



| Flash |

Sale of Custom Phishlets for Evilginx3 Tool

F-2024-03-20a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Phishing, Multi-Factor Authentication Bypass,
Deep & Dark Web, Data Theft

March 20, 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 20, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Sale of Custom Phishlets for Evilginx3 Tool

> Key Findings

- On March 11, 2024, the well-regarded threat actor “blackdatabase” announced the sale of custom phishlets for Evilginx3 on the dark web forum xss.
- The phishlets for sale target multiple companies; prices start at USD 500 and range up to USD 5,000 for phishlets targeting specified financial sector entities.
- Evilginx3, when used in conjunction with phishlets, could enable attackers to steal session data, facilitate multi-factor authentication (MFA) bypass, and grant seamless access to sensitive data and funds stored in bank accounts.

| Details

On March 11, 2024, blackdatabase announced the sale of custom phishlets for Evilginx3 on the dark web 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, 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



blackdatabase
RAID-массив
Пользователь

Joined: Dec 25, 2021
Messages: 51
Reaction score: 5
Deposit: 0.0011 \$

Mar 11, 2024

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

- Verify the active window[.]location URL. For any anomalous results, prevent the site from rendering, warn the user, or disable logins.
- Adopt an organization-wide zero-trust cybersecurity architecture, ensuring that access to devices, networks, and information is kept at what is minimally required for operations based upon a principle of least privilege. Continuously test and scrutinize the legitimacy of trust in place.
- Implement phishing-resistant MFA protocols compliant with FIDO2 or PKI standards, complex passwords, unique credentials, and the separation of user and privileged accounts.
- Develop a clear and comprehensive incident response strategy consisting of business resilience and continuity plans—including third-party services' incident reporting procedures and key authorities.

| 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%