



| Brief |

The Underground Economist: Volume 6, Issue 22

B-2026-10-22b

Classification: TLP:CLEAR

Criticality: LOW

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

October 22, 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 October 22, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 6, Issue 22

| Actor Advertises a Tool for Uninstalling Antivirus Software

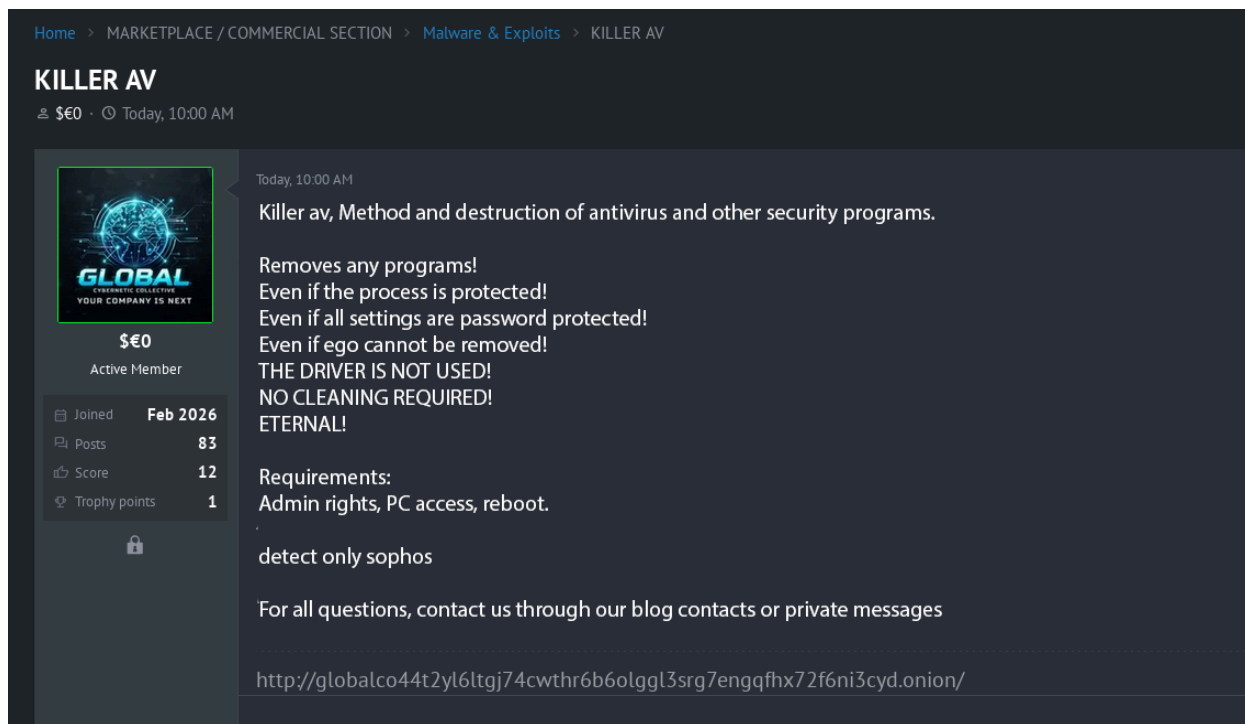
On October 21, 2026, moderately credible threat actor “\$€0” published a thread on the dark web forum T1erOne advertising a tool that reportedly uninstalls antivirus (AV) software and other security products, including those with password-locked settings or “undeletable” components. The actor claims that the tool works without a need for loading drivers or follow-up interactions.

- According to the seller, the tool can currently be detected only by Sophos, a UK-based security software and hardware company.
- The actor did not include any pricing information publicly and directed interested buyers to contact them privately.

Many known AV killer techniques rely on loading a legitimate but vulnerable driver, which defenders are increasingly capable of blocking; however, if the actor’s claim is true, those controls would be insufficient to block this tool.

The tool allegedly requires administrator rights, access to the machine, and a reboot. Given these requirements, ZeroFox assesses that the method/tool is likely a post-compromise tool rather than one that facilitates initial access.

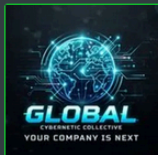
- A successful incursion would likely escalate from an alert to the complete loss of security tooling, with no discernible warning signs. Once cybersecurity solutions are disabled, attackers have a smoother path to malware deployment.



Home > MARKETPLACE / COMMERCIAL SECTION > Malware & Exploits > KILLER AV

KILLER AV

\$€0 · Today, 10:00 AM



\$€0
Active Member

Joined **Feb 2026**
Posts **83**
Score **12**
Trophy points **1**

Today, 10:00 AM

Killer av, Method and destruction of antivirus and other security programs.

Removes any programs!
Even if the process is protected!
Even if all settings are password protected!
Even if ego cannot be removed!
THE DRIVER IS NOT USED!
NO CLEANING REQUIRED!
ETERNAL!

Requirements:
Admin rights, PC access, reboot.

detect only sophos

For all questions, contact us through our blog contacts or private messages

<http://globalco44t2yl6ltgj74cwthr6b6olgg13srg7engqfmx72f6ni3cyd.onion/>

\$€0's TierOne post

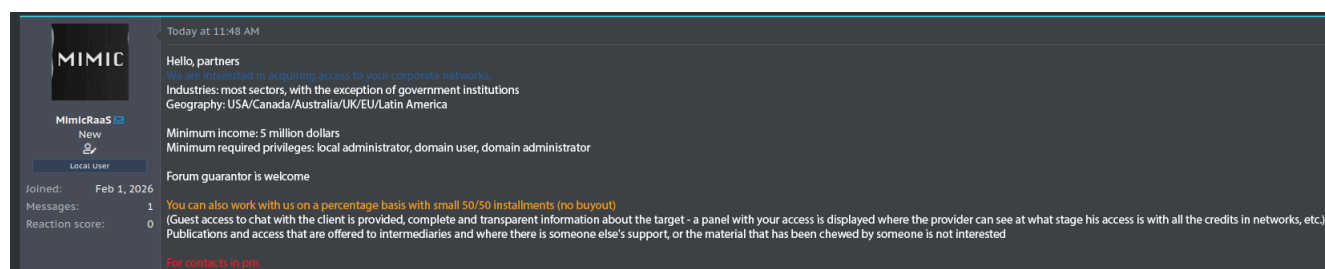
Source: ZeroFox Intelligence

| RaaS Operation Seeks Corporate Initial Access Brokers

On October 21, 2026, untested threat actor "MimicRaaS" posted on the dark web forum ReHub seeking initial access brokers (IABs) to procure access to corporate networks. The actor's operational footprint, compensation models, and explicitly stated target parameters almost certainly indicate they are a ransomware-as-a-service (RaaS) syndicate or a highly resourced core affiliate.

- The actor stated that the desired target regions are the United States, Canada, Australia, and the United Kingdom, as well as European Union and Latin American countries. MimicRaaS explicitly excluded governmental entities.

- The actor asserted that desired target organizations must have a minimum income (likely meaning annual revenue) of USD 5 million.
- MimicRaaS stated the minimum required privileges for access were local administrator, domain user, or domain administrator rights.



MimicRaaS's ReHub post

Source: ZeroFox Intelligence

MimicRaaS offers a highly formalized partnership structure, further corroborating their almost certain status as a structured RaaS operation. At this time, ZeroFox cannot confirm whether the threat actor represents a genuinely emerging ransomware syndicate or a splinter faction from a recently disrupted operation. The explicit exclusion of government entities aligns with standard Russian-language cybercrime syndicate operations.

| Yandex Disruption Unlikely to Impact Threat Actors

Overnight on October 7–8, 2026, drone strikes almost certainly launched by Ukrainian forces struck a Yandex data center in the Ryazan Oblast of Russia, resulting in a fire at the data center in the city of Sasovo and affecting part of the Yandex Cloud infrastructure.¹ The Sasovo site housed two of Yandex's three supercomputers; there have been no public disclosures regarding the extent of damage.² Immediately following the strikes, the status page for the Yandex Cloud service stated that its ru-central-b region was unavailable.³

¹ [hXXps://www.theregister\[.\]com/off-prem/2026/10/09/ukrainian-drone-attack-takes-out-russian-datacenter/5302137](https://www.theregister.com/off-prem/2026/10/09/ukrainian-drone-attack-takes-out-russian-datacenter/5302137)

² [hXXps://meduza\[.\]io/en/feature/2026/10/08/ukraine-strikes-yandex-data-center-housing-two-of-the-company-s-supercomputers](https://meduza[.]io/en/feature/2026/10/08/ukraine-strikes-yandex-data-center-housing-two-of-the-company-s-supercomputers)

³ [hXXps://www.theregister\[.\]com/off-prem/2026/10/09/ukrainian-drone-attack-takes-out-russian-datacenter/5302137](https://www.theregister.com/off-prem/2026/10/09/ukrainian-drone-attack-takes-out-russian-datacenter/5302137)

- Yandex is a Russian technology company that is often referred to as “Russia’s Google.” The company dominates the Russian market for email, search, and mapping services.
- It is very likely that Russian-language threat actors extensively use Yandex’s legitimate services to establish infrastructure needed for criminal operations.

On October 9, 2026, Yandex said that “several data center modules are completely disabled”⁴ at its Kaluga facility, which was likely the result of subsequent Ukrainian drone strikes. In the early morning hours of October 11, 2026, a strike on the company’s data center near Vladimir caused what Yandex deemed a “complete shutdown.”⁵ The three sites—Sasovo, Kaluga, and Vladimir—constitute half of Yandex’s six data centers.⁶

Overall, the Yandex disruptions have likely had limited impact on ransomware and digital extortion (R&DE) threat actors. Prior to the strikes, traffic from the Yandex Cloud network was roughly 95 percent automated, and none of it came from verified bots. After the strikes, bot traffic from that network fell about 40 percent, WordPress plugin probing fell 90 percent, and scanner traffic fell 93 percent.⁷

On October 8, 2026, several Russian-language deep and dark web (DDW) forums experienced system outages around the same time as these very likely Ukrainian attacks on Yandex data centers in Russia. Following the strikes, the Russian government likely increased restrictions on virtual private network (VPN) services; one Russian-language Telegram-based source stated that Russian government activities had rendered only Telegram still available for threat actor communications. Additionally, at least one prominent automatic infostealer was also offline around the same time.⁸

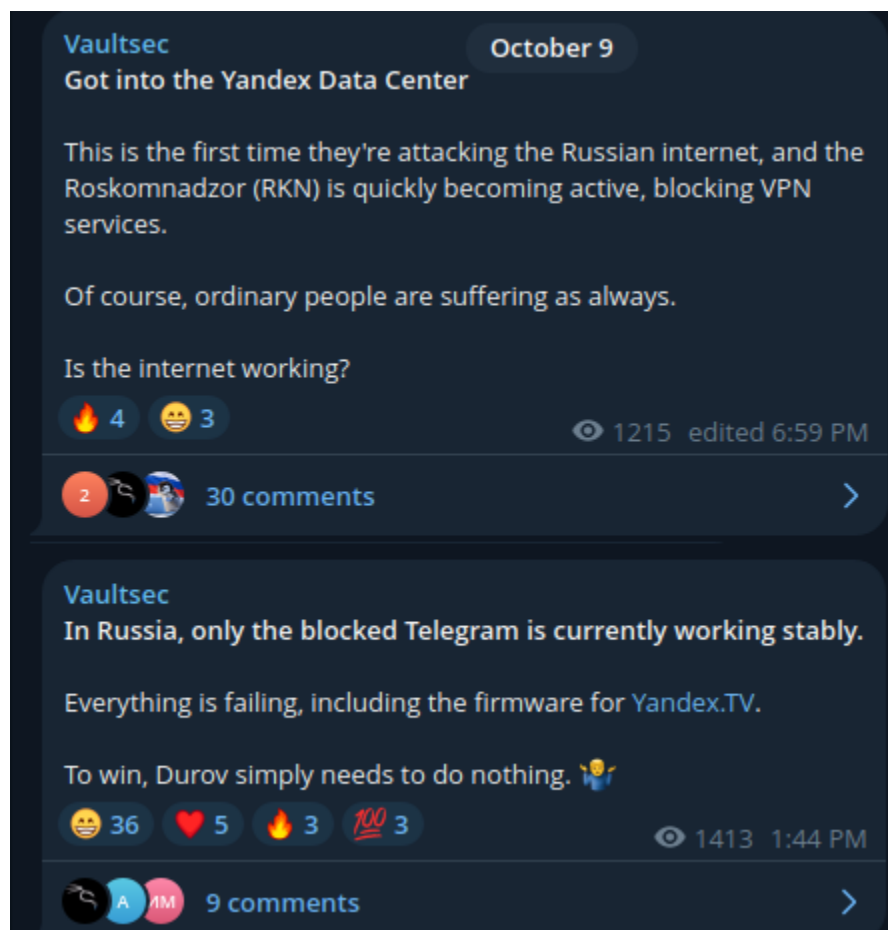
⁴ [hXXps://www.themoscowtimes\[.\]com/2026/10/09/ukraine-drones-hit-second-yandex-data-center-in-two-days-a93927](https://www.themoscowtimes.com/2026/10/09/ukraine-drones-hit-second-yandex-data-center-in-two-days-a93927).

⁵ [hXXps://www.themoscowtimes\[.\]com/2026/10/11/russias-yandex-says-data-center-in-vladimir-shut-down-after-drone-attack-a93942](https://www.themoscowtimes.com/2026/10/11/russias-yandex-says-data-center-in-vladimir-shut-down-after-drone-attack-a93942)

⁶ [hXXps://meduza\[.\]io/en/cards/ukrainian-drone-strikes-have-plunged-russia-s-internet-into-crisis-meduza-explains-why-the-damage-has-been-so-extensive-and-why-a-full-recovery-will-likely-take-months](https://meduza[.]io/en/cards/ukrainian-drone-strikes-have-plunged-russia-s-internet-into-crisis-meduza-explains-why-the-damage-has-been-so-extensive-and-why-a-full-recovery-will-likely-take-months)

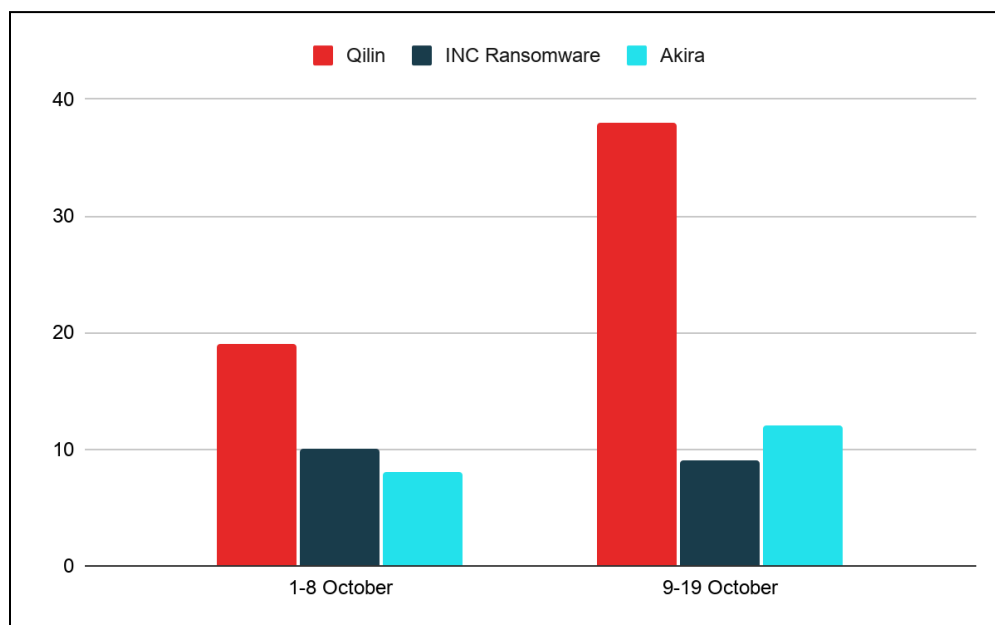
⁷ [hXXps://blog.cloudflare\[.\]com/yandex-outage/](https://blog.cloudflare[.]com/yandex-outage/)

⁸ ZeroFox Intelligence

**Telegram post regarding VPN restrictions (Translated from the Russian by ZeroFox)**

Source: ZeroFox Intelligence

However, ZeroFox has observed increases in both bot request traffic and ransomware leak site activity across the entire Russia-origin R&DE ecosystem—suggesting that threat actors almost certainly maintained backup infrastructure hosted on other services and pivoted to those backups quickly. Additionally, the most active likely Russian R&DE threat actors continued operations at or above pre-strike levels, also almost certainly suggesting continuity of operations via backup infrastructure.

**Major likely Russian threat actor incidents pre- and post-strikes***Source: ZeroFox Intelligence*

Although the strikes almost certainly caused significant disruptions to Yandex, its cloud services, and its extensive Russian client base, they are very unlikely to have any major impact on Russian threat actor infrastructure or activity. After the drone strikes, ZeroFox observed that nearly all major Russian threat actor activity remained at or above normal operational pace. It is almost certain that Russian threat actors will continue to operate mostly unabated throughout the reconstitution and recovery time for Yandex services.

| Threat Actor Advertises Beta-Stage macOS Stealer and Seeks Partnership

On October 7, 2026, threat actor “MiraxBot” advertised a beta-stage macOS information stealer on the predominantly Russian-language dark web forum Exploit and later promoted the tool on Telegram. The actor stated they were recruiting forum users to test the malware and claimed to offer free access to users with a good reputation and paid access to others. MiraxBot also said they were seeking established partners to scale operations outside the United States and United Kingdom.

- MiraxBot is reportedly the developer behind the established “Mirax” Android malware-as-a-service (MaaS) and banking remote access trojan (RAT) targeting Android users across Europe.⁹ According to the claimed operator’s XSS advertisement in March 2026, the Android version is advertised as a banking bot that allows operators to remotely control infected devices and conduct targeted theft of banking credentials and authentication data.¹⁰
- The capabilities of the established Android version of Mirax reportedly include credential theft, screen manipulation, and data collection. The tool also reportedly turns infected devices into SOCKS5 residential proxies, extending its use beyond direct theft to routing other malicious activity through victims’ IP addresses.¹¹
- If the macOS stealer reaches a stable final release, it is likely to be offered through a similar MaaS or rental model as the Android version—particularly given MiraxBot’s existing subscription-based business model and stated interest in partnerships to expand their operations.

The post claims the Mirax macOS stealer can steal credentials, browser data, cryptocurrency wallet information, messaging app data, VPN credentials, Secure Shell (SSH)/GNU Privacy Guard (GPG) keys, developer/cloud configuration files, email data, and selected user files from macOS systems. Additionally, the actor claims the tool can collect a victim’s macOS login password and provide an inventory of installed applications.

- The operator’s posts describe intended/advertised functionality, not evidence that every capability works successfully in the beta build.
- MiraxBot’s Exploit post primarily promotes the Mirax macOS stealer and its capabilities, while the Telegram post focuses on commercial partnerships, geographic expansion, and broader operational capabilities.

⁹ [hXXps://www.securityweek\[.\]com/mirax-rat-targeting-android-users-in-europe/](https://www.securityweek[.]com/mirax-rat-targeting-android-users-in-europe/)

¹⁰ https://cloud.zerofox.com/intelligence/advanced_dark_web/112429

¹¹ [hXXps://thehackernews\[.\]com/2026/04/mirax-android-rat-turns-devices-into.html](https://thehackernews[.]com/2026/04/mirax-android-rat-turns-devices-into.html)

**Mirax MacOS stealer [BETA]**

Follow1

By MiraxBot, 6 hours ago in Malware

Start new topicReply to this topic

**MiraxBot**

kilobyte

31 posts

Joined 11/12/25 (ID: 218474)

Activity

virology / malware

Deposit 0.018451

Car warranty

Posted 6 hours ago (edited)

Greetings to all forum members!

I'd like to invite you to participate in beta testing of a new product from the Mirax team, focused on macOS.

We'll offer users with good standing the opportunity to test the product for free. Anyone else interested will need to pay for the server to participate.

If you are interested, please write to the contacts below.

The product's functionality will be described in detail below.

[@MiraxSupp - TG Support](#)

[@mirax_rat - TG Channel invite](#)

macOS Backup – What to Collect from a Mac

Only what's actually on the computer is archived. If there's no app or file, the block is skipped.

Keychain

- The login.keychain-db file
- For keychain v2 format (if access was possible):

Browser secrets (Chrome Safe Storage and similar) — JSON

Stored internet passwords from the keychain - JSON- The macOS login password entered when starting the agent is sent to the server along with the archive (for recovery on another Mac)

Browsers

Chromium family (if installed):

Google Chrome, Chrome Beta, Chrome Canary, Microsoft Edge, Brave, Vivaldi, Opera, Opera GX, Arc, Yandex Browser, Orion, CocCoc, Chromium

Typically from a profile: logins, cookies, history, bookmarks, settings.

Crypto extension data - see separate section below (not all extensions in a row).

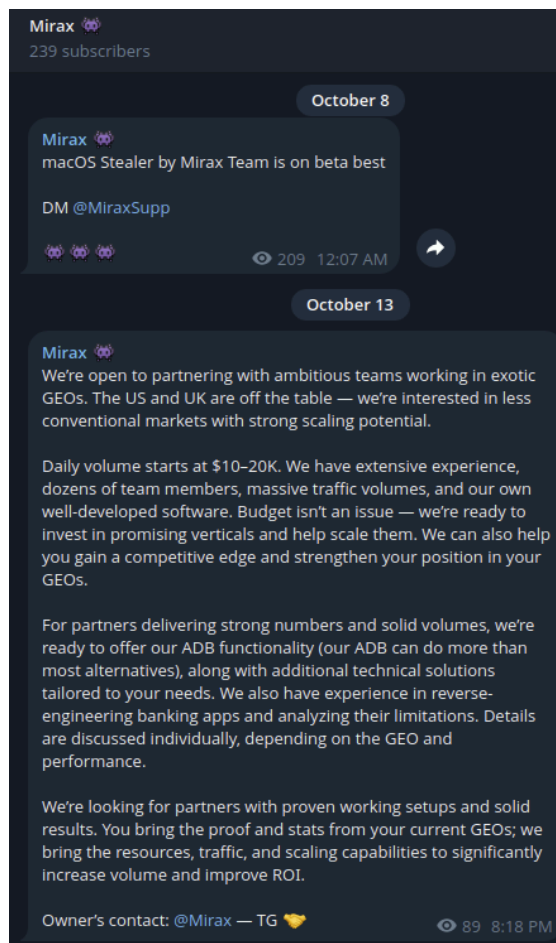
Firefox family:

Firefox, Firefox Developer Edition, Waterfox, LibreWolf

Typical: profile settings, history/bookmarks, logins, key4.db, cookies, formhistory, extensions and related files.

MiraxBot's Exploit post regarding the Mirax beta-stage macOS stealer

Source: ZeroFox Intelligence



Mirax's Telegram post inviting partnership

Source: ZeroFox Intelligence

Given that the two products target different operating systems and appear designed around different forms of access, the macOS stealer likely represents an expansion of Mirax's credential and financial data theft capabilities beyond its established Android-focused MaaS.

The Mirax macOS stealer allegedly remains under active development, and its advertised capabilities are likely to change as testing progresses. The free access offered to reputable forum members is likely intended to generate testing feedback and establish credibility before wider commercialization.

If released with its advertised functionality, the Android and macOS versions of the stealers are likely to enable Mirax operators to harvest data from both platforms, giving

them broader access to victims' credentials, financial information, authentication data, and other sensitive information and enabling account takeover and financial theft. The availability of both versions is also likely to attract IABs seeking stolen credentials, VPN access, cloud credentials, or other data that could facilitate broader access to compromised organizations.

| 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 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.