ENZOIC

BATTLING ACCOUNT TAKEOVER RISKS WITHOUT COMPROMISING USER EXPERIENCE

Account takeover schemes are costing consumers, banks, retail organizations, and other online businesses billions of dollars each year. Threat actors have come up with dead simple and extremely effective means of using stolen passwords from a breach at one institution to take over accounts at numerous institutions all over the Internet. The attacks they've devised are automated and conducted at a mind-boggling scale.

These cybercriminals rake in the cash by taking advantage of three universal truths online today:

- easy access to stolen credentials on Dark Web,
- users' propensity to reuse passwords, and
- the market's inclination to make user authentication as easy as possible

This confluence of factors has put organizations in a difficult spot when it comes to protecting their transactional platforms and the consumers who use them. Organizations can't afford to ignore the growing risks associated with account takeover. But at the same time, they need to do so without chasing their users away with a poor customer experience at log-in.

Striking the right balance requires developers, cybersecurity professionals, product managers, and executives to come together to understand the mechanics behind rampant account takeovers and why popular methods of mitigation like two-factor authentication aren't moving the needle on the problem.

THE MECHANICS BEHIND ACCOUNT TAKEOVER

The technology and business world today faces an epidemic of stolen passwords and credential exposures. In 2019 alone, security researchers have found caches of stolen credentials held by criminals on the Dark Web totaling up to billions of username-password combinations. Attackers scoop up passwords from around the web like candy, using methods like phishing, implanting automated credential stealer malware on endpoints, and hacking corporate servers to seek out databases full of them.

These hunting expeditions to score massive numbers of stolen credentials serve to fuel more profitable forms of cybercrime, typically committed against organizations totally unrelated to those from which the initial credential was compromised.

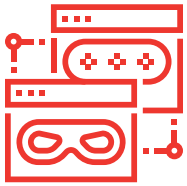
75%
of people reuse passwords across websites

The attackers are able to do this due to the alarming rate at which most users today reuse login credentials across accounts. A study earlier this year showed that 75 percent of people reuse passwords across websites, and 47 percent admit to reusing passwords across both employer and personal accounts.[1]

Counting on these high password reuse statistics, attackers will steal any and every credential they can get their hands on from across the web, even from very low-value websites that hold no direct possibility for criminal monetization. The goal is to aggregate these stolen goods to feed into an increasingly popular attack technique called credential stuffing.

Credential stuffing essentially scales up and automates the process of taking credentials stolen on one site and trying them out on a variety of unrelated sites. Attackers use a potent combination of credential stuffing tools that utilize distributed botnets, headless browsers and scripting to automatically punch in login requests into valuable sites. These tools can try hundreds of millions of credential combinations in a day, making it look like each login is coming from different IP addresses to get around any filtering technology that a site may have in place to block fraudulent traffic. Attackers like credential stuffing better than automated brute force attacks against login mechanisms because they're harder to detect, they yield better results, and because they can reuse the same repository of stolen passwords over and over again against sites all around the web.

According to researchers with Akamai, credential stuffing attacks powered an incredible 30 billion fraudulent login attempts in 2018. On average, attackers were making 115 million credential stuffing login attempts online per day.[2] At such tremendous volumes, even a slim percentage of success in taking over valuable accounts using credential stuffing stands to yield the bad guys huge upside in the form of financial fraud and theft of more valuable data held in these compromised accounts.



30B
fraudulent login attempts in 2019

In fact, numerous studies over the last year have confirmed that compromised

[1] *securityboulevard.com/2019/01/old-password-habits-die-hard-if-they-ever-die-at-all/;*
[2] *darkreading.com/edge/credential-stuffing-attacks-behind-30-billion-login-attempts-in-2018/d/d-id/1334371;*

credentials are the number one cause of breaches today.[3] And credit card fraud losses related to account takeover have skyrocketed in recent years. In 2017 account takeover fraud increased by 300 percent. Last year it dipped slightly from there, but still accounts for $4 billion in losses.[4]

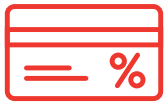
TYPES OF ACCOUNTS AT RISK

Financial Accounts

It's intuitive to understand the attraction that criminals have to attempt takeovers of obvious account types like bank accounts, credit card accounts, or online retail accounts. Once they've achieved control over these financial type of accounts, it doesn't take much added work to directly steal funds or valuable goods that can be easily resold.

However, these accounts are just the tip of the iceberg when it comes to the accounts in the crosshairs for credential stuffing attempts. Not only are credential stuffing attacks deluging the kinds of consumer-facing organizations that one might expect to bear the brunt of financial fraud, they're also making a dent at other organizations as well. In the era of the app economy where every business is a software business, the variety of accounts that hold value to cybercriminals has broadened considerably.

These less obvious account types include:



Loyalty Points and Consumer Rewards Accounts

For example, in late 2018 and early 2019 attackers struck Dunkin' Donuts loyalty program accounts with a series of credential stuffing attacks with the aim to steal and resell the stored value of the rewards, coupons, and points held by these accounts on the black market.[5]

Online Streaming Services

Security researchers have dubbed the ecosystem around account takeover of over-the-top (OTT) streaming services as the "Bank of OTT."[6] Attackers use credential stuffing to compromise these accounts with the sole purpose of selling illegal access to their streaming content through illegal entertainment streaming services. Users of the legitimate accounts are not impacted by the compromise, but the services themselves are being bilked by criminals — and their underground customers — piggybacking on paid accounts.

Gaming Sites

Between November 2017 and March 2019, attackers targeted the gaming industry with more than 12 billion credential

[3] *enterprise.verizon.com/resources/reports/dbir/;* [4] *info.rippleshot.com/blog/javelin-fraud-trends-report;* [5] *threatpost.com/dunkin-credential-stuffing/141754/;*
[6] *infosecurity-magazine.com/blogs/rise-account-takeover-media-1-1-1-1/*

stuffing attacks.[7] With characters buffed up with traits borne of hundreds of hours of gameplay, and other in-game tools and items holding a great degree of value and resale-ability within the online gaming community this industry has attracted a great deal of attention from cybercriminals. What's more, online gaming isn't regulated the way that financial organizations might be, so it provides a low-risk hunting ground for crooks looking to fly under the law enforcement radar.

Online SaaS Services

Online application or email services provide a range of valuable resources for criminals who can take over their accounts through credential stuffing. For example, automated account takeover attacks against Office 365 accounts earlier this year[8] were then turned around to feed into a lucrative phishing campaign—the bad guys used successfully compromised accounts to send the phishing messages. Similarly, attackers target cloud computing accounts to steal compute power to operate a range of illicit online activities.

THE SHORTCOMINGS OF 2FA AND BOT DETECTION

To many within the security community, solving the problem of credential stuffing and account takeover is 'simply' a matter of deploying two-factor authentication (2FA). Requiring the user to provide another means of proving they are who they claim to be—either through biometrics like fingerprint authentication, SMS authenticators, one-time passwords or the like—definitely adds a higher level of assurance that would thwart would-be account fraud.

The truth is that most customers highly dislike 2FA due to the friction it adds to the login process and overall customer experience.

67%

of consumers don't use any kind of 2FA for their personal accounts

According to recent studies, 67% of consumers don't use any kind of 2FA for their personal accounts, and only a little over half even use it at work. Even when consumer sites make it extremely easy to use, such as the case with Google, users still buck against the technology. This spring The New York Times reported that Google can't get more than 10 percent of its users to sign up for 2FA.[9]

Consequently, product owners and line-of-business managers have some serious reservations about 2FA. These leaders are spending millions of dollars on digital transformation efforts to improve customer experience. They don't want to threaten the ROI from those efforts by gumming up their systems with a 2FA-powered login that reduces user satisfaction.

What's more 2FA isn't even necessarily a slam dunk in terms of account takeover risk mitigation. The rise in mobile account takeovers tracked by Javelin Research in the 2019 Identity Fraud Study[10] points to the fact that many attackers recognize that SMS-based 2FA is one of the most prevalent and least obtrusive methods of 2FA today. They're starting to subvert these protections by taking over mobile phone accounts used to provide the second method of identity verification.

And so the promise of 2FA remains illusory for most consumer-facing organizations today.

[7] *helpnetsecurity.com/2019/06/14/gaming-community-credential-stuffing-attacks/;* [8] *infosecurity-magazine.com/news/researchers-warn-office-365-1/;*
[9] *nytimes.com/2019/03/27/technology/personaltech/two-step-authentication.html?smid=nytcore-ios-share);* [10] *info.rippleshot.com/blog/javelin-fraud-trends-report*

Meantime, in reaction to 2FA's failure to launch, many organizations have responded to the risk of account takeover by instituting bot or fraud detection technology to stop automated credential stuffing or detect anomalous account behavior. While in theory this should be a good risk mitigation measure, it adds its own unique friction points that are perhaps even more troublesome than 2FA.

The trouble with these rules-based detection methods is that attackers quickly adjust their tactics to evade the detection rules. So organizations must constantly deal with out-of-date rule sets that frequently miss truly fraudulent behavior. On the flip side, the organizations that respond to this frustration by increasingly tightening rules so as not to let fraudsters fall through the cracks end up alienating their users in the process, because these tougher rules are more likely to dredge up false positives that get in the way of legitimate use of accounts. This leaves fraud professionals in a quandary because if they turn up the sensitivity of their detection rules they're more likely to introduce friction by interrupting valid transactions, but if they turn down sensitivity they experience loss due to missing many attacks that operate in the margins.

HOW ENZOIC IS DIFFERENT

Enzoic takes an approach that is both different and complementary to 2FA and fraud detection technology. Enzoic provides an added level of protection from credential stuffing and account takeover without adding friction to the customer experience. The abiding philosophy behind the Enzoic approach is to screen passwords for risk without getting in the way of login attempts. Enzoic gives organizations the power to cross-check current credentials for signs that they may have been reused or compromised elsewhere.

HOW IT WORKS

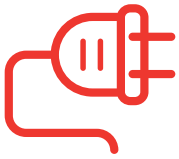
Enzoic threat researchers scour the public internet and the Dark Web to find information and technical clues about all of the compromised credential details circulating online today. Our researchers correlate details about how the credentials were exposed, add additional details about unsafe passwords currently used in cybercriminal password cracking dictionaries and combo-lists and turn it all into valuable threat intelligence that then feeds into our credential screening solutions.

API Services

The flagship product using our credential screening intelligence, Enzoic for Account Takeover is an enterprise REST API that works in real-time in the background of user login, account set-up, and password reset activity. Completely transparent to the user, the screening process does not impede activity by uncompromised accounts. And even when signs of compromised are flagged by the API, organizations have the flexibility to decide how to respond based on their risk and user friction tolerance.

Some organizations use the API to initiate step-up authentication when a credential is flagged, introducing 2FA only to those accounts that have been identified as at risk for account takeover. Others require password resets. Still others may reduce privileges for the account or use other threat mitigation tactics to respond to the risk, including bot

or fraud detection. In this way, friction is only introduced when risk appears higher for a particular set of passwords.



Active Directory Plug-in
Enzoic's threat intelligence also powers Enzoic for Active Directory (AD), a tool meant to help IT and security professionals take a proactive approach in securing their AD environment without resorting to irritating users with heavy-handed policies that force everyone to reset passwords on a regular basis.

The plugin filters new passwords against Enzoic threat intelligence to automatically restrict selection of any password identified as previously compromised. Additionally, it continuously checks existing passwords against newly discovered compromised credentials to trigger immediate alerts. All this is done without Enzoic ever storing password data in the process.

Enzoic Exposure Alerts
Enzoic threat intelligence can also be used by security analysts to enrich their threat feeds in security operations center and SIEM environments. Security teams can subscribe by domain or named account and receive alerts about compromised accounts in real-time.

The Enzoic suite of solutions can provide a range of use cases for password screening. Development teams can utilize our APIs and plugins for enterprise applications, platforms resold to enterprise, within risk-based authentication systems and more. Enzoic's credential screening provides an effectively elegant way to reduce the risk of credential stuffing and account takeover without adding friction to the customer experience.

To learn more, visit *enzoic.com/account-takeover-prevention/*