



| Brief |

The Underground Economist: Volume 4, Issue 18

B-2024-09-19a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web

September 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 (EDT) on September 19, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 18

Threat Actor Seeks Collaborators for Ethereum Wallet Attacks

On September 15, 2024, actor “mastermind1983” announced in the deep and dark web (DDW) forum Exploit that they are seeking collaborators for the execution of a “worldwide robbery” of Ethereum wallets. According to the post, the actor has collated 40,000 Ether (ETH) addresses, each of which has a balance above USD 45,000.

- Ethereum is a decentralized blockchain, for which ETH is the native cryptocurrency used for a variety of transactions and applications.

Mastermind1983 claimed that they have the ability to not only link ETH addresses to specific wallets but also to access the wallet owner’s personal information, such as their name and address. However, mastermind1983 claims they lack the capability to exploit this information; they are therefore seeking “professionals” able to target the wallets with brute force attacks in order to obtain seed phrases and private keys before stealing funds.

- In comparison to other cryptocurrencies, ETH is often considered lacking in many security and anonymization features. By operating on a public ledger such as Blockchain, ETH users are exposed to an increased risk of transactions being identified and linked to identifiable information.

- This risk is exacerbated when ETH users submit their personally identifiable information (PII) to third-party platforms in order to satisfy know-your-customer (KYC) policies or publicly associate their wallet addresses with personal or location information on social media platforms.

M**[HAVE \$500M+ CONFIRMED ETH ADDRESSES] [NEED TEAMS WORLDWIDE ROBBERY]**

By mastermind1983, 18 hours ago in [Job] - search, execution of work

Posted 18 hours ago (edited)

I have data (40,000 Records above \$45,000) confirming the eth address of hundreds of thousands of user in crypto, their balance, and doxx/home address, also have the knowledge to confirm if they are using metamask/trezor/ledger/other wallet, can do extensive research on the victim

I am looking for professionals, if you know them, we can work all they need to do is force entry, and gain wallet seedphrase/private key as the dump is DeFi

Exploit post by mastermind1983 advertising brute checker tool*Source: ZeroFox Intelligence*

The actor included a sample line of information in the post that displays an ETH address and its alleged owner's name, email address, and address. The format of the sample indicates there is a likely chance that at least some of the information obtained originated from unspecified database dumps.

Although obtaining Ethereum wallet addresses and linking them to PII does not require particularly sophisticated research techniques, mastermind1983's claim to have obtained such a large number of them—all with significant balances—is rarely observed in DDW forums.

Mastermind1983 carries very little reputation in the forum, though ZeroFox observed a significant Bitcoin deposit with the escrow service, which is a positive credibility indicator. If the advertisement is legitimate, it very likely reflects an imminent danger to Ethereum users. However, the "worldwide robbery" advertised is unlikely to materialize due to the likely difficulties that would be encountered in brute forcing thousands of 256-bit private keys, processing and storing them, and extracting funds from thousands of wallets simultaneously.

| Brute Checkers Targeting Corporate Networks Announced for Sale

So far in September 2024, ZeroFox has observed the emergence and advertisement of two separate brute checker tools designed to target corporate networks. Both announcements were made in the DDW forum Exploit and offer the full source code for the product rather than a software-as-a-service (SaaS) model.

- A brute checker is a type of malware which, once deployed on a victim network, seeks to gain access to various software such as applications, email accounts, cryptocurrency wallets, cloud storage services, or social media accounts.
- The techniques and features leveraged by brute checkers sold in DDW forums vary significantly. Lower-sophistication tools often use brute force techniques to guess correct credentials and passwords. Others leverage predefined dictionaries or username-password combinations obtained from malicious stealer logs.

On September 15, 2024, untested actor "Fix" announced that they are selling the source code for a brute checker tool that is capable of multithreading and targeting applications popular in corporate environments, such as Citrix, Outlook Web App (OWA), and RDWeb. The asking price is USD 375, and enquiries are made by the encrypted messaging platform Tox.

Posted 18 hours ago (edited)

Hello friends, I want to present to your attention the checker of corporate networks and more.

We work to facilitate many processes, always approach our business with creativity and responsibility, quickly solve tasks - this means that our product can be trusted.

Advantages:

- * **Stable operation in multithreading.**
- * **Does not allow skipping lines.**
- * **Complete source code - which means that all your logs are only with you.**
- * **Easy configuration.**
- * **Quick response and solution to your problem.**
- * **Low price on the market.**

Exploit post by Fix advertising brute checker tool

Source: ZeroFox Intelligence

On September 13, 2024, an actor known as "kiberphant0m" (who has a positive reputation in Exploit) announced for sale of the source code for a brute checker that is

designed to specifically target unprotected remote desktop protocol (RDP) ports. This tool was advertised for USD 350, also a relatively low price for the source code.

The tool is capable of targeting both Windows and Linux networks and is allegedly able to bypass “honeypots”, which likely refers to various isolated, monitored networks that often mimic parts of a network that are deemed high-value to threat actors. Other alleged features include multithreading, memory optimization, and the inclusion of combolists.

Selling Golang RDP Bruteforcer (RUNS ON WINDOWS AND LINUX) -- NO HONEYPOTS OR FALSE POSITIVES!

kiberphant0m · Пятница в 07:29 · brute bruteforce bruteforcer golang golang brute rdp rdp access rdp brute rdp bruteforce rdp bruter

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

+ Новая сделка



kiberphant0m
RAID-массив

Пользователь

Регистрация: 07.01.2024
Сообщения: 65
Реакции: 4
Гарант сделки: 2

Пятница в 07:29

Цена: 300\$
Контакты: <https://t.me/cyb3rph4nt0m>

Selling Golang RDP Bruteforcer (RUNS ON WINDOWS AND LINUX)

Details:

Multi-Threaded Support. (Golang uses semaphores)
Cross-Platform Compatibility: Both Windows and Linux (any OS).
Telegram Bot Notifications. (Get notified of successful brutes in real time, eliminating the need to check manually)
Real-Time detection of RDP (Does not log honeypots).
Never a false positive!

Exploit post by kiberphant0m advertising brute checker tool

Source: ZeroFox Intelligence

Neither advertisement specified any restriction on sales, indicating a likely chance that sales could be made to numerous buyers. The tools are very likely to appeal to a wide range of threat actors that require initial network access to conduct further malicious activity; this includes the exfiltration of data that can be sold or leveraged to conduct subsequent social engineering attacks or the deployment of further malicious software, such as ransomware. While brute checker tools have been less prominent in DDW forums so far in 2024 in comparison to 2023, their production and procurement is observed on an ongoing basis, reflecting their continued perceived value amongst DDW threat actors.

| New Exploitation of Existing Vulnerability Announced for Sale

On September 6, 2024, an actor known as “skng” posted in the dark web forum xss advertising a new malicious script that is allegedly designed to target Fortinet software solutions. According to skng, the product enables the exploitation of an existing vulnerability known as CVE-2022-40684, which was discovered in early October 2022. Skng is offering the malicious script to two separate buyers only at a cost of USD 3,500 each, which is very likely indicative of attempts to prevent the vulnerability from being identified and mitigated by the software manufacturer or security researchers. Skng further specifies that transactions must use escrow.

- CVE-2022-40684 is an authentication bypass vulnerability with a CVSSv3 score of 9.8 and is classified as “critical.” The vulnerability affects some versions of FortiOS, FortiProxy, and FortiSwitchManager and allows an unauthenticated attacker to perform administrative operations via specially crafted HTTP or HTTPS requests.
- Successfully exploited, CVE-2022-40684 can allow the attacker to gain access to privileged administrative interfaces without being in possession of legitimate credentials. Shortly after the vulnerability’s discovery, mitigating software patches were released alongside customer advisory notices.

According to the post, approximately 95 percent of the software currently in use cannot be targeted due to users not using lightweight directory access protocol (LDAP) accounts. Skng alleges that the advertised script can remedy this issue, enabling the targeting of a much larger pool of users. It is likely that the malicious script does not enable the targeting of software using up-to-date security patches, but rather, a larger proportion of unpatched systems. If it enabled the targeting of patched software, the price would likely be significantly higher.

- No further detail is provided as to how the script enables exploitation, though the actor promises potential buyers more information and the answers to other questions via private message.

The transaction is carried out exclusively through the guarantor and in no other way!

Sale in 2 hands.

Price: 3.5k\$

First contact in PM.

 Complaint

 son of carding

[EXPLOIT] New Fortinet script based on CVE-2022-40684

 skng ·  Friday at 03:49

AUTOMATIC GUARANTOR CAN BE USED IN THIS TOPIC!

 New deal



skng

config user ldap

Premium

Registration: 10/30/2022
Messages: 40
Reactions: 18

Friday at 03:49

Price: 3.5k\$
Contacts: P.M.

Approximately 95% of targets from this exploit are not worked out (since they do not have accounts in LDAP).
In this topic I sell a solution that allows you to break into these targets.
All questions and information about the script in PM (only for potential buyers).
After the purchase, you receive full instructions on how to work with the script.

xss post by skng advertising new malicious script

Source: ZeroFox Intelligence

Although skng carries a positive reputation in the xss forum, another well-regarded actor known as “barnaul” commented beneath the post claiming that the script is not useful. Due to the lack of detail provided in the post, the effectiveness of the script cannot be determined.

- Criticizing each other's offerings is very commonly observed in DDW forums, even amongst competent and well-regarded actors. There is a likely chance that barnaul's negative response was prompted by a failure to obtain details from skng.



snkg
config user ldap
Premium
Registration: 10/30/2022
Messages: 42
Reactions: 18

Monday at 03:09

barnaul said: 

Just create an ldap user in the config, lol? And how will it be added to ldap (which may not even exist)?

Hi. There is no point in creating an ldap user, since it will not work anyway. Here is a slightly different solution, if you are interested, I will tell you more in PM.

 Complaint

xss post by barnaul questioning the validity of malicious script

Source: ZeroFox Intelligence

The vast majority of network exploitation leverages old or existing vulnerabilities that have since been remedied by software manufacturers. Threat actors are able to both capitalize on the users that have not conducted the appropriate software updates and leverage malicious DDW services that specialize in uncovering and monetizing new methods of exploiting existing and patched vulnerabilities, such as the script offered by skng.

| New Ransomware-as-a-Service Emerges

On September 5, 2024, untested actor “InvaderX” posted in the DDW forum RAMP (where they had registered several days earlier) announcing that they are seeking affiliates for their new InvaderX ransomware-as-a-service (RaaS).

- A list of technical features was provided in the post that correlated to an August 14, 2024, RAMP post previously reported by ZeroFox in which actor “Nikazon” announced the sale of the source code for their locker ransomware.¹
- Nikazon’s post received significantly positive feedback from high-profile forum users who claimed to have previously worked with either Nikazon or the ransomware.
- It is very likely that Nikazon’s ransomware has been acquired and is now being operated as a service by InvaderX.

¹ [hXXps://www.zerofox\[.\]com/blog/the-underground-economist-volume-4-issue-17/](https://www.zerofox[.]com/blog/the-underground-economist-volume-4-issue-17/)

The post specifies relatively advanced technical features of the malware, which allegedly include three encryption modes, encryption of connected storage assets, and privilege escalation to terminate obstructive processes and services. InvaderX also allegedly offers distributed denial-of-service (DDoS), which is likely intended to work alongside data encryption and exfiltration to exert additional leverage upon the victim.

InvaderX outlines their RaaS targeting policy, which prohibits attacking entities based in member states of the intergovernmental organization BRICS—the first instance of such a targeting policy ZeroFox has observed.

- BRICS is a geopolitical bloc that aims to nurture the economic growth and political coordination of its member states, as well as influence reforms of international organizations such as the World Bank and the International Monetary Fund. As of the writing of this report, BRICS member states include Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Iran, and the United Arab Emirates (UAE).

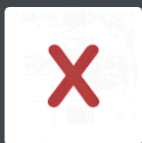
InvaderX [RaaS]

Reply

InvaderX · Thursday at 11:48 AM

Forums > Market \ Market > Partners Program \ RaaS \ Partner Progr...

Watch



InvaderX

Sep 1, 2024

Messages2

Reaction score0

Points1

Thursday at 11:48 AM

< □ #1

Welcome! We are recruiting teams of **experienced** pentesters for our affiliate program . Fast and reliable software written in Rust. Proprietary configuration format with Twofish encryption and serialization. XChaCha12 parallel encryption algorithm is used, the key is encrypted each time with ECIES protection (elliptic curve encryption scheme). Protection against key stream theft is implemented using our own file-based one-time number generator. **Three encryption modes:** - headeronly mode, - smart mode (proprietary algorithm based on hashing the metadata value) - full mode. The software handles errors and memory safety to ensure stability at each launch. **Windows:** - disk and share encryption - automatic share search - asynchronous file indexing - process privilege escalation to terminate processes and stop services - SMB network distribution. **ESXi:** - each binary metamorphoses and re-encrypts itself at each launch - deletes snapshots and turns off the VM - deletes shell history - optional safe self-removal after launch - ignoring most signals that can interrupt the operation of the software. **Additionally, we can provide a call, DDOS** We are open to the wishes of advertisers for further improvements to the software **We do not work in the CIS and BRICS countries.** First contact PM.

RAMP post by InvaderX advertising new RaaS

Source: ZeroFox Intelligence

The majority of RaaS operations are based in or have strong affiliation with Russia and its neighboring countries and, as such usually prohibit the targeting of entities based within the Commonwealth of Independent States (CIS). The prohibiting of BRICS-based targeting is likely reflective of either InvaderX's affiliation with a state that is a BRICS

member but not necessarily CIS or their sentiment that BRICS represents a geopolitical opposition to “the West” and, as such, should not be targeted.

As of the writing of this report, ZeroFox has not observed any attacks from InvaderX or identified any associated digital infrastructure, such as a victim leak site. It is very likely that the operation remains in the process of establishing the necessary infrastructure and acquiring competent affiliates with which to collaborate. So far in 2024, several new RaaS services have displayed notable efficacy and speed in gaining traction and maintaining high attack tempos. Given the alleged features and capabilities of InvaderX’s RaaS, it is likely that the operation will pose a threat to organizations globally in the coming months.

| 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%