



Brief

The Underground Economist: Volume 3, Issue 25

B-2023-12-22a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Ransomware, Deep and Dark Web

December 22, 2023

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 22, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 3, Issue 25

| Network Access Sale Linked to Chandrayaan-3 Mission

On December 6, 2023, network access broker RobinHood announced on Russian-language dark web forum RAMP the sale of likely network access to an unnamed India-based enterprise in the Defense and Aerospace sector. The compromised organization is alleged to have “active ongoing main partnership with recent *[sic]* achieved India moon landing mission Chandrayan-3.” The price requested is USD 5,000. The post states that access includes:

- Remote Desktop Protocol (RDP), AnyDesk, and user logins
- Over 30 terabytes of data

Judging from the long-standing positive reputation of RobinHood, the post likely represents a legitimate network access sale. RobinHood is also willing to accept escrow at the buyer’s expense—a positive indicator of an actor’s reliability. The advertised access is very likely designed to appeal to Russian ransomware and digital extortion collectives, as the forum was built and is dominated by Russian-speaking actors. High-profile targets on the network access market—particularly those with geopolitical implications—often draw widespread attention from extortion collectives.

- The targeted company's partnership with Chandrayan-3 will draw threat actors that are keen to hit back at organizations contributing to the success of Russia's competitors.
- The access broker RobinHood is very likely linked to the recently-announced Kuiper Ransomware-as-a-Service (Raas) operation.



[SELLING] RDP // LA // INDIA DEFENSE AEROSPACE

👤 RobinHood · 🕒 Wednesday at 6:26 AM

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



KUIPER
posting...

Wednesday at 6:26 AM

Geo: INDIA
Sector: Defense and aerospace
Access: RDP
Privileges: LA

Includes:
RDP, AnyDesk, +30 clear text creds domain\user\pass (Access to multiple hosts over network)

Info:
+30TB of data just counting FS machine.
Active ongoing main partnership with recent "achieved" India moon landing mission Chandrayan-3

Price: 5k

Escrow preferred if not old client.

👤 mineissorryforme and achillesec

RobinHood
Member
Feb 18, 2023

Messages 35
Reaction score 19
Points 8

RAMP post advertising access to an Indian Defense and Aerospace Organization

Source: ZeroFox Collections

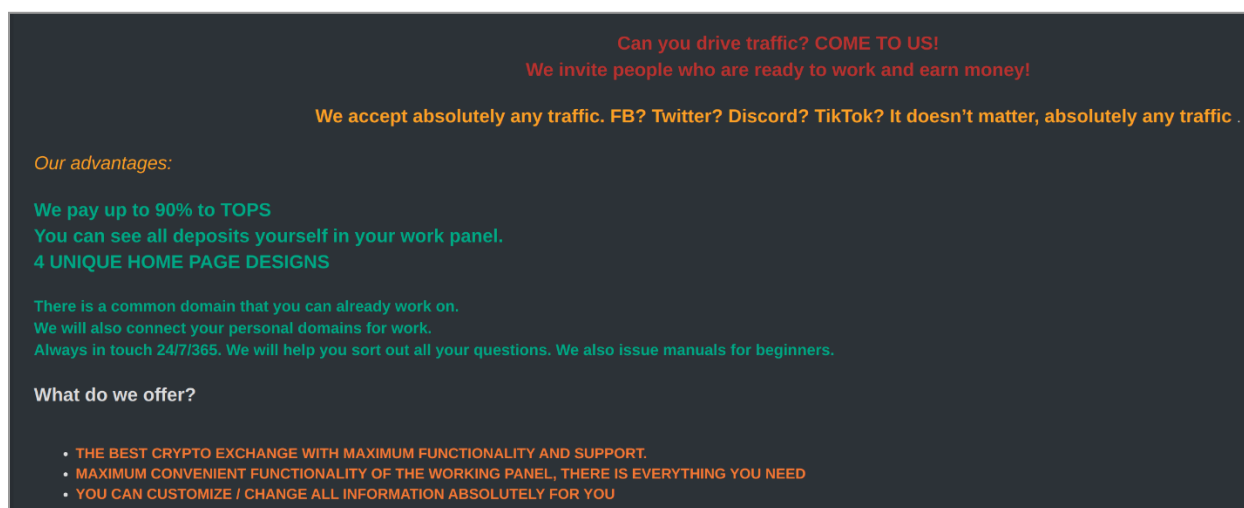
| New Crypto Scam Platform Announced in Dark Web Community

On December 7, 2023, untested Russian-speaking threat actor NoMoneyNoLife announced a yet-unnamed, new crypto scam platform in dark web community "Gate2Dark." The platform functions as a fake cryptocurrency exchange and encompasses many functions typically utilized in legitimate counterparts.

The post claims that the threat actor is searching for affiliates who can drive traffic to the platform so that victims register and deposit/transfer funds into the scam exchange. These roles are very likely similar to those undertaken by affiliates of Raas operations,

though likely much less sophisticated. Affiliates are also provided with a manual to guide their progress on the platform.

- The post advises that successful “traffic” specialists can receive up to 90 percent of the funds stolen in crypto scam attacks leveraging the platform. Amongst Raas affiliates, this percentage is very likely considered a high payout rate.



Can you drive traffic? COME TO US!
We invite people who are ready to work and earn money!

We accept absolutely any traffic. FB? Twitter? Discord? TikTok? It doesn't matter, absolutely any traffic .

Our advantages:

We pay up to 90% to TOPS
You can see all deposits yourself in your work panel.
4 UNIQUE HOME PAGE DESIGNS

There is a common domain that you can already work on.
We will also connect your personal domains for work.
Always in touch 24/7/365. We will help you sort out all your questions. We also issue manuals for beginners.

What do we offer?

- THE BEST CRYPTO EXCHANGE WITH MAXIMUM FUNCTIONALITY AND SUPPORT.
- MAXIMUM CONVENIENT FUNCTIONALITY OF THE WORKING PANEL, THERE IS EVERYTHING YOU NEED
- YOU CAN CUSTOMIZE / CHANGE ALL INFORMATION ABSOLUTELY FOR YOU

Gate2Dark post advertising new Crypto Scam-as-a-Service offering

Source: ZeroFox Collections

The threat actor noted that the platform can be outfitted with different designs, as well as linked to affiliates’ own domains, and that further customization can be carried out in order to fit users’ own targeting approach. Other advertised features include:

- The logging of all victim actions
- Metamask integration via seed phrase phished from victim
- Platform support to victim in order to remain undetected for as long as possible
- Access to future updates and features

EXCHANGE FUNCTIONAL:

- — Personal domains
- - FAST PUMP/DUMP
- — The ability to buy mammoth crypto from your bank card directly on the exchange
- — Staking
- — Inflated P2P
- — Support on your or our side
- — Automatic support responses.
- — Logging of all client actions
- — Various errors in output, + text editing
- Connecting MetaMask (Seed)
- The project is frequently updated, new features are added.

No experience? No problem, we even take beginners. The main desire

is to work with us, not for us! Human attitude and mutual understanding. BEST% ON THE MARKET!

Gate2Dark post advertising features of new Crypto Scam-as-a-Service offering

Source: ZeroFox Collections

The proliferation of RaaS, access-as-a-service (AaaS), and malware-as-a-service (MaaS) in deep and dark web marketplaces in recent years is likely indicative of the lucrative opportunities and efficiency of as-a-service offerings. Crypto Scam-as-a-Service offerings are likely to pose an increasing threat to cryptocurrency users and legitimate platforms, with a roughly even chance that they require less expertise to operate than other as-a-service offerings.

| Data Protection Legislation Set to be Leveraged in BlackMail of Victims

On December 16, 2023, untested threat actor hackerGPT announced that they will lead a team of “data hunters” to target victims set to be penalized by specific data protection legislation. Posting on dark web platform RAMP, hackerGPT implied that they have already begun to act, but a lack of exploitable network access has forced them to enter the access-brokering market. They are now seeking the services of corporate network access dealers, though allege that they are competent enough to exploit the initial foothold, once established, and exfiltrate data.

APT team in search of corporate access

hackerGPT · Saturday at 10:49 PM

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

Jump to new Watch



hackerGPT
Nov 26, 2023

Messages	1
Reaction score	0
Points	1

Report

Saturday at 10:49 PM

New < > #1

We position ourselves as data hunters. Our goal is documentation, for the leakage of which the company is obliged to pay fines as a percentage of its turnover. Due to the lack of material, it was decided to go public in order to find several partners who could provide our team with the necessary amount of access to corporate networks. The quality of access processing is very high, bypassing all security systems that exist today. For serious partners, more detailed information in PM.

Like Reply

hackerGPT post seeking Access-as-a-Service Brokers

Source: ZeroFox Collections

The post alludes to specific data protection legislation that governs the penalization of organizations that experience data leaks and the subsequent fines, which are based on a percentage of the organization's revenue. As a company's revenue is often publicly available, threat actors are able to negotiate a ransom demand by allowing the buy-back of stolen data at a cost likely just below that of the fine.

Threat actors conducting this form of data kidnapping (data exfiltration omitting the deployment of ransomware) are likely to prioritize European Union (EU)-based companies that are subject to the General Data Protection Regulation (GDPR), which can systematically enforce fines.

- U.S.-based organizations will also likely be targeted in this manner, though data protection legislation governing them is less comprehensive. This likely means that attacks would target organizations falling within different, industry-specific data protection legislation. This would very likely require additional research and effort by threat actors.

- U.S.-based organizations that handle the data of EU residents are also likely to be prioritized as targets, due to their subjection to GDPR.

Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies, with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- 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.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| 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%