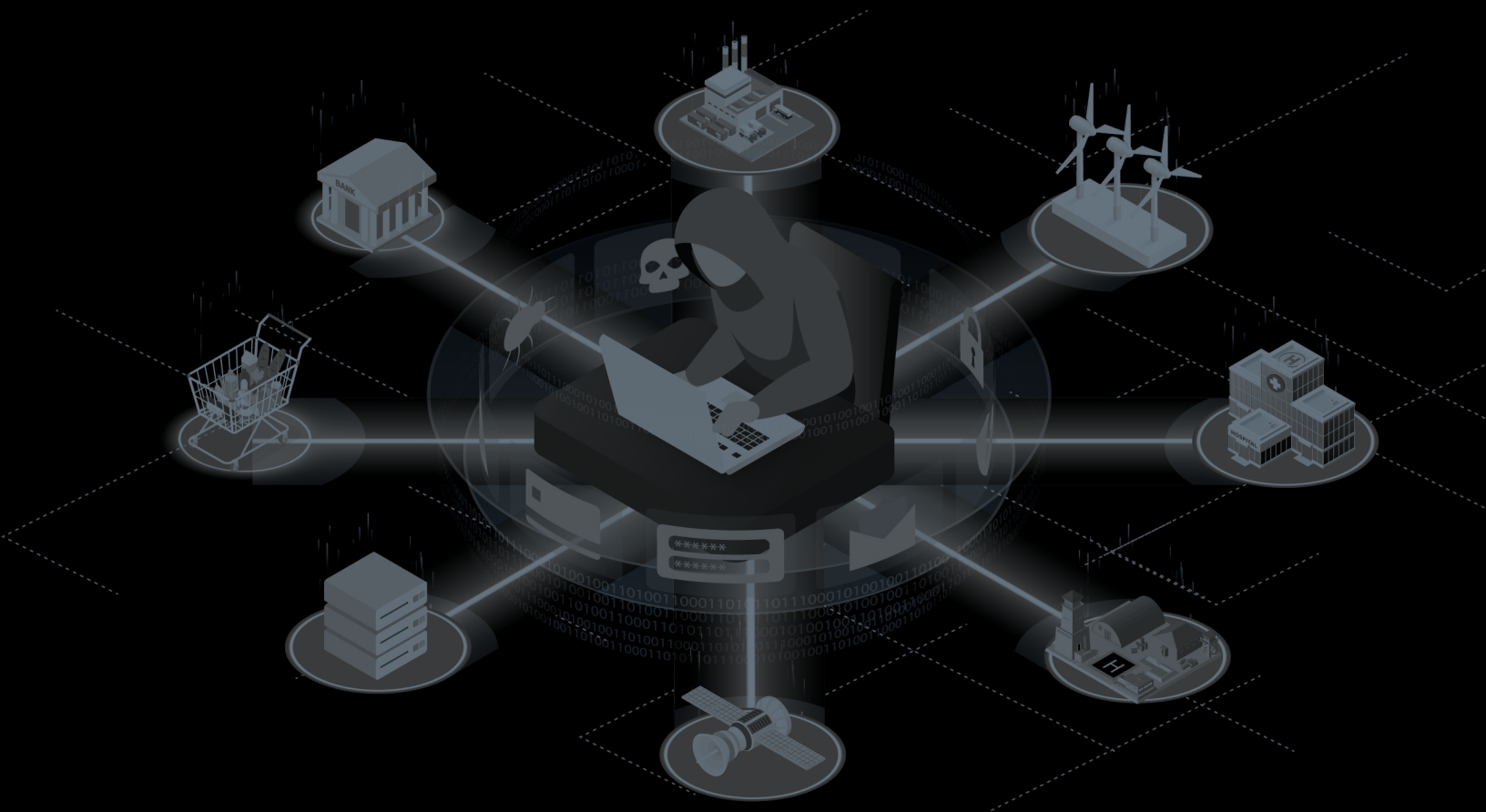
Fortune 1000 Identity Exposure Report

2022



SpyCloud

SpyCloud

Table of Contents

SpyCloud

Overview

As the world began rebounding from the pandemic last year, the move forward into a digital age marched on. More enterprises embraced hybrid work models rather than requiring a complete return to the office, and employees continued to juggle more account logins for web and cloud apps. And the lines between work and personal spaces – and devices – remained blurred.

These trends played well into the hands of cybercriminals, especially since employees' bad password habits didn't change. Falling back on weak and reused passwords has been a problem for a long time, but the explosion of digital tools is a gift to malicious actors.

Over the last several years, large companies have been investing heavily in sophisticated security measures. Every new device or digital account an employee adds, however, creates yet another path to sidestepping those measures and providing access to the company's assets. All a malicious intruder needs is a set of employee credentials that have been exposed in a breach, but in many cases, attackers have much more information at their disposal, including highly sensitive personally identifiable information (PII) siphoned from malware-infected devices that can be used to circumvent MFA and invade corporate networks.

For the third year in a row, SpyCloud has analyzed our entire database to understand the scope of breach exposure affecting large enterprises on the Fortune 1000 list. With well over 200 billion assets recaptured to date from the criminal underground, SpyCloud maintains the industry's largest repository of recovered stolen credentials and PII, collected as quickly as possible after exposure using human intelligence.

To perform our analysis, we searched for records containing Fortune 1000 corporate email domains, excluding "freemail" domains that are available to consumers. For example, if a Fortune 1000 employee signed up for a breached third-party site using their corporate email address, such as jonsmith@example.com, we were able to associate the resulting breach record to their employer.

For our analysis, we looked at more than **687 million breach assets** in our database tied directly to Fortune 1000 employee emails. In this report, we take a look at the top patterns across all 21 industry sectors, identify the ones with the highest risks, and then delve into a more detailed analysis of each.

About SpyCloud Data

SpyCloud's proprietary engine collects, curates, enriches, and analyzes recaptured data from breaches, malware-infected devices, and other sources from the criminal underground – transforming it into actionable insights that enable enterprises to quickly identify legitimate users vs. potential criminals using stolen information, and take action to prevent account takeover, ransomware, and online fraud.

Learn more at spycloud.com.

200+ Billion
Recaptured Assets

25+ Billion
Total Passwords

30+ Billion
Email Addresses

50+
Breach Sources Collected Per Week

Key Findings

1. Password reuse is rampant among Fortune 1000 employees.

We found a **64% password reuse rate** among Fortune 1000 email addresses in our database that have been exposed in more than one breach. This is 4 points higher than the 60% password reuse rate we see across our entire database, but it's even more concerning because high password reuse is a trend we see with Fortune 1000 employees year after year. It means that even their old exposures matter; criminals will use them against the employees and their enterprises for years as long as the habit remains unchanged. It's also a growing concern among CISOs in light of intensifying ransomware attacks that are stemming from exposed, reused credentials.

2. Exposure from data breaches continues to grow in the double digits.

Breach records associated with Fortune 1000 employees grew 18% year-over-year to **126.6 million**. A breach record is a set of data tied to a single user within a given breach, and includes individual breach assets (pieces of data within a record) such as a password and phone number. The quantity of breach *assets* tied directly to Fortune 1000 employees grew 26% year-over-year to **687.23 million**. The five sectors with the highest year-over-year growth in breach assets are telecommunications, media, industrials, technology, and business services.

3. The technology sector leads the way for the highest and most severe exposure.

The technology industry has the highest exposure both for breach records and passwords – as well as the highest numbers of malware-infected employees and consumers. We discovered **26.73 million** breach records in our database that are tied to technology companies. This number comprises 21% of all exposed breach records among Fortune 1000 companies (the highest share among all sectors). Additionally, technology company employees had more than **7 million** exposed credentials, comprising 26% of the total in the Fortune 1000 dataset (also the highest percentage of all sectors).

Things got much worse when we looked at malware infections. Technology companies, by far, have the highest number of infected employee devices (**34,078** of the 69,174 total) and infected consumer devices (**20.6 million** out of 28.9 million total for all Fortune 1000 companies). For context, the numbers for the second highest sectors were 4,584 infected employees (telecommunications) and 2.9 million infected consumers (media). As the technology industry has embraced remote or hybrid work, the blurred lines between work and personal devices may have led to this extreme exposure – and the sector's elevated risk as a result.

4. PII exposure is growing and especially affecting sectors like finance, retail, and telecommunications.

The financial sector had the highest number of PII assets exposed last year – **70.78 million** (comprising almost 18% of the Fortune 1000's total PII exposure). Retail companies weren't far behind, with **69 million** exposed PII assets. Financial companies also had the highest proportion of exposed geolocation assets (23%) and phone assets (21%). But when it came to the average number of PII assets per company, the numbers for telecommunications were jarring – nearly **2.75 million** compared to the average of 395,633 across all industries. Cybercriminals use PII in social engineering and phishing schemes to gain access into a company and steal sensitive data. It's especially concerning to see large PII exposure among employees of sectors that are entrusted with vast amounts of consumer data.

5. Critical infrastructure sectors carry the torch for worst password hygiene.

Among most Fortune 1000 companies, we consistently find company names in the top 10 most popular passwords. In far too many cases, we're seeing as many as half of the 10 most popular passwords at a specific company containing that company's name. These are foundational misses in password hygiene across the board – but especially worrisome for critical infrastructure industries. Overall, we identified 4 critical infrastructure industries (aerospace and defense, chemical, industrial, and energy) where company names are one of the top 3-5 most popular passwords.

SpyCloud

At-a-Glance: Fortune 1000 Identity Exposure

18,974

TOTAL BREACH SOURCES

Total number of breaches in the SpyCloud database that include records tied to Fortune 1000 corporate email address.

126,590,382

TOTAL CORPORATE BREACH RECORDS

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.

687,234,099

TOTAL BREACH ASSETS

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

27,363,632

TOTAL PLAINTEXT CORPORATE CREDENTIALS

Total number of Fortune 1000 corporate 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.

134,945

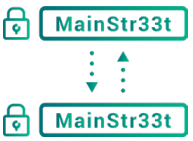
TOTAL C-LEVEL EXECUTIVES EXPOSED

Exposed corporate credentials that are tied to Fortune 1000 executives with high-ranking titles, putting them at increased risk of targeted account takeover attempts and business email compromise (BEC) fraud.

64%

PASSWORD REUSE

Among the Fortune 1000 employees who appear in more than one breach, this is the rate of password reuse we have observed. This includes exact passwords and slight variations that criminals can easily match.



69,174

MALWARE-INFECTED EMPLOYEES

Fortune 1000 employees whose data appears in recaptured botnet logs from infostealer malware. This high-severity exposure puts them at high risk of ATO and fraud, and makes the enterprise vulnerable to ransomware attacks.

Corporate Credential Exposure of the Fortune 1000

Exposed Corporate Credentials by Sector

Across the SpyCloud dataset, we discovered nearly **27.36 million pairs of credentials** with Fortune 1000 corporate email addresses and plaintext passwords. The three sectors that have the highest exposure by far are technology (7.07 million), telecommunications (6.35 million), and financial (3.56 million). While the high numbers for financial and technology may be partially due to the sector size (164 and 120 companies, respectively), the telecommunications sector's exposure is extreme given it only includes 10 enterprises.

While not every credential pair will match corporate login details, the ones that do match represent substantial risk for these enterprises – and their customers and partners.

When credentials are exposed in a data breach, cybercriminals inevitably test them against a variety of other online sites, 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.

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, and some corporate password policies even encourage bad habits. Outdated policies like strict complexity rules and mandatory 90-day password rotations make passwords harder to remember, leading employees to make insecure choices like recycling versions of their favorite passwords. That's why guidance from the National Institute of Standards and Technology (NIST) calls for organizations to proactively check for "commonly used, expected, or compromised" passwords to effectively mitigate the risk posed by human behavior.

In the SpyCloud database, we found:

Fortune 1000 Sector	Number of Companies	Total Exposed Corporate Credentials	Average Corporate Credentials per Company
Aerospace & Defense	20	490,065	24,503
Apparel	13	141,860	10,912
Business Services	55	493,538	8,973
Chemicals	29	328,590	11,331
Energy	95	811,061	8,537
Engineering & Construction	33	263,810	7,994
Financials	164	3,569,835	21,767
Food & Drug Stores	9	51,637	5,737
Food, Bev & Tobacco	37	267,378	7,226
Health Care	82	1,536,579	18,739
Hotels, Restaurants & Leisure	25	370,165	14,807
Household Products	25	366,923	14,677
Industrials	52	1,307,875	25,151
Materials	44	242,085	5,502
Media	27	1,608,749	59,583
Motor Vehicles & Parts	21	383,087	18,242
Retailing	73	872,138	11,947
Technology	120	7,071,515	58,929
Telecomm	10	6,354,314	635,431
Transportation	36	588,843	16,357
Wholesalers	30	243,585	8,120

Password Reuse: Worst Offenders by Sector

Within our dataset of Fortune 1000 corporate breach exposures, we calculated the average password reuse rate by taking the number of employees using the same exposed plaintext password across multiple sites, then divided by the number of all employees with exposed passwords. We found a **64% average reuse rate**, and two of the 21 sectors really stood out when it comes to their password reuse percentage:

- Aerospace & Defense (75%)
- Motor Vehicles & Parts (75%)

Employees with multiple reused passwords in our dataset may or may not reuse passwords at work – we can't tell for sure without checking their actual work passwords. However, password reuse across their third-party breach-exposed accounts does provide an indication of employees' overall password hygiene.

TOP 100 REUSED PASSWORDS OF 2021

```
pass  123456  password  123456789  12345678
qwerty  12345  111111  1234567890  qwerty123
123123  1234567  1q2w3e  DEFAULT  1234
000000  qwertyuiop  abc123  123321
1q2w3e4r5t  iloveyou  11111111  654321
a123456  666666  123123123  1q2w3e4r  987654321
admin  x4ivygA51F  asdasd  password1  123456a
1qaz2wsx  Password  zinch  112233  zxcvbnm
123qwe  qwe123  asdfghjkl  fuk19600  121212
7777777  UNKNOWN  123456789a  dragon  123654
homelesspa  azerty  5201314  555555  00000000
159753  q1w2e3r4t5y6  1234qwer  yuantuo2012
Sojdlg123aljg  aaaaaa  abcd1234  qazwsx
3rJs1la7qE  12345678910  princess
monkey  football  88888888  q1w2e3r4  qwer1234
147258369  0123456789  pokemon
1qaz2wsx3edc  asdfgh  0987654321  sunshine
222222  Aa123456  killer  2011-10-10
[redacted]you  mynoob  michael  ashley
col123456  daniel  999999  google  777777
3Odi15ngxB  superman  naruto  changeme  qwerty1
123abc  shadow  789456123
```

In the SpyCloud database, we found:

Rank	Sector	Password Reuse
1	Aerospace & Defense Motor Vehicles & Parts	75%
2	Industrials Media	66%
3	Apparel Chemicals Financials Healthcare	65%
4	Household Products Technology Wholesalers	64%
5	Business Services Energy Materials Retailing	63%
6	Food, Beverages & Tobacco	62%
7	Engineering & Construction Hotels, Restaurants & Leisure	60%
8	Transportation	59%
9	Food & Drug Stores Telecommunications	53%

Favorite Passwords of Fortune 1000 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 they're trying to crack corporate passwords. However, banning the use of the company name in passwords may not be enough. Organizations need to find ways of protecting employees from themselves.

Fortune 1000 employees follow the same patterns as the rest of us. Each of the passwords below appeared hundreds or even thousands of times within our dataset. We've redacted company names, as well as several variations of a popular four-letter word that we opted not to print. Interestingly, we observed that this particular word, year after year, is mostly popular with media companies, and employees at Fortune 1000 enterprises have a much higher affinity to it than those working at their UK FTSE 100 counterparts.

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.

PASSWORD

appears in 235,200 passwords

123456

appears in 99,913 passwords

TopSecret123

appears in 9,708 passwords

Data Siphoned by Malware

The Danger of Infected Employees

Not all of the exposed data in this report comes from data breaches. SpyCloud also recaptures information collected by botnets. Malware with keylogging components, or "infostealers," can siphon information such as browser history, autocomplete data, web session cookies, screenshots, system information, crypto wallets, and login credentials from an unsuspecting user's infected device.

Like breach data, information stolen through malware infections is collected by cybercriminals, shared in small circles, and sold on criminal marketplaces.

When SpyCloud recaptures these bot logs, we parse out the infected victim's username, password, URL, and cookies in order to help organizations protect themselves and their users. For this report, we searched these records for Fortune 1000 corporate email addresses to identify employees who may be using infected personal or corporate devices.

The technology sector leads all industries for the number of infected employees from Fortune 1000 companies with 34,078, which represents nearly half of all those observed in our database. Telecommunications, financial services, retail and health care round out the top five industries with infected employees.

The breadth of data captured by these infections can have disastrous consequences for enterprises, whether the affected device is personal or corporate. Malware siphons everything from browser history to login data for work and third-party resources. Bad actors can use this information to bypass multi-factor authentication, log into corporate networks, steal sensitive data, authorize 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.

In the SpyCloud database, we found:

Fortune 1000 Sector	Malware-Infected Employees
Aerospace & Defense	332
Apparel	616
Business Services	2,312
Chemicals	611
Energy	1,253
Engineering & Construction	771
Financials	4,141
Food & Drug Stores	201
Food, Beverages & Tobacco	1,189
Health Care	3,232
Hotel, Restaurants & Leisure	1,064
Household Products	829
Industrials	2,910
Materials	546
Media	2,579
Motor Vehicles & Parts	1,575
Retailing	4,135
Technology	34,078
Telecommunications	4,584
Transportation	1,702
Wholesalers	514
TOTAL	**69,174**

Stolen credentials are often the first attack vector for cybercriminals, and ransomware poses a major risk from infected employee devices. A recent SpyCloud report found that **IT security professionals ranked compromised credentials as the second riskiest entry point in ransomware attacks** (not far behind phishing). The risk is especially high when employees' devices are infected with malware that steals authentication data, given that a specialized criminal group known as initial access brokers sell those freshly harvested employee credentials to ransomware operators. This perhaps explains why 79% of our surveyed security leaders and practitioners said that last year's high-profile ransomware attacks elevated their concern about compromised and weak credentials used by their employees and customers.

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. And even after the device is cleaned up, those exposed credentials continue to put the organization at risk.

Risk From Infected Consumers Just As High

In addition to infected employees, we also identified nearly **28.89 million infected consumers** of Fortune 1000 services.

These are users of Fortune 1000 consumer-facing sites where botnet logs show 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.fortune1000company.com).

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

In the SpyCloud database, we found:

Fortune 1000 Sector	Malware-Infected Consumers
Aerospace & Defense	873
Apparel	95,542
Business Services	2,151,740
Chemicals	3,377
Energy	22,227
Engineering & Construction	6,230
Financials	61,735
Food & Drug Stores	47,241
Food, Beverages & Tobacco	23,603
Health Care	33,984
Hotel, Restaurants & Leisure	82,628
Household Products	27,842
Industrials	16,969
Materials	691
Media	2,930,296
Motor Vehicles & Parts	15,232
Retailing	2,556,714
Technology	20,636,961
Telecommunications	119,571
Transportation	49,399
Wholesalers	4,967
TOTAL	**28,887,822**

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.

One of the most widely used Windows infostealers that SpyCloud researchers observed over the course of the last year is RedLine Stealer. Available for purchase on the underground for about $800 (or $200 a month as malware-as-a-service subscription), RedLine Stealer is typically distributed through phishing campaigns, malicious search results for free or cracked software, and comment links in online videos. And it's an especially tricky malware to fight – security researchers found it can masquerade as legitimate downloads for software, such as Windows updates.

The true number of infected consumers for these sectors 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 enterprises.

Beyond Credentials: Other Exposures by Asset Type

A breach asset is a piece of information connected to a single breach record. In addition to login credentials, breach assets can include phone numbers, addresses, social security numbers, credit ratings, and much more – any type of information that can be obtained in a data breach. While stolen credentials provide an obvious entry point for malicious actors, other types of breach 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 **687.23 million breach assets** tied to Fortune 1000 employees last year. This represents a **26.8%** growth in assets year-over-year.

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 Fortune 1000 employee exposure for each asset type by sector.

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, social security information, and credit ratings.

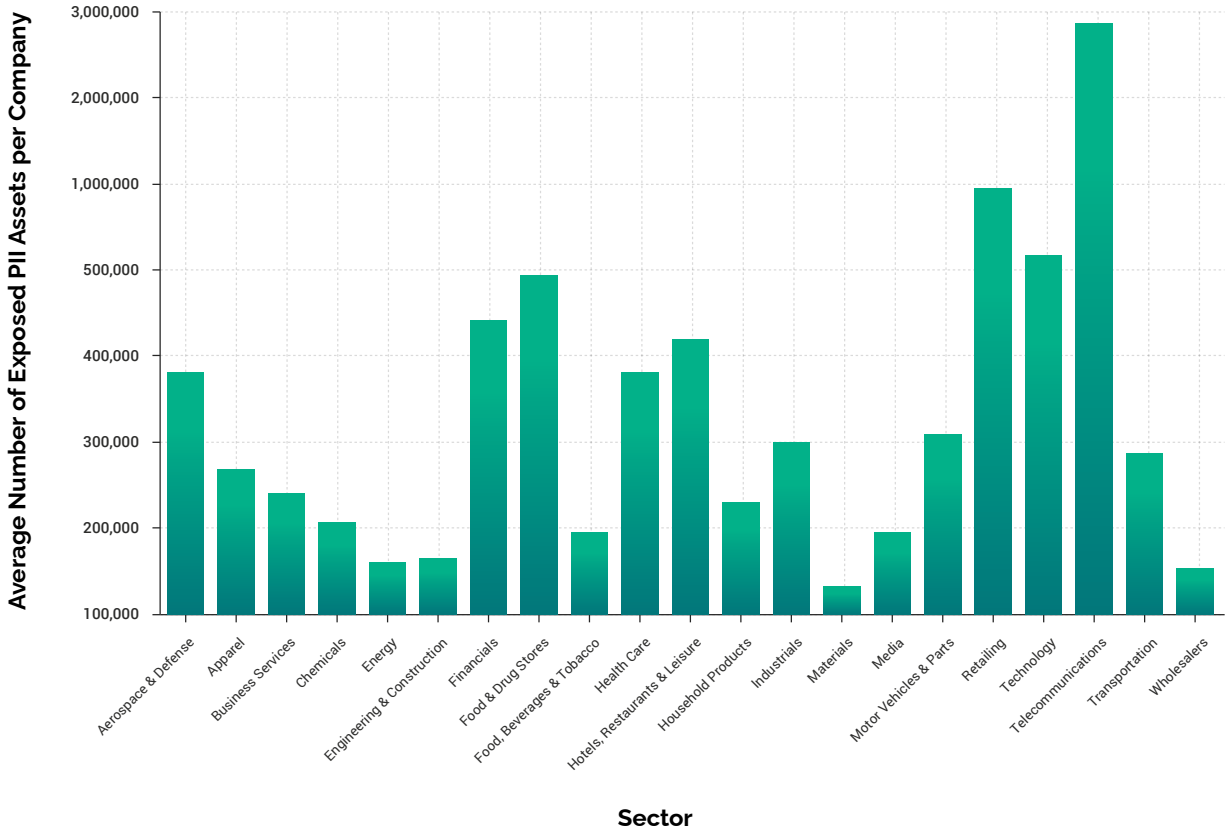
How It Helps Criminals

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

Exposures by Sector: Average Number of Exposed PII Assets per Company



Asset Type: Phone Assets

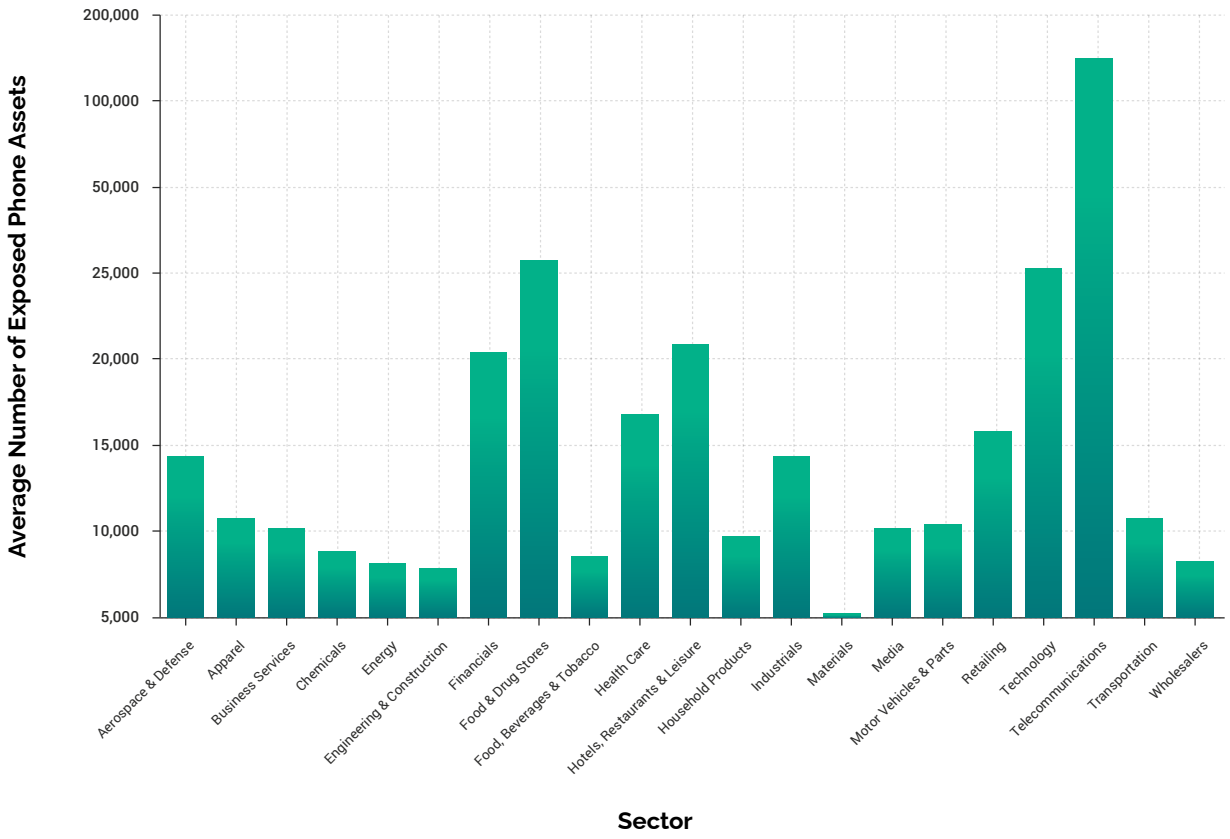
What It Is

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.

Exposures by Sector: Average Number of Exposed Phone Assets per Company



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.

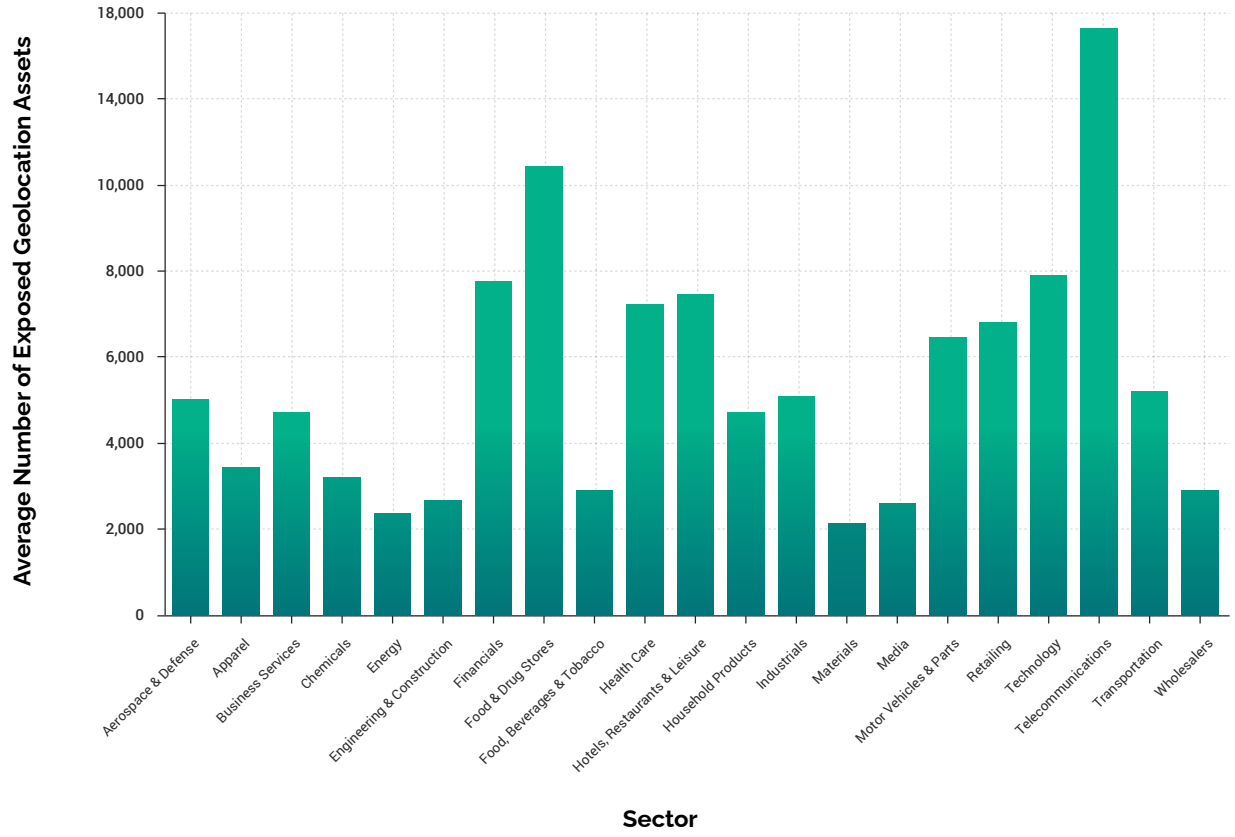
How It Helps Criminals

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 VPN 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

Exposures by Sector: Average Number of Exposed Geolocation Assets per Company



Asset Type: Financial

What It Is

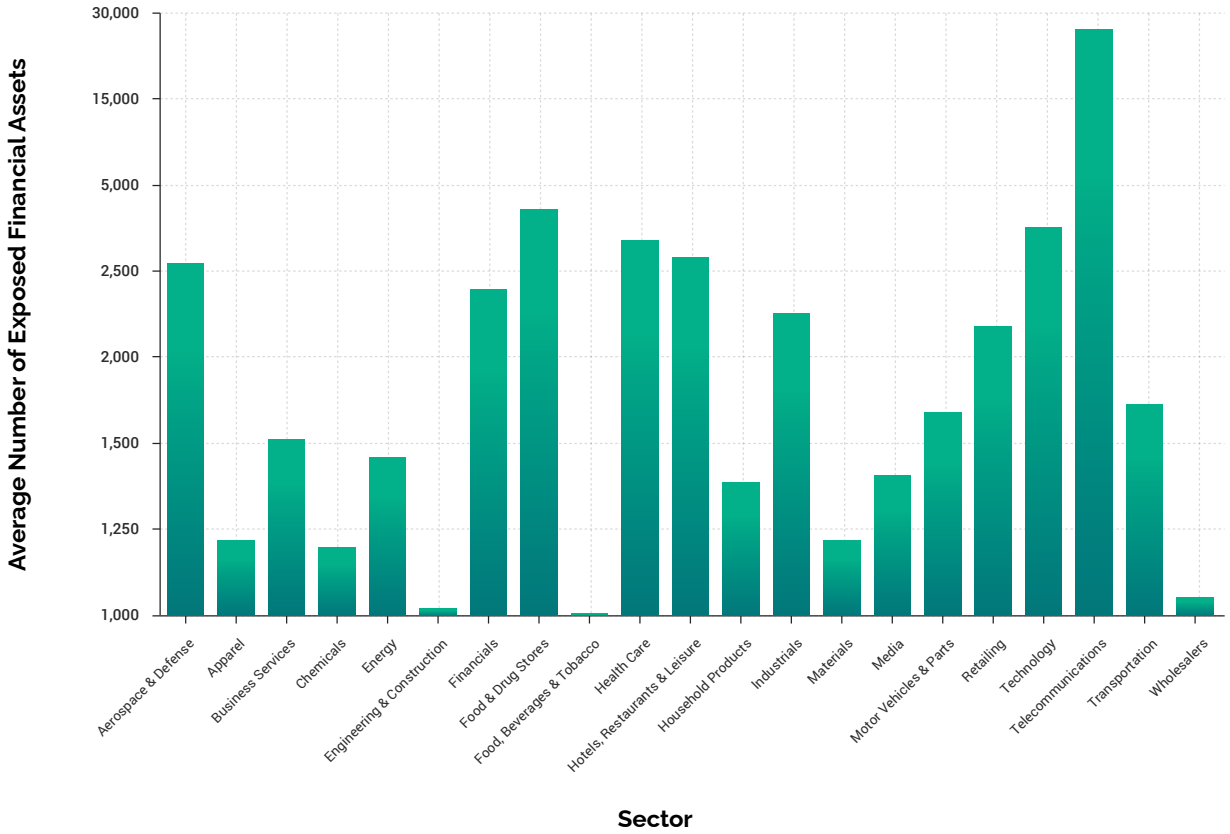
Financial assets include credit card numbers, bank account numbers, and tax IDs. While this information all technically qualifies as PII, we have separated them into their own category due to the severity of the exposure.

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

Exposures by Sector: Average Number of Exposed Financial Assets per Company



Asset Type: Social

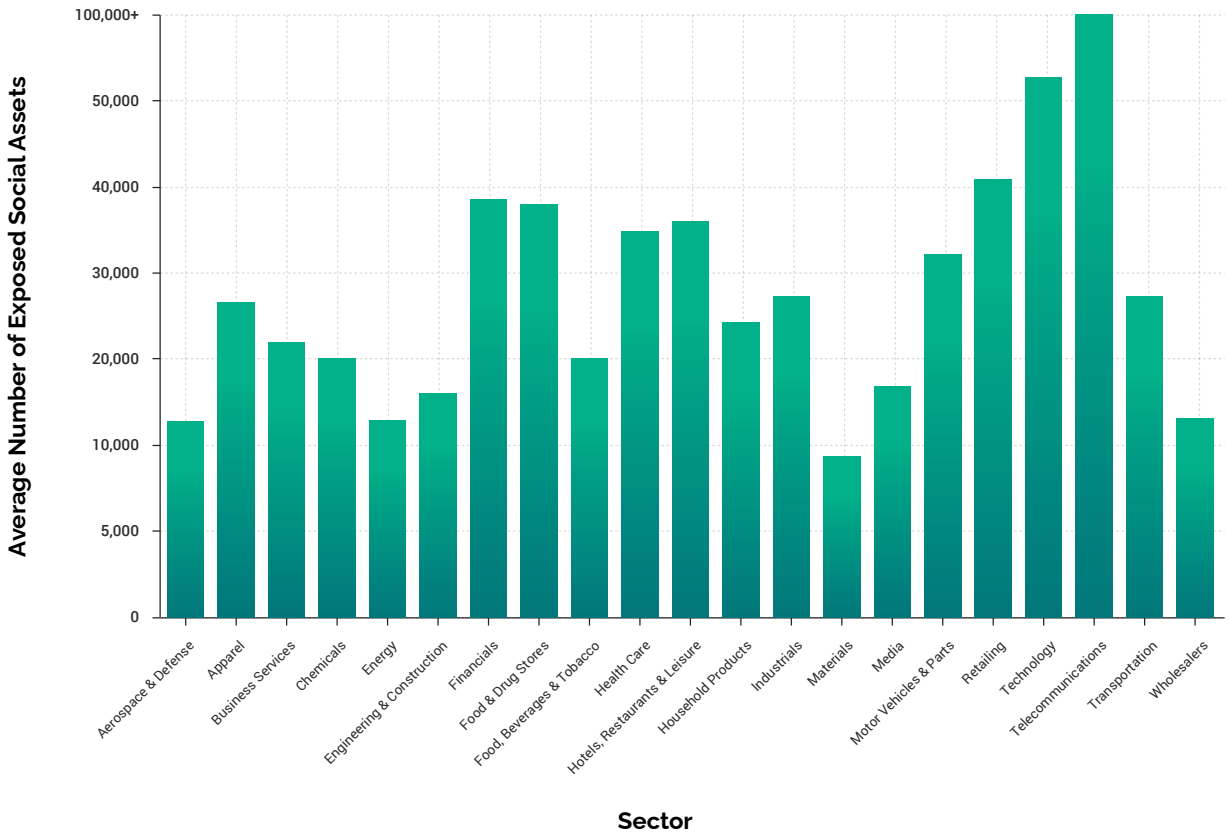
What It Is

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.

Exposures by Sector: Average Number of Exposed Social Assets per Company



Asset Type: Account

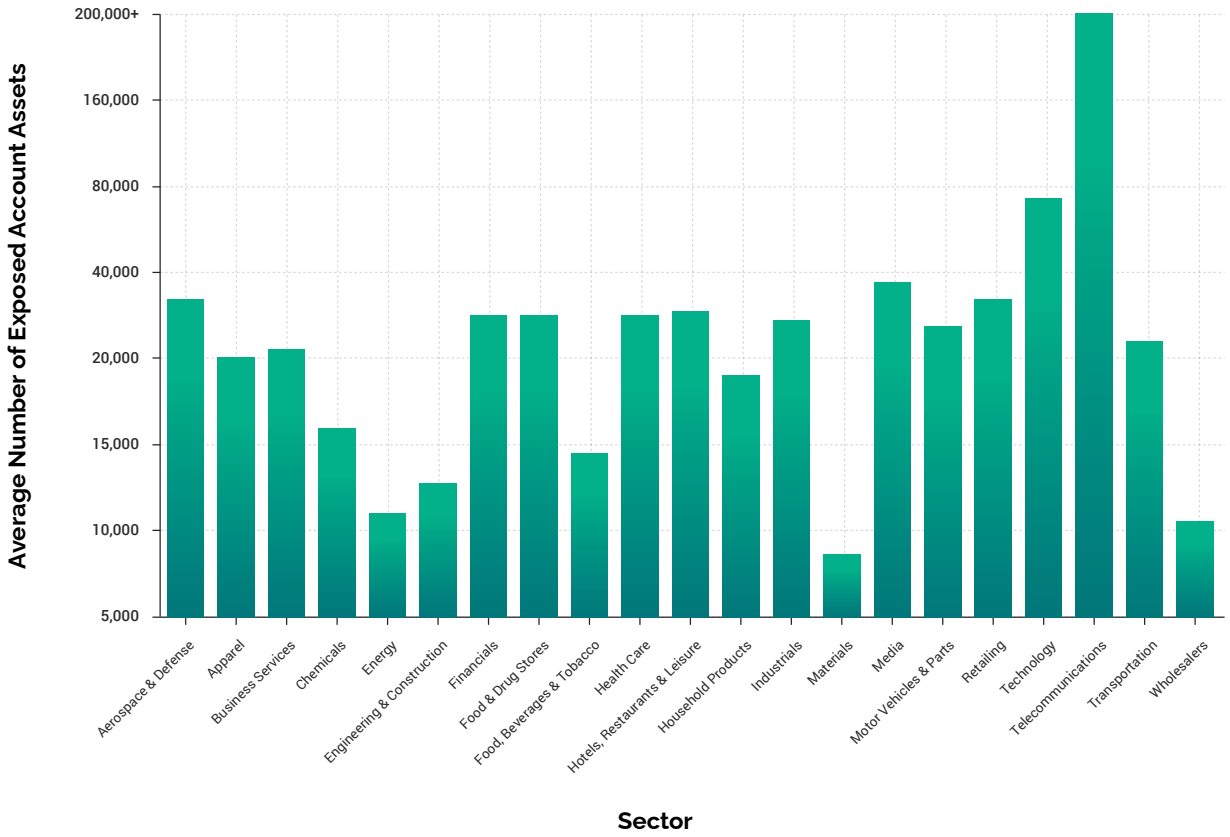
What It Is

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.

Exposures by Sector: Average Number of Exposed Account Assets per Company



Asset Type: Combo List Appearances

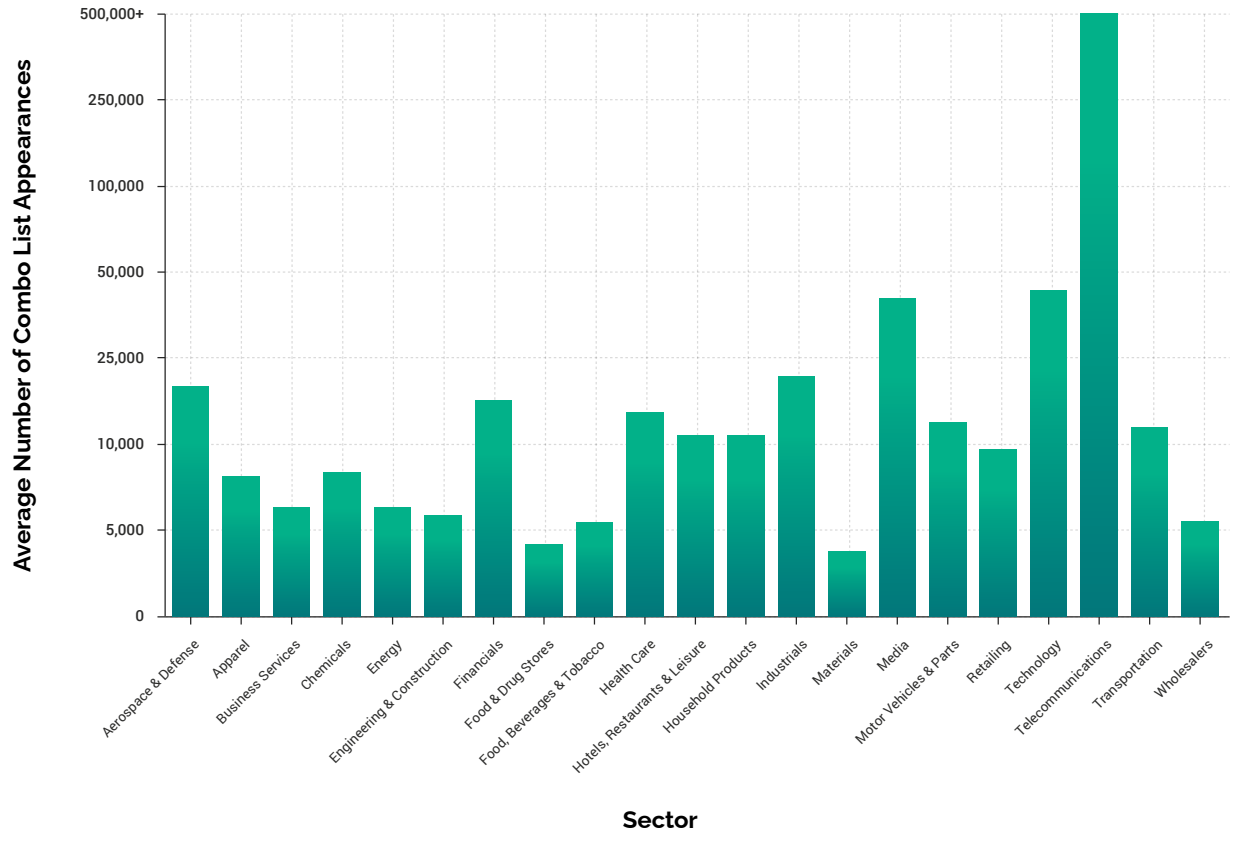
What It Is

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.

Exposures by Sector: Average Number of Combo List Appearances per Company



Fortune 1000 Identity Exposure by Sector

To provide additional insight into the sector exposure of the Fortune 1000, we have broken out our analysis by sector, using the classifications designated by Fortune.

INFOGRAPHIC

2022 Aerospace & Defense Sector Exposure

SpyCloud

20 COMPANIES FROM THE AEROSPACE SECTOR

3,538

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

2,498,285

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

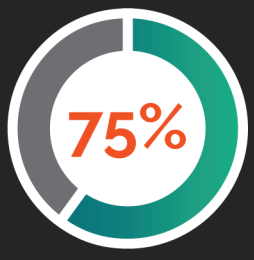
Average number of breach records per company in this sector: 124,914

13,201,895

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 660,095



PASSWORD REUSE RATE

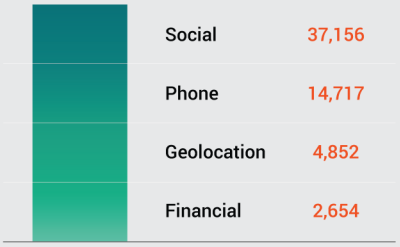
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

7,580,294

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 379,015



490,065

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

24,503 Average number of exposed credentials per company

1,411 Exposed C-level executives

332 Malware-infected employees

INFOGRAPHIC

2022 Apparel Sector Exposure

SpyCloud

13 COMPANIES FROM THE APPAREL SECTOR

2,671

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

936,139

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

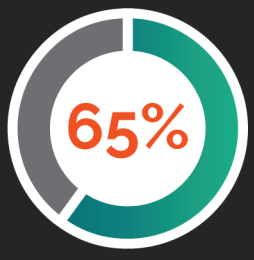
Average number of breach records per company in this sector: 72,011

5,617,419

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 432,109



PASSWORD REUSE RATE

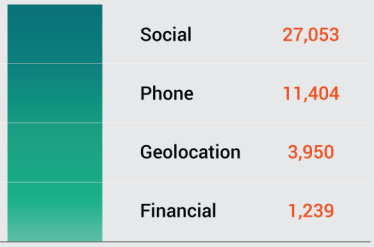
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

3,423,699

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 263,361



141,860

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

10,912 Average number of exposed credentials per company

1,502 Exposed C-level executives

616 Malware-infected employees

INFOGRAPHIC

2022 Business Services Sector Exposure

SpyCloud

55 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Advertising, Marketing
- Diversified Outsourcing Services
- Education
- Equipment Leasing
- Financial Data Services
- Miscellaneous
- Temporary Help
- Waste Management

4,918

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

3,693,339

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

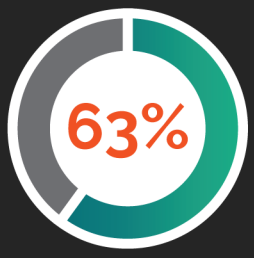
Average number of breach records per company in this sector: 67,152

22,252,637

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 404,593



PASSWORD REUSE RATE

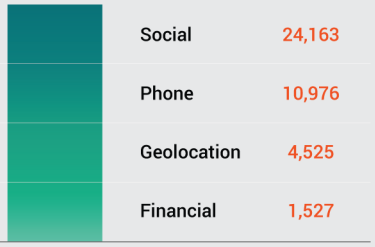
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

13,519,551

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 245,810



493,538

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

8,973 Average number of exposed credentials per company

6,321 Exposed C-level executives

2,312 Malware-infected employees

INFOGRAPHIC

2022 Chemicals Sector Exposure

SpyCloud

29 COMPANIES FROM THE CHEMICALS SECTOR

4,557

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,886,388

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

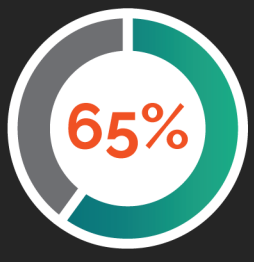
Average number of breach records per company in this sector: 65,048

10,354,733

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 357,060



PASSWORD REUSE RATE

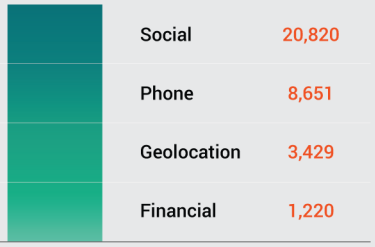
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

6,057,725

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 208,887



328,590

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

11,331 Average number of exposed credentials per company

1,732 Exposed C-level executives

611 Malware-infected employees

INFOGRAPHIC

2022 Energy Sector Exposure

SpyCloud

95 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Energy
- Mining, Crude-Oil Production
- Miscellaneous
- Oil and Gas Equipment
- Services
- Petroleum Refining
- Pipelines
- Utilities: Gas and Electric

5,337

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

4,654,277

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

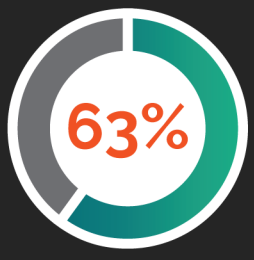
Average number of breach records per company in this sector: 48,992

25,718,271

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 270,719



PASSWORD REUSE RATE

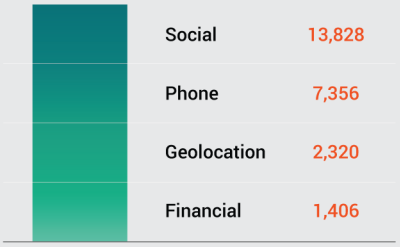
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

15,182,972

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 159,821



811,061

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

8,537 Average number of exposed credentials per company

5,386 Exposed C-level executives

1,253 Malware-infected employees

INFOGRAPHIC

2022 Engineering & Construction Sector Exposure

SpyCloud

33 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Engineering • Construction • Homebuilding

3,378

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,700,228

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

Average number of breach records per company in this sector: 51,522

9,212,639

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 279,171

PASSWORD REUSE RATE

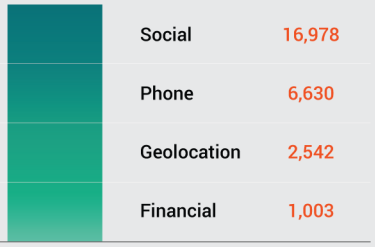
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

5,400,642

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 163,656



263,810

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

7,994 Average number of exposed credentials per company

3,148 Exposed C-level executives

771 Malware-infected employees

INFOGRAPHIC

2022 Financial Sector Exposure

SpyCloud

164 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Commercial Banks
- Diversified Financials
- Real Estate
- Securities
- Insurance: Life, Health (Mutual)
- Insurance: Life, Health (Stock)
- Insurance: Property and Casualty (Mutual)
- Insurance: Property and Casualty (Stock)

8,342

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

21,501,239

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

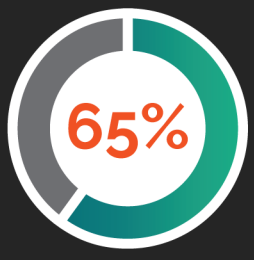
Average number of breach records per company in this sector: 131,105

119,686,816

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 729,798



PASSWORD REUSE RATE

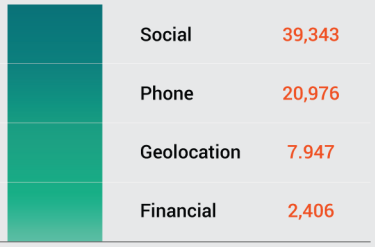
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

70,775,565

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 431,558



3,569,835

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

21,767 Average number of exposed credentials per company

40,114 Exposed C-level executives

4,141 Malware-infected employees

INFOGRAPHIC

2022 Food & Drug Stores Sector Exposure

SpyCloud

9 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Grocery & Food Stores • Pharmacy & Drug Stores

1,156

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,062,721

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

Average number of breach records per company in this sector: 118,080

6,919,621

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 768,847

PASSWORD REUSE RATE

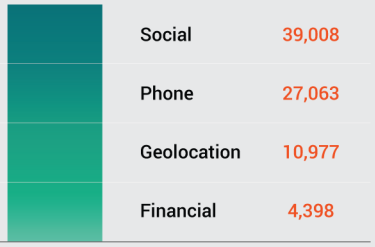
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

4,470,881

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 496,765



51,637

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

5,737 Average number of exposed credentials per company

945 Exposed C-level executives

201 Malware-infected employees

INFOGRAPHIC

2022 Food, Beverages & Tobacco Sector Exposure

SpyCloud

37 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Beverage Products
- Food Consumer Products
- Food Production
- Tobacco Products

4,270

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,960,899

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

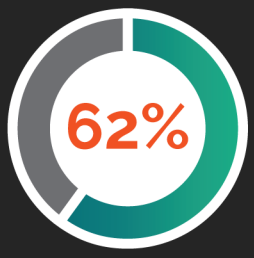
Average number of breach records per company in this sector: 52,997

11,612,197

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 313,843



PASSWORD REUSE RATE

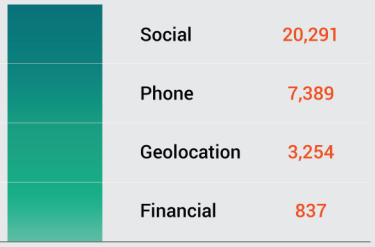
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

7,064,850

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 190,942



267,378

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

7,226 Average number of exposed credentials per company

2,585 Exposed C-level executives

1,189 Malware-infected employees

INFOGRAPHIC

2022 Health Care Sector Exposure

SpyCloud

82 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Insurance and Managed Care
- Medical Facilities
- Pharmacy and Other Services
- Medical Products and Equipment
- Pharmaceuticals
- Scientific, Photographic and Control Equipment
- Wholesalers

7,488

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

9,374,817

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

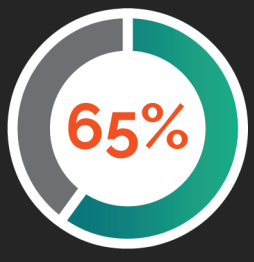
Average number of breach records per company in this sector: 114,327

53,614,188

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 653,832



PASSWORD REUSE RATE

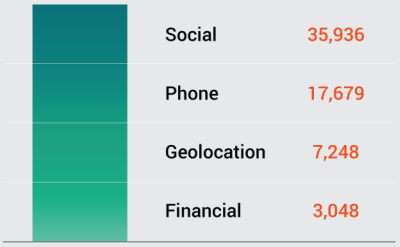
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

31,746,095

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 387,148



1,536,579

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

18,739 Average number of exposed credentials per company

10,022 Exposed C-level executives

3,232 Malware-infected employees

INFOGRAPHIC

2022 Hotels, Restaurants & Leisure Sector Exposure

SpyCloud

25 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Food Services • Hotels, Casinos & Resorts

3,818

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

2,923,558

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

Average number of breach records per company in this sector: 116,942

17,089,929

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 683,597

PASSWORD REUSE RATE

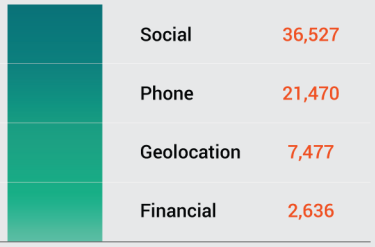
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

10,409,056

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 416,362



370,165

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

14,807 Average number of exposed credentials per company

8,948 Exposed C-level executives

1,064 Malware-infected employees

INFOGRAPHIC

2022 Household Products Sector Exposure

SpyCloud

25 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Home Equipment
- Furnishings
- Household and Personal Products
- Miscellaneous
- Toys
- Sporting Goods

4,676

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,784,530

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

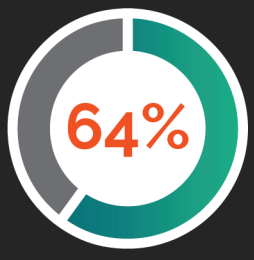
Average number of breach records per company in this sector: 71,381

9,968,945

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 398,758



PASSWORD REUSE RATE

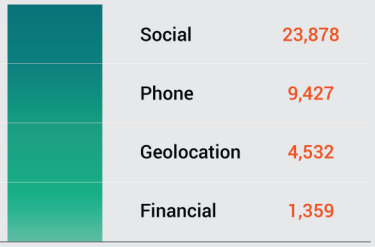
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

5,749,201

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 229,968



366,923

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

14,677 Average number of exposed credentials per company

2,638 Exposed C-level executives

829 Malware-infected employees

INFOGRAPHIC

2022 Industrials Sector Exposure

SpyCloud

52 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Construction and Farm Machinery
Electronics, Electrical Equipment
Industrial Machinery
Miscellaneous

8,033

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

5,638,047

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

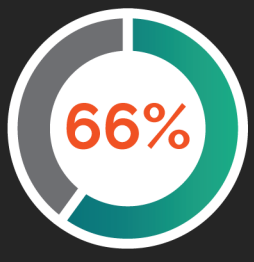
Average number of breach records per company in this sector: 108,424

28,421,603

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 546,569



PASSWORD REUSE RATE

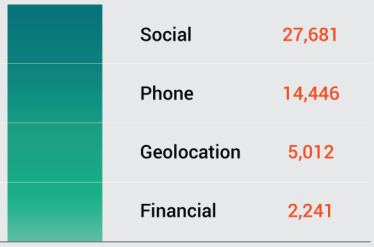
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

15,611,978

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 300,230



1,307,875

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

25,151 Average number of exposed credentials per company

5,956 Exposed C-level executives

2,910 Malware-infected employees

INFOGRAPHIC

2022 Materials Sector Exposure

SpyCloud

44 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Building Materials, Glass
- Forest and Paper Products
- Metals
- Miscellaneous
- Packaging
- Containers

3,618

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,491,603

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

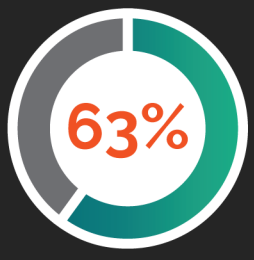
Average number of breach records per company in this sector: 33,900

8,339,117

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 189,525



PASSWORD REUSE RATE

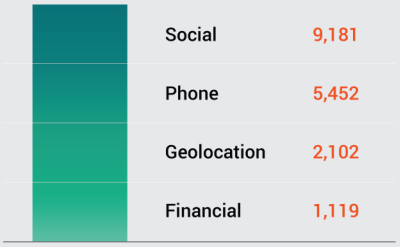
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

4,912,063

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 111,638



242,085

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

5,502 Average number of exposed credentials per company

2,370 Exposed C-level executives

546 Malware-infected employees

INFOGRAPHIC

2022 Media Sector Exposure

SpyCloud

27 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Entertainment • Publishing • Printing

4,644

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

3,123,364

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

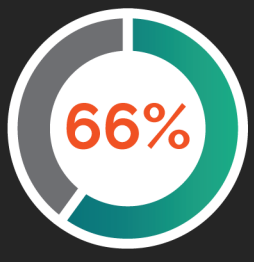
Average number of breach records per company in this sector: 115,680

13,804,140

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 511,264



PASSWORD REUSE RATE

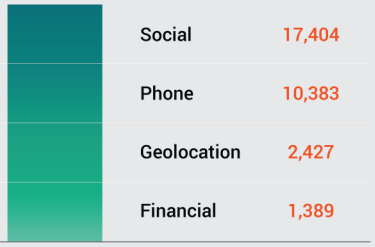
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

5,160,124

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 191,116



1,608,749

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

59,583 Average number of exposed credentials per company

2,333 Exposed C-level executives

2,579 Malware-infected employees

INFOGRAPHIC

2022 Motor Vehicles & Parts Sector Exposure

SpyCloud

21 COMPANIES FROM THE MOTOR VEHICLES & PARTS SECTOR

5,099

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,860,465

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

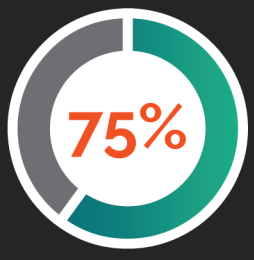
Average number of breach records per company in this sector: 88,594

10,970,560

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 522,408



PASSWORD REUSE RATE

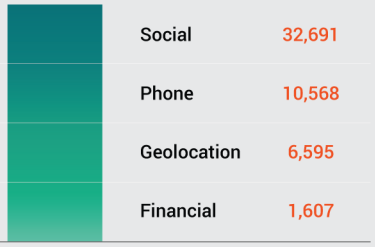
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

6,451,307

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 307,205



383,087

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

18,242 Average number of exposed credentials per company

2,059 Exposed C-level executives

1,575 Malware-infected employees

INFOGRAPHIC

2022 Retail Sector Exposure

SpyCloud

73 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Automotive Retailing, Services
- General Merchandisers
- Internet Services and Retailing
- Specialty Retailers: Apparel
- Specialty Retailers: Other
- Wholesalers: Electronics and Office Equipment

4,746

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

15,416,209

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

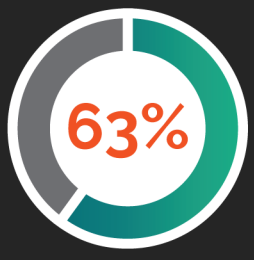
Average number of breach records per company in this sector: 211,181

95,218,309

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 1,304,360



PASSWORD REUSE RATE

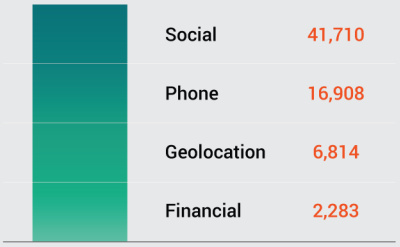
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

68,930,495

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 944,253



872,138

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

11,947 Average number of exposed credentials per company

11,207 Exposed C-level executives

4,135 Malware-infected employees

INFOGRAPHIC

2022 Technology Sector Exposure

SpyCloud

120 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Computer Software
- Computers, Office Equipment
- Information Technology Services
- Internet Services and Retailing
- Network and Other Communications Equipment
- Scientific, Photographic and Control Equipment
- Semiconductors and Other Electronic Components

13,915

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

26,735,026

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

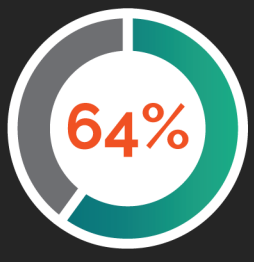
Average number of breach records per company in this sector: 222,792

139,267,855

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 1,160,565



PASSWORD REUSE RATE

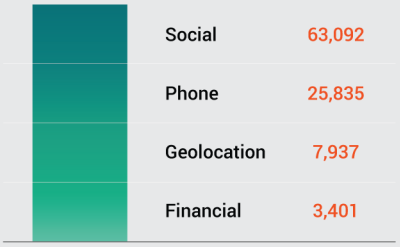
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

70,390,955

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 586,591



7,071,515

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

58,929 Average number of exposed credentials per company

16,482 Exposed C-level executives

34,078 Malware-infected employees

INFOGRAPHIC

2022 Telecommunications Sector Exposure

SpyCloud

10 COMPANIES FROM THE TELECOM SECTOR

6,974

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

13,567,951

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

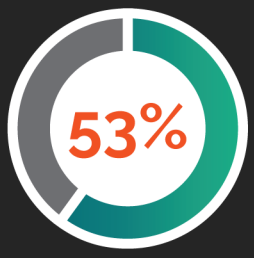
Average number of breach records per company in this sector: 1,356,795

59,702,255

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 5,970,226



PASSWORD REUSE RATE

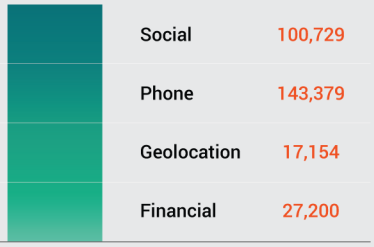
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

27,460,853

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 2,746,085



6,354,314

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

635,431 Average number of exposed credentials per company

2,356 Exposed C-level executives

4,584 Malware-infected employees

INFOGRAPHIC

2022 Transportation Sector Exposure

SpyCloud

36 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Airlines
- Mail, Package, and Freight Delivery
- Railroads
- Shipping
- Transportation and Logistics
- Transportation Equipment
- Trucking, Truck Leasing

5,235

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

3,326,399

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

Average number of breach records per company in this sector: 92,400

18,207,246

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 505,757

PASSWORD REUSE RATE

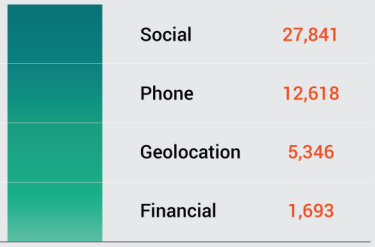
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

10,577,628

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 293,823



588,843

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

16,357 Average number of exposed credentials per company

4,499 Exposed C-level executives

1,702 Malware-infected employees

INFOGRAPHIC

2022 Wholesale Sector Exposure

SpyCloud

30 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Wholesalers: Diversified
Wholesalers: Electronics and Office Equipment
Wholesalers: Food and Grocery

3,056

TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,454,898

TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets.

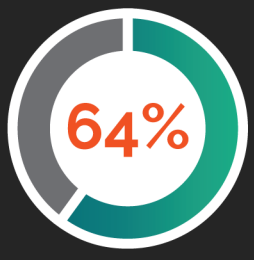
Average number of breach records per company in this sector: 48,497

8,053,724

TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 268,457



PASSWORD REUSE RATE

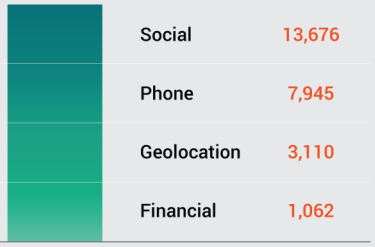
A metric that measures the number of employees using the same exposed plaintext password across multiple sites, divided by the number of all employees with exposed passwords.

4,756,602

TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, phone numbers, social security numbers, social handles, and more.

Average PII Assets per Company: 158,553



243,585

TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.

8,120 Average number of exposed credentials per company

2,931 Exposed C-level executives

514 Malware-infected employees

SpyCloud

Your Plan of Action

SpyCloud's analysis of Fortune 1000 companies' exposure of third-party breaches has revealed more than 687.23 million breach assets in criminals' hands, 27.36 million of which are plaintext passwords tied to Fortune 1000 company employees. Combined with high rates of password reuse, these exposures represent significant cyber risks for these organizations and the companies and consumers doing business with them.

To defend against account takeover, malware, ransomware and other malicious cyberattacks, Fortune 1000 companies 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 minimize 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 multi-factor authentication on critical accounts, and mandate the use of password managers, as well as leverage continuous, actionable intelligence into their users' exposure – especially in industries entrusted with a vast amount of sensitive consumer data.

Essentially the enterprise must protect users from themselves. But breaking bad cyber hygiene habits is an uphill battle. The most effective way to minimize your exposure is by using data from the criminal underground against the adversaries. This data adds an advanced layer of protection by helping you understand your riskiest users (such as those with stolen device fingerprints due to a malware infection) and take corrective action before criminals can exploit that data.

About SpyCloud

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Our products leverage a proprietary engine that collects, curates, enriches, and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. Our 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 10 largest global enterprises, midsize companies, and government agencies around the world. Headquartered in Austin, Texas, SpyCloud is home to over 150 cybersecurity experts who aim to make the internet a safer place.

Enterprise Protection

Learn More

Consumer Fraud Protection

Learn More

Cybercrime Investigations

Learn More

Data Partnerships

Learn More

Learn more at **spycloud.com**

SpyCloud