SpyCloud

2020
Annual Credential Exposure Report

The SpyCloud 2020 Annual Credential Exposure Report uncovers the tactics cybercriminals used in 2019 to take over accounts. They're still leveraging stolen passwords, but now they're launching sophisticated, targeted attacks that cause more damage at a smaller scale.

2020 Credential Exposure

Every year, the SpyCloud Credential Exposure Report examines the data cybercriminals have been sharing over the last year and what it means for enterprises and consumers. Our 2020 report shows that password reuse continues to be a serious problem, leaving enterprises and their customers vulnerable to account takeover (ATO).

ATO remains a lucrative endeavor for cybercriminals. Once a bad actor cracks a user's weak password or leverages a reused password to gain entry into multiple accounts, they often have free rein to access the corporate data, funds, and PII contained within, and can wreak havoc on the lives and finances of victims. ATO affects individuals and companies alike, exposing sensitive data that can threaten credit scores, bank accounts, and brand reputations.

While automated attacks represent the largest volume of account takeover attacks, SpyCloud customers have shared that 80 percent of their losses came from just 10 percent of attacks. These attacks can be quite creative, difficult to detect, and highly effective, ranging from MFA bypass via social engineering to SIM swapping, to extortion and blackmail.

Victims of these attacks are typically high-profile, wealthy individuals, C-levels, and developers with desirable systems access—making the damage that much more serious. These "targeted ATO attacks" occur early in the breach timeline, when stolen credentials are fresh. Addressing exposed user accounts as quickly as possible after a breach helps prevent both targeted attacks and automated credential stuffing attacks.

SpyCloud recovers breach data early in the breach timeline using a combination of human intelligence and automation. After a breach occurs, criminals limit access to a small group of trusted associates to preserve the data's value, typically monetizing the information over the course of 18 to 24 months before allowing it to leak to public sources.

Total Exposed Credentials Recovered

640

Total Breach Sources Recovered by SpyCloud in 2019

9B

Total Recovered Credentials

SpyCloud researchers infiltrate criminal networks to identify and recover stolen data months or years before it reaches a broader criminal audience or goes public. As a result, the data analyzed for this report provides insight into breaches that have been freshly released to criminal marketplaces over the last year. This data will gradually become accessible to a wider criminal audience and will continue to be leveraged for as long as people reuse those compromised passwords.

Here are some of the trends we've seen over the last 12 months.

Credential Exposure Trends

More data than ever available to criminals

2019 was a record year for cybercriminals. During the first half of the year alone, data breaches increased 54 percent, compared to the first half of 2018. In line with that early 2019 statistic, our researchers observed a noticeable uptick in the amount of data available on the criminal underground over the last year; anecdotally, they noticed increases in both the number of threat actors sharing data and the volume of data that is being shared. Our analysis of the data collected last year reflects that shift, with 9 billion breach records collected in 2019, compared to 3.5 billion collected in 2018.

Rampant password reuse across accounts

Password reuse remains extremely common. Across the 9 billion exposed credentials SpyCloud recovered over the last year, we found that **28 percent of affected users had recycled at least one password** across more than one account. **Just over 94 percent of those reused passwords were exact matches**; the other 6 percent were reused with slight variations that are easy for criminals to identify with automated tools. For example, a user might have selected the password "Sprinkles" for one account and "Sprinkles1" for another.

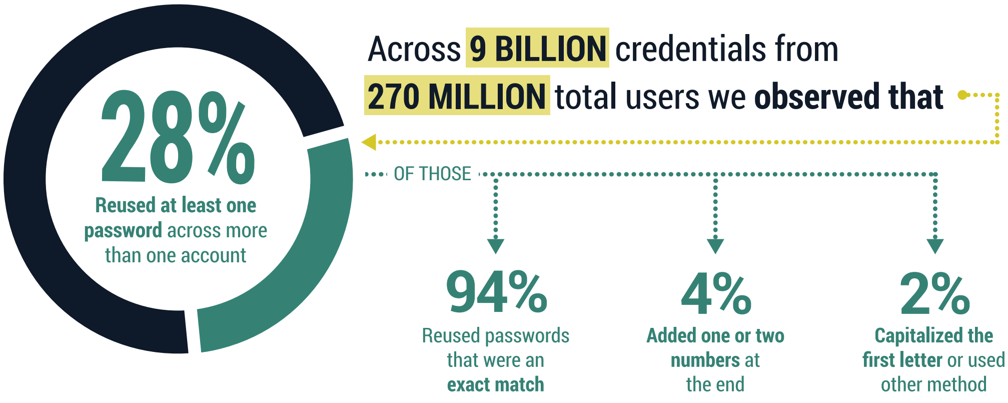
Criminals generally profit from some amount of password reuse when they acquire stolen credentials, which they test against a variety of other sites to identify accounts they can access and take over. Sophisticated crimeware makes it possible for criminals to test for both exact matches and slight variations, and even evade detection by staying under specific login attempt thresholds. Any site with an online login is fair game, including bank accounts, corporate systems, and consumer applications.

Public data is old data

2019 kicked off with the widely-reported release of the Collection Combolists, a set of seven combolists containing billions of stolen credentials shared by actor GnosticPlayers in what media outlets dubbed a "superbreach." Based on the extensive media coverage these lists received, you might expect that collecting these combolists accounted for a substantial portion of the breach data we collected last year. However, when SpyCloud acquired and analyzed the GnosticPlayers combolists, we found that only about 12 percent of the 3 billion deduplicated breach records were previously unknown to us. Because SpyCloud researchers typically recover stolen data months or years before it becomes public, we had already ingested the vast majority of the stolen credentials long ago.

Recovering breach data early in the breach timeline means we typically can't talk about specific breaches until they're old news, particularly when doing so could jeopardize an ongoing investigation or interfere with our researchers' undercover work. Our researchers' access to criminal communities means we often acquire stolen data before a victim organization is even aware that they have been breached. In these cases, we practice responsible disclosure and support the efforts of the affected organizations and law enforcement to bring the responsible parties to justice.

Public data holds less value for cybercriminals because many impacted users have already been affected by fraud, leading them to change their passwords or habits. However, criminals continue to profit from old passwords as long as people persist in reusing them.



More breaches from vulnerable servers

Our researchers noticed a more worrisome trend for security teams: an increase in the number of breaches related to unsecured servers that have been shared on the criminal underground over the last year. Criminals use open-source tools to search for vulnerable servers, exfiltrate exposed data, and share, trade, or sell the data to other malicious actors. Often, the servers have been misconfigured by database administrators.

One potential driver may be increased enterprise adoption of cloud infrastructure. Unlike on-premises servers that must be secured internally, cloud servers can be created by anyone, enabling employees with limited cloud security experience to set up vulnerable servers without informing colleagues. In addition, new 0day vulnerabilities come out all the time that can suddenly put companies and data at risk. If a new server is left unsecured for even a week, criminals have plenty of time to dump the data.

Here, it's important to note that our researchers focus on recovering breach data that is available to cybercriminals. Often, media reports on unsecured servers or databases when an independent security researcher identifies data that has been exposed to the internet where cybercriminals could theoretically access it but may not have. We occasionally work with this type of independent researcher to help them responsibly disclose the exposed data to affected parties.

In contrast, a data breach occurs when an organization has an incident and the data is confirmed to have been accessed by criminals. We see breach data traded privately within criminal communities before ultimately trickling onto the public "deep and dark web" where it can be used in credential stuffing attacks.

In particular, a vBulletin 0day that came out in September 2019 led to an influx of database breaches available on the underground. An anonymous source disclosed a Python script to a security mailing list that detailed a remote code execution (RCE) vulnerability in vBulletin that allows a remote attacker to execute arbitrary system commands on a server hosting the vBulletin forum software. Attackers using this RCE can gain essentially the same access to a database as a developer. This vulnerability led to a spike in vBulletin databases being leaked, compromised, and shared by criminals.

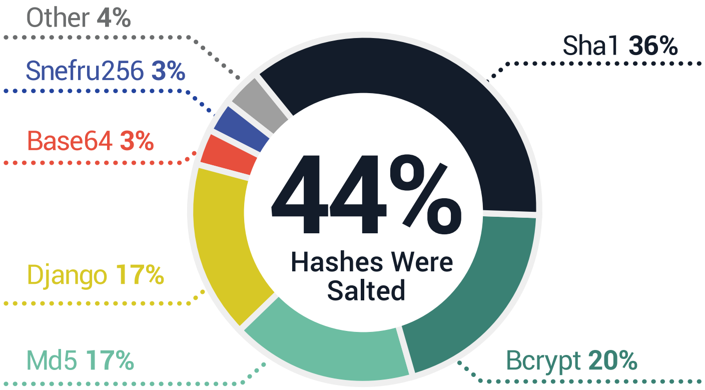
To understand the scope of this change, we compared the five-month period before this vulnerability came out to the five-month period afterward. Since the vulnerability was publicly disclosed, **we have seen a 292 percent increase in vBulletin databases released on the underground**.

Password Hashing Is Often Not Enough

A common misconception is that by storing a hashed form of the user password rather than the plaintext password itself, web applications are safe because user accounts are protected. The problem with this is that many organizations hash passwords using weak and outdated hashing algorithms, such as unsalted md5 and sha1, which provide little protection. Fraudsters use software to rapidly convert hashed passwords into the plaintext passwords they use for ATO attacks. SpyCloud research has shown that many of these hashing functions can be cracked in minutes or seconds.

When SpyCloud recovers data from closed criminal communities, we often receive passwords in a hashed format—but it's only a matter of time before criminals start sharing plaintext credentials. We crack passwords in-house to operationalize the data for enterprise security teams, helping our customers identify exposed users and reset their passwords before account takeover attempts begin.

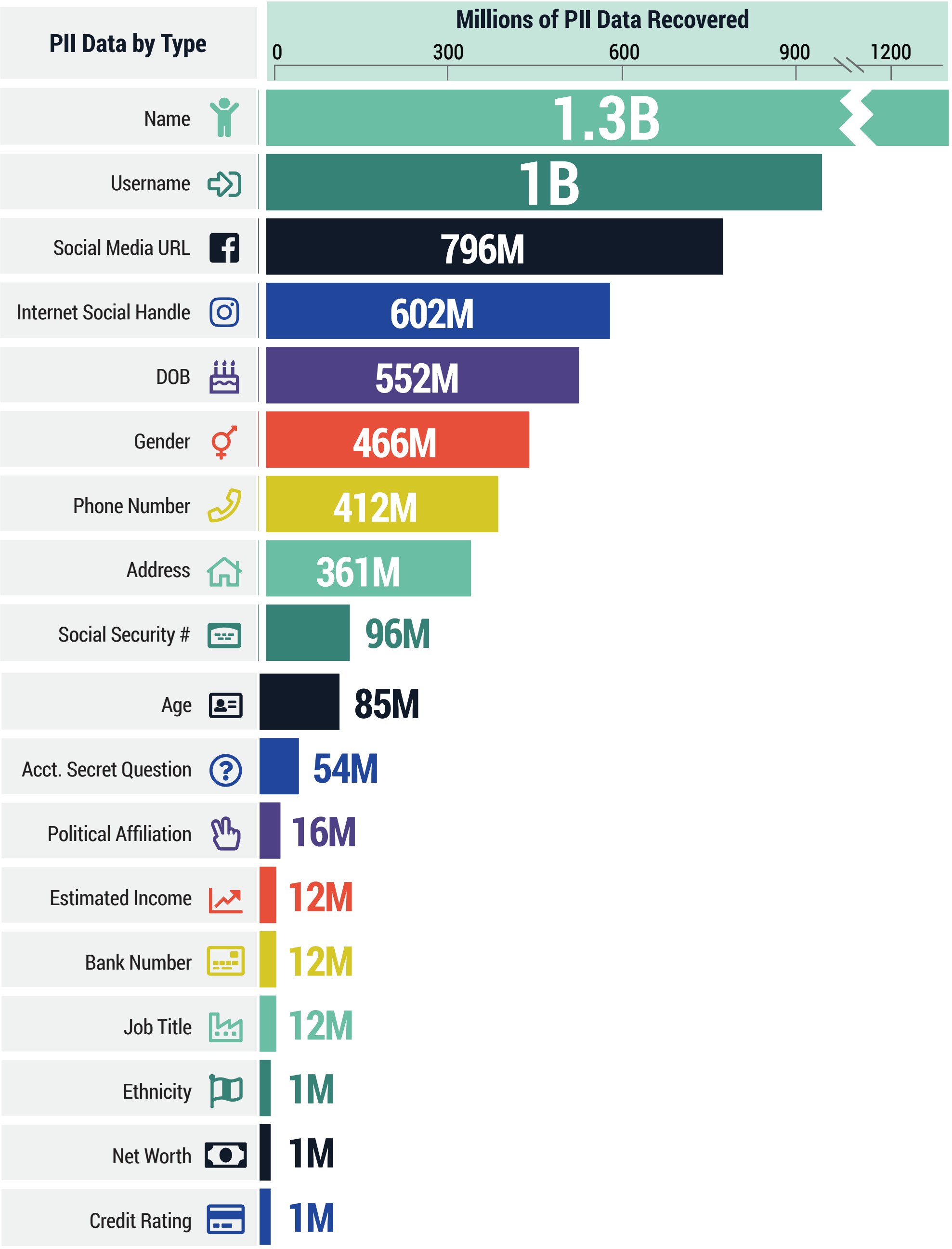
Companies that are serious about protecting their employees, consumers, sensitive corporate data, and PII must modernize their password hashing efforts. Only the strongest hashing functions stand a chance against savvy cybercriminals. We recommend that organizations follow NIST guidelines for authentication as they make decisions about how to store authentication secrets.



Personally Identifiable Information Is Gold

Cybercriminals know that the key to many accounts is personally identifiable information (PII), information that can be used to identify a particular individual. PII may be personal, but it is rarely private. Examples of PII are usernames, gender, social security number, driver's license number, credit card numbers, and even medical records. These types of personal data are stored in countless systems, many of which are not properly protected. PII data is often the only thing standing between a cybercriminal and the account. Over the last year, SpyCloud has discovered an eye-opening amount of exposed PII data.

Recovered PII by SpyCloud in 2019:



2020 Top Leaked Passwords Per Country

Interestingly, the most widely used plaintext passwords last year were associated with specific company breaches. For instance, the Dubsmash data breach resulted in over 100 million accounts being dumped onto the dark web in February. This breach revealed "dubsmash" as the most widely used plaintext password in the U.S., Canada, Czech Republic, Hong Kong, and India, and the second most used password in even more countries. Similarly, the Evite breach of more than 100 million accounts in 2019 made "evite" the second most commonly used password in the U.S.

It's hard to tell whether users from these different countries have truly chosen a brand name as their password at high rates, or if a breached organization has made a decision to store their own brand name as some type of default value for certain users. It's possible that both may be the case, especially since we know that users commonly fall into the trap of choosing simple, memorable passwords. Brand names are easy to remember. Unfortunately, criminals are well aware of this common password habit, which is why NIST calls out company names as "expected" user passwords.

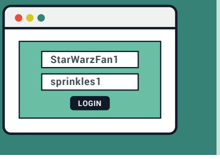
What about other countries? Some lean towards religious figures, such as "mohammad" in Afghanistan and Dominica, and "jesuscrist" in Angola. Others opt for common cultural names, such as "maria," "catalina," "valentina," and "ahmed." In some cases, simple phrases are popular; "iloveyou" was a common plaintext password among multiple countries.

Clearly, the average web user—regardless of location—still doesn't understand the importance of choosing unique and difficult-to-guess passwords. That's one reason the latest NIST guidelines put the onus on enterprises to check user passwords for any that are "commonly-used, expected, or compromised." With so many passwords to remember across countless accounts, people do what's easiest: choose a password that's easy to remember... and, unfortunately, to guess. While this may be more convenient for account owners, it's giving cybercriminals simple access into their accounts.

As cybercrime continues to evolve and increase in volume and scope, companies cannot wait to take action. A proactive approach and commitment to a modern strategy to prevent breaches and account takeover is the only way to truly protect users and the organization's assets as a whole. Security leaders should not rely on legacy applications or partial solutions. **SpyCloud is the only company with a comprehensive and easy-to-use solution capable of preventing ATO before it happens.**

REUSED PASSWORDS

TOP 100



123456 123456789 qwerty 12345 **password** qwerty123 1q2w3e 12345678
DEFAULT 111111 1234567890 1234567 123123 000000 10pace abc123
qwertyuiop 1q2w3e4r5t (null) 123321 1234 password1 30media 59trick
654321 24crow 59mile 19weed 666666 66bob **iloveyou** qwe123 7777777
)ryan 1q2w3e4r asdasd 555555 1qaz2wsx 987654321 123qwe 123456a
zxcvbnm 121212 **dragon** qazwsx 112233 **monkey** 123123123 159753
1234qwer 777777 11111111 qwerty1 a123456 asdfgh 222222 asdfghjkl
123654 gfhjkm unknown yuantuo2012 homelesspa 123456q 88888888
123abc 999999 qwer1234 **aaaaaa** asdasd123 football 1111111
123456789a 11111 0987654321 zxcvbn q1w2e3r4 q1w2e3r4t5 qwert
qazwsxedc princess **Password** 1234561 samsung target123 f***you
789456123 3rJs1la7qE **tinkle** killer 1g2w3e4r 888888 **sunshine**
qweasdzxc 159357 master myspace1 1111 gwerty123 zag12wsx 12345a

Visit our blog to see an interactive map of the top leaked passwords by country

SpyCloud

Check your corporate exposure at spycloud.com