SpyCloud

ANNUAL IDENTITY EXPOSURE REPORT 2023

TABLE OF CONTENTS

IN 2022:

SpyCloud

19,921,715 records
average breach size

721 MILLION
TOTAL EXPOSED CREDENTIALS

TOTAL BREACH SOURCES
1,316

8.6 BILLION
total PII recaptured

72%
of users in 2022 breaches were reusing previously exposed passwords

GOVERNMENT

391,343
credentials

61%
US & INTL password reuse rate

!

123456
#1 reused plaintext password

MALWARE

22.3 MILLION
unique infected machines

22 BILLION
device and session cookies

1.8 BILLION
phone numbers

1.4 BILLION
full names

802 MILLION
addresses

753 MILLION
social media handles

416 MILLION
dates of birth

332 MILLION
international IDs / full SSNs

67 MILLION
credit card #s

36.5 MILLION
drivers licenses / passport #s

2.5 MILLION
bank account #s

PASSWORD TRENDS

123456
TOP PLAINTEXT PASSWORD

7 MILLION
LOVE/FAMILY THEME

261,496
STREAMING & TV SERVICES

238,597
TRENDING MUSICAL ARTISTS

OVERVIEW

For the last six years, SpyCloud has examined the trends related to identity exposure in the criminal underground to understand how this data puts organizations and consumers at risk of cybercrime including ransomware attacks, data breaches, account takeovers, and online fraud. Every year, SpyCloud's researchers analyze the data they've recaptured during the last 12 months from the deepest layers of the darknet and explore the implications of these findings. Our annual Identity Exposure Report is the result of our research into these trends.

In 2022, we observed that malicious actors are increasingly relying on the high quality and quantity of data exfiltrated straight from user devices by malware. **Nearly half of the data we recaptured came from botnets, which are commonly used to deploy information-stealing malware.**

This is a dangerous trend because botnet data is highly accurate and very effective in enabling cybercriminals to impersonate an individual online – using exposed identity elements to perpetrate a broad range of cybercrimes. Yet most consumers and organizations are unaware of the breadth of their exposed data that is readily available to cybercriminals.

Digital identities have become embedded in everyone's professional and personal lives, and securing these identities is increasingly difficult. The growing number of exposed identities offers bad actors ample opportunities to monetize the data in new ways. Losses from cybercrime to all industries in the US alone are estimated to be as high as **4.1%** of the total gross domestic product. As long as tactics like siphoning identity data from infostealer malware yield a high rate of return for cybercriminals, the losses to enterprises will continue to mount.

Because SpyCloud recaptures data months and sometimes years earlier in the attack lifecycle than what may be publicly reported, along with freshly harvested authentication data from malware-infected devices, we can provide unique insights into how these shifts impact organizations – and help them secure their employee and customer accounts before the exposed digital identities are used to cause harm.

ABOUT SPYCLOUD'S DATA

SpyCloud's proprietary Cybercrime Analytics™ engine collects, curates, enriches, and analyzes recaptured data from breaches, malware victims' devices, and other sources in the criminal underground – transforming it into action with automated solutions that enable enterprises to quickly identify legitimate users vs. potential criminals using stolen information, and proactively prevent account takeover, ransomware, and online fraud.

For the purposes of this report, it is important to understand 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. SpyCloud recaptures this data from darknet sources and notifies businesses when their employees' or consumers' email addresses, usernames, passwords, and PII is found.

What we call malware victim data is information exfiltrated from infostealer-infected devices – typically usernames and passwords, device and session cookies, autofill data, cryptocurrency wallets, and device and system details that can be used to impersonate victims.

TOP 2022 TRENDS

TREND 1

Growing Credential Exposure Due to Malware Infections

Credentials continue to play a leading role in cybersecurity incidents, with the **Verizon 2022 Data Breach Investigations Report** calling them out as one of the “four key paths to your real estate” – responsible for 45% of non-error, non-misuse breaches. While this story has been familiar for some time, there is an alarming shift in the exposed credentials trend. Threat actors are moving away from traditional account takeover (for example, tactics like using credential pairs from combo lists for credential stuffing attacks). Instead, they are more commonly gaining entry with other forms of authentication data stolen directly from user devices and browsers infected with infostealers, malware designed to stealthily siphon data.

Massive data breaches or dark web leaks that result in millions of exposed passwords always raise the alarm, and rightfully so, but what many people don’t realize is that exposed passwords are just as likely to come from malware-infected devices.

In 2022, we recovered **721.5 million** exposed credentials from the criminal underground from a total of **1,316 sources**. Of those credentials, **349.6 million** – **48.5%** – came from botnet logs.

While robot networks or “botnets” in the past were employed largely to launch distributed denial-of-service attacks, today they are commonly used for deploying infostealer-specific malware at a larger scale. Infecting machines to siphon credentials, browser session cookies, and other data that can be used to impersonate a user identity is now a prevalent tactic. It’s simply a matter of economics because stealing information is almost always about financial gain and the return on investment (ROI) from infostealer-siphoned data is much greater than it is from old data that has been circulated around the dark web for months or years.

Infostealers are relatively cheap for criminal actors to buy – as low as $200-$300 – and easy to deploy. Many are designed to not only avoid detection by anti-malware solutions, but also leave no trace of infection. This "dissolvable malware" means security teams may have no knowledge of an infection having occurred and cannot take proper remediation steps.

But what makes infostealers especially attractive for cybercriminals – and boosts their ROI – is their success rate and effectiveness. The siphoned credentials are accurate and valid since they are fresh, while the stolen session cookies and tokens allow threat actors to bypass multi-factor authentication (MFA) so they can assume the user identity without any friction – sometimes long after the initial infection takes place – making the stolen data far more harmful as it can lead to additional attacks.

Endpoint security products have detected ever-increasing levels of malware attempts, with more than **4 billion** observed last year. As the associated data exfiltrated by infostealer malware becomes more ubiquitous, the follow-on path into organizations is much easier for actors to access. And the growing popularity of malware-as-a-service models means that data siphoned in this manner will continue to grow in abundance.

> What makes this trend even more troublesome is that password reuse rates remain high. Our data shows a nearly **72% reuse rate** for users exposed in two or more breaches in the last year, an **8-point jump from 64%** in the previous year's report.

Despite enterprises' attempts to enhance user awareness training programs, the message about password hygiene to bolster security and cybersecurity awareness to thwart cyber attacks has yet to impact password use, as can be seen in recaptured breach data. The combination of continued high password reuse rates and malware-infected devices leads to a much higher risk of identity exposure for consumers and organizations, and continues to be top of mind at all levels of organizations concerned about the impact these exposures cause for potential follow-on attacks like ransomware. Adding insult to injury, the risk for enterprises continues to increase significantly when an employee's session cookies are siphoned by malware, giving cybercriminals the ability to log into corporate applications, bypassing MFA, and negating the need for passwords in the first place.

721.5+ MILLION
EXPOSED CREDENTIALS

1,316
SOURCES

349.6 MILLION
FROM BOTNET LOGS

72%
PASSWORD REUSE RATE

The Short Route from Infostealer to Ransomware Attack

Ransomware has been the “new normal” for organizations for the last few years, with the cost of remediation alone averaging **$1.4 million**. But in 2022, ransomware had a banner year, **outranking** traditional data breaches as the top cyber exposure concern globally.

SpyCloud’s 2022 Ransomware Defense Report uncovered a significant decrease in the number of organizations that *haven’t* been hit by ransomware in the past 12 months and a significant increase in the number of those that experienced multiple attacks. The report found, for instance, that 50% of organizations were hit with ransomware two to five times in the past year, compared to 34% the year before.

The flourishing underground economy drives the proliferation of ransomware attacks because it enables a breadth of specialists to monetize their services and cater to “customers” like ransomware gangs. Ransomware operators outsource initial access to a specialized group commonly referred to as initial access brokers (IABs). These brokers’ sole job is to provide verified access into a network, and malware logs are extremely valuable for this purpose because they contain accurate authentication data for impersonating an employee.

The malware infection logs SpyCloud researchers observe are the same infections that IABs package to deliver access to ransomware syndicates. One popular market by itself had **4.5 million** logs available for sale in October 2022, a 40% increase from July. While infostealers like **RedLine Stealer** dominated the market, there was an upsurge in advertisements for new or enhanced variants.

The broker-operator partnership is lucrative for both sides. The “anything-as-a-service” model of the criminal underground makes it easy – and cheap – for IABs to buy an email list and infostealer malware, spin up a control-and-command domain, and launch a phishing campaign that infects thousands of devices and exfiltrates a fresh crop of credentials.

From the ransomware operators’ perspective, why go through the trouble of targeting someone, gaining access, and escalating privileges when they can just pay another actor a small sum for current, accurate data that greatly improves their degree of success?

SEE HOW A MALWARE-INFECTED DEVICE CAN OPEN THE DOOR FOR CYBERCRIMINALS TO PERPETRATE RANSOMWARE IN OUR POST-INFECTION REMEDIATION GUIDE

Government Sector Remains at High Risk

The commercial sector doesn't have the undivided attention of cybercriminals. Research suggests that the number of cybersecurity incidents within government organizations grew by **95%** globally in 2022, with China, India, and the US the most targeted nations.

To learn how government agencies fared in breaches last year, we analyze our recaptured data for emails associated with government domains. **We uncovered 695 breaches containing .gov emails in 2022, a nearly 14% increase from 611 in 2021.**

The government sector is at even higher risk from malware-infected devices than enterprises. SpyCloud data shows that **74% of exposed government credentials across the globe in 2022 were exfiltrated by malware** (compared to 48.5% across the board). However, both private and public sectors have to combat third-party risk. We found **24,000 malware infections among just a sample of defense contractors**, with exposures including plaintext passwords and admin credentials.

Government employees also show the same poor hygiene habits as their peers in the private sector. **Password reuse by government employees remains high – 61% of users with more than one password exposed in the last year were guilty of reusing passwords across multiple accounts**. This is consistent with the reuse rate we showed in the previous year's report. The list of the most common exposed passwords associated with government emails is also a cause for concern: the top three are 123456, 12345678, and password.

The Year In Pop Culture Passwords

Commonly used passwords give us a glimpse into pop culture trends. So every year, we take a look at which of the year's burning topics make it into our list of the top recaptured passwords.

Considering that many people are obsessed with music and celebrities, we are never surprised to see some of the year's hottest artists on the list. In 2022, two artists who dominated our collective fascination were Taylor Swift and Bad Bunny, climbing to the top of music charts – and our exposed password list. Swift had a blockbuster end to the year with the release of her 10th album, "Midnights," which reportedly generated **$230 million** in sales by the end of 2022, thus resulting in passwords using taylor/taylor swift/swiftie/midnights (186,000). Not to be outdone, Bad Bunny was Spotify's **most-streamed** artist in 2022, inspiring the passwords bad bunny/titi/verano – the latter two among his popular songs (141,000).

Various other pop culture topics equally reflected some of the year's most talked-about events:

- The growing popularity of streaming TV services (youtube/netflix/hulu) | **261,000**
- The death of Britain's Queen Elizabeth (queen/queen elizabeth/royal family) | **167,000**
- Elon Musk's Twitter acquisition (twitter/elon musk) | **74,000**
- The second coming of Bennifer – Jennifer Lopez and Ben Affleck finally tying the knot (jennifer lopez/jlo/ben affleck/bennifer) | **46,000**

As expected, top recaptured popular passwords also included russia/russian war, ukraine/ukraine war, and trump – but what really gave us the warm fuzzies (and nevertheless still dangerous to use) was love/family/kids/wife/husband/boyfriend showing up collectively more than 7 million times.

TREND 3

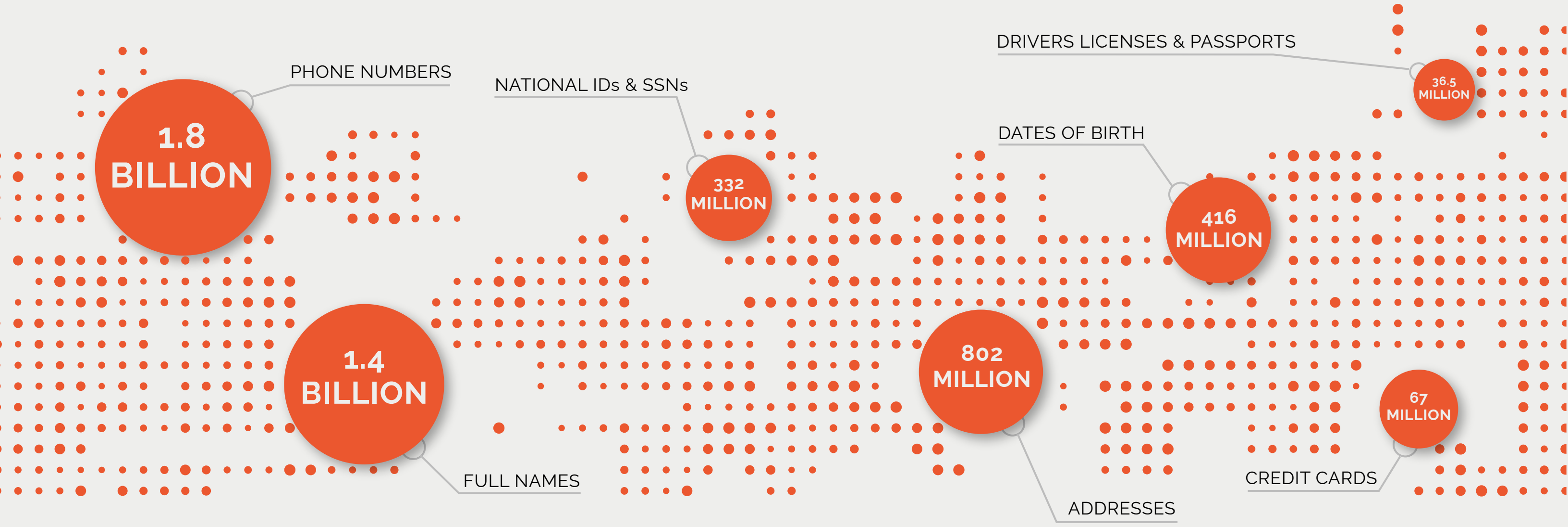
Vast PII Exposure Helps Criminals Innovate

A 2022 global consumer survey by Experian found that **58%** of respondents either have been a victim of identity fraud or knew someone who was, while 53% said the same about account takeover, and 58% about online fraud. In recent years, synthetic identity fraud – where criminals mix together stolen and fake identity data from multiple consumers – has become the **largest form** of identity theft.

Stolen PII fuels these trends, especially as consumers increasingly rely on their digital identities for everyday transactions. **In 2022, SpyCloud recaptured 8.6 billion PII assets, bringing the total in our database to 60 billion.**

The types of data we recapture is very broad, including fields like name, address, employer name, estimated income, language, political affiliation, and number of children.

The categories with some of the largest number of assets recaptured last year included:



All these are data points that fraudsters use to create synthetic identities. These constructed identities can be used in a number of ways: to open new accounts, make large purchases, apply for credit, and – ironically – even to **get hired** for jobs that have access to sensitive data.

The abundance of PII on the criminal underground enables fraudsters to find new, creative ways of monetizing the stolen data. One group, for example, used synthetic identities to defraud financial institutions to the tune of **$1 million** by borrowing large sums they weren't planning to pay back, and to defraud the US government of nearly $1 million with fake applications for the Paycheck Protection Program. Unfortunately, synthetic identity fraud remains one of the hardest types of fraud to detect for organizations, whether in the private or public sector.

SPOTLIGHT ON MALWARE:
HOW INFECTIONS CREATE IDENTITY EXPOSURE

As previously outlined, infostealers have become a pervasive tactic because they are easy to deploy and yield accurate, valid data. Infostealer logs are growing abundant on the criminal underground, giving extremely valuable data access to a new wave of cybercriminals.

As one example, our researchers uncovered a stolen dataset last May with 11.2 million records containing 135.2 million assets in a database of logs exfiltrated by Raccoon Stealer malware. First detected in April 2019, this infostealer quickly rose in popularity for procuring credit card information, passwords, and cryptocurrency wallets. The payload is generally deployed via exploit kits, phishing, and compromised software downloads. Raccoon is typically sold to criminals as malware-as-a-service for as little as **$75** a week for an entry-level subscription.

It is worth noting that although the US government shut down Raccoon operations last March, the group behind it reemerged in June, advertising a new and improved version, Raccoon 2.0 – a testament to the **criminal operators' resilience**. The new version quickly gained steam: between July and October, the use of Raccoon grew from **11% to 22%**, based on log advertisements observed by some researchers.

Along with our observations of Raccoon and RedLine Stealer contributing to great volume in our recaptured data plus continuing to take a lot of media attention with their attacks and impacts, it's interesting to note that many other publicly unnamed infostealers were also highly represented in last year's data to the tune of 47.5 million records.

A sampling of what infostealer logs typically contain:

BROWSER DATA

Stored session cookies and credentials (including usernames, passwords, and associated URLs), as well as browser autofill and form-fill data.

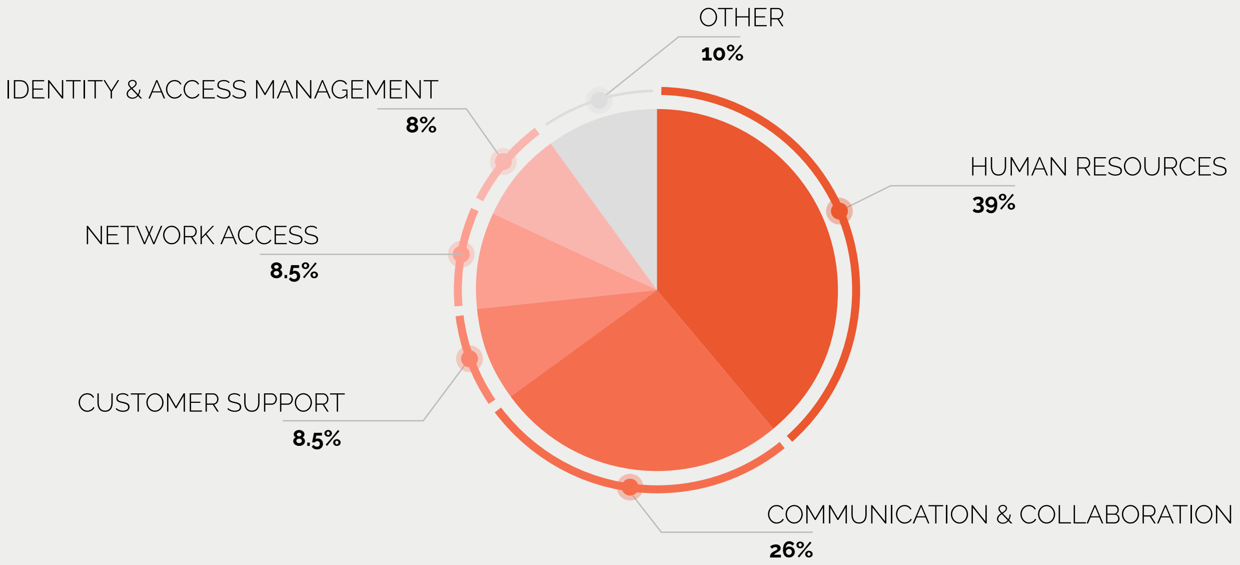
DEVICE/SYSTEM DATA

Hardware, installed software, IP address, running processes, location data, and screenshots.

All of this is data that allows threat actors to emulate the device "fingerprint" and look completely indistinguishable from the user identity. Since many companies use these fingerprints to confirm identity and detect fraud, cybercriminals can use them nefariously to bypass security checks and enter systems undetected.

Additionally, the malware logs contain credentials and potentially session cookies from every third-party application an employee uses – including subdomains like sso.mycompany.com or mycompany.thirdparty.com and shadow IT applications that fall outside the visibility of traditional monitoring solutions.

Last year, we recovered millions of third-party application credentials harvested by malware. The applications included a range of popular business tools. The top five most common categories were:



One of the groups known for using infostealers to obtain credentials and session cookies is **Lapsus$**, which was blamed for several **high-profile attacks** on technology companies early last year. Lapsus$ used **RedLine Stealer**, a popular infostealer that first appeared underground in 2020.

While some infostealers are designed to remove themselves after execution, others create persistent access. That means bad actors have access to the current data for as long as the device remains infected, even if the user changes passwords. The underground marketplace **Genesis** even advertises its commitment to keep the stolen data and the compromised systems' fingerprints up to date. According to our research, Genesis Market had more than 430,000 stolen identities for sale as of early last year – and there are many other marketplaces like this one.

Session Cookies: The Ultimate Steal

Any authentication data siphoned by malware gives cybercriminals the upper hand, but they hit the jackpot with session cookies. Stored in a browser, session cookies authenticate a user on a website for a period of time. Cybercriminals import the stolen cookies into readily available anti-detect browsers to hijack a session – often bypassing MFA and taking over an account without the need for credentials.

In total, we recaptured nearly 22 billion device and session cookie records last year. **Session hijacking** essentially turns bad actors into employee clones, giving them access to sensitive information and the opportunity to escalate privileges and carry out their objectives. Consumers are also at high risk because stolen cookies allow criminal actors to perpetrate fraud by draining accounts and loyalty points, making fraudulent purchases, and opening new credit.

Cookies are a perfect example of criminals focusing on the quality of data being stolen rather than their previous mindset that more is more.

Password Managers Not Foolproof

The exfiltrated malware data we recaptured included a total of 117,657 master passwords from eight password managers, most of them considered top of the market. Each of those passwords can be used to decrypt an individual's entire password vault, providing immediate access to not only all the accounts but any other sensitive data the person stores in the password manager – this can be anything from mailing address and payment data to passport number and MFA recovery codes. Pair this data with the session cookies contained in the same malware logs, and the tremendous risk to individuals and businesses is undeniable.

While using password managers and MFA should remain a best practice, these tools are not infallible. Especially since threat actors appear to have sights on these tools, if the recent wave of **MFA bypass attacks** is any indication.

TOP NOTABLE DATA BREACHES OF 2022

While plenty of data breaches make the headlines every year, thousands more are likely perpetrated, kept in small, private circles of criminals focused on monetizing the information before selling it to a broader audience on the darknet. SpyCloud recaptures data as quickly as possible after the breach occurs, ingesting the data as a "Sensitive Source" until it is reported publicly by the victim organization.

Last year, we especially noted many geopolitical-related incidents of exposed data on the darknet, with both Russian and Ukrainian hackers targeting a gamut of industries including finance and healthcare. Organizations and individuals' data is at risk across the world, no matter the industry and no matter the company size.

Here are some of the most notable breaches that were being shared on the darknet in 2022:

SERASA EXPERIAN, BRAZIL

223,739,215

records leaked

A database of Brazilian citizens' PII originally offered on the darknet in early 2021 was being privately shared on the internet again in February 2022. The data included names, national IDs, vehicle information, and other personal information. The database was advertised as "**Serasa Experian**" and reports speculated that the PII was stolen from Serasa, a Brazilian subsidiary of Experian. However, **Experian said** the data was not stolen from Serasa and there was no evidence of compromised systems.

UKRAINIAN VOTERS

32,310,705

records leaked

Data belonging to Ukrainian voters was leaked in September, with names, addresses, and additional personal information from 2019 voting records.

PRIVATBANK

26,835,098

records leaked

Data belonging to the Ukrainian financial company PrivatBank was leaked on a Telegram channel in September. The data contained names, email addresses, phone numbers, passport numbers, usernames, and other personal information.

RUSSIAN FEDERATION DATABASES

24,911,323

records leaked

A collection of compromised databases pertaining to the Russian Federation was allegedly shared on a hacking forum. The data contained passwords, email addresses, IPs, usernames, and other personal information.

GEMOTEST

24,248,936

records leaked

Data from the Russian medical testing provider Gemotest was published privately on the internet in September. The data contained email addresses and other personal information.

INDIHOME

12,619,882

records leaked

User data including email addresses and other personal information was allegedly leaked from the state-owned Indonesian internet service IndiHome in August. Although the leak was being shared privately on the internet, **government officials stated** there was no breach of customer data.

ADECCO

12,235,521

records leaked

User data from Swiss-based Adecco, the second-largest global provider of human resources and temporary staffing, was published on an underground forum. The information included email addresses, passwords, social security numbers, dates of birth, and other personal data.

STATSNET

11,517,982

records leaked

The Kazakh contractor screening portal Statsnet was allegedly breached at an unknown date. The breach was being shared privately on the internet and contains email addresses and additional personal information.

TELCEL

9,709,331

records leaked

Data belonging to the Mexican communications company Telcel was leaked online and was being shared privately on the internet. The data contains emails, addresses, and additional personal information.

TURKISH CITIZENS DATA

8,340,970

records leaked

Data of Turkish citizens including names, addresses, phone numbers, and other personal information was leaked on a hacking forum in October. The source of the leak was unknown.

WAKANIM

6,697,064

records leaked

User data of the European subscription-based streaming service Wakanim was leaked on a hacking forum in August. The leak included sensitive information like names, email addresses, usernames, and phone numbers.

One final note regarding the notable breaches of 2022: some of these criminally traded or sold databases date back to more than five years since their initial exposure. As we stated previously about password reuse, the slow burn of "old" data can still cause quite the headache for security teams and users if not actioned on quickly.

TAKING ACTION ON STOLEN DATA

Malware poses a daunting threat to organizations, as evidenced by our recapture of 22 billion cookies and 48.5% of credentials exfiltrated from infected devices last year.

For the typical security operations team, malware infection response entails identifying an infected device, isolating it from the network, and reimaging it. This creates a false sense of security because while it cuts off the cybercriminal from the device itself, it does not address the risk that comes from the already- stolen cookies, credentials, and other sensitive data. Once the employee device is infected with an infostealer, it only takes seconds to exfiltrate this data straight from the endpoint, yet the risk to the organization remains for a very long time.

Malware infections often occur outside an enterprise's traditional perimeter, creating an overwhelming challenge for security teams: you can't protect what you can't see. And even for teams that have heightened visibility, the response typically focuses on the device itself, despite most critical systems and applications being accessed via the cloud with credentials. Better protection for the enterprise and the user requires the ability to see what data was actually stolen and then prioritizing and remediating the most critical exposures. If you remove criminals' largest source of targeting information – exposed employee data – you can stop attacks before they happen.

To reduce the risks associated with ransomware that results from malware infections and exfiltrated data, security teams can take proactive steps to reduce the exposure of employee and third-party identities. This includes empowering employees to be aware of their own cyber practices and the impact they have on the business, as well as addressing any data that is already stolen. Additionally, security teams should also incorporate robust **Post-Infection Remediation** – a framework of additional steps to existing incident response protocols, designed to negate opportunities for ransomware and other critical threats by resetting the application credentials and invalidating session cookies siphoned by infostealer malware. This optimized remediation that includes recaptured exfiltrated data enables the SOC to seamlessly and comprehensively disrupt cybercriminals before they can act on the stolen data and neutralize the risk of ransomware from these exposures. However, until post-infection remediation is broadly adopted, remediation steps will continue to offer incomplete protection from further compromise.

PROTECTING YOUR ORGANIZATION AGAINST IDENTITY EXPOSURE

Last year, global malware volume reached a **fever pitch**, and SpyCloud's own findings indicate that the risk of identity exposure from malware-infected devices is growing. With almost half of our recaptured data coming from infected devices, it is clear that organizations can no longer afford mitigation strategies that only go part of the way.

BYOD, unmanaged and under-managed devices, and exposed third-party applications create blind spots for your security team. So does the lack of knowledge about identity data circulating on the darknet. The best way to protect users from themselves is by leveraging the data criminals know about your business and your consumers from data breaches and malware infections to turn the tables and prevent cybercrime such as account takeover, online fraud, and ransomware.

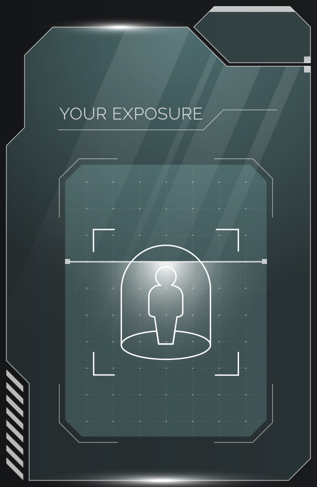
Using recaptured data from the darknet adds an advanced layer of protection that helps you understand your riskiest users. Solutions powered by this data allow enterprises to quickly identify and take action on exposed credentials, web session cookies, and PII – preventing exposures from progressing to full-blown security incidents and better assessing users to minimize and prevent online fraud. Adding this layer of defense allows you to close the gaps in your existing security frameworks to protect employees, customers, your brand, and your bottom line.

By gaining a comprehensive understanding of the full scope of your organization's exposure, you will be in a much better position to fully remediate the risks.

WHAT'S NEXT

Our researchers' ongoing observations of activities in the criminal underground, along with our 2022 findings, indicate that bad actors are just hitting their stride when it comes to leveraging infostealers. As the "anything-as-a-service" underground economy continues to offer high quality and quantity of malware-siphoned data, we expect to see many more organized gangs and small-time actors alike taking advantage of this abundance of identity data to threaten both individuals and businesses.

The key to disrupting criminals' ability to profit from stolen data is to understand what bad actors know about your organization and customers – and use these insights to respond accordingly. SpyCloud uses the same data criminals have in hand to power our automated prevention solutions, giving power back to the enterprise and leveling the playing field against cybercriminals. Only SpyCloud provides actionable analytics based on the world's largest collection of recaptured data, enabling enterprises to quickly identify and protect vulnerable users.



CHECK YOUR DARKNET EXPOSURE TODAY

and reveal details about your company, customer, and personal risk.

Knowing what's out there is the first step to protecting yourself and your organization from identity exposure that can lead to account takeover, ransomware, and online fraud.

CHECK YOUR EXPOSURE

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, protect their business from consumer fraud losses, 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 nearly 200 cybersecurity experts whose mission is to make the internet a safer place.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.