



| Brief |

The Underground Economist: Volume 4, Issue 19

B-2024-11-22a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor, Malware,
Ransomware and Digital Extortion

November 22, 2024

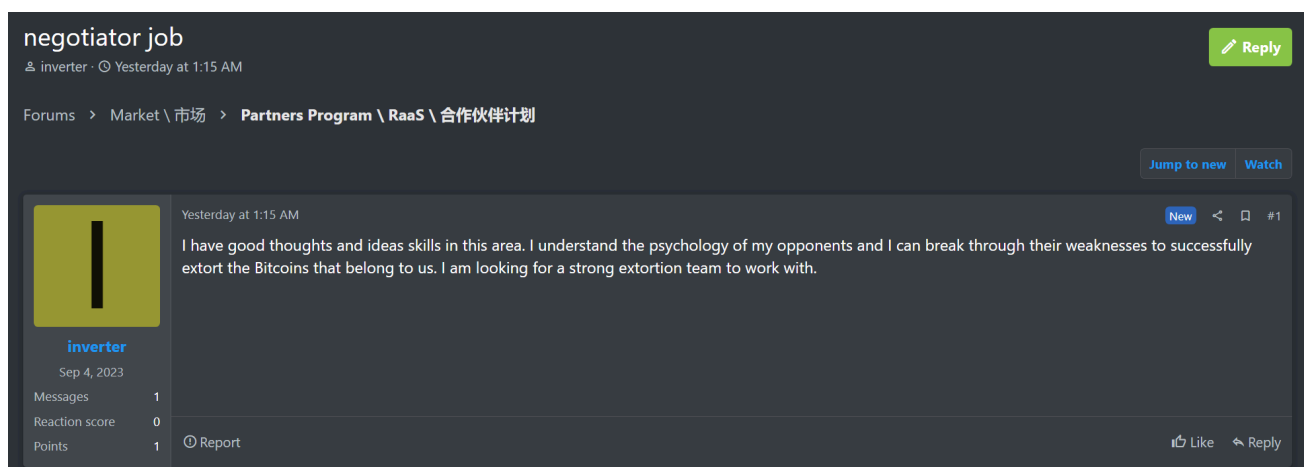
Scope Note

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 November 22, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 19

Extortion “Negotiator” Seeks Employment in Dark Web Forum

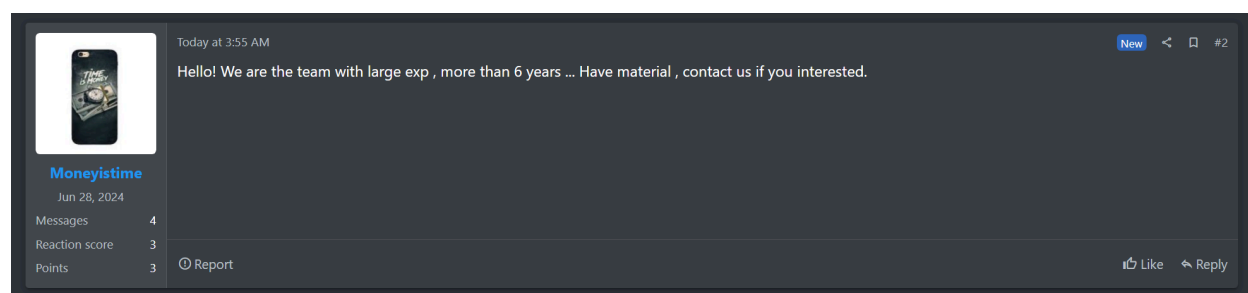
On November 17, 2024, an actor with the alias “inverter” posted in the Russian-speaking dark web forum RAMP announcing they were seeking employment with a ransomware collective. Inverter, who has an untested reputation in the forum, detailed that they could work as a “negotiator” due to their ability to “understand psychology” and “break through” their victim’s weaknesses.



RAMP post by inverter seeking work as a negotiator

Source: ZeroFox Intelligence

Less than 24 hours later, the post received a reply from actor “Moneyistime” (who has a positive reputation in the forum) stating that their team would like to work with inverter. Moneyistime did not specify the name of their collective or operation but claimed to represent a team with more than six years of experience.



RAMP response by Moneyistime displaying interest in employing inverter

Source: ZeroFox Intelligence

Instances of ransomware and digital extortion (R&DE) actors seeking individuals to fill a negotiator-type vacancy are rare in deep and dark web (DDW) forums. While negotiation is a key aspect of R&DE attacks, from both the attacker's and victim's perspectives, the process is not typically conducted by a dedicated negotiator. Instead, it is often overseen by a member of the R&DE collective that is proficient in the victim's native language and has well-researched the victim's industry, likely payout propensity, and any relevant local legal guidance. There is a roughly even chance that a perceived need to employ a specialist role is reflective of anticipated large-scale operations resulting in drawn-out negotiations.

Inverter being almost immediately contacted by an alleged ransomware actor is very likely indicative of the continued issues that extortion collectives face with seeking and obtaining trustworthy and vetted affiliates. These difficulties have been exemplified by many threat actor posts throughout 2024. Following significant law enforcement (LE) operations earlier in the year, ZeroFox has observed multiple instances of R&DE collectives approaching hiring and affiliation with significantly increased scrutiny.

| Allegedly Functional Stripe Accounts Announced for Sale

On November 17, 2024, actor “Verdena77” posted in the dark web forum Exploit, advertising the sale of accounts for the payment processor platform Stripe. Verdena77, who has an untested reputation in the forum, claimed that the accounts are registered to U.S.-based business entities, which were very likely self-registered for purposes of bypassing Stripe’s know-your-customer (KYC) security protocols.

- As with similar online payment processing services, registering a Stripe account requires the provision of details associated with the applying individual and their associated business. This is often both for the purposes of preventing the platform’s misuse and satisfying regulatory requirements.

Such advertisements are rare in DDW forums, especially in comparison to that of other counterfeit and verification services. This is primarily due to the high-effort approach required to create numerous illegitimate accounts. Verdena77 did not specify the quantity available or the asking price, instead advising interested parties to contact them discreetly.

V

Verdena77

byte

•

V

Paid registration

0

4 posts

Joined

10/27/24 (ID: 180139)

Activity

кардинг / carding

Autogaran

0

SELLING USA STRIPE ACCOUNT SELF-REGISTERED 2-7 days payout

By Verdena77, 1 hour ago in [Payment systems] - exchange, sale, identification, distribution

Posted 1 hour ago (edited)

Self registered USA Stripe account for sale

Offering for sale high quality USA Stripe.com accounts

Details:

- self registered with USA Business information (LLC - INC)
- business domain
- business private email access
- website landing page
- ovpn/socks5 used for the access
- cookies
- possibility to have the access to the bank account linked to Stripe
- 7 or 2 days payout

All accounts are ready to be used

I'm open to evaluate your offers

If interested contact me in Private Message or telegram

t.me/verdena7

Exploit post by Verdena77 advertising Stripe accounts

Source: ZeroFox Intelligence

There is no evidence that Verdena77 or the advertised services are credible, and no feedback is available from buyers at the time of writing. However, if Verdena77's offerings are legitimate, they will almost certainly be of interest to an array of financially motivated threat actors seeking a method by which to conduct cashout and carding operations. Should an actor be in possession of stolen personally identifiable information (PII) and personal financial information (PFI), an unattributable Stripe account will increase their chances of successfully stealing funds.

| New Drainer-as-a-Service Announced in Dark Web Forum

On November 8, 2024, actor "DRAIN" posed in the dark web forum Exploit announcing the launch of a new drainer-as-a-service with seemingly comprehensive features. DRAIN is newly registered to the forum but has already established a positive reputation.

- A drainer-as-a-service is a malicious offering designed to enable the theft of cryptocurrency from user wallets. While their techniques vary, drainer-as-a-service offerings typically employ ready-to-use malicious scripts, phishing kits and anonymity services, and feature some form of technical support. These services can often be rented via either a subscription-based pricing model or payments made to the service provider based upon a proportion of profit.

DRAIN's service allegedly includes numerous features to assist the user in bypassing cryptowallet security protocols. Some of those highlighted in the advertisement include:

- "Complete transparency", which likely alludes to the users ability to view the tool's code and to control the operation to some extent. This is likely intended to reassure users of the tool's effectiveness and potential customization.
- Phishing features, such as the redirecting of victims to a fake domain impersonating their intended destination in order to steal input information, as well as ad-based phishing.
- Unspecified "active bypass methods" designed to bypass anti-fraud and other security measures.

New topic, What did we do with the updates?

t.me/Dra1nSupport

We Claim It! You Won't Find Anything Like This Anywhere Else.

Complete Transparency!

No more traffic loss / no more MetaMask red errors / Rabby bypass / Trust Wallet bypass / WalletConnect transactions with dynamic prompts! (Prompts do not auto-refresh but respond to wallet activity.)
You can see all your compiles with complete transparency! No hidden or obscured code—only clarity for users.

Why Are We Doing This?

The concept behind a drainer is straightforward, but it can become very complex in practice. That's why we're offering you the chance to see exactly what's happening, with insights into everything running in the background.
Don't think of this as just another piece of code to replicate—if it were that simple, we wouldn't be so open about it.

Like any work, there are challenges here too.

Who Are We?

We began working independently as a team five years ago. Over the past three years, we've refined our drainers, adding hundreds of unique features beyond what's available in the market.

Yes, we claim there's nothing like this.

With no bypass limits, it will work in every scenario.

You can test it; unlike other filters with arbitrary limits of \$50k-\$100k, we have 7 active bypass methods and are confident in their reliability.

We're open to new members, and you don't need previous stats to join.

To us, all members are equal—no one has special privileges.

We have completed our mission to be completely transparent to our users while protecting our system.

There is no direct access to the site, you can only register to the site with a ref code, and you can only log in to the site via ref or user id.

Otherwise, you will never be able to access the site.

Binance & Mexc & Coinbase :

These drainers are completely private, let's take a look at how they work.

The connections are made through the APIs of real URLs, for example, you will get a binance.com/parametres link, then you will spread that link to the users.
and if that victim logs into binance from that link, they will lose all their assets.

**** 1 Approval causes all assets to be lost, continuous approval is not required******Ddos & Ads Drainer :**

These are features that you can only use against your competitors, since they are costly for us, members who have reached a certain status will use them.
and you can't attack DRA1N users, we can detect which one is our user from the .js file and in this case the bot won't work against our own members.

But you can attack everyone else.

TrackerLink Certificated :

This is a feature that allows you to appear with the original domain in Google ads and then visit the fake site when the user clicks.

In the example ad, ether.fi will appear and when you click on the ad, you will be directed to fakesite.com.

Exploit post by DRAIN advertising drainer-as-a-service*Source: ZeroFox Intelligence*

Registrations to DRAIN's service were reported immediately after the thread's creation, likely indicating that some specific users were privately notified about its launch. Positive reactions were also quickly observed—including from actors with positive reputations, such as "aptget".

Pelazor
byte
●



Paid registration

1

11 posts

Joined

10/23/24 (ID: 179905)

Activity

кардинг / carding

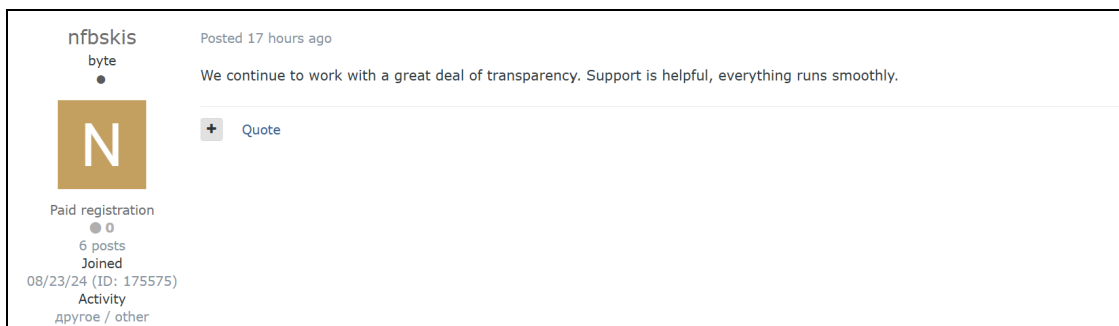
Posted 18 hours ago

Just completed the onboarding. Everything very smooth. Support responsive and helpful. So far it looks like a professional operation

+

Quote

Positive response to new drainer-as-a-service*Source: ZeroFox Intelligence*



Positive response to new drainer-as-a-service

Source: ZeroFox Intelligence

DRAIN's service cannot be purchased outright; only the option to rent is available. However, rather than buyers paying a monthly subscription fee, users pay a proportion of their profits to the developers. There is a very likely chance that DRAIN and their advertised service is credible and poses a threat to cryptocurrency holders globally. The comprehensive and advanced alleged features of the service are very likely indicative of innovation from increasingly professionalized threat actors, as well as an intent to lower technical accessibility requirements for would-be threat actors.

| Dark Web Actor Announces Malicious Chrome Extension for Sale

On November 4 and November 5, 2024, untested actor "PatrickDust" (on Exploit) and "patrick_star_dust" (on RAMP) posted in both Russian-speaking dark web forums advertising their new tool for rent dubbed "iNARi". The tool is allegedly a malicious, multifunctional extension for the web browser Google Chrome that utilizes the latest Chrome Extension framework Manifest V3. The requested price of the tool is USD 5,000 per month, plus a 10 percent profit-share to be paid to developers. This price is notably high and reflective of high expectations for iNARi's deployment.

Exhaustive features are not provided, but, according to the advertisement, iNARi is designed to redirect unsuspecting Chrome users to malicious domains, collecting sensitive user data such as credentials and email addresses, as well as session cookies. The tool is also allegedly able to bypass some security protocols, such as virtual private networks (VPNs), proxy servers, and other anti-fraud mechanisms.

Technical details

- Manifesto V3
- Bidirectional communication via websockets (holds load)
- Dropper for Windows in C# (hidden installation via patching chrome files), current detections 0/26 ([avcheck](#))
- Convenient control panel (web interface)
- Loadable injects (an attack vector can be developed and implemented after infection)

Details of cooperation

1) Product cost: rent \$5000 /month + 10% of profit. We understand that everyone has different verticals, so the payment format is discussed with each partner individually. The cost includes:

- Extension
- Dropper for Windows
- Dedicated infrastructure for each client
- Regular updates and technical support
- Help and advice on integrating your injects into our tool

2) Development of injects for your tasks is discussed individually, as it takes some time (depending on the complexity of the inject)

3) Start of cooperation: write in PM or TG, specify the vertical and method of monetization. We discuss improvements and adaptation of functionality, if necessary. We create a separate chat, where we will interact in the future. We deploy the infrastructure and get to work.

Features of Malicious Chrome Extension

Source: ZeroFox Intelligence

The apparent comprehensive approach is reflective of a diverse tool which—if legitimate and functions as advertised—offers the attacker the ability to exploit a large number of Chrome-based threat vectors and can lead to subsequent data theft, network compromise, or malware deployment. Although malicious browser extensions have been available for purchase or rent in DDW forums for a long time, the versatility and apparent sophistication of iNARi appears indicative of threat actor innovation.

| 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%