



| Brief |

The Underground Economist: Volume 4, Issue 16

B-2024-08-23a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web

August 23, 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 August 23, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 16

New Version of Octo Bot Available in Dark Web Marketplace

On August 20, 2024, threat actor “goodluck” posted in the dark web forum Exploit, announcing that a new version of their Octo 1 malware, Octo 2, is now available. The post follows goodluck’s announcement of the upgraded malware in November 2023 and a partial release of a beta version at the start of 2024.

- Octo 2 is allegedly available to any buyer, with customers of the previous Octo 1 able to upgrade via a private messaging channel. Goodluck did not specify a price for Octo 2 in the announcement.
- As is standard practice for products sold in dark web forums, using Octo 2 to target victims located in the Commonwealth of Independent States (CIS) is forbidden. According to the post, Chinese organizations are also off-limits.

Octo 1 is a popular Android remote access banking trojan that has been highly sought after amongst threat actors since a similar bot named “Sova” ceased to be available following a 2021 exit scam.

- Octo 1’s most notable feature is its hidden virtual network computing (HVNC) capability, which enables the attacker to remotely control the infected device without the victim’s knowledge.

- It is also able to block certain push notifications, intercept SMS communications, and conduct keylogging to steal input information. Octo 1 has almost certainly been leveraged in numerous campaigns targeting financial institutions across the globe.

goodluck
kilobyte
●●

Seller
 **11**
34 posts
Joined
08/07/20 (ID: 107085)
Activity
кодинг / coder

Posted Wednesday at 03:03 PM

Привет!

На данный момент Окто 2 доступен для аренды бывшими клиентами Окто 1 (не турецкой версии, разумеется)
Публичный релиз Окто 2 - 20 августа 2024.
Приглашение в приватный канал с новостями можете получить у селлера - **@octo_sup**

Hello!

Octo 2 is available for the former Octo 1 customers (non-Turkish version, obviously)
Octo 2 public release date is 20. August 2024.
You can get invite to the private channel with news from our seller: **@octo_sup**

Exploit post advertising the release of Octo 2

Source: ZeroFox Intelligence

While goodluck did not specify their perceived areas of improvements to Octo 2, they did publish a list of features promised to users. Some information about the bot was also provided, which included:

- Has an Android Package (APK) size of less than 5 megabytes
- Requires only one permission from the victim
- Has a high survival rate, with an expected lifetime of several months
- Can be used to target devices operating Android versions 9-13

Android versions 9-13 roughly encompass devices manufactured between 2018 and 2023, which comprise approximately 55-64 percent of all Android devices globally. There is a likely chance that future developments to Octo 2 will add support for the most recent Android version, 14.

Functions

- Hidden VNC provides full device control
- Black Screen VNC protection
- Web Injects, URL Injects
- CC grabber (as a part of injects)
- Google Authenticator code grabber
- Cookie Stealer
- Keylogger collects all holder actions, browser URLs, input data
- SMS Intercept
- Push Notifications intercept
- Lock for App / SMS / Push Notification / Device
- Send SMS, USSD (Call forwarding), Push notification
- Open URL in device's browser
- Run app on device, install apps
- Uninstall apps/bot

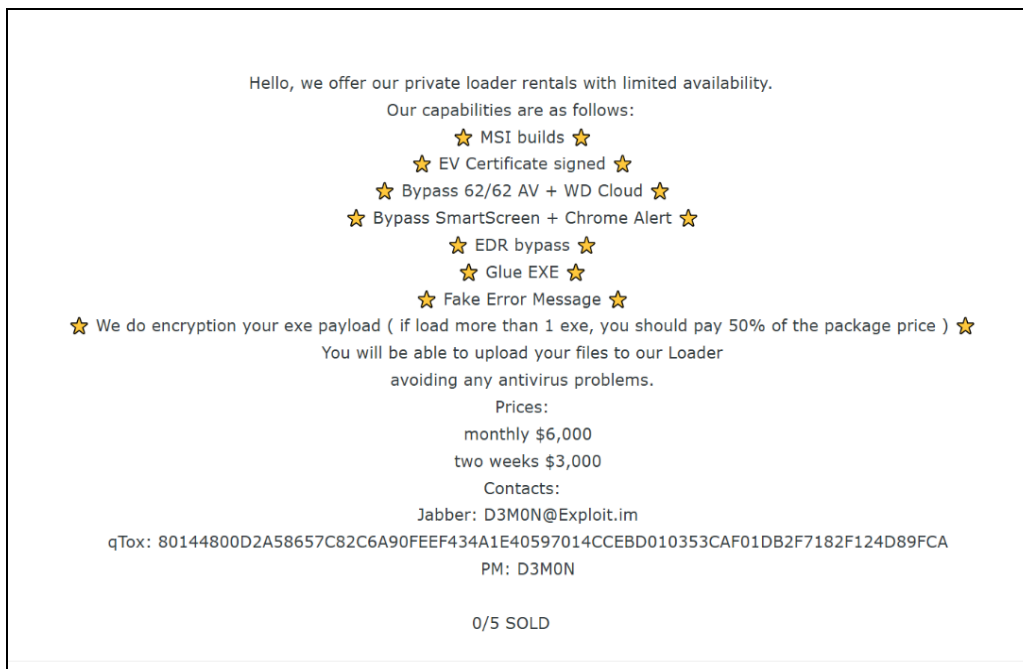
Exploit post advertising Octo 2 functions

Source: ZeroFox Intelligence

| New High-Profile Loader Malware Announced for Sale

On August 18, 2024, positive-reputation threat actor “D3M0N” posted in the dark web forum Exploit advertising a new loader malware with an allegedly limited availability. D3M0N also claimed that their “team” can offer the buyer a further service of encrypting their intended payload subsequent to the loader being successfully deployed in order to make it as fully undetectable (FUD) as possible.

- A loader is a type of malware that functions as a delivery mechanism for deploying additional subsequent payloads. They are deployed via means such as phishing or vulnerability exploitation, with the primary purposes of evading the target network’s security defenses, establishing persistence, and downloading further malware.



Exploit post advertising D3M0N's loader malware

Source: ZeroFox Intelligence

The price for the loader is advertised as USD 6,00 per week or USD 3,000 for two weeks. This is significantly higher than the prices typically observed in malware-as-a-service advertisements, particularly for loaders. This very likely reflects D3M0N's perception of the tool as innovative and potentially effective, and also indicates D3M0N anticipates high demand. Many of the features listed are not often seen in loader-as-a-service offerings, and some appear relatively state-of-the-art, notably:

- The ability to distribute via MSI (Microsoft Installer) builds
- The ability to bypass 62 different anti-virus products
- A "glue" technique used to combine multiple executables into a single, benign-looking file
- The ability to display fake error messages (these may, for example, fool the victim into believing that the executable failed to run)
- The ability to sign the build with an Extended Validation (EV) certificate, increasing its authenticity and decreasing the chance of detection
- The alleged inclusion of a download link, making the loader ready to distribute via social engineering campaigns or spam communications

The advertisement quickly gained traction and responses from multiple alleged positive-reputation buyers that praised the seller's competency along with the product's efficacy. Given that the advertisement specifies that the loader is "private", there is a likely chance that it has already been leveraged in a limited number of cyberattacks prior to being advertised in the Exploit forum. Its advertisement as a service will very likely result in its increased use—particularly if all the alleged features are legitimate capabilities and positive feedback continues.

| New InfoStealer Targets MacOS Devices

On August 12, 2024, positive-reputation actor "Oxel" announced in the deep and dark web (DDW) forum xss that they are now offering a new stealer malware named "Banshee", which is designed to steal data from MacOS users. The price is USD 3,000 per month, with the first two buyers receiving free three-day subscriptions.

- A stealer is a type of malware designed to compile various types of information from a victim network into a stealer log, which is extracted by the attacker via a command and control server before being exploited or sold in DDW marketplaces.
- Compared to other operating systems, stealers designed to target MacOS devices are relatively rare in DDW marketplaces. The most prominent are Atomic Stealer (AMOS), MetaStealer, MacStealer, CherryPie, and XLoader.
- The advertised price for Banshee is notably high—almost three times higher than AMOS, which is currently one of the most expensive MacOS stealers.



Xss post advertising Banshee

Source: ZeroFox Intelligence

Oxel did not specify features of Banshee that were sufficiently notable or innovative enough to justify the high price, with the exception of the malware allegedly being able to steal information from a significant number of MacOS applications—including web browsers, cryptocurrency wallets, and various extensions. As of the time of writing, Oxel's post has received no visible traction, though a subsequent post warned of fake Telegram channels impersonating the sale—which itself indicates other threat actors perceive there will be interest in the product.

List of Zero and One-Day Vulnerabilities Announced for Sale

On August 11, 2024, positive-reputation actor "streetsphinx" posted in the popular hacking forum BreachForums advertising over 2,000 alleged zero and one-day vulnerabilities for sale. Streetsphinx enclosed a .txt file that discloses 245 of the supposedly-affected organizations, the vast majority of which are IT software and hardware manufacturers, network security specialists, and software-as-a-service (SaaS) providers. Listed prices range between USD 350 and USD 250,000, with the higher end figures very likely alluding to the alleged zero-day vulnerabilities.

- Streetsphinx did not provide the exact price for each vulnerability, how sales will take place, or the names of the remaining organizations that do not appear in the .txt file list.

- A subsequent post by streetsphinx claimed that they would sell the entire list of vulnerabilities to a single buyer. However, this is very unlikely to occur, as the quantity and the indicated prices would result in an approximate cost of several million U.S. dollars.
- A zero-day vulnerability refers to a vulnerability that is unknown to the original software manufacturer—meaning no remedy or security patch yet exists. A one-day vulnerability refers to a vulnerability for which a security patch is available but has not yet been applied by an intended target. Zero-day vulnerabilities demand significantly higher monetary value in DDW marketplaces due to the severe threat posed to organizations using the vulnerable software.

Yesterday, 11:25 AM (This post was last modified: Yesterday, 04:28 PM by streetsphinx.)

We are offering a wide range of 1day and Zeroday vulnerabilities for sale. Each file is provided with a detailed report, a pcap file, and a proof of concept (PoC) file.
Pricing: Prices start at \$300 and can go up to \$250,000.

Additional Information:

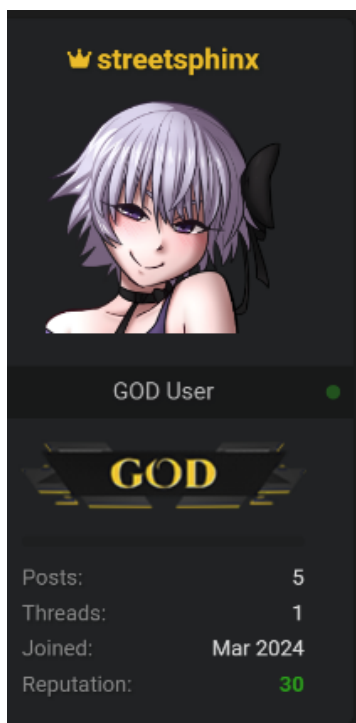
- Our list includes over 2,000 1day vulnerabilities (and no, this is not from exploit db).
- More than 300 Zeroday vulnerabilities are available.

For understandable reasons, we will not specify the applications or vulnerable software here.

BreachForums post advertising alleged vulnerabilities

Source: ZeroFox Intelligence

Streetsphinx elaborated that each of the vulnerabilities will be sold with a detailed “report”, a .pcap (packet capture file), and a proof of concept (PoC). In order to make a purchase, interested buyers are directed to make contact via an advertised Telegram channel and to pay in XMR cryptocurrency. A duplicate advertisement was posted to the dark web forum xss on August 13, 2024, with the likely intent of reaching potential buyers with more purchasing power. The post was subsequently deleted from both forums, with no update or explanation from streetsphinx.

**Streetsphinx's BreachForums profile**

Source: ZeroFox Intelligence

There is a roughly even chance that the post was an ineffective scam attempt in light of the large number of alleged vulnerabilities for sale—particularly the possession of multiple zero-day vulnerabilities, which are relatively infrequent and often sold as a stand-alone product. The chance of the advertisement being legitimate and reflective of hundreds of zero-day and one-day vulnerabilities for sale is very low for the same reasons and is made more unlikely by the prompt deletion of the posts.

The most likely scenario is that the advertisement was partially accurate but greatly exaggerated in order to attract attention. The presence of large numbers of one-day vulnerabilities is feasible, but there is a likely chance that many would have been patched by intended victims prior to exploitation and rendered ineffective. It is unlikely that any legitimate zero-day vulnerabilities were available for sale.

| 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.
- Ensure social media accounts are configured with organic security features, such as phishing-resistant multi-factor authentication (MFA) and complex, unique passwords.
- 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%