Exposed Customer Credentials

Tactics, Risks, Mitigation

2023

Cyberint

TABLE OF CONTENTS

INTRODUCTION

Within the cybercriminal world, the theft of users' credentials is a growing industry. The market for compromised credential is vast and has huge potential due to the online availability of cheap malware kits, the increase in active theft operations around the world, and the increasing sophistication of techniques implemented by threat actors.

In the technological ecosystem of today, almost every website and application utilize passwords to authenticate its users, who have to deal with an increasing number of online accounts. As the need grows, users tend to reuse the same account-passwords combinations for many of the online services they use. Unfortunately, these widespread use and reuse of passwords makes them attractive targets for cybercriminals, knowing that **passwords can be stolen from company's accounts are providing an entry point to other accounts and services**.

Each year, billions of compromised credentials appear online, either on the dark web, clear web, paste sites or in data dumps shared by cybercriminals. **These credentials are then used by threat actors for account takeover attacks, fraud, and data theft.** While businesses try to protect their own sensitive information from attacks, customer information is stored in vulnerable databases all over the web, resulting in identity fraud losses of a total of $52 billion and affecting 42 million U.S. adults in 2022 alone.[1]

The identification of compromised customer accounts, targeted domains, and vulnerable passwords enables organizations to proactively build a better defense against account takeovers and fraudulent activities. Furthermore, **the constant identification of customer accounts that have been compromised, provides ongoing fraud monitoring without impacting the user experience.** Additionally, collected data can be used to gain insight into the targeted domains and most vulnerable passwords, which helps to prioritize risk mitigation strategies and protect the organization's customers and their own reputation.

[1] https://www.globenewswire.com/news-release/2022/03/29/2412099/0/en/Identity-Fraud-Losses-Total-52-Billion-in-2021-Impacting-42-Million-U-S-Adults.html

USES OF COMPROMISED CREDENTIALS

An organization's customers' credentials are a valuable good on the cybercriminal market for 2 main incentives:

1. They are relatively easy and cheap to obtain, requiring little effort from novice threat actors to get their hands on

2. The credentials can be developed and abused in a variety of other fraudulent activities, such as:
   - **Acquiring Additional PIIs and Data** – after entering an account, threat actors can harvest more information, for example, credit cards, phone numbers, addresses, IDs, etc.
   - **Spam** – a legitimate account is a good tool for scams and other deceitful activities.
   - **Phishing** – under the disguise of a legitimate account, threat actors target the account owner's contacts.
   - **Ransom Attacks** – owners of valuable accounts might be forced to pay ransom for their accounts
   - **Financial Fraud** – accounts with access to financial data and the ability to execute transactions, such as credit cards, withdrawing funds and wiring money, are especially valuable to threat actors. Financial Fraud and Transaction Laundering can be executed with standard currencies, as well as cryptocurrencies, and even loyalty points or gift card credit.
   - **Promo Abuse** – threat actors rely on multi-accounting techniques to gain as many sign-up or referral bonuses as possible.
   - **Card Testing** - some accounts are only used to make small purchases, or to test credit cards. This helps threat actors to check the validity of stolen credit cards, which can then fuel their criminal buying sprees.
   - **Acquiring Access to Premium Accounts** – especially popular for services with fee/membership-based services, such as Netflix, Spotify, and others
   - **Money Laundering or Money Mule Transactions**
   - **Social Media Engagement** - compromised accounts are used to run "bot farms" for social media engagement manipulation, such as followers and likes.

TACTICS AND TECHNIQUES

The foundation for exposed customer credentials is fraudulent access to a user's account credentials. Below are some tactics how attackers usually compromise legitimate accounts:

- **Brute-force attacks** - The attacker links a username/password combination across many accounts until one yield results. These include so-called" dictionary attacks," in which attackers use common passwords and dictionary terms to guess passwords.
- **Credential Stuffing** – utilization of the bad habit to use the same password for multiple accounts. If one of those passwords is leaked in an unrelated data breach, any other account with the same username and password is at risk.
- **Phishing** - remains an effective way to get a victim's password. Without controls such as multifactor authentication (MFA), lost credentials can lead to compromised accounts.
- **Malware Attacks** - Keyloggers, stealers, and other varieties of malware can expose user credentials, giving attackers control of victims' accounts.
- **Dark Markets** - Attackers can download cracked passwords from darknet markets to attempt ATO on the same user accounts on their target site.
- **Security Vulnerabilities Exploitation** - unpatched security holes are used to gain unauthorized access to a system. For example, Cross-Site Scripting (XSS) and Server Side Request Forgery (SSRF).
- **Social Engineering Attacks** – threat actors contact people in person and attempt to extract login information.

COMMON ATTACK VECTORS THAT UTILIZE CREDENTIALS

CREDENTIAL THEFT

Credential theft occurs when threat actors steal credentials and use them to gain access to services or applications to steadily escalate their privileges or to access bank accounts, e-commerce sites, and other platforms as customers. For credential-based attacks against customers, **credential theft can lead to significant financial losses due to financial platform breaches,** while recent attacks on healthcare platforms can result in the loss of Personally Identifiable Information (PII). Threat actors use a variety of techniques to gain credentials, including brute force attacks, phishing, website spoofing, or injecting malicious code into login or checkout pages.

The fresher the compromised credentials, the higher the chance threat actors can achieve their financial objective. However, credentials are rarely used by threat actors in "real-time." Unless the credential is compromised in highly targeted attacks, threat actors require time to analyze the reams of data that they have captured. This process of filtration and extraction enables them to pull out 'prime' credentials either to sell on illegal marketplaces or use them for further exploitation. However, the sooner the compromised credentials are detected, the faster security teams can remediate them. If stolen credential information can be detected very early on, no more than a few days after they have been compromised, the impact of the theft on the business can be massively reduced.

CREDENTIALS' STUFFING

Credentials' stuffing is a type of cyber-attack that usually involves repeated attempts to log in to online accounts using usernames and passwords stolen from other online services. It takes advantage of humans' natural tendency to reuse passwords to deal with the ever-increasing number of online accounts that need to be managed- the threat actors knew that usernames and passwords used on one website could also be used on the other six and are happily exploiting this weakness.

Unlike many other types of cyberattacks, credential stuffing attacks often require little technical knowledge. **Threat actors often use free, easily accessible software that can broadcast hundreds of simultaneous login attempts without any human intervention.** A single threat actor can easily send hundreds of thousands or even millions of login attempts to a single web service.

Although most login attempts fail in a credential stuffing attack, due to the sheer number of attempts, **a single attack can still result in thousands of accounts being compromised.** Threat actors have several ways to monetize these compromised accounts, for example, by using a credit card saved by a customer to make fraudulent purchases; stealing and selling gift cards that a customer has saved on an account; using customer details stolen from an account to conduct a phishing attack, or by simply selling login credentials to someone else on the dark web.

ACCOUNT TAKEOVERS (ATO)

An account takeover is an identity attack in which attackers gain unauthorized access using a variety of attack vectors, including credential stuffing, phishing, and session hijacking, to gain access to customers' legitimate accounts and steal something of value. In layman's terms, someone logs into an account that isn't theirs, often referred to as "account hacking."

Account takeovers are used by threat actors in various ways, for example, to steal sensitive personal information, impersonate the account owner, gain access to funds and/or payment cards, as an entry point to defraud the owner's contacts or other fraudulent schemes.

It is important to note that **ATO fraud is not limited to bank and credit card accounts**: attackers could also use reward cards and services, including points saved on hotel accounts and airline miles. This scam is gaining traction because targeted users rarely check their reward accounts for scams compared to credit cards and bank accounts.

ATOs usually start with the above-described credential stuffing techniques and are automated using scripts that contain potentially thousands of credentials and user accounts. Revenue generated from a successful advanced attack can reach millions on darknet markets.

The emergence of darknet markets has popularized account takeover attacks: Attackers no longer need to steal directly from targeted users, which reduces personal liability. On the contrary, attackers looking to steal directly from users can simply purchase valid accounts on darknet markets without completing the tedious task of password cracking. The increase in financial accounts and products has additionally populated the market. Targeted users often have many financial accounts spread across multiple websites, making them attractive to threat actors. More financial accounts and an online presence means an increased attack surface for ATO fraud.

When attackers choose to sell authenticated accounts, they are expecting a have a high payout for their efforts: the value of just one hacked account depends on the amount of data stolen and the type of account. With potentially thousands of accounts, an attacker could have a hefty payday selling on darknet markets and limit detection compared to directly stealing from victims.

IMPACT

Exposed Customer Credentials might not seem like one of the business's responsibilities, as long as they are not the result of an internal breach, however, they can be very damaging, not only to the business's brand reputation but also have financial and even legal implications. Furthermore, it should be kept in mind that, with a high probability, users will blame the business for any damage occurring through exposed credentials and account takeovers, blaming it on the company's lack of security and fraud-prevention measures.

FINANCIAL IMPLICATIONS

- Increased Transaction Disputes
- Increased Chargebacks
- High Customer Churn
- Revenue Loss
- Eventually Financial Penalties/Fines

Chargebacks are a huge cost for e-commerce websites, especially those using a third-party payment gateway. When the chargeback rate is high, compared to the total number of sales, the processing payment gateway company might raise the transaction fees, which can translate to very significant losses. Therefore, credit card chargeback prevention is vital for any business.

REPUTATIONAL IMPLICATIONS

- Brand/Image Degradation
- Customer Churn
- Financial Penalties/fines
- Reputational Loss with Financial Institutions

Brand and reputation may suffer, as the company may find itself unfairly accused of a data breach, which might lead to negative publicity, fines, and lost business. Furthermore, loss of customers and future revenues may occur, as customers whose accounts are taken over lose trust in the brand and walk away, creating bad publicity for the company.

HOW TO IDENTIFY A COMPROMISED CUSTOMER ACCOUNT

Attacks resulting in exposed customer credentials often can be identified by the organization mainly after a customer files a claim or complaint. Proper bot and online fraud protection should be the minimum that a business implements on their online assets in order to detect this kind of attack and prevent the exposure of customer credentials and account takeovers. Below are some important signs to detect attack takeovers on the business's websites:

- **IP Addresses from unusual geographic locations** - a sudden rise of IP addresses from one or more countries outside the usual access locations can be a good indicator of attacks using exposed customer credentials. Particular attention should be directed at changes in the access location for accounts with recent account changes.
- **Multiple Accounts Share the Same Details** - when similar changes to PIIs (email, delivery address, etc.) are applied across more than one account, it might be a sign of an account takeover attack.
- **Unknown/Obfuscated Device Models** – a higher-than-usual ratio of unknown devices, is a warning sign.
- **Multiple Accounts accessed by the Same Device or IP** - often attackers do not spoof or mask their device between logging into different accounts, meaning that if they steal and access more than one account, they will all be linked to one device. However, this indicator should not be considered stand-alone proof, taking into account cases when devices are legitimately shared by multiple.
- **Detection of Suspicious VPN Proxies or TOR Usage –** any other use of emulators and virtual machines
- **Unusual Number of Chargeback Requests**
- **Mass Login Attempts on one Account**
- **Mass Password Reset Requests**
- **Unusually Large Purchases OR Large Transfers**

RECOMMENDATIONS

Compromised Customer credentials are so prevalent that most businesses cannot avoid them. Therefore, any company that maintains online accounts for its customers should have a data security plan that includes strong safeguards to protect customers.

Furthermore, account takeovers involving compromised customer credentials are difficult to detect because they rely on social engineering techniques: threat actors may impersonate the victim or use other methods to trick the account holder into giving them their login information. Account owners often do not realize that their account has been compromised until it's too late.

Like with everything else, organizations should look to a holistic approach when it comes to their cyber-defense, as there is no single measure or technology that can achieve total coverage. Even the Multifactor Authentication can be bypassed. More information about this topic can be found in Cyberint's report "Cookie O'clock." Therefore, it is highly recommended to put in place different complementary solutions to minimize both risk and impact. Companies should also consider how strong their defense mechanisms are in all threat stages: before, during and after an attack.

Furthermore, it is important to note that the effectiveness of the recommendations mentioned above will likely change over time as threat actors adopt new tactics and techniques. Businesses should regularly evaluate the effectiveness of their own controls and implement new adequate strategies.

IMMEDIATE STEPS

- **Freezing the Compromised Account** – to prevent the threat actor to perform any fraudulent activities on the compromised account.
- **Freeze/Cancel all ongoing Transactions** – ask for verification from the legitimate Account Owner
- **Forced Password Reset**
- **Informing the legitimate Account Owner**

CREDENTIAL THEFT

Continuous cyber-hygiene can help prevent attacks, as well as mitigate their impact if and when one happens. Threat actors are constantly testing new ways to exploit the company's and customer's infrastructure, so remaining static when it comes to security protocols is a sure way to get breached.

- **Education** is key to mitigating attacks. It is in the interest of both parties, companies, and customers, to know how to identify potentially malicious activity. The ability to recognize when credentials might be compromised can save a huge amount of pain and financial loss.
- **Smart Password Use**: Password reuse should be avoided at all costs, as well as a strong password policy should help to prevent credential theft.
- **Strong Password Policies** prevent the risk of easy-to-guess passwords.

- **Multifactor Authentication (MFA)**: a threat actor is less likely to have access to more than one factor of the authentication process.

CREDENTIALS STUFFING

3. Defending against credential-stuffing attacks:
    - Bot Detection
    - Multifactor Authentication
    - Preventing Reuse of Compromised Passwords
4. Detect credential stuffing violations:
    - Monitoring customer activity
    - Monitoring customer fraud reports
    - Monitoring of account activity
5. Prevent fraud and misuse of customer information:
    - Threat Intelligence and third-party fraud detection (as provided by Cyberint)
    - Re-authentication at the time of purchase
    - Preventing Gift Card Theft
6. Respond to credential-stuffing events:
    - Investigation and Remediation of the incidents
    - Notifying Customers

ACCOUNT TAKEOVER

Users and website owners should take basic precautions to prevent ATO attacks:

- Users should always read emails from financial institutions and call customer service immediately after receiving suspicious alerts.
- **Educating customers**:
    - Dangers and warning signs of phishing
    - Investigating links in emails before clicking
    - Smart Password Use
- **Deployment of MFA**
- **Set a limit on login attempts**
- Configuring the fraud detection systems to display a CAPTCHA after a specific number of authentication attempts
- Send notifications of any account changes to customers

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City