



| Brief |

The Underground Economist: Volume 5, Issue 17

B-2025-08-28b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor,
Cryptocurrency

August 28, 2025

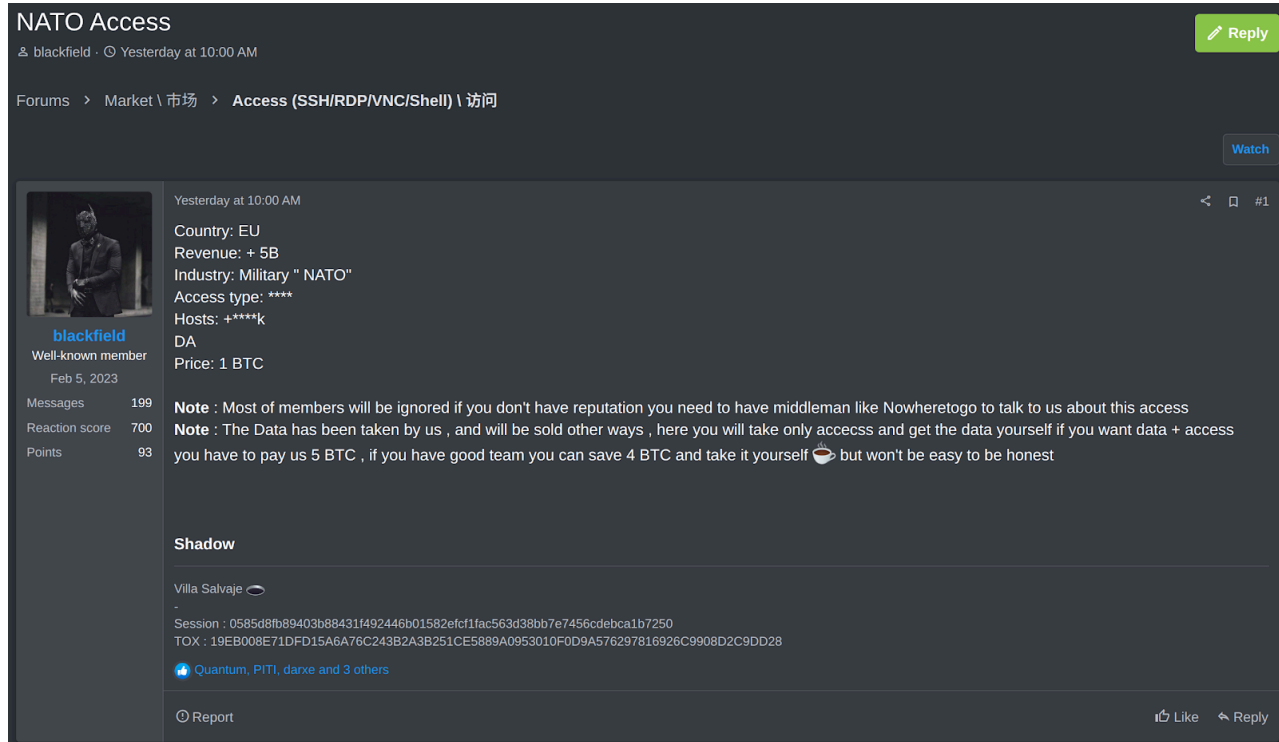
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 10:30 AM (EDT) on August 28, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 17

| Data Allegedly for Sale from European Union NATO-affiliated Company

On August 26, 2025, a prominent threat actor known as “blackfield” posted on the Russian-language dark web forum RAMP, advertising alleged access to an unnamed European Union NATO-affiliated company with revenues exceeding USD 5 billion. The access type and number of hosts were censored in the post at the time of writing this report; however, blackfield also claimed to have domain access privileges to the unnamed company’s active directory (AD) environment. The actor is selling the singular access vector for 1 BTC or approximately USD 112,447.

- The actor also claimed to have exfiltrated the alleged data, which blackfield is offering for sale in addition to the domain access privileges for a total of 5 BTC or approximately USD 562,235.
- The actor noted that buyers of the access alone could exfiltrate the data themselves but that it “won’t be easy to be honest.”



NATO Access

& blackfield · Yesterday at 10:00 AM

Forums > Market \ 市场 > Access (SSH/RDP/VNC/Shell) \ 访问

blackfield
Well-known member
Feb 5, 2023

Messages 199
Reaction score 700
Points 93

Yesterday at 10:00 AM

Country: EU
Revenue: + 5B
Industry: Military " NATO"
Access type: ****
Hosts: +****k
DA
Price: 1 BTC

Note : Most of members will be ignored if you don't have reputation you need to have middleman like Nowheretogo to talk to us about this access
Note : The Data has been taken by us , and will be sold other ways , here you will take only access and get the data yourself if you want data + access you have to pay us 5 BTC , if you have good team you can save 4 BTC and take it yourself but won't be easy to be honest

Shadow

Villa Salvaje

Session : 0585d8fb89403b88431f492446b01582efcf1fac563d38bb7e7456cdebca1b7250
TOX : 19EB008E71DFD15A6A76C243B2A3B251CE5889A0953010F0D9A576297816926C9908D2C9DD28

Quantum, PITI, darx and 3 others

Report Like Reply

blackfield's RAMP post

Source: ZeroFox Intelligence

The actor is well-known in RAMP with positive reputational scoring from other forum users, which likely legitimizes blackfield's claims for potential buyers. ZeroFox has observed blackfield predominantly targeting Israel-based assets, but the actor has also conducted attacks against U.S.-based entities or other NATO allies.

ZeroFox is unable to verify the access type and number of hosts blackfield is offering; however, analysis of the actor's post suggests it is likely root access and that the number of compromised hosts exceeds 1,000. Root access (also known as "superusers") grants a user unrestricted read, write, and execute privileges across an entire system; if used maliciously, an actor could significantly disrupt or exfiltrate data from company systems.

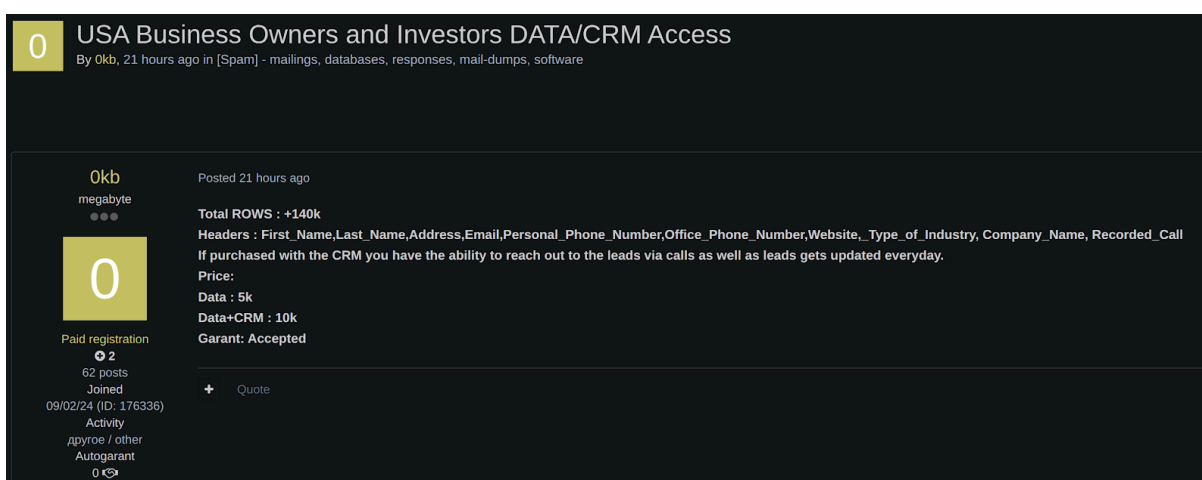
Dataset Containing U.S.-based Business Owners' and Investors' Information

On August 26, 2025, an actor using the alias "0kb" posted on the dark web forum Exploit, advertising alleged access to over 140,000 rows of customer relationship management

(CRM) data records containing information on U.S.-based business owners and investors. The actor priced the dataset at USD 5,000; the dataset plus the CRM access is priced at USD 10,000, with availability for buyers to pay escrow. The actor also claimed that the CRM access can be leveraged by buyers to contact leads directly via calls and receive daily lead updates. According to 0kb, the headers allegedly include:

- First and last name
- Address
- Email address
- Personal phone number
- Office phone number
- Website
- Industry type
- Company name
- Recorded call

Content management system and CRM compromises pose a significant risk to organizations, as they can provide malicious actors with direct access to thousands—or potentially millions—of contacts, depending on the size of the targeted company. Data exposed from CRM systems can be used in subsequent targeted spear phishing campaigns or result in financial losses, fines, lawsuits, and reputational damage.



The screenshot shows a ZeroFox exploit post. At the top, the title is "USA Business Owners and Investors DATA/CRM Access" by user "0kb", posted 21 hours ago. The post content includes: "Total ROWS : +140k", "Headers : First_Name,Last_Name,Address,Email,Personal_Phone_Number,Office_Phone_Number,Website,_Type_of_Industry, Company_Name, Recorded_Call", "If purchased with the CRM you have the ability to reach out to the leads via calls as well as leads gets updated everyday.", "Price: Data : 5k, Data+CRM : 10k, Garant: Accepted". On the left, the user profile for "0kb" is shown, indicating a paid registration, 62 posts, and a join date of 09/02/24.

0kb's Exploit post

Source: ZeroFox Intelligence

| New Infostealer Announced on Dark Web Forum

On August 16, 2025, an actor using the alias “KatzStealer” posted on the dark web forum Exploit, announcing the release of a new infostealer named “Katz Stealer”. Notably, the Katz Stealer infostealer allegedly has the following features:

- **Ultra-lightweight.** This likely means the malware is very small in size and uses minimal system resources, making it easier to bypass detection tools such as antivirus or endpoint detection and response (EDR).
- **High hit-rate.** This likely refers to the malware being very successful at either compromising targets or data exfiltration. A high hit-rate will very likely be attractive to cybercriminals aiming for high return on investment (ROI).
- **Requires no dependencies.** This likely references the infostealer being able to execute without needing to install or load external libraries or software, making deployment easier.
- **Build size is 30 KB to 100 KB.** This is a very small executable size in comparison to other infostealers (most are between 100–200KB), which will almost certainly enable faster download/execution.
- **Browser data extraction.** The infostealer reportedly can extract data from a broad range of modern web browsers such as Chrome, Edge, Opera, Brave, and Firefox, which will very likely maximize credential and session token theft (including passwords, cookies, and autofill data).
- **Targets over 90 cryptocurrency extensions.** There is likely a special focus on browser-based wallets such as MetaMask, Phantom, and Binance Wallet due to crypto theft being very popular among stealer-as-a-service (SaaS) operations.
- **Two-factor authentication.** As is becoming increasingly common among other SaaS services such as LummaC, the Katz Stealer infostealer offers two-factor authentication (2FA) as an added layer of security for users.

Stub technical information:**! ALL CIS are fully blocked !**

- Developed entirely in C/Assembly.
- Over 95% of the codebase uses custom libraries; no CRT, no STL, no default system libraries.
- Direct WinAPI usage for all system interactions.
- Ultra-compact: build size ranges from 30 KB to 100 KB depending on enabled functions.
- Tested on Windows 7–11, x32/x64, with latest updates.
- No dependencies, no installation required.
- Silent operation: does not kill browsers or generate any noise.
- Binary morpher: dynamic runtime string encryption/decryption and advanced control flow flattening techniques for evasion.
- Crypt is needed scantime without crypt, stealer is fully clean (FUD), but crypt is essential so the pure stub doesn't leak anywhere.
- Automatically Exodus and MetaMask brute-force using common passwords

KatzStealer's Exploit post

Source: ZeroFox Intelligence

According to KatzStealer, panel licenses for this new infostealer are available for USD 100 for one month, USD 270 for three months, and USD 480 for six months. This is competitive pricing, falling between mainstream infostealers like RedLine (approximately USD 100 to 150 per month) and premium variants such as LummaC2 (approximately USD 250 per month).

- As is common for most other infostealers, KatzStealer states in the post that using Katz Stealer against Commonwealth of Independent States (CIS) countries is prohibited.

Notably, the user "xorit" commented on KatzStealer's post, providing positive feedback about the service. Xorit noted that the stealer was built entirely from scratch in the programming language C/ASM, with the ability to bypass most antivirus solutions without any additional obfuscation or packers; most malware typically require this to aid in avoiding detection.

- Notably, KatzStealer's credibility can not be judged at this time as they only joined Exploit in May 2025.

Stub Collection information:

- Chromium & Gecko Browsers Cookies (+v130 Supported), Passwords, Autofill, oAuth tokens, CVV2, IBANs, Wallets Extensions (+90) and More
- Support most Hardware Wallet +15 (including Exodus, Atomic, and more)
- Support most messengers +5 apps (discord, canary token, tdata and more)
- Support most FTP +6 Clients (FileZilla, Totalcommander and more)
- Support most VPN Clients (OpenVPN, Mullvad and more)
- Support most Credentials +15 (Anydesk, Pidgin, Tox and More)
- Support most Passwords Manager +5 (1Password, NordPass and more)
- Support Windows CRM, Steam Memory Dump
- System Information, Running Process, Installed Applications, Desktop Screenshot
- Anti VM Detection & Anti Debugging

KatzStealer's Exploit post continued


Source: ZeroFox Intelligence



The Katz Stealer infostealer is likely to generate high interest among an array of financially motivated threat actors due to its alleged combination of stealth, efficiency, and accessibility. Its ability to bypass most antivirus solutions without the use of external packers or obfuscation reduces setup complexity while increasing deployment success rates. The lightweight build size, rapid data exfiltration speeds, and broad targeting scope (browsers, crypto extensions, and wallet apps) very likely make it well-suited for both mass deployment and targeted operations.

| Guide to Prevent Deanonymization and IP Leaks Posted on Dark Web Forum

On August 14, 2025, the actor "devilish" posted on the dark web forum Dread, providing a comprehensive guide to help operators of private websites prevent IP leaks and a method to help avoid deanonymization. Devilish's guide on preventing IP leaks on clear web rotators likely comprises measures to stop the rotators from exposing real IP addresses in order to ensure any browsing activity or ad campaigns stay private and secure.

- Devilish suggested that, if someone is using DDoS Guard as a budget-friendly distributed-denial-of-service solution, they should use IPTables to lock web ports 80 and 443 to only DDoS Guard's IP ranges in order to avoid IP leaks.
- The actor also attached a screenshot demonstrating a part of this process in the post.

 6

by  **devilish**  12 hours ago

Preventing IP leaks on clear-web rotators, here's the solutions.

We see a lot of [/d/newmarkets](#) candidates with clear-web mirrors or rotators, which is not a problem per-se, but we see a lot of them leaking IP's in very bad ways. If it's just a static page, it's mostly fine. But for a mirror to your market, that cannot roll, so here's the solutions and hopefully someone will read this.

If you're using DDOS Guard, which is the ideal solution, I recommend using IPTables to restrict your web ports 80 and 443 to only their IP ranges, ensuring no IP leaks can happen. How do you do this? Here's a small code snippet for you.

```
iptables -I INPUT -s 77.220.207.0/24 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 77.220.207.0/24 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 45.10.240.0/24 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 45.10.240.0/24 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 45.10.241.0/24 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 45.10.241.0/24 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 45.10.242.0/24 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 45.10.242.0/24 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 186.2.160.0/24 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 186.2.160.0/24 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 186.2.164.0/24 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 186.2.164.0/24 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 186.2.167.0/24 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 186.2.167.0/24 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 186.2.168.0/24 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 186.2.168.0/24 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 185.178.209.197 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 185.178.209.197 -p tcp --dport 443 -j ACCEPT
iptables -I INPUT -s 190.115.30.44 -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -s 190.115.30.44 -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 443 -j DROP
```

You must have IPTables installed, I assume you are smart enough to run "apt install iptables" and then to save your rules by running "apt install iptables-persistent" as root. If you're using Cloudflare, which is free but less recommended if you ask me, you need to do a little more work. You need to generate an SSL certificate for your origin server from their SSL/TLS panel in the dashboard, and save them somewhere. Download their origin CA certificate and enable Full (Strict) SSL protection, as well as authenticated origin pulls. Nginx config would have the following lines in it.

devilish's Dread post

Source: ZeroFox Intelligence

The tips and guidelines provided in devilish's post are comprehensive enough for a person well-versed in networking technology to understand. Researchers have observed several other guides on preventing deanonymization, but the additional tips on mitigating the risk of IP leaks on clear web rotators are not commonly discussed. Even though the guide does not apply to dark web domains, it is likely useful for private clearnet domains.

Several clearnet sites associated with illicit dark web marketplaces and forums have previously been dismantled by law enforcement:

- On July 22, 2025, European law enforcement agencies arrested the suspected leader of well-regarded Russian-language cybercrime forum XSS and took down its main website, [xss\[.\]is](#).
- In May 2025, the eXch cryptocurrency exchange, allegedly involved in money laundering and operating a criminal trading platform, was accessible on both the

clearnet and the darknet before it was targeted in a German law enforcement operation.¹

- A clearnet domain associated with prominent English-language dark web forum BreachForums was also available before both the marketplace and the website became inaccessible in April 2025, amid rumors of law enforcement campaigns and vulnerabilities in its infrastructure.

Devilish's guide is likely to gain traction with existing or potential illicit online marketplace operators seeking to secure their private websites or backup domains on the clearnet. With popular dark web marketplaces such as BreachForums and XSS facing operational disruptions, several new markets have come online in the cybercrime sphere. If the operators of these websites choose to have backup clearnet domains, they will very likely rely on guides like devilish's to evade law enforcement or prevent compromise by competing marketplaces.

Several threat actors also use clear web systems such as proxies, virtual private network endpoints, or traffic rotators to move money, store stolen data, or host phishing sites. They are likely to be interested in devilish's guide to help prevent IP leaks and avoid being unmasked, as taking these steps will likely make it more difficult for investigators to track their servers or real identities.

¹

[hXXps://www.bka\[.\]de/DE/Presse/Listenseite_Pressemitteilungen/2025/Presse2025/250509_exch_abgeschaltet.htm](https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2025/Presse2025/250509_exch_abgeschaltet.htm)

| 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%