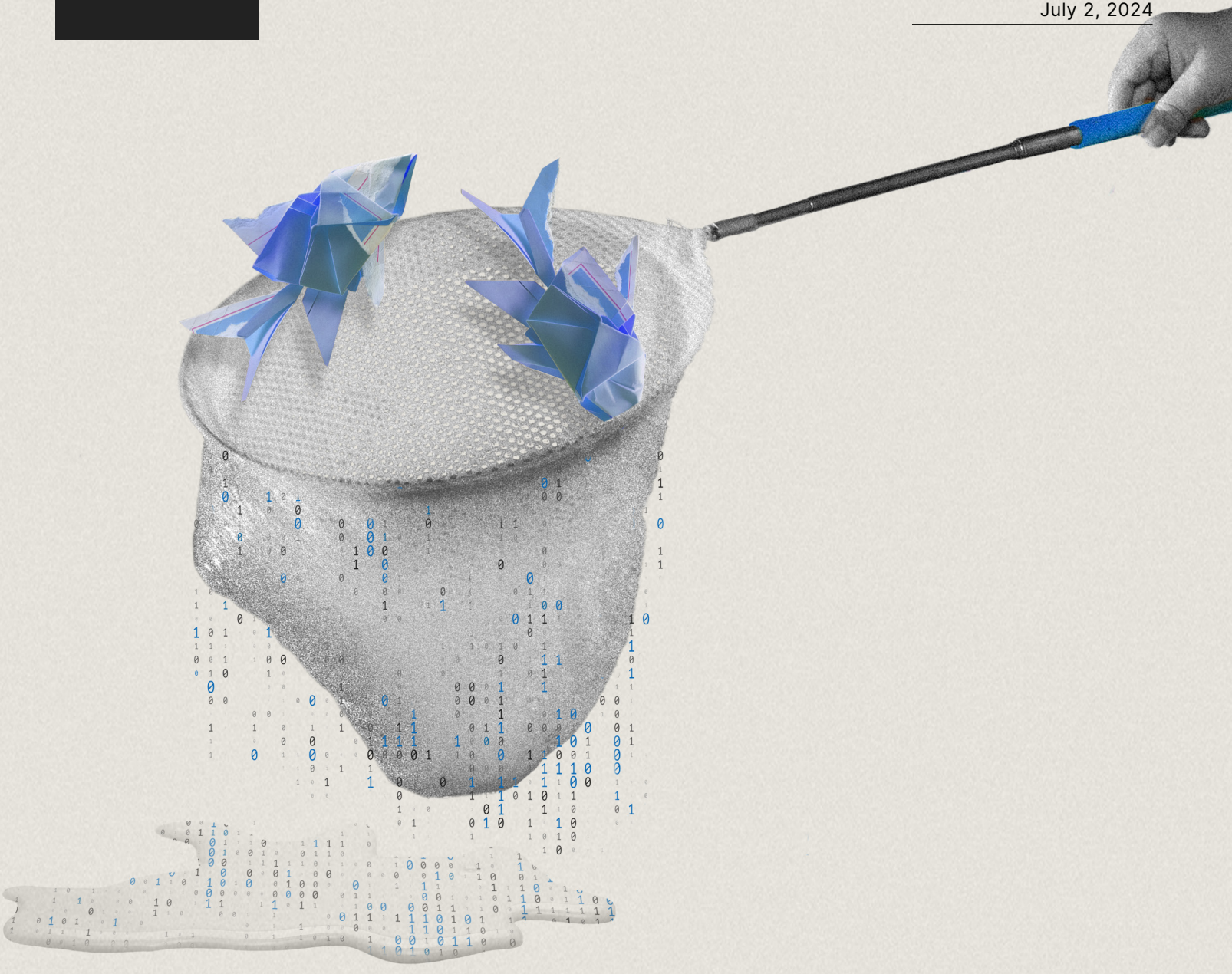
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

July 2, 2024



Caught in the Net: Using Infostealer Logs to Unmask CSAM Consumers

Using the infostealer malware data in Recorded Future's Identity Intelligence, we identified 3,300 unique consumers of child sexual abuse material, tracked new sources, and arrived at geographic and behavioral trends.

In three case studies, Insikt Group identified two individuals and surfaced digital artifacts, including cryptocurrency addresses, from a third individual using infostealer data and open-source intelligence.

As demand for infostealer logs grows, the Identity Intelligence Module's data set is expected to provide evolving insights for investigators tracking CSAM consumers.

Executive Summary

In this proof-of-concept (PoC) report, we used Recorded Future Identity Intelligence's vast trove of information stealer ("infostealer") malware data to identify consumers of child sexual abuse material (CSAM), surface additional sources, and arrive at geographic and behavioral trends for the most popular sources. We have high confidence in these assessments due to the nature of the infostealer log data source and follow-up research performed. We also conducted sample user investigations for three individuals who had accounts on multiple CSAM sources, which we believe can be replicated for any of the over 3,000 individuals identified in our research. Based on our findings, we assess that having accounts on multiple known CSAM sources may indicate an increased likelihood for a user to have committed or to potentially commit crimes against children. Our study demonstrates that infostealer logs can be used by investigators and law enforcement partners to track child exploitation on the dark web and provide insight into a part of the dark web that is especially difficult to trace.

Recorded Future has escalated to law enforcement all relevant information that was reviewed as part of this analysis, and has reported all relevant material to the appropriate authorities.

Key Findings

- Infostealer logs can be used to identify CSAM consumers and new sources and trends in CSAM communities.
- By querying Recorded Future Identity Intelligence infostealer data, we identified approximately 3,300 unique users with accounts on at least one CSAM source. Approximately 4.2% of the observed unique users had credentials to multiple sources.
- In three case studies, we used the data contained in infostealer logs and open-source intelligence (OSINT) to identify two individuals. We also found further digital artifacts, including cryptocurrency addresses, belonging to a third individual.
- As the cybercriminal demand for infostealer logs and malware-as-a-service (MaaS) ecosystems continues to grow, we anticipate that infostealer log datasets will continue to provide current and evolving insights into CSAM consumers.

Background

Infostealer malware is capable of stealing a wide range of users' sensitive information, including account login credentials, cryptocurrency wallets, payment card data, operating system (OS) information, browser cookies, screenshots, and browser autofill data. The most common attack vectors used for distributing infostealers are phishing and spam campaigns, fake update websites, SEO poisoning, and malvertising. An especially popular infection vector in the last year has been "cracked" software (software that has had its copy protection removed), marketed to users seeking to illegally obtain licensed software.

After exfiltrating data from victims, threat actors can use the stolen data and credentials to gain unauthorized access to networks, escalate privileges, and perform ransomware attacks on organizations. Additionally, threat actors may monetize this information by selling it to other cybercriminals. The stolen data, known as "infostealer logs", regularly ends up on dark web sources, allowing cybercriminals to purchase the data and potentially use it to gain access to an organization's network or systems. The wide net cast by this type of malware makes it increasingly probable that cybercriminals themselves may end up ensnared within it. Such conclusions have also been reached by researchers at Hudson Rock, who identified 120,000 instances of infostealer infections of users with login credentials to cybercrime forums. Similarly, users of CSAM websites are also certainly contained within this dataset.

The anonymity offered by Tor-based websites with .onion domains provides a platform and a sense of security for those producing and consuming CSAM. A 2015 study found that in an analysis of 80,000 unique .onion addresses, approximately 2% of the websites were related to child abuse websites. The same study found that despite the relatively low number of child abuse websites, approximately 80% of dark web browsing activity was directed toward websites hosting CSAM.

Since the majority of CSAM websites are hosted on Tor, one way for individuals to discover such sources is via "hidden wikis", which list .onion domains. Such websites serve as guides to illicit content, while ostensibly allowing users to maintain anonymity. We have observed nearly 10,000 references to hidden wikis in the Recorded Future Intelligence Cloud in the last year, indicating the continued popularity of this method. The 2015 study also noted that even once users accessed CSAM forums from such wikis, the landing pages were characterized by their simplicity, often requiring users to obtain invitations from existing members for access.

Another study, published in August 2023, found that a high volume of CSAM is generated and shared on a daily basis on dark web forums. The study collected dark web data related to CSAM in a dataset the researchers termed "ATLAS", which they used to analyze 353,000 posts across eight dark web forums and identify approximately 35,400 unique users. The forums that were identified in this study are similar to the popular forums we discovered during our research, including "boysrus", "Amorzinho", and "Resistance". These three forums had similar post counts, each comprising approximately 9% of the total number of posts in the ATLAS dataset. Of the posts that were in the dataset, English was the most commonly used language, with 221,876 posts (around 83.25% of the identified posts), followed by Russian (24,415 posts), and Portuguese (6,594 posts).

Additionally, law enforcement investigations into CSAM websites on the dark web found that, in most instances, website administrators lacked technical sophistication. For instance, during Operation Pacifier, conducted in 2015 by the FBI targeting the darknet platform Playpen, investigators identified the administrator and creator of the platform as a resident of Naples, Florida, after he inadvertently revealed his IP address. This individual established the darknet website, which was active between August 2014 and February 2015, and reportedly had over 215,000 members and hosted approximately 23,000 sexually explicit images and videos of children. Similarly, law enforcement identified and arrested hundreds of individuals associated with accounts on the CSAM-hosting platform "Welcome to

Video" due to those individuals' misunderstanding of how anonymity worked in Bitcoin (BTC) transactions. We hypothesize that the relative technical immaturity of those visiting and registering on websites hosting CSAM may correlate to low overall cyber hygiene. In turn, we believe that this increases the likelihood of such individuals being infected in widespread infostealer malware campaigns, potentially creating a unique opportunity to leverage the dataset to enumerate and analyze them.

Methodology

The method we used to conduct our research can be summarized as follows:

1. We created a list of known high-fidelity CSAM domains.
2. Using this list of domains, we queried Recorded Future Identity Intelligence proprietary data to identify users with login credentials to these domains.
3. By grouping users based on each source, we identified trends, patterns, and quantitative conclusions within each group.

In order to determine the names and domains of dark web sources that host CSAM, we collaborated with non-profit organizations that focus on anti-human trafficking efforts and child safety online, including World Childhood Foundation and the Anti-Human Trafficking Intelligence Initiative (ATII). Their expertise on the subject allowed us to understand the nature of CSAM distribution on the dark web and finalize a list of popular sources where CSAM is hosted and consumed.

We were then able to further expand this list by querying the Recorded Future Intelligence Cloud for mentions of these sources. As mentioned in the **Background** section above, many of these domains were contained within hidden wiki link collections alongside other domains with names suggestive of a CSAM focus. We also identified similar kinds of domains within credential package listings for sale on dark web shops such as Russian Market, 2easy Shop, and Genesis Store (now defunct), in which cybercriminals frequently list the domains for which stolen credentials are for sale in their listings to entice buyers. A pattern that emerged during our research was that CSAM consumers were frequently active on multiple websites, which led us to additional sources. Once we had further augmented our lists, we were then able to once again confirm newly discovered sources with our non-profit partners, such as World Childhood Foundation and ATII, creating a source discovery feedback loop.

In our next step, we queried Recorded Future's Identity Intelligence, which provides real-time access to infostealer log information and can provide intelligence related to both employee and customer identities, allowing organizations to prevent breaches before damage is widely spread. As of April 2024, there were approximately 25 billion credentials in Recorded Future's Identity Intelligence, with a new credential ingestion rate of 150 million credentials per month. We queried this dataset for authentication records associated with known CSAM sources indexed between February 2021 and February 2024 and analyzed the resulting data to arrive at an approximate unique user count.

This analysis required some de-duplication, as many of the users had been compromised by different infostealers at various points, or had multiple accounts on several sources. Our primary method for de-duplicating these entries was to compare OS usernames and PC names, which are typically contained within the infostealer logs. However, we believe that the true number of unique users is almost certainly higher due to default or popular OS usernames (such as “Administrator” or “user”) being reused across devices.

Findings

Using the methodology described above, we identified a total of 3,324 unique credentials that were used to access known CSAM websites between February 2021 and February 2024. This data allowed us to collect statistics about individual sources, such as the top country codes and IP addresses accessing them, as well as data about individual users, including their usernames, IP addresses, and system information. This more granular data also enabled us to identify common login and use patterns among individual users, as well as those common to specific sources. This data can allow law enforcement to:

- Have a better understanding of the underlying infrastructure used to host these websites
- Uncover techniques used by CSAM consumers to mask their identities and logins
- Identify potential CSAM consumers and producers

Please note that all source names in this report are shortened and obfuscated to avoid sharing the real names or URLs associated with these sources.

Source Breakdown

Using our list of CSAM domains obtained from non-profit and victim advocacy organizations, supplemented with the newly discovered sources identified in dark web source listings, we were able to rank CSAM hosting websites by the number of compromised credentials in the last three years. The top ten sources identified below were kidflix4m, alice34, gk3fgh, 243vn, club, xian, myteens, 3dboys, myboys, and boyvi6. Of note, at least one video streaming source alleged that it did not use JavaScript; likely in an effort to increase the anonymity and privacy of its users who may be concerned about their IP addresses or session details being exposed.

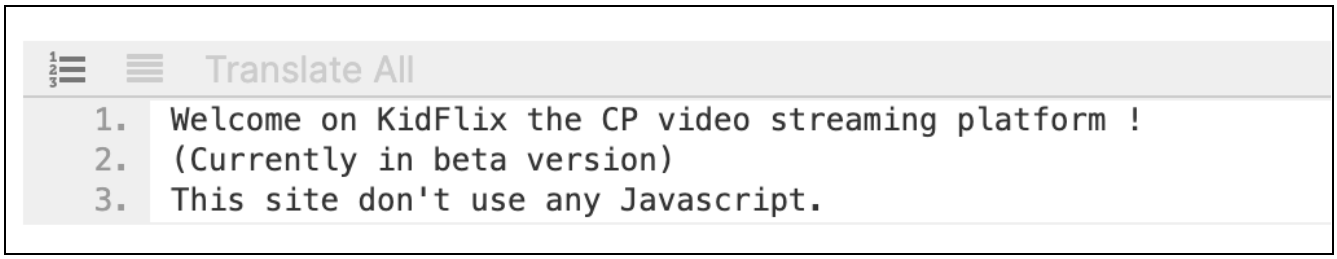


Figure 1: *Indexed web page content from the kidflix4m source, potentially for obfuscation purposes (Source: Recorded Future)*

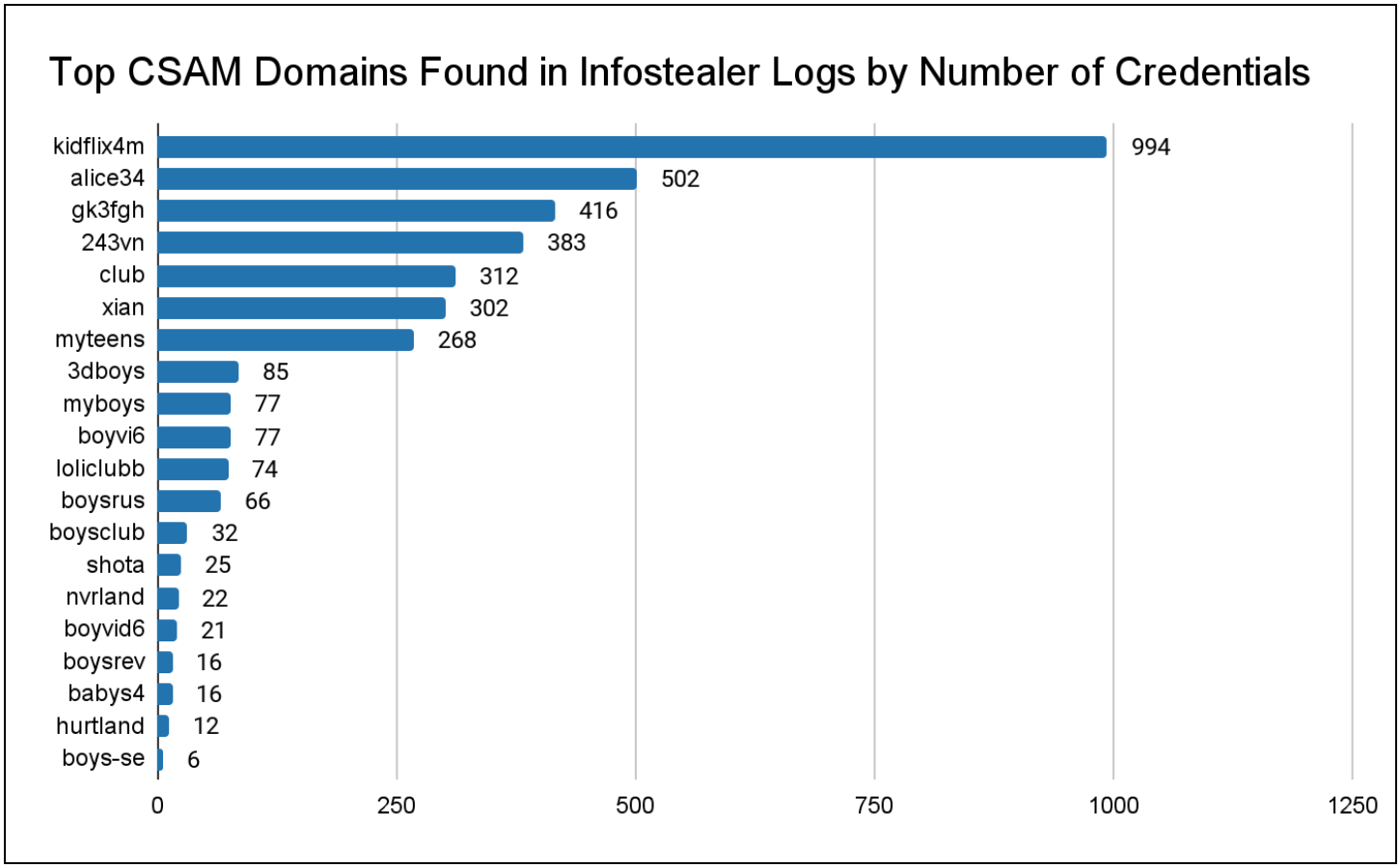


Figure 2: *Top CSAM sources found in infostealer logs between February 2021 and February 2024, by number of logs containing authentication credentials (Source: Recorded Future Identity Intelligence)*

The content and nature of sources vary from discussion-based forums to image-sharing websites and video-streaming platforms. We believe that multiple sources contain or specifically focus on “hurtcore”, an extreme form of exploitative content usually involving bodily harm.

Geographic Trends

Across nearly all identified sources, we found that Brazil, India, and the United States (US) had the highest counts of users with credentials to known CSAM communities, though this is likely an overrepresentation due to dataset sourcing. This is particularly noticeable in sources with high overall identified users, namely kidflix4m, alice34, and Amorzinho, with Brazilian users emerging as the primary user group in each case.

Source	Unique Users	Top Countries (by # users)	Top Countries (normalized)
kidflix4m	308	1. Brazil (129) 2. India (108) 3. US (73)	1. Ukraine 2. Nepal 3. Czech Republic
alice34	192	1. Brazil (88) 2. US (39) 3. India (39)	1. Oman 2. Jordan 3. Japan
Amorzinho	173	1. Brazil (137) 2. US (29) 3. India (20)	1. Japan 2. Brazil 3. Great Britain
myteens	112	1. Brazil (50) 2. India (19) 3. US (14)	1. Myanmar 2. Ukraine 3. Japan
boysrus	37	1. US (10 users) 2. Brazil (9 users) 3. Algeria (7 users)	1. Jordan 2. Algeria 3. Portugal
Resistance	54	1. Brazil (25) 2. US (18) 3. Algeria (6)	1. Cuba 2. Japan 3. Australia

Table 1: *Geographical breakdown of CSAM sources and users as identified by infostealer logs (Source: Recorded Future Identity Intelligence)*

However, we assess that this is almost certainly an effect of an overall data bias in infostealer infections more broadly. According to Recorded Future's full infostealer dataset collected over a sample period between August 27, 2023, and February 27, 2024, we saw largely the same trends: Brazil overwhelmingly dominated the counts for the highest number of infostealer logs, followed by India and then the US.

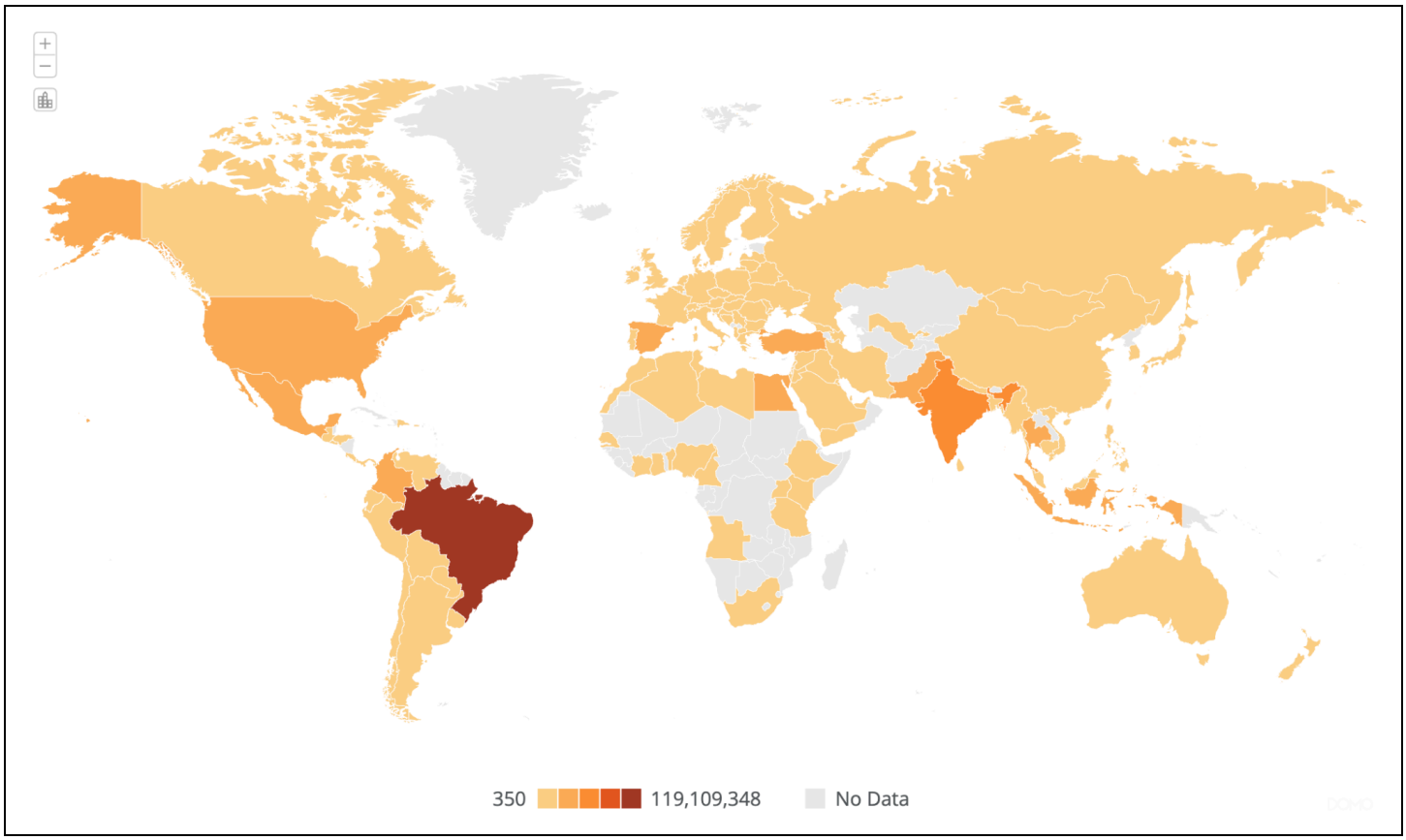


Figure 3: *Recorded Future Identity Intelligence infostealer logs indexed between August 27, 2023, and February 27, 2024 (Source: Recorded Future)*

Both Insikt Group and external vendors have observed that Brazil has seen the highest rates of infostealer infection in the last several years. SOCRadar has attributed this overrepresentation to high levels of software piracy in Brazil, making these users increasingly susceptible to infostealer-laden "cracked" or unlicensed software sources, which have emerged as a prominent infection vector to spread this malware.

The US and India also figure among the top sources for infostealer infection, which is likely a result of relative population size paired with increased technical literacy rates, with India and the US both being in the top three countries by population size as of 2023 (1.428 billion and ~340 million, respectively). Notably, China is the second-largest country by population size and has the largest number of internet users in 2024 (1.425 billion and 1.05 billion people, respectively), but does not figure prominently in any of our sources. The reason for this is almost certainly the relatively closed nature of the Chinese online ecosystem, likely making Chinese users less susceptible to infostealer infection techniques that rely on Google and Facebook Ads or SEO poisoning. It is also likely that the majority of infostealer command-and-control (C2) traffic is blocked by China's internet censorship protocols, as these infostealer variants are mostly advertised in Russian- and English-language sources and are likely hosted outside of China.

The above data bias complicates any geographic analysis conducted on a source-by-source basis. To overcome this challenge, we analyzed our full infostealer log dataset and focused on sources with a relatively large number of unique users. For each source, we calculated the proportion of users from specific countries by dividing the raw count of infostealer logs from each country by the total number of infostealer logs for that source. This normalization process allowed us to compare the relative prevalence of users from different countries across sources, regardless of the total number of logs associated with each source. This allowed us to pull out some more potentially interesting insights for kidflix, alice34, and Amorzinho.

The source kidflix4m was primarily found to be present in infostealer logs from users in Eastern Europe, including Ukraine, the Czech Republic, and Poland, though individuals from Nepal and Australia were also among the most frequent users. Oman and Jordan were the top two countries from which users visited alice34, as well as Japan, Bulgaria, and Russia. Despite the data bias, Amorzinho remained a top source for Brazilian users, likely because it is a Brazilian source itself ("amorzinho" means "darling" in Portuguese), though we also observed relatively high counts of users from Japan and Britain.

Although normalizing the data likely allows for a more directionally accurate analysis of geographic trends associated with each CSAM source, we emphasize that our dataset is still too small to make any concrete conclusions from the resulting proportions. For the most statistically accurate and reliable insights, these counts must be continuously re-calculated and re-evaluated as more data becomes available. Such geographic analysis is likely to be particularly useful in source profiling in order to plan and allocate law enforcement efforts according to each country's jurisdiction, particularly when seeking to conduct takedowns or focus prosecution efforts.

Log Analysis

By performing a more granular and manual analysis of the extracted logs, we were able to extract insights about potential authentication strategies used by these various sources, extract key digital artifacts to use as pivot points, and identify prolific users. To narrow down the 3,706 total logs for this proof-of-concept research, we identified 362 logs associated with users that had accounts on multiple CSAM sources, further de-duplicated to 141 unique users. We identified these "repeat offenders" by looking at the individual usernames that were used to login to services, as well as OS usernames that are associated with the infected device.

Among the extracted artifacts from this sample set were ten active cryptocurrency wallet addresses, as well as information that allowed us to identify two users presented in "case studies", one of which we were able to link to a previously prosecuted sex offender in the US state of Ohio.

Source Usage Patterns

One login username that we observed 96 times across different infected machines and IP addresses was "*amorzinho@amorzinho[.]com*", which was used in all cases to log in to the "Amorzinho" CSAM

forum. In many of those cases, we observed users logging into the website both using this credential and a more personalized username at a later time.

We observed this activity pattern with another prominent CSAM forum, "Resistance", where the login "*member@resistance[.]onion*" was used in the same way. Although we were unable to identify any references to this login pattern on our dark web source collections, one explanation for this activity may be that it is a way for users of these forums to follow an "invite-only" registration strategy to prevent outsiders from infiltrating the boards. One potential way for this to work is if the website requires users to first login using a shared credential prior to making an account to access the full site, with the credential being shared in more hidden channels such as closed chat rooms, though we do not have sufficient evidence to support this hypothesis at this time. Several websites also showed logins under usernames like "*real@email[.]net*", "*a@aa[.]aa*", and "*x@y[.]net*", which is likely an indicator of a lack of email verification required for some of these websites.

Another login pattern we observed in our dataset surfaced in the "myteens" source. Nearly all 268 users of this forum in our dataset appeared to have randomly generated six-character usernames (for example, "7j5v0g" and "62vzkg"), with the exception of "*marcos****@gmail[.]com*", "*baseadogab****@gmail[.]com*", "gbariea", and "irish2sxy4u", all of whom had a longer non-random username in addition to the randomly generated string. The website may use random username generation as an additional anonymity measure; it is possible that the individuals with more unique credentials occupy an administrative, developer, or moderator role on the website, though we were unable to definitively determine this from this data alone.

On Cryptocurrency Wallets

Cryptocurrency tracing, particularly as it relates to online CSAM communities, can be a powerful tool to identify administrators, producers, and consumers of harmful material, as well as lead investigators to real-life instances of children being abused. Previous law enforcement operations, such as the 2019 takedown of the CSAM website Welcome to Video, have used incidentally discovered cryptocurrency wallets to orchestrate takedowns, arrest abusers, and rescue children who were either actively being harmed or at risk of harm.

Separately, many infostealer variants on criminal sources boast the capability to exfiltrate victims' cryptocurrency wallet data, with the likely goal of cryptocurrency theft. Of the 141 "repeat offenders" we identified, we identified only one with a cryptocurrency wallet in the data package — the infostealer logs for this individual included an encrypted Electrum wallet. We were unable to extract useful data from this wallet, but instead were able to identify cryptocurrency-related data contained in their infostealer log data for thirteen other users. The majority of these were found in users' autofill data and included cryptocurrency wallet addresses and browsing history related to cryptocurrency-related websites. Most importantly, we were able to extract 24 cryptocurrency wallet addresses for further analysis.

Of these, fourteen appeared to be Ethereum (ETH) addresses, three were TRON addresses, three were BTC addresses, and two were Litecoin (LTC). Of the wallets we were able to surface, approximately ten had transaction histories, and we were able to link the wallets to exchanges such as Binance, CoinExchange, and BitMart. More significantly, in our preliminary analysis of these addresses, we found two that were connected to CSAM distributors based on OSINT findings:

- bc1qrtfc2t9k[...]02y48ref6tw4
- bc1q5ctpkga[...]3m6qd8he7c5

According to OSINT analysis, the above two addresses were assessed on November 16, 2021, and were associated with a subscription rate to an unspecified source, for the USD equivalent of $35 in BTC. Although we were unable to link a specific transaction ID or personal wallet to these entries, we believe that an analysis of the corresponding credentials to CSAM domains may provide a useful direction in connecting wallet addresses to sources and distributors. Furthermore, continuous monitoring of this log data may provide future insights into cryptocurrency wallets tied to both new and existing CSAM sources.

Sample User Investigations

From 141 repeat offenders identified over 362 log references, we chose three users for a case study to provide sample investigative workflows and illuminate the types of external accounts, usernames, and other indicators that can be identified.

d****: Previous Offender

The first case study is for an investigative workflow on a user we are identifying as “d****”, based on the username associated with their infected machine. This workflow demonstrates that having accounts on multiple known CSAM sources can be used as an indicator to surface individuals who are likely to have committed or to potentially commit crimes against children. We successfully identified this user using the data points in the infostealer logs, which revealed that they had previously been convicted of child exploitation and were arrested in a sting operation where they attempted to meet a minor for “lewd purposes”.

The starting point of our investigation for d**** was the fact that they maintained accounts on the following CSAM websites:

- Resistance
- 243vn
- alice34m
- Amorzinho

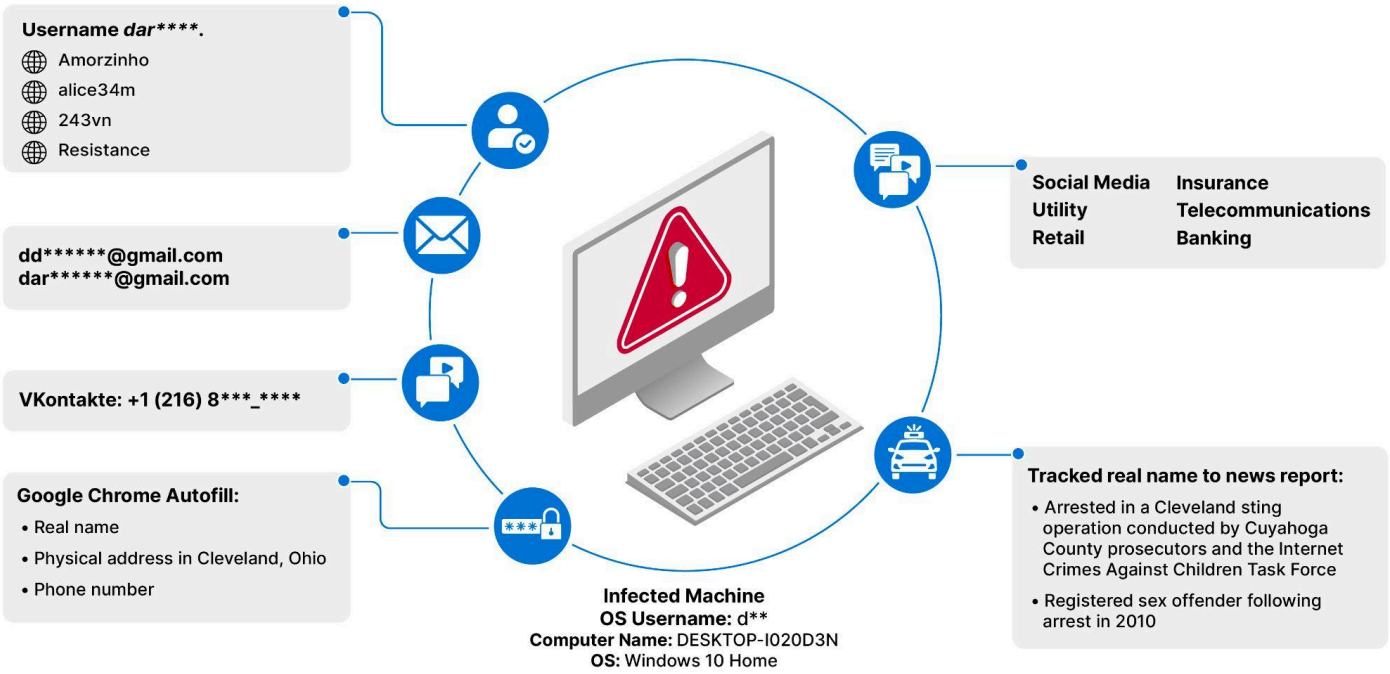


Figure 4: *A diagram showing artifacts contained in infostealer logs associated with the user "d****" (Source: Recorded Future)*

Using the credentials within the infostealer records for d****, we also identified numerous accounts on clear web services that are tied to this individual's identity, including the following:

- Facebook (dd*****@gmail.com)
- Google (dd*****@gmail.com, dar*****@gmail.com)
- FirstEnergy
- Assurance Wireless
- Walmart
- VK (Using phone number (216) 8**-****)
- Ohio SSP Benefits
- Windows Live
- AT&T
- Tyson Foods
- Wells Fargo

Using Google Chrome autofill data contained in the infostealer records, we were able to identify this individual's likely address as a location in Cleveland, Ohio, as well as their full name, phone number, and additional email addresses. This information allowed us to potentially connect this individual to public reporting from 2019 by local area news.

According to this news report, an individual matching the first and last name identified in our data source was arrested in a sting operation conducted by local law enforcement and the Internet Crimes

Against Children Task Force, which resulted in the arrest of multiple additional suspects. The individual identified in our infostealer source had also previously been convicted in 2010 for engaging in sexual relations with and giving drugs to a 14-year-old girl, for which the individual served one year in prison. We were able to connect this individual to a sex offender registry listing and assess that this is almost certainly the user identified as d**** in the infostealer logs.

docto: Unreported Abuser

Another individual found in our dataset, with the username "docto" on their infected machine, was registered on nine confirmed CSAM websites, including the following:

- boyvi6
- 243vn
- boysclub
- alice34m
- loliclubbly
- kidflix4m
- Amorzinho
- Resistance
- boysrus

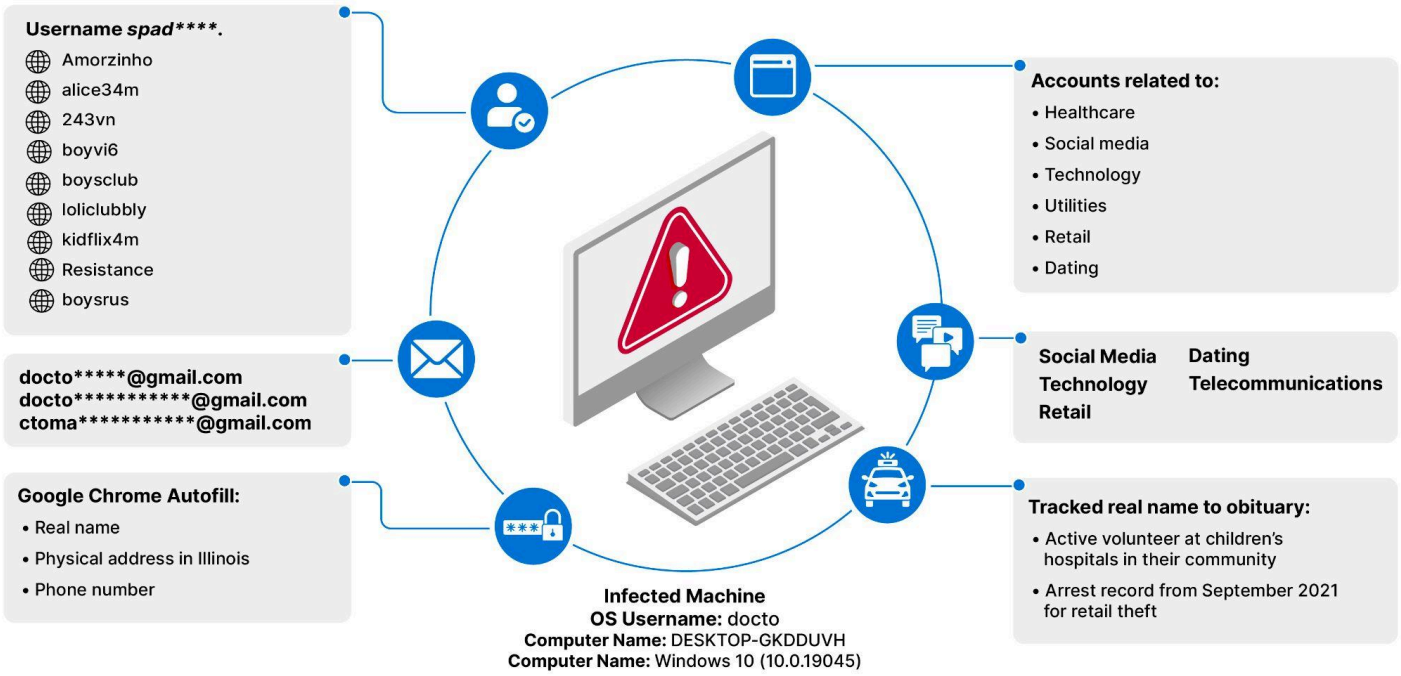


Figure 5: *A diagram showing artifacts contained in infostealer logs associated with the user "docto" (Source: Recorded Future)*

The workflow we employed for docto showcases that infostealer log-based investigations can be used to surface and identify individuals who have avoided law enforcement scrutiny and essentially "flown under the radar" despite engaging in exploitative behavior online. Using data points from infostealer logs and open-source reporting, we linked docto to a real-life individual who shares multiple characteristics, including name, nickname, geographic location, and interest in and history of healthcare employment. The individual appears to have been actively seeking out volunteer and employment

opportunities that would give them access to children, and their Google search history indicates they may have been a guardian to a child. Despite their membership in multiple CSAM-focused forums, they would not have been flagged in any background check since they had no prior child exploitation-related convictions.

In addition to the above, we identified credentials likely associated with this individual to clear web websites and services, including but not limited to the following:

- Facebook
- Google
- Several Illinois government websites, including Illinois ABE (Application for Benefits Eligibility, *abe.illinois[.]gov*) and Illinois Job Link (*illinoisjoblink.illinois[.]gov*)
- Several job application websites in the healthcare industry
- A forum called “Hypnosis for Guys”
- T-Mobile
- Windows Live
- Grindr

We also observed Google searches pulled by the infostealers for “how much money can I make on Illinois unemployment with one child”, as well as several Google searches for children’s hospitals in the area.

Additionally, the user’s browser autofill data allowed us to pinpoint their full name, physical address, and several phone numbers. Using this information, we identified an obituary for this individual from January 2024, in which the description states that they were an active volunteer at children’s hospitals in their community. This potentially corresponds to our above findings regarding Google searches made by this individual and accounts they maintained on healthcare employment-related websites. The additional information we gathered is concerning when considering their registration on nine CSAM websites.

Using their full name and approximate location, we also identified a likely arrest record from September 2021, in which this individual was arrested for retail theft.

Bertty: Cryptocurrency User

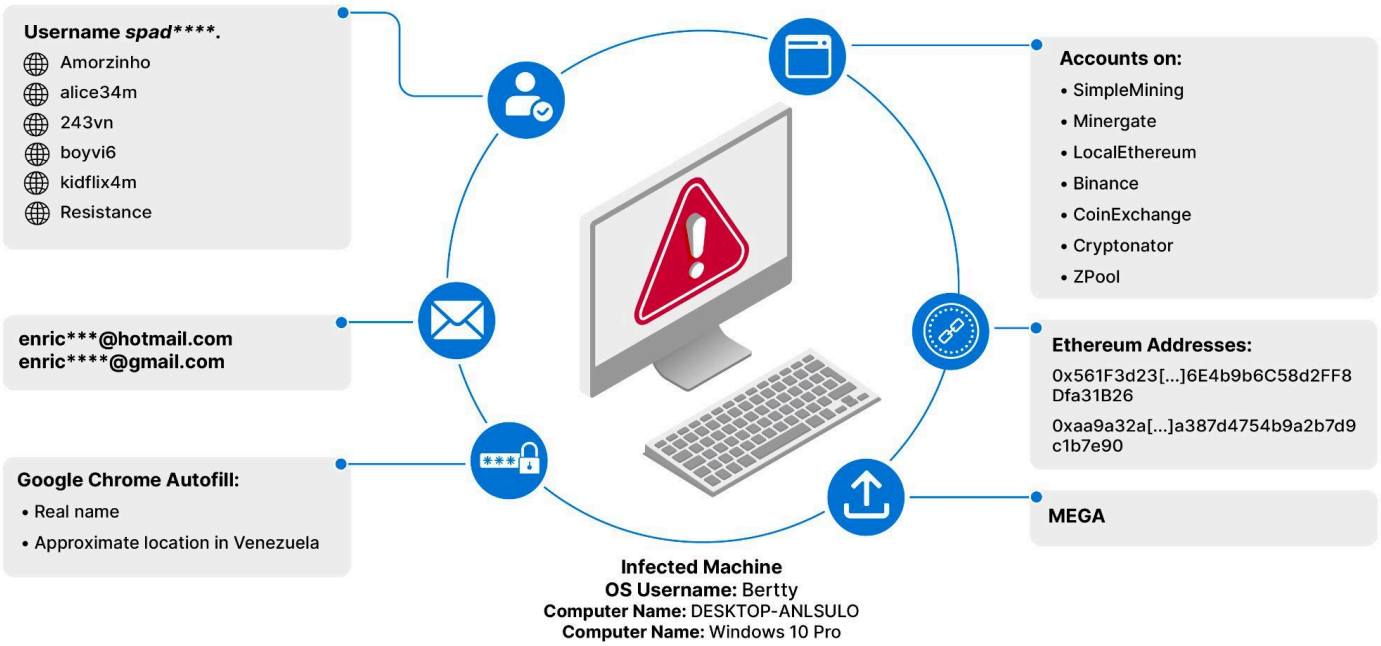


Figure 6: *A diagram showing artifacts contained in infostealer logs associated with the user "Bertty" (Source: Recorded Future)*

In evaluating users whose infostealer logs included cryptocurrency wallet addresses, we identified one individual linked to two ETH addresses with historical transactions. This user, "Bertty" on their infected machine, was found to have accounts on the following CSAM websites:

- alice34m
- 243vn
- Resistance (two mirrors)
- Amorzinho
- kidflix4m

The presence of active cryptocurrency wallets (one of which was found to have 23 transactions), makes this individual a candidate for further investigation into the purchase and production of CSAM material, as these communities are known to use cryptocurrency to perform transactions. Furthermore, this individual was found to have the MEGA desktop application installed on their computer, which is a desktop client for the MEGA file-sharing service. The user also had a large number of `mega[.]nz` file paths in their browsing history, which is a trend we have observed across the CSAM-affiliated infostealer logs we have collected. MEGA is a privacy-centered cloud storage and sharing service based in New Zealand that has been connected to numerous cases of CSAM sharing and storage. According to a transparency report published by MEGA itself, between 2022 and 2023, between 6% to 10% of all created links on the service were to CSAM content, with over 25,000 such links disabled in

Q3 2022. The service was also linked more anecdotally to several criminal cases involving individuals in the US, Australia, and New Zealand, where defendants were found to be manufacturing, distributing, and receiving CSAM using the service [1, 2, 3]. Although the mere presence of MEGA links and the desktop application in this individual's browsing history are not definitive indicators of their distribution of CSAM, an investigation into cryptocurrency transactions is a potentially valuable lead for similar datasets when individuals are suspected of manufacturing, buying, and selling such content.

Several other data points we were able to identify included the user's likely status as a student in Venezuela, and we were also able to identify the individual's likely full name, place of birth, and physical address.

Outlook

Infostealer malware and stolen credentials are projected to remain a cornerstone of the cybercriminal economy due to the high demand by threat actors seeking initial access to targets. The proliferation of the MaaS model will almost certainly expand the marketing of stolen credentials as an efficient and profitable means for cybercriminals to capitalize on leaked credentials. Similarly, like other aspects of the cybercriminal underground, CSAM producers and consumers will almost certainly continue to seek online platforms to anonymously share illicit content.

Analyzing infostealer logs will likely continue to provide a useful keyhole view into CSAM sources and the use patterns of their members. These insights can be used to track source lifecycles, identify new mirrors and sources, and de-anonymize users. In the event of source takedowns, such a dataset may provide insights into user migration patterns and platform successors. Ultimately, we believe that utilization of this dataset will facilitate prosecution and takedown efforts and debunk the veneer of anonymity assumed by individuals seeking to harm children.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com