



| Brief |

The Underground Economist: Volume 4, Issue 7

B-2024-03-28a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Phishing

March 28, 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 March 28, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 7

| Threat Actor Seeks Suppliers of Stolen Credit Card Databases

On March 25, 2024, untested Russian-speaking threat actor “grossoman15” announced in the deep and dark web (DDW) forum exploit, the intent to launch a new credit card shop named “Tucker Carlson.” The actor also advertised the search for a supplier who is able to provide the details for a minimum of 20,000 stolen cards.

- According to the advertisement, the cards provided should be at least 10 percent “cardable.” This almost certainly alludes to the card’s ability to make successful transactions.
- The majority of databases containing stolen credit card details almost certainly contain information pertaining to cards that are usable due to them being unused, redundant, or blocked by banks following detection of unusual activity.

The actor specified that they are seeking Russian-speaking sellers that have access to card details from the United States, Canada, Australia, and the United Kingdom. The compensation for vendors is an average of USD 100 per 1,000 cards, though this is dependent on their originating country, format, validity, billing information and other, unspecified factors.

**Tucker Carlson Is Looking For CC's Suppliers**

By grossoman15, 2 hours ago in [Finance] - billing, banks, accounts, logs

Follow 1

Start new topic

Reply to this topic

grossoman15

byte



Paid registration

0

3 posts

Joined

01/08/20 (ID: 98953)

Activity

carding

Posted 2 hours ago

Looking for suppliers:

- CC's 2022-2023 databases with a validity of 10% or more.
- Minimum wage - from 20000 pieces with 10% validity.

I am looking for regular deliveries from adequate Russian-speaking people, I am ready to sell any volumes in the shortest possible time to let you earn from the second CC's.

- Country USA,CA,UK,AU etc in more detail when communicating;
- CVV and unexpired EXP date, with billing info and full data;
- From 20000 SS, I am not interested in the origin of the cards, whether they were traded or driven from them, but the ancient dead public and generated databases are not interested, this is all quickly checked, please do not waste your and my time!

Payment is made immediately, I test part of the lines, then we jointly decide the final price (it directly depends on many factors - geo, format, validity, billing info, etc. on average \$100+ per 1000 CC.

The first contact is via - PM, then TOX, Jabber.

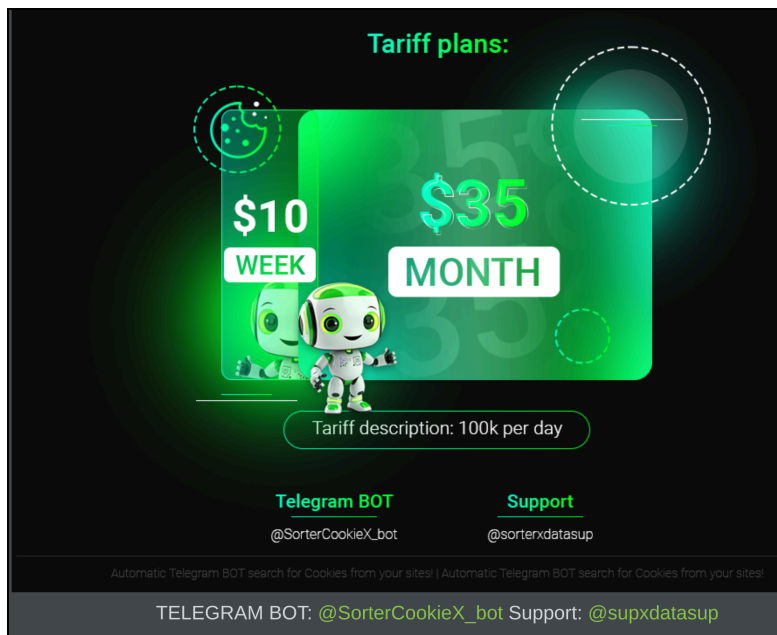
Exploit post advertising the "Tucker Carlson" credit card shop

Source: ZeroFox Intelligence

Launch of Telegram-Based Automated Session Cookies Sales Service

On March, 24, 2024, vetted actor "SorterPassX" announced the launch of a Telegram-based session cookies sales service on the Russian-speaking BlackHatForum (BHF). The service—which offers a swathe of session cookies for sale—enables buyers to streamline account takeovers or potentially collect and resell the cookies for financial gain. Stolen login data remains one of the most valuable resources for threat actors on the DDW.

- The session cookie sales service is offered at low prices— USD 10 per week or USD 35 per month for up to 100,000 requests for session cookies per day.
- SorterPassX claimed that the cookies are deleted locally after the upload to the cloud storage which is available for buyers, meaning there is likely limited recycling of stolen data.



Post Promoting SorterPassX's Telegram-Based Session Cookies Sales Service

Source: ZeroFox Intelligence

The service sells session cookies parsed from botnet and infostealer logs. These cookies are harvested as part of a separate, Telegram-based service also run by SorterPassX which allows seamless purchasing of credentials stolen by botnet and stealer malware.

- The original SorterPassX credentials selling service was announced in April 2022 and remains operational and reasonably successful.

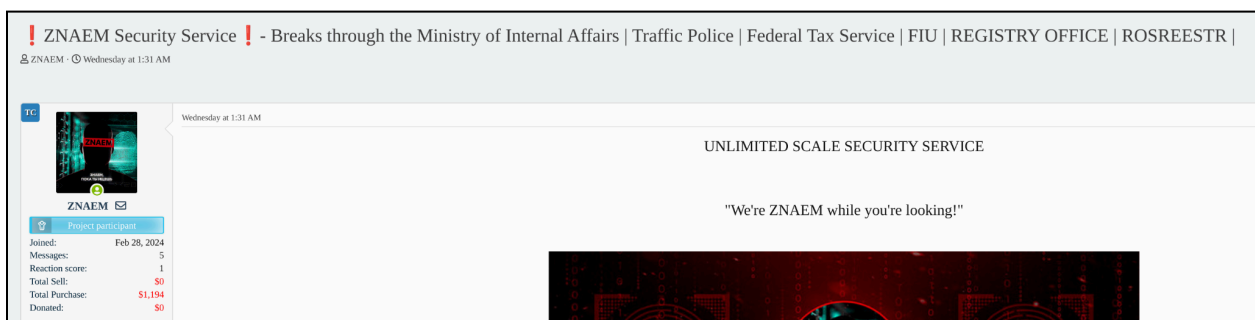
The service will likely gain traction in DDW communities. Automated DDW shops for botnet and infostealer logs are rare but offer considerable opportunities for follow-on malicious activity and financial gain. SorterPassX's service will likely fill a gap in this market.

- Since the closure of the Genesis Market in 2023, session takeover facilitation has been restricted to a limited number of cookies collected by stealers whose output is listed for public sale.

| New “Breach” Service offers access to Russian Government Institutions

On March 13, 2024, the untested actor “ZNAEM” posted an announcement in the Russian-speaking DDW forum WWH-Club, advertising a new service named “Znaem Security Service”. The service offers “extensive” access to information from databases belonging to various Russian Government departments, including:

- The Russian Ministry of Internal Affairs,
- The Russian Road Safety Department,
- The Social Fund of Russia,
- The Federal Service for Supervision of Communications, Information, Technology and Mass Media (RKN),
- The Russian National Credit Bureau,
- The Russian Federal Tax Service.



WWH-Club post advertising Znaem Security Service

Source: ZeroFox Intelligence

Users of the service are purportedly able to purchase information via the submission of specific queries. The information is then sought by “punching through employees,” which very likely relates to the obtaining of information directly from employees within the target organization.

- While similar services often rely upon leaked data, it is likely that Znaem Security Service has at least some “live” access, whereby employees are tasked with gathering bespoke information.

- Information requested from these organizations is very likely to include personal, identifiable information (PII), which could be implicated in future phishing attacks or sold in DDW forums. Non-malicious requests are also very likely made.

The service explicitly announces that it does not sell illicit network access to the advertised organizations, nor does it use such access to gather requested information.

- The targeting of entities within Russia and the Commonwealth of Independent States (CIS) is generally considered bad practice within Russian-speaking DDW forums and in stark contrast to the acceptable norms expected from frequenters. Such activity can result in scrutiny from peers and moderation or blacklisting from some Russian-speaking platforms.
- It is likely that the services provided by Znaem Security Service are generally considered acceptable, with a distinction being made between attacks that directly breach the networks of CIS organizations—such as digital extortion and vulnerability exploitation, and those that leverage insider employees to provide information voluntarily.

✓ Breakthroughs and searches of any difficulty level.

✓ Any transaction through the guarantor, the commission is at our expense.

✓ Full confidentiality, we do not transfer data to third parties.

We do not use "merged or manual databases", only online by punching through employees

WWH-Club post advertising Znaem Security Service

Source: ZeroFox Intelligence

The majority of the post is written in English rather than Russian, which is atypical for posts within a Russian-speaking DDW forum. This is likely an attempt to appeal to forum members from English-speaking countries due to a perception that they would pay more for information. It is also very likely an attempt to reach additional Western customers who are conducting research or investigations into Russia-based individuals or organizations.

ZNAEM had deposited a financial sum into the forum's escrow service to guarantee future customers and ensure credibility. It is very likely that the service is able to provide the services advertised.

| Sale of Custom Phishlets for Evilginx3 Tool

On March 11, 2024, blackdatabase announced the sale of custom phishlets for Evilginx3 on the DDW forum xss. The actor listed commonly used phishlets with prices starting at USD 500 for an outlook[.]com phishlet and ranging up to USD 5,000 for phishlets targeting banking services, including Wells Fargo and Chase. The post has gained significant traction within the xss community, indicating a high level of interest from potential buyers.

Evilginx3 is a sophisticated reverse proxy tool for "in-the-middle" attacks against various online services, enabling threat actors to obtain login credentials and harvest session cookies to facilitate MFA bypass. While the third version of the tool was released publicly in May 2023, it did not include the phishlet component that enables malicious actors to adapt the software to attack particular websites.

- Evilginx3 mirrors a website to lure users into entering credentials via phishlets, and configuration files in YAML format used for proxying a legitimate website into a phishing domain. These phishlets specify how Evilginx3 intercepts and manipulates web traffic between a victim and a legitimate service to capture credentials and session tokens.
- While similar phishlets are often available in open sources, many of these are likely to be out of date or ineffective; blackdatabase's high asking price likely indicates the phishlets sold are believed to be currently deployable.
- Notably, Google was not explicitly listed in the post, likely indicating that the actor is unable to write or provide such a phishlet.

Reverse Proxy/MITM phishing solution (sell), Custom phishlets evilginx 3

blackdatabase · Mar 11, 2024

ESCROW AVAILABLE IN THIS THREAD!

New deal

Mar 11, 2024

 **blackdatabase**
RAID-массив
Пользователь
Joined: Dec 25, 2021
Messages: 51
Reaction score: 5
Deposit: 0.0011 \$

Цена: \$500 - \$5000
Контакты: @blackdatabase

For sale evilginx3 phishlets:

- azure.com = \$3k
- amazon.com = \$2k
- aws.amazon.com = \$3k
- office365 = \$1k
- outlook = \$500
- ads.microsoft.com = \$3k
- mobile.de = \$5k
- autoscout24 = \$5k
- Amadeus Selling Platform Connect = \$3k
- Facebook = \$3k
- blockchain.com \$5k (Automatic collection of 12 words)
- wells Fargo = \$5k
- citi = \$5k
- bofa = \$5k
- chase = \$5k

Any custom phishlets template can be made, execution time 1-15 days.

Blackdatabase's post advertising the sale of Evilginx3 phishlets

Source: ZeroFox Intelligence

The sale of custom Evilginx3 phishlets very likely poses a significant risk to high-profile organizations globally. Evilginx3, when used in conjunction with phishlets, offers a substantial advantage to threat actors over live panel phishing pages. Instead of being limited to credential theft, leveraging Evilginx3 in conjunction with phishlets could enable attackers to steal session data, facilitating MFA bypass and granting seamless access to sensitive data and funds stored in bank accounts.

- Each phishlet will very likely be sold to multiple buyers and should not be considered a single-purchase option.
- ZeroFox has observed multiple threat actors seeking Evilginx3 phishlets in recent months.

| 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 the 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

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%