Infostealer Malware on the Dark Web

accenture.com/us-en/blogs/security/information-stealer-malware-on-dark-web

Share

Information stealer (infostealer) malware—malicious software designed to steal victim information, including passwords—has become one of the most discussed malware types on the cybercriminal underground in 2022 according to Accenture's Cyber Threat Intelligence team (ACTI). This is due to infostealers' ability to harvest cookie data, usernames, and passwords, their cheap cost, and their availability as a malware-as-a-service offering, which allows actors with few resources or little technical knowledge to deploy the malware and access others' networks.

While more organizations worldwide are implementing multi-factor authentication (MFA) at an increasing rate to protect against the theft of user credentials, this protection is proving insufficient. In 2022, ACTI saw cyber threat actors successfully combine stolen credentials and social engineering to carry out high-profile breaches; the success of those breaches only further increased the demand for infostealers on the dark web. In addition, the volume of victim data included in logs for sale on underground marketplaces rose between June and October of 2022. The popularity spike in infostealers also drove underground actors to advertise on the dark web a variety of new infostealer malware variants.

MFA fatigue attacks

In 2022, the high-profile breaches of several large organizations illustrated the ease at which threat actors can breach network defenses using stolen employee credentials and leveraging MFA fatigue attacks. MFA fatigue attacks involve repeated attempts to log on to an MFA-enabled account using stolen credentials, thereby bombarding a potential victim with MFA push requests. In such scenarios, some MFA request recipients accept MFA requests to stop the requests from appearing on connected devices, unknowingly granting criminal access to the now-victims' systems. In one such attack, threat actors also used a popular messaging app to contact victims, purporting to be the victim organization's IT department and social engineering the victim into accepting MFA requests.

The notorious LAPSUS$ group relied on MFA fatigue attacks for several of its operations in 2022. Microsoft investigated LAPSUS$ and concluded the group had obtained credentials by:

- Deploying the malicious RedLine infostealer to obtain passwords and session tokens.

- Purchasing credentials and session tokens on criminal underground forums.
- Paying employees at targeted organizations or their suppliers and business partners for access to credentials and MFA approvals.
- Searching public code repositories for exposed credentials.

This group serves as just one example of real-world criminal use of infostealers in combination with MFA fatigue attacks that have contributed to the surge in popularity for infostealers and the growth of compromised credential marketplaces.

The rise of compromised credential marketplaces

ACTI monitors several of the most prominent compromised credential marketplaces and found a marked increase in the number of logs for sale from July to October 2022.

Russian Market

Access to the Russian Market site allows visitors to search for inventory by malware used, victim operating system, and victim location. This site was among the most popular markets in 2022 based on volume of logs available for sale, with victim data sold for an average price of $10 per log. The total number of logs for sale in this market rose by nearly 40% from approximately 3.3 million to 4.5 million between July and October 2022.

Malware

In log advertisements, Russian Market vendors include the malware they used to obtain credentials for sale. So far in 2022, RedLine, Raccoon Stealer, Vidar, Taurus, and AZORult are the five infostealers actors have used to obtain the logs on Russian Market (see Figure 1). Between July and October 2022, RedLine remained the dominant infostealer; however, its use decreased from 56% of the total market to 48% in October 2022. Use of the popular Raccoon Stealer, on the other hand, increased from 11% to 22% between July and October 2022, coinciding with the release of Raccoon Stealer v2 on June 30, 2022.

<<< Start >>>

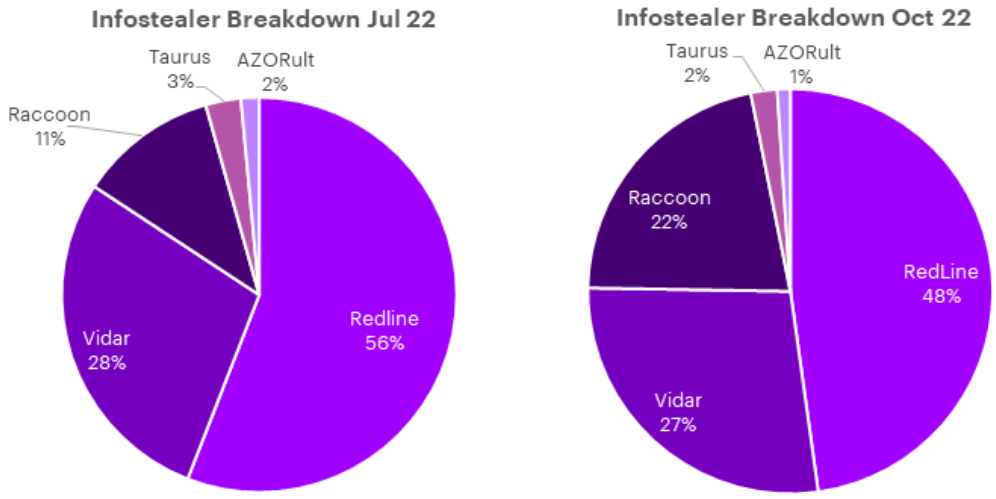

Figure 1: Infostealers cybercriminals used most to obtain the credentials for sale on Russian Market in July and October 2022

<<< End >>>

Victimology

From July to October 2022, the top three countries with the highest number of infostealer victims on Russian Market were India, Indonesia, and Brazil. These countries making up the highest number of infostealer victims is likely due to the vast population of each country combined with a relative low level of cybersecurity awareness in each nation. Between July and October 2022, the number of infostealer victims in these counties increased by 33% in India, 30% in Indonesia, and 40% in Brazil. The remaining seven of the top 10 countries were Pakistan, Vietnam, Egypt, Thailand, Philippines, Turkey, and the U.S.

What's next?

Shift toward private sales for quality logs

Private log sales, which are common on dark web forums, usually involve sellers fostering relationships with trusted buyers who are willing to pay a little more than buyers on open marketplaces. Often, sellers offer the best logs to trusted buyers first and sell the remaining logs on marketplace's general pages. While ACTI expects marketplaces selling infostealer-obtained logs to continue to thrive, the ever-increasing volume of stolen data available on these forums will lead to the highest-quality logs inevitably becoming harder to find as trusted buyers begin to obtain high-value logs through private sales.

To cater to buyers wanting high-quality logs, the operators of Russian Market added a pre-order option on the forum's Stealer Logs section in October 2022. Users with a balance of US$1,000 in their general accounts on the site can provide a list of domains they wish to

target and will receive notifications of the availability of logs affecting those domains before those logs become available to the rest of the market.

Cybercriminals advertise wave of new infostealer-related products on the dark web
With the success of infostealers in 2022, there have been a wave of advertisements for new variants of stealers, enhanced infostealers, and infostealer source code available on the cybercriminal underground. The following is a table of notable related advertisements on dark web forums from July to October 2022:

Date	Forum	Malware Name	Price in US Currency
Jul-19-22	Breached	Whisper	$100
Jul-20-22	Sinisterly	Gomorrah v5	$150
Jul-29-22	LolzGuru	Erbium	$1,000
Jul-31-22	XSS	BlackIce	$120
Aug-15-22	XSS	LummaC	$1,000
Aug-29-22	Exploit	Rhadamanthys	$999
Aug-30-22	Opencard	GRIM_NOID	$300
Sep-02-22	XSS	BLUEFOX v2	$350
Sep-18-22	Exploit	Psigo	$321
Oct-01-22	Exploit	AcridRain	$400
Oct-08-22	XSS	Unnamed	$90

Figure 2: Table of Infostealers Malware Advertisements and Pricing from July to October 2022

The sale of these new strains, combined with the availability of enhanced infostealers and infostealer source code will lead to increased dark web log sale activity both on marketplaces' "public" spaces and through private sales.

New kids on the block

Meta Stealer
While Raccoon, Redline, and Vidar continue to account for the majority of dark web marketplace stock, one new infostealer has forced its way in: Meta Stealer. Underground users first advertised this infostealer on cybercrime forums in March 2022, with advertisements stating that developers heavily based its code on that of Redline but that

Meta Stealer had additional features and was less detectible by anti-virus and endpoint detection software. As of November 2022, Meta Stealer costs US$150 per month or US$1,000 for a lifetime license.

Since May 2022, Meta Stealer logs have been appearing on 2easy Market, which has added approximately 13,000 logs as of November 4, 2022. ACTI expects Meta Stealer to see increased popularity as those behind more-established strains lose interest, lose control, or find it too tough to continue to bypass anti-virus and endpoint protection software.

Rhadamanthys

As Figure 2 references, the Rhadamanthys infostealer appeared on the Exploit forum on August 29, 2022. The following factors indicate Rhadamanthys is a genuine, powerful infostealer and ads for it are not scams or for sales of a revamped version of previously leaked malware code:

- Very positive feedback (commenters on the forum thread have praised the quality of the build and its low anti-virus software detection rate)
- The level of detail on the infostealer the actors operating the forum thread provided
- The use of a guarantor
- The samples of the malware the sellers shared with forum members
- The support of the actors behind the Rhadamanthys forum accounts

ACTI assesses Rhadamanthys is a powerful tool for those looking to gain access to corporate networks. The malware can obtain credentials and information from a host of platforms including major browsers, email clients, messaging platforms, and crypto apps and wallets. In addition, it targets logs from MFA apps, including Authenticator, Authy, EOS Authenticator, and GAuth Authenticator, as well as Outlook and Slack, and harvests cookies. This infostealer can also use a control panel to export cookies (Figure 3) and plug them into a bespoke browser, which helps bypass the need for passwords to access targeted domains. The bespoke browser is Genesium—the browser the operators of the underground marketplace Genesis Market created and have used.

<<< Start >>>

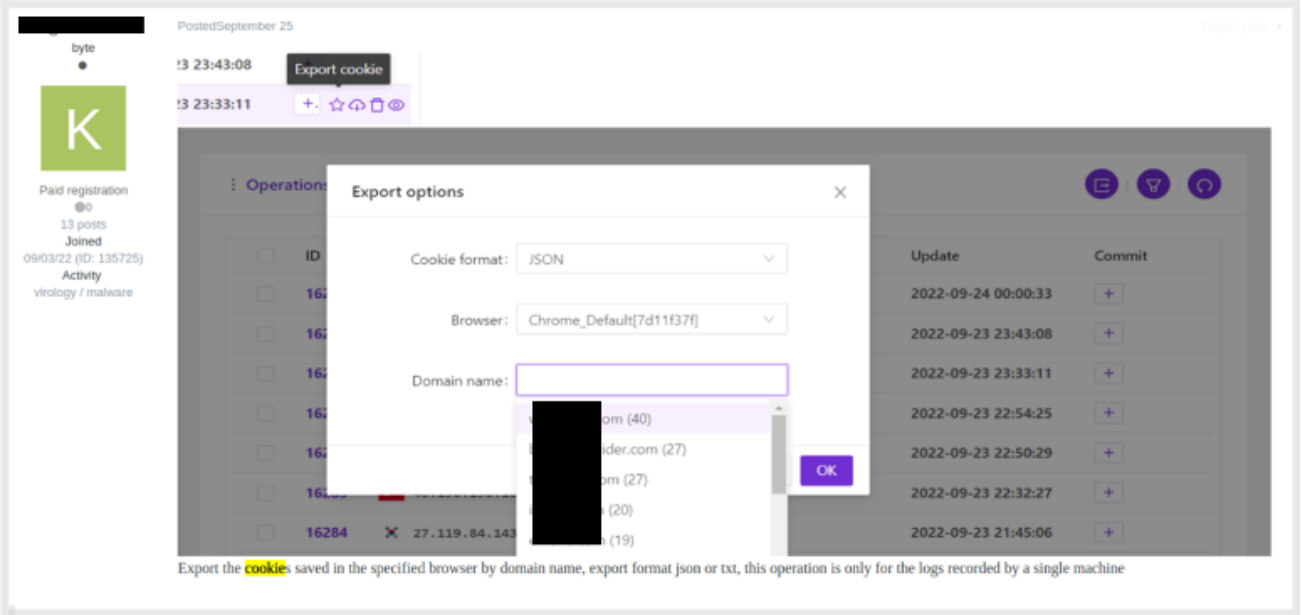

Figure 3: Export Cookie Functionality of Rhadamanthys Stealer

<<< End >>>

ACTI expects to see Rhadamanthys grow in popularity and become a market leader, and for other dark web infostealer vendors to look to emulate this level of success.

Law enforcement action unlikely to stem the tide

On October 26, 2022, the U.S. Department of Justice announced the arrest of a major player behind the Raccoon Stealer operation and the FBI stated it had dismantled Raccoon Stealer infrastructure. However, on October 30, 2022, the operators of the "raccoonstealer" account on the Exploit forum stated the project is still running and servers remain safe, as Figure 4 illustrates.

<<< Start >>>

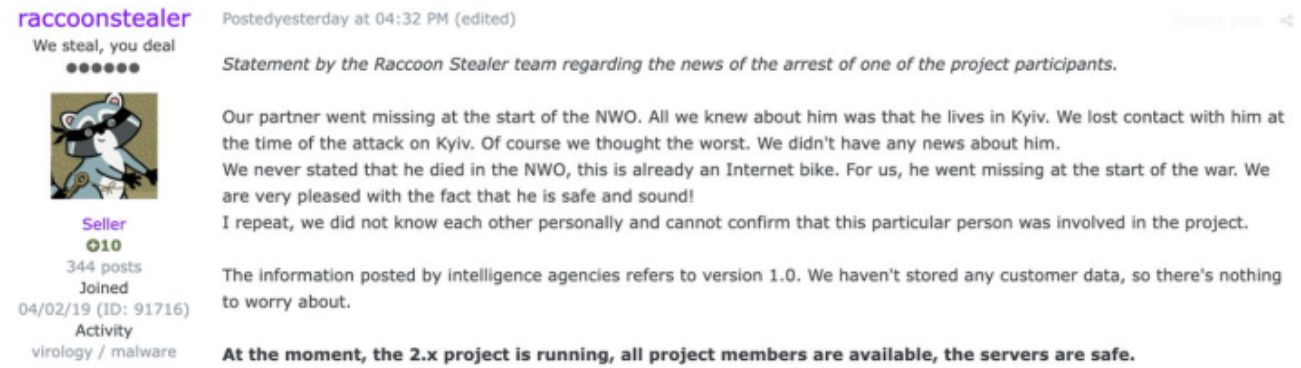

Figure 4: Update From raccoonstealer Account on Exploit Forum on October 30, 2022

<<< End >>>

Regardless of whether the arrest ultimately affects Raccoon Stealer operations, it might motivate other actors to try to fill the space Raccoon Stealer could leave behind.

Conclusion and mitigation

ACTI expects the infostealer landscape to continue to evolve and pose a significant risk to organizations in 2023. Organizations should examine how they authenticate user access to their systems and consider moving away from MFA push notifications and toward number-matching MFA systems and the use of biometrics to dull the effects of infostealers. Organizations should also fully train staff on the dangers of MFA fatigue attacks, social engineering attempts, and how to secure online accounts. Monitoring of dark web sources to obtain threat intelligence on the latest tactics, techniques, and procedures relating to infostealer malware should also help get ahead of the latest threats in this sphere.

The Accenture Cyber Threat Intelligence (ACTI) team provides actionable intelligence and relevant decision support to help organizations detect, analyze and mitigate threats.

***Accenture Security** is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.*

Paul Mansfield

Cyber Threat Intelligence Analyst

Paul is a lead analyst on Accenture's iDefense Reconnaissance Team, producing actionable intelligence and tracking threat actors.

Follow me:

Thomas "Mannie" Willkan

Cyber Threat Intelligence Consultant

Thomas 'Mannie' Willkan is a Senior Threat Intelligence professional specialising in emerging technologies and the Dark Web criminal underground.

Follow me:

Howard Marshall

Managing Director – Accenture Security, Global Cyber Threat Intelligence Lead

As the global lead for the Cyber Threat Intelligence (CTI) program, Howard directs a team of highly skilled cybersecurity specialists.

Follow me:

Subscription Center

Subscribe to Security Blog Subscribe to Security Blog

Subscribe