nevis®

Making security an experience

White Paper

Credential Stuffing

In recent years, credential stuffing has developed into one of the preferred methods used by cybercriminals due to the clever automation possibilities. Read on to learn what makes credential stuffing so dangerous and how you can protect yourself against it.

Content

Introduction

The goal of every company and authority is to offer its customers a unique, individual and secure user experience. And for good reason: ensuring convenient access to online user accounts and the associated services builds customer loyalty and economic success. In addition, however, the security of individual user accounts must be guaranteed at all times.

Unfortunately, the security of user data for online accounts is often still not as good as it should be. One frequent reason for this is the lack of effective security measures for user authentication. However, users themselves are often guilty of not taking the protection of their personal login data seriously enough – and are taking unnecessary risks as a result.

This is why credential stuffing has emerged in recent years as one of the most effective methods used by cybercriminals to gain access to sensitive data in third-party online accounts and to manipulate or misuse this data. This can have catastrophic consequences – and not just for the affected users. Other service providers and companies can also suffer enormous damage – both in terms of tangible financial losses as well as reputational damage. Customers whose data is compromised will depart and be forever lost for future business – and they will do so in large numbers.

On the following pages, we explain how credential stuffing works and present strategies to minimize the risk of account takeovers (ATO).

What is credential stuffing?

The term 'credentials' refers to the login data that users type in when they log onto an online user account. 'Stuffing' describes the automated process used to 'fill out' these types of login input screens.

With credential stuffing, cybercriminals simply try out many combinations of user names and passwords in order to gain access to user accounts. Rather than doing things merely by hand, a systematic approach is taken: They utilise automated bots that con process thousands of possibilities in a very short time.

But why has the scam tactic of credential stuffing become so much more important in recent times? Because it is so easy to use and does not require significant expenditure by the cybercriminals. **In 2019 alone, 80 percent of attacks against web applications were launched using stolen login data**.

What distinguishes credential stuffing from a brute force attack?

Whereas brute force attacks simply involve trying out random password combinations in order to achieve a few hits after numerous attempts, credential stuffing attacks are based from the outset on existing and genuine combinations of user names and passwords. This is why even complex passwords no longer present an obstacle to cybercriminals using this method. However, the stolen login data may be out of date and may not necessarily lead to the desired result. Despite this, the likelihood of it yielding one or even multiple hits is extraordinarily high. Insiders put the success rate of attacks using credential stuffing in the range from 0.5 to 3 percent.

How does this differ from social engineering?

Social engineering involves phishing (or 'angling') for passwords. For example, emails that appear deceptively genuine lure users to fake websites of their bank or another important institution – where they unwittingly share their user data with criminals when they try to log in. In the case of credential stuffing, the online fraudsters are already in the possession of unique combinations of user names and passwords. All they have to do is to 'feed' the data into various online portals with the help of bots until they achieve a hit with a valid combination.

How do cybercriminals get hold of the account data of other users?

In the Darknet, it's possible to find what are called 'combo lists' (such as the notorious 'Collection X'), in which a total of around 3.3 billion unique combinations of user names and passwords are compiled in searchable databases (as of early 2021). This data often originates from major cyberattacks against the online portals of Gmail, LinkedIn, Microsoft, Napster, Netflix, Nintendo, Zoom or from the world of cryptocurrencies. These lists are equipped with convenient tools that can typically be used to fool bot detectors (CAPTCHA tests such as the series of images in which one must identify different features like bridges, traffic lights, trucks or similar items before you can log in).

A lucrative trade in lists, bots and additional tools is conducted among cybercriminals. All the same, these basic requirements for credential stuffing attacks can usually be purchased very cheaply – sometimes they are available free of charge. In 2020, for instance, security firm Cyble **purchased over 530,000 data records from stolen Zoom accounts for a mere 0.0020 US Cent each**. This makes credential stuffing all the more attractive for fraudsters – because the potential 'yield' from an attack does not require any substantial investment.

Money is no obstacle: credential stuffing tools available at bargain prices

In the report Credential Stuffing 2021, the security experts at F5 provide a startling calculation that shows just how little cybercriminals need to invest in their credential stuffing activities:

Access to the login data of 2.3 billion users	$ 0,00
Tool configuration	$ 50,00
100,000 CAPTCHAs ('Completely Automated Public Turing test to tell Computers and Humans Apart')	$ 139,00
10 global IPs	$ 10,00

This means:
100,000 account takeover attempts (ATO) can be purchased for less than 200 USD.

Credential stuffing – an easy game for cybercriminals

Even cybercriminals who are not technically skilled can quickly gain unauthorised access to the online accounts of unsuspecting consumers or company employees with the help of credential stuffing. This is particularly effective with B2C companies that communicate with their customers mainly via a website, online shop and smartphone apps – and where user accounts are accessed with a user name and password without additional secure authentication procedures.

Why you should take the threat of credential stuffing seriously

Nowadays, credential stuffing attacks account for 29 percent – by far the largest proportion – of attacks against user accounts. According to Aberdeen Strategy Research, **76 percent of B2C companies in the EMEA economic region reported that the account data of their online customers had been successfully compromised** in the past year. It is estimated that credential stuffing attacks account for around one in every 20 login attempts. The IT security firm Shape Security even assumes that, on average, 80 to 90 percent of the login traffic of any online shop can be traced back to credential stuffing attacks.

Attacks often go unnoticed

Many credential stuffing attacks are not even noticed because they do not intrude into the technical infrastructure and do not exploit any IT security vulnerabilities. What's more, most attacks are launched via botnets from multiple IP addresses – which makes it more difficult to identify and block the perpetrators.

Cybercriminals profit from our laziness

It's often the innocent users of online accounts themselves who make it even easier for attackers to cause catastrophic damage. According to the Nevis Security Barometer 2021, for example, 44 percent of consumers in Germany have used the same passwords for years and for multiple user accounts, some of which have long since been closed. A particular shocking finding of a CyLab study by Carnegie Mellon University is that **only 33 percent of users change their access data even if a privacy breach is uncovered**. A leaked password open the gates wide for cybercriminals – often to multiple accounts with different online services.

What do cybercriminals do with stolen login data?

The study by Aberdeen Strategy Research discovered that the consequences of credential stuffing can be extremely varied. Affected B2C companies in the EMEA region mainly had to deal with the following:

- *Setting up new accounts (e.g. credit applications) –* ***34%***
- *Fraudulent transactions –* ***39%***
- *False chargebacks –* ***18%***
- *False refusals –* ***34%***
- *Transfer of money and other valuables (for example, premiums or loyalty points) –* ***11%***
- *Fraudulent purchases (for example, consumer items or value cards)*
- *Theft of digital content and services (for example downloads or the use of streaming services)*

Which industries are particularly affected by credential stuffing?

In reality, credential stuffing can affect all sectors in which the customer journey is based to a certain degree on online customer accounts:

The traditional financial sector

All providers of financial services (current, savings and business accounts, certificates of deposit, company and personal loans, mortgages, etc.) for companies and private individuals

- Business banks
- Credit unions
- Regional savings banks

FinTech

Providers of technology-based financial and insurance services such as

- Cryptocurrency exchanges
- Digital extension of credit
- Mobile payment systems

Insurers

Providers of insurance services for consumers

- Property and liability insurance
- Household contents insurance
- Car insurance

Telecommunications

Providers of telephone, Internet, cable TV and streaming services that are linked to online accounts

Energy providers

Electricity, water and gas utilities with online customer accounts

Healthcare

Hospitals, doctors and other service providers from the healthcare sector who process the cost and administrative expenses of therapies for their patients through health insurance policies. Online treatment services such as Tele-Health or mobile apps also play a role here in achieving the desired health outcomes.

Online shopping portals & online marketplaces

Amazon, eBay & others

Social media platforms

Facebook, Instagram, LinkedIn, etc.

Consumer electronics

Manufacturers of modern TV devices, smart-home infrastructures and smart household appliances, which are linked to online accounts

The computer and video-game sector

Providers of computer and video games that are linked with online access

Online gambling

Providers of online poker and casino games or sports betting services

How credential stuffing harms companies

In its study, Aberdeen Strategy Research investigated the effects of credential stuffing on ten different B2C sectors. The conclusion? **Account takeovers (ATO) have now reached a level that is causing significant economic damage in all B2C categories examined in the EMEA region**. It's also interesting to note that **ATOs have the most serious impact on the three sectors with the comparatively lowest profitability – property and accident insurance, healthcare providers and online gambling**.

Credential stuffing attacks not only cause financial losses, but also additional work and bureaucratic expense. Added to this are the long-term effects such as the loss of trust among customers or a tainted company reputation:

- Privacy violations with customers
- Additional service and support costs
- Outages caused by IT maintenance work and downtimes
- Integration of call centres for processing customer enquiries about privacy breaches, help resetting passwords, etc.
- Reduction in the total number of monthly active users. Users who leave for security reasons and close their accounts
- Loss of market share to competitors
- Stricter controls by industry supervisory bodies

How users can protect themselves against credential stuffing

The first security check

Many users ask themselves whether their access data for various online accounts is still secure. Different security companies now offer simple online tools that can quickly check whether email addresses, passwords or even mobile phone numbers appear in the combo lists used by cybercriminals for credential stuffing attacks. One example of a very reliable, effective and absolutely secure service is **haveibeenpwned.com**, which allows you to find out in seconds whether your login data has been compromised and is circulating in the relevant lists. If so, change the passwords affected as soon as possible!

Use as many different passwords as possible

Anyone who uses the same password for multiple user accounts runs the risk of cybercriminals hacking into multiple accounts with a credential stuffing attack. This is why we recommend that you create a unique password for every online account. The password should also be as complex as possible.

Change passwords regularly

The more often you change passwords, the lower the probability of your current login data being used for credential stuffing attacks.

Password managers – helpful memory aids

Admittedly, it is difficult to remember complex passwords – all the more so since most people have a whole range of online accounts. This is why many users often use just one password for multiple accounts for the sake of convenience – which also makes them particularly vulnerable to attacks by brazen online fraudsters.

However, a solution is available in the form of a password manager, which can even generate complex passwords and save them for the next login. This takes a load off your mind – you simply have to remember the access data for the password manager. Naturally, even password managers cannot guarantee total security – as they can also be hacked under certain circumstances by fraudsters. This is why it is always good if companies reinforce online access procedures using passwords with additional security mechanisms that even cybercriminals struggle to overcome…

Security checklist for online users

- ☑ Regularly check using trustworthy online services such as **haveibeenpwned.com** whether the user names, email addresses, passwords and mobile phone numbers you use have previously been compromised.
- ☑ Chose a separate, unique and complex password for every online account.
- ☑ Change your passwords regularly.
- ☑ Use a password manager to simplify logins with complex passwords that are generated automatically.

How companies can repel credential stuffing attacks

Passwords are an ancient instrument for protecting data against unauthorised access – and from a modern perspective, they are neither secure nor user-friendly. Is has become all too easy for crooks to hack into online accounts that are only protected by user names and passwords. This problem will further intensify in the coming years given the possibilities of quantum computing. This is why many companies already rely on the convenience of modern customer identity and access management packages – these offering enhanced security functions for recording and managing customer data.

How to escape the password dilemma: biometrics

Given the technical capabilities of modern computers and smartphones, the password as a 'security factor' for user accounts has long since become obsolete. Biometric features such as fingerprints, iris scans or facial recognition offer virtually insurmountable protection against online fraudsters – and the vast majority of devices available today have long since incorporated the ability to use these types of technologies for user authentication.

The benefits of biometric features for user authentication:

- **Maximum protection:** Biometric features such as fingerprints, iris and facial features are unique to every person and therefore virtually forgery-proof
- **Logins without passwords:** The use of biometric features for user authentication renders the unsecure process of user names and passwords obsolete
- **Maximum user convenience:** Biometric user authentication offers a far more convenient way to access an online account. For example, a fingerprint scan that takes just seconds can replace the tedious process of remembering and typing in passwords
- **Greater customer frequency and customer loyalty:** Improved security and usability when it comes to accessing an online account makes the customer journey more attractive and turns it into a positive experience
- **Good for the company image:** These days, reliable protection against online fraud is one of the most important factors for a first-class company reputation

Two-factor authentication (2FA) and multi-factor authentication (MFA)

The security of online accounts can be further enhanced if two (2FA) or more (MFA) identity checking procedures are used during the login. For example, the login procedure for the user account can require different factors:

- **Something that the user knows:** For example, a password, a PIN or other information that only the user has access to
- **Something that the user is:** Unique biometric features such as fingerprints, facial features or the iris
- **Something that the user possesses:** Logging into the user account requires that it is unlocked by a second device – typically via an authentication app on a smartphone or an external token

Since online fraudsters involved in credential stuffing only have access to stolen user names and passwords, they are unable to overcome the additional security barriers presented by two-factor and multi-factor authentication.

Even more convenient and secure: the FIDO standard

Thanks to globalisation, business and consumer behaviour today has become international. We transact with companies on the other side of the planet and order goods from providers that have global reach. The customer data associated with bank accounts and credit card numbers is often stored on foreign servers and used for transactions all over the world.

With this in mind, the FIDO alliance, which was founded in 2012, develops international standards to enable simple, quick and secure authentication on the Internet. The latest FIDO2 standard systematically harnesses the capabilities of modern hardware. Newer computers and smartphones equipped with crypto chips and the Trusted Platform Module (TPM) have access to technologies that use a secret security key to uniquely authenticate a user who wants to access an online portal. This security key cannot be read out and cannot be hacked by cybercriminals.

CIAM: efficient customer identity management for companies

Customer identity and access management (CIAM) is the latest and greatest way to record and manage customer profiles. CIAM combines all processes relating to user accounts for companies. More importantly, these customer identity management systems deliver a consistent, secure and positive customer experience across all platforms – from laptops to tablets and smartphones.

The benefits of a powerful CIAM system:

- Customer registration
- Self-service account management for customers
- Consent & preference management for personalising customer accounts while also adhering to all privacy regulations
- Data access governance & management for managing and controlling access rights to all types of data
- Optimum protection against cybercriminals and unauthorised data access by means of two-factor and/or multi-factor authentication and single-sign-on processes (SSO)
- The possibility of using biometric data in the authentication process
- Support for FIDO standards
- Takes account of all international data protection regulations

Conclusion: credential stuffing can be effectively avoided today

Anyone who still relies exclusively on combinations of user names and passwords to secure customer accounts is guilty of gross negligence. Despite this, there are still countless companies that are unwittingly playing into the hands of cybercriminals involved in credential stuffing attacks in this way. In doing so, they're not only risking irreparable damage to their reputation – but also a mass departure of customers. **According to a study by PriceWaterhouseCoopers, a single negative experience can cause one fifth to one third of customers to turn their backs on a company or a brand forever**. In reality, today's customers expect three things above all else:

- **The best possible customer experience:** A seamless, convenient user experience across all hardware platforms
- **Quick reactions:** Prompt, perfectly coordinated services
- **Reliable data protection:** Optimum preventive measures against privacy breaches and the compromising of critical personal data

A modern system for customer identity and access management (CIAM) optimises a company's ability to meet the high expectations of customers today and strengthens their loyalty to companies and brands. The justified desire for user-friendliness, security and privacy can easily be met with sophisticated technologies for two-factor or multi-factor authentication.

The costs of implementing a CIAM solution are manageable – and a worthwhile investment to prevent the inevitable loss of image and customers that would result from a successful credential stuffing attack.

nevis®

Making security an experience

About Nevis

Nevis develops security solutions for the digital world of tomorrow. Our portfolio includes passwordless logins, which are intuitive to use and offer optimal protection of user data. Nevis is the market leader for Identity and Access Management in Switzerland, and it protects over 80 percent of all e-banking transactions. Government authorities and leading service providers and industrial companies across the globe rely on Nevis solutions. The specialist in authentication operates offices in Switzerland, Germany, the United Kingdom, and Hungary.

These materials are provided by Nevis Security AG for informational purposes only, without representation or warranty of any kind, and Nevis Security AG shall not be liable for errors or omissions with respect to the materials. The only warranties for Nevis Security AG products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, Nevis Security AG has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein.

This document, or any related presentation, and strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by Nevis Security AG at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

Follow us

www.nevis.net