January 2023

Dissecting the Dark Web Stealer Malware Lifecycle with the MITRE ATT&CK Framework

by Eric Clay

Table of Contents

Stealer malware is a type of Remote Access Trojan (RAT) that infects corporate and personal computers, establishes communication with command and control infrastructure (C2) and exfiltrates sensitive data. Variants of stealer malware include Raccoon, Vidar, Aurora, and Redline among others. Stealer malware infects computers, extracts valuable data such as browser fingerprints, cryptocurrency wallets, VPN logins, cached data, saved credentials, and system information. Threat actors then sell these logs for cybercriminals and other threat actors to purchase on specialized markets and Telegram channels.

Unlike traditional credential stuffing attacks, threat actors aren't buying one set of information and using it to try and breach many accounts, they are instead purchasing access to mimic a single user and gaining access to all of that user's passwords saved in web browsers and other data found on a host. In addition, in many cases logs will include active cookies which can be used for session hijacking attacks. Once purchased by the final threat actor in the supply chain, stealer logs can be used to facilitate account takeover attacks, financial fraud, and ransomware.

Executive Summary

- Infected Device Markets continue to grow on the dark web, clear web, and illicit Telegram channels.
- Even unsophisticated threat actors can steal information that allows them to impersonate a victim's browser fingerprint for as little as $10, and gain access to hundreds of unique logins stored in the browser, and the potential to bypass corporate 2FA Controls.
- Listings are often priced **based on the type** of logins that the infected device has access to.
- Monitoring for these listings manually is almost impossible, traditional approaches to dark web monitoring are often ineffective for finding IOC's related to infected device markets.
- Initial Access Brokers often buy stealer logs with sensitive corporate logins present, validate access, conduct additional reconnaissance, enrich data about the company, and then resell logs on specialized dark web forums for thousands to tens of thousands of dollars.
- Even in cases in which threat actors may not be able to use stealer malware to bypass MFA controls, they can always resort to MFA fatigue attacks.

The Lifecycle of a Stealer Malware Attack

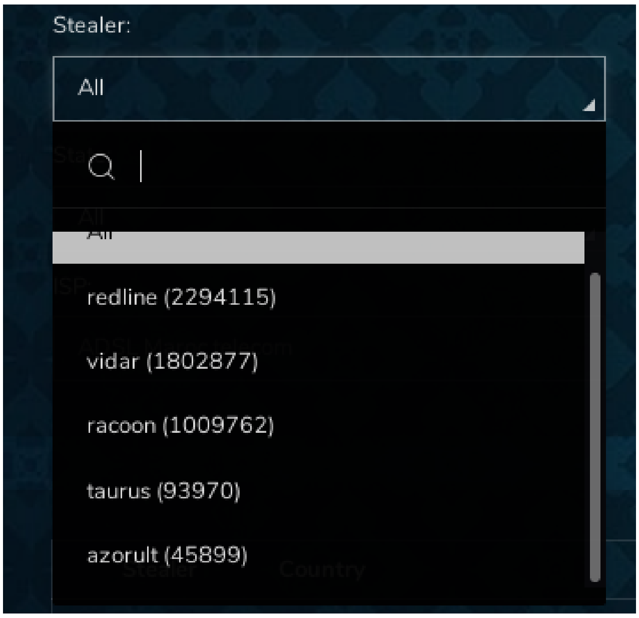
Much like a modern supply chain, stealer malware attacks don't happen in a vacuum, instead attacks are facilitated by a number of specialized threat actors across dark web markets and forums each performing a specific role. It is also worth noting that while there is a "standard" lifecycle, not all stealer malware attacks operate within it. It is not difficult to imagine a hacktivist or threat actor with a specific target in mind purchasing stealer malware, distributing it themselves against a target, and escalating privileges once initial access is established. However, generally speaking attacks happen in the following order:

1. **Malware as a Service (MaaS) vendor sells stealer malware and associated C2 infrastructure on specialized Telegram channels**
2. **Threat actor purchases malware and sets up or purchases distribution infrastructure**
3. **Stealer malware is distributed and executed on victims' computers**
4. **Data is exfiltrated back to C2 infrastructure**
5. **Threat actor/group sells logs on specialized markets and Telegram channels**
6. **Other threat actors purchase corporate logs through initial access brokers**
7. **Corporate logs with access to sensitive environments are auctioned off**
8. **A new threat actor purchases access and leverages it for financial fraud, account takeover attacks and Ransomware**

We're going to break down the process and align the stealer malware lifecycle with MITRE ATT&CK. We chose MITRE ATT&CK due to its relevance in enterprise system compromise and because we couldn't find any other vendors or researchers who had mapped it. It's worth noting that not every variant of stealer malware will align with each listed function on MITRE ATT&CK, and not every MITRE ATT&CK function will be applicable to every stealer malware variant. Instead, we tried to model the average attack, rather than map MITRE ATT&CK functions to every possible variation of stealer malware.

Stealer Malware Variants up for Sale (MaaS)

Stealer malware has been rapidly increasing in popularity since 2019 and is almost always purchased from a Malware as a Service (MaaS) vendor. These variants are typically sold based on either a lifetime license or a monthly subscription, and are exclusively available on dedicated Telegram channels. There are many stealer malware variants, but some of the most common ones we see are Vidar, Raccoon, Redline, Aurora, Prynt, Ducktail, Taurus, Azorult, and Jupyter. Newer variants fetch a higher premium, with Redline and Aurora currently leading in both their feature sets and sophistication. Aurora is a particularly high-risk variant and has unique features such as the ability to steal cached documents and PDF files. As of December 2022, Aurora also represents a significant threat since its novelty means that many anti-virus and EDR tools are unable to detect its associated signatures.



Stealer:

All

All

redline (2294115)

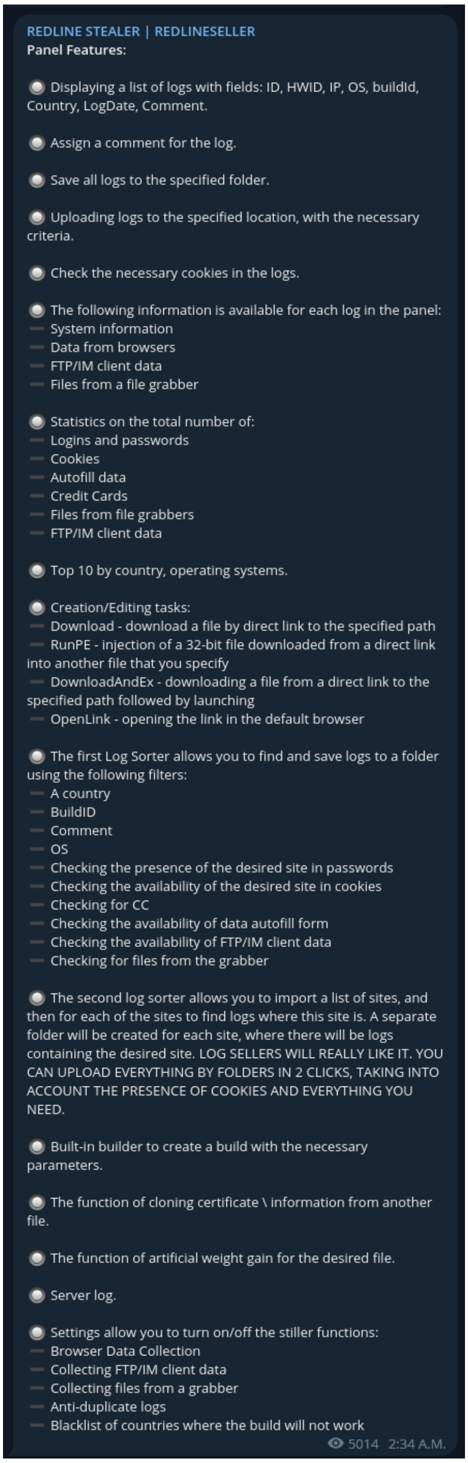
vidar (1802877)

racoon (1009762)

taurus (93970)

azorult (45899)

Stealer malware is typically sold with associated command and control infrastructure that provides actors a place to receive, sort, and extract valuable information from the logs received. For example a Redline C2P Panel is advertised as having the following features:



REDLINE STEALER | REDLINESELLER
Panel Features:

● Displaying a list of logs with fields: ID, HWID, IP, OS, buildId, Country, LogDate, Comment.

● Assign a comment for the log.

● Save all logs to the specified folder.

● Uploading logs to the specified location, with the necessary criteria.

● Check the necessary cookies in the logs.

● The following information is available for each log in the panel:
— System information
— Data from browsers
— FTP/IM client data
— Files from a file grabber

● Statistics on the total number of:
— Logins and passwords
— Cookies
— Autofill data
— Credit Cards
— Files from file grabbers
— FTP/IM client data

● Top 10 by country, operating systems.

● Creation/Editing tasks:
— Download - download a file by direct link to the specified path
— RunPE - injection of a 32-bit file downloaded from a direct link into another file that you specify
— DownloadAndEx - downloading a file from a direct link to the specified path followed by launching
— OpenLink - opening the link in the default browser

● The first Log Sorter allows you to find and save logs to a folder using the following filters:
— A country
— BuildID
— Comment
— OS
— Checking the presence of the desired site in passwords
— Checking the availability of the desired site in cookies
— Checking for CC
— Checking the availability of data autofill form
— Checking the availability of FTP/IM client data
— Checking for files from the grabber

● The second log sorter allows you to import a list of sites, and then for each of the sites to find logs where this site is. A separate folder will be created for each site, where there will be logs containing the desired site. LOG SELLERS WILL REALLY LIKE IT. YOU CAN UPLOAD EVERYTHING BY FOLDERS IN 2 CLICKS, TAKING INTO ACCOUNT THE PRESENCE OF COOKIES AND EVERYTHING YOU NEED.

● Built-in builder to create a build with the necessary parameters.

● The function of cloning certificate \ information from another file.

● The function of artificial weight gain for the desired file.

● Server log.

● Settings allow you to turn on/off the stiller functions:
— Browser Data Collection
— Collecting FTP/IM client data
— Collecting files from a grabber
— Anti-duplicate logs
— Blacklist of countries where the build will not work

5014 2:34 A.M.

> Threat Actors would still need to acquire, purchase or leverage existing compromised systems to use as infrastructure for attacks.

This phase of the attack maps to the Resource Development portion MITRE's ATT&CK Framework:

- **T1587 Obtain Capabilities**
  - **T1588.001 Malware:** The lifecycle of most stealer malware attacks begins with the threat actor purchasing access from a dedicated Malware as a Service (MaaS) Vendor on an Illicit Telegram Marketplace

- **T1583 Acquire Infrastructure**
  - **ID: T1583.001 Domain Infrastructure:** Setting up lookalike domains is a common tactic for both broad based phishing campaigns and spear phishing attacks against specific companies
  - **T1583.006 Web Services:** On average stealer malware comes with C2 Infrastructure needed to communicate, sort, and derive information from infected devices. Threat Actors must find other sources to acquire distribution infrastructure such as web services, virtual services, DNS, and other vectors.

Stealer Malware Distribution

Typically once access to a stealer malware variant is purchased either on a monthly or lifetime basis, the threat actor will look for ways to distribute it. In some cases an actor may purchase stealer malware in order to attack a specific target or industry that has already been defined. However, more often a group will purchase stealer malware with predefined distribution in order to gather logs then sell them via specialized marketplaces and Telegram channels; in many cases targeted at consumers with incidental corporate information capture as an added bonus.

We commonly see stealer malware variants distributed through phishing emails, malicious social media advertisements, infected office documents, hacked Facebook accounts, illicit software downloads, and malicious website popups. In other cases they may be included in “freeware” downloads for PDF editing software, video editing software, and other types of cracked software.

Surprisingly, many unsophisticated actors have relatively uninteresting use-cases such as stealing access to VPN accounts, Netflix accounts, and other low-value consumer applications. It is worth noting that personal VPN accounts seem to be of particular interest to many threat actors since numerous variants of stealer malware specifically seek to capture VPN credentials. However, many malware distributors deliberately target corporations and large enterprises in order to increase the value of a stealer log. As part of our stealer malware report in early 2022, we found that on average 53% of accounts for sale on Russian Market were Windows 10 Enterprise accounts, suggesting that fingerprints with corporate access are a lucrative target for threat actors. This phase of the lifecycle maps to **the initial access phase** of the MITRE ATT&CK lifecycle and includes the following tactics:

- **T1189 Drive-by Compromise:** Stealer malware is often distributed through illicit ads, pop ups, and other mediums on legitimate websites
- **T1133 External Remote Services:** In some cases threat actors may purchase credentials to accounts, or even infected devices with access to VPNs and other corporate information to use as a vector to enhance distribution of malware within the organization
- **T1566 Phishing:**
  - **T1566.003 Spear Phishing Via Service:** Certain threat actors may opt to send spear phishing messages containing stealer malware via LinkedIn, Facebook, Twitter, and other social media sites rather than directly send links or attachments to a corporate email address. We would expect to see this behavior with more targeted/sophisticated threat actors that have specific targets in mind
  - **T1566.002 Spear Phishing Link:** In many cases threat actors may include a link with a sense of urgency to click on it, purporting to be from the board of directors, CEO, or other key executives. Clicking on the link will typically take the user to a third-party site where stealer malware would be automatically downloaded and executed on the device
  - **T1566.001 Spear Phishing Via Attachment:** Stealer malware can also be incorporated into .pdf and .doc files through Macros and delivered via phishing email campaigns
- **T1078 Valid Accounts :**
  - **T1078.004 Cloud Accounts:** Sophisticated threat actors with a specific target in mind may purchase credentials and compromise cloud email or social media accounts to use as a mechanism for distribution of stealer malware to other trusted parties to abuse Trusted Relationships

The Stealer Malware has been Distributed. Now What?

Each variant of stealer malware works slightly differently with various measures in place to maintain persistence, bypass existing security software, and report back to C2 infrastructure so we will use a general example . Once stealer malware has been distributed there are typically a few steps that are required before it can begin exfiltrating data back to C2 infrastructure.

- Stealer malware is downloaded or installed through illicit ads, freeware, or phishing emails
- Typically a .exe is downloaded with a powershell script, which is used to obfuscate the malicious code
- Persistence mechanisms are added such as creating registry keys and adding itself to startup
- Junk files are created to make detection & analysis more difficult
- Malware begins attempting to establish live communication with C2 Infrastructure
- Additional modules are remotely downloaded from C2 infrastructure
- Host information, screen capture, and initial logs are sent back to C2 infrastructure
- Continuous data exfiltration from the infected machine begins

Each variant of stealer malware targets different types of information on a computer. At a base level, most attempt to capture:

- OS Version
- ISP
- Active Cookies
- IP Address
- FTP Client
- VPN Credentials
- Browser Cache (found in some variants)
- Geographic Location of the Device
- Browser Fingerprints (To be used for session hijacking and account compromise via saved credentials)
- Cryptocurrency Wallets
- Browser History
- Saved Credit Cards

This phase maps to MITRE ATT&CK's Execution, Persistence, and Defense Evasion.

Execution:

- **T1203 Exploitation for Client Execution:** Every variant of stealer malware requires the exploitation of vulnerabilities in code for an OS and often a web browser as well. Most commonly, multiple files are downloaded and powershell is used to execute in the background with some versions not requiring malware to be written to the disk
- **T1204 User Execution:** Once stealer malware has been downloaded onto the device from a cracked application, malicious link, or other some variants require a document or file to be opened first, with some variants executing when the file is closed
- **T1407 Windows Management Instrumentation:** Variants of Stealer Malware such as Aurora execute commands via Windows Management Instrumentation in order to collect system information[1]

Persistence:

- **T1547 Boot or Logon Autostart Execution:** Variants of stealer malware like Jupityr aren't written to the disk, but instead use registry keys to autostart on system startup, providing an additional layer of obfuscation and making it more difficult for anti-virus and EDR platforms to detect signatures[2]
- **T1543 Create or Modify System Process:** Certain variants of stealer malware such as Redline use system processes to extract system information

Defense Evasion:

- **T1036 Masquerading:** Most variants will either randomize process and file names or run under seemingly innocuous names to disguise harmful activity. Some variants of Redline are saved with the filename winlogin.exe
- **T1112 Modify Registry:** Some variants of stealer malware like Aurora and Redline modify the registry to enable the unobfuscated malware to load on system startup
- **T1027 Obfuscated Files or Information:** Numerous Stealer Malware variants include obfuscation to make it more difficult for EDR & Anti-virus systems to detect it. For example, Blackguard uses powershell to enable obfuscation, while Redline is obfuscated in .NET executables[3, 4]

[1] https://www.bleepingcomputer.com/news/security/aurora-infostealer-malware-increasingly-adopted-by-cybergangs/
[2] https://blogs.blackberry.com/en/2022/01/threat-thursday-jupyter-infostealer-is-a-master-of-disguise
[3] https://blogs.blackberry.com/en/2021/07/threat-thursday-redline-infostealer
[4] https://www.zscaler.com/blogs/security-research/analysis-blackguard-new-info-stealer-malware-being-sold-russian-hacking

Stealer Malware Collection & Exfiltration

Once a system is infected and the stealer malware has established communication with C2 infrastructure, data collection & exfiltration begins. The specific type of collection that occurs heavily depends on the variant in question, with newer variants typically featuring advanced capabilities to collect more information across the infected system.

Broadly speaking most begin by stealing credentials from password stores such as browsers, along with cookies and metadata that can enable threat actors to conduct session hijacking attacks using stored cookies. Cryptocurrency wallets, VPN credentials, and FTP client information are also targets of almost all variants.

Credential Access:

- **T1555 Credentials from Password Stores**
  - **T1555.003 Credentials from Web Browsers:** Stealing credentials & metadata from web browsers is a core component stealer malware, The number and type of stolen browser credentials heavily influence the value of the malware at later stages of the lifecycle if it resold
- **T1056 Input Capture**
  - **T1056.001 Keylogging:** Some variants such as Gomorrah incorporate keylogging capabilities which can be used for sending 2FA tokens back in near-real time to threat actors to compromise secured accounts
- **T1539 Steal Web Session Cookie:** Web session cookies are stolen and exfiltrated back to C2 infrastructure to be used for session hijacking and bypassing multi-factor authentication controls

Discovery:

- **T1217 Browser Bookmark Discovery:** Most variants of stealer malware will export a full browser fingerprint including bookmarks saved in the browser
- **T1083 File and Directory Discovery:** Prior to data exfiltration, most stealer malware will perform File and application discovery to identify cryptocurrency wallets, VPN credentials, and FTP credentials
- **T1518 Software Discovery**
  - **T1518.001 Security Software Discovery:** Most Stealer Malware variants return the anti-virus software installed which is then listed as logs are resold on dedicated marketplaces. For example Redline uses a WMI Query to obtain a list of firewalls, anti-virus, and antispyware software being run on the infected machine[5]
- **T1082 System Information Discovery:** All variants of stealer malware collect basic information about the host which is sent back to C2 infrastructure and listed as part of a marketplace listing. System information collected typically includes:
  - Operating System
  - IP Address
  - Location
  - ISP

Collection:

- **T1560 Archive Collected Data:** Prior to exfiltration data will be compressed and sent back to C2 infrastructure. The methodology used varies by the type of stealer malware being sent. Some variants such as Jupytr encrypt data prior to exfiltration in order to avoid packet sniffing and anomaly detection[6], while others simply encode information in base64[7]
- **T1119 Automated Collection:** Data is automatically collected from the system, with some variants allowing for cached data to be collected
- **T1115 Clipboard Data:** A few variants such as Aurora collect data found in the clipboard for exfiltration

[5] https://securityscorecard.com/research/detailed-analysis-redline-stealer
[5] https://blogs.blackberry.com/en/2022/01/threat-thursday-jupyter-infostealer-is-a-master-of-disguise
[5] https://www.bleepingcomputer.com/news/security/aurora-infostealer-malware-increasingly-adopted-by-cybergangs/

Exfiltration:
T1020 Automated Exfiltration: Once credentials, screenshots, host data, and other sensitive information have been collected data is automatically exfiltrated to C2 infrastructure, either through Base64 without encryption, or through encrypted channels.

A Tale of Three Platforms: Stealer Logs for Free and Stealer Logs for Sale

After collection, there are multiple things that could happen. If the attack has been targeted the threat actor may directly use the information provided or attempt to escalate privileges and compromise additional accounts with newfound access. However, in most cases those utilizing stealer logs are focused on commercializing them and selling them to other threat actors who will then use them to perpetrate fraud schemes.

Stealer logs are commonly found for sale on two dedicated marketplaces, Genesis Market and Russian Market, as well as innumerable illicit Telegram channels.

Genesis Market:
Genesis Market is operated as clear web marketplaces and clearinghouse for stealer logs. Genesis is one of the easier to use marketplaces, and includes easy software to mimic purchased browser fingerprints to make their offering valuable to even unsophisticated threat actors.
When buying a bot on Genesis, the malicious actor not only gains access to the victim's credentials of all listed "Resources", but the marketplace in itself offers a very detailed guide explaining how to use the bot fingerprint.

The listings on Genesis provide the following information before purchase:

- The country where the bot is located
- The number of resources attached to the bot
- The number of browsers from which information was stolen (Fingerprints)
- The date on which the bot was installed, and last updated
- A partial IP address
- The operating system of the bot
- A list of all resources available

Russian Market:
Russian Market is a dark web shop, specialized in the sale of various fraud-related items; from stolen credit cards, Paypal accounts, to our subject at hand, Stealer Logs. When browsing for Stealer Logs, each listing contains information about the victim's device; you can usually expect to find:

- The stealer malware family
- The computer's operating System
- The country in which the computer is located
- A list of the services (websites) for which a login is available
- The directory content of the archive made by the stealer software
- The date on which the device was infected

Illicit Telegram Channels:
The way that Stealer malware is distributed on Telegram channels varies widely based on the channel. In many cases, logs may be given out for free, sometimes in the hundreds of thousands, with access to "VIP" channels put up for sale for a monthly subscription fee. In one particular case we noted a room for sale for $100/monthly which provided access to a minimum of 1000 new logs per day, with a specific room for "VIP's" accessible for $150/monthly and limited to only a few users.

Infected Device Pricing

It is worth taking a moment to examine how threat actors are pricing and packaging infected devices. Our analysis found that multiple factors can heavily influence the price of an infected device to include:

- Geographic location (Bots within the U.S., Canada, and Europe are typically priced higher)
- Types of logins, devices with access to financial services accounts typically fetch a higher price
- Age, the older an infected device is the less valuable it is as it is more likely to be discovered and cookies are more likely to be expired
- Number of log-ins included

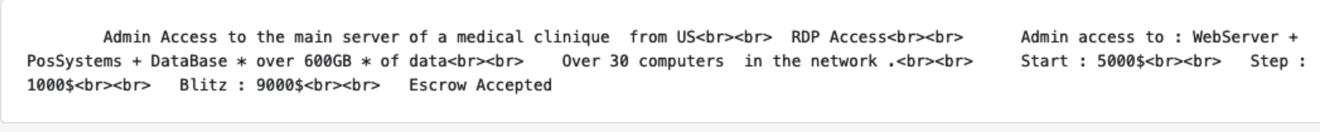
Salvagers, Initial Access Brokers, and Dark Web Forums

A select few stealer logs don't go directly to market. Instead they are diverted based on the types of logins they contain, to be resold by Initial Access Brokers for thousands, rather than hundreds of dollars. Highly sophisticated threat actors sift through thousands of stealer logs to find a diamond in the rough.

Examples "high value" logs include those with logins such as:

- Corporatename.passwordmanager.com
- Vpn.corporatename.com
- Corporatename.wordpress.com

And other combinations that could indicate access to valuable internal corporate logins which could be used to further escalate privileges. These logs are then often auctioned off on highly specialized dark web forums through Initial Access Brokers, which sell access to corporate IT environments rather than stealer logs themselves.

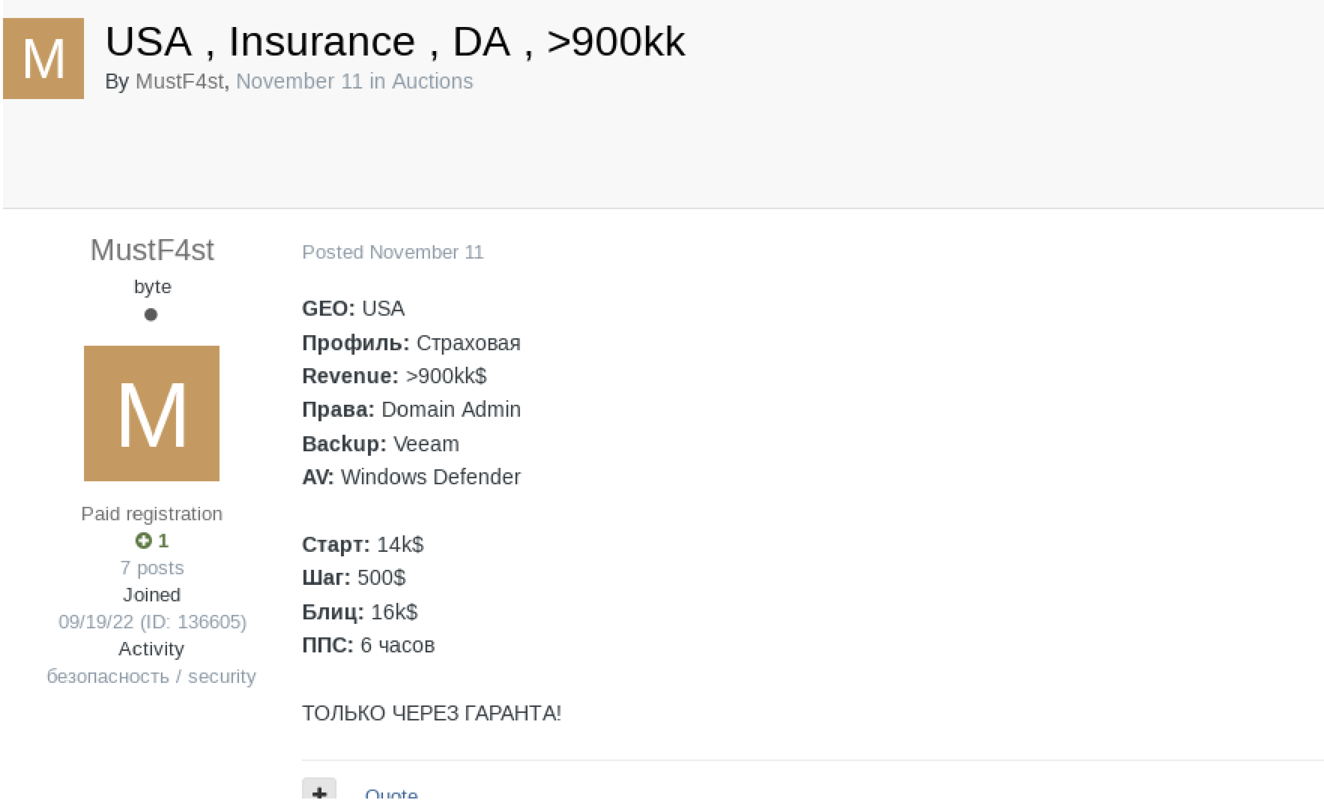


```
        Admin Access to the main server of a medical clinique  from US<br><br>  RDP Access<br><br>      Admin access to : WebServer +
PosSystems + DataBase * over 600GB * of data<br><br>    Over 30 computers  in the network .<br><br>     Start : 5000$<br><br>   Step :
1000$<br><br>   Blitz : 9000$<br><br>   Escrow Accepted
```

White Glove Cybercrime Service: What is the Value of an IAB

Initial Access Brokers take stealer logs a step further, validate access, and potentially move laterally through networks and services to build value for the end purchaser. The price that IAB's charge typically varies based on the type of access established, the number of hosts, the revenue of the company in question, and whether bank accounts have been compromised. One of the more interesting trends we have seen in recent years is that IAB's seem to be openly using third-party data enrichment solutions often used by corporate sales teams. In many cases they will abstract away the details of the initial compromise as part of the auction.

It is worth thinking of IAB's as the white glove service for cybercriminals. Rather than selling raw logs, they add value through reconnaissance, data enrichment, validation of access, and in some cases access expansion.



M

USA , Insurance , DA , >900kk

By MustF4st, November 11 in Auctions

MustF4st

byte

●

M

Paid registration

⊕ 1

7 posts

Joined

09/19/22 (ID: 136605)

Activity

безопасность / security

Posted November 11

GEO: USA

Профиль: Страховая

Revenue: >900kk$

Права: Domain Admin

Backup: Veeam

AV: Windows Defender

Старт: 14k$

Шаг: 500$

Блиц: 16k$

ППС: 6 часов

ТОЛЬКО ЧЕРЕЗ ГАРАНТА!

Prices can vary significantly based on the information, size of the company, and the level of access gained. Ranging from a few hundred dollars for access to small organizations, to tens of thousands of dollars for access to enterprise accounts with associated bank accounts. Information that initial access brokers list typically includes:

- Geographical Location
- Company Revenue
- Type of Access Obtained
- AV/EDR Tool Employed
- Industry
- Number of Devices Compromised (if applicable)

Much like a legitimate auction, a starting price is listed, along with step prices and a “blitz” price which functions as a buyout to end the auction early with payments typically being made in Monero or Bitcoin.

Leveraging Access

The final step in the stealer malware lifecycle is the final purchaser leveraging the obtained access to either directly deliver malware or ransomware, commit financial fraud, or attempt to escalate privileges with the information obtained.

With some additional steps towards impersonation, threat actors may be able to hijack active session cookies to bypass 2FA controls to log directly into accounts. In other cases the actor may need to couple social engineering with credential access, through a tactic like MFA Bombing or spear phishing.

Double & Triple Extortion Ransomware Attacks

Delivering ransomware is an obvious application for purchased stealer malware logs. With browser credentials, active session cookies, and potential access to corporate infrastructure, it is relatively easy for threat actors to abuse trusted relationships and deliver ransomware across an enterprise. Ransomware gangs and more sophisticated threat groups may attempt to launch double and triple extortion ransomware campaigns designed to exert maximum pressure to force the victim to pay the ransom.

Financial Fraud

Almost all attacks by cybercrime groups are financially motivated in the end, the primary difference between most attacks is how they plan to monetize it. Attacks can be monetized through ransomware, extortion, credential theft & reselling, intellectual property theft, selling confidential records, and by conducting direct financial fraud. In many cases stealer logs may contain logins to bank accounts directly, or access may be enhanced through an IAB that provides credentials to multiple accounts. Threat actors can then log-in directly and begin transferring money to offshore accounts or convert cash into cryptocurrencies such as ETH, BTC, or Monero.

Credential Compromise and Reselling

In cases where valuable corporate access has been compromised through stealer malware, threat actors may attempt to escalate privileges and move laterally through cloud services or a network in order to gain access to credentials. These can then be resold on dark web marketplaces and Telegram channels.

APT's & Persistent Access

While there are few documented cases, it is not difficult to imagine APT's leveraging stealer logs sold on marketplaces to enhance existing access or establish presence in a corporate environment in order to carry out further attacks at a later point in time.

This phase maps to MITRE ATT&CK Impact Phase

- **T1531 Account Access Removal:** Utilizing browser fingerprints coupled with stolen credentials and data is a common way for adversaries to facilitate account takeover attacks. Victims may be locked out of legitimate accounts, permissions may be changed, and adversaries may attempt to gain access to additional accounts
- **T1485 Data Destruction:** Data may be altered or destroyed depending on the motivations of the adversary
- **T1486 Data Encryption for Impact:** Stealer Malware can be leveraged as a mechanism to facilitate account takeover attacks and privileged network access enabling delivery of ransomware

Disrupting the Stealer Malware Supply Chain: Concrete Recommendations

Stealer Malware attacks aren't as easy to disrupt as traditional dark web driven credential stuffing attacks. Accurately identifying IOC's related to devices infected with stealer malware requires several additional steps compared with simply monitoring corporate email accounts to ascertain whether they are part of a data breach. The following are best practices you can use to mitigate the risk of stealer malware to your organization & improve detection capabilities for listings that may contain logins unique to you.

- **Keep Virus Definitions up to Date:** Much like a nuclear arms race, Malware as a Service groups continually innovate to avoid detection. Keep virus definitions up to date to protect against older variants of stealer malware. Many anti-virus solutions likely won't include definitions for newly released variants such as Aurora, however they can improve detection & remediation capabilities for older variants such as Raccoon

- **Improve Password Governance:** Employees often work-from-home and use personal devices in accordance with BYOD policies. This can result in corporate log-in's being stored as saved passwords in browsers such as Chrome, Firefox & Safari, representing an excellent target for theft. Utilize a password manager company wide, require MFA controls to access the password manager using authentication tokens, and disallow "remember this device" settings, requiring 2FA for each log-in

- **Monitor Infected Device Markets:** Due to the nature of how stealer logs are sold, there is rarely directly identifiable information listed on a marketplace without making a purchase. However, partial IP's, geographic locations, and internal corporate domains often provide enough context to allow security teams to narrow down potential infected machines

- **Set Up Automated Processes to Detect Newly Staged Attack Infrastructure:** Prior to conducting a targeted attack, threat actors often set up lookalike domains and email infrastructure designed to impersonate your organization. Conducting continuous cyber reconnaissance for lookalike domains and other malicious infrastructure can provide an early warning of an impending attack

- **Utilize Web & Email Filtering to Screen Malicious Sites and Emails:** The precise distribution method of stealer malware depends heavily on the adversary responsible. However the vast majority is distributed through cracked software, phishing emails, drive by downloads, and other easily defeated vectors. Robust web and email filtering can significantly reduce the potential exposure to infostealer malware downloads

Reducing risk from stealer malware attacks is an exercise in defense in depth. No single control or family of controls will likely be sufficient to reduce risk to an acceptable inherent level. Instead risk must be reduced by layering controls across multiple families from technical controls like web filtering, IDS & IPS, to governance controls such as minimum password standards and routinely updating anti-virus products.

About Flare Systems

Flare is the proactive external cyber threat detection solution for organizations. Our AI-driven technology constantly scans the online world, including the dark and clear web, to discover unknown events, automatically prioritize risks and deliver actionable intelligence you can use instantly to improve security.

Want to learn about how Flare can support dark web monitoring for leaked credentials?

Free Trial   Book a Demo

flare.systems
hello@flare.systems