P1

2024

SpyCloud

IDENTITY EXPOSURE REPORT

ANALYSIS OF NEXT-LEVEL CYBER THREATS, UNLOCKED

<PRESS START>

TABLE OF CONTENTS

THE DIGITAL IDENTITY IN 2023 ... 2

WELCOME TO THE SHOWDOWN: CYBERCRIMINALS STEP UP THEIR GAME ... 3

- THE FIGHT OVER DIGITAL IDENTITIES ... 4
- WHY WE DO THIS REPORT ... 5
- OUR SECRET WEAPON: SPYCLOUD RECAPTURED DATA ... 6

TRENDS ... 6

- USER VS. CRIMINAL: THE 2023 IDENTITY EXPOSURE ARENA ... 7
- DIGITAL IDENTITIES ARE A TOP ATTACK VECTOR ... 8
- MALWARE INFECTIONS AS A MAJOR PLAYER IN IDENTITY EXPOSURE ... 9
- 123456: EXPOSED POPULAR PASSWORDS ... 10
- SINGLED OUT: THE GOVERNMENT SECTOR ... 11
- PASS GO, COLLECT 200 PII ... 12

MALWARE TRUMPS ALL, THOUGH ... 15

- MALWARE'S NEXT MOVE: INFOSTEALER FAMILIES TO WATCH ... 16
- AND A NEW CHARACTER ENTERS THE GAME: MOBILE MALWARE ... 17
- OTHER EASTER EGGS ... 17

THE VICTORY TOKEN: STOLEN SESSION COOKIES ... 18

GOTTA RECAPTURE 'EM ALL: NOTABLE DATA BREACHES ... 19

TURNING THE GAME IN YOUR FAVOR - AND AGAINST CYBERCRIMINALS ... 22

- THE STAKES ARE HIGH: WHAT'S NEXT ... 23

THE AVERAGE PLAYER

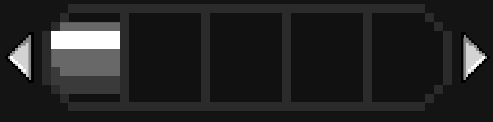
4 UNIQUE EXPOSED
USERNAMES / EMAIL ADDRESSES

67% OF EMAILS
ACCOMPANIED BY A COMPROMISED PASSWORD

9 BREACHES

15 BREACH RECORDS

1 IN 4 RECORDS
CONTAINED INFORMATION ABOUT THE USER NETWORK OR PHYSICAL LOCATION



1 IN 5 CHANCE
OF ALREADY BEING THE VICTIM OF AN INFOSTEALER INFECTION

--- BASED ON A SAMPLE OF DATA SPYCLOUD RECAPTURED FROM THE CRIMINAL UNDERGROUND IN 2023.

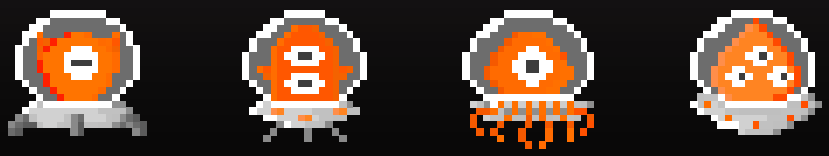
THE DIGITAL IDENTITY IN 2023

Based on our analysis of the average digital identity exposed and traded in the criminal underground last year

SpyCloud

STAGE 1

WELCOME TO THE SHOWDOWN:



CYBERCRIMINALS STEP UP THEIR GAME

BACK

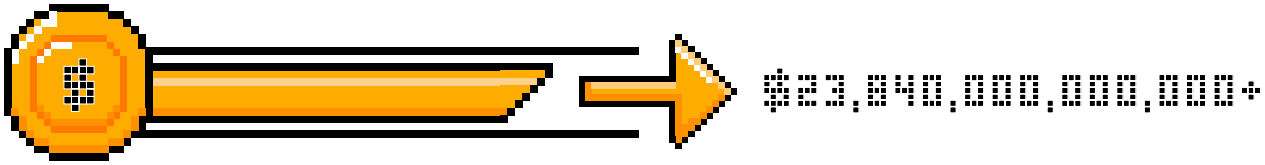
NEXT

THE FIGHT OVER DIGITAL IDENTITIES

Digital identities are embedded in our lives, and their expansiveness makes it harder and harder to protect our accounts and business systems from attacks. Data stolen by criminals and traded between bad actors has continued to scale dramatically each year. Case in point: **SpyCloud's total collection of recaptured data has grown to more than 43.7 billion distinct identity records.**

And to further complicate an already complex threat landscape, malicious actors are moving beyond the traditional use of stolen username and password pairs to perpetrate crimes against consumers and organizations. Using expanded datasets, criminals have increased the scope of their attack patterns, based upon identity records that come from different sources and that can be linked together using PII, like social security numbers or social handles. In this way, users now have to worry about their combined digital identity, which can be formed by cross-referencing the information that has been stolen about them from dozens or hundreds of sources.

To make matters even worse, criminals have responded to improved authentication technologies by sidestepping user authentication methods altogether. Bad actors are able to access stolen session cookies and 2FA secrets to impersonate their victims, making it extremely difficult to differentiate between legitimate users and criminals.



*Cybercriminals are clearly cashing in on this opportunity, which is why the global cost of cybercrime is forecasted to nearly triple by 2027, from **$8.44 trillion in 2022** to **$23.84 trillion**.*

*We see this exponential growth reflected in our own repository of data recaptured from the darknet, which totals **more than 560 billion stolen assets** as of the publishing of this report.*

As you'll see in this report, we've observed an increase in next-generation identity attacks that force us to expand our definition of digital identities and the measures we use to protect ourselves.

WHY WE DO THIS REPORT

Threats to digital identities are nothing new. However, the fast pace and stealthy nature of a dynamic criminal underground makes it hard for security teams to keep up and proactively defend against new threats.

SpyCloud researchers and data scientists examine the trends related to identity exposure in the criminal underground every year. We keep a tight pulse on darknet activity to understand how stolen data exposes organizations and consumers to cybercrimes like account takeover, session hijacking, fraud, and ransomware.

While we consistently see the number of exposed identities growing, in recent years we've also detected a shift in the type of data that malicious actors rely on to compromise identities. In response to this shift, we continue to expand our datasets to explore how emerging and evolving threats put consumers and organizations at further risk.

The most alarming trend we see today – bar none – is malware. **Infostealers** and other types of malware exfiltrate valid authentication data like login credentials and session cookies, and are even beginning to target passkeys. In the hands of criminals, this data makes it easy for attackers to mimic consumers' or employees' access to networks and applications with a high degree of success.

IN 2023:

61% of the breaches we recaptured were malware-related[2]. *This finding reflects the tremendous value cybercriminals gain with high-quality data exfiltrated by malware.*

Most organizations and consumers still are not aware of the massive breadth of digital identity data that is easily stolen from infected devices and made readily available on the darknet. This report aims to illuminate lesser-understood threats and underscore the risk they pose, so you can protect users and minimize impacts to your organization.

[2] *Data representative of 3,478 recaptured breaches analyzed by SpyCloud.*

OUR SECRET WEAPON: SPYCLOUD RECAPTURED DATA

SpyCloud collects, curates, enriches, analyzes, and automates the remediation of recaptured data from breaches, malware infections, and other sources in the criminal underground. With SpyCloud, security teams act on true evidence of compromise to mitigate the risk of damaging attacks that rely on the use of stolen data – preventing account takeover, session hijacking, ransomware, and online fraud.

For the purposes of this report, let's define how SpyCloud differentiates third-party breach data from malware victim data.

DATA BREACHES occur when information is stolen through unauthorized access to a network or system, typically exposing credentials and personally identifiable information (PII). Individuals are exposed in those breaches through no fault of their own. We call the set of data tied to a single user exposed in a breach a breach record. SpyCloud recaptures third-party breach data from darknet sources and notifies businesses when their employees' or customers' email addresses, usernames, passwords, and PII are found.

MALWARE is software specifically designed to harm or exploit computer systems, networks, or users. **Malware** can take various forms. SpyCloud largely focuses on recapturing infostealer malware and Trojan malware infection data. What we call **malware victim data** is information exfiltrated from infected devices – typically usernames and passwords, session cookies, autofill data, PII, and device and system details that can be used to impersonate victims (and, conversely, **to unmask cybercriminals**).

STAGE 2

TRENDS

BACK

NEXT

SpyCloud

USER VS CRIMINAL:
THE 2023 IDENTITY EXPOSURE ARENA

AVERAGE BREACH SIZE
1,979,357 RECORDS

100,000
MASTER PASSWORDS FROM POPULAR PASSWORD MANAGERS

61% OF BREACHES
WERE MALWARE RELATED

74% OF USERS
IN BREACHES REUSED COMPROMISED PASSWORDS

RECAPTURED EMAIL ADDRESSES
1.64 BILLION

4.7 MILLION
RECAPTURED THIRD-PARTY SOFTWARE CREDENTIALS

RECAPTURED PASSWORDS
1.38 BILLION

52 ACTIVE
INFOSTEALER FAMILIES

RECAPTURED PII ASSETS
32.22 BILLION

MACBOOK USERS
TARGETED BY BROADLY USED INFOSTEALERS

4 ENTIRELY NEW
INFOSTEALER FAMILIES: ATOMIC STEALER, MYSTIC, EXELA, ATLANTIDA

NEW DATA TYPES
SESSION COOKIES, CREDIT CARD INFO, API KEYS AND WEBHOOKS, CRYPTO ADDRESSES

WHAT WE FOUND IN THE CRIMINAL UNDERGROUND

DIGITAL IDENTITIES ARE A TOP ATTACK VECTOR

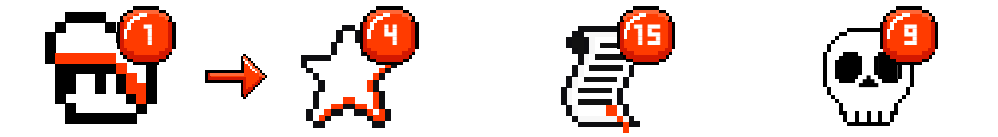
Cloud applications, remote work, mobile device use, and online services have placed digital identities at the heart of our personal and professional lives. Consequently, the digital identity has become a top attack vector – **90%** of surveyed organizations reported an identity-related breach in the past year.

Stolen credentials are still a popular tool for criminals to gain initial entry to systems and applications. But digital identities have evolved well beyond the traditional username and password combination, and all signs point to malicious actors exploiting each piece of data they can steal.

To deepen their capabilities, actors now also leverage the vast amounts of information available to them on the darknet to cross-reference stolen datasets. Working in this way, passwords used by an individual across different email addresses or usernames can be mixed and matched, increasing the total amount of PII that an actor may use in an attack.

Add to that – logs siphoned from infected devices can include data like IP addresses, credit card information, authentication or session cookies, and dozens of other data points. This combination of the person's identity and device details hands cybercriminals the keys to an even wider range of possible attacks.

SpyCloud's data shows that the scale of identity exposure today is massive. Our analysis of random email address samples recaptured in 2023 found that for a given person's digital identity, there is, on average:



With malicious actors gathering and using data across many stolen datasets, this type of information and associated access details and PII provide a slew of opportunities for malicious actors to gain access into an organization or application.

WHAT WE MEAN BY DIGITAL IDENTITY

The definition of a credential has evolved and no longer constitutes just a username and password. Each authentication layer in your network serves as a credential, broadening the possibilities for criminals sidestepping authentication methods and security measures to gain access.

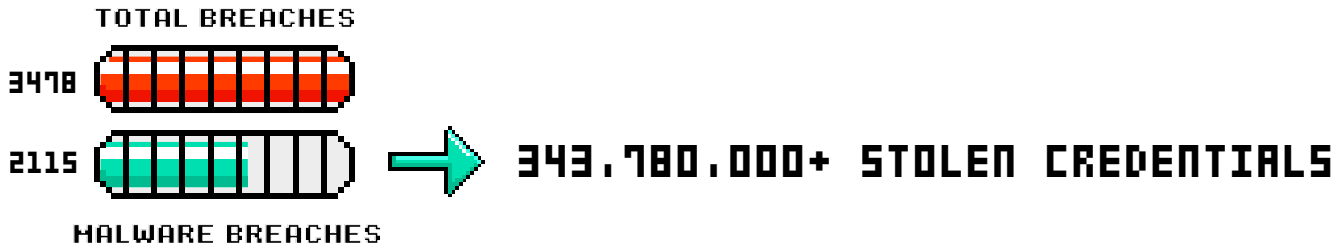
MALWARE INFECTIONS AS A MAJOR PLAYER IN IDENTITY EXPOSURE

The rapid rise of malware, specifically infostealers, is one of the biggest trends we continue to observe. In 2023 alone, infostealer malware use **tripled**. **We saw stealers skyrocket in our recaptured data, with as many as 1 in 5 people already the victims of an infostealer infection.**

Robot networks or "botnets" can deploy infostealers at scale, silently infecting machines without raising any flags for users or Security Operations Center (SOC) teams. Due to the nonpersistent design of most of this class of malware, it can take just seconds to siphon authentication and financial data – all without detection by antivirus software. Not surprisingly, this trend has the SOC's attention: in SpyCloud's 2023 Malware Readiness & Defense Report, respondents ranked infostealers as one of their **top three concerns**.

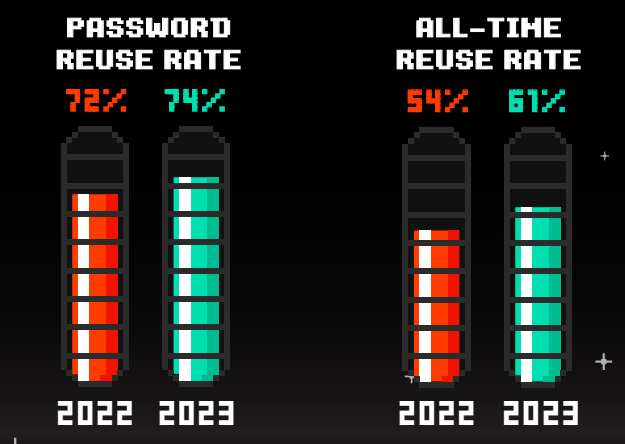
The reasons behind infostealers' climb to stardom are clear. They are cheap, highly effective in exfiltrating a treasure trove of useful data, and yield a high return on investment. The shift to malware-as-a-service models is an additional boon – and research suggests that **24%** of malware distributed as a service is from infostealer families.

SpyCloud's data illustrates how pervasive and considerable the infostealer threat is. Of the 3,478 breaches we analyzed, 2,115 – or **61% of total breaches** – were malware-related and included **343.78 million stolen credentials**. With valid credentials in hand, cybercriminals have a shortcut into employee and customer accounts.



AND TO MAKE THINGS WORSE...

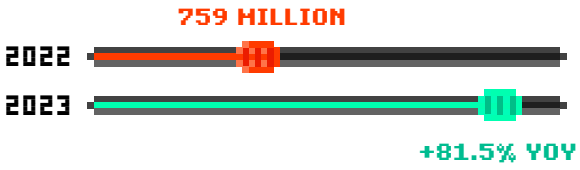
Password reuse rates remain incredibly high among users exposed in two or more breaches over the course of a year, and our research shows that – unfortunately – security awareness and password policies aren't improving password hygiene. The story is similar for the all-time reuse rate, which is the running average from when SpyCloud began recapturing data in 2016.



123456: EXPOSED POPULAR PASSWORDS

Every year, it comes as no surprise to see “123456” and its variations at the top of the common passwords list, but commonly-used passwords also give us a glimpse into burning topics that dominate pop culture. So, what preoccupied our collective minds last year?

SpyCloud recaptured a total of nearly 1.38 billion passwords circulating the darknet in 2023.



The hottest pop culture trend was **fantasy football**. As of 2023, an estimated 29.2 million Americans play it, which perhaps explains why the basewords football/fantasy football/ffl/NFL showed up **over 1.1 million times** on our list of most commonly compromised passwords. Other **pop culture topics** that wormed their way into hearts and passwords last year included:

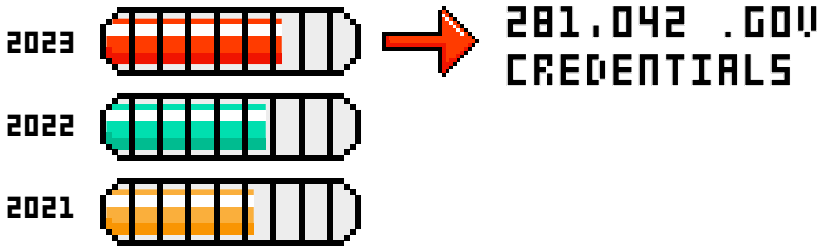
1,134,737	**THE FIVE-MONTH HOLLYWOOD WRITERS' STRIKE** WGA / hollywood / SAG / AFTRA / strike	
1,006,519	**THE NBA PLAYOFFS – MOST WATCHED IN 5 YEARS** NBA / NBA basketball / bball / NBA playoffs	
717,032	**THE BIG "HALO: THE MASTER CHIEF" UPDATE** halo / master chief / xbox	
398,464	**GLOBAL SOCCER LEGEND LEO MESSI SIGNS TO MIAMI** inter miami / mls / leagues cup / messi	
335,989	**UFOS CREATE A STIR IN CONGRESS** aliens / UFO / area51	
268,318	**BETHESDA GAMES LAUNCHES A NEW UNIVERSE** starfield / constellation / bethesda / xbox	
257,885	**MILEY CYRUS'S TOP-CHARTING YEAR** miley / miley cyrus / used to be young / flowers	
149,273	**THE BILLION-DOLLAR BOX-OFFICE HIT: "BARBIE"** barbie / barbie movie / hi barbie / i am kenough / barbie world	
119,289	**TAYLOR SWIFT REMAINS TOP-OF-MIND** taylor swift / taytay swift / swiftie / eras tour / tswift / midnights	

SINGLED OUT: THE GOVERNMENT SECTOR

Digital identity exposure may have even bigger implications for the government sector, given that **nation-states** and other sophisticated actors target critical infrastructure agencies. Yet SpyCloud data shows that government identity exposure continues to be a growing problem.

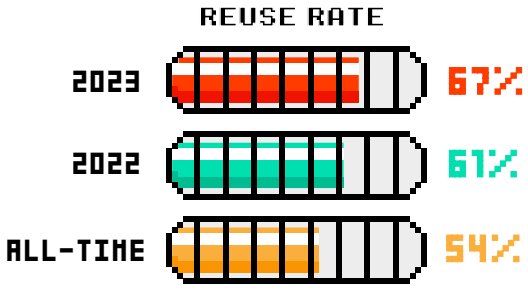
To learn how government agencies fared in breaches last year, we analyzed our recaptured data for emails associated with government domains.

723 BREACHES CONTAINED .GOV EMAILS IN 2023, compared to 695 in 2022 and 611 in 2021. The recaptured records contained 281,042 .gov credentials.



The story didn't get better when we analyzed password reuse rates among government employees.

WE FOUND A 67% REUSE RATE FOR .GOV USERS EXPOSED IN TWO OR MORE BREACHES IN THE LAST YEAR, an uptick from the previous year's 61%. The all-time .gov reuse rate remains high as well at 54% – meaning users aren't just reusing older passwords but are potentially using exposed passwords from as far back as 2016.[3]

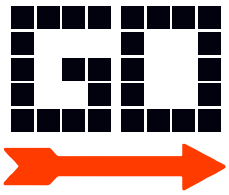


Government employees are just as guilty as their commercial sector peers of using easy-to-guess passwords.

The **most common passwords associated with .gov emails** were:

PASSWORD PASS1 123456

[3] *SpyCloud began recapturing data in 2016, our founding year.*



PASS GO, COLLECT 200 PII

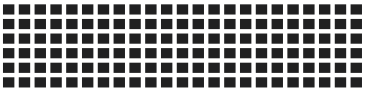
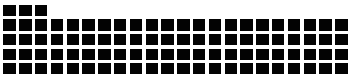
PII exposure remains a major concern for users and organizations. Nearly **70%** of surveyed businesses say their fraud losses have risen in recent years. Vast amounts of exposed PII fuel these trends.

SPYCLOUD RECAPTURED 32.22 BILLION PII ASSETS IN 2023

WE FOUND NEARLY 200 TYPES OF PII

ranging from everyday details like **names** and **addresses** to more concerning types like **passport numbers**, **dates of birth**, **credit cards**, and **social security numbers**.

The categories with some of the largest numbers in 2023 included:

3.16 BILLION	FULL NAME	
2.14 BILLION	PHONE NUMBER	
920.25 MILLION	DATE OF BIRTH	
171.61 MILLION	SOCIAL SECURITY & NATIONAL ID NUMBER	
36.97 MILLION	CREDIT CARD NUMBER	
16.03 MILLION	DRIVER'S LICENSE & PASSPORT NUMBERS	

STAGE 3

MALWARE TRUMPS ALL, THOUGH

BACK

NEXT

As noted earlier, our analysis of digital identity exposure expands every year in response to darknet and cybercriminal trends. We're tracking more advanced forms of malware as well as collecting new forms of exfiltrated data that fuel new identity risks. For this year's report, we doubled down on our efforts to understand the impact of malware, following a notable shift in threat actors' tactics and the amplified role of underground marketplaces.

Botnet malware is not new – it dates back to the '90s. But the technology has improved drastically since then, progressing beyond the original use cases of distributed denial of service (DDoS) attacks and spam. Today's sophisticated botnets are largely used to deploy infostealers that can evade antivirus and other endpoint protection solutions.

Infostealers are typically sold for a low malware-as-a-service subscription, which removes any barrier of entry for a fresh crop of cybercriminals. Entire underground marketplaces specialize in the sale of bots and botnet logs, and they have seen unprecedented growth. One leader in this segment, coined "Russian Market," offered **5 million** infostealer logs for sale on a single day in February 2023 alone. This marketplace had an astounding 670% increase in the number of logs for sale between June 2021 and May 2023.

These markets are very resilient, if the case of Genesis Market is any indication. In April 2023, the FBI took down this prominent, invitation-only marketplace that specialized in bots. But **some remnants** continued operating on Tor and even expanded their offerings to botnet logs.

SpyCloud is grateful for a strong partnership with the FBI. *The FBI shares breach data recaptured from large criminal websites it disables to support our mutual mission to protect citizens. We combine this data with our own to gain a broader picture of underground trends. Recent examples of this collaboration include the Genesis Market and QakBot takedowns.*

LAST YEAR ALONE, WE RECAPTURED:

More than
343.78 MILLION
malware-exfiltrated
credentials

Including more than
100,000 master
passwords

from eight market-leading password managers. Each of these master passwords represents the proverbial keys to the kingdom, unlocking access to hundreds of user accounts, and proving that no security tool is infallible. While password managers and other authentication controls like **MFA** are solid best practices, organizations need to think beyond traditional guardrails to address the risk from malware-exfiltrated data

Infostealer logs contain far more than credentials. The breadth of data includes not only everything cybercriminals need to emulate a device fingerprint and take over a digital identity, but also financial information such as credit card information, crypto wallet info, and even device screenshots.

Additionally, SpyCloud recaptured more than 4.7 million third-party application credentials harvested by malware on managed and unmanaged devices, including many popular business tools.

The top five most common categories of third-party tools in our recaptured data included:

# OF CREDENTIALS	THIRD-PARTY SOFTWARE CATEGORY
1,996,335	COMMUNICATION AND COLLABORATION
1,025,172	HUMAN RESOURCES
714,181	SOFTWARE DEVELOPMENT / IT SECURITY TOOLS
207,847	CUSTOMER SUPPORT
204,447	IDENTITY AND ACCESS MANAGEMENT

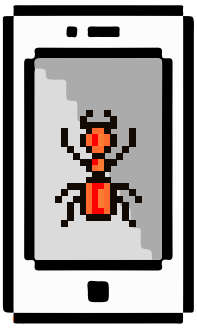
An even bigger challenge for security is that traditional malware infection remediation methods – such as wiping the device – don't truly protect organizations. Removing the initial malware infection doesn't stop attackers from operationalizing the already-stolen data to impersonate a digital identity and carry out follow-on attacks like ransomware. According to SpyCloud's 2023 Ransomware Defense Report, nearly **one-third** of North American and European companies victimized by ransomware in 2023 **had an infostealer infection prior to being attacked**.

MALWARE'S NEXT MOVE: INFOSTEALER FAMILIES TO WATCH

The records we recaptured in 2023 were siphoned by 52 infostealer families. Four of these families were new to the scene last year: Atomic Stealer, Mystic, Exela, and Atlantida. Two others, LummaC2 and RisePro, emerged in the second half of 2022 but grew exponentially in 2023. For instance, LummaC2 records in our recaptured data **skyrocketed by more than 2,000%** in less than six months.

It was more than Lumma Stealer's rapid surge that caught our attention. This strain came with new features previously not available in commodity infostealers, such as exfiltration of local password manager vaults and configuration files from remote desktop software. SpyCloud researchers also found evidence of exfiltrated browser-based 2FA secrets. This is all on top of typical capabilities like stealing saved credentials and session cookies, local files, crypto wallet private keys, and cached browser data like autofills.

Our researchers' analysis of data exfiltrated by LummaC2 showed that a log from a successful infection was **three times as large** as those from other infostealers, including prominent families like Raccoon and RedLine Stealer.



AND A NEW CHARACTER ENTERS THE GAME: MOBILE MALWARE

It's obvious that there's now a universal dependence on smartphones and tablets, which in turn creates a pressing need for better visibility into mobile device threats. And this threat is on the rise. Researchers found a **51%** increase in the number of unique mobile malware samples in 2022, coinciding with a **record** number of mobile phishing attacks.

SpyCloud's data reflects those observations. To date, we have focused on recapturing mobile banking Trojan logs due to their impact on businesses and consumers. Many of these logs include not only complete credit card details but also information like birth dates, social security numbers, and mobile device PINs.

We recaptured more than **10.58 million mobile records** siphoned by malware between August and December of 2023. While financial fraud is a major motive behind mobile malware attacks, a successful attack can also lead to sensitive data compromise, disruption of operations, and reputational damage. Yet IT and SOC teams have limited or no visibility into mobile devices and struggle to secure them – leaving a massive gap in exposure.

OTHER EASTER EGGS

The emerging trends we observed in 2023 had a recurring theme: malicious actors are taking full advantage of the expanding digital identity. Targeted data now ranges from financial information to API keys and webhooks.

API keys and webhooks are of particular concern because they enable service provider abuse that unlocks sensitive data. Cybercriminals steal API keys through malware infections and distribute them to other bad actors. Even if an infected device is remediated, the stolen keys can be used for follow-on attacks for as long as they remain active. But SOC teams usually don't know when this data is stolen and consequently cannot undertake proper **post-infection remediation**, like rotating exposed keys.

Other stolen data that speaks to the trend includes:

CRYPTO WALLET DATA

Several infostealers, including Raccoon and RedLine Stealer, have been modified to steal crypto wallet information. New families, like LummaC2, come ready with this capability. These stealers harvest keys from so-called hot wallets, which hold digital cryptocurrency. Many users of cryptocurrency assume their wallets are anonymous, but infostealers put PII and wallet details together in the hands of cybercriminals. With this data available in the criminal underground, the expectation people have of their identities being masked from their transaction history is no longer true.

macOS MALWARE

Concerns about infostealers are no longer limited to Windows. SpyCloud researchers have observed an uptick in macOS infections, especially from Atomic macOS Stealer variants. This infostealer harvests system information, keychain passwords, files, crypto wallet info, and even macOS passwords. SOC teams need to watch these developments closely because personal devices like MacBooks are frequently used at home to access corporate networks and applications.

2FA TOKENS

Organizations have made strides toward hardening their credentials, adding 2FA/MFA as an additional protection layer. So of course malicious actors are adapting and looking for vulnerabilities in these same tools. As noted earlier, newer infostealer families like LummaC2 are already stealing 2FA tokens. Criminals are also adapting to a passwordless future, developing ways to steal passkeys or sidestepping authentication altogether through **session hijacking** and other forms of next-generation account takeover.

STAGE 4

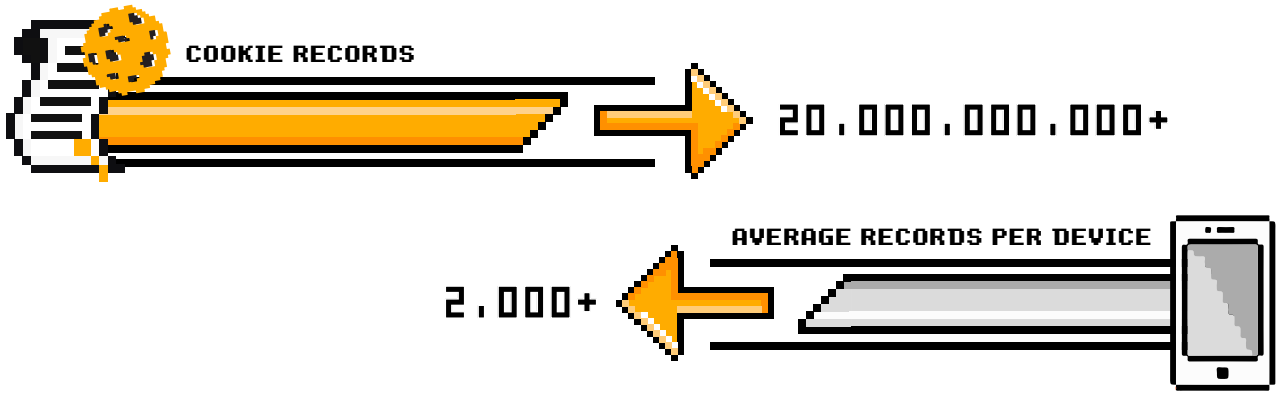
THE VICTORY TOKEN:

STOLEN SESSION COOKIES

BACK

NEXT

All infostealer-siphoned data is immensely valuable due to its high fidelity, but session cookies and tokens stored in a browser are a true bonanza. With a valid cookie in hand, criminals can simply sidestep any authentication mechanism including MFA and hijack a session in an instant.



Last year, SpyCloud recaptured more than **20 billion cookie records**, with an average of more than **2,000 records per infected device**. This indicates that leveraging malware-siphoned session cookies for next-generation account takeover is quickly becoming a valued tactic. As more organizations adopt passwordless authentication, we expect to see this method escalate.

Session hijacking turns cybercriminals into employee clones and gives them unfettered access to sensitive applications and data. Yet many SOC teams don't yet have the tools to remediate this threat. Our **Malware Readiness & Defense Report** shows that 39% of surveyed organizations don't terminate session cookies at the sign of exposure – and 27% don't routinely review logs for signs of compromise.

Consumers are equally at risk because session hijacking enables bad actors to make fraudulent purchases, open new credit lines, and drain loyalty accounts.

STAGE 5

GOTTA RECAPTURE 'EM ALL:

NOTABLE DATA BREACHES

BACK NEXT

Plenty of high-profile data breaches make the news every year. But there are thousands of other large breaches that no one hears about – no one outside of a select group of criminals, that is.

These breaches are first shared only in small, private criminal channels for fast, high-return monetization before they're offered to a broader darknet audience. SpyCloud recaptures this data as quickly as possible; we ingest it into our data daily as a "sensitive source" until the breached organization reports it publicly.

Here are some of the data leaks that caught our attention circulating on the darknet last year:

WHATSAPP | 364,664,942 RECORDS LEAKED

Data allegedly belonging to messaging platform WhatsApp, owned by Meta, was leaked online at an unknown date. The data contained phone numbers and other personal information. This leak was being privately shared on a messaging platform.

TWITTER (NOW X) | 203,873,329 RECORDS LEAKED

In January 2023, scraped user data belonging to the social media company Twitter (now X), was leaked on a hacking forum. The data contained email addresses, full names, screen names, and other personal information. Some of the scraped data was made available in the forum for free. The threat actor responsible for collecting the data reportedly manipulated a bug in an exposed Twitter API to scrape the records. The API vulnerability existed between June 2021 and January 2022, allegedly allowing other intrusions.

LUXOTTICA | 203,570,178 RECORDS LEAKED

Data allegedly belonging to Italian eyewear conglomerate company Luxottica was leaked at an unknown date. The leak, which contained names, email addresses, phone numbers, addresses, and other personal information, was being publicly shared in online forums. The company later confirmed that it suffered a data breach in 2021 and blamed it on a third-party incident. The breach impacted 70 million customers.

UNIONPAY CHINA | 127,873,081 RECORDS LEAKED

Data allegedly belonging to UnionPay, a Chinese state-backed financial services corporation headquartered in Shanghai, was leaked in April 2023. The data contained names, email addresses, phone numbers, addresses, national identification numbers, credit card information, and other personal information. This leak was being privately shared online.

EYE4FRAUD | 74,397,057 RECORDS LEAKED

PII data of U.S. mobile phone users was leaked at an unknown date. The source of the leak was allegedly a 2020 hack of Eye4Fraud, which offers fraud protection for ecommerce merchants. The data contained phone numbers, full names, physical addresses, email addresses, and other personal information. The leak was being shared publicly on online forums.

US PII | 248,259,727 RECORDS LEAKED

PII data allegedly belonging to U.S. residents was leaked online at an unknown date. The data contained names, addresses, geolocations, and other personal information. This source of the leak – which was being shared privately in underground criminal communities – was not known.

MOAB | MORE THAN 26 BILLION RECORDS LEAKED

A massive data leak dubbed MOAB (which stands for "the Mother Of All Breaches") was reported by security researchers in early 2024. The leak included 12 terabytes of data such as credentials from thousands of "meticulously compiled and reindexed leaks, breaches, and privately sold databases" over the years, as well as some new data. SpyCloud's analysis found that **94% of the data was already in our repository**, but approximately 1.6 billion records were new, meaning they were previously either released in sample format only or had not been released publicly.[4]

[4] Our Responsible Disclosure team regularly engages with organizations identified in breaches to ensure they have access to the raw data and can remediate any potential user or employee exposure due to the release of the information.

STAGE 5

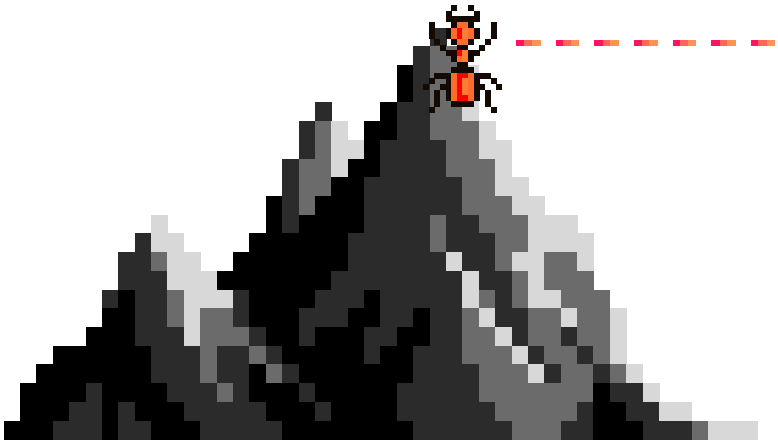
TURNING THE GAME IN YOUR FAVOR

AND AGAINST CYBERCRIMINALS

IT'S DANGEROUS TO GO ALONE!
TAKE SPYCLOUD.

BACK

NEXT



2023 was a pinnacle year for malware, particularly infostealer malware, as well as other tactics, techniques, and procedures (TTPs) that cast an increasingly broad net to steal identity-related data. With malware logs and robust stolen datasets now abundant commodities, security teams should brace for ongoing and relentless attacks on digital identities. And as cybercriminals innovate, digital identity exposure will surge further.

THE STAKES ARE HIGH: WHAT'S NEXT

The corresponding rise in cybercrime, from account takeover and online fraud to session hijacking and ransomware, means we have to start thinking about next-generation approaches if we hope to keep pace – let alone outpace – cybercriminals.

Today, protecting your organization against attacks that stem from exposed identity data means shifting from a device-centric focus to an identity-centric approach. Security teams need quick and accurate evidence when any component of an employee, contractor, vendor, or customer's identity is compromised. With early access to recaptured darknet data, teams can negate the value of stolen information by quickly identifying their riskiest users and acting quickly to protect them.

SpyCloud recaptures data at breakneck pace to power automated prevention solutions that transfer the power back to organizations. Lower your exposure risk and protect your employee and customer digital identities with the power of SpyCloud.

To learn more about how SpyCloud solutions level the playing field against cybercriminals and to check your company's darknet exposure, visit: SPYCLOUD.COM

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.