



| Brief |

The Underground Economist: Volume 4, Issue 21

B-2024-12-19b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

December 19, 2024

Scope Note

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 9:00 AM (EST) on December 19, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 21

Threat Actor Announces Zero-Day Vulnerability for Sale

On December 16, 2024, untested threat actor “Chrome0Day” posted in the Russian-speaking dark web forum Exploit advertising an alleged remote code execution (RCE) zero-day vulnerability affecting the Google Chrome and Microsoft Edge web browsers. Chrome0Day also requested information surrounding bug bounty companies that would be interested in buying the vulnerability but specified they must pay in cryptocurrency and not require personal details in order to issue a reward. Chrome0Day added that those able to provide contact information would receive compensation. The vulnerability is also available for purchase by any interested party for a price of USD 100,000, likely via the private Telegram channel link Chrome0Day included in the post.

Posted 10 hours ago

I have found a 0-day vulnerability in Chrome/Edge.

If you know any credible bug bounty firm that pay in crypto and won't scam me after I disclose the vulnerability and it gets patched, please send me their contact details. I will offer a finder's fee only if they can pay in crypto. The firm must not require any personal information from me in order to be eligible for the reward once the vulnerability is patched.

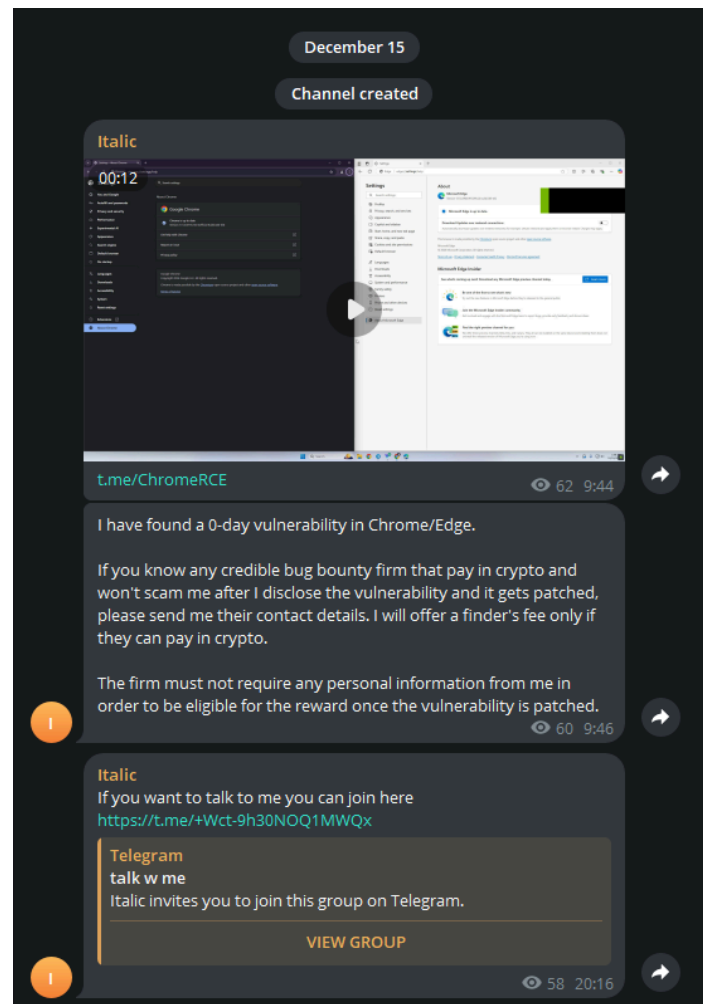
If you are wanting to buy yourself, then you must be trusted or show proof of funds so I know you won't scam me.

I don't see an option to upload a video here, but the proof of concept is in here: t.me/ChromeRCE

Price: \$100k+ Crypto ONLY

Chrome0Day's exploit[.]in post advertising zero-day vulnerability

Source: ZeroFox Intelligence

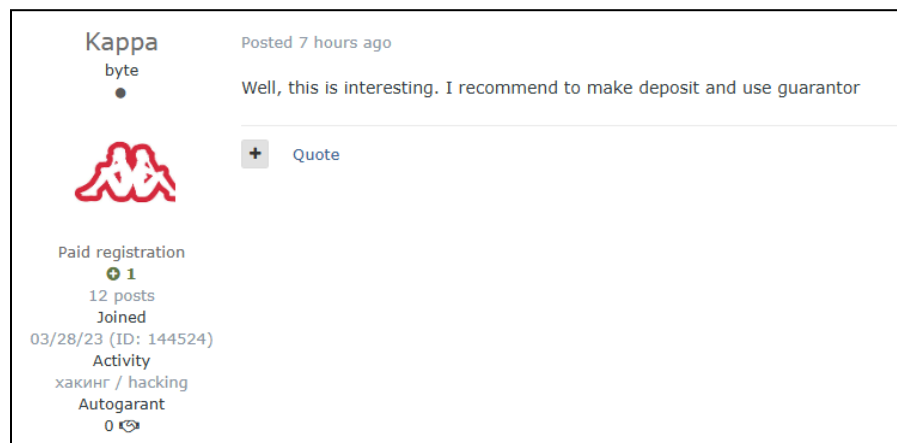


Chrome0Day's linked Telegram channel

Source: ZeroFox Intelligence

The Telegram channel contained a video that allegedly features a limited demonstration of the vulnerability being exploited. In the video, opening a file named "heap.html" with either Google Chrome or Microsoft Edge appeared to execute the Windows Calculator application. However, it is not clear from the rendered content what HTML code is inside the file.

The Exploit post received good feedback from the actor “Kappa”, who has a positive reputation in the forum. Kappa advised Chrome0Day to make a financial deposit on the community and to offer the use of an escrow guarantor, almost certainly to increase the perceived reliability of both the actor and the vulnerability.



Response from Kappa

Source: ZeroFox Intelligence

ZeroFox has observed numerous advertisements of zero-day vulnerabilities in Russian-speaking deep and dark web (DDW) forums during 2024, though many are very likely attempts to scam buyers. Chrome0Day’s intent to sell the vulnerability to a bug bounty program is reflective of increased credibility—and if the use of escrow is offered, there is a likely chance that it will be purchased.

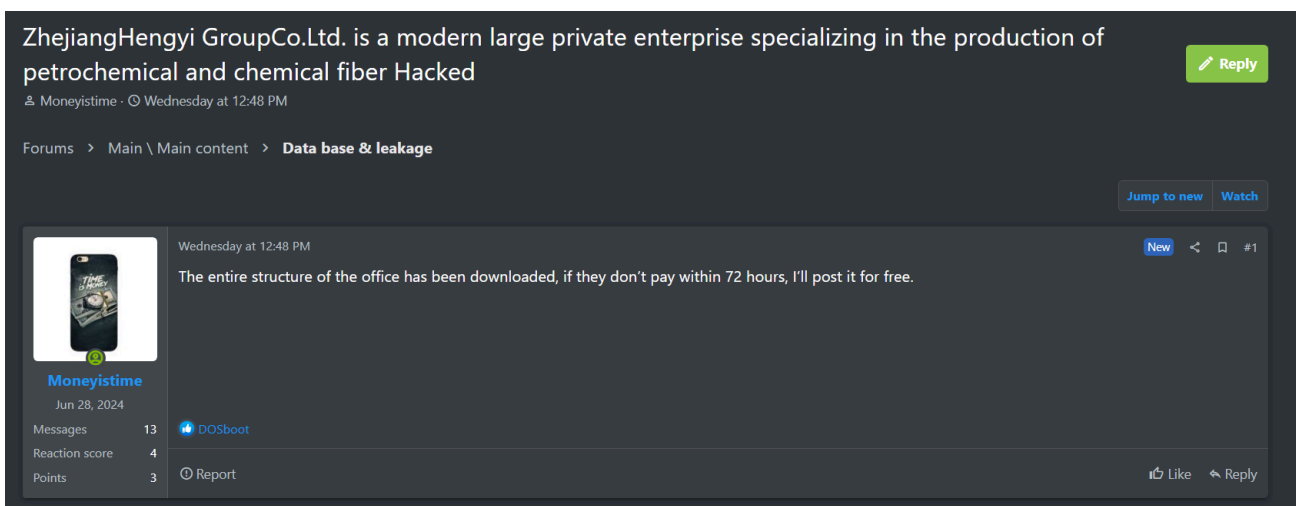
Russian-Speaking Cyber Criminal Admits Targeting Chinese Entity

On December 11, 2024, well-regarded actor “Moneyistime” posted in the Russian-speaking dark web forum RAMP, claiming to have successfully breached and exfiltrated data from a Chinese petrochemical and chemical fiber production organization.

Moneyistime claimed that the stolen data would be posted in the forum and made available for free if the organization did not meet their extortion demands within 72 hours. No data has been published as of the writing of this report, indicating a very likely chance

that the ransom was paid. If this is the case, it would be a notably rare instance of details surrounding the targeting of a Chinese entity by a Russian-speaking actor being announced publicly in a Russian-speaking forum.

While many Russian-speaking forums forbid the targeting of entities located in the Commonwealth of Independent States (CIS), they do not explicitly prohibit the targeting of China-based entities. Instead, such activity is considered unusual and misaligned with many of the “norms” that govern such marketplaces. There is a likely chance that such events—specifically, the lack of moderator or peer repercussions—will result in targeting of China-based organizations being perceived as increasingly permissible, particularly given that China is already almost certainly viewed as a highly lucrative environment within which to operate.



Moneyistime's RAMP post advertising extortion of Chinese entity

Source: ZeroFox Intelligence

Geopolitical factors almost certainly influence both the written rules and unwritten norms that govern DDW forums and marketplaces. Recent events have increased strain on Russia-China relations: namely, China's reluctance to overtly support Russia in the ongoing Russia-Ukraine conflict, Chinese compliance with some Western sanctions targeting the Russian economy, and suspected Chinese cyber activity targeting Russian government entities throughout 2024. This gradual shift in perception and permissibility is also very likely to result in an increased demand from buyers seeking Chinese information.

| Dark Web Actors Announce Mass Sale of Network Access

Since 2023, ZeroFox has observed a significant uptick in initial access broker (IAB) bulk sales on the dark web, a trend which has continued throughout the end of 2024. These sales have been conducted by both untested and well-regarded actors and likely correlate with the increased use of corporate-access brute checkers.

On December 7, 2024, untested actor “antigov” announced the sale of more than 200 instances of network access to Indonesian government entities associated with the desa[.]id domain on the Russian-speaking dark web forum xss. The compromised network nodes allegedly contained unspecified sensitive information regarding Indonesian President Prabowo Subianto’s administration. The actor stated that a single sale to one buyer would occur and listed a non-negotiable price of USD 19,000. Although this price is notably high for an Indonesian-based target, antigov claimed that the purchase includes a “lifetime access warranty” as long as the domain remains on its current server.

- The desa[.]id second-level domain (SLD) first launched in 2013 in order to provide an online presence for Indonesian village-level government entities—the smallest level of government in the country. At the time, most village-level government entities reportedly could not utilize the go[.]id SLD, which was reserved for district and city-level governments.¹

¹ [hXXps://www.beritasatu\[.\]com/news/111315/domain-desaid-diluncurkan-untuk-promosikan-potensi-desa](https://www.beritasatu.com/news/111315/domain-desaid-diluncurkan-untuk-promosikan-potensi-desa)

Root access to over 200+ Indonesian administrative government desa.id

antigov · Суббота в 03:11

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

Новая сделка



antigov
флорид-диск
Пользователь

Регистрация: 04.12.2024
Сообщения: 6
Реакции: 0

Суббота в 03:11

Цена: \$19,000
Контакты: Direct message on site or

Hello XSS !

Today, I am offering root access to over 200+ Indonesian government administrative (desa.id).
Access will be sold only once.

Privilege you will receive:

- Full root access to all server
- Defense services for all access
- Secret administrative document / presidential document
- Lifetime access warranty (as long as they are not moved to another server)

Price: \$19,000

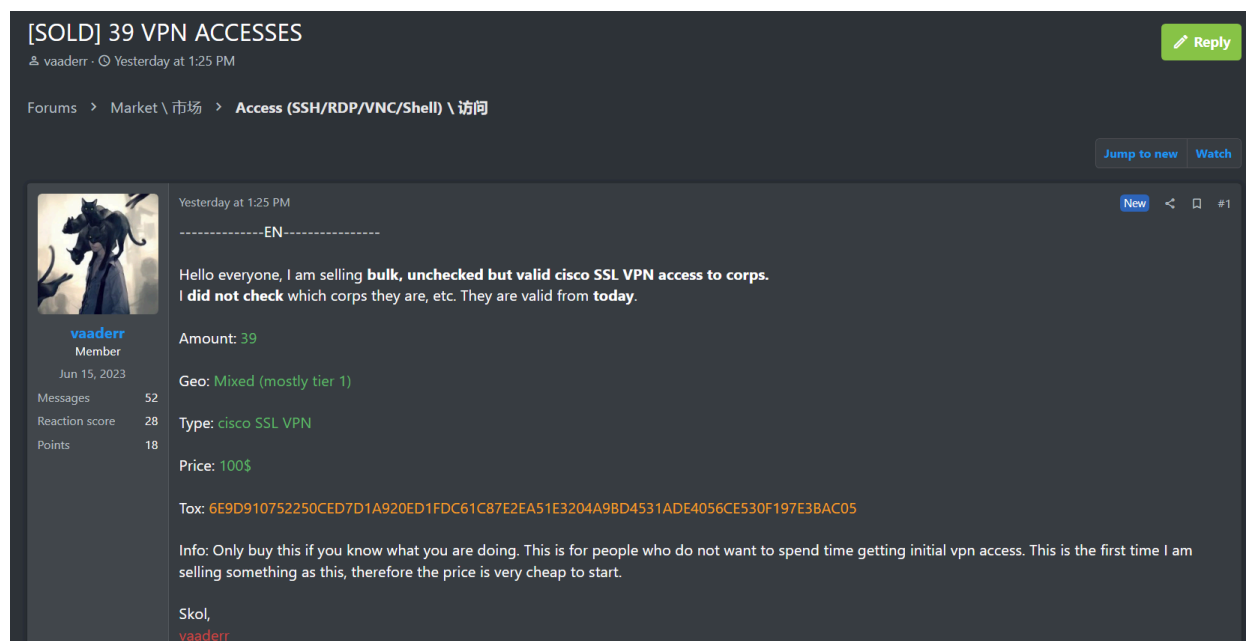
PRICE IS NOT NEGOTIABLE !

* Please provide proof of funds for further details before asking me to proof the access
* Serious Buyer ONLY
* Contact me directly here or on Telegram: <https://t.me/pemaw>
* Deals only with XSS ESCROW

Antigov's xss post advertising Indonesian government network access

Source: ZeroFox Intelligence

Antigov claimed that the buyer would receive root access to the server, which allegedly provides the highest level of authentication and administrative privileges. This level of access would likely allow a buyer to maintain complete control over the server, including modifying or disabling security protocols. Although antigov is an untested actor, their intent to only conduct sales via the forum's escrow service indicates there is an increased chance this is a legitimate advertisement.



Vaaderr's RAMP post advertising Cisco SSL VPN access

Source: ZeroFox Intelligence

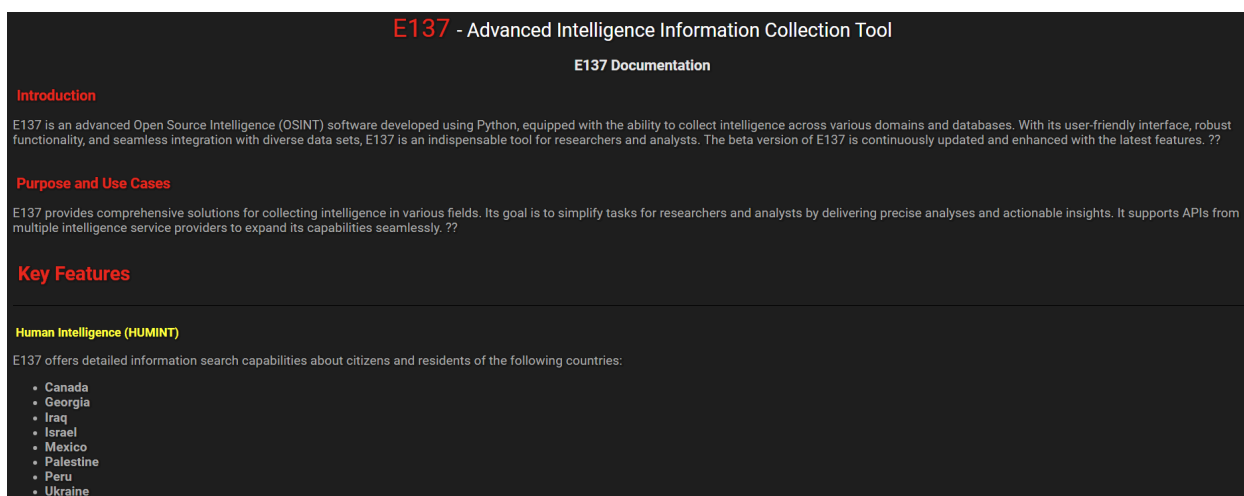
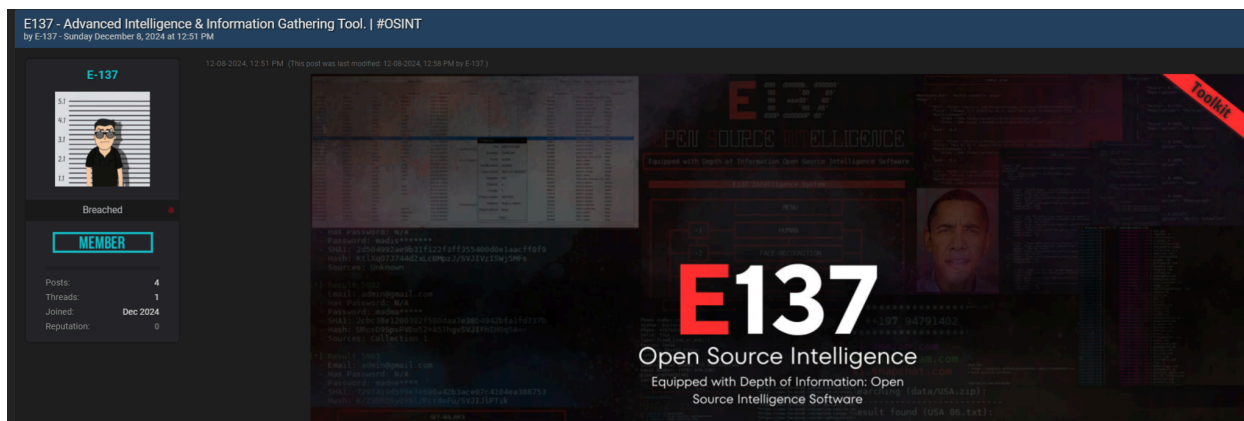
Dark Web Actors Advertise New Automated OSINT Tools

ZeroFox continues to observe an increased demand for automated Open Source Intelligence (OSINT) tools amongst DDW threat actors. While OSINT tools are commonly utilized for licit activity in a variety of industries, malicious actors have capitalized on the tools' advanced data collection capabilities for personal profit and to encourage subsequent illicit activity. ZeroFox assesses that the DDW market for these tools will continue to increase in the early months of 2025.

On December 8, 2024, untested actor "E-137" advertised a custom OSINT tool dubbed "EI37" that can reportedly gather information from numerous databases and domains across the web. E-137 states the purpose of their self-titled tool is to "provide comprehensive solutions for collecting intelligence in various fields" and to "simplify tasks for researchers and analysts."

- In addition to EI37's own data repositories, the custom tool reportedly integrates a variety of separate free OSINT tools into its platform (such as Spiderfoot, Web-check, and Recon-ng) and includes the ability to support Application

Programming Interfaces (APIs) from several undisclosed intelligence service providers.



E-137's post advertising custom OSINT tool

Source: ZeroFox Intelligence

In the post, E-137 highlighted the various advanced features of the tool, including its alleged ability to collect personally identifiable information (PII) pertaining to citizens of Canada, Ukraine, Georgia, Palestine, Israel, Iraq, Mexico, and Peru. E-137 further claimed that the tool can be customized to pull citizen PII for additional countries as desired.

- Of note, the section discussing the PII collection ability is listed under a heading titled "Human Intelligence (HUMINT)". While this could be interpreted in the traditional Intelligence Community (IC) sense that the data was derived from human sources, it also could be interpreted as the actor misunderstanding the

definition of HUMINT and instead defining it as the intelligence collected on individuals—including PII.

In addition to its primary function of collecting PII, E137 allegedly provides the following search functionalities and features, supported in part by a variety of supplemental OSINT tools:

- Search functionality for PII such as email addresses, telephone numbers, usernames, and social media accounts
- Search functionality for personal financial information (PFI) such as associated credit card information—including card type, issuing institution, and currency code—based on a provided card's Bank Identification Number (BIN)
- Search functionality for records associated with cryptocurrency addresses via blockchain networks
- Facial recognition technology to identify a target and accurately capture their online presence
- Web infrastructure data collection, including WHOIS information, Autonomous System Number (ASN) details, Secure Sockets Layer (SSL) certificate analysis, port scanning, subdomain discovery, and Domain Name System (DNS) queries
- Automated metadata extraction

Web OSINT

E137 offers comprehensive web intelligence gathering capabilities, including:

- Email scanner
- Ownership duration
- Hosting provider
- Redirect checks
- Port scanning
- Website security analysis
- Bypassing Cloudflare protection
- Subdomain discovery
- Network range analysis
- ASN details
- WHOIS data
- IP information
- DNS queries
- SSL certificate analysis

Top 3 Tools

E137 integrates popular tools such as:

- **Recon-ng:** Broad functionality for collecting, organizing, and analyzing online and offline intelligence.
- **Spiderfoot:** Automatic intelligence gathering on domains, IPs, and email addresses for detailed footprint analysis.
- **Web-check:** Scans web applications for vulnerabilities, misconfigurations, and weaknesses, providing detailed reports.

Contact Information

If you are interested in the E137 toolkit, feel free to contact me for more information:

- **Telegram:** @Ex137

Note: To keep this brief, some features are not listed. For detailed information, please refer to the documentation: [E137 Documentation](#)

You can also explore similar projects on my Telegram channel: [@infosbyte](#)

It is open to negotiation and will be sold to more than one person.

Price: 2500 \$

Details of several of E137's capabilities

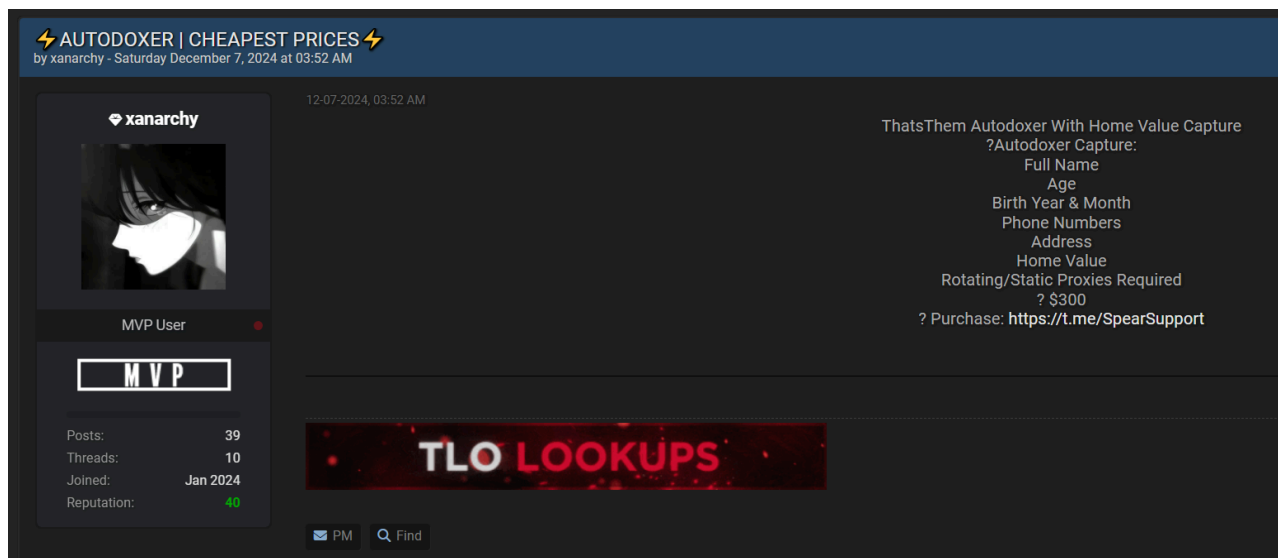
Source: ZeroFox Intelligence

According to E-137, the tool will be sold to multiple buyers for USD 2,500 each, though the price is negotiable. The high asking price for the tool almost certainly reflects the myriad of advanced capabilities it allegedly offers. Additionally, the inclusion of less common abilities—such as pulling credit card data based on BINs, finding records associated with cryptocurrency addresses, and automating metadata extraction—increases the value and utility of the tool.

- Despite E-137's curated mention of licit use cases, the tool provides threat actors with the ability to conduct numerous illicit follow-on activities—including Business Email Compromise (BEC), financial theft, distributed denial-of-service (DDoS) attacks, and doxxing.

ZeroFox observed another automated OSINT tool on December 7, 2024, when positive-reputation actor “xanarchy” posted in the deep web forum BreachForums advertising a new custom automated doxxing tool dubbed “ThatsThem” for USD 300. The tool is allegedly capable of collecting a target's PII, including their full name, age, birth month and year, telephone numbers, home address, and home value. The latter

functionality indicates there is a likely chance that the tool extracts data from public databases related to consumer reports.



Xanarchy's BreachForums post advertising automated doxxing tool

Source: ZeroFox Intelligence

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%