



SpyCloud

White Paper: Understanding the Underground
Market for Stolen Credentials

Executive Summary

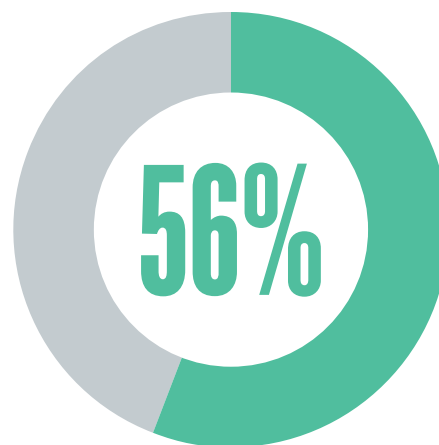
We rely on passwords to access the services we use every day. From emails and dating services to sensitive health data and even intricate analysis of our DNA, passwords protect some of our most important information. Their value, however, is not just personal. Even after the fall of the large darknet markets, such as Hansa and AlphaBay, there still exists a sophisticated underground ecosystem that thrives upon the sale and trade of stolen credentials.

Criminals can use these credentials to cash out bank accounts and max out credit cards. With our password in hand, criminals can also resell access to many of our compromised online accounts at scale. **Though it's nearly impossible to say exactly how much money flows through the underground, it's estimated that the largest dark markets netted up to \$500,000 per day in 2015.** This was just two years before major darknet markets AlphaBay and Hansa were [taken down last year](#).

In light of [recent NIST guidance](#), the strongest passwords are those which are both easy to remember and hard to guess. However, multi-factor authentication isn't ubiquitous among services. In effect, the password still represents a single point of failure, especially for services that don't enforce multi-factor authentication. Moreover, authentication interfaces which require "something you know" as an additional factor can easily be thwarted by criminals who know how to leverage open-source research on their targets. The sophistication of tradecraft leveraged by actors who are motivated by more than modest financial rewards is reflected in the methods they choose.

Criminals who are able to procure passwords through phishing scams are likely to leverage those passwords multiple times through different services. The criminals' motivations vary greatly. The average internet user offers novice and experienced hackers the potential for financial gain, while "bigger fish" demand more advanced tradecraft.

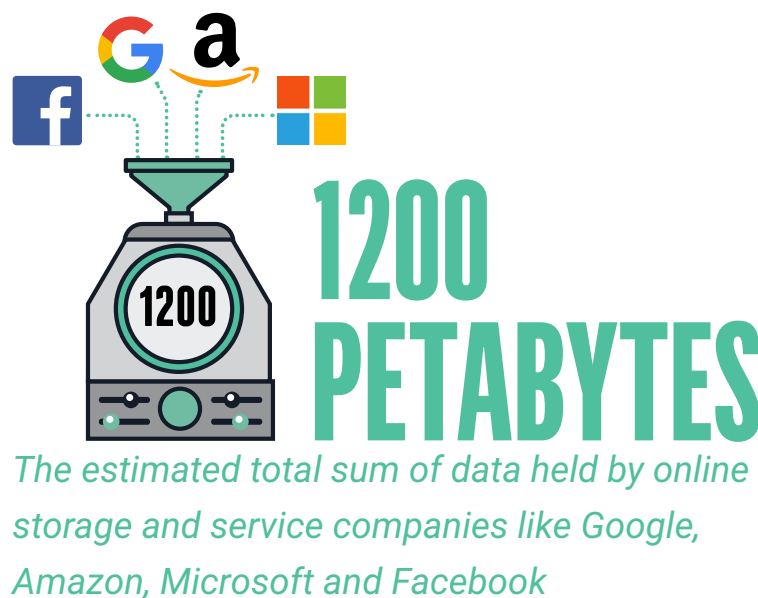
Targeted phishing scams that make it through corporate email filters must be convincing enough to fool today's more security-conscious targets. The inclusion of information that could only be obtained through careful and patient social engineering schemes must also be present. Real names and information that seemingly could only be known to vetted individuals can make many high-profile victims anybody's fool. [On average](#), people over the age of 55 maintain twelve



56 percent of all internet users use the same password across all of their accounts. It's no surprise that password reuse was the number one cause of stolen credentials in 2017.

passwords, millennials manage eight, and members of “generation z” keep up with only five passwords. Regardless of age, however, [56 percent of all internet users](#) use the same password across all of their accounts. It's no surprise that password reuse was the [number one cause of stolen credentials in 2017](#).

In addition, new data retention guidelines, such as Europe's General Data Protection Regulation (GDPR) and Russia's data localization laws, further drive up the value of stolen credentials. Experts estimate the total sum of data held by online storage and service companies like Google, Amazon, Microsoft and Facebook (“the big four”) totals [over 1,200 petabytes](#). That data contains PII, financial information, intimate personal photos, conversations and personal data that wasn't intended to be “shared” in the first place.



Phishing, stealing and extracting: Credential Theft Tradecraft

Credential theft can occur through various blends of both technical and non-technical means. Differing by motivation and capability, threat actors gather, extract, filter, validate and ultimately profit from the credentials they harvest. Financial gain and repetition motivate nearly all actors. From a security analyst's perspective, any criminal's motivation is inextricably linked to his capability. Particularly high-capability actors may be motivated by more than just money, while financially-motivated actors may be concerned primarily with bolstering their reputation. There is no common rubric for any one actor. At SpyCloud, we have observed a multitude of methods in the wild that leverage credential theft. We have grouped them into the following categories:

Phishing

Phishing operations come in many flavors. When examining any actor's behavior, it's important to consider their intent. Customer- and employee-targeted account takeover operations involve actors who are financially motivated. Most phishing campaigns are widespread and attempt to victimize as many victims as possible for the purpose of financial gain. On the other hand, attackers experienced in corporate account takeover operations are generally focused on larger, asset-rich targets that are harder to infiltrate and take over. In these cases, employees are often one of the first barriers to entry once an actor has finished their recon, completed exploit weaponization, and is ready for [delivery](#).

Spear Phishing

It's [been written](#) that when it comes to security, the human factor is any organization's Achilles Heel.

John Podesta of Hillary Clinton's former presidential campaign [was the human factor](#) that led to the compromise and release of Hillary Clinton's private emails. Podesta reportedly clicked on a spear-phishing email disguised by attackers to resemble a legitimate security alert from Google. In reality, attackers [had used a link-shortener](#) to disguise a link embedded in the email as belonging to Google. Once Podesta clicked the link, attackers were able to take ownership of his email account. This, of course, is what allowed the attackers to access and publicly release the information therein.

To his credit, it's been reported that Podesta's own IT contact [counseled him](#) that the email was "legitimate," although he meant to say it was "illegitimate." The "human factor" does not always denote any single person. Several factors can be interdependent and any single mistake may fall on the shoulders of many.

Snapchat's employees were also affected by phishing which ended up exposing a number of customer accounts in March 2016. [According to Snapchat](#), one of its employees fell victim to a phishing email that revealed payroll information about Snapchat employees. According to Snapchat, the phishing email was written to appear to originate from the company's CEO, Evan Spiegel. This type of spear phishing, often dubbed business email compromise (BEC) or CEO fraud, is in a league of its own.



Vulnerabilities and Exploits:

The success of phishing methods depends primarily on the social engineering component they use to trick victims into sending sensitive information to criminals. These vulnerabilities can be present in the authentication mechanism for a physical server or within a company's website. Hardware and software vulnerabilities have led to some of the largest data breaches of our time.

Malware

Some breaches utilize a combination of both social engineering and technical means. This was the case with the Olympic Vision BEC campaign. The campaign, [detected by security researchers](#) from TrendMicro in March 2016, targeted companies in the U.S. and Asia in the real estate, manufacturing and construction sectors. The emails crafted by those behind the campaign contained a keylogger now dubbed "Olympic Vision" which was contained in attachments. Once opened, the attachments installed a backdoor through which the attackers



were able to [log keystrokes and take screenshots](#) for the purpose of stealing personal information and performing network reconnaissance.

Luckily, more advanced business email compromise (BEC) and phishing campaigns with technical components can be defended against through keen awareness of the malware they leverage. Emails containing billing information can be valuable in making sure staff are alerted when a fraudulent transaction is initiated. Organizations can be proactive in patching their network defenses for IoC's associated with malware used in BEC campaigns, [such as Olympic Vision and HawkEye](#).

According to the FBI, BEC has seen a 1,300 percent increase in exposed losses since January 2015, totaling over \$3 billion. Furthermore, undetected attackers may use their tactics to obtain access to an organization, taking note of its billing systems, vendors and even the communication styles of employees. Once inside, attackers may spend months studying their environments before launching an attack.

[Olympic Vision](#), for example, gathers its target's computer name, saved browser credentials, FTP clients, IM clients, email clients, keystrokes, network information, screenshots, clipboard information, and text. This is extremely valuable information, especially for coders who are able to tweak existing exploits already designed to leverage those vulnerabilities.

In 2015, attackers weaponized .doc and .cpl files to [execute a backdoor called Carbanak](#) within more than 100 different banks worldwide. Attackers delivered these documents through spear-phishing emails. The backdoors allowed the attackers to perform enough reconnaissance to pull off their infamous compromise of the banks' payment systems. The Carbanak campaign resulted in the loss of between \$2.5 and \$10 million from each affected bank. Paid "mules" coordinated with those running the campaign, waiting at ATMs at predetermined times to collect money cashed-out from compromised accounts. Careful planning, reconnaissance, sophisticated malware, a convincing social engineering component, and even international coordination have all gone into recipes for the most successful ATOs.

[Security researchers](#) discovered a mass-phishing campaign against JPMorgan Chase customers in the aftermath of the [2015 JPMorgan Chase breach](#). The campaign involved a website which redirected users to an exploit kit. The exploit kit was contained within a spoofed Java update that executed upon download. According to researchers, the exploit attempted to install the Dyre banking trojan and was not detected by anti-virus software. The researchers reportedly detected this activity during an analysis of global email trends. Just days before the attack, researchers at Proofpoint security firm [discovered the phishing campaign](#) targeting JPMorgan Chase customers. Researchers revealed that some customers [were sent emails](#) that attempted to collect online banking credentials and infect machines with malware.

Careful planning, reconnaissance, sophisticated malware, a convincing social engineering component, and even international coordination have all gone into recipes for the most successful ATOs.



Session Hijacking

Session Hijacking occurs when an actor is able to intercept an active session token in real time while the victim is already logged in. Because the session token has already been authenticated, the actor need not guess a password. They can even bypass multi-factor authentication.

Such was the case for [GitLab](#) which occurred in August 2017. GitLab utilizes [private session tokens which never expire](#). In addition, these tokens were only 20 characters long, which meant that they were particularly susceptible to brute-forcing. The persistence of these tokens, combined with their short length, represented a significant vulnerability for GitLab and one that was reported to the company by a security researcher.

In April 2017, [a Brazilian bank fell victim](#) to attackers who were able to perform session hijacking on virtually every online customer who was using the site at the time of the attack. Criminals were able to mock the bank's website by changing the bank's Domain Name System registrations and redirecting customers to the phishing sites.

It's important to note that this heist, despite the sophisticated session hijacking, would not have been successful without the construction of the phishing pages. In other words, despite the attackers' impressive technical tradecraft, the attack wouldn't have been successful without a convincing social engineering component.

Session Hijacking occurs when an actor is able to intercept an active session token in real time while the victim is already logged in. Because the session token has already been authenticated, the actor need not guess a password.

Credential Stuffing

The cycle of credential theft, validation and exploitation follows a familiar pattern among diverse sets of cybercriminals. Whether stolen credentials offer access to unlimited Uber rides or someone else's savings, those seeking to exploit them largely do so for financial gain. Novice criminals may enjoy the cheap thrills of going after ride-sharing, pizza delivery app accounts, and other low-hanging fruit.

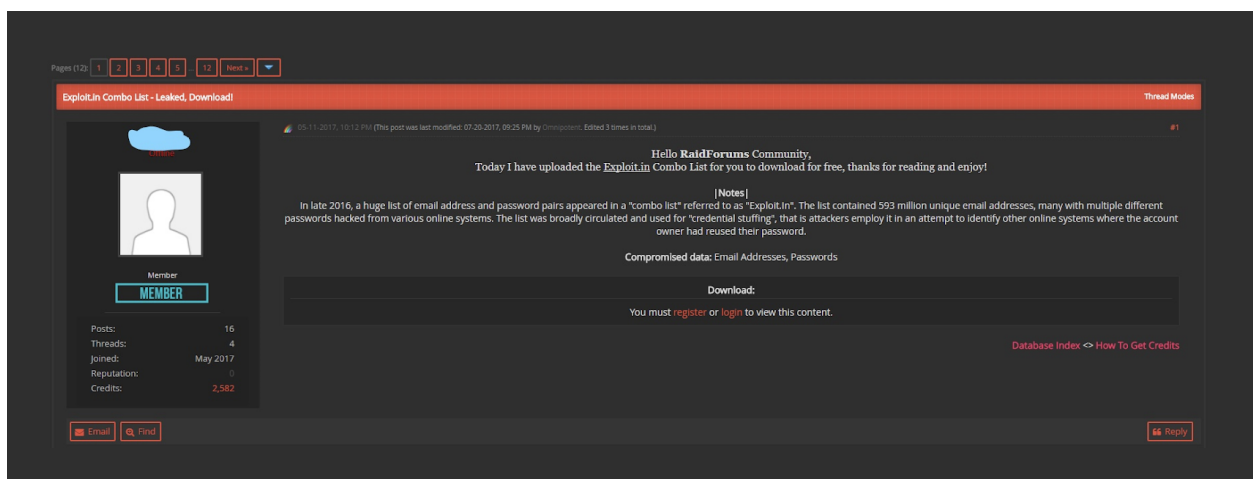


Figure 1: Screenshot of a member of an online community RaidForums discussing the release of a “huge combo list” from 2016 to high-tier hacking site Exploit[.]in

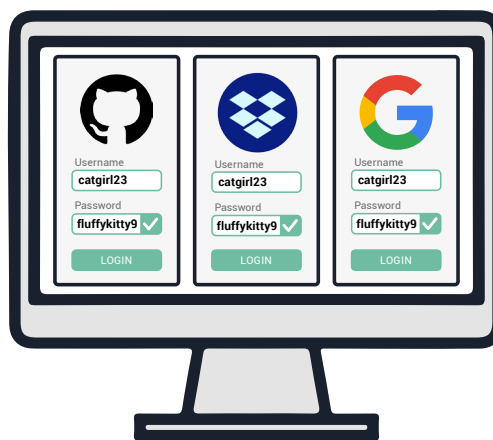
Also called “cracking” tools, credential-stuffing tools allow criminals to test lists of stolen credentials en masse against targeted web or mobile applications. Criminals load large sets of breached credentials against web applications until the automated testing yields a match. If the victim hasn’t yet set up multi-factor authentication, the account can then be taken over by the criminal. Criminals familiar with the prevalence of password reuse between accounts may leverage cracked password across multiple accounts. Once an account is cracked, successful attackers can enjoy the service for free.

Credentials harvested from service-specific account takeover require quality control as well. Although these types of ATOs don’t rise to the level of sophistication required for credit card fraud, criminals still need to validate these accounts before cashing them out. Credential stuffing attacks leverage “combo lists” of dumped passwords or dictionary lists and rely upon the prevalence of password reuse for their success. If a criminal puts in the effort to obtain a working password, answer security questions, and account access, he or she will also want to know that the account is both valid and high-value.

Nulled[.]to (which used to be Nulled[.]io) is a popular “cracking” community whose tagline is “expect the unexpected.” The tagline is fitting; Nulled itself has been hacked in the past. Contributing members of Nulled and similar sites are not compensated for their contributions, rather for the credibility they gain in their respective communities. This credibility is driven by the successful use of every configuration file, combo list, and tutorial guide posted by contributing members. Members who hardly contribute anything while using posted content are known collectively as “leechers.” Most credential stuffing tools require certain custom input files in order to work. Writing and posting these inputs, combo lists and config files doesn’t make community members money. These tools allow people to break into accounts and use services without paying for them, whether it’s a pizza delivery app, an online video game account or a media-streaming service.

Nulled[.]to describes itself as “a cracking community, [with] tons of cracked/nulled tools to offer.” Nulled and its ilk aren’t hidden sites requiring TOR use. Nor are they marketplaces. Their social hierarchy is based on “cred” and “vouching.” They’re still taking over accounts, however. The fall of darknet Marketplaces like [AlphaBay and Hansa](#) had little-to-no effect on these communities and they still exist today, often operating on [fast-flux domains](#).

Nulled itself got the unexpected last year. It [was breached](#) in May 2016, exposing some 500,000 members’ email addresses, IP addresses, login credentials and private messages. Because the successful use of cracking tools to gain access to someone else’s account to get “free” stuff is



Attackers are seeing up to a 2 percent success rate for gaining access to accounts simply due to password reuse. This may sound like a relatively insignificant proportion, but it equivocates to billions of dollars worldwide in automated fraud losses.

technically theft, it's safe to assume that members were not happy about the breach. This is especially true for those who [used their work and \[.\]gov email addresses](#) to sign up for the site.

In our article [Criminals are using these tools to “crack” your website](#), we went over some of the most popular “cracking” tools which utilize the input files that are bought, sold and traded within cracking communities like Nulled. Tools such as [Sentry\[.\]MBA](#), Vertex and Apex aren't new, but they still function. The inputs that work with them, such as configuration files and combo lists, are still being traded online.



These are just a few of the several hundred multilingual clearnet sites that act as incubators for the so-called “cracking scene.” As contributing members advance their skills, they may find more lucrative work elsewhere in the underground. Many of these sites also offer tutorials on how to use cracking tools, like Sentry MBA, or even write configuration files themselves.

On average, attackers are seeing up to a [2 percent success rate](#) for gaining access to these accounts simply due to password reuse. This may sound like a relatively insignificant proportion, but it equates to billions of dollars worldwide in automated fraud losses.

When leveraged by credential stuffing tool Sentry MBA, the configuration file specifies technical parameters about its target. These parameters, along with long lists of commonly-used passwords (combo lists), can be used to break into user accounts of popular web and mobile services. Files are in .txt format and contain the target's URL, password rules and field markers for web forms. This “config

file" was posted by a member of Nulled for the enjoyment of his peers and the benefit his own status within the community.

Rinse and Repeat: The Cycle of Credential Filtering and Validation

There exists no shortage of ways in which cybercriminals can leverage stolen credentials. What is done with credentials once they are harvested hinges upon the data criminals already have at their disposal and the validity of the credentials they've compromised. Criminals specializing in credit card fraud (often

"Carders" know that certain victim data is required to use stolen credit cards. Known as "fullz", victim addresses, dates of birth, CVVs and stolen credit card numbers can be used to make purchases on their behalf by criminals.

called "carders") know that certain victim data is required to use stolen credit cards. Known as "fullz", victim addresses, dates of birth, CVVs and stolen credit card numbers can be used to make purchases on their behalf by criminals.

Bank account fraud is more complex. These types of ATOs typically require careful planning, a sophisticated social engineering component, and the cooperation of two or more criminals. Criminals call banks posing as customers who have lost their debit card or forgotten their identifying information. They display a sense of urgency in their interactions with bank

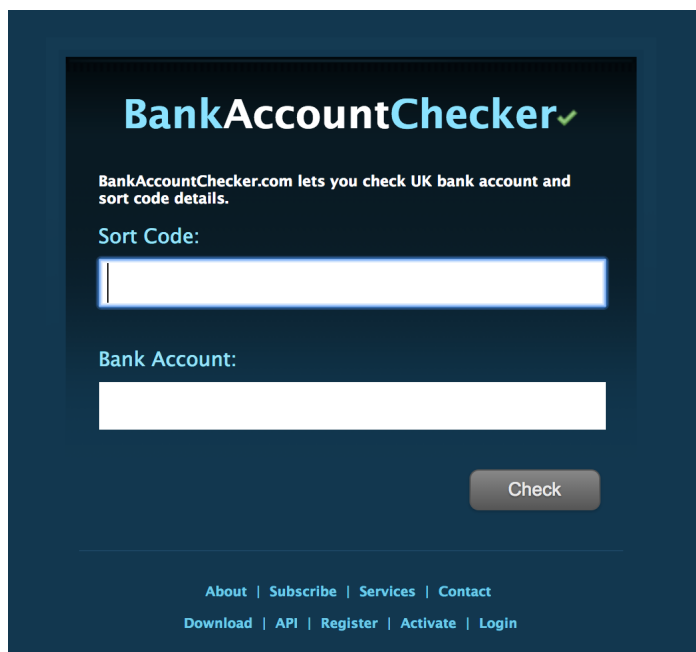
The image shows a web browser window displaying the 'BankAccountChecker' website. The site has a dark blue background with white text. At the top, the title 'BankAccountChecker' is followed by a green checkmark icon. Below the title, a line of text states: 'BankAccountChecker.com lets you check UK bank account and sort code details.' There are two input fields: 'Sort Code:' and 'Bank Account:'. A 'Check' button is located below the 'Bank Account' field. At the bottom of the page, there are several links: 'About | Subscribe | Services | Contact' and 'Download | API | Register | Activate | Login'.

Figure 2: Though not always used for nefarious purposes, bank account checkers such as the one above can be used to check the validity of accounts before they are taken over.



Figure 3: Complaint from a carding customer after being scammed by a vendor



Figure 4: Conversation posted by a carding customer claiming that the fullz he bought were invalid.

employees. Some of these attacks are sophisticated and require the cooperation of an insider to cash out compromised accounts. Others may take several months to siphon funds slowly into mule accounts. In both cases, account validation is built into the ATO process. However, for the lower-hanging fruit of credit card and service-specific fraud, credential filtering and validation are a must after extraction.

The techniques used by criminals to validate the credentials they collect depend largely upon the types of accounts they seek to take over. When it comes to credit card fraud, filtering and validation are essential due to the sheer amount of credit card numbers and fullz that are collected. Criminals need a way to validate that the credit cards will work before selling them to customers. Otherwise, potential buyers may publicly damage the reputation of fullz vendors for scamming them.

Figure 3 shows what can happen to a fraud vendor when a transaction goes wrong.

Even in the carding world, there is no honor among thieves. Taken from the Crdclub forum, the post from the customer above shows a complaint against credit card vendor who feels he was ripped off. The vendor approached the customer after he or she posted on the forum soliciting Australian fullz. He claims he paid \$10.00 for the fullz he never received.

Figure 4 shows a post on the forum BitCoinTalk claiming he was scammed by a vendor who sent him six dead dumps (credit card dumps containing invalid credentials) instead of working fullz. The fear of being ghosted by a vendor after purchasing a low-quality set of fullz is valid for carders and one that is largely assuaged by credit card account checkers. In the carding world, it's not uncommon to purchase a set of fullz with a 50 percent failure rate. However, a dump with no or very few valid fullz is of almost no use to a carder unless they were actually looking for "dead" fullz.

The account checker in Figure 5 allows carders to check their fullz in real time to see if they work. Criminals need only run their fullz through a credit card account checker and provide the following information fields: credit card number, expiration date and CVV. Several of these checkers exist and can be used online. Once fullz are harvested, checked and sold on the dark web or within private networks, it's a simple routine of "rinse and repeat" for veteran carders.

Service-specific account checkers also exist for services that have been cracked using credential stuffing tools as shown in Figures 6 and 7. **The Fortnite account checker in Figure 7, like**



Figure 5: Screenshot of a credit card account checker.

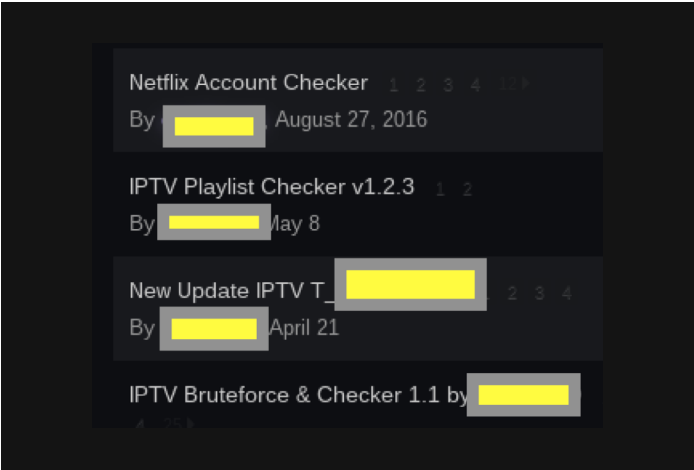


Figure 6: Custom account checkers for services such as Netflix and IPTV Playlist advertised on a "cracking" forum.

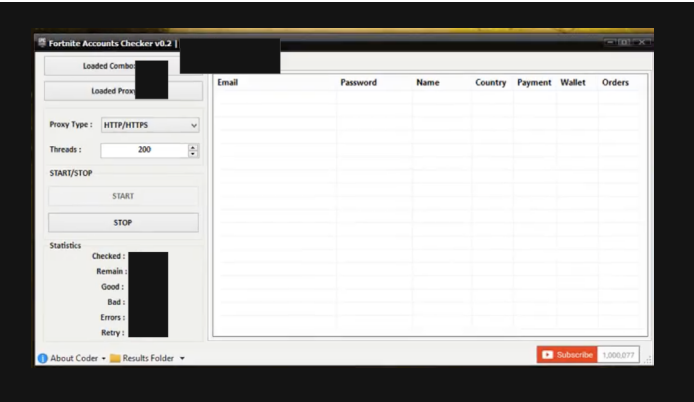


Figure 7: Account checker developed specifically to validate Fortnite accounts which are taken over via credential stuffing attacks.

other service-specific checkers, requires inputs for the victim's email address, password, name, country and payment information.

These types of account checkers are web-based checkers. In essence, all account checkers are automated programs which are designed to check mass credentials against a targeted application. They can also take the form of custom, standalone programs, such as the long-used Windows-based [Sentry MBA](#) credential stuffing tool. The success and noisiness of these programs depends upon how they were programmed. Some mass credential stuffing tools [harness the power of bot-nets](#) and run traffic through proxies in order to obfuscate originating IPs. Once these accounts are cracked, they are either "cashed out" or sold as is within trusted networks on or the dark web.

Cashing Out: Credential Sale, Profit and Use

Last year's coordinated Operation Bayonet took down Hansa and AlphaBay. Despite these seizures, underground credential enterprises have not disappeared. The fall of these markets represented a paradigm shift in how credentials are bought and sold on the underground.

Some things haven't changed. High-value sales within closed and trusted groups, from high profile actors to trusted clients, continue as they always have. The seizures only changed how criminals can advertise their wares publicly. Buyers and members of various fraud communities who existed previous to market seizures can still converse with contacts they maintained from the days of AlphaBay and its ilk.

High-profile vendors have long been aware that security researchers used screenshots from the easily-accessed dark markets such as AlphaBay and Hansa in their public-facing research. Companies published actor profiles on specific vendors. If any credible vendor set up shop on one of these public markets, he didn't do so for long. At the very least, he used an alternate identity as to not cross-contaminate public reporting with his underground persona.

How are criminals selling credentials now?

According to our own research, the savviest credential vendors weren't on AlphaBay or Hansa. These high-capability criminals, whose livelihoods are largely funded by credential theft, almost always sell credential sets privately and directly to trusted clients. Advertising is done through word-of-mouth, "vouching" and referral services.

As in many criminal circles, trust between vendors and clients is not earned overnight. Once a potential buyer does gain access to a trusted circle, the value of the credentials he could buy directly from a well-known vendor eclipses any comparable credential set he could have bought on AlphaBay or Hansa. In short: the fall of these markets has failed to affect meaningful criminal enterprises dealing in stolen credentials and high-value transactions are still being completed today.

Last year's coordinated Operation Bayonet took down Hansa and AlphaBay. Despite these seizures, underground credential enterprises have not disappeared. The fall of these markets represented a paradigm shift in how credentials are bought and sold on the underground.

In 2015, some prices for the common items on the dark web were estimated at the following prices:



Social security numbers

\$30



Dates of birth

\$11



Health insurance credentials

\$20



Credit card numbers with
expirations dates and CVV

\$4-\$12



PayPal accounts (vary by
account value)

\$50-\$8,000



U.S. credit card fullz

\$30



UK credit card fullz

\$20-\$40



Canadian credit card fullz

\$21-\$40



Australian credit card fullz

\$21-\$40



European credit card fullz

\$25-\$45



Healthcare records

\$20-\$50

Darknet changes will make the prices of certain credential types become increasingly more volatile. As new markets come online and old markets are seized, some vendors lose their market share, while private vendors can raise prices for wares that become scarcer.

It's important to note that these prices are only an estimate. Further, since markets have come offline, it's difficult to estimate how prices have changed for wares that are only being sold in closed networks.

Financially-motivated criminals of all types can make money off of selling accounts. How much largely depends on the magnitude of complexity the ATO required as well as the potential value of the account. For example, a bank account login for an account worth over \$150,000 might not sell for nearly as much if the seller only has access to the password and not answers to security questions, physical addresses, and other information that would be required to gain access to the account and siphon the funds elsewhere.

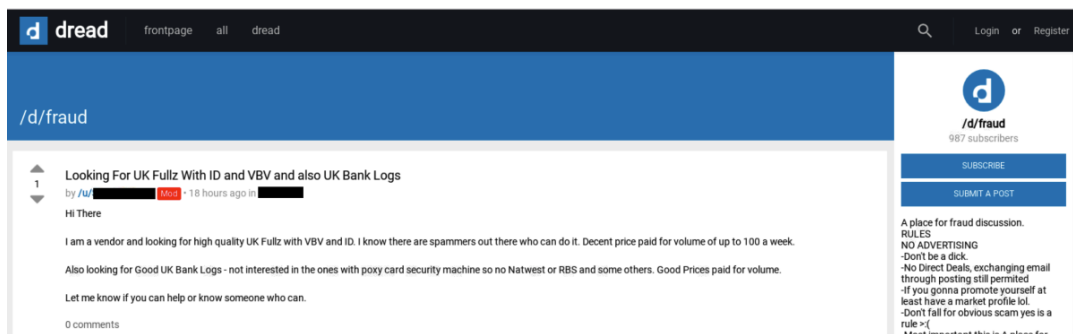
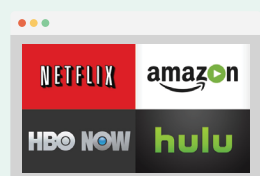


Figure 8: Screenshot of someone soliciting UK bank login credentials on the Dread dark web forum.

Reselling Account Access

Streaming, dating and gaming accounts, for example, command lower values than do accounts that are more difficult to take over. The Netflix accounts shown in Figure 9, for example, were obtained by those in the underground “cracking” scene using credential stuffing tools. These accounts being sold for only a few dollars each.

Although these types of accounts may be easier to take over, profits from selling them still add up significantly over time. Given they're easier to take over than bank accounts, it may be more lucrative for



Streaming account credentials

\$1-\$9



Int'l hotel chain program
accts 50,000 points

\$75/acct



Int'l hotel chain program
accts 150,000 points

\$140/acct



U.S. airline loyalty accts
50,000 miles

\$99/acct



U.S. airline loyalty accts
100,000 miles

\$149/acct



U.S. airline loyalty accts
150,000 miles

\$199/acct



Facebook acct credentials

\$2-\$4/acct



uTorrent acct credentials

\$600/acct



PlayStation acct credentials

\$35/acct

the majority of actors to spend their time cashing them out rather than going after higher-value accounts.

Some criminals may prefer to use the credentials they steal for themselves rather than resell them on the dark web or directly to another criminal. Criminals may command higher values for credentials that have been stolen through custom phishing campaigns or even through manipulation schemes such as [sextortion](#).

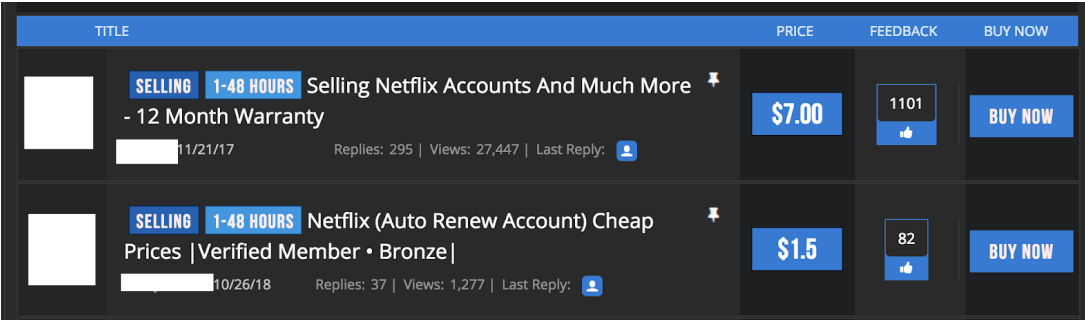


Figure 9: Cracked Netflix accounts being sold on an open-source hacking forum.

How SpyCloud Can Help

Account Takeover (ATO) attacks have become an extremely lucrative business for cybercriminals, particularly due to widespread password reuse. Cybercriminals exploit compromised accounts for financial gain by pilfering financial or personally identifiable information (PII) directly or by selling access to these accounts on underground markets.

Customers can help protect their organizations by storing credentials the right way. We recommend all credentials be stored by your corporate- and customer-facing applications using a strong cryptographic hashing algorithm like bcrypt, Argon2 or scrypt. If you mandate this across the board, you will render potentially-leaked credentials nearly useless to criminals. The computational requirement makes it infeasible to crack these algorithms (today). Any of these stolen hashed passwords, therefore, cannot easily be decrypted and used against your customers, thus limiting your overall liability.

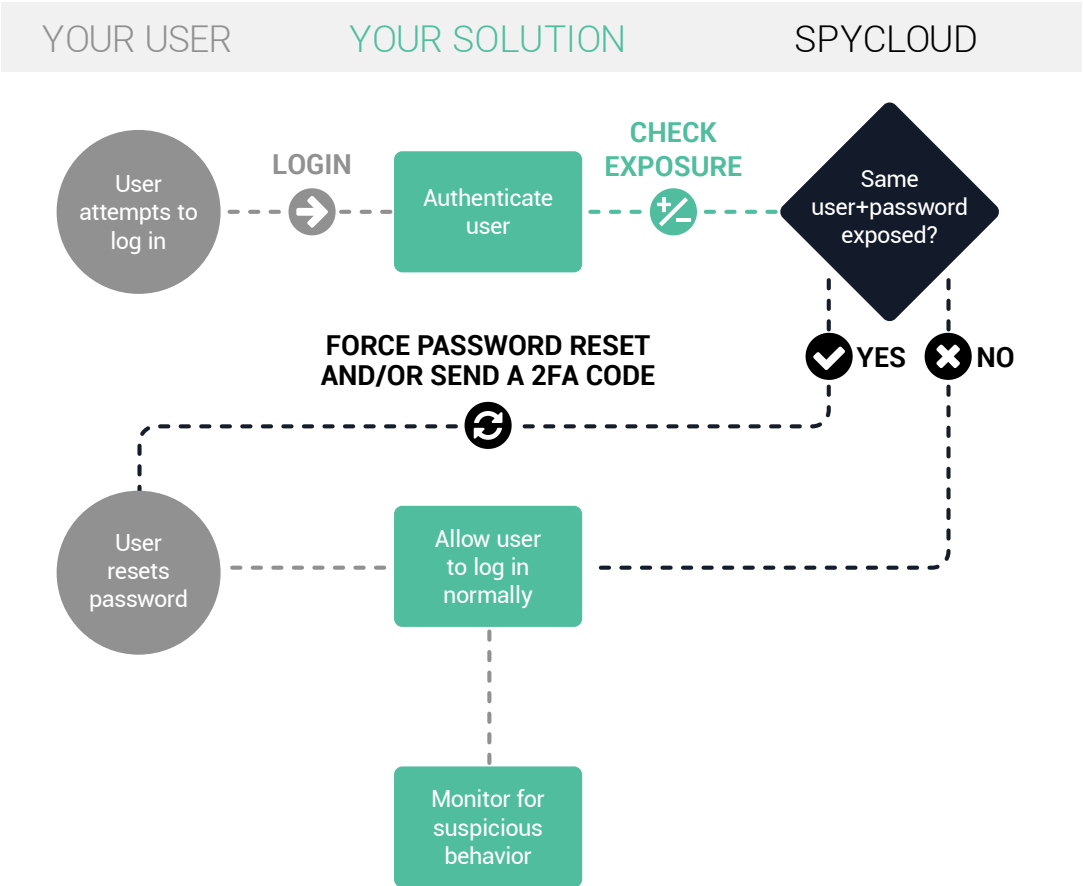


Figure 10: Protect Your Customer Accounts

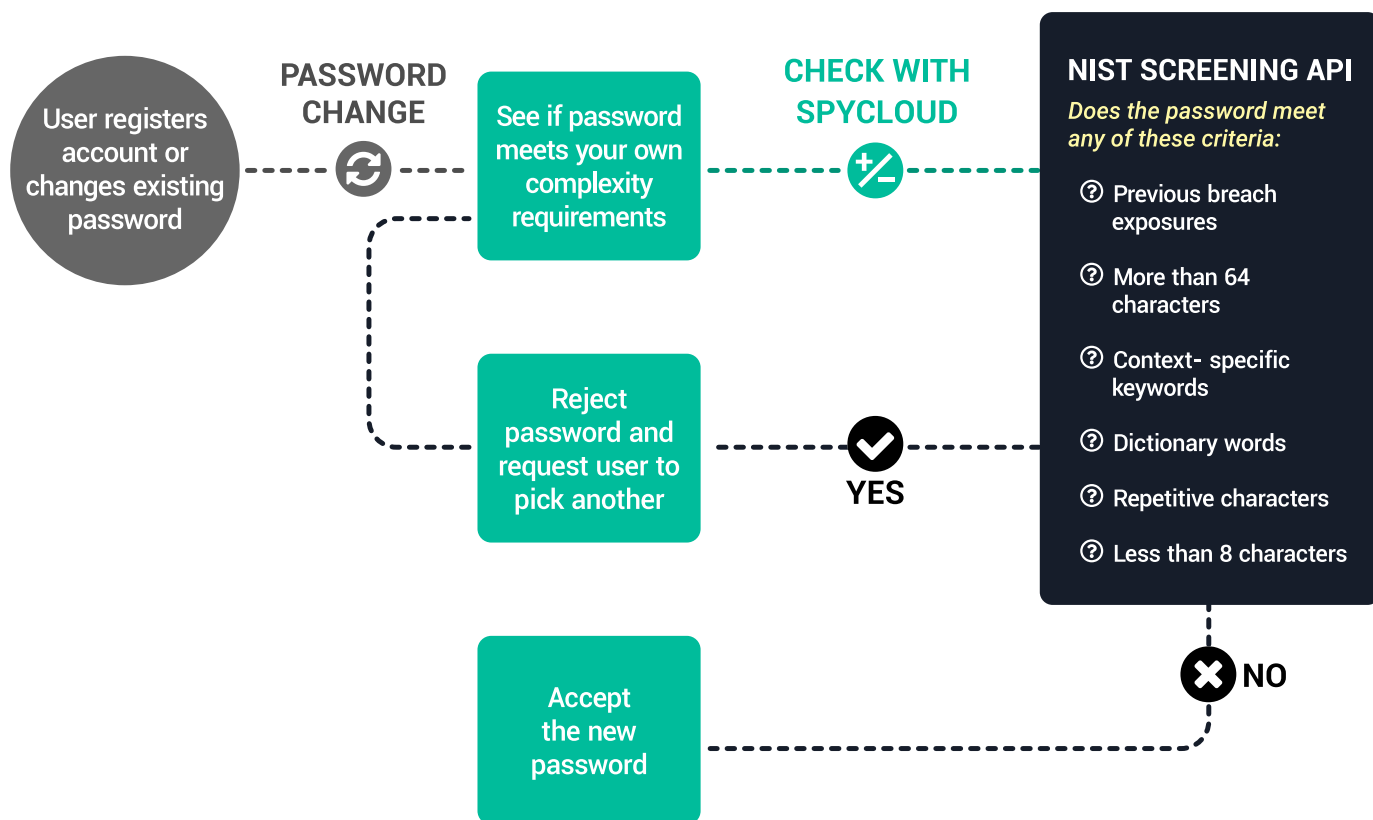


Figure 11: NIST Password Screening

NIST's new guidelines on password strength can also help keep your credentials safe. Special Publication 800-63B now recommends all applications with user accounts "compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised." NIST recommended this extra check due to the modern success rate of brute force and credential stuffing attacks.

Customers can help protect their organizations by storing credentials the right way.

SpyCloud recommends all credentials be stored by your corporate- and customer-facing applications using a strong cryptographic hashing algorithm like bcrypt, Argon2 or scrypt.