# The Growing Threat from Infostealers

secureworks.com/research/the-growing-threat-from-infostealers

## Summary

Secureworks® Counter Threat Unit™ (CTU) researchers have observed infostealers (also known as stealers) playing an increasingly important role in the cybercrime ecosystem. This type of malware can steal sensitive information such as login credentials, financial details, and personal data from compromised computers and networks. Infostealers can be installed on a computer or device via phishing attacks, infected websites, and malicious software downloads. Once installed, they can execute and exit very quickly; many infostealers finish collecting and transmitting stolen data within several seconds to a minute of total runtime. The data is then packaged and sold as logs. Threat actors could use stolen credentials in these logs to gain unauthorized access to enterprise networks via remote access services such as virtual private networks (VPNs) and Microsoft Office Web Access (OWA). This unauthorized access can result in the exfiltration of sensitive data or the deployment of ransomware, which can cause significant financial loss and reputational damage. Although the name 'infostealer' implies data theft, this malware has evolved over time to include deployment of additional tools and malware.

## Underground forums and marketplaces

Infostealers are often sold as a monthly subscription service. The price can range from $50 to over $1,000 USD per month for access to a stealer command and control (C2) server operated by the developer. The service often features a range of support functions, including multiple ways to view, download, and share stolen data. Self-hosted stealer C2 servers are also available and are usually sold for a flat fee.

Underground forums provide a shared space for threat actors to discuss ongoing projects, request new features, and provide malware reviews. They also offer a marketplace to advertise new and existing stealers. Underground forums such as XSS . is and exploit . in are popular with threat actors involved in the development and deployment of infostealers.

These forums consist of subforums and sections that host a range of topics. They also contain administrative areas to control announcements, sales, and memberships. Many underground forums have a dedicated marketplace and enforce stringent rules to sell illegal products such as infostealers. Larger, high-profile forums offer an escrow service to mediate transactions between vendors and customers, building trust in the marketplace and providing a degree of control over interactions.

Stealer logs are available from underground forums, marketplaces, and other online platforms that cater to threat actors interested in obtaining credentials, financial information, personal data, banking details, cryptocurrency wallets, and other sensitive, secret, or valuable information. These marketplaces are often only accessible through Tor or the Invisible Internet Project (I2P) anonymity services and usually have strict rules and regulations regarding the types of information that can be traded. The offerings are typically only accessible to members who have been approved by the marketplace's administrators or who pay an entry fee. Some marketplaces only sell infostealer logs and have built their infrastructure to facilitate these transactions. Other forums offer many illicit wares for sale and have sections that include logs obtained from infostealers.

A burgeoning market also exists for after-action tools. Infostealers can lower the bar for entry to cybercrime, but the uninitiated can find the logs to be challenging to parse. Multiple vendors sell tools to assist in log parsing, enabling cybercriminals to extract data of interest from the raw logs.

## Russian Market

Russian Market is by far the biggest underground marketplace for infostealer logs, and it has ties to the now-defunct Amigos Marketplace. As of this publication, Russian Market offers over five million logs for sale, which is roughly ten times more than its nearest rival. Historically, the marketplace predominantly sold logs obtained through five infostealers: RedLine, Raccoon, Vidar, Taurus, and AZORult. As of late February 2023, it stopped carrying Taurus and AZORult logs. Since December 2022, researchers observed RisePRO

infostealer logs for sale through the marketplace, although total offerings remain low. Table 1 lists the number of infostealer logs for sale on Russian Market as of the end of February 2023.

| Stealer | Number of available logs |
|---|---|
| Raccoon | 2,114,549 |
| Vidar | 1,816,800 |
| RedLine | 1,415,458 |
| RisePRO | 3,833 |
| Total | 5,350,640 |

*Table 1. Number of infostealer logs available for purchase on Russian Market as of the end of February 2023.*

In October 2022, Russian Market changed its operating model to allow users to preorder credentials (see Figure 1). This feature requires that buyers deposit $1,000 USD into the site's escrow system. Buyers can then request credentials based on a domain name (from a specific organization) or a 'mask' (from a specific application). Although there are no guarantees that preorders will be fulfilled, this feature could lead to specific targeting of organizations and sectors rather than relying just on opportunistic attacks.

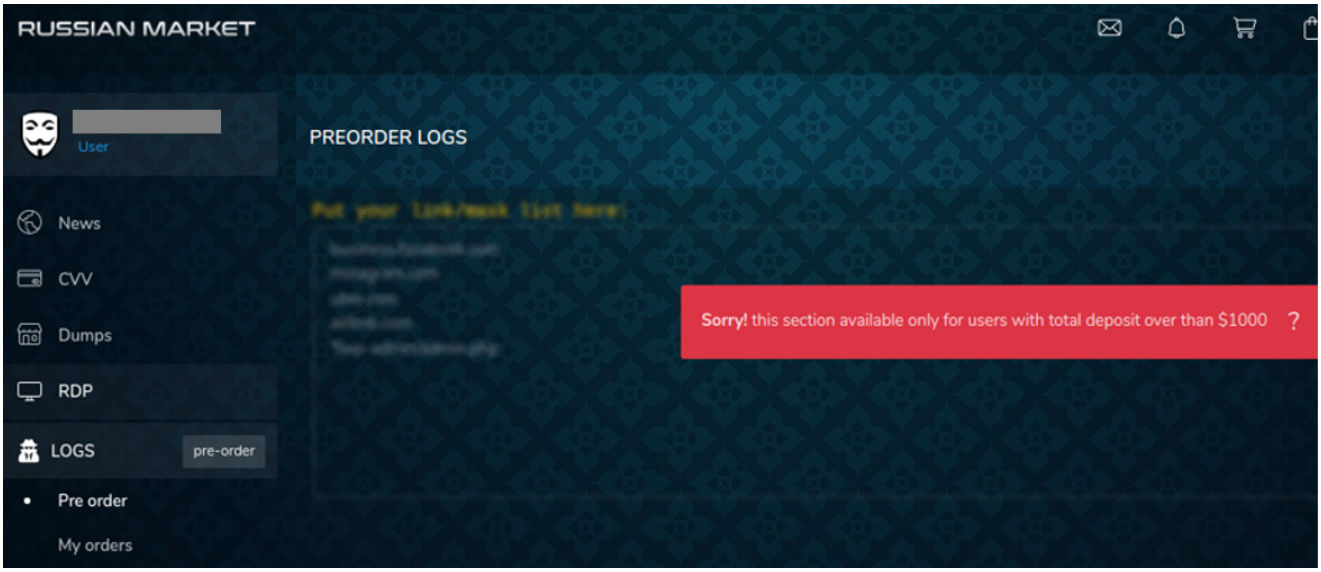

*Figure 1. Russian Market interface for preorder logs. (Source: Secureworks)*

## Genesis Market

Genesis Market is an invitation-only marketplace that specializes in the sale of bots rather than logs. Bots are computers that were infected with infostealer malware to steal information and the browser fingerprint from a victim's web browser. The browser fingerprint can be used to impersonate the victim and access the victim's bank accounts, take over accounts, and make fraudulent purchases. A threat actor who purchases a bot has exclusive access to the data, including updates of the victim's data from the infected device.

Genesis Market provides a custom browser plugin to customers and distinguishes itself among the competition by including more automation for site users. These features effectively render the bots as logs, removing the need to manually parse details and lowering the technical bar to entry. As of February 2023, Genesis Market listed over 450,000 bots from nearly every country (see Figure 2).

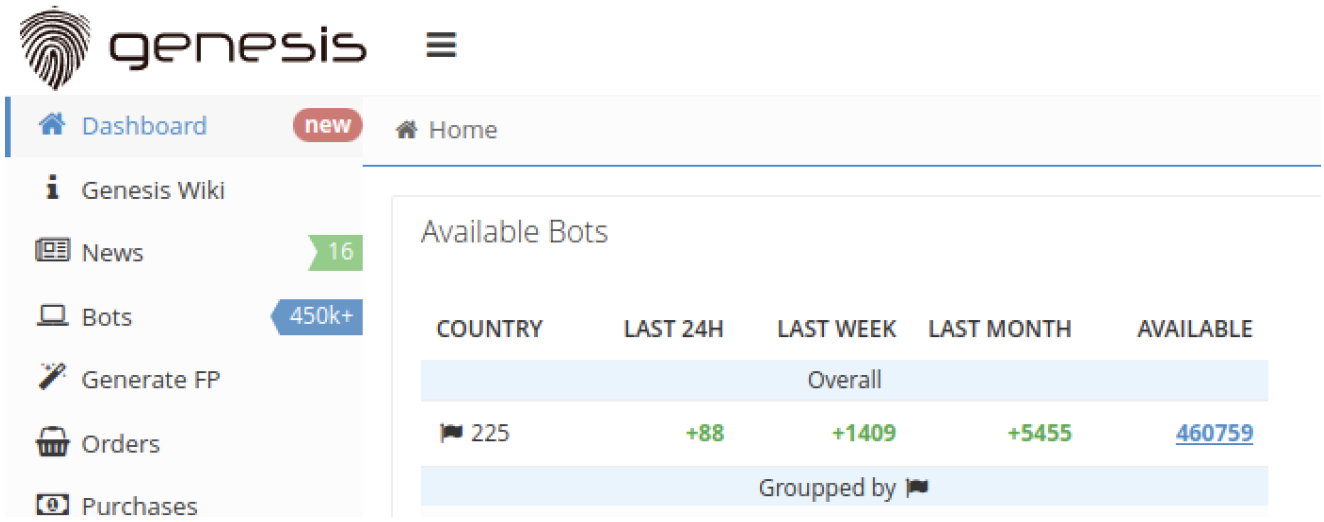


*Figure 2. Number of available bots for sale on Genesis Market as of February 2023. (Source: Secureworks)*

On April 4, 2023, Genesis Market was the target of a coordinated international law enforcement action led by the U.S. Federal Bureau of Investigation (FBI). Despite the arrests of multiple users and the takedown of 11 domains, Operation Cookie Monster did not completely shutter the marketplace. As of this publication, the Tor version of Genesis Market remains operational. Logs have been added for sale since the takedown, albeit at a slower rate than usual.

## 2easy

The 2easy marketplace has rapidly grown since it was established in 2018. Like Genesis Market, 2easy is automated, allowing buyers to add money to wallets and purchase logs without directly interacting with the seller. Unlike other sites, 2easy does not provide samples or previews. However, logs are reportedly less expensive than those on Genesis Market and Russian Market.

Threat actors who purchase logs through the 2easy marketplace receive an archive file from the selected bot. The file's content depends on the stealer and its unique capabilities. RedLine has historically been the favorite infostealer for threat actors selling logs through 2easy, but the marketplace also sells Raccoon, Vidar, and AZORult logs. As of February 2023, 2easy offered over 750,000 logs for sale (see Figure 3).

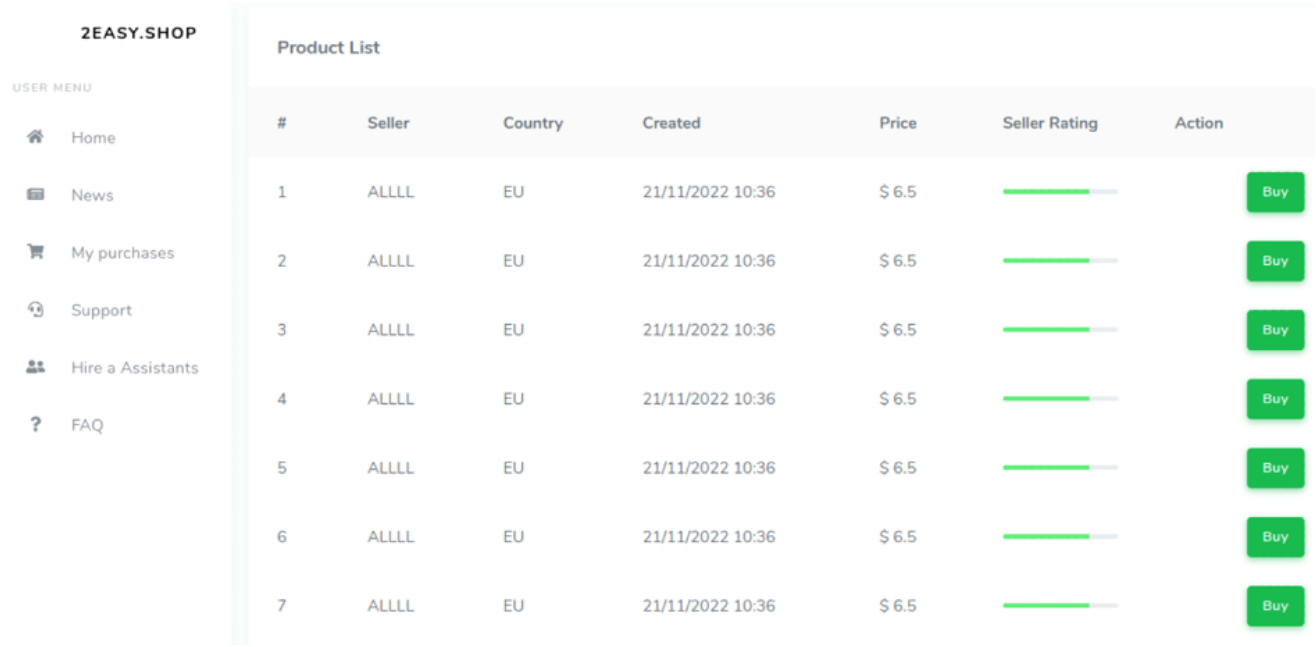


*Figure 3. Logs for sale on the 2easy marketplace. (Source: Secureworks)*

## Telegram

As demonstrated by the April 2023 Genesis Market takedown, one of the risks to sellers using traditional forums and marketplaces is the threat of law enforcement action. Another example was RaidForums, which was established in 2015 and became one of the most popular criminal marketplaces offering credentials and infostealers. In 2022, a coordinated international law enforcement investigation dubbed Operation TOURNIQUET resulted in the seizure of three domains and the arrest of RaidForums's founder and chief administrator. In addition, several cybercrime forums were breached in 2021 and their user data was stolen and either leaked or sold online. These takedowns and breaches undermine the security and integrity of the platforms and can degrade sellers' confidence in the anonymity offered by the forums. As a result, many cybercriminals use the Telegram messaging platform to advertise their services.

Telegram is a multi-platform messaging service that has an estimated 700 million monthly users. Benefits of this platform for cybercriminals include its focus on privacy, encryption, and an open-source application programming interface (API) that allows 'unofficial clients' (alternative messaging apps that use Telegram's API) to communicate with the official app and web interface. The end-to-end encryption and support for private and anonymous channels are ideal for selling and trading stolen data and information. Telegram users can

subscribe to channels on which owners can post content, or they can become members of groups and participate in discussions. Cybercriminals use these channels and groups to sell infostealers such as Titan Stealer. Some channels are hidden and require specific invitations or permissions to access. There has reportedly been a significant increase in the use of Telegram to sell illicit goods and services. Over 120,000 messages were published across more than 300 Telegram public channels and groups between the beginning of 2019 and the second quarter of 2022. RedLine, Anubis, SpiderMan, Oski Stealer, and Loki Stealer are prominently represented on Telegram. RaccoonV2 operators extensively use Telegram for announcements, business discussions, and reporting stolen data.

Despite the simplicity of selling goods over Telegram, it remains more popular for selling illicit goods such as drugs rather than for selling malware due to its primary function as a messaging platform. This limitation makes it difficult for sellers to migrate from traditional underground forums and marketplaces that feature advanced search capabilities and a way for sellers to build reputation, which is important when establishing trust with buyers. CTU™ researchers have observed scammers on Telegram mimicking real threat actors by creating fake profiles based on listings from forums such as Breached. This lack of reputation status and the prevalence of scammers is likely to undermine trust, preventing threat actors from fully adopting Telegram.

## Infostealer variants

Infostealers rose to prominence in 2006 with the ZeuS trojan, which targeted online banking credentials. After the ZeuS source code was leaked in March 2011, the creation of multiple variants boosted the popularity of this type of malware and inspired the development of infostealers with increasingly sophisticated capabilities. Some infostealers can be tailored or customized for specific targets and goals. For example, LokiBot has been prominent since 2016 and was one of the first infostealers that targeted the Android operating system. The Ducktail infostealer was first observed in 2022 and specifically targeted Facebook business accounts. Infostealers such as BHUNT specialize in stealing cryptocurrency, while state-sponsored threat groups such as IRON TILDEN use custom versions to conduct espionage.

CTU researchers analyzed the Russian Market marketplace to understand each infostealer's properties and capabilities. The table in the Appendix compares features of the most common infostealers in 2022 but may not be a comprehensive view. Much of the information related to targeted browser extensions and applications is only found through the infostealer configurations. These configurations specify what information to extract from a compromised system, but they frequently change.

### RedLine

RedLine emerged in March 2020, and its logs are the best seller on Russian Market. RedLine is sold standalone or as a subscription. As of March 2023, standalone copies (the 'PRO' version) were advertised on Telegram for $900 USD, with subscriptions available for $150 per month or $400 for three months (see Figure 4). This malware steals information from web browsers, including saved credentials, autocomplete data, credit card information, and cryptocurrency wallets. While running on an infected system, RedLine takes a system inventory of the username, location data, hardware configuration, and installed security software.

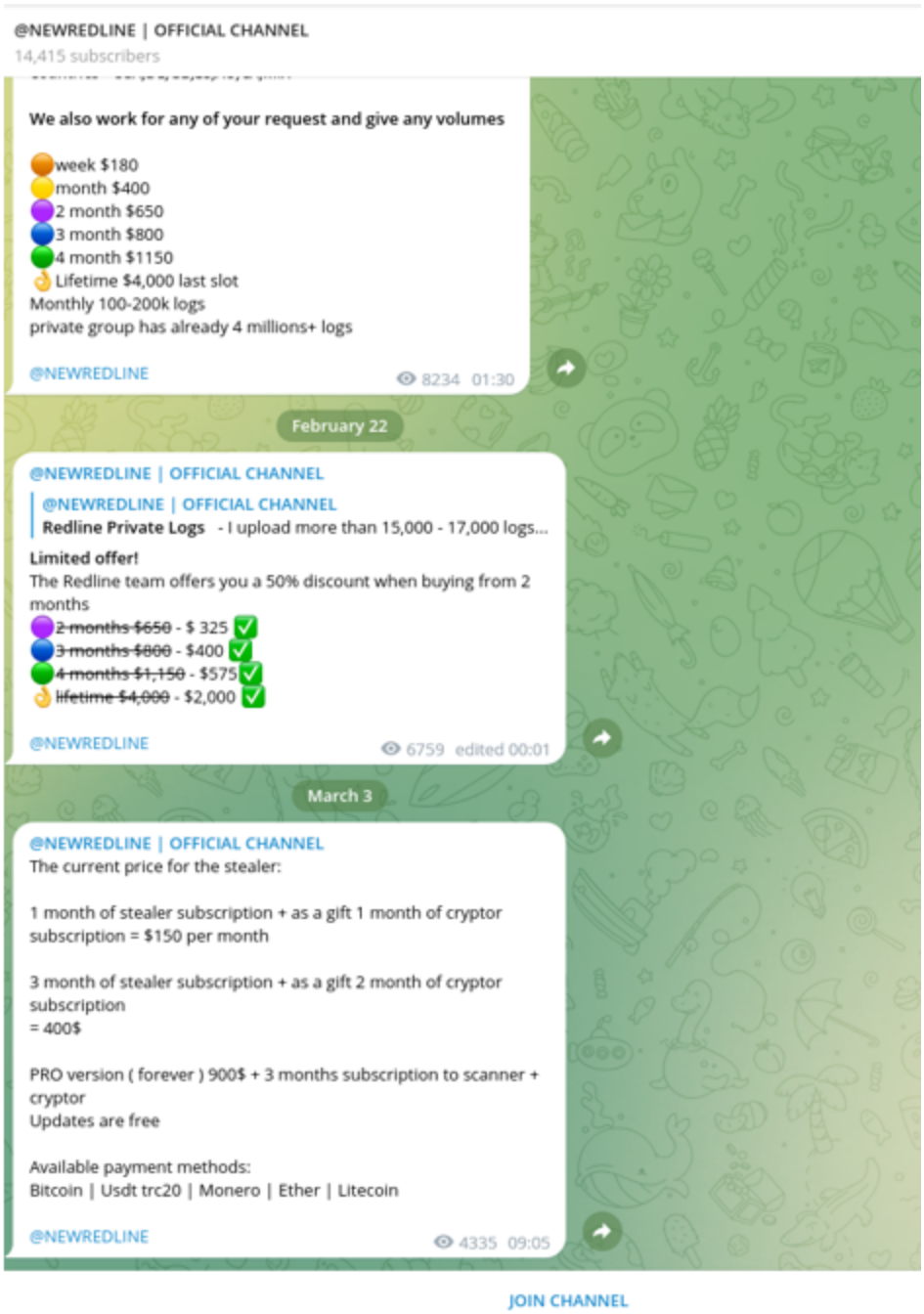


*Figure 4. RedLine Telegram channel listing prices and deals. (Source: Secureworks)*

RedLine is distributed via cracked games, applications, and services, as well as via phishing campaigns and malicious ads. CTU researchers have observed multiple instances of threat actors using malicious Microsoft OneNote files to deliver RedLine. RedLine has also been observed using YouTube for self-propagation and has been linked by CTU researchers to SM Viewbot malware. SM Viewbot promotes YouTube videos to lure users who are searching for cracked software. Victims who download installers advertised in the video descriptions may infect their systems with infostealers.

RedLine's execution process is straightforward. Once executed, the malware decodes XOR-encoded data such as the C2 server IP address and a unique ID. After the decoding process, RedLine requests configuration data from the C2 server, which instructs RedLine on what information to collect from the compromised system. Information related to the configuration data is then collected from the compromised system, converted into XML format, and transmitted to the C2 server via a Simple Object Access Protocol (SOAP) message.

## Raccoon

The original Raccoon Stealer emerged in 2019. It operated as a malware-as-a-service (MaaS) model and was advertised on underground forums. The cost was $75 USD per week or $200 per month. It did not include a distribution mechanism, so customers had to devise a method to install the infostealer on compromised systems. The Raccoon Stealer panel was hosted on a Tor site.

Following Russia's invasion of Ukraine in early 2022, the threat actors responsible for Raccoon Stealer announced that they were shutting down their operations, implying that a group member had died. However, the threat actors released a new version of the malware named RaccoonV2 in May 2022 (see Figure 5). While Raccoon Stealer and RaccoonV2 share similar functionality, CTU analysis confirms that RaccoonV2 represents a significant rewrite of the malware.


*Figure 5. Raccoon Stealer Telegram channel giving details of the new build. (Source: Secureworks)*

RaccoonV2 remains under active development as of this publication. The developers encoded more of the code strings in later versions and changed the encoding method, moving from Base64 to XOR. They continually alter elements of the malware to improve defense evasion, including changes to the User-Agents and mutexes, presumably to

circumvent indicator-based detections. To hinder static and dynamic analysis, updates included intermixing chunks of code with thousands of bytes of opcodes from superfluous Windows API function calls.

The RaccoonV2 infostealer obtains its configuration file from a hard-coded C2 server. This file specifies what data the malware should steal (e.g., password files, credit card information, web browser data, email messages, cryptocurrency wallets, browser cookies). This data is stored as individual files in the %APPDATA%\LocalLow directory before it is sent to the malware C2 server via an HTTP POST request.

RaccoonV2 has occasionally been deployed alongside other infostealers such as RedLine. It has been observed downloading and executing malware such as SmokeLoader, cryptocurrency wallet hijackers, Amadey, Remcos, AZORult, Allcome Clipper, SystemBC, and cryptocurrency miners.

## Vidar

Vidar primarily operates as an infostealer but has also been used to deploy ransomware. The malware was first observed in 2019 during a prolific malvertising campaign where threat actors used the Fallout exploit kit to distribute Vidar and GandCrab as secondary payloads. Vidar is sold on underground forums and Telegram channels (see Figure 6) as a standalone product, usually for between $130 USD per week to $750 for three months. Vidar provides an admin panel that lets customers configure the malware and monitor infections (see Figure 7).

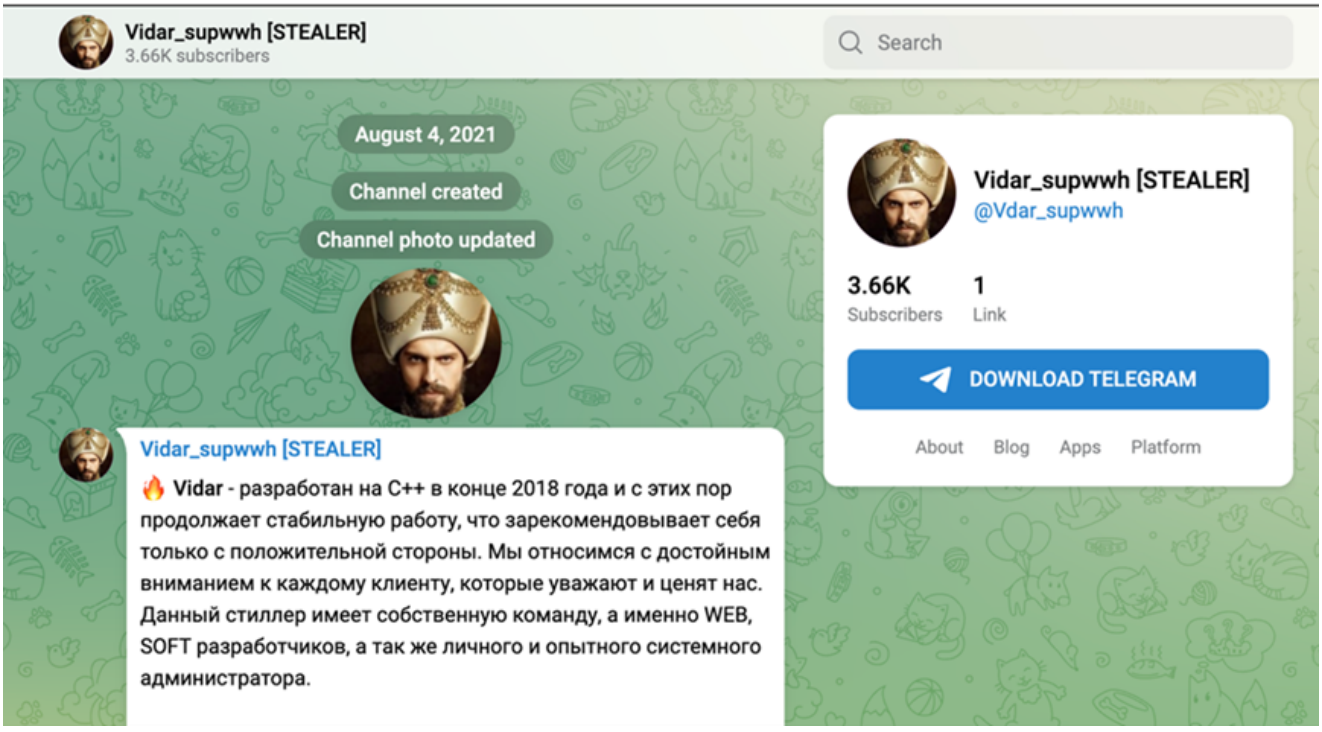

*Figure 6. Vidar Telegram channel. (Source: Secureworks)*

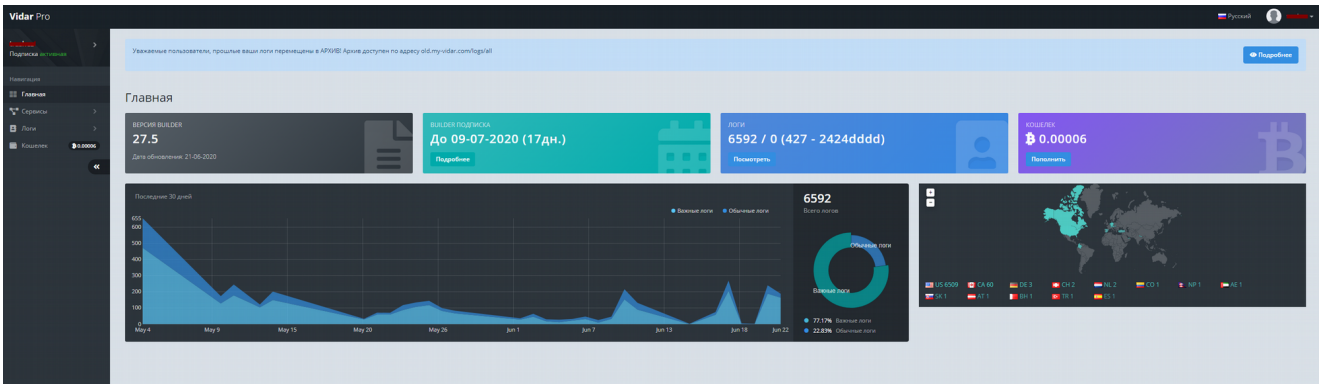

*Figure 7. Vidar infostealer admin panel. (Source: Secureworks)*

Vidar is a Windows-based stealer that is written in C++ and based on the Arkei stealer. It steals system data such as machine ID, operating system, computer name, display resolution, keyboard language, hardware information, network information, and a list of installed software. Vidar can extract browser artifacts, the contents of some cryptocurrency wallets, PayPal data, session data, and screenshots.

In addition to stealing sensitive data, Vidar can deliver secondary payloads such as the SystemBC proxy malware. Because Vidar is available to any paying threat actor, the delivery method varies and may include phishing emails or pirated software.

In early 2022, CTU researchers observed Vidar creating profiles on the Mastodon social networking platform to obtain and post C2 IP addresses. The Mastodon sites used by Vidar have thousands of members, and it is unlikely that the threat actors manage or control the infrastructure. Vidar verifies that the compromised system is not located in the Commonwealth of Independent States (CIS) by checking the computer language and keyboard settings. It then contacts the C2 server, which responds with the malware configuration. Vidar exfiltrates host and system information from infected devices and sends the data to the C2 server via HTTP form data POST requests.

## Taurus

The 'Taurus Project,' as the infostealer was named by its developers, was first observed in the second quarter of 2020. It is the fourth-most prolific stealer on Russian Market, even though it has been inactive since late 2021. Taurus was primarily advertised on Russian-language forums and will not execute within CIS countries. There are indications that the group responsible for this malware was also responsible for the 'Predator the Thief' infostealer, either directly or through the sale of the original software to a third party. Taurus can steal VPN credentials, social media details, cryptocurrency credentials; take screenshots of the victim's desktop; and exfiltrate the system's software installation and configuration information. This data can be used to further exploit the compromised system. Taurus includes a dashboard that lets threat actors monitor infections by geographic region and customize the malware configuration to specify targeted information.

Taurus was predominantly distributed via spam emails containing a malicious attachment. Opening the attached document prompts the victim to enable macros, which then executes a PowerShell script that initiates the download of additional payloads. Stolen data is exfiltrated as a ZIP file to a C2 server whose URL is built at runtime. Figure 8 shows the infection process.

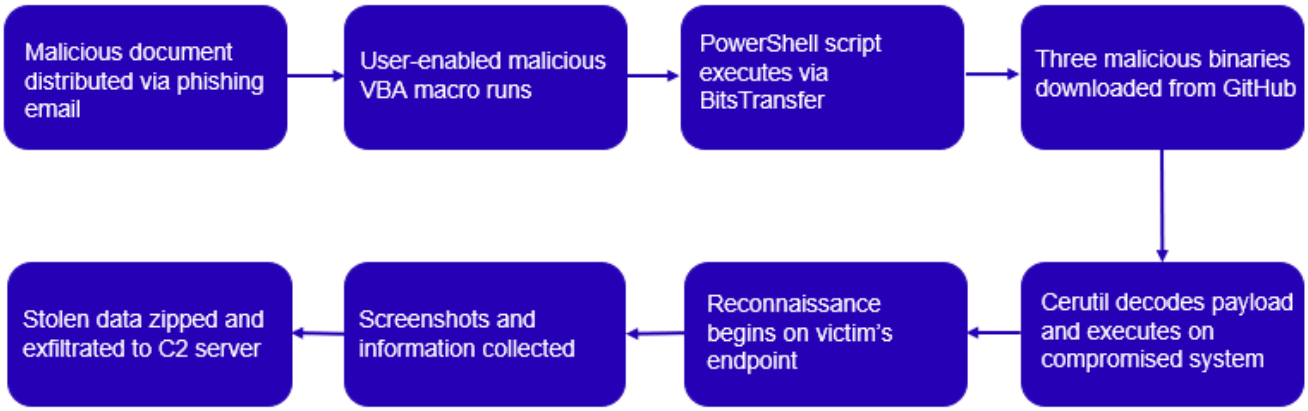

*Figure 8. Infection process for the Taurus infostealer. (Source: Secureworks)*

## Rhadamanthys

The Rhadamanthys infostealer was first observed in the third quarter of 2022. It quickly established its reputation on underground forums due to the active development and deployment of user-friendly features that align with market demands. Rhadamanthys targets a wide range of applications, wallets, and user data on an infected device. The developers appear receptive to suggestions for regular updates and enhancements (see Figure 9). Rhadamanthys operates using a MaaS model and has been observed using phishing emails and Google Ads as the initial infection vector.

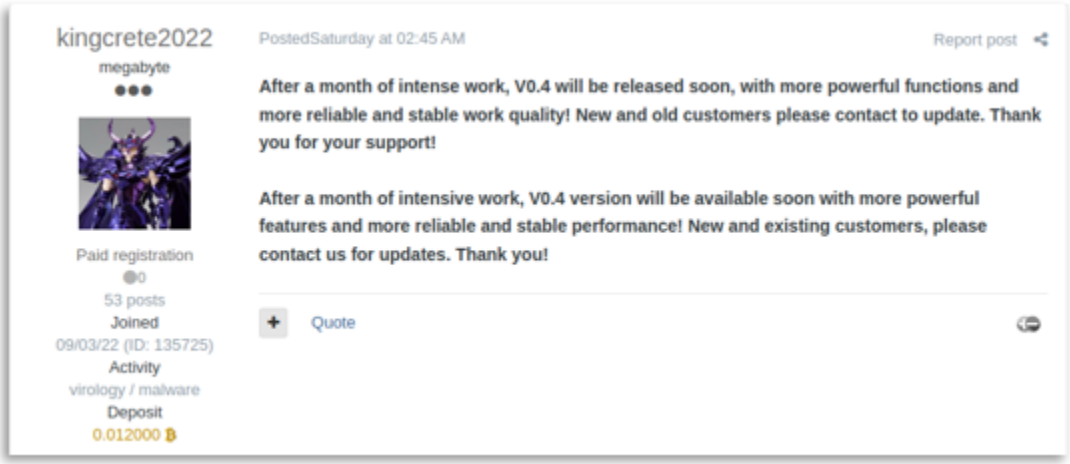

*Figure 9. Forum post announcing Rhadamanthys updates. (Source: Secureworks)*

CTU researchers observed a threat actor named "kingcrete2022" advertising Rhadamanthys in September 2022 for $250 USD for 30 days or $550 for 90 days, payable in Monero or Bitcoin. In November 2022, a threat actor named 'Kingcrete' uploaded two videos to Vimeo.

One video was an overview of the 'v0.3.2 updates.' The second video was named 'Wallter Crack and Customized Dictionaries' and showed how the infostealer targets cryptocurrency wallets. Both videos show details of the Rhadamanthys admin panel and a walkthrough of how it is used.

Rhadamanthys is written in C++. It evades detection by operating in system memory and by creating a mutex to ensure that only one instance is running. It uses the Al-Khaser anti-analysis tool to detect and avoid running in researcher sandboxes and virtual machines (VMs). Rhadamanthys is custom-packed with several stages that include dropping a custom loader DLL that decodes and executes an encoded payload via a command-line argument. The custom loader executes shellcode in a novel way by abusing the callback mechanism of the Windows CryptEnumOIDInfo() function and masquerades as a Nullsoft Scriptable Install System (NSIS) installer running the PrintUIEntry export (see Figure 10).

```
C:\Users\\AppData\Roaming\nsis_uns42f98.dll,PrintUIEntry |5CQkOhiAAAA|1TKr5GsMwYD|67sD
```

*Figure 10. Example of Rhadamanthys masquerading as an NSIS installer. (Source: Secureworks)*

Rhadamanthys decodes the C2 URL used for initial communication using a generated 128-byte XOR key. The configuration file it receives from the C2 server is disguised as a JFIF image via steganography. The infostealer uses the WebSocket protocol to encrypt post-infection traffic, which includes stolen and exfiltrated data. Rhadamanthys can also be configured to run arbitrary executables.

## State-sponsored stealers

Infostealers are not exclusively used by cybercriminals. Because infostealers can discreetly and efficiently exfiltrate sensitive data from targeted systems, they are commonly and effectively used by state-sponsored threat groups that focus on cyberespionage operations. During the conflict in Ukraine, Russian threat actors deployed the Graphiron infostealer to target Ukrainian organizations. This infostealer is similar to the GraphSteel malware previously used against Ukraine but includes enhanced capabilities. Graphiron is Go-based malware that can steal system and application data, screenshots, account credentials, and private keys. It consists of a downloader and a secondary information-stealing payload. The downloader checks for various security software and malware analysis tools before downloading the payload. Graphiron uses AES encryption with hard-coded keys to communicate with the C2 server through port 443.

Chinese state-sponsored threat groups have also been observed using infostealers in pursuit of their objectives. Reports of a 2022 espionage campaign targeting various government and public entities in Asia identified a custom Infostealer.Logdatter infostealer that logged

keystrokes, captured screenshots, stole clipboard data, downloaded files, injected code, and both connected to and queried SQL databases. This campaign has been attributed to the BRONZE ATLAS threat group.

## The infostealer ecosystem

Much like the general cybercriminal ecosystem, the successful development and deployment of infostealers relies on individuals with a broad range of skills, roles, and responsibilities. These individuals include developers, initial access brokers (IABs), and customers (see Figure 11). The rise of MaaS operations has lowered the technical barrier to entry into cybercrime. It has also fostered innovation among developers as they improve their products and appeal to a broad audience of potential customers on underground forums and marketplaces.

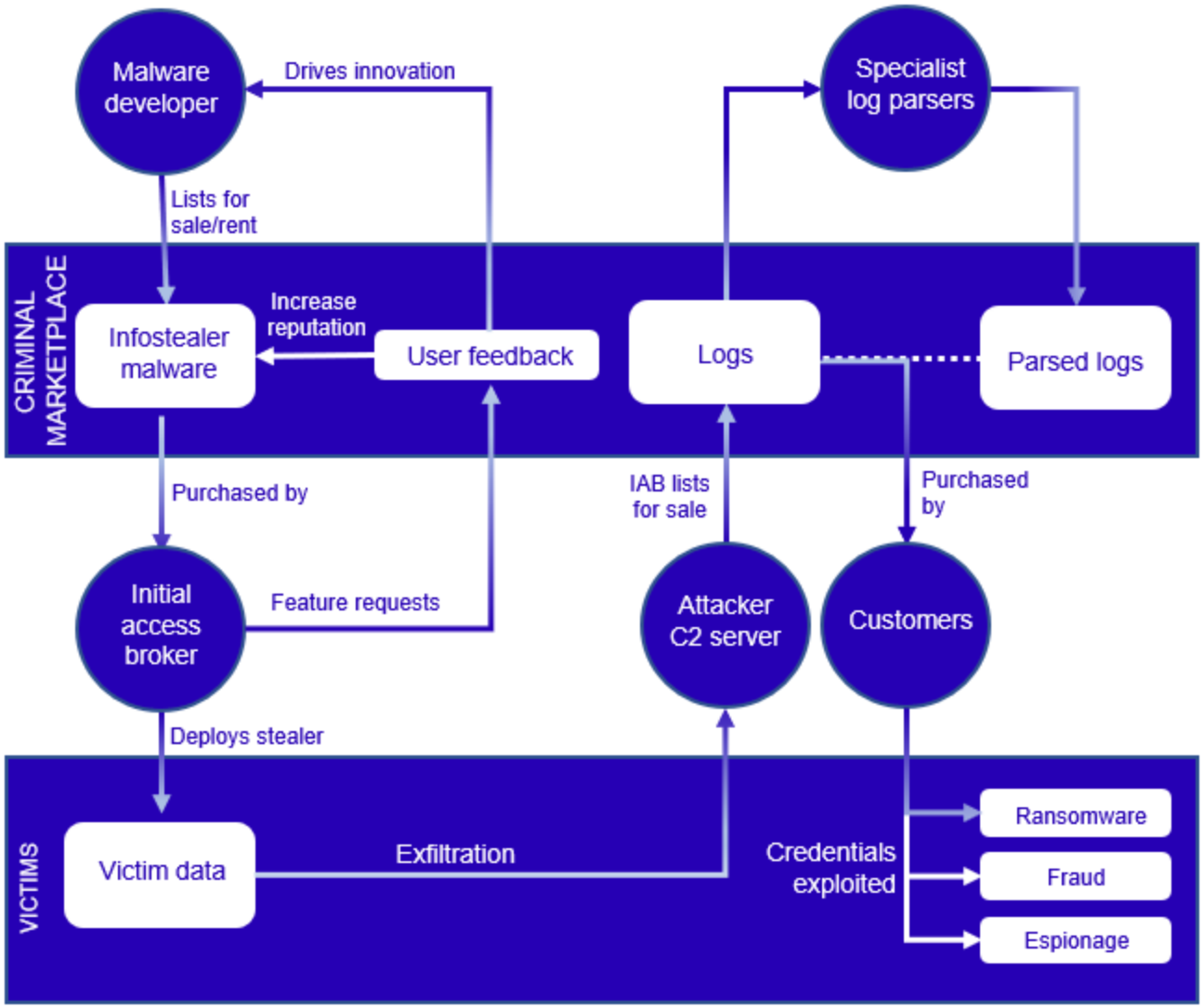


*Figure 11. An overview of roles and relationships in the infostealer ecosystem. (Source: Secureworks)*

### Developers

Malware developers are responsible for writing and maintaining the code that will be packaged and sold on underground forums, typically to IABs. With MaaS being the most common business model in the infostealer marketplace, developers can dedicate more time and effort to ensuring their malware contains a range of features, taking feedback from users, and iterating the malware to constantly evolve and improve. Forums allow customers to leave feedback, enhancing the seller's reputation and potentially increasing the popularity of the malware.

## Initial access brokers

IABs are individuals or groups that rent access to tools from MaaS operators on underground forums and marketplaces. They then deploy these infostealers via phishing or malicious ad campaigns to infect systems. These infostealers steal data from the compromised system and exfiltrate it to a C2 server. This stolen data, typically including credentials for services such as Remote Desktop Protocol (RDP), VPNs, email accounts, and cryptocurrency wallets, is then sold to threat actors who use it for malicious purposes.

## Customers

Due to diverse types of data that infostealers can obtain from a compromised system, threat actors often purchase the data for a wide range of purposes. Financially motivated cybercriminals may purchase credentials for cryptocurrency wallets, online banking, or other financial services and abuse them to make fraudulent withdrawals or transactions. Ransomware groups commonly seek infostealer logs, as credentials for RDP, VPNs, and corporate accounts can provide initial access into enterprises prior to data exfiltration and encryption. The value of infostealers to ransomware groups has increased with the success of the ransomware-as-a-service (RaaS) model and the growth of 'hack-and-leak' sites. For example, the LockBit ransomware operators reportedly offered to purchase the Raccoon Stealer source code.

## Specialist log parsers

Log marketplaces such as Genesis Market have built-in parsing as a browser extension, which allows customers to seamlessly access device fingerprints and victim data. Other marketplaces like Russian Market and 2easy sell raw logs that require parsing to interpret and use the content. Parsing infostealer logs purchased from a underground marketplace can be a complex task, as the logs are often in various formats and contain a large amount of data. This challenge has created a secondary market for individuals selling parser tools to customers who have either deployed the infostealers and want to sell structured data or to buyers in possession of bulk raw logs (see Figures 12 and 13).

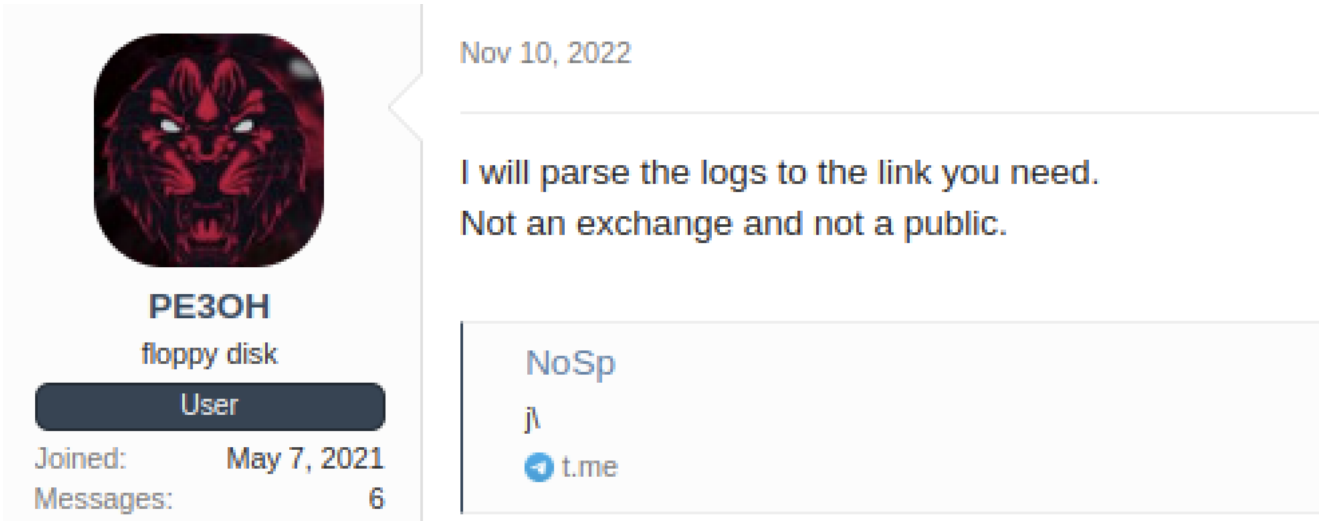


*Figure 12. Threat actor offering to parse stealer logs to find specific links. (Source: Secureworks)*

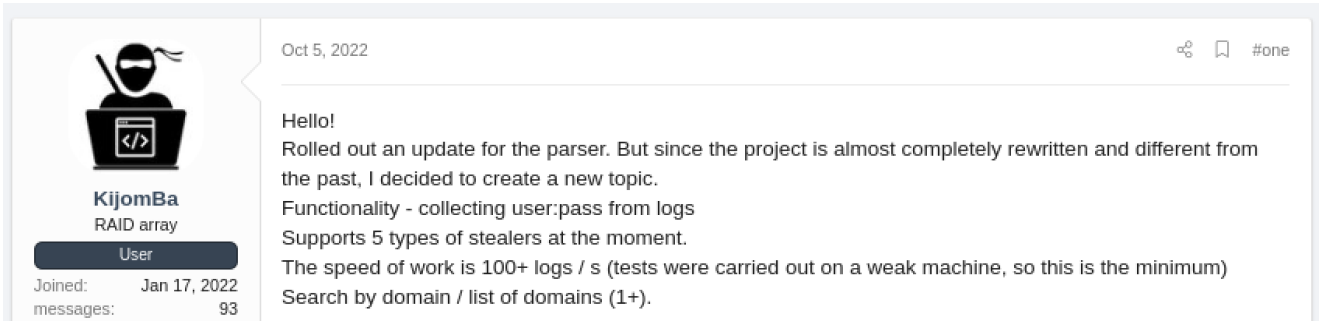


*Figure 13. Threat actor selling a parser for large batches of stealer logs. (Source: Secureworks)*

## Conclusion

In 2022, stolen credentials featured heavily in Secureworks incident response engagements. Infostealer malware poses a significant threat to individuals and organizations. Its ability to steal sensitive information such as passwords and financial information has far-reaching consequences for victims. This type of malware is becoming increasingly sophisticated, making it more difficult for victims to detect and remove. Additionally, the evolution of criminal marketplaces allows relatively low-skilled threat actors to access tools with advanced capabilities to attack many victims.

The migration to remote work driven by the COVID-19 pandemic and sustained post-pandemic exposes users and organizations to even greater risk from infostealers. Bring your own device (BYOD) policies that let users access corporate assets from infected personal devices can lead to compromises of corporate systems.

To mitigate this threat, individuals and organizations must take proactive steps to secure their systems. These steps include keeping software up to date, using strong and unique passwords that must not be stored in web browsers, and being wary of suspicious emails or

downloads. It is also crucial to invest in security solutions that can detect and block infostealer malware. By taking these actions, individuals and organizations can reduce their risk of compromise.

## References


Abrams, Lawrence. “Raccoon Stealer malware suspends operations due to war in Ukraine.” Bleeping Computer. March 25, 2022. https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/

Arghire, Ionut. “Someone Is Hacking Cybercrime Forums and Leaking User Data.” SecurityWeek. March 5, 2021. https://www.securityweek.com/someone-hacking-cybercrime-forums-and-leaking-user-data/

Armer, Jon, et al. “New Malware Variant: Project Taurus Infostealer Follows in Predator the Thief's Footprints.” Infoblox. 2019. https://www.infoblox.com/wp-content/uploads/threat-intelligence-report-project-taurus-infostealer-follows-in-predator-the-thiefs-footprints.pdf

Ceci, L. “Telegram messenger global MAU 2014-2022.” Statista. November 7, 2022. https://www.statista.com/statistics/234038/telegram-messenger-mau-users/

Cyble Research & Intelligence Labs. “Rhadamanthys: New Stealer Spreading Through Google Ads.” January 12, 2023. https://blog.cyble.com/2023/01/12/rhadamanthys-new-stealer-spreading-through-google-ads/

Dewan, Tarun and Chaturvedi, Stuti. “New PHP Variant of Ducktail Infostealer Targeting Facebook Business Accounts.” Zscaler. October 13, 2022. https://www.zscaler.com/blogs/security-research/new-php-variant-ducktail-infostealer-targeting-facebook-business-accounts

eSentire. “eSentire Threat Intelligence Malware Analysis: Raccoon Stealer v2.0.” August 31, 2022. https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-raccoon-stealer-v2-0

Europol. “One of the world's biggest hacker forums taken down.” April 12, 2022. https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

Flashpoint. “RisePro” Stealer and Pay-Per-Install Malware “PrivateLoader.” December 19, 2022. https://flashpoint.io/blog/risepro-stealer-and-pay-per-install-malware-privateloader/

Joe Sandbox Cloud. “Windows Analysis Report IuXJUPoEo6.exe.” Accessed March 30, 2022. https://www.joesandbox.com/analysis/464621/0/html

Kathiresan, Karthikkumar. “The Titan Stealer: Notorious Telegram Malware Campaign - Uptycs.” Uptycs. January 23, 2023. https://www.uptycs.com/blog/titan-stealer-telegram-malware-campaign

Kingcrete. Rhadamanthys walkthrough videos. Vimeo. Accessed March 30, 2023. https://vimeo.com/user185512701

Kupreev, Oleg. “Self-spreading stealer attacks gamers via YouTube.” Kaspersky. September 15, 2022. https://securelist.com/self-spreading-stealer-attacks-gamers-via-youtube/107407/

Leyden, John. “ZeuS cybercrime cookbook on sale in underground forums.” The Register. March 23, 2011. https://www.theregister.com/2011/03/23/zeus_source_code_sale/

Malware-Traffic-Analysis.net. “RHADAMANTHYS STEALER.” January 3, 2023. https://www.malware-traffic-analysis.net/2023/01/03/index.html

Mandiant Threat Intelligence. “Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities.” November 25, 2022. https://www.mandiant.com/resources/blog/spear-phish-ukrainian-entities

Muncaster, Phil. “New Info-Stealer Discovered as Russia Prepares Fresh Offensive.” Infosecurity Magazine. February 9, 2023. https://www.infosecurity-magazine.com/news/new-infostealer-discovered-russia/

Positive Technologies. “Positive Technologies: cybercrime market in Telegram is growing.” November 18, 2022. https://www.ptsecurity.com/ww-en/about/news/positive-technologies-cybercrime-market-in-telegram-is-growing/

Secureworks. “BRONZE ATLAS.” Accessed March 30, 2023. https://www.secureworks.com/research/threat-profiles/bronze-atlas

Secureworks. “IRON TILDEN.” Accessed March 30, 2023. https://www.secureworks.com/research/threat-profiles/iron-tilden

Secureworks. “Learning from Incident Response: 2022 Year in Review.” March 16, 2023. https://www.secureworks.com/resources/rp-irs-learning-from-incident-response-team-2022-year-in-review

Secureworks. “ZeuS Banking Trojan Report.” March 10, 2010. https://www.secureworks.com/research/zeus

Segura, Jerome. “Vidar and GandCrab: stealer and ransomware combo observed in the wild.” Malwarebtes. January 4, 2019. https://www.malwarebytes.com/blog/news/2019/01/vidar-gandcrab-stealer-and-ransomware-combo-observed-in-the-wild

Threat Hunter Team. “New Wave of Espionage Activity Targets Asian Governments.” Symantec. September 13, 2022. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments

Toulas, Bill. “2easy now a significant dark web marketplace for stolen data.” Bleeping Computer. December 21, 2021. https://www.bleepingcomputer.com/news/security/2easy-now-a-significant-dark-web-marketplace-for-stolen-data/

Toulas, Bill. “New BHUNT malware targets your crypto wallets and passwords.” Bleeping Computer. January 19, 2022. https://www.bleepingcomputer.com/news/security/new-bhunt-malware-targets-your-crypto-wallets-and-passwords/

U.S. Cybersecurity & Infrastructure Security Agency. “LokiBot Malware.” October 24, 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-266a

U.S. Department of Justice. “Criminal Marketplace Disrupted in International Cyber Operation.” April 5, 2023. https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation

## Appendix — Infostealer comparison

The following chart compares five of the most common infostealers in 2022.

| **Infostealer** | **RedLine** | **RaccoonV2** | **Vidar** | **Taurus** | **Rhadamanthys** |
|---|---|---|---|---|---|
| Status | Active | Active | Active | Not active | Active |
| Pricing | $150 per month, $800 for lifetime | $75 per week, $200 per month + $50 per build with clipper | $130 per week, $300 per month, $750 per 3 months | $150 for lifetime, $50 per update or rebuild, $10 per prefix change | $250 for 30 days, $550 for 90 days VIP: $300 for 30 days, $750 for 90 days |
| Cracked versions | Widely available | Limited availability | Widely available | Unknown | Unknown |
| Language | .NET | C/C++ | C++ | C++ | C++ |
| SaaS or self-hosted | Self-hosted | SaaS | SaaS | Self-hosted | SaaS |

| Infostealer | RedLine | RaccoonV2 | Vidar | Taurus | Rhadamanthys |
|---|---|---|---|---|---|
| Reserved C2 domains | Some | Infinite | Infinite | 1 per build | 5 per build, proxies owned by the distributor and pointing to the RaccoonV2 server |
| Multi-browser support? | Yes | Yes | Yes | Yes | Yes |
| Supported applications | WinSCP, WinFTP Pro, FileZilla | Gecko-based applications, Google Authenticator browser extension, KeePassXC-Browser extension, KeePass Tusk browser extension, BitWarden browser extension, Microsoft Autofill browser extension | WinSCP, WinFTP Pro, FileZilla | WinSCP, WinFTP Pro, FileZilla | Cyberduck, FTP Navigator, FTPRush, FlashFXP, SmartFTP, Total Commander, WinSCP, WS_FTP, Core FTP |
| Supported wallets | Atomic Wallet, Armory, Authenticator, Binance Wallet, BitApp Wallet, BoltX, Brave Wallet, Coin98 Wallet, Coinbase, Coinomi, Electrum, Equal, Exodus, Guarda, GuildWallet, Harmony, | Atomic Wallet, Auro Wallet, Binance Wallet, BitKeep, Braavos, Blockstream Green, Brave Wallet, Coin98, Coinbase, Coinomi, Cosmostation, Cyano Wallet, Daedalus, Electron Cash, Electrum, Electrum-LTC, Enkrypt, Eternl, EVER Wallet, | Binance Wallet, Guarda, Jaxx Liberty, MetaMask, Ronin, TronLink | Not Applicable | Armory, Atomic Wallet, AtomicDEX, Binance Wallet, Bisq, Bitcoin Core, Bitcoin Gold, Bytecoin Wallet, Coinomi, Dash Core, DeFi Wallet, DeFiChain Electrum, Dogecoin, Electron Cash, Electrum, Electrum-LTC, Exodus, Frame, Guarda, Jaxx |

| | | | | | |
|---|---|---|---|---|---|
| **Infostealer** | **RedLine** | **RaccoonV2** | **Vidar** | **Taurus** | **Rhadamanthys** |
| | iWallet, Jaxx Liberty, KardiaChain. Liquality, Maiar DeFi Wallet, MathWallet, MetaMask, Nami, Oxygen, Pali Wallet, Phantom, Ronin Wallet, Saturn Wallet, Temple Wallet, Terra Station, TON Crystal, TronLink, Waves, Wombat, XDEFI, Yoroi | Exodus, Finnie, GameStop Wallet, GeroWallet, Goby, Guarda, GuildWallet, HashPack, ICONex, Jaxx Liberty, Keplr, KHC, Leap, Ledger Live, Liquality, Martian, MetaMask, MetaX, Nami, NeoLine, OKX, Petra, Phantom, Polymesh Wallet, Pontem, Rabby, Ronin Wallet, Saturn Wallet, Sender Wallet, Slope Wallet, Solflare, Stargazer, Temple, Terra Station, TezBox, TON Crystal, TronLink, Trust Wallet, Wasabi, Keeper Wallet, XDEFI | | | Liberty, Litecoin Core, MyCrypto, MyMonero, SafePay Solar, TokenPocket, Wasabi, Zap, Zecwallet Lite |

| Infostealer | RedLine | RaccoonV2 | Vidar | Taurus | Rhadamanthys |
|---|---|---|---|---|---|
| Other targeted applications | Battle.net, BlackHawk Web Browser, Discord, Foxmail, Thunderbird, NordVPN, NVIDIA GeForce Experience, OpenVPN, Outlook, Pidgin, ProtonVPN, Steam, Telegram | Discord, Signal, Telegram | GAuth, Telegram | Authy, Discord, Foxmail, Outlook, Pidgin, Steam | Authy, AzireVPN, CheckMail, Claws Mail, eM Client, Foxmail, Global AB, Gmail Notifier Pro, KeePass, Mailbird, NordVPN, NoteFly, Notezilla, OpenVPN, Outlook, Pidgin, Postbox, PrivateVPN ProtonVPN, Psi, RoboForm, SecureCRT, Simple Sticky Notes, TeamViewer, Thunderbird, Tox, TrulyMail, WinAuth, Windscribe |

Back to more Threat Analyses and Advisories