



Brief

An Introduction to Stealer Logs

B-2024-08-20a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Data Breach, Stealer Logs

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

Brief | An Introduction to Stealer Logs

Key Points

- A stealer log is a series of data files generated and compiled by malicious software known as “infostealers.” The log contains personal and sensitive information that has been collated and extracted by a cyber threat actor.
- Numerous data-stealing techniques are leveraged by infostealers; form grabbing, keylogging, credential dumping, and screen scraping are all commonly used to uncover and extract information from the target endpoints.
- Threat actors responsible for the production of stealer logs often seek to sell the stolen data in deep and dark web (DDW) forums, supplying cybercriminals with a constant trove of stolen information.
- The information found in stealer logs (such as credentials, personal financial details, browser information, and hardware specifications) is used to enable and enhance a broad array of cyberattacks.
- The mitigation strategies of individuals and organizations must be as diverse as the stealer logs themselves and address the full scope of network access vectors that can be targeted by an attacker in possession of credentials, cookies, and tokens or other browser data.

| What Is a Stealer Log?

A stealer log is a series of data files generated and compiled by malicious software known as “infostealers.” The log contains personal and sensitive information that has been collated from infected endpoints before being extracted to a command server controlled by a cyber threat actor, where it can be further exploited. Organizations face a significant threat from infostealers and stealer logs, primarily due to their abundance in DDW marketplaces and forums, their constant adaptation, and the innate appeal of stolen data to a broad variety of threat actors.

Numerous data-stealing techniques are leveraged by infostealers, depending on the malware strain deployed. Form grabbing, keylogging, credential dumping, and screen scraping are all commonly-observed in such attacks, which usually seek to uncover and extract information from elements of the targeted endpoint device.

- **Web Browsers** – Web browsers typically store various types of information, particularly when using their default settings. Infostealers often search for this information in file paths associated with local browser app folders.

Data sought from web browsers includes personally identifiable information (PII) such as usernames and passwords, which—while usually encrypted—are often stored in close proximity to the decryption key that is also extracted. Browser password managers also often store the associated URL or login portal alongside this information, enabling the infostealer to obtain everything needed to compromise a given account. Personal financial information (PFI) such as credit card numbers and expiration dates that are used for auto-fill purposes can also be obtained from web data or local storage folders.

- **Email Clients** – Modern email clients store significant amounts of information that often includes PII and PFI. Additionally—given its ability to enhance targeted social engineering attacks—data contained in email content, attachments, personal and organizational calendars, and contact lists can be perceived as lucrative by a threat actor.
- **Applications** – Like web browsers, many applications store login details to enhance user experience. Usernames or login email addresses are often

"remembered" by the application and are susceptible to access by infostealers. While passwords are not as often readily available, they can sometimes be obtained via the interception of temporarily stored memory. Various types of applications are at risk of being targeted by infostealers, such as social media and instant messaging apps, password managers, cloud storage platforms, gaming portals, and cryptocurrency wallets. Infostealers can either be programmed to seek predetermined associated file paths or have the capability to dynamically seek commonly used applications or running processes.

Infostealers can also seek information associated with a connected network (such as credentials and configurations) as well as information that can assist in bypassing authentication procedures and enabling persistent access (such as cookies, access tokens, and other session data). Infostealers also look for data surrounding system hardware and installed software, as this can aid the threat actor in identifying vulnerabilities and establishing the most effective subsequent attack techniques.

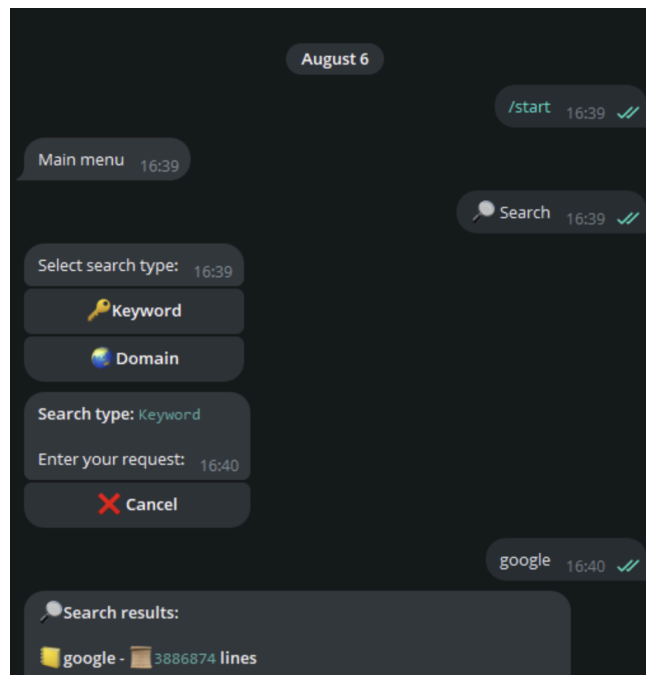
The quantity of stolen data also varies significantly. Stealer logs range from a few megabytes for those containing usernames and passwords to tens of megabytes for those consisting of extensive browser information to hundreds of megabytes or more for those that house large data sets or images.

- Depending on the malware leveraged and the threat actor's intent, the extracted information can also be encrypted. This can aid in the attacker's obfuscation, make it more difficult for victims to determine what information has been stolen, safeguard the data's integrity during transmission, and protect information deemed particularly sensitive from other threat actors.

In its raw form, a stealer log is usually stored as a series of .txt files packaged in an archive file such as a .zip or .rar. At this point the log may be structured in a relatively unorganized way and contain some information that is unusable, irrelevant, or carries no monetary value.

Logs at this stage are often subject to some level of parsing, an indistinct process intended to organize the contents into distinguished categories (such as credentials, credit card details, and browser data) as well as to determine the legitimacy and usability of information.

Parsing is usually undertaken by specialized programs often included within the leveraged stealer malware service, bot programs available in instant messaging (IM) platforms such as Telegram, or bespoke written scripts.



A Telegram-based bot designed to parse session cookies from stealer logs

Source: ZeroFox Collections

The extent to which raw stealer logs are parsed depends upon the stealer malware leveraged and its configuration, the data contained, and how the threat actor intends to conduct subsequent exploitation. Some of the possible benefits of parsing data from stealer logs include:

- Increased ease of navigation and searchability;
- An easier format for victim behavior analysis to take place;
- An opportunity to remove any irrelevant, invalid, or otherwise unusable data; and
- A data format more likely to be compatible with software programs and automated tools used to further exploit the data, lessening the need for custom scripts.

The threat actor responsible for obtaining the stealer log may choose to advertise it for sale in specialized stealer log marketplaces that exist in both DDW forums and IM platforms. In 2024, the most popular stealer marketplaces are almost certainly Russian

Market, Exodus, and the recently advertised-for-sale 2EasyShop, as well as numerous Telegram-based bot services. These marketplaces often categorize and group victim data together by region, sector, or type, enabling buyers to easily obtain the information they seek. Additionally, logs are also traded in DDW forums such as xss, Exploit, and Blackhat Forum, though in lesser quantities.

Information	Price Range
Raw stealer logs containing a variety of data such as credentials, financial information, session tokens, and hardware specifications	Between USD 1 and USD 25, depending on the marketplace Generally, Exodus (which sets prices according to the number of affected assets) demands the highest prices and Russian Market (which sets prices according to the age of the log) demands the lowest.
Datasets with a focus on session tokens and browser cookies	Often granted via a subscription fee, with many services charging approximately USD 30 for one week access, USD 60 for one month access, or USD 500 for lifetime access
ULP rows (rows of information detailing login credentials accompanied by a URL to their relevant login portal)	Usually granted via a subscription fee, with many services charging approximately USD 60 for one month access or USD 500 for lifetime access Can also occasionally be obtained for free, particularly by members with enhanced reputations or in return for specific forum currencies
LP sets and combologs (datasets containing multiple login and password combinations) Combolist are often compilations of this data and are usually outdated and unusable.	Similar pricing structures to ULP rows Well-known cloud-based service AggressorDB charges USD 720 for three months, granting access to all available LP rows for the length of the subscription.

The stealer log demands various prices depending on factors such as the information contained, its age (the date of information extracted), and the country of the victim (areas deemed more lucrative generally fetch a higher price).

- Buyers of this information may opt to exploit the data in subsequent cyberattacks or repackage it into larger sets of stolen data, which may demand a higher price.
- Alternatively, the threat actor may leverage the stolen data themselves. This is more likely if the stolen information enables straightforward network access—and the attacker possesses the technical expertise to exploit it. Following this activity, the data may be sold nonetheless.

Name	Original Size	Compressed Size	Mode	CRC checksum	Method	Date
Telegram	528.4 KiB					
browsers	525.4 KiB					
autofills	14.6 KiB					
Chrome_1-64_Default.txt	1.1 KiB	498 B	-rw-r--r--	4059D5A0	Deflate	8/14/22 11:41 AM
Chrome_1-64_Profile 1.txt	2.1 KiB	935 B	-rw-r--r--	AF24B2FE	Deflate	8/14/22 11:41 AM
Chrome_1-64_Profile 4.txt	246 B	213 B	-rw-r--r--	2477C453	Deflate	8/14/22 11:41 AM
Edge_4-64_Default.txt	10.5 KiB	3.5 KiB	-rw-r--r--	CA4B9CB1	Deflate	8/14/22 11:41 AM
Edge_4-64_Profile 1.txt	702 B	415 B	-rw-r--r--	C16E8307	Deflate	8/14/22 11:41 AM
cookies	510.8 KiB					
Chrome_1-64_Default.txt	151.2 KiB	62.6 KiB	-rw-r--r--	90D12A08	Deflate	8/14/22 11:41 AM
Chrome_1-64_Profile 1.txt	7.1 KiB	2.6 KiB	-rw-r--r--	CB97E9A5	Deflate	8/14/22 11:41 AM
Chrome_1-64_Profile 4.txt	22.6 KiB	9.9 KiB	-rw-r--r--	F502C64E	Deflate	8/14/22 11:41 AM
Edge_4-64_Profile 2.txt	9.1 KiB	4.4 KiB	-rw-r--r--	94420FFA	Deflate	8/14/22 11:41 AM
Edge_4-64_Profile 3.txt	1.7 KiB	773 B	-rw-r--r--	06B15965	Deflate	8/14/22 11:41 AM

Example of a stealer log structure (IP addresses concealed by ZeroFox)

Source: ZeroFox Collections

```
URL: http://apps.ug.edu.gh/sme/login.php
Username: 
Password: 
Application: Google_[Chrome]_Profile 2
=====
URL: https://www.chelseafc.com/content/cfc/en/homepage/security/vindicia/login.html
Username: 
Password: 
Application: Google_[Chrome]_Profile 2
=====
URL: http://admission1.ug.edu.gh/resapply/login.php
Username: 
Password: 
Application: Google_[Chrome]_Profile 2
```

Unparsed Redline stealer log (credentials concealed by ZeroFox)

Source: ZeroFox Collections

| Who Is Creating and Buying Stealer Logs?

Threat actors leveraging stealer malware vary significantly in their technical expertise, experience, resources, and motivations. The vast majority are almost certainly financially-motivated, seeking to generate illicit funds either through the sale of stealer logs or by exploiting their contents. However, stealer malware is also used by threat actors with political, ideological, and punitive motivations.

- **Financially motivated** – Malicious individuals and groups leverage stealer malware for financial gain. Some cybercriminals opt to use the stolen data themselves to enable further malicious exploitation, such as the deployment of further malware, digital extortion, or account takeover. Other cybercriminals use them to establish initial network access that can then be sold, providing a supply to the array of threat actors seeking to conduct malicious cyber activity.
- **Ideologically motivated** – Various hacktivists that are motivated by ideology deploy stealer malware with the ultimate aim of causing disruption or inflicting reputational damage. Hactivist groups often target organizations deemed to be associated with a particular ideological, political, or social belief, such as government departments, religious institutions, and non-governmental organizations (NGOs).

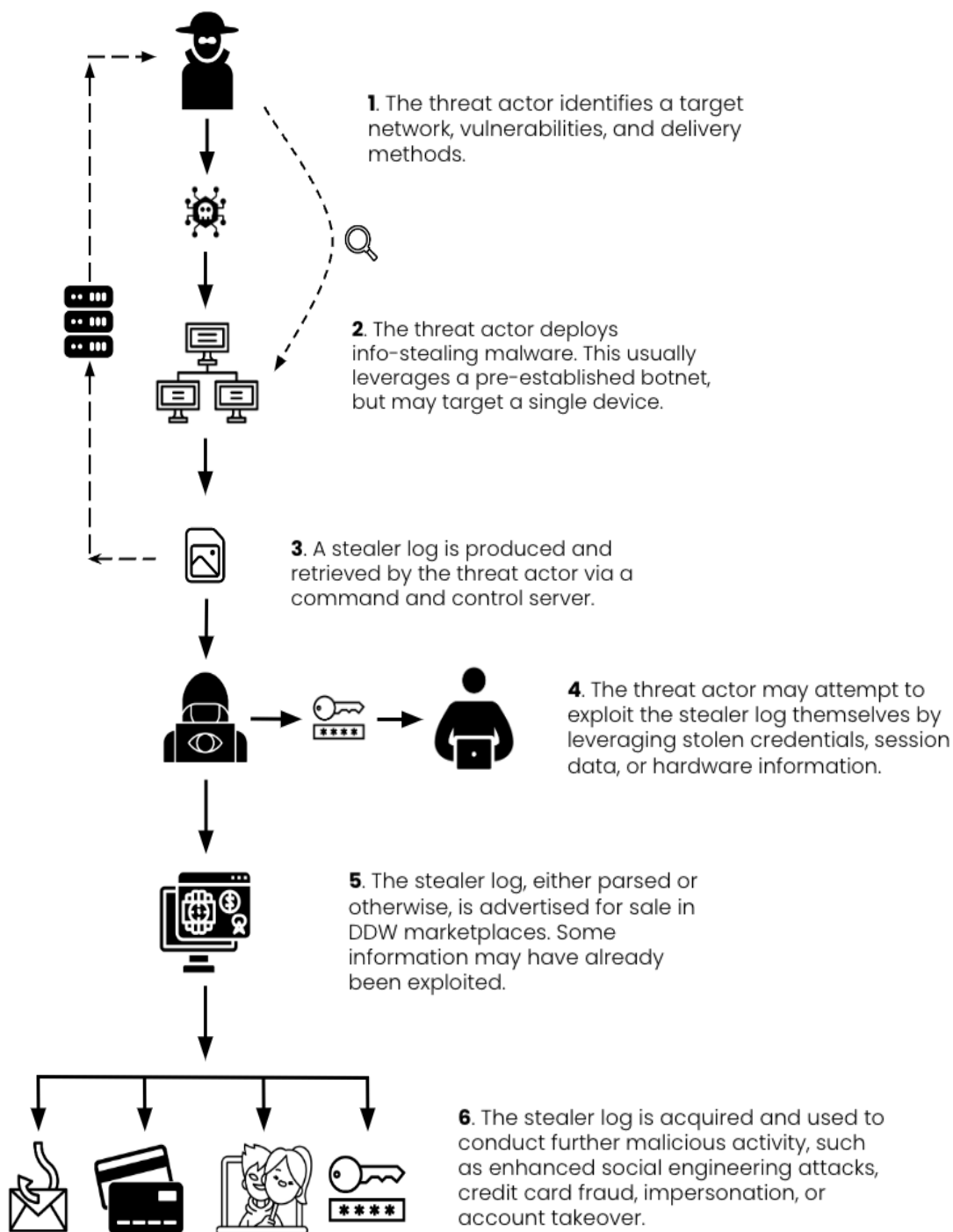
Stolen credentials can be used to gain access to personal and corporate communications before leaking them with the intent of causing embarrassment and public distrust. Session cookies are also exploited, granting the attacker initial access and enabling lateral movement toward areas of the network containing sensitive information, which can be leaked or used as extortion leverage.

- **Politically motivated** – Highly capable advanced persistent threat (APT) groups and nation state-sponsored or affiliated cyber capabilities use stealer malware to target both opposing state governments and associated NGOs, often in espionage campaigns. These threat actors are usually seeking to gather information that can be used to improve their geopolitical stature; achieve a strategic military, technological, or economic advantage; or conduct sabotage by stealing sensitive or proprietary information.

While almost certainly less prominent, a threat also exists from employees and other insiders, as well as competing organizations. Both can gain advantage from illicitly obtaining proprietary, trade, and customer information, with the former most likely seeking financial gain or punitive retribution and the latter pursuing a competitive edge over their rivals.

The majority of prominent stealers are operated as a service and are often advertised as either stealer-as-a-service (SaaS) or malware-as-a-service (MaaS). These services offer threat actors a multifaceted and relatively inexpensive method of deploying versatile malware and also lower the bar for required technical expertise. Many stealers are available to threat actors, offering a variety of stealing techniques, reputations, information targeted, prices, code languages, customizations, obfuscation methods, and antivirus evasion. As of the writing of this report, some of the most prominent stealers include StealC, Vidar, and LummaC2.

Stealer Service	Price Options	Features
StealC	USD 200 - 1 Month USD 500 - 3 Months USD 800 - 6 Months	- Steals information from web browsers, instant messaging platforms, and email clients - Can be configured with customized file-grabbing capabilities - Based upon other prominent stealers, such as Vidar and Raccoon
Vidar	USD 130 - 7 Days USD 200 - 14 Days USD 300 - 30 Days USD 580 - 60 Days USD 750 - 90 Days	- Steals information such as IP addresses, credentials, and banking data - Can be used to facilitate further malware - Customizable functionality
LummaC2	Different packages that include varying functionalities: USD 250 - "Experienced" USD 500 - "Professional" USD 1,000 - "Corporate"	- Targets information found in browser extensions, cryptocurrency wallets, and multi-factor authentication (MFA) tokens - Novel anti-sandbox techniques that aid in avoiding detection, evading security methods, and establishing persistence



Overview displaying the production, sale, and exploitation of a stealer log

Source: ZeroFox Collections

Brief | An Introduction to Stealer Logs

B-2024-08-20a

TLP: CLEAR



Country	Links
Buenos Aires F.D. ISP: Telecom Argentina S.A.	localhost localhost localhost localhost extranet.ort.edu.ar aulavirtual.instituto.ort.edu.ar 10.20.1.1 alumni.education allaccess.com.ar disneyplus.com
Buenos Aires ISP: Telecentro S.A.	campus.filo.uba.ar festival.movibeta.com rider.cabify.com campus.filo.uba.ar facebook.com es-la.facebook.com es-la.facebook.com id.rec.uba.ar elculturalsanmartin.tuentrada.com meetings.webex.cisco.com Show more...
Buenos Aires ISP: Telecentro S.A.	cablevision.com.ar id.apple.com telecentro.com.ar radiopaedia.org tickets.hoyts.com.ar guarani-medicina.unlp.edu.ar cytec.ddns.net servicioscorp.anses.gob.ar dytlatlata.org entradauno.com Show more...
Santa Cruz ISP: Red Intercable Digital S.A.	facebook.com canva.com mercadolibre.com auth.afip.gob.ar mobile.market.teamviewer.teamviewer.com www.afip freelancer.com account.box.com 192.168.1.1 idpsesion.telecom.com.ar Show more...
Buenos Aires ISP: Telecentro S.A.	netflix.com nudeishop.com.ar disneyplus.com chimera-tool.com
Buenos Aires ISP: Telecentro S.A.	mercadolibre.com facebook.com facebook.com mercadolibre.com accounts.google.com
Buenos Aires ISP: Telecom Argentina S.A.	sesion.personal.com.ar paypal.com id.argentina.gob.ar user.supermercadosdia.com.ar idpsesion.telecom.com.ar servidub.com.ar illis.com.ar idmsa.apple.com 181.31.120.144 sso.arba.gov.ar Show more...

Stealer logs advertised in Russian Market

Source: ZeroFox Collections

	Country	Seller	Files	Info	Date upload	
Links (413) Cookie (4364)	RS	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)	TR	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 \$

Stealer logs advertised in 2EasyShop

Source: ZeroFox Collections

| What Are Some Common Misconceptions Surrounding Stealer Logs?

“Data contained in stealer logs is new, relevant, valuable, and exploitable.”

- Stealer logs for sale often contain old or outdated credentials and information, many of which have appeared in numerous previous data breaches. By the time exploitation is attempted, victim users may have changed passwords or closed accounts, rendering the data obsolete. Stealer logs also often contain fake or manipulated information to bolster the file size and attract potential buyers.
- While some logs contain valuable corporate credentials, many are from personal devices with limited value to threat actors. Research indicates that about 1 percent of logs pertain to corporate victims.¹
- Not all data in stealer logs is immediately exploitable. Factors such as MFA, account lockouts, and changed passwords can limit the utility of stolen credentials.

“Organizational data in a stealer log must have come from a recent data breach.”

- Threat actors often compile stealer logs from multiple sources and timeframes. This means that a single compilation may contain information collected over an extended period, not just data from recent infections or breaches. Additionally, threat actors often resell and repackage stealer logs in various combinations. This can lead to fresher data sitting alongside older data, creating a misleading perception of the data’s recency.

“My organization or network was targeted specifically.”

- While stealer logs may contain corporate information, this does not necessarily imply that the organization was specifically targeted. The presence of such data is

¹ [hXXps://sosintel\[.\]co\[.\]uk/stealer-logs-what-you-need-to-know/](https://sosintel[.]co[.]uk/stealer-logs-what-you-need-to-know/)

often a result of broader, non-targeted malware campaigns that affect individual users who happen to have access to corporate resources. This information is often obtained via breaches of third parties when employees leverage corporate credentials on their personal devices or use corporate devices for personal use.

“My information in a stealer log indicates that a broad compromise of my network has taken place.”

- The presence of corporate credentials in stealer logs does not automatically mean the organization itself has been breached. The presence of corporate credentials in stealer logs is often a result of individual user compromises rather than a wider organizational breach.

| How Can the Threat Be Mitigated?

The diverse information found in stealer logs is leveraged for malicious activities by a range of threat actors of different capabilities and motivations. The mitigation strategies of individuals and organizations must therefore be equally holistic, addressing the full scope of network access vectors that can be targeted by an attacker in possession of credentials, cookies and tokens, or other browser data. Ensuring that basic cyber hygiene measures are properly enacted and scrutinized can reduce the likelihood of both being targeted by stealer malware and any subsequent exploitation.

- 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 MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform 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 DDW forums.
- Ensure employees are aware of contemporary cyber threats and educated in how to recognize and report suspicious activity.
- Configure ongoing monitoring for Compromised Account Credentials.

| 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%