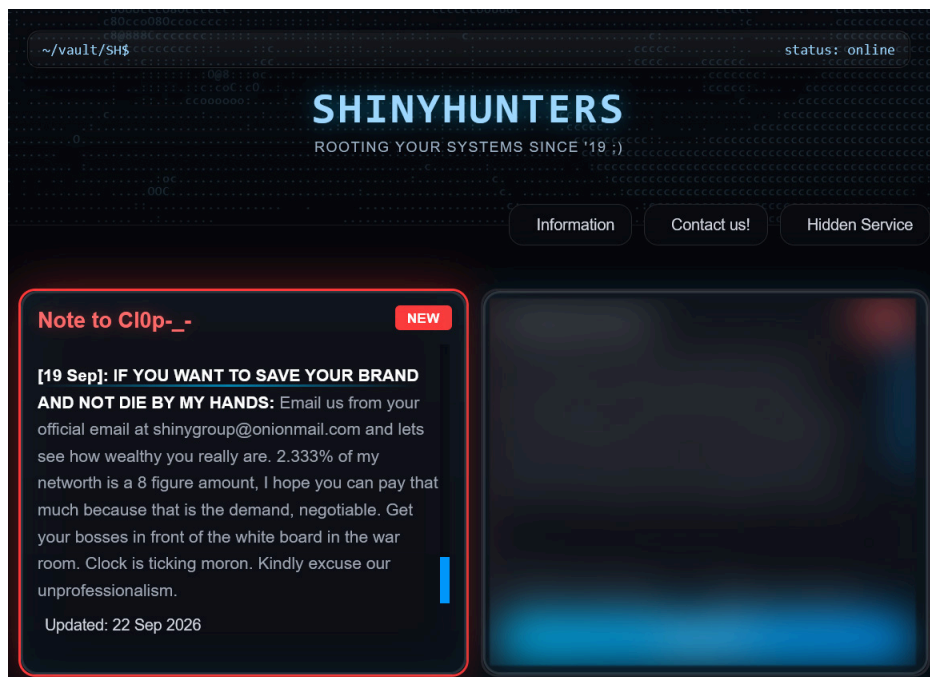
The admin of Prime Market is very likely trying to make money before shutting down the marketplace. Owners of dark web forums are known to extort vendors and users before going dark—often as they feel law enforcement closing in. There is a roughly even chance the owner of Prime Market has information that law enforcement is getting close to shutting down the site, and they are attempting to benefit financially as much as possible before that happens.

| ShinyHunters Attacks CI0p Ransomware Leak Site

On September 18, 2026, R&DE collective ShinyHunters gained unauthorized access to a dark web leak site belonging to fellow R&DE threat collective CI0p. The attack began when ShinyHunters exploited what the group claims was an unauthenticated file upload vulnerability on CI0p's site; ShinyHunters allegedly exploited the vulnerability to upload a small text file that contained a note warning CI0p not to threaten the group.¹

¹ [hXXps://www.bleepingcomputer\[.\]com/news/security/shinyhunters-hacks-clop-leak-site-threatens-to-extort-ransomware-gang/](https://www.bleepingcomputer.com/news/security/shinyhunters-hacks-clop-leak-site-threatens-to-extort-ransomware-gang/)

Several hours later, ShinyHunters reportedly told a journalist that it had defaced CI0p's leak site.² The defaced leak site now includes a link to ShinyHunters' own dark web leak site, as well as a message taunting CI0p.



Noted to CI0p added to ShinyHunters' dark web leak site

Source: ZeroFox Intelligence

ShinyHunters claims to have stolen significant amounts of data from CI0p, including its source code³—likely meaning the source code for CI0p's ransomware-as-a-service (RaaS) software and tools.

- It is also likely that ShinyHunters obtained system activity indicators and authentication logs.
- There is a roughly even chance that ShinyHunters gained access to the IP addresses of individuals connected to CI0p.

ZeroFox assesses that this incident will likely have a significant impact on CI0p's R&DE activity over the next six months. ShinyHunters exploiting CI0p's leak site, stealing data, and very likely gaining access to CI0p's source code will likely have consequences that

² *Ibid.*

³ *Ibid.*

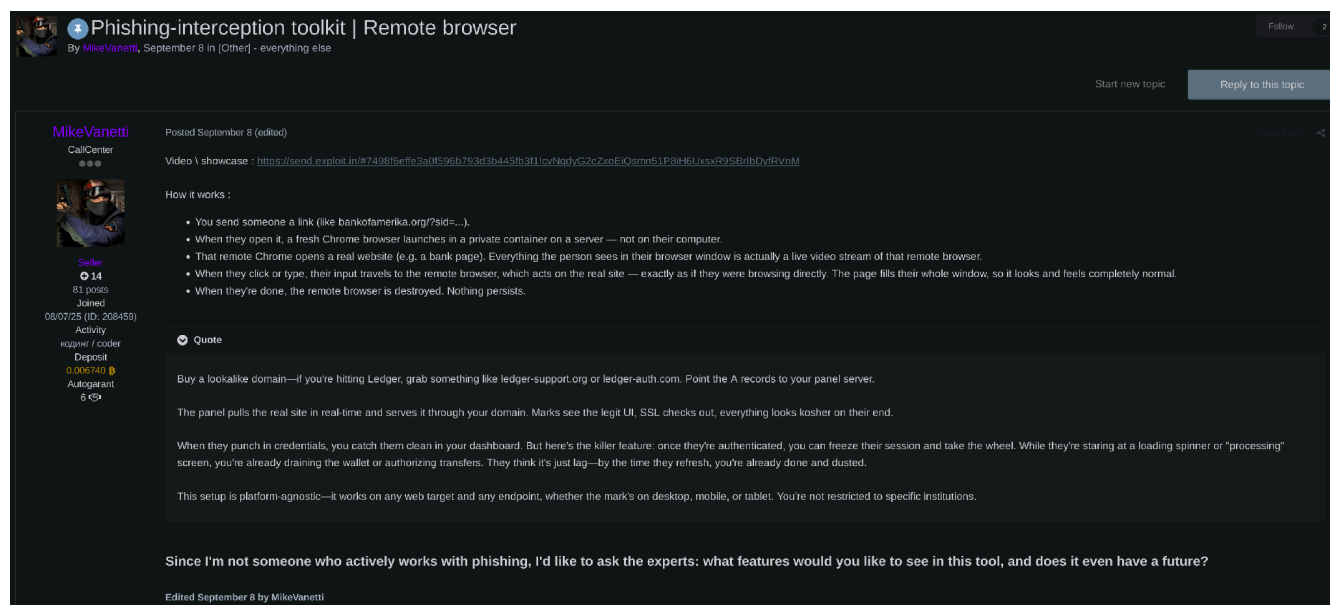
extend beyond just reputational damage. Unless CI0p comes to a rapid agreement with ShinyHunters not to release the stolen data—and ShinyHunters actually returns CI0p's data and source code—ZeroFox assesses that CI0p will likely be unable to conduct successful R&DE operations, causing a tangible, if temporary, degradation of the threat actor group's ability to impact organizations.

Additionally, ZeroFox assesses that rivalries and attacks between R&DE collectives will very likely lead to greater fragmentation across the threat landscape. Such fragmentation will almost certainly see new threat actors and splinter groups, creating a more crowded R&DE ecosystem and almost certainly leading to an increase in incidents.

| Exploit User Introduces an Alleged Phishing Tool with a Remote Browser Capability

On September 8, 2026, vetted threat actor "MikeVanetti" posted on the Exploit forum announcing a "Phishing-interception toolkit" allegedly built around a remotely hosted browser. The actor has not quoted a price or encouraged forum users to contact them to purchase the toolkit, suggesting they very likely made the post to solicit feedback and gauge interest rather than advertise an active sale.

- The actor joined the Exploit forum in 2025 and has made 81 posts so far.
- The current post centered around a phishing-interception toolkit likely refers to a man-in-the-middle tactic, with infrastructure placed between the victim and the legitimate website to enable threat actors to observe and manipulate the victim's interaction with that site.



MikeVanetti's post on the Exploit forum

Source: ZeroFox Intelligence

MikeVanetti describes the toolkit as enabling users to trick victims into interacting with a real website through a browser running on the attacker's server rather than directly on the victim's device. Victims see and use the website normally, while their clicks and keystrokes are transmitted to the remote browser controlled by the attacker, after which the victim's remote browser session is destroyed.

- The post appears intended to generate discussion around a remote browser phishing concept that proxies victims' interactions with legitimate websites through an attacker-controlled browser session. The actor asks forum users what features they would want and whether the tool has future potential, indicating that the offering is likely at a development or concept-validation stage.
- The post also presents the browser's potential use cases, including proxying legitimate websites through a look-alike domain, capturing victims' credentials, and potentially taking control of their authenticated sessions.

Although the title indicates a focus on phishing, most of the post discusses the remote browser's capabilities and potential use cases without clearly demonstrating how it would facilitate phishing. MikeVanetti also claims not to have actively worked with phishing services and seeks feedback on features and tool potential. This likely suggests

the actor is still exploring how remote browser technology can be adapted for phishing campaigns.

Given the absence of pricing, purchase instructions, or a direct solicitation for buyers, combined with the actor's request for feedback, the post likely represents an attempt to validate interest in and refine a potential phishing tool for a future offering. Based on the proposed use cases, the future offering is likely to be a remote browser phishing toolkit that could be incorporated into broader credential- and session-theft operations.

If the discussion attracts interest from other forum users, their feedback is likely to provide the actor with insight into features that would potentially make the toolkit more useful to phishing operators and inform subsequent development.

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 multi-factor authentication (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.