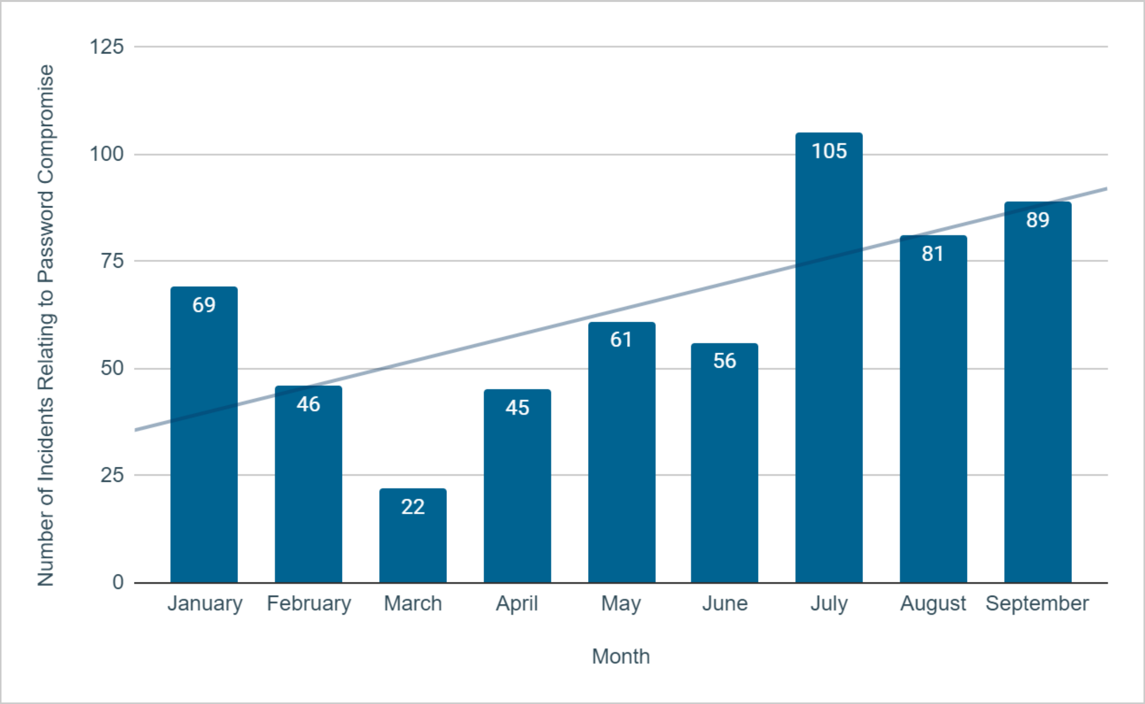
Wr0ng P@$$w0rd! : Hackers Continue to Thrive on Weak Passwords

Author: Hansika Saxena

Editor: Deepanjli Paulraj

Cyber security and data preservation is primarily dependent on secured authentication. Despite their multiple flaws, passwords have long dominated authentication systems and continue to do so. Its irreplaceability stems from its unparalleled deployability and ease of use. Although security experts have proposed numerous methods for securing passwords, the security of user-selected passwords remains a major concern.

According to XVigil data, 11.4% of underground activity recorded in the first three quarters of 2022 was related to password compromise or tools and services to aid in the same. Passwords from approximately 4 billion records were compromised. Over time, cybercriminals have shown an increased interest in compromising passwords and have discovered numerous efficient methods to crack strong passwords, such as password guessing, dictionary attack, hash guessing, rainbow table, password sniffing, brute force attack, etc.



Number of password compromised incidents observed in the first 3 quarters of 2022

A good password system should be able to prevent not just unauthorized users from accessing the system, but also logged-in users from performing actions they are not permitted to perform. In this paper, we discuss the various password related issues and how users can ensure their protection against the oldest breach method known to man.

The Bane of Weak Passwords Continues

Passwords are only as strong as the number and uniqueness of characters used to create them. Due to the increasing number of data breaches, websites need users to adhere to a specific set of minimal requirements for a string of characters to pass as a password. These typically require passwords to be strings of 8 to 15 characters long that contain at least one capital letter, one special character, one small letter, one number, and so on.

In order to comply with such password creation policies, users frequently engage in one or more of the following poor password creation practices:

- Using certain basic terms and common words (such as P@$$w0rd, qwerty, 12345, etc.)
- Simple-to-remember strings that include personal information such as their birth dates, pets' names, etc., that hackers can gather from social media and previous data breaches. .
- Reusing the same password across multiple accounts. Research shows that about 40% of individuals reuse 81-90% of their passwords.

Passwords are also seriously threatened by improper coding practices on the part of developers. Embedded credentials (also known as 'hard-coded credentials') are plain text, unencrypted credentials that are embedded within code.

The XVigil GitHub repository monitor was able to record a total of **11,850 compromised credentials** in 2022. Embedded credentials may be:

- Set as the device's factory default.
- Included by a person into the code, such as through the use of a DevOps tool or data repository.
- Incorporated in applications and used for app-to-app communications.

Types of Password Attacks

A password attack involves taking advantage of a system authorization flaw while making use of some automatic password attack tools to expedite the password-cracking process. Given that the username-password combination is one of the more established means of account authentication, attackers have developed numerous strategies for guessing passwords that are easy to crack. The following section discusses the four most typical password hacks employed by hackers.

Non-electronic Accounts

This is frequently the attacker's initial attempt to obtain target system passwords. No technical knowledge is required to carry out these attacks, hence they are also referred to as non-technical attacks. The most common types are as follows:

Shoulder Surfing

Literally looking over someone's shoulder as they type in a username and password.

Social Engineering

- Sending phishing emails or texts to users in order to trick them into clicking on a link that installs malware (such as keyloggers, information stealers, etc).
- Scanning at a user's social media accounts for personal information such as birth dates, pet names, etc.

Eavesdropping

Password eavesdropping is the exposure of a password as a result of being overheard. This can be accidental or intentional and includes both voice and digital eavesdropping.

Dumpster Diving

A low-tech method of gathering information that involves retrieving documents (mostly notes), from the trash, that contain information.

Active Online Attacks

This is probably one of the simplest ways to gain unauthorized administrator-level access to a machine. In this method, an attacker actively communicates with the target to gain password access by applying a variety of password-creation techniques. Many a time attackers generate potential password combinations by gathering data from social media accounts or other online sources and even use the default password provided by manufacturers.

Brute Force

This is the easiest and most common method of attack, where a program creates passwords by experimenting with different combinations of letters and digits, starting with weak and obvious passwords. This is a rather slow process that requires hackers to switch between accounts in order to evade lockout detection tools. Two most common types of brute forcing techniques are:

- **Credential stuffing:** This method relies on users' tendency to use the same password across multiple accounts. Attackers stuff credentials (from a list of stolen usernames and passwords) on different accounts, until they find a match.
- **Password spraying:** This involves testing a few widely used passwords on multiple accounts at once. On portals using single sign-on or cloud-based authentication, this technique can prove to be quite risky.

Dictionary Attack

This method exploits the fact that individuals frequently choose simple terms and short passwords. Hence, the attacker attempts to access accounts by utilizing a curated list of words including numbers and alphabets (dictionary) or a program that cycles through popular combinations.

Malware

Malware or viruses such as keyloggers, trojan, spyware, etc., that operate in the background and monitor keystrokes and passwords are used by attackers to identify usernames, passwords, and the websites on which each was used. This method of credential stealing typically depends on the user falling for another attack (such as phishing) that downloads the program on their device.

Hash Injection

Using a compromised hash that is injected into a local session, an attacker can obtain the hash for the domain admin account which in turn can be used to log into other systems.

Spidering

Spidering is a password hacking technique that exploits the fact that most businesses use passwords that incorporate some sort of corporate information. A potential attacker only needs to collect this data from business websites, social media accounts, etc. and utilize it to create word lists which can then be used in a dictionary or brute force attack.

Passive Online Attacks

A passive online attack has no effect on the system whatsoever. In this, instead of communicating with the machine, the attacker passively observes the data flowing to and from the system over the channel. The observed data is then used by the attacker to enter the system. One of the following techniques are usually used to perform passive online attacks:

Wire-sniffing/Traffic Interception

The attacker uses software, such as packet sniffers, to monitor and record network traffic. With any luck, they are able to capture some confidential information or passwords.

Man-in-the-Middle Attack

Much like wire-sniffing, the attacker's application keeps a track of information as it flows. However, with this technique, the software is introduced into the stream of activity while typically pretending to be a website or application.

Offline Attacks

Password hashing is the process of converting a plaintext password into an incomprehensible string by running it through a hashing algorithm (such as SHA, MD5, bcrypt, etc). Once a string of characters (in this case password) is hashed it is impossible to reverse it , i.e. you can not "unhash" or "dehash" it.

Password attacks that attempt to retrieve clear text passwords from a password hash dump are referred to as offline attacks. These attacks are usually time consuming but also frequently successful. The following are the most popular methods used by attackers to carry out offline attacks:

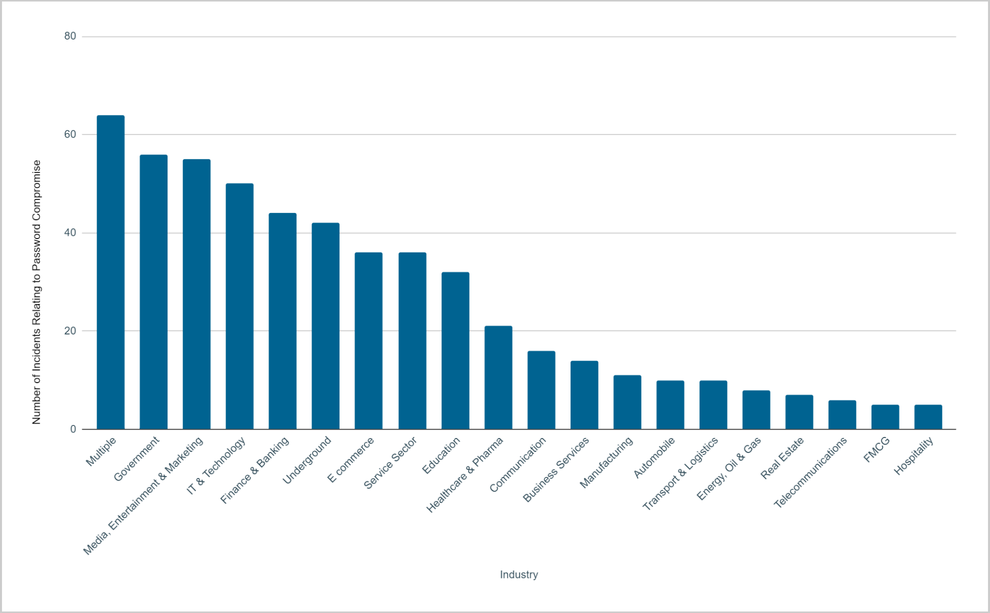
- **Rainbow Table Attack**
  The Rainbow table is a complicated and strong security mechanism that contains a list of commonly used passwords along with their pre-computed hashes. The attacker runs algorithms to crack the password by comparing its hash with the values in the rainbow table. This is a rather time-consuming yet efficient approach.
- **Distributed Network Attack (DNA)**
  DNA is a new and modified approach to rainbow table technology. Instead of using the processing power of a single machine, it makes use of the processing power of machines across a network to recover passwords from hashes via rainbow tables.
- **Pass-the-Hash (PtH) Attack**
  PtH enables an attacker to access a resource by using the underlying NT LAN Manager (NTLM) hash of the password instead of the user's real human-readable password. Almost any server or service that accepts LM or NTLM authentication is susceptible to PtH attacks. Although PtH usually targets Windows operating systems, they can also be used to take advantage of Linux and Unix endpoints.

Major Trends Observed in 2022

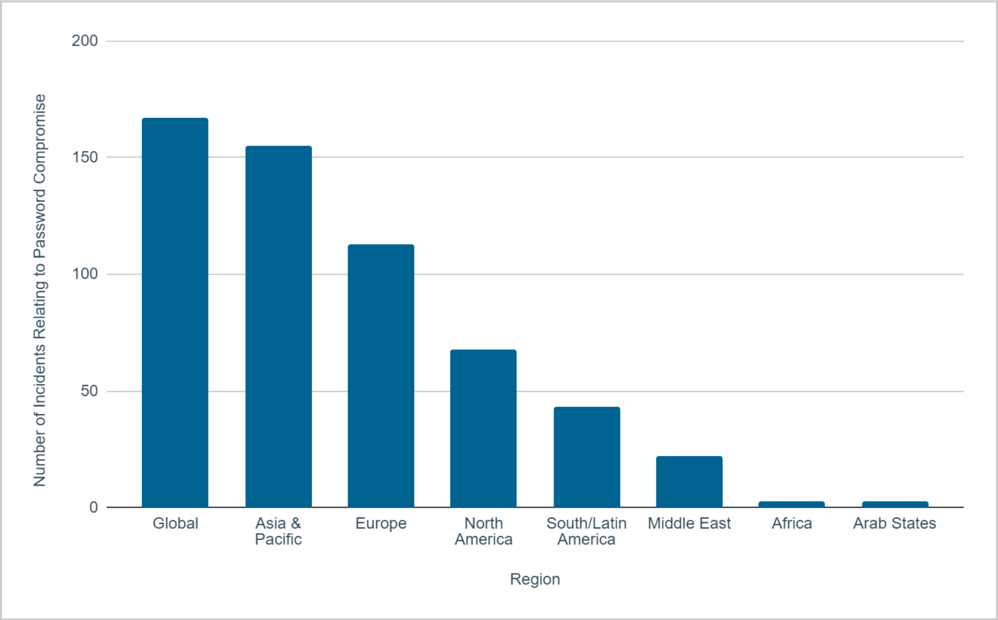
Data collected by XVigil reveals some really interesting patterns in the industries that were most frequently targeted by password compromise and other related attacks. The most targeted sectors were government, media, information technology, and finance, which highlights two interesting facts:

- Attackers maximize their profits by focusing on these industries.
- Individuals in this industry are more likely to engage in bad password practices (such as using weak passwords, reusing passwords, etc.).

Another intriguing observation was that the issue of password compromise is not limited to any particular region, but is a global one.



Number of password compromise incidents observed in various sectors



Number of password compromise incidents observed in various regions

Preventive Measures

As people's reliance on digital systems grows, so does the number of cyberattacks. In the event of a security breach, attackers typically target passwords and authentication systems first. As the trend suggests, implementing a few password security measures can benefit people all over the world. The following is a list of preventive measures that will prevent individuals from becoming easy prey for cybercriminals.

The Not So Secret Password Recipe

It is no longer a secret that poor password hygiene leads to the success of a majority of password cracking incidents. Although measures like using a combination of capital and lowercase characters, numbers, and symbols, etc., won't totally safeguard you, it will greatly discourage hackers. Here, is a short list of things to remember while creating your passwords:

- Create passwords of length greater than 20 characters
- Use a variety of characters including numbers, symbols, etc.
- Avoid using incremental patterns, common phrases, personal information, website names, etc.
- Use a password generator and management tool (Refer to the Password Managers section)
- Reset and rotate passwords regularly
- If possible, use features like single sign-on, multi-factor authentication (MFA), biometric authentication, etc.

Foster Strong Password Policies

By creating specific password policies, organizations can help to prevent password hacks and encourage individuals to adopt better password standards.

- Design a lockout policy, i.e. a policy which freezes accounts after a predetermined number of incorrect password entries
- Necessitate the use of password management and generation tools
- Have scheduled and mandatory password resets
- Use technology that is more difficult to breach, such as MFA, biometric authentication, etc.
- Implement risk-based authentication (RBA) systems

Will New Technologies Reduce Password Attacks?

Technology improvements have made it easier for threat actors to crack users' passwords over time, but they have also given software engineers the freedom to create tools that make it easier for consumers to construct secure passwords without having to remember them. Here are two important technologies that would help businesses and individuals protect their passwords.

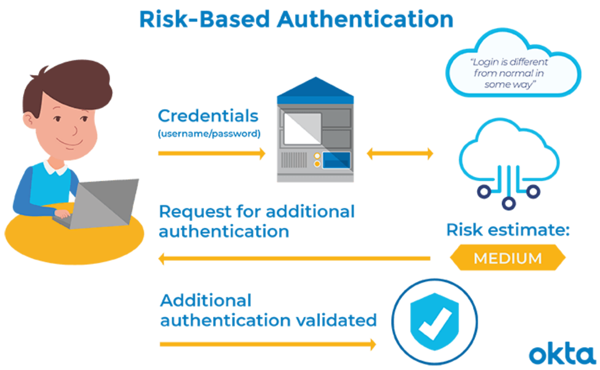
Password Managers

These are one of the most useful and helpful tools that allow individuals to store, generate, and manage their passwords for various local applications as well as online services. Typically there are three types of password managers (PMs):

- **Browser built-ins**: As the name suggests, these are provided and built into browsers such as Google Chrome, Microsoft Edge, Internet Explorer, Firefox, etc.
- **OS built-ins:** These are built into operating systems. For example, Keychain by Apple, Samsung Pass, etc.
- **Standalones:** These PMs are typically provided by third party vendors and have to be installed separately. For example, Dashlane, 1Password, LastPass, KeePass, RoboForm, etc.

Security professionals strongly recommended the use of PMs to address the majority of current password authentication problems. However, an aversion has been noticed in the usage of PMs, mostly because users do not fully trust these programs. A possible solution to this problem can be using the most popular and open-source PMs such as Google Chrome's PM , Bitwarden, and KeePass.

Risk-Based Authentication (RBA)


Risk-Based Authentication
"Login is different from normal in some way"
Credentials
(username/password)
Request for additional authentication
Risk estimate:
MEDIUM
Additional authentication validated
okta

Infographic explaining RBA (Source: Okta)

RBA is a flexible security technique to enhance systems that use password-based authentication. During a login session, the RBA monitors various features and if the values of observed features considerably deviate from those previously seen, users are required to give additional authentication information for verification. Although RBA offers the potential to provide more usable authentication, its usability and security perceptions have not been thoroughly researched. There are a number of RBA softwares available in the market such as Duo Security, Kount, Sift, Okta Adaptive Multi-Factor Authentication, IBM Security Verify, etc.

Conclusion

The traditional text-based password system is the most widely used and easily obtainable authentication system. However, as previously stated, it has numerous limitations. While security relies on a variety of tools, passwords are one of the most basic and yet effective ways to prevent cyber attacks.

Depending on the data hosted by the application, compromised passwords can allow sensitive information to be exposed, distributed denial-of-service attacks, financial fraud, and other sophisticated attacks. The recent hack on Uber shows that a single password hack on a company's system can take many forms and harm or disrupt the normal operation of the entire organization.Thus, being proactive on the password front will help in better security of individuals and businesses.

References

- Uber’s Intranet Compromised Via Social Engineering - CloudSEK
- Generating and Managing Strong Passwords using Hotel Mnemonic
- BioTouchPass: Handwritten Passwords for Touchscreen Biometrics
- Image Based Password Authentication System
- 4 TYPES OF PASSWORD ATTACKS COMMONLY USED BY ETHICAL HACKERS
- Password Attacks | Infosavvy Security and IT Management Training
- Everything You Need to Know About Password Attacks and Prevention
- Microsoft warns over uptick in password spraying attacks | ZDNET
- Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply chain to give context to our customers’ digital risks.

To learn more about CloudSEK, visit https://cloudsek.com/.