SpyCloud

LONDON'S FTSE 100

(AND THEIR SUBSIDIARIES)

IDENTITY EXPOSURE REPORT

2023

SpyCloud

TABLE OF CONTENTS

OVERVIEW

Digital identities are now embedded in employees' lives, and protecting these identities has become more urgent for organisations. Yet doing so is increasingly difficult because the exposure of these identities creates a vicious cycle – as the number of exposures soars, the data available on the criminal underground becomes more plentiful, allowing malicious actors to find new ways to monetise it, which, in turn, can lead to more exposed identities. Despite hefty investments in cyber defenses and anti-fraud measures, organisations often find themselves at the losing end of the battle. To understand how exposed employee identities – and the changing trends – impact organisations, SpyCloud combs through our entire database of assets recaptured from the criminal underground each year and analyses the dark web exposure of employees of the top 100 FTSE companies and their subsidiaries.

For years, stolen credentials have been a favorite tool for cybercriminals looking for ways to infiltrate organisations and perpetrate fraud and other crimes. More recently, however, SpyCloud researchers have noted a shift in tactics: bad actors prefer to use credentials and other authentication data stolen by malware rather than relying on "traditional" breach databases and combo lists. Malware-exfiltrated data is incredibly fresh and accurate, increasing the attackers' return on investment and the follow-on attack success rate. And with more of this high-quality data available in abundance on the criminal underground, this tactic has grown prevalent.

In response to this shift, the trends observed by SpyCloud researchers in this year's annual FTSE 100 and their subsidiaries' Identity Exposure Report have evolved as well – in our fourth year for this report, we take a closer look at malware infections and how they affect identity exposure. For this year's analysis, we looked at more than **52.25 million breach and 55.41 million malware-exfiltrated cookie records** in our database that are tied directly to FTSE 100 and subsidiaries' employee accounts recaptured from the criminal underground.

To perform our analysis, we searched for records containing FTSE 100 and subsidiary corporate email domains, excluding "freemail" domains that are available to consumers. For example, if a FTSE 100 employee signed up for a breached third-party site using their corporate email address, such as jonsmith@acme.com, we were able to associate the resulting breach record to their employer.

ABOUT SPYCLOUD'S DATA

SpyCloud's proprietary Cybercrime Analytics Engine collects, curates, enriches, and analyses recaptured data from breaches, malware victims' devices, and other sources in the criminal underground – transforming raw data into action with automated solutions that enable organisations 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 unauthorised 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 are identified through our analysis as exposed, requiring remediation on stolen passwords or extra scrutiny on suspicious transactions.

What we call malware victim data is information exfiltrated from infostealer-infected devices – typically usernames and passwords, device and session cookies, autofill data, cryptocurrency addresses, and device and system details that can be used to impersonate victims via account takeover, session hijacking, or social engineering.

KEY FINDINGS

1. Password reuse rates are prevalent, with the electricity sector as the worst offender.

Password reuse remains rampant among FTSE 100 and their subsidiaries' employees. We found a **65% password reuse rate** among FTSE 100 and subsidiaries' email addresses in our database that have been exposed in more than one breach. Things are getting worse rather than improving – the password reuse rate was 64% in the previous year. Unfortunately, we see this trend at FTSE companies and their subsidiaries every year, indicating that all the user education and training continues to fall on deaf ears of the employees. The industry that is far ahead in this category is electricity (80%), with banks not too far behind (76%). Industrial engineering, food and drug retailers, and retail hospitality are tied in third place (75%).

2. Despite the rise in malware, exposure from data breaches continues to affect every sector, especially industrial support services.

Last year, every sector had exposures included in either a data breach or malware infection and potentially both. Exclusive of malware-exfiltrated data, we recaptured **nearly 10.2 million breach records** associated with FTSE 100 and subsidiary employees. For breach records alone, the banks sector has the highest number of exposed records (1.86 million) and exposed assets (9.58 million). The other sectors in the top five spots for breach records are telecommunications services (1.11 million), media (996,445), pharmaceutical and biotechnology (835,854), and oil, gas, and coal (713,975). The same sectors also follow banks with the highest number of exposed assets, but in a slightly different order: media (5.64 million); telecommunications (4.88 million), pharmaceuticals and biotechnology (4.11 million), and oil, gas, and coal (3.63 million).

3

3. PII exposure maintains steady climb, with the banks sector once again in the lead.

Two themes recurring from the previous year gave us pause for concern: the number of exposed PII assets continues to grow, and the banks sector has the most PII exposure. We recaptured nearly **28.35 million PII assets** (compared to 27.56 million the year before), putting organisations at risk by arming cybercriminals with data to use in social engineering, phishing schemes, and the development of synthetic identities to perpetrate fraud. Of those PII assets, 5.21 million – 18% – came from the banks industry. Synthetic identity fraud (the mixing of stolen and fake identity data from multiple consumers) has become **the largest form** of identity theft in recent years, and the massive amount of consumer PII available on the criminal underground makes it far too easy for fraudsters to create synthetic identities to open new accounts, apply for credit, and perpetrate other financial fraud. Which is why it's especially alarming to see the banks sector at the top in this category.

4

4. Malware tactics are prevalent, and session cookies are the ultimate malware-exfiltrated steal.

With a total of **675,327 malware-infected employees and consumers across all FTSE sectors**, exposure stemming from this insidious tactic is rampant. Infostealers – malware designed specifically for stealing all manner of personal, authentication, and system data – have been growing in popularity, and many marketplaces now cater to malicious actors like initial access brokers (IABs), who use infostealers to deliver access to ransomware operators. Increasingly, these marketplaces offer botnet logs, which contain malware-exfiltrated data ranging from credentials and PII to browser session cookies. To put this into perspective: of the total breach assets we recaptured across the entire SpyCloud database last year, 58.6% came from botnet logs. Specifically, we also recovered **55.41 million session cookie records** associated with FTSE 100 companies and subsidiaries – which are the most prized type of malware data because of its high accuracy. With browser session cookies in hand, bad actors can become an identity's clone and bypass authentication to seamlessly hijack a session, allowing them to gain unfettered access to an organisation's network, access sensitive data, perpetrate fraud, and launch hamrful cyberattacks including ransomware and more. While cybercriminals' mindset in the past may have been "more is more" in terms of stolen data, this is no longer the case with session cookies – this data is of such high quality that they are practically guaranteed success. Among the FTSE sectors, the lion's share of session cookies we recovered – 70% – came from industrial support services (38.55 million), followed by media (5.7 million), travel and leisure (4.1 million), retailers (1.79 million), and food and drug retailers (1.01 million).

5. Banking sector has the most severe exposure, with telecommunications and media not far behind.

Each of these three industries stood out in its own way, but they had one thing in common: they are far ahead of others in terms of exposure, with wide-reaching implications. As mentioned in the above findings, the banks sector has the most breach records (1.86 million), the most exposed third-party breach assets (9.58 million), the most PII records (5.21 million), and the second-highest password reuse rate (76%, or 4 points higher than the 72% reuse rate across our **entire database**), but that's just for starters. The banks sector also has the highest number of recaptured credentials pairs (634,114), exposed C-level employees (3,127), number of employees reusing passwords (15,073) – and we can go on. But possibly the most alarming is the number of malware-infected consumers (5,633) in this sector, as this is a known gateway for fraud. The kind of sensitive data that consumers entrust to banks impacts not only the individual, but also opens the door for wider fraud opportunities against these banks and financial institutions – and seeing this sector in such poor shape is an eye-opener.

Additionally, regarding malware infections, the telecommunications sector is at the top with 4,284 malware-infected employees. This represents a quarter of all infected employees across all FTSE sectors and is almost double the number in the second-highest sector in this category (media, with 2,167 infected employees). Lastly, media has the highest number of malware-infected consumers by far: 229,267, or 35% of all infected consumers across FTSE companies and their subsidiaries. Similar to the fraud impact in regards to banking's high number of infected consumers, other organisations are at just as high a risk because mitigation costs can be extremely high and reducing impacts to the business while balancing customer experience is still a tightrope for many of them.

SpyCloud

AT-A-GLANCE:
FTSE 100 IDENTITY EXPOSURE

TOTAL BREACH SOURCES

10,726

Total number of breaches in the SpyCloud database that include records tied to FTSE 100 and their subsidiaries' corporate email addresses.

TOTAL CORPORATE BREACH RECORDS

10,183,481

A breach record is the set of data tied to a single user within a given breach. Ex: Information tied to jsmith@acme.com within a set of data stolen in a breach of example.com.

TOTAL BREACH ASSETS

52,250,294

A breach asset is a piece of information contained within a breach record. Ex: a password, an address, a phone number, credit card, session cookie, etc.

TOTAL SESSION COOKIE RECORDS

55,413,207

A session cookie or token is a string of characters that a website or server uses to remember visitors, making it easier to visit the site again without authenticating. Similar to a breach record, a cookie record can contain a set of data tied to a single session or cookie that can be a combination of the cookie's ID, value, expiration, domain, etc. With a valid cookie in hand, cybercriminals can mirror a user and bypass authentication to seamlessly hijack a session, allowing them to access sensitive data, escalate employee privileges, and much more.

TOTAL PLAINTEXT CORPORATE BREACH & MALWARE-EXFILTRATED CREDENTIALS

2,750,855

Total number of FTSE 100 and their subsidiaries' email address and plaintext password pairs that are available to criminals. If employees have reused these passwords, criminals can easily exploit the exposed credential pairs to gain access to corporate systems.

TOTAL C-LEVEL EXECUTIVES EXPOSED

15,345

Exposed corporate credentials that are tied to FTSE 100 and their subsidiaries' executives with high-ranking titles, putting them at increased risk of targeted account takeover and business email compromise (BEC) fraud.

PASSWORD REUSE

65%

Among the FTSE 100, this is the rate at which a password was exposed more than once compared to the total exposed passwords for FTSE 100 and their subsidiaries' employees. This includes exact passwords and slight variations that criminals can easily match.

MALWARE-INFECTED EMPLOYEES

17,181

FTSE 100 employees whose data appears in logs exfiltrated from infostealer malware-infected devices. These high-severity exposures puts them at high risk of ATO and fraud, and makes the enterprise vulnerable to ransomware attacks.

CORPORATE CREDENTIAL EXPOSURE OF THE FTSE 100

Exposed Corporate Credentials

SpyCloud researchers discovered more than **2.75 million pairs of credentials** with FTSE 100 or subsidiary corporate email addresses and plaintext passwords. With 634,114 of those associated with banks, this industry has the highest number of exposed credentials by far. Rounding out the top three are telecommunications service providers (427,502) and oil and gas producers (216,268).

While not every credential pair will match corporate login details, the ones that do match or even have a partial match represent substantial risk for these enterprises – and their customers and partners – with criminals' advanced ability to easily crack passwords.

When credentials are exposed in a data breach, cybercriminals inevitably test them against a variety of other online sites, known as **credential stuffing**, taking over any other accounts protected by the same login information. If those stolen credentials contain a corporate email domain, criminals have an obvious clue that they could provide access to valuable enterprise systems, customer data, and intellectual property. And some of the most valuable are credentials belonging to members of an oranisation's C-suite. Cybercriminals target C-suite executives and other employees with high-ranking titles or high levels of access to attempt account takeover and business email compromise (BEC) fraud. These scams cost enterprises an enormous amount: total BEC losses in 2022 reached **$2.7 billion** from nearly 22,000 complaints.

In our data set, we also found **84,297 records from 15,345 exposed C-level employees**. Fraudsters use this data for phishing and social engineering to take control over an executive's email account, then use that email account to impersonate the executive and compel employees, vendors, or other trusted partners to pay fraudulent invoices, transfer funds illegally, reveal sensitive information, and more. BEC fraud has wide implications, putting at risk everything from sensitive data and intellectual property to a company's financials.

In theory, corporate passwords should be strong given the importance of the assets they protect and the robust guidance often provided by corporate security teams. In practice, many employees use bad password hygiene at work simply out of perceived ease, and some corporate password policies (such as 90-day password rotation) may even encourage bad habits.

FTSE 100 INDUSTRY	TOTAL EXPOSED CORPORATE CREDENTIALS
AEROSPACE & DEFENCE	117,290
ASSET MANAGERS	3,641
BANKS	634,114
BEVERAGES	45,481
CHEMICALS	2,210
CLOSED END INVESTMENTS	1,814
CONSTRUCTION & MATERIALS	5,104
ELECTRICITY	3,568
ELECTRONIC & ELECTRICAL EQUIP.	4,636
EQUITY INVESTMENT INSTRUMENTS	1,578
FINANCIAL SERVICES	29,243
FOOD & DRUG RETAILERS	68,226
FOOD PRODUCERS	9,513
GAS, WATER & MULTI-UTILITIES	28,065
GENERAL INDUSTRIALS	28,979
GENERAL RETAILERS	5,676
HEALTH CARE EQUIP. & SERVICES	17,004
HOUSEHOLD GOODS & HOME CONSTRUCTION	25,747
INDUSTRIAL ENGINEERING	5,062
INDUSTRIAL SUPPORT SERVICES	53,675

FTSE 100 INDUSTRY	TOTAL EXPOSED CORPORATE CREDENTIALS
INDUSTRIAL TRANSPORTATION	4,655
LIFE INSURANCE	48,812
MEDIA	200,079
MEDICAL EQUIP. & SERVICES	3,535
MINING	54,338
NONLIFE INSURANCE	7,241
OIL & GAS PRODUCERS	216,268
OIL, GAS & COAL	167,453
PERSONAL GOODS	158,837
PHARMACEUTICALS & BIOTECHNOLOGY	209,207
PRECIOUS METALS & MINING	698
REAL ESTATE INVESTMENT TRUSTS	3,990
RETAIL HOSPITALITY	471
RETAILERS	11,174
SOFTWARE & COMPUTER SERVICES	27,383
SUPPORT SERVICES	25,921
TELECOMMUNICATIONS SERVICE PROVIDERS	427,502
TOBACCO	42,306
TRAVEL & LEISURE	50,359
TOTAL	2,750,855

Password Reuse

Within our dataset of FTSE 100 and subsidiary corporate breach exposures, we found a **65% password reuse rate** - meaning the same password was found in one or more breaches. This represents an uptick from the previous year's 64% and only a 7-point difference from the password reuse across our entire database (72%). Employees with multiple reused passwords in our dataset may or may not reuse passwords at work; however, password reuse across their third-party breach-exposed accounts does provide an indication of employees' overall password hygiene, which remains a challenge for organisations.

FTSE 100 INDUSTRY	AVERAGE PASSWORD REUSE
ELECTRICITY	80%
BANKS	76%
FOOD & DRUG RETAILERS | RETAIL HOSPITALITY INDUSTRIAL ENGINEERING	75%
FOOD PRODUCERS	73%
MEDIA	71%
AEROSPACE & DEFENCE	70%
ELECTRONIC & ELECTRICAL EQUIPMENT	69%
SUPPORT SERVICES	68%
GENERAL RETAILERS | NONLIFE INSURANCE	67%
GAS, WATER & MULTI-UTILITIES | OIL & GAS PRODUCERS	66%

FAVORITE PASSWORDS OF FTSE 100 EMPLOYEES

With hundreds of accounts to keep track of, it's no wonder people take shortcuts to remember their login credentials. In addition to recycling variations of a few favorites across every account, people often use simple passwords that are easy to remember – and easy for criminals to guess. Criminals often use lists of common passwords in password spraying attacks, putting accounts with weak passwords at risk even if the user hasn't intentionally reused that password.

One of the worst shortcuts employees can take is to include their company's name in their passwords; it's one of the first things criminals will enter into their account checker tools when trying to crack corporate passwords. However, banning the use of the company name in passwords may not be enough. Organisations need to find ways of protecting employees from themselves.

FTSE 100 employees follow the same patterns as a lot of users. Each of the passwords below appeared hundreds or even thousands of times within our dataset. We've redacted company names, which appear frequently. "Password" and "123456" are a perennial favorite both for FTSE 100 and subsidiaries and their Fortune 1000 counterparts – they were the first and second top passwords respectively for FTSE and subsidiary employees, and also the top two for Fortune 1000, just reversed.

While most of these examples would fail to pass basic corporate password policies, people tend to transform a base password in predictable ways to bypass complexity rules. For example, "password" might become "Password1" or "Passw0rd!" at work.

Unfortunately, criminals are well-aware of these patterns, and automated tools make it easy for them to test variations of exposed passwords at scale.

DATA SIPHONED BY MALWARE

The Danger of Infected Employees

With the growing focus of criminals to leverage hard-to-detect tactics, such as infostealer malware, to extract information from unsuspecting users, our report is inclusive of this recaptured data as well as data from third-party breaches. Infostealer malware exfiltrates all manner of information, including browser history, autocomplete data, web session cookies, screenshots, system information, crypto wallets, and login credentials from an unsuspecting user's infected device. This type of malware poses a significant threat not only because it harvests fresh, accurate authentication data, but an increasingly common type of malware is configured to be non-persistent, meaning it deletes itself after data is stolen from a victim's machine.

Many people don't realise that credentials, PII, and other data available on the criminal underground are just as likely to come from infostealers as they are from large data breaches. **Of the 52.5 million third-party breach assets of FTSE 100 and subsidiaries, 58.6% came from botnets (30.64 million)**. **Likewise, of the 28.35 million PII assets we recaptured, 56% came from botnets (15.88 million)**. Information stolen through malware infections is collected by cybercriminals and shared in small circles or sold at high values on criminal marketplaces.

When SpyCloud recaptures malware-exfiltrated data, we parse out the infected victim's usernames, passwords, target URLs, cookies, and other types of stolen assets in order to help organisations protect themselves and their users. For this report, we searched these records for FTSE 100 and subsidiary corporate email addresses to identify employees who may be using infected managed devices or personal/unmanaged ones to access the corporate network or work applications.

In total, we've identified **17,181 malware-infected employees** within the FTSE 100 and their subsidiaries. Telecommunications, media, personal goods, food and drug retailers, and banks are the industries with the highest infection numbers.

The breadth of data captured by infostealers can have disastrous consequences for enterprises, whether the affected device is personal or corporate, since this malware exfiltrates everything from browser history to login data for work and third-party resources. Bad actors can use this information to bypass multi-factor authentication (MFA), log into corporate networks, steal sensitive data, authorise fraudulent transactions, and more. Even without exact corporate logins, criminals can easily extort, trick, or impersonate the victim to extend their access to corporate resources.

Ransomware is a malware problem. Often, bad actors use information or access that was gathered through malware infections as a basis for ransomware attacks. Stolen credentials are often the first attack vector for cybercriminals, and infected employee devices create a high ransomware risk. The risk is especially high when employees' devices are infected with malware that steals authentication data, given that IABs sell those freshly harvested employee credentials to ransomware operators. This authentication data allows the criminal to masquerade as the user, making it difficult for an organisation to quickly detect and properly remediate the infection.

Keep in mind that one infected device can expose hundreds of credential pairs given the prolific number of applications and work accounts each employee has. Even after an infected device is cleaned up or wiped, those exposed credentials are already out on the dark web and can continue to put the organisation and individual at further risk.

Additionally, **we recaptured a total of 28,549 credential sets collected by criminals, specifically allowing access to 7,502 cloud-based applications**, including popular enterprise apps like email, SSO, cloud hosting environments, customer relationship management software, payroll management, video conference platforms, source code repositories, and much more. Since these third-party applications are typically outside of IT's control, they can't be monitored by traditional security solutions, creating a blind spot for most enterprise security teams and yet another pathway into the organisation.

Data stolen from these applications can be used to aid attacks or can be the goal of the attack itself, such as when **source code** is stolen.

Exfiltrated Cookies are the New Passwords

While credential exposures plague enterprises, it's the growing threat of stolen session cookies that needs more mindshare. As criminal tactics evolve, bad actors are finding that the level of effort to hijack a session with malware-stolen cookies is significantly less than social engineering methods like phishing that require an action from the victim.

Session hijacking is a risk facing both employees and consumers. For organisations, stolen cookies can give cybercriminals an all-access pass to enterprise networks, allowing them to view sensitive information, escalate privileges, encrypt files, and launch ransomware. On the consumer side, fraudsters use stolen session cookies to take over accounts to make fraudulent purchases, drain loyalty cards and points, and more. With over 55 million stolen session cookie records tied to employees and consumers of the FTSE 100 and their subsidiaries that make authentication measures like MFA easy to bypass, it's no wonder cybercriminals are quick to use this data to continually circumvent existing defense measures. (and delete to access accounts and sessions.) Preventing session hijacking is not impossible. It requires rapid identification of stolen cookies and invalidation of active sessions that could put a business at risk.

Risk From Infected Consumers Remains High

In addition to infected employees, we also identified **658,146 infected consumers** of FTSE 100 services, with 35% of them in the media industry.

These are users of FTSE 100 and subsidiary consumer-facing sites where our recaptured data shows that they were infected while entering their username and password on the login page (e.g., jim@example.com was infected while logging into signin.ftse100company.com).

Consumers with infected devices and the resulting exposed data cost enterprises a lot of internal resources and money in customer service hours and fraud losses, impacting their bottom line.

The risk of fraud and identity theft is especially high because malware often siphons data that establishes a browser or device fingerprint (a combination of operating system, IP address, browser type, system fonts, browser extensions, bookmarks, and other data). Companies frequently use browser fingerprints to authenticate customers, and cybercriminals can use the fingerprints to successfully impersonate consumers without raising any red flags.

The true number of infected consumers for these industries is likely higher; for example, we excluded many consumer-only domains from this analysis. We've also nixed credentials with usernames instead of email addresses because it's unclear whether they are employee or consumer records. However, each one of these infected consumers is at extremely high risk of account takeover, identity theft, and online fraud, which can result in substantial losses and brand damage for affected organisations.

Why are infected consumers the organisation's problem? Here are just a few ways cybercriminals exploit information stolen via malware:

- Steal a victim's identity to commit fraud, such as opening loans in their name
- Transfer funds from crypto wallets, investment portfolios, payment applications, and other accounts
- Place fraudulent orders using credit card information or gift cards stored within accounts
- Siphon loyalty points associated with accounts
- Commit warranty fraud using stored device information
- Change shipping addresses to facilitate package theft and drop-shipping
- Stalk or blackmail victims using browser history and other stolen data
- Sell login details and browser fingerprints to other criminals

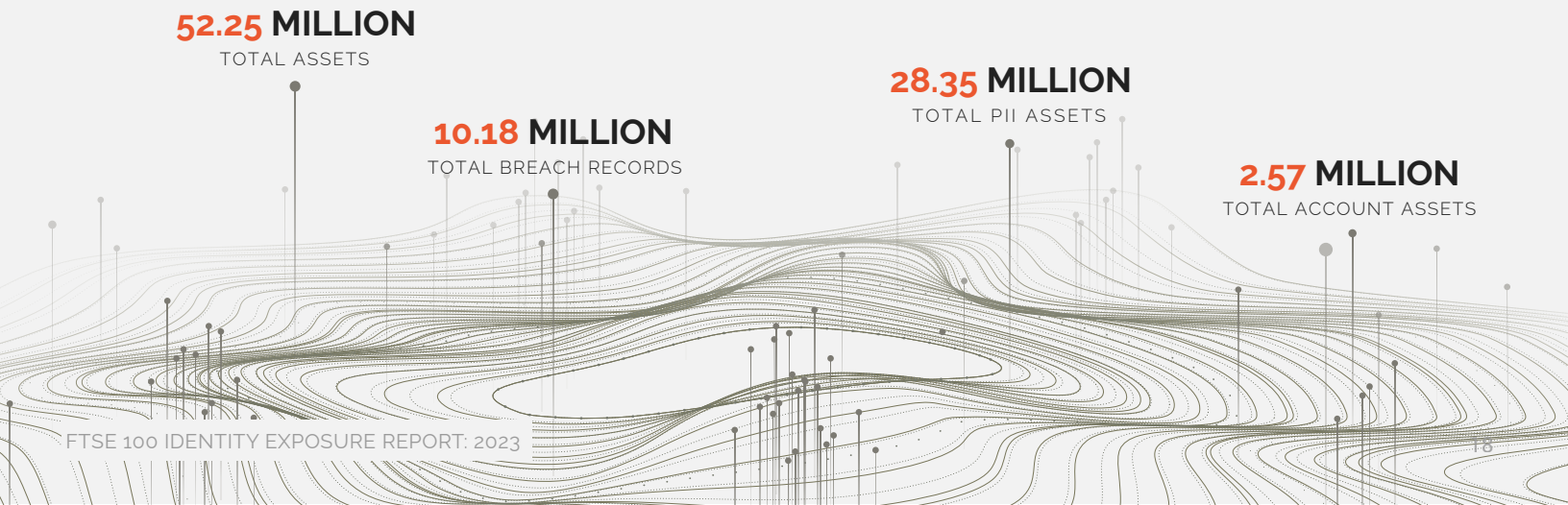
BEYOND CREDENTIALS:
OTHER EXPOSURES BY ASSET TYPE

In addition to login credentials, breach or malware-exfiltrated assets can include phone numbers, addresses, social security numbers, credit ratings, browser session tokens, and much more. While stolen credentials provide an obvious entry point for malicious actors, other types of darknet exposed assets can also create tremendous value for cybercriminals, whether for consumer fraud or as a means of gaining access to enterprise networks, data, intellectual property, and funds.

Criminals may engage in highly-targeted, manual attacks against victims with privileged access to corporate resources, such as C-suite leaders, senior executives, system administrators, and developers. Given the potential payoff associated with these targets, it's no wonder criminals are willing to invest substantial effort and creativity to take over their accounts.

In total, SpyCloud has collected 52.25 million breach and 55.41 million malware-exfiltrated session cookie records tied to FTSE 100 and subsidiaries' employees. We also found 84,297 records tied to the C-suite, which puts the companies at high risk for targeted schemes such as business email compromise, also known as CEO fraud, which are a leading cause of financial losses stemming from cybercrime.

Within the SpyCloud dataset, we have segmented certain types of assets into categories to help quantify different types of exposure. Let's break down how a few of these asset types can be used by cybercriminals and look at FTSE 100 employee exposure for each asset type.



ASSET TYPE:
PERSONALLY IDENTIFIABLE INFORMATION (PII)

WHAT IT IS

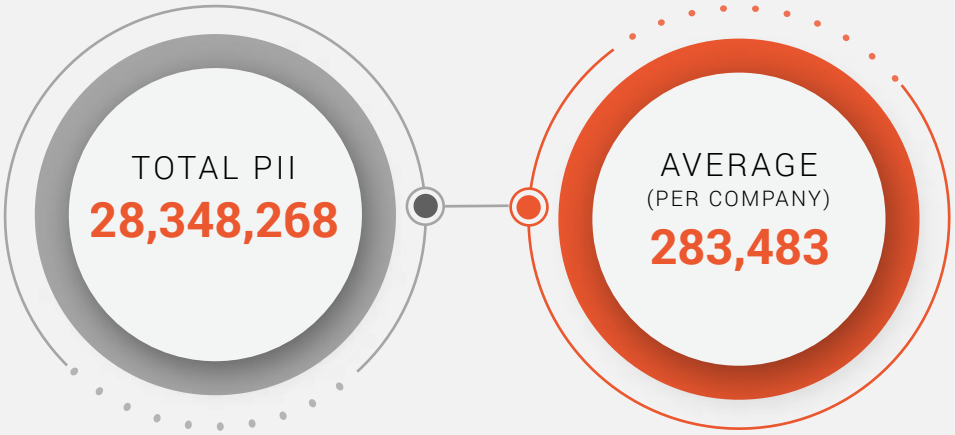
Personally identifiable information (PII) is data that could be used to identify an individual person. For the purposes of this report, SpyCloud has excluded some forms of PII that have been broken out into separate categories below, such as phone and financial assets. However, this category includes many other types of personal data such as addresses, NINOs, and credit ratings.

HOW IT HELPS CRIMINALS

PII can provide criminals with many lucrative paths for committing fraud or stealing corporate data, particularly when they have access to full packages of victims' information, or "fullz."

Using stolen PII, criminals can:

- Steal a victim's identity to commit fraud
- Craft detailed, credible spear phishing messages
- Answer security questions to reset MFA
- Submit fraudulent applications



PII

COOKIES / TOKENS

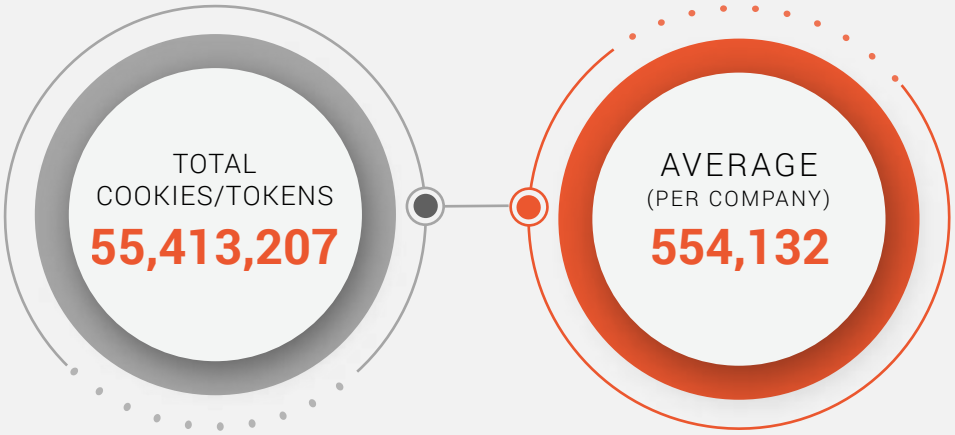
ASSET TYPE:
SESSION COOKIES OR TOKENS

WHAT IT IS

Session cookies or tokens authenticate users on a given website for a period of time. When you log into a site or application, the server sets a temporary session cookie in your browser. This lets the application remember that you're logged in and authenticated. Some cookies may last only 24-48 hours, while others last for months.

HOW IT HELPS CRIMINALS

Stolen session cookies allow bad actors to infiltrate organisations through session hijacking. With cookies in hand, criminals use anti-detect browsers with a browser plug-in to authenticate as the legitimate user, bypassing MFA to access an active web session. In 2022, SpyCloud recaptured tens of billions of cookies from the darknet – underscoring the scale of the data available to criminals and their ability to take over an account by essentially becoming a clone of that employee in your environment without the need for credentials.



ASSET TYPE:
PHONE ASSETS

WHAT IT IS

Phone assets are stolen phone numbers.

HOW IT HELPS CRIMINALS

In combination with stolen credentials, criminals can use phone assets to bypass multi-factor authentication using tactics such as SIM swapping and phone porting. With a simple phone call to a mobile carrier and some light social engineering, criminals can divert a victim's phone service to their own device. Once the attacker has control of the victim's phone number, they receive all SMS-based authentication messages and can easily log into sensitive accounts undetected.

ASSET TYPE:
GEOLOCATION

WHAT IT IS

Geolocation assets consist of latitude and longitude pairings that pinpoint users' physical locations. This is typically the location of the IP that a user last logged in from. That location sometimes correlates with their address, but not always, which is why this data has been separated from PII assets.

HOW IT HELPS CRIMINALS

Criminals can use geolocation data (or addresses) to craft targeted attacks against high-value victims such as employees with privileged access to corporate data.

Examples include:

- Using a residential proxy to mimic traffic from a user's location, avoiding controls that flag logins from unexpected locations
- Crafting spear phishing emails that reference the user's location, such as an event invitation that contains a malicious link
- Guessing the answers to knowledge-based security questions

GEOLOCATION

ASSET TYPE:
FINANCIAL

FINANCIAL

WHAT IT IS

Financial assets include credit card numbers, bank account numbers, and tax IDs. While this information all technically qualifies as PII, we have separated them into their own category due to the severity of the exposure.

HOW IT HELPS CRIMINALS

Criminals can use stolen credit card numbers and other financial information to harm your enterprise by:

- Making fraudulent purchases on corporate cards
- Reselling card numbers to other criminals
- Draining funds from accounts
- Collecting victims' tax refunds

ASSET TYPE:
SOCIAL

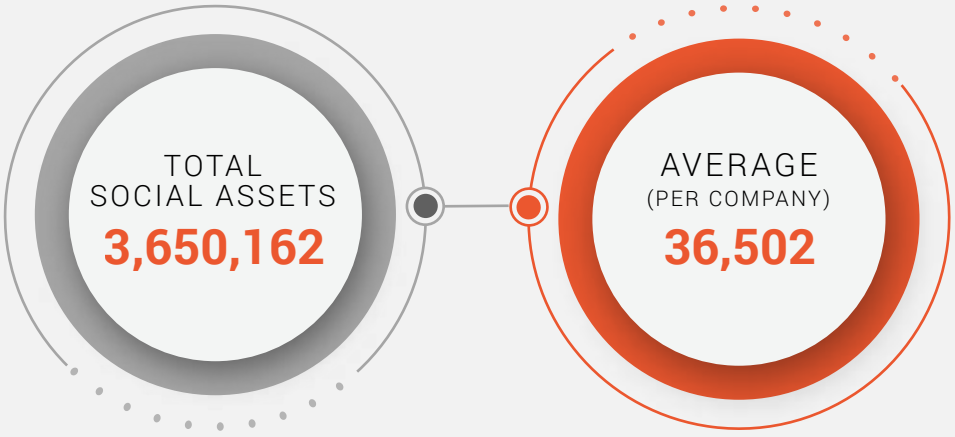
SOCIAL

WHAT IT IS

Social assets include social media handles that are tied to the breached account.

HOW IT HELPS CRIMINALS

Social assets can help criminals connect the dots between personal and corporate identities, which can be particularly useful in targeted attacks. An attacker may move laterally from one account to another, first compromising a social media account with limited protections in place and then using that access to compromise higher-value accounts or accounts belonging to the victim's trusted associates. Data shared on social media may also provide the attacker with insights that can aid in answering security questions or crafting believable spear phishing attacks.



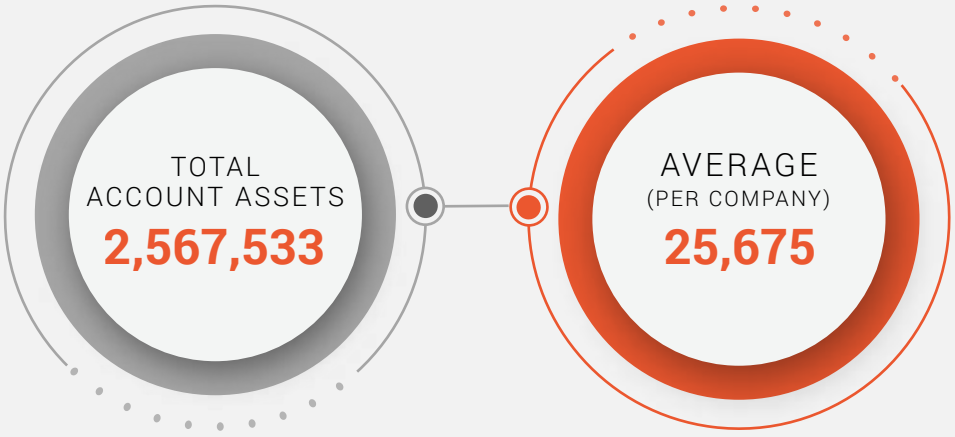
ASSET TYPE:
ACCOUNT

WHAT IT IS

Account assets are data related to the breached account itself – including secret answers to the security questions that many sites use as an extra layer of authentication. Account assets also encompass user activity records, such as the date an account was created and most recent login date.

HOW IT HELPS CRIMINALS

Access to users' secret answers makes it easy for attackers to bypass authentication measures and take over accounts. In addition, criminals may use account activity records to engender trust and convince users to share additional information, such as their password. For example, an attacker might list recent actions a user has taken on specific dates and ask them to "verify" their validity by taking a risky action like clicking a phishing link.



ASSET TYPE:
COMBO LIST APPEARANCES

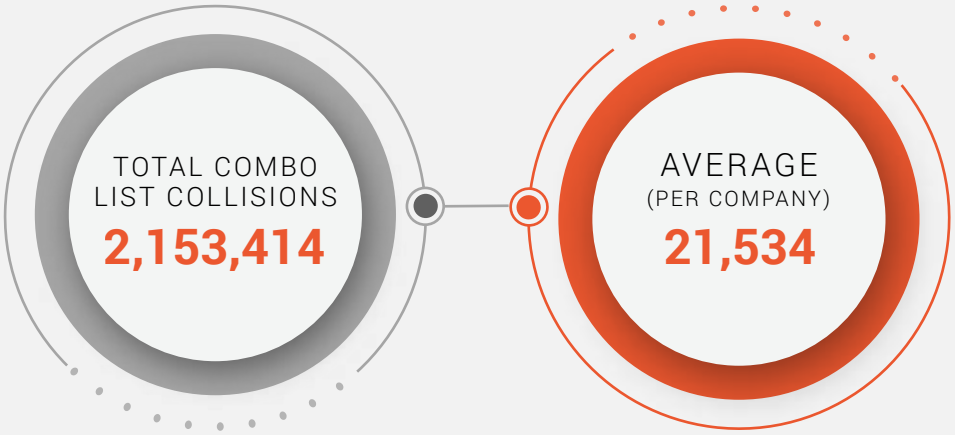
COMBO LIST

WHAT IT IS

Short for combination list, a combo list contains pairs of passwords and usernames or email addresses obtained from various breaches. SpyCloud finds that the vast majority of the data we see in combo lists is old – ingested months or even years prior to the list publication. Our focus is on recapturing data immediately after a breach occurs.

HOW IT HELPS CRIMINALS

Inexpensive or even freely available on the underground, combo lists are used for credential stuffing. Cybercriminals take advantage of the high password reuse rates among users and try the logins from the combo lists on other websites or apps. Any accounts using the same credentials found on a combo list remain in jeopardy. Combo lists serve as a good reminder that even old data can still be useful to criminals.



100 companies
AND THEIR SUBSIDIARIES

SPANNING THESE INDUSTRIES

Basic Materials
Consumer Discretionary
Consumer Staples
Energy
Financials
Health Care
Industrials
Real Estate
Technology
Telecommunications
Utilities

LONDON'S FTSE 100

SpyCloud

52,250,294
TOTAL BREACH ASSETS

522,503
AVERAGE # OF BREACH ASSETS **PER COMPANY**

10,726
TOTAL BREACH SOURCES

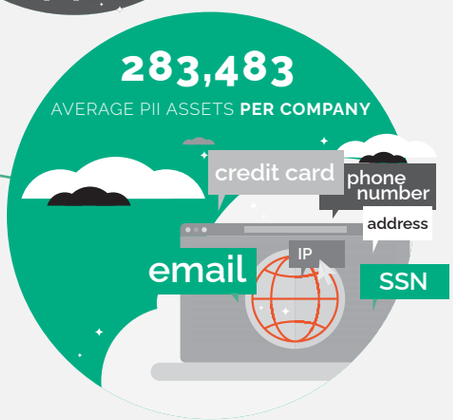
10,183,481
TOTAL BREACH RECORDS

101,835
AVERAGE # OF BREACH RECORDS **PER COMPANY**

65%
PASSWORD REUSE

28,348,268
TOTAL PII ASSETS

283,483
AVERAGE PII ASSETS **PER COMPANY**



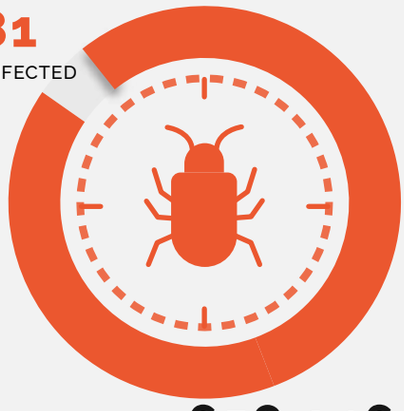
TYPES OF ASSETS (AVG PER COMPANY)

36,502	SOCIAL
25,675	ACCOUNTS
8,182	PHONE
5,170	GEOLOCATION
$ 710	FINANCIAL

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- password
- old123ma

17,181
MALWARE-INFECTED EMPLOYEES



658,146
MALWARE-INFECTED CONSUMERS

YOUR PLAN OF ACTION

SpyCloud's analysis of FTSE 100 companies' and their subsidiaries' exposure as a result of third-party breaches and malware- exfiltrated data has revealed millions of corporate assets in criminals' hands, 2.75 million of which are plaintext passwords tied to company employees. Combined with high rates of password reuse, these exposures represent significant cyber risks for these organisations and the companies and consumers doing business with them.

To defend account takeover, session hijacking, malware, ransomware, and other malicious cyberattacks, FTSE 100 companies and their subsidiaries cannot bet solely on their employees to keep them safe and rather should think of users as consumers whose behavior expands the attack surface multi-fold. To minimise exposure and safeguard data, enterprises need to enforce strong enterprise password policy with SSO where possible, create clear company policies on the use of business and personal devices, enforce MFA on critical accounts, and mandate the use of password managers, as well as leverage automated solutions that remediate their users' exposure – especially in industries entrusted with a vast amount of sensitive consumer data.

Given the growing prevalence of malware-siphoned data used by cybercriminals, security teams can take proactive steps to reduce the risk of exposed employee, contractor, and vendor identities. We recommend implementing 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.

Simply changing passwords after a malware infection does not guarantee active user sessions or trusted device tokens will be invalidated. Since information-stealing malware also siphons device and web session cookies, neglecting to address potentially stolen cookies leaves the victim's accounts vulnerable to session hijacking through device impersonation. For applications that fall outside your security team's purview, it may be necessary to contact the third-party cloud service provider and request that the compromised user sessions be invalidated as part of post-infection remediation efforts.

With millions of FTSE 100 and their subsidiaries' employee identities exposed, it's imperative that security teams act quickly on what cybercriminals have in hand to neutralize their risk of cyberattacks stemming from the use of this stolen data.

SpyCloud

LEARN HOW INCORPORATING

POST-INFECTION REMEDIATION

TO EXISTING INCIDENT RESPONSE PROTOCOLS HELPS ENTERPRISES NEGATE OPPORTUNITIES FOR RANSOMWARE AND OTHER CRITICAL THREATS.

GET THE GUIDE

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**.