



| Flash |

Malicious Stealer Log Marketplace Advertised for Sale

F-2024-08-07a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor, Stealer Logs

August 7, 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 7, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Malicious Stealer Log Marketplace Advertised for Sale

› Key Findings

- On July 30, 2024, user “2Easy.Shop” (which is almost certainly synonymous with the official handle of the malicious marketplace 2EasyShop) announced in a deep and dark web (DDW) forum that the stealer log marketplace is available for purchase.
- 2EasyShop—described by the poster as a “ready-made, configured, highly profitable business”—is a DDW marketplace that specializes in advertising and selling stealer logs, which are compilations of information that have been stolen from devices and networks infected with malware.
- Given the very likely growing demand among various types of cyber threat actors for the information contained within stealer logs, it is likely that a sale will take place. If the auction fails, there is a roughly even chance that the site will remain closed until a sale occurs.
- A successful deal at the asking price would very likely reinvigorate 2EasyShop, resulting in more reliable service, an increased supply of logs, and higher volume of sales that almost certainly pose a threat to individuals and organizations.

Details

On July 30, 2024, user 2Easy.Shop—which is almost certainly synonymous with the official handle of the malicious marketplace 2EasyShop—posted in the DDW forum Exploit. The announcement claimed that 2EasyShop, its digital infrastructure, and its domain will be auctioned and sold to the highest bidder. The minimum bid is USD 150,000, bid increments are set at USD 10,000, and the instant purchase price is USD 200,000. While the auction is set to take place in Exploit, it is not known if it will occur publicly.

2Easy.Shop - Logs Marketplace

By 2Easy.Shop, July 30 in Auctions

Ready-made, configured, highly profitable business.

- Top server, domain.
- Logs for 4 years (displayed on shop windows by sellers, not for personal use).
- Contacts of all (30+) sellers for the entire period of work.
- Telegram channel 1800+ subscribers <https://t.me/+UOi2JQYKnsGavS5q>
- Access to forums (54 forums), EXCEPT Exploit and WWH, is discussed separately.

We are also discussing the transfer of contacts of partners - with whom cooperation has been agreed and placement of individual sales branches on the site. Self-regs, bank accounts, CC, e-gifts, DOC'S, socks vpn, DDOS, fullz, call center, liken sphere, cash out and so on. The list is VERY long.

Start 150k\$

Step 10k\$

Blitz 200k\$

Exploit post advertising the auction of 2EasyShop

Source: ZeroFox Intelligence

2EasyShop, described by the poster as a “ready-made, configured, highly profitable business”, is a DDW marketplace that specializes in advertising and selling stealer logs.

- Stealer logs are compilations of various types of information that have been stolen from devices and networks infected with a strain of malware known as a stealer. Typically, stealer logs are composed of information such as URL login and password combinations, personally identifiable information (PII), personal financial information (PFI), network and system information, and web browser data such as cookies and session tokens.

- The diversity of information found in stealer logs ensures an ongoing demand from a vast array of cyber threat actors, who leverage them to enable initial network access, enhance social engineering attacks, or conduct fraudulent activities.

According to the advertisement, the purchase also includes:

- A supply of private stealer logs that have not been circulated elsewhere and contact details of over 30 sellers (likely individuals leveraging established malware distribution operations that regularly sell on 2EasyShop);
- An associated Telegram channel and access to 54 unspecified forums in which to advertise via a 2EasyShop official handle; and
- A long list of contacts and alluded-to capabilities that are very likely indicative of access to fraudulent services, such as bank accounts created leveraging stolen PII.

On August 3, 2024, 2EasyShop reposted the rules of the auction and claimed that the auction time will be extended by 72 hours. As of August 6, 2024, the thread has received no visible traction and no new announcements have been posted, though it is unknown if conversation or negotiations are taking place by private means.

2EasyShop launched in approximately 2018 and experienced significant initial growth. Despite claims of overly assertive administrative staff and the site generally featuring older and lower quantities of logs than rival sites, the shop quickly became a competitor to other stealer log marketplaces, such as Genesis and Russian Market. The platform is fully automated (meaning customers can create an account, add funds, and make purchases all without interacting with sellers), and a diverse array of information is available due to sellers leveraging a number of different stealers.

However, in recent years 2EasyShop has become associated with frequent and lengthy periods of interrupted service and administrative issues.

- In Q2 2023, 2EasyShop's previous domain was hijacked by threat actors who conducted subsequent phishing attacks targeting the platform's customers, damaging its reputation.

Flash | Malicious Stealer Log Marketplace Advertised for Sale

F-2024-08-07a

TLP: CLEAR



- In February 2024, 2EasyShop's administrators claimed to have lost access to customers' wallets. While no further detail was made available surrounding this issue, it was followed by periods of downtime.

		Country	Seller	Files	Info	Date upload	
Links (413)	Cookie (4364)	IR	DarkSeller	archive.zip	Info	19/11/2023 19:38	1.56 \$
Links (1272)	Cookie (8471)	IQ	DarkSeller	archive.zip	Info	18/11/2023 11:38	1.95 \$
Links (62)	Cookie (992)	BR	DarkSeller	archive.zip	Info	18/11/2023 11:24	1.95 \$
Links (1174)	Cookie (2369)	IT	DarkSeller	archive.zip	Info	13/11/2023 20:11	2.47 \$
Links (555)	Cookie (5330)	SI	DarkSeller	archive.zip	Info	13/11/2023 19:49	2.47 \$
Links (154)	Cookie (1404)	MA	DarkSeller	archive.zip	Info	13/11/2023 19:09	2.47 \$
Links (452)	Cookie (1129)	GR	DarkSeller	archive.zip	Info	13/11/2023 18:57	2.47 \$
Links (156)	Cookie (1283)	EG	DarkSeller	archive.zip	Info	13/11/2023 18:46	2.47 \$
Links (211)	Cookie (409)	YE	DarkSeller	archive.zip	Info	26/10/2023 08:46	1.30 \$
Links (281)	Cookie (764)	YE	ALLL	archive.zip	Info	12/10/2023 12:51	6.50 \$

2EasyShop marketplace, showing stealer logs available for purchase

Source: ZeroFox Intelligence

While 2EasyShop did not specify a reason for listing the platform on Exploit for sale, it is likely the culmination of a series of errors and issues that resulted in a diminishing reputation and customer base. Other stealer log marketplaces have grown significantly in popularity—notably the recently-launched DDW service Exodus, which quickly drew significant attention.

Given the very likely growing demand among various types of cyber threat actors for the information contained within stealer logs, it is likely that a sale will take place. If the auction fails, there is a roughly even chance that the site will remain closed until a sale occurs, though the asking price may be reduced. Should the platform become non-operational, a number of sellers that primarily use 2EasyShop would very likely move to Russian Market, Genesis, Telegram-based services, or smaller DDW marketplaces.

A successful deal at the asking price would very likely reinvigorate 2EasyShop, resulting in more reliable service, an increased supply of logs, and a higher volume of sales that almost certainly pose a threat to individuals and organizations.

| Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- 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).
- Utilize ZeroFox Intelligence and our proprietary platform to understand potential exposure in stealer logs.

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%