SpyCloud

FORTUNE 1000 IDENTITY EXPOSURE REPORT 2023

SpyCloud

TABLE OF CONTENTS

OVERVIEW

The number of exposed identities continues to soar every year, providing cybercriminals with new opportunities to monetize stolen data in lucrative ways. With digital identities now a ubiquitous part of employees' lives, keeping up with the evolving threat tactics is more critical than ever for any organization – yet increasingly challenging, despite hefty investments in security and anti-fraud measures. To understand how exposed employee identities impact organizations, SpyCloud combs through our entire database of assets recaptured from the criminal underground every year and analyzes the darknet exposure of employees of large enterprises on the Fortune 1000 list.

While stolen credentials have long been malicious actors' favorite pathway for infiltrating organizations and perpetrating fraud and other crimes, we have been observing a new development in recent years: they are moving from using "traditional" breach databases and combo lists toward credentials and other authentication data stolen by malware. What makes this tactic a favorite for cybercriminals is its extremely high return on investment – malware-exfiltrated data is not only abundant, but it's incredibly fresh and accurate, increasing the success rate for follow-on attacks.

In response to this shift, the trends observed by SpyCloud researchers in this year's annual Fortune 1000 Identity Exposure Report have evolved as well, and 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 **2.27 billion breach and malware-exfiltrated assets** in our database that are tied directly to Fortune 1000 employee accounts and were recaptured from the criminal underground over the course of 2022.

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@acme.com, we were able to associate the resulting breach record to their employer.

In this report, we 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'S DATA

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

For the purposes of this report, it is important to understand how SpyCloud differentiates third-party breach data from malware data. Data breaches occur when information is stolen through unauthorized access to a network or system, typically exposing credentials and personally identifiable information (PII). Individuals are exposed in those breaches through no fault of their own. SpyCloud recaptures this data from darknet sources and notifies businesses when their employees or consumers are identified through our analysis as exposed, requiring remediation on stolen passwords or extra scrutiny on suspicious transactions.

What we call malware 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 have not improved, with the financials sector struggling the most.

Password reuse continues to be rampant among Fortune 1000 employees. We found a **62% password reuse rate** among Fortune 1000 employees that have been exposed more than once. This is only 2 points lower than last year – not much of an improvement. We see this trend at Fortune 1000 enterprises every year, indicating that most user education and training falls on employees' deaf ears. The industry that carries the torch as the worst offender in this category is financials (68% password reuse rate), which is alarming considering the kind of sensitive data consumers entrust to financial institutions that can impact not only the individual, but also opens the door for wider fraud opportunities.

2. Despite the rise in malware, exposure from data breaches has steadily inclined – especially in retail.

Exclusive of malware-exfiltrated data, we have recaptured **132.43 million breach records** associated with Fortune 1000 employees, a 4.6% increase from 2021. This amounts to **725.63 million breach assets (individual data points)**, a 5.6% increase compared to last year. The technology, financials, and retailing sectors are leading with the highest numbers of total breach assets. Retailing, in particular, stood out: it's also in the top three industries for the average number of breach records per company (197,205) and the average number of assets per company (nearly 1.22 million).

3. Cybercriminals are doubling down on malware.

Among the **171,528 malware-infected employees** tied to Fortune 1000 companies and **31 million malware-infected customers** of these companies that we detected, a whopping **1.87 billion cookie records** have been exfiltrated from infected devices. With stolen cookies, criminals can perform session hijacking of active sessions without the need for credentials and can bypass MFA. The exposure stemming from this insidious tactic appears to have spiraled out of control, and cybercriminals are only getting started. Infostealers – malware designed specifically for stealing all manner of personal, authentication, and system data – are quickly growing in popularity, as are underground marketplaces that cater to malicious actors like initial access brokers (IABs), who use infostealers to deliver access to ransomware operators.

Technology has the highest number of infected employees (67,723) across 119 companies, but no industry is immune to malware infections, and the access cybercriminals can gain to confidential and valuable systems and assets is scary at many levels. The breakdown of the four sectors rounding out the top five for the highest number of infected employees includes:

- **Financials:** In second place behind technology with 15,274 infected employees across 167 companies, a nearly 300% increase year-over-year.
- **Retailing:** In third place with 11,950 malware-infected employees across 81 companies.
- **Health Care:** Not far behind with 9,884 malware-infected employees across 76 companies.
- **Telecommunications:** In fifth place with more than 8,000 infected employees across the 9 companies on the Fortune 1000 list.

4. Cybercriminals hit the jackpot with session cookies, especially in technology, retailing, and business services.

Of all malware-exfiltrated authentication data, browser session cookies are the most prized. Each cookie allows a cybercriminal to become a legitimate user's clone and bypass authentication to seamlessly hijack a session. As mentioned, we recaptured **1.87 billion malware cookie records** last year, with the lion's share coming from technology (1.51 billion), followed by retailing (200.12 million) and business services (61.70 million). With these tokens in hand, bad actors can gain unfettered access to an enterprise's network and masquerade as a legitimate user to launch harmful cyber attacks including ransomware, access sensitive data, and perpetrate fraud. 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.

5. PII exposure is growing, with technology, financials, and retailing maintaining their lead.

Exposed PII puts organizations at risk by arming cybercriminals with data to use in social engineering, phishing schemes, and the development of synthetic identities to perpetrate fraud. Technology and financials remained in the top spots among sectors with the most PII exposure last year, albeit they swapped places. With 77.41 million PII assets exposed, technology bumped financials (74.61 million) down a notch in terms of the most PII-exposed industries, while retailing maintained third place with 71.39 million PII assets. Each of these industries saw growth in exposure from 2021, while overall, the total number of PII assets exposed across all industries, **423.28 million**, represents a 7% increase year-over-year. Retailing and technology also have the second- and third-highest number of average PII assets exposed per company (881,360 and 650,499 respectively). The leader in this latter category, telecommunications, also repeated the previous year's feat: with an average of 3.21 million exposed PII assets per company, the sector far surpasses the average of 423,277 across all industries.

6

6. Password hygiene leaves much to be desired.

Just like with our findings about password reuse rates, our list of the top recaptured passwords shows that despite emphasis on employee security awareness and training, habits are not changing. We saw a recurring theme, with “password” and “123456” as the most common recaptured plaintext passwords, but also noted a new trend: a lot of first names in the top 100 exposed passwords list. This finding aligns with the 7 million passwords recaptured across our entire database in 2022 containing the words love, family, kids, wife, husband, and boyfriend. This indicates, perhaps, that Fortune 1000 employees, like many of us, were a bit more sentimental last year after surviving two brutal years of pandemic chaos. Regardless of their reasons for using names in their passwords, employees are putting their companies in danger by choosing passwords that cybercriminals can easily guess after casually perusing social media.

SpyCloud

AT-A-GLANCE:
FORTUNE 1000 IDENTITY EXPOSURE

TOTAL BREACH SOURCES

19,661

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

TOTAL CORPORATE BREACH RECORDS

132,429,971

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

725,634,806

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

TOTAL SESSION COOKIE RECORDS

1,865,557,005

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 simulate 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

27,475,565

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.

TOTAL C-LEVEL EXECUTIVES EXPOSED

87,741

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

PASSWORD REUSE

62%

Among the Fortune 1000 employees, this is the rate at which a password was exposed more than once compared to the total exposed passwords for Fortune 1000 employees. This includes exact passwords and slight variations that criminals can easily match.

MALWARE-INFECTED EMPLOYEES

171,528

Fortune 1000 employees whose data appears in logs exfiltrated from infostealer malware-infected devices. These high-severity exposures put them at risk of ATO and fraud, and make 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 **27.48 million pairs of credentials** with Fortune 1000 corporate email addresses and plaintext passwords. Similar to last year, the three sectors with the highest exposure by far are technology (7.52 million), telecommunications (6.34 million), and financials (3.64 million). While the high numbers for financials and technology may be partially due to the sector size (167 and 119 companies, respectively), the telecommunications sector's exposure is extreme given it only includes nine enterprises.

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, 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 organization's C-suite. Cybercriminals target C-suite executives and senior leaders to attempt account takeover and business email compromise (BEC) fraud. These scams cost enterprises an enormous amount: according to the FBI, total BEC losses in 2022 reached **$2.7B from nearly 22,000 complaints**.

In our dataset, we found **935,786 stolen assets from 87,741 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, passwords associated with corporate accounts 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 a 90-day password rotation) may even encourage bad habits.

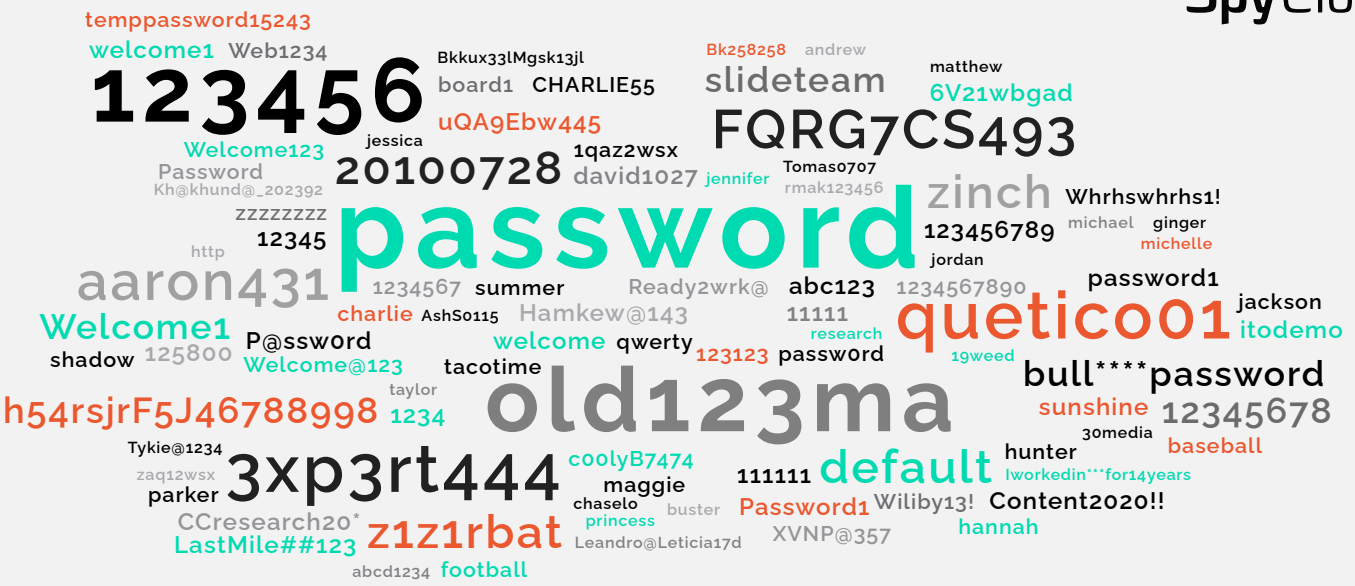
FORTUNE 1000 SECTOR	NUMBER OF COMPANIES	TOTAL EXPOSED CORPORATE CREDENTIALS	AVG CORPORATE CREDENTIALS PER COMPANY
AEROSPACE & DEFENSE	17	668,004	39,294
APPAREL	16	152,867	9,554
BUSINESS SERVICES	51	501,545	9,834
CHEMICALS	29	331,267	11,423
ENERGY	101	832,946	8,247
ENGINEERING & CONSTRUCTION	32	271,454	8,483
FINANCIALS	167	3,641,651	21,806
FOOD & DRUG STORES	9	53,233	5,915
FOOD, BEVERAGES & TOBACCO	34	275,568	8,105
HEALTH CARE	76	1,543,853	20,314
HOTELS, RESTAURANTS & LEISURE	25	485,664	19,427
HOUSEHOLD PRODUCTS	26	388,691	14,950
INDUSTRIALS	50	1,233,537	24,671
MATERIALS	46	247,665	5,384
MEDIA	28	730,323	26,083
MOTOR VEHICLES & PARTS	19	541,008	28,474
RETAILING	81	908,630	11,218
TECHNOLOGY	119	7,518,582	63,181
TELECOMMUNICATIONS	9	6,366,177	704,020
TRANSPORTATION	35	598,535	17,101
WHOLESALERS	30	214,365	7,146

PASSWORD REUSE:
WORST OFFENDERS BY SECTOR

Our analysis found a **62% average reuse rate last year, only a 2 point decrease from 2021 and a 10 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 – we can't tell for sure without checking their actual work passwords. However, password reuse across their third-party breach and malware-exposed accounts does provide an indication of employees' overall password hygiene.

FORTUNE 1000 SECTOR	AVERAGE PASSWORD REUSE
FINANCIALS	68%
MOTOR VEHICLES & PARTS | TRANSPORTATION	67%
FOOD & DRUG STORES | INDUSTRIALS	66%
AEROSPACE & DEFENSE | RETAILING	65%
ENGINEERING & CONSTRUCTION | MEDIA | MATERIALS HOUSEHOLD PRODUCTS	64%
CHEMICALS | FOOD, BEVERAGES & TOBACCO | HEALTH CARE	63%
APPAREL | BUSINESS SERVICES	62%
ENERGY	61%
TECHNOLOGY	60%
TELECOMMUNICATIONS	59%
WHOLESALERS | HOTELS, RESTAURANTS & LEISURE	55%



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 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. Most of the passwords above 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 – and very prominent – 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.

DATA SIPHONED BY MALWARE

The Danger of Infected Employees

With the growing focus of criminals to leverage hard-to-detect measures like 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 from the infected device, including browser history, autocomplete data, session cookies, screenshots, system information, crypto addresses, target URLs, and login credentials. This type of malware poses a significant threat because not only does it harvest 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 realize that credentials available on the criminal underground are just as likely to come from infostealers as they are from large data breaches – across our entire dataset, we recaptured 27.48 million exposed credentials belonging to Fortune 1000 employees from the criminal underground and nearly **340,000 of those came from malware logs**. High-value information stolen through malware infections is typically shared in small circles or sold at a premium to ransomware operators.

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 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 managed devices or personal/unmanaged devices to access the corporate network or work applications.

Like last year, the **technology sector** once again leads all industries for the number of infected employees from Fortune 1000 companies with **67,723**, which represents **39.5%** of all those observed in our database. **Financials**, **retailing**, **health care**, and **telecommunications** also maintained their lead to round out the top five sectors with infected employees in our findings.

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 use this information to bypass multi-factor authentication, log into corporate networks, steal sensitive data, authorize fraudulent transactions, and more.

In our view, ransomware is a malware problem. Often, bad actors use information or access which was gathered through malware infections as the basis for ransomware attacks. Attackers are exploiting infected systems to exfiltrate data that can aid an attack, identify potential entry points to corporate resources, and deliver executable files.

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 in criminals' hands and continue to put the organization and individual at further risk unless proper post-infection remediation steps are taken.

Additionally, **we recaptured a total of 223,098 credential pairs exfiltrated by malware that specifically allow access to over 56,000 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, their exposure is a blind spot for most enterprise security teams.

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 organizations, 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 close to 2 billion stolen session cookie records tied to employees and consumers of Fortune 1000 companies 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. 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 nearly **30.75 million infected consumers** of Fortune 1000 services, representing a 6.4% increase from 2021.

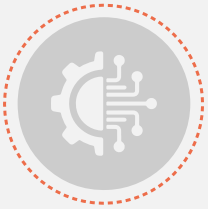
These are users of Fortune 1000 consumer-facing sites where our recaptured data shows that they were infected while entering their username and password on the login page (e.g., jim@example.com was infected while logging into signin.fortune1000company.com).

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 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.

Industries with the Most Malware-Infected Consumers



TECH

Over 13.22 MILLION malware-infected consumers:
While tech is the industry with the largest malware exposure this year, the 35% decline from last year is due to the ebb and flow of organizations included in the annual Fortune list.

MEDIA

+49%

Nearly 6 MILLION:
Almost double the previous year's 2.9 million.

RETAILING

+56%

5.88 MILLION:
More than double 2.56 million in 2021.

BUSINESS SERVICES

+49%

4.04 MILLION:
Almost double 2.15 million in 2021.

FINANCIALS

+794%

551,879:
Almost 8x the previous year's 61,735.

The increase in the financials sector is astonishing, yet it reflects global identity cyber threats and fraud trends. In recent years, synthetic identity fraud (the mixing of stolen and fake identity data from multiple consumers) has become **the largest form** of identity theft. The massive amount of consumers' personally identifiable information (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.

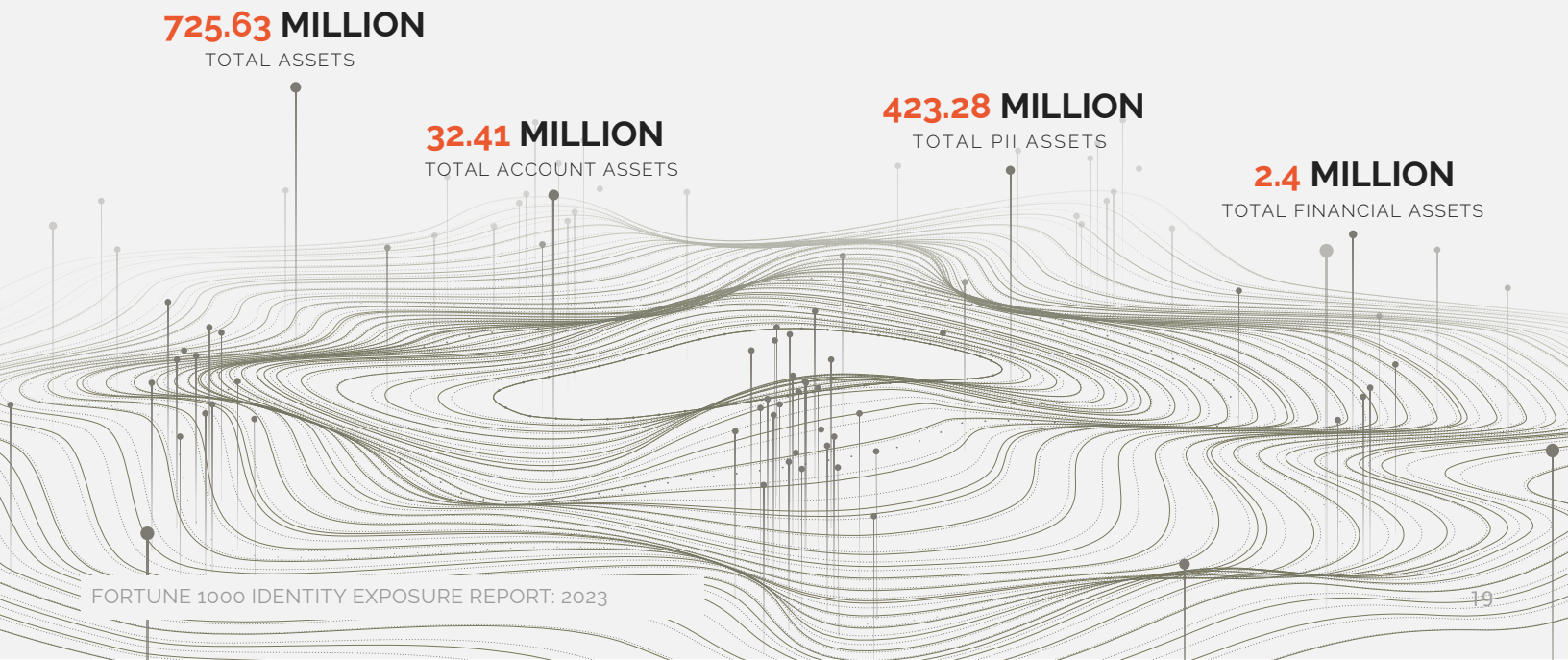
FORTUNE 1000 SECTOR	MALWARE-INFECTED EMPLOYEES	MALWARE-INFECTED CONSUMERS
AEROSPACE & DEFENSE	1,431	1,690
APPAREL	1,585	219,092
BUSINESS SERVICES	5,608	4,038,028
CHEMICALS	2,289	5,848
ENERGY	6,810	37,224
ENGINEERING & CONSTRUCTION	2,425	10,715
FINANCIALS	15,274	551,879
FOOD & DRUG STORES	893	81,631
FOOD, BEVERAGES & TOBACCO	4,002	49,219
HEALTH CARE	9,884	59,524
HOTELS, RESTAURANTS & LEISURE	3,175	150,860
HOUSEHOLD PRODUCTS	2,510	54,186
INDUSTRIALS	6,111	32,153
MATERIALS	2,747	1,209
MEDIA	6,478	5,997,678
MOTOR VEHICLES & PARTS	4,765	41,647
RETAILING	11,950	5,876,758
TECHNOLOGY	67,723	13,222,813
TELECOMMUNICATIONS	8,015	197,874
TRANSPORTATION	5,261	110,317
WHOLESALERS	2,592	8,045

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 more than **725.63 million breach assets** and **1.87 billion malware-exfiltrated session cookie records** tied to Fortune 1000 employees last 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)

PII

WHAT IT IS

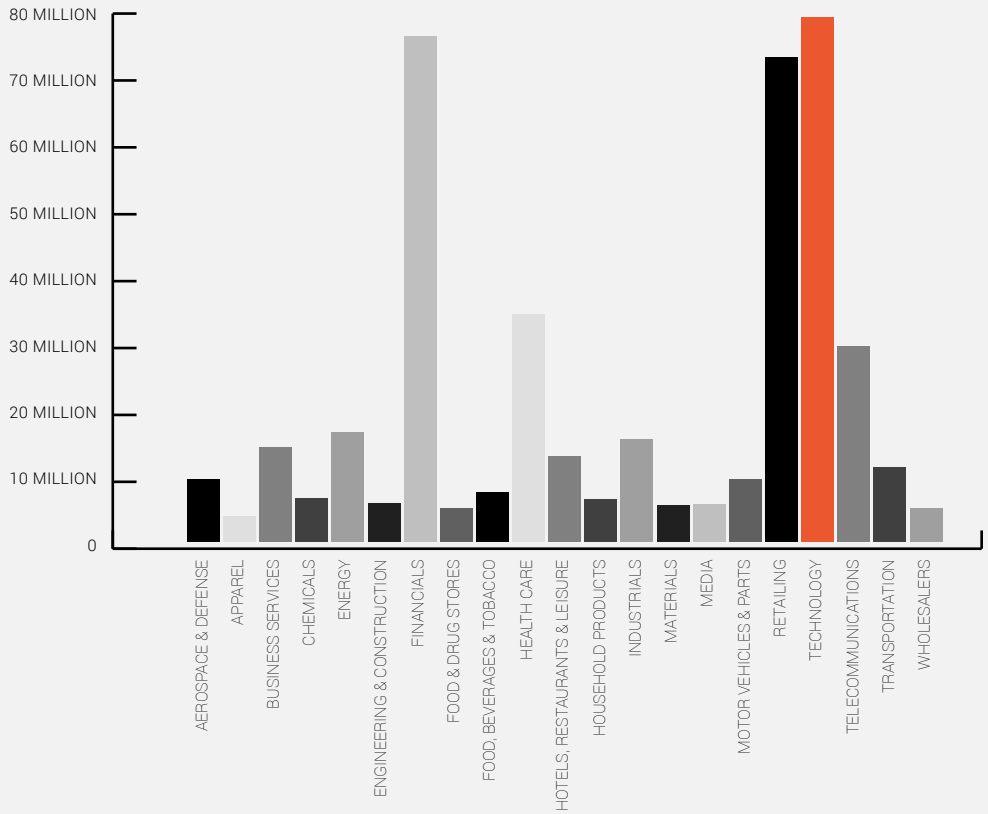
Personally identifiable information (PII) is data that could be used to identify an individual person. For the purposes of this report, SpyCloud has excluded some forms of PII that have been broken out into separate categories below, such as phone and financial assets. However, this category includes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



COOKIES & TOKENS

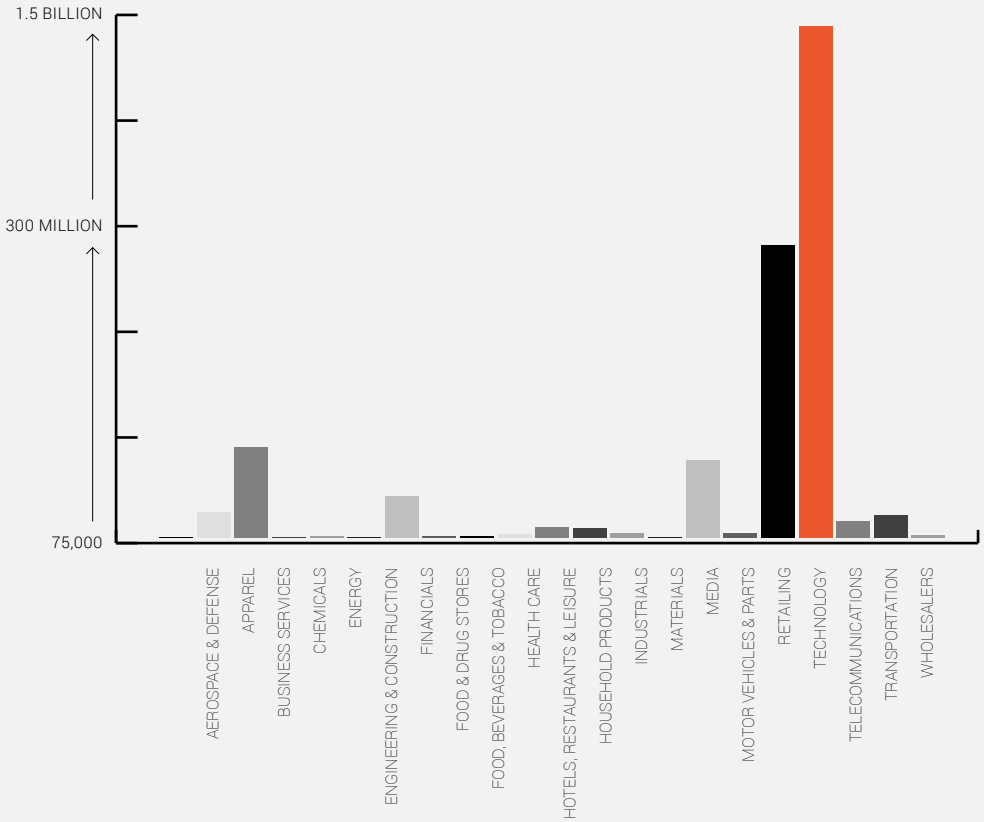
ASSET TYPE:
SESSION COOKIES OR TOKENS

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 organizations 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

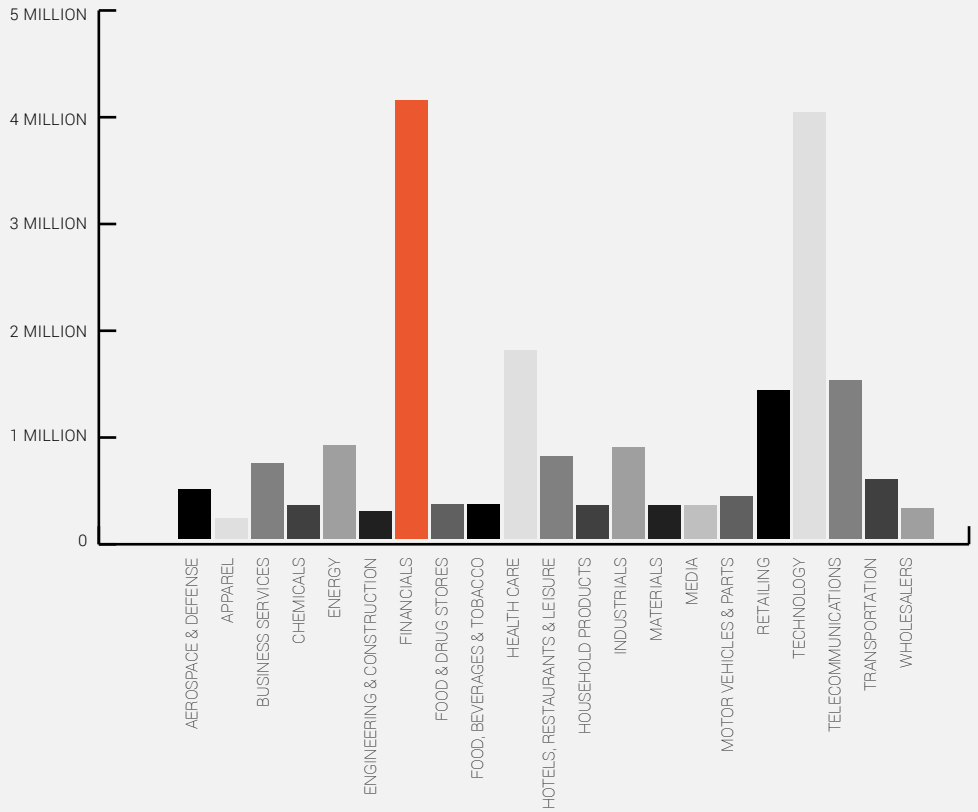
PHONE

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

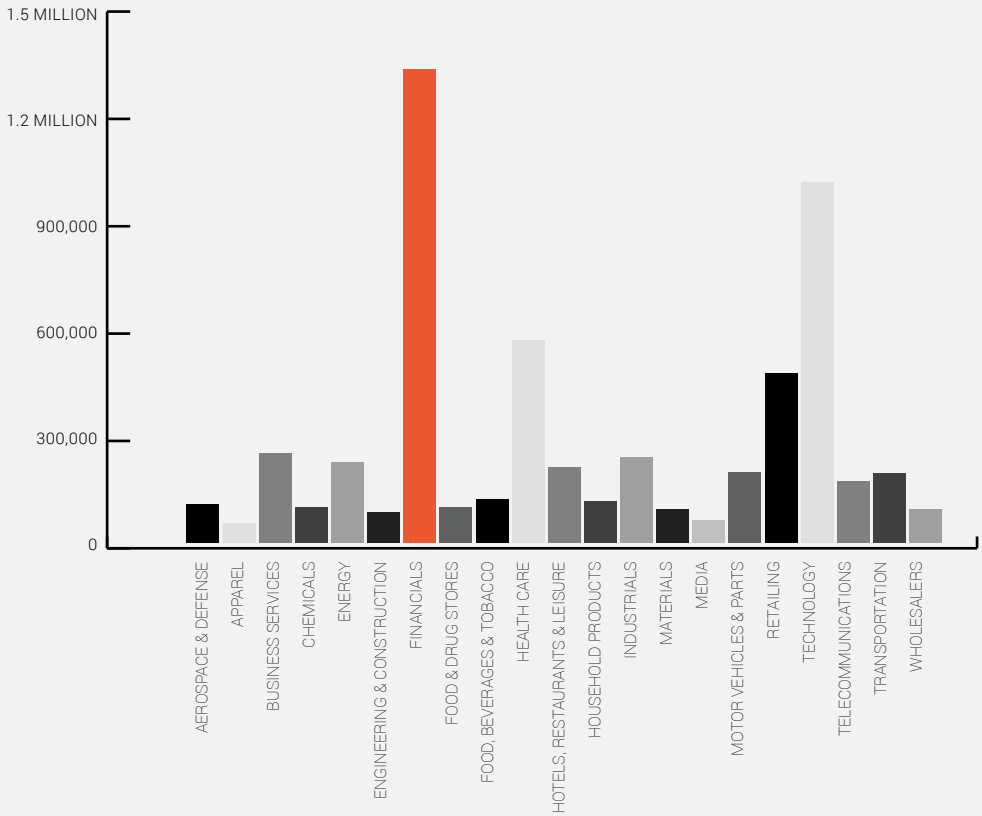
Geolocation assets consist of latitude and longitude pairings that pinpoint users' physical locations. This is typically the location of the IP that a user last logged in from. That location sometimes correlates with their address, but not always, which is why this data has been separated from PII assets.

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



ASSET TYPE:
FINANCIAL

WHAT IT IS

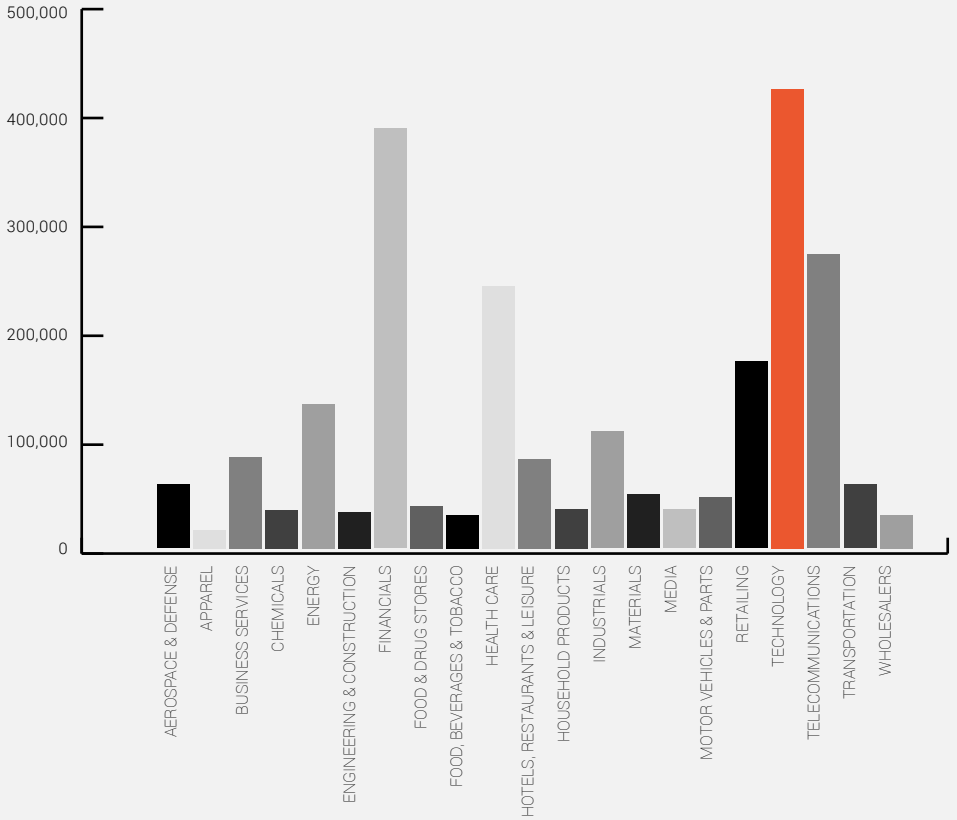
Financial assets include credit card numbers, bank account numbers, and tax IDs. While this information all technically qualifies as PII, we have separated them into their own category due to the severity of the exposure.

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

FINANCIAL



ASSET TYPE:
SOCIAL

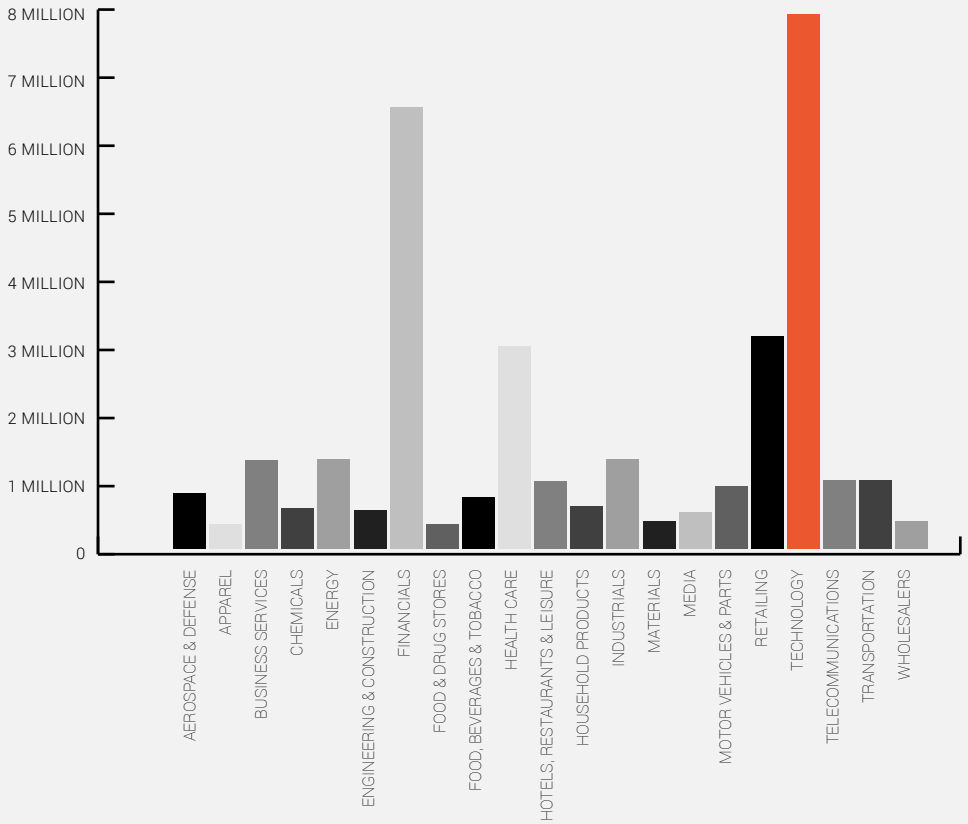
SOCIAL

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.



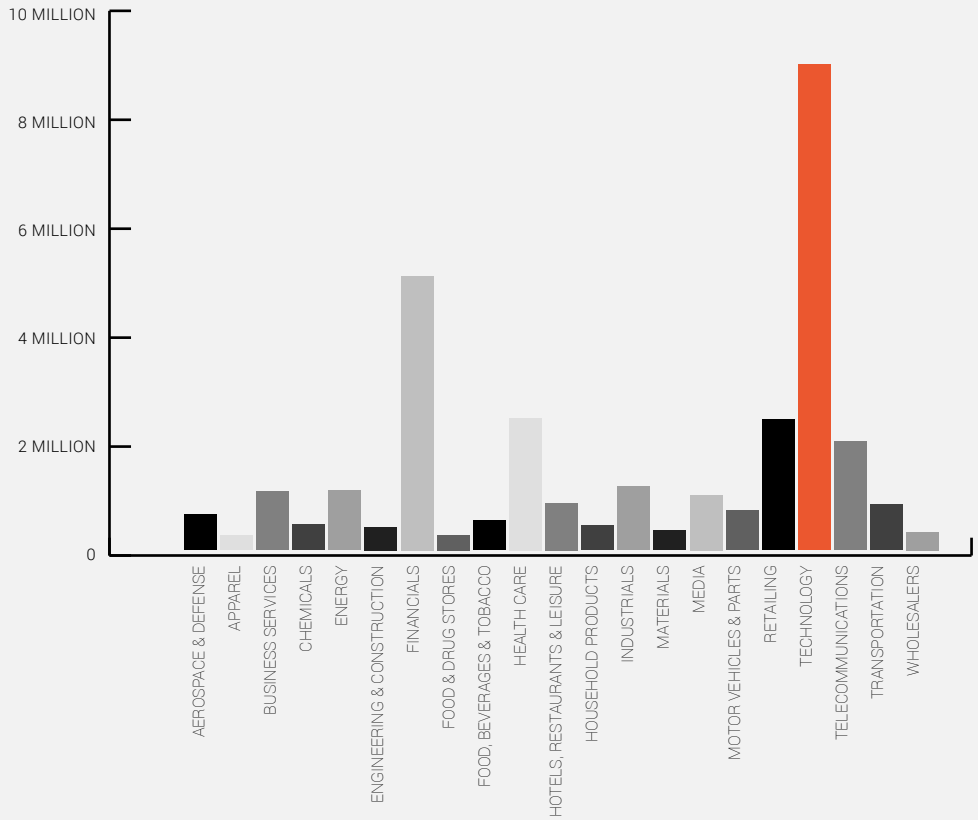
ASSET TYPE:
ACCOUNT

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

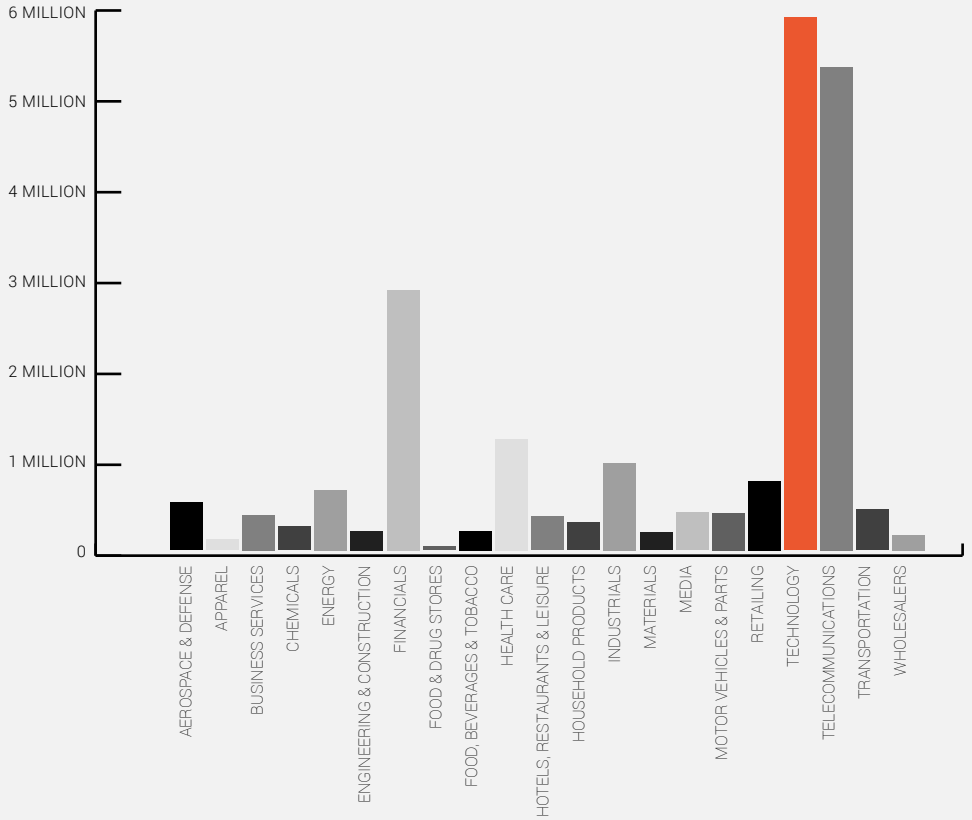
COMBO LIST

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.



SpyCloud

FORTUNE 1000 IDENTITY EXPOSURE BY SECTOR

SpyCloud

AEROSPACE & DEFENSE

17 companies

The companies in this report represent 17 of the largest US companies in the **Aerospace & Defense Industry**.

16,086,095
TOTAL BREACH ASSETS

946,241
AVERAGE # OF BREACH ASSETS **PER COMPANY**

4,154
TOTAL BREACH SOURCES

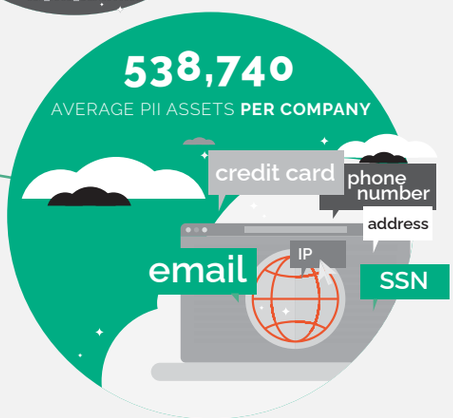
3,061,738
TOTAL BREACH RECORDS

180,102
AVERAGE # OF BREACH RECORDS **PER COMPANY**

65%
PASSWORD REUSE

9,158,578
TOTAL PII ASSETS

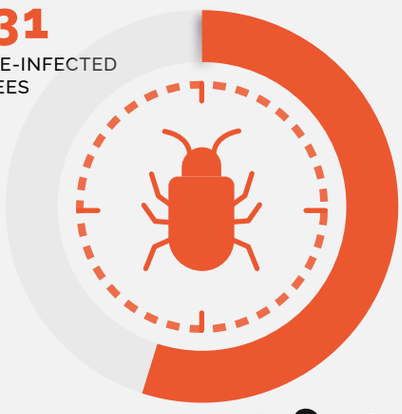
538,740
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

48,011	SOCIAL
39,906	ACCOUNTS
27,013	PHONE
6,319	GEOLOCATION
3,510	FINANCIAL

1,431
MALWARE-INFECTED EMPLOYEES



1,690
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- password
- aaron431

SpyCloud

APPAREL

16
companies

The companies in this report represent 16 of the largest US companies in the **Apparel Industry.**

380,970
AVERAGE # OF BREACH ASSETS **PER COMPANY**

6,095,520
TOTAL BREACH ASSETS

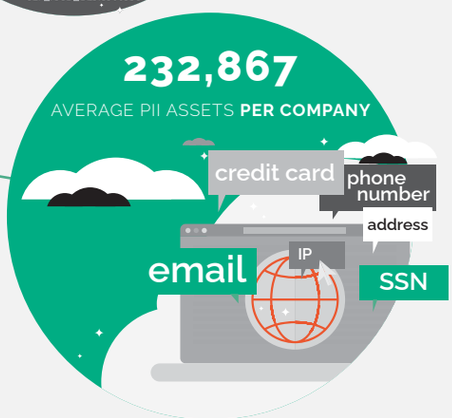
3,044
TOTAL BREACH SOURCES

63,017
AVERAGE # OF BREACH RECORDS **PER COMPANY**

1,008,269
TOTAL BREACH RECORDS

62%
PASSWORD REUSE

232,867
AVERAGE PII ASSETS **PER COMPANY**

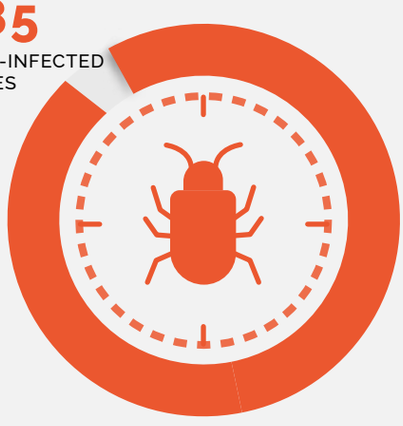


3,725,875
TOTAL PII ASSETS

TYPES OF ASSETS (AVG PER COMPANY)

22,553	SOCIAL
17,103	ACCOUNTS
11,559	PHONE
3,350	GEOLOCATION
1,078	FINANCIAL

1,585
MALWARE-INFECTED EMPLOYEES



219,092
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- newmember
- 123456
- aaron431

SpyCloud

BUSINESS SERVICES

51 companies

The companies in this report represent 51 of the largest US companies in the **Business Services Industry.**

22,831,636
TOTAL BREACH ASSETS

447,679
AVERAGE # OF BREACH ASSETS **PER COMPANY**

5,322
TOTAL BREACH SOURCES

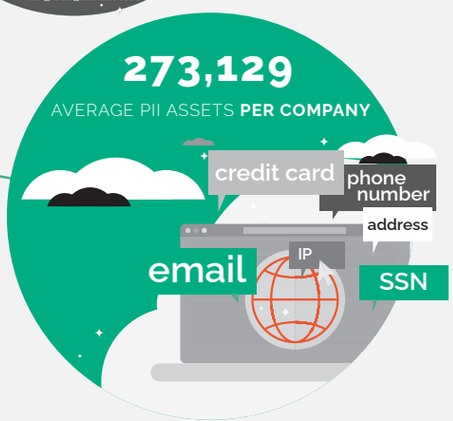
3,761,130
TOTAL BREACH RECORDS

73,748
AVERAGE # OF BREACH RECORDS **PER COMPANY**

62%
PASSWORD REUSE

13,929,574
TOTAL PII ASSETS

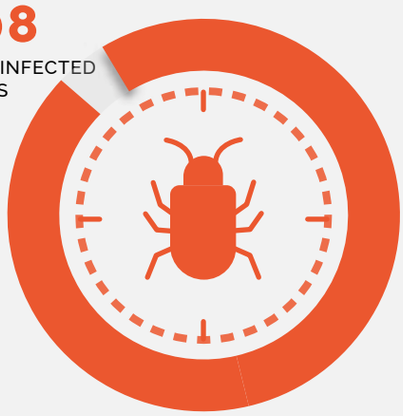
273,129
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

25,524	SOCIAL
21,773	ACCOUNTS
13,533	PHONE
4,861	GEOLOCATION
1,676	FINANCIAL

5,608
MALWARE-INFECTED EMPLOYEES



4,038,028
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- aaron431
- 123456

SpyCloud

CHEMICALS

29
companies

The companies in this report represent 29 of the largest US companies in the **Chemicals Industry.**

10,833,368
TOTAL BREACH ASSETS

373,564
AVERAGE # OF BREACH ASSETS **PER COMPANY**

4,902
TOTAL BREACH SOURCES

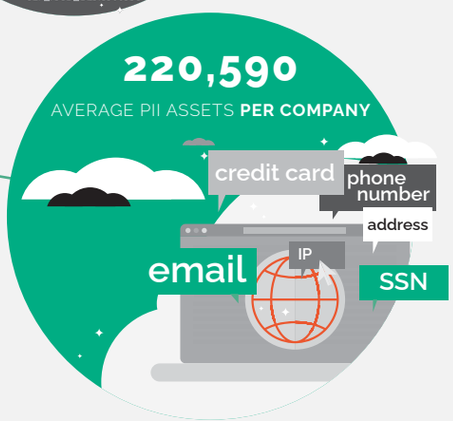
1,944,699
TOTAL BREACH RECORDS

67,059
AVERAGE # OF BREACH RECORDS **PER COMPANY**

63%
PASSWORD REUSE

6,397,111
TOTAL PII ASSETS

220,590
AVERAGE PII ASSETS **PER COMPANY**



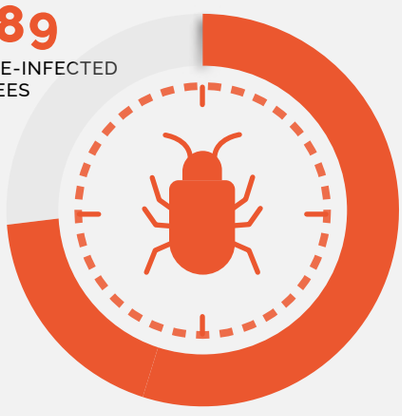
TYPES OF ASSETS (AVG PER COMPANY)

20,681	SOCIAL
16,909	ACCOUNTS
10,689	PHONE
3,390	GEOLOCATION
1,231	FINANCIAL

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- pass1
- password

2,289
MALWARE-INFECTED EMPLOYEES



5,848
MALWARE-INFECTED CONSUMERS

SpyCloud

ENERGY

101
companies

The companies in this report represent 101 of the largest US companies in the **Energy Industry.**

268,661
AVERAGE # OF BREACH ASSETS **PER COMPANY**

27,134,735
TOTAL BREACH ASSETS

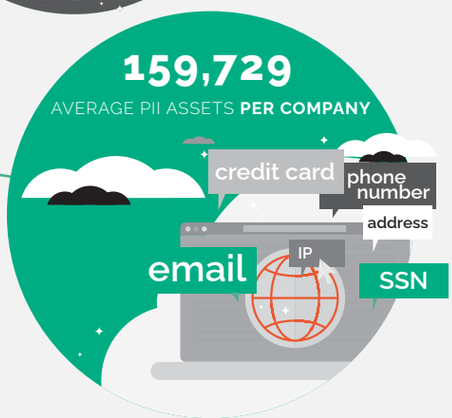
5,761
TOTAL BREACH SOURCES

48,083
AVERAGE # OF BREACH RECORDS **PER COMPANY**

4,856,367
TOTAL BREACH RECORDS

61%
PASSWORD REUSE

159,729
AVERAGE PII ASSETS **PER COMPANY**

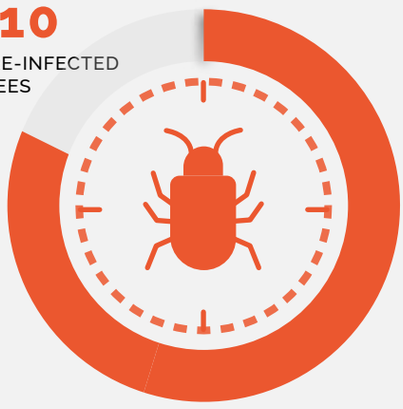


16,132,648
TOTAL PII ASSETS

TYPES OF ASSETS (AVG PER COMPANY)

12,988	SOCIAL
11,154	ACCOUNTS
8,556	PHONE
2,189	GEOLOCATION
1,337	FINANCIAL

6,810
MALWARE-INFECTED EMPLOYEES



37,224
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- 123456
- aaron431

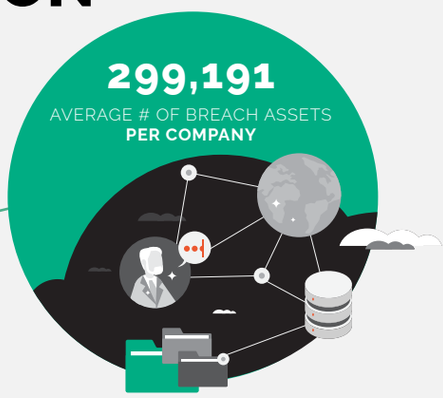
SpyCloud

ENGINEERING & CONSTRUCTION

32
companies

The companies in this report represent 32 of the largest US companies in the **Engineering & Construction Industry.**

9,574,115
TOTAL BREACH ASSETS



3,683
TOTAL BREACH SOURCES

1,753,734
TOTAL BREACH RECORDS

64%
PASSWORD REUSE

5,631,959
TOTAL PII ASSETS

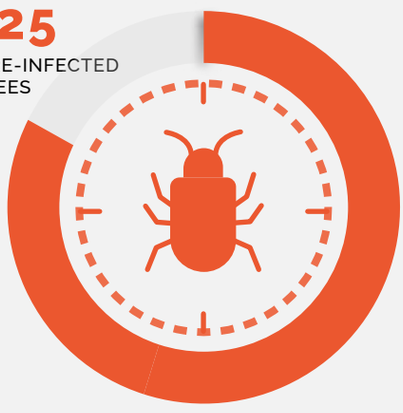
TYPES OF ASSETS (AVG PER COMPANY)

17,524	SOCIAL
13,758	ACCOUNTS
8,008	PHONE
2,625	GEOLOCATION
1,054	FINANCIAL

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- 123456
- *NO-PASSWORD*

2,425
MALWARE-INFECTED EMPLOYEES



10,715
MALWARE-INFECTED CONSUMERS

SpyCloud

FINANCIALS

167 companies

The companies in this report represent 167 of the largest US companies in the **Financials Industry.**

125,031,742
TOTAL BREACH ASSETS

748,693
AVERAGE # OF BREACH ASSETS **PER COMPANY**

8,878
TOTAL BREACH SOURCES

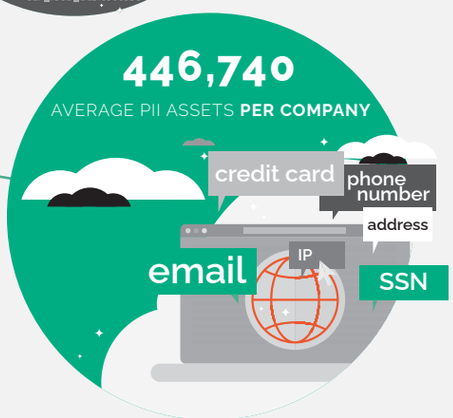
22,137,676
TOTAL BREACH RECORDS

132,561
AVERAGE # OF BREACH RECORDS **PER COMPANY**

68%
PASSWORD REUSE

74,605,649
TOTAL PII ASSETS

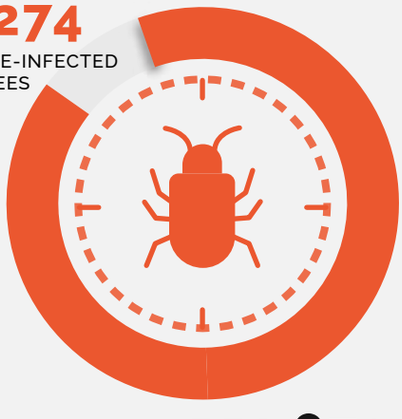
446,740
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

38,654	SOCIAL
31,175	ACCOUNTS
24,126	PHONE
7,820	GEOLOCATION
2,353	FINANCIAL

15,274
MALWARE-INFECTED EMPLOYEES



551,879
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- 456a33
- aaron431

SpyCloud

FOOD & DRUG STORES

9
companies

The companies in this report represent 9 of the largest US companies in the **Food & Drug Stores Industry.**

7,614,599
TOTAL BREACH ASSETS

846,067
AVERAGE # OF BREACH ASSETS **PER COMPANY**

1,345
TOTAL BREACH SOURCES

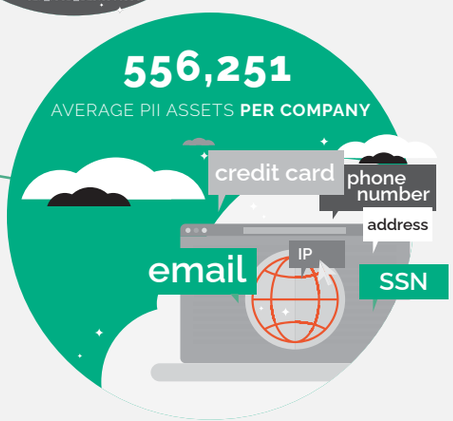
1,137,785
TOTAL BREACH RECORDS

126,421
AVERAGE # OF BREACH RECORDS **PER COMPANY**

66%
PASSWORD REUSE

5,006,257
TOTAL PII ASSETS

556,251
AVERAGE PII ASSETS **PER COMPANY**



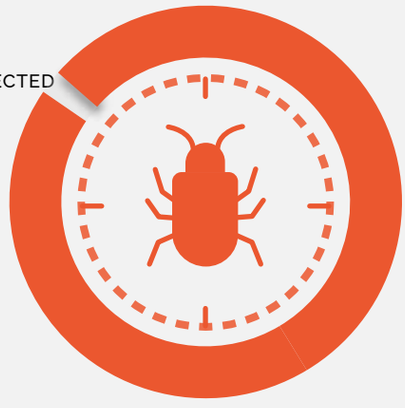
TYPES OF ASSETS (AVG PER COMPANY)

39,143	SOCIAL
31,952	ACCOUNTS
34,754	PHONE
10,981	GEOLOCATION
4,407	FINANCIAL

TOP NOTEWORTHY EXPOSED PASSWORDS

- aaron431
- password
- simply123

893
MALWARE-INFECTED EMPLOYEES



81,631
MALWARE-INFECTED CONSUMERS

SpyCloud

FOOD, BEVERAGES & TOBACCO

34
companies

The companies in this report represent 34 of the largest US companies in the **Food, Beverages, & Tobacco Industry.**

12,065,999
TOTAL BREACH ASSETS

354,882
AVERAGE # OF BREACH ASSETS **PER COMPANY**

4,681
TOTAL BREACH SOURCES

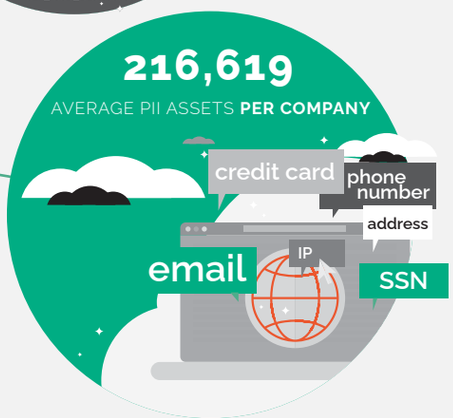
2,018,743
TOTAL BREACH RECORDS

59,375
AVERAGE # OF BREACH RECORDS **PER COMPANY**

63%
PASSWORD REUSE

7,365,049
TOTAL PII ASSETS

216,619
AVERAGE PII ASSETS **PER COMPANY**



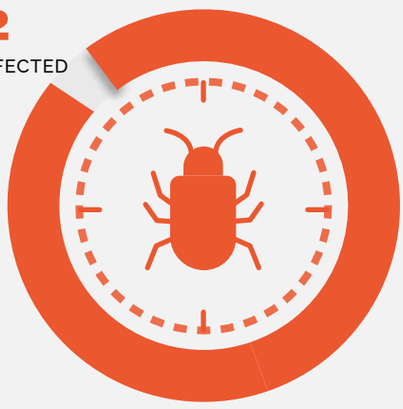
TYPES OF ASSETS (AVG PER COMPANY)

22,068	SOCIAL
16,414	ACCOUNTS
9,401	PHONE
3,526	GEOLOCATION
915	FINANCIAL

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- 123456
- aaron431

4,002
MALWARE-INFECTED EMPLOYEES



49,219
MALWARE-INFECTED CONSUMERS

SpyCloud

HEALTH CARE

76
companies

The companies in this report represent 76 of the largest US companies in the **Health Care Industry.**

56,153,936
TOTAL BREACH ASSETS

738,868
AVERAGE # OF BREACH ASSETS **PER COMPANY**

7,863
TOTAL BREACH SOURCES

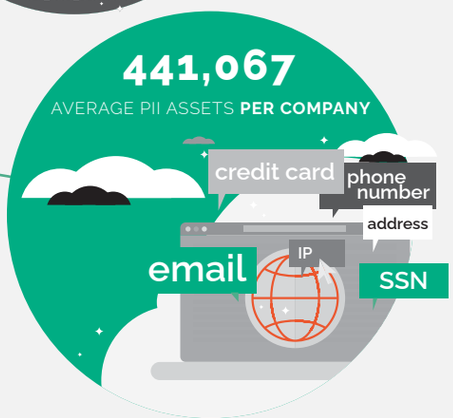
9,702,473
TOTAL BREACH RECORDS

127,664
AVERAGE # OF BREACH RECORDS **PER COMPANY**

63%
PASSWORD REUSE

33,521,121
TOTAL PII ASSETS

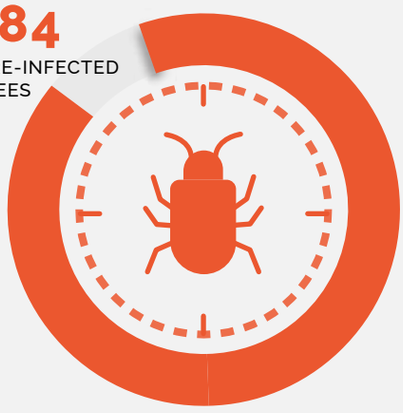
441,067
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

38,957	SOCIAL
33,022	ACCOUNTS
22,823	PHONE
7,625	GEOLOCATION
3,230	FINANCIAL

9,884
MALWARE-INFECTED EMPLOYEES



59,524
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- 123456
- aaron431

SpyCloud

HOTELS, RESTAURANTS & LEISURE

25 companies

The companies in this report represent 25 of the largest US companies in the **Hotels, Restaurants & Leisure Industry.**

20,734,651 TOTAL BREACH ASSETS

829,386 AVERAGE # OF BREACH ASSETS **PER COMPANY**

4,119 TOTAL BREACH SOURCES

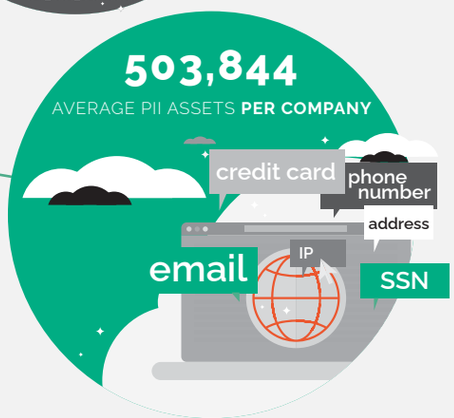
3,568,942 TOTAL BREACH RECORDS

142,758 AVERAGE # OF BREACH RECORDS **PER COMPANY**

55% PASSWORD REUSE

12,596,096 TOTAL PII ASSETS

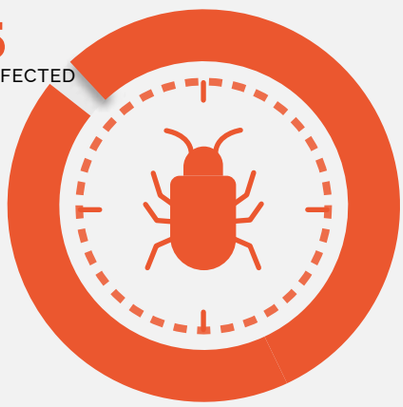
503,844 AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

39,491	SOCIAL
35,692	ACCOUNTS
30,476	PHONE
8,298	GEOLOCATION
3,346	FINANCIAL

3,175 MALWARE-INFECTED EMPLOYEES



150,860 MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- Hello123
- password

SpyCloud

HOUSEHOLD PRODUCTS

26
companies

The companies in this report represent 26 of the largest US companies in the **Household Products Industry.**

10,886,484
TOTAL BREACH ASSETS

418,711
AVERAGE # OF BREACH ASSETS **PER COMPANY**

5,092
TOTAL BREACH SOURCES

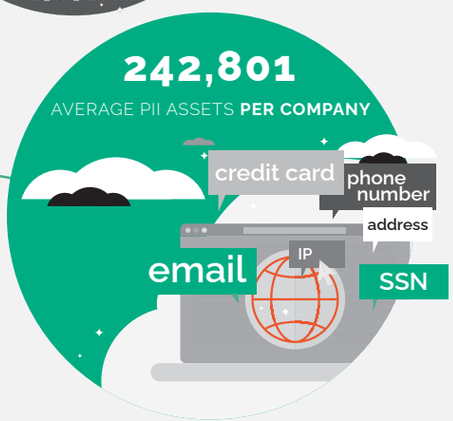
1,937,568
TOTAL BREACH RECORDS

74,522
AVERAGE # OF BREACH RECORDS **PER COMPANY**

64%
PASSWORD REUSE

6,312,836
TOTAL PII ASSETS

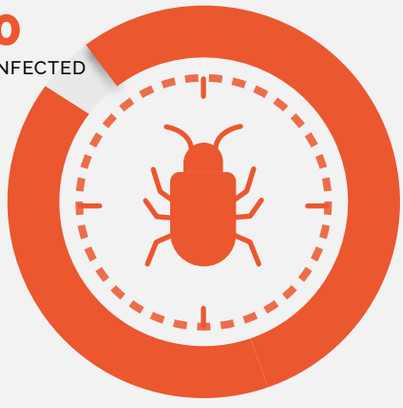
242,801
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

23,658	SOCIAL
18,236	ACCOUNTS
12,013	PHONE
4,410	GEOLOCATION
1,408	FINANCIAL

2,510
MALWARE-INFECTED EMPLOYEES



54,186
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- passport
- 123456
- password

SpyCloud

INDUSTRIALS

50 companies

The companies in this report represent 50 of the largest US companies in the **Industrials Industry.**

27,308,200
TOTAL BREACH ASSETS

546,164
AVERAGE # OF BREACH ASSETS **PER COMPANY**

8,419
TOTAL BREACH SOURCES

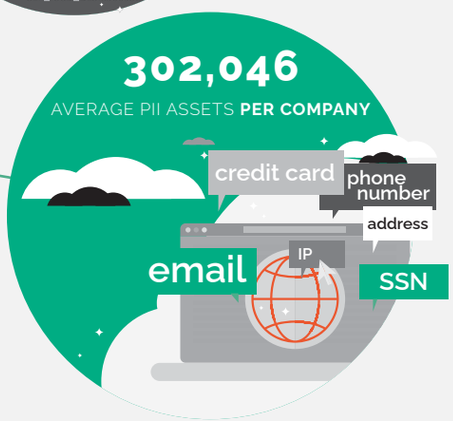
5,371,072
TOTAL BREACH RECORDS

107,421
AVERAGE # OF BREACH RECORDS **PER COMPANY**

66%
PASSWORD REUSE

15,102,307
TOTAL PII ASSETS

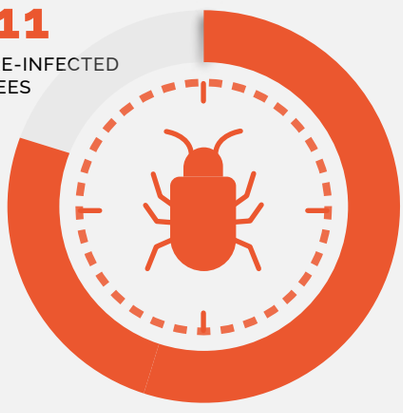
302,046
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

26,221	SOCIAL
24,156	ACCOUNTS
16,816	PHONE
4,698	GEOLOCATION
2,183	FINANCIAL

6,111
MALWARE-INFECTED EMPLOYEES



32,153
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- password
- aaron431

SpyCloud

MATERIALS

46
companies

The companies in this report represent 46 of the largest US companies in the **Materials Industry.**

8,900,584
TOTAL BREACH ASSETS

193,491
AVERAGE # OF BREACH ASSETS **PER COMPANY**

3,928
TOTAL BREACH SOURCES

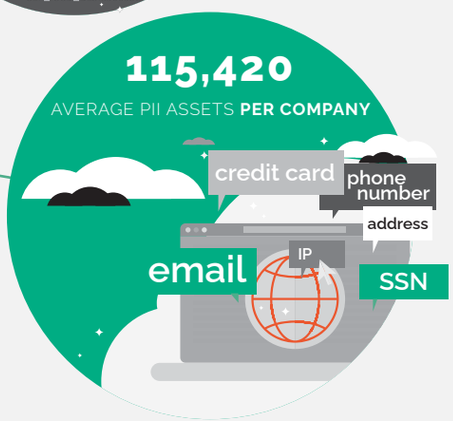
1,562,578
TOTAL BREACH RECORDS

33,969
AVERAGE # OF BREACH RECORDS **PER COMPANY**

64%
PASSWORD REUSE

5,309,328
TOTAL PII ASSETS

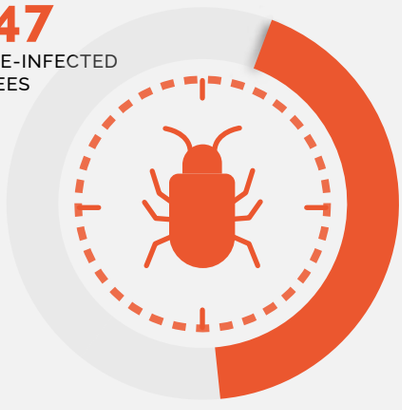
115,420
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

8,680	SOCIAL
8,060	ACCOUNTS
6,693	PHONE
1,986	GEOLOCATION
1,090	FINANCIAL

2,747
MALWARE-INFECTED EMPLOYEES



1,209
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- aaron431
- password
- 123456

SpyCloud

MEDIA

28
companies

The companies in this report represent 28 of the largest US companies in the **Media Industry.**

12,010,540
TOTAL BREACH ASSETS

428,948
AVERAGE # OF BREACH ASSETS **PER COMPANY**

4,603
TOTAL BREACH SOURCES

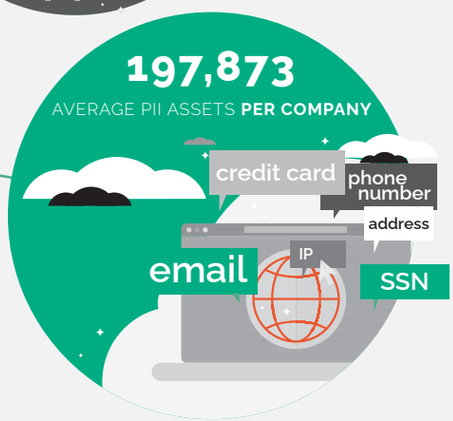
2,309,005
TOTAL BREACH RECORDS

82,464
AVERAGE # OF BREACH RECORDS **PER COMPANY**

64%
PASSWORD REUSE

5,540,447
TOTAL PII ASSETS

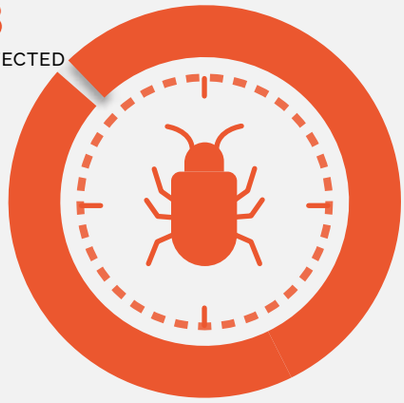
197,873
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

18,981	SOCIAL
37,421	ACCOUNTS
11,004	PHONE
2,184	GEOLOCATION
1,296	FINANCIAL

6,478
MALWARE-INFECTED EMPLOYEES



5,997,678
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- TopSecret123
- 123123123

SpyCloud

MOTOR VEHICLES & PARTS

19
companies

The companies in this report represent 19 of the largest US companies in the **Motor Vehicles & Parts Industry.**

15,614,341
TOTAL BREACH ASSETS

821,807
AVERAGE # OF BREACH ASSETS **PER COMPANY**

5,554
TOTAL BREACH SOURCES

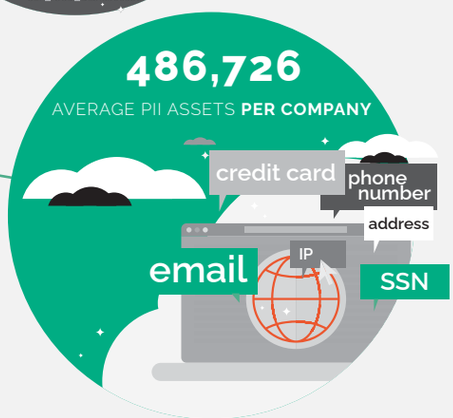
2,638,333
TOTAL BREACH RECORDS

138,860
AVERAGE # OF BREACH RECORDS **PER COMPANY**

67%
PASSWORD REUSE

9,247,801
TOTAL PII ASSETS

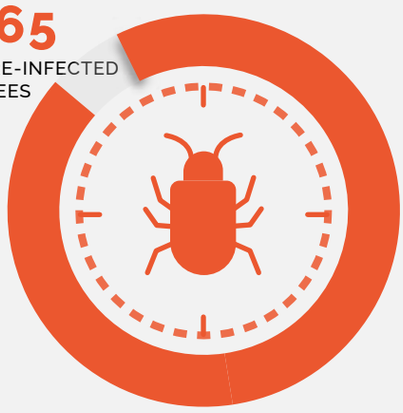
486,726
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

48,314	SOCIAL
39,808	ACCOUNTS
20,408	PHONE
10,161	GEOLOCATION
2,506	FINANCIAL

4,765
MALWARE-INFECTED EMPLOYEES



41,647
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- password
- aaron431

SpyCloud

RETAILING

81
companies

The companies in this report represent 81 of the largest US companies in the **Retailing Industry.**

98,471,298
TOTAL BREACH ASSETS

1,215,695
AVERAGE # OF BREACH ASSETS **PER COMPANY**

5,263
TOTAL BREACH SOURCES

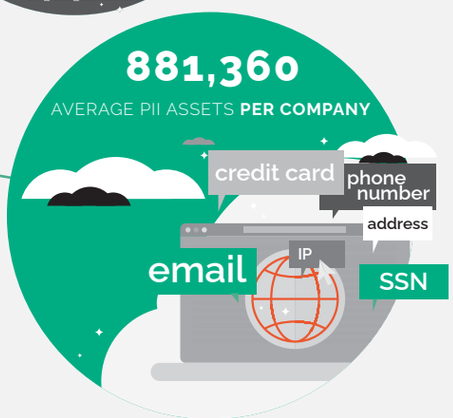
15,973,568
TOTAL BREACH RECORDS

197,205
AVERAGE # OF BREACH RECORDS **PER COMPANY**

65%
PASSWORD REUSE

71,390,159
TOTAL PII ASSETS

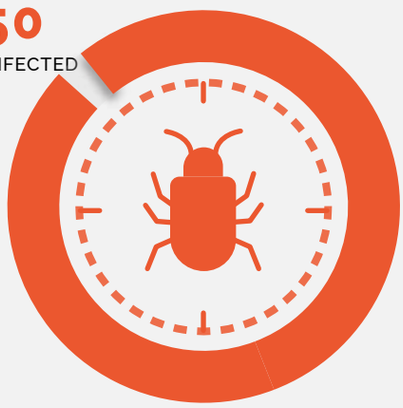
881,360
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

38,380	SOCIAL
30,618	ACCOUNTS
19,120	PHONE
6,192	GEOLOCATION
2,156	FINANCIAL

11,950
MALWARE-INFECTED EMPLOYEES



5,876,758
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- 123456
- aaron431

SpyCloud

TECHNOLOGY

119
companies

The companies in this report represent 119 of the largest US companies in the **Technology Industry.**

149,240,716
TOTAL BREACH ASSETS

1,254,124
AVERAGE # OF BREACH ASSETS **PER COMPANY**

14,610
TOTAL BREACH SOURCES

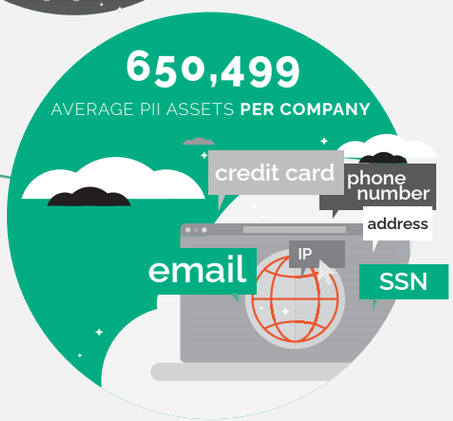
28,995,928
TOTAL BREACH RECORDS

243,663
AVERAGE # OF BREACH RECORDS **PER COMPANY**

60%
PASSWORD REUSE

77,409,402
TOTAL PII ASSETS

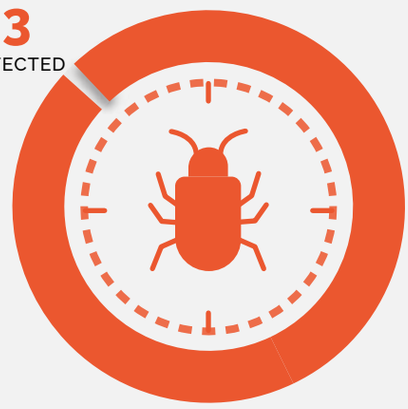
650,499
AVERAGE PII ASSETS **PER COMPANY**



TYPES OF ASSETS (AVG PER COMPANY)

65,694	SOCIAL
77,491	ACCOUNTS
32,949	PHONE
8,343	GEOLOCATION
3,613	FINANCIAL

67,723
MALWARE-INFECTED EMPLOYEES



13,222,813
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- password
- research

SpyCloud

TELECOMMUNICATIONS

9 companies

The companies in this report represent 9 of the largest US companies in the **Telecommunications Industry.**

61,912,409
TOTAL BREACH ASSETS

6,879,157
AVERAGE # OF BREACH ASSETS **PER COMPANY**

7,412
TOTAL BREACH SOURCES

13,820,290
TOTAL BREACH RECORDS

1,535,588
AVERAGE # OF BREACH RECORDS **PER COMPANY**

59%
PASSWORD REUSE

28,901,489
TOTAL PII ASSETS

3,211,277
AVERAGE PII ASSETS **PER COMPANY**

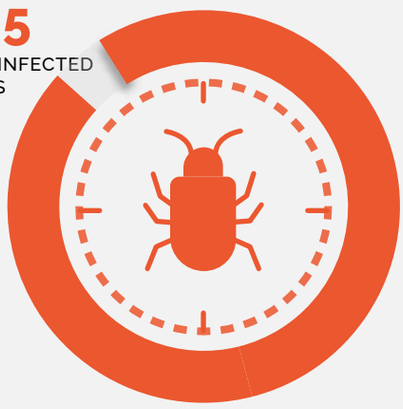
TYPES OF ASSETS (AVG PER COMPANY)

110,917	SOCIAL
229,757	ACCOUNTS
183,282	PHONE
18,977	GEOLOCATION
$ 30,580	FINANCIAL

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- password
- password1

8,015
MALWARE-INFECTED EMPLOYEES



197,874
MALWARE-INFECTED CONSUMERS

SpyCloud

TRANSPORTATION

35 companies

The companies in this report represent 35 of the largest US companies in the **Transportation Industry.**

539,969
AVERAGE # OF BREACH ASSETS **PER COMPANY**

18,898,930
TOTAL BREACH ASSETS

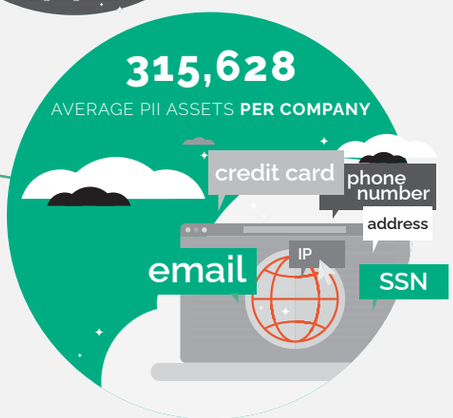
5,676
TOTAL BREACH SOURCES

97,651
AVERAGE # OF BREACH RECORDS **PER COMPANY**

3,417,777
TOTAL BREACH RECORDS

67%
PASSWORD REUSE

315,628
AVERAGE PII ASSETS **PER COMPANY**

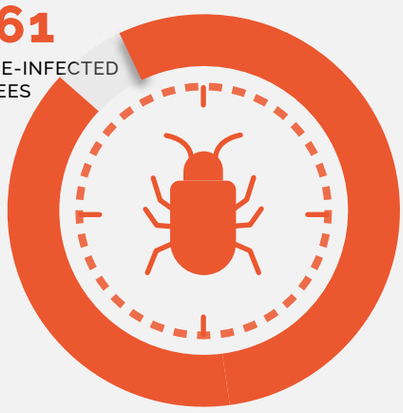


11,046,976
TOTAL PII ASSETS

TYPES OF ASSETS (AVG PER COMPANY)

28,477	SOCIAL
24,746	ACCOUNTS
15,576	PHONE
5,478	GEOLOCATION
1,707	FINANCIAL

5,261
MALWARE-INFECTED EMPLOYEES



110,317
MALWARE-INFECTED CONSUMERS

TOP NOTEWORTHY EXPOSED PASSWORDS

- 123456
- password
- 123456789

SpyCloud

WHOLESALERS

30
companies

The companies in this report represent 30 of the largest US companies in the **Wholesalers Industry.**

8,234,908
TOTAL BREACH ASSETS

274,497
AVERAGE # OF BREACH ASSETS **PER COMPANY**

3,155
TOTAL BREACH SOURCES

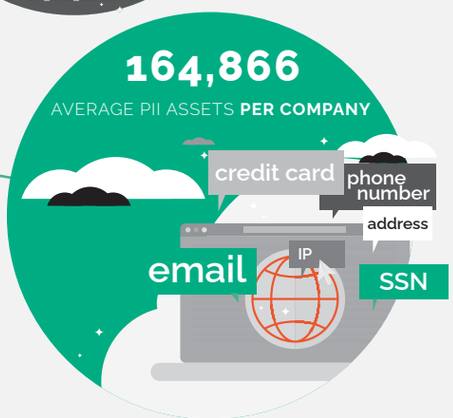
1,452,296
TOTAL BREACH RECORDS

48,410
AVERAGE # OF BREACH RECORDS **PER COMPANY**

55%
PASSWORD REUSE

4,945,983
TOTAL PII ASSETS

164,866
AVERAGE PII ASSETS **PER COMPANY**



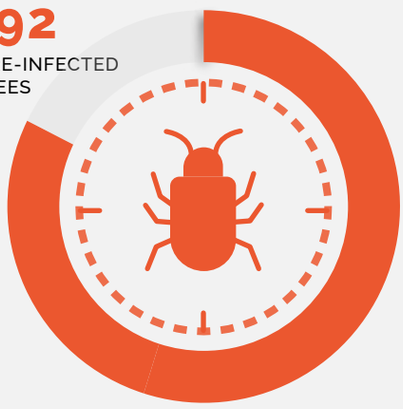
TYPES OF ASSETS (AVG PER COMPANY)

13,452	SOCIAL
11,429	ACCOUNTS
9,230	PHONE
3,082	GEOLOCATION
1,041	FINANCIAL

TOP NOTEWORTHY EXPOSED PASSWORDS

- password
- 123456
- aaron431

2,592
MALWARE-INFECTED EMPLOYEES



8,045
MALWARE-INFECTED CONSUMERS

YOUR PLAN OF ACTION

SpyCloud's analysis of Fortune 1000 companies' exposure of third-party breaches and malware-exfiltrated data has revealed over 1.87 billion stolen cookie records, and 725 million stolen assets in criminals' hands – 27.48 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, session hijacking, 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 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 Fortune 1000 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**.