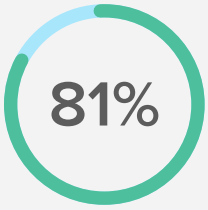
5 Identity Attacks That Exploit Your Broken Authentication

okta

5 Identity Attacks That Exploit Your Broken Authentication

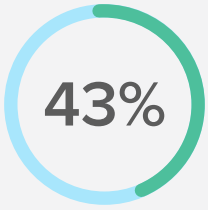
Stolen or Weak Passwords



of breaches leveraged either stolen and/or weak passwords.

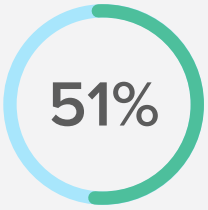
Social Attacks

Social attacks, such as phishing, accounted for



of attacks that resulted in a data breach.

Credential-Stealing Software



of data breaches involved some form of credential-stealing malware.

Traditional authentication methods that rely on usernames and password integrity are widely considered to be broken. In fact, “Broken Authentication” sits at #2 in the OWASP Top 10 for application security risks. As organizations begin to move more sensitive data to cloud apps to take advantage of the productivity gains, the traditional perimeter expands to wherever the user is logging in from.

In other words, the identity becomes the perimeter.

Threat agents have recognized this as a security gap and are exploiting the natural proclivity for your employees to trust an inbound email from a familiar source, or their tendency to reuse passwords across personal and professional accounts.

Let’s discuss the identity attacks that are most likely to impact your organization.

Attack #1

Broad-based phishing campaigns

Why are phishing campaigns such a popular method of attack? Simply put, the numbers are in the attacker's favor.

A broad-based phishing campaign recognizes that threat agents have to gain access to only a few accounts or one admin account to compromise the organization. Yet with just a light touch of social engineering and a list of email addresses, phishing attacks can successfully compromise 1 out of 20 employees from even a well-trained organization.

Credential theft from phishing is often the first stage of the cyber kill chain. According to the Verizon 2017 Data Breach Investigations Report, 81% of breaches used stolen and/or weak credentials.

Anatomy of the attack:

1. Attacker acquires a list of emails or phone numbers and designs a generic call to action that's relevant for that list (such as a fake Google login page).
2. The phishing message is broadly distributed, and the attacker waits to see which credentials are collected.
3. The attacker uses stolen credentials to access the data they are after or adopts that identity for a more targeted attack on a high-value employee.

Attack #2

Spear phishing campaigns

Spear phishing is a targeted form of phishing that often involves more research designing the target list and phishing message. As opposed to broad-based campaigns, spear phishing typically focuses on a small number of employees to evade automated filters.

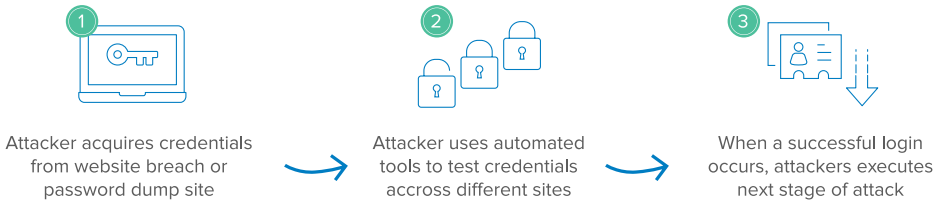
The level of social engineering is also more sophisticated, with messages being more personal and the malicious call-to-action playing on emotions such as curiosity, fear, or rewards.

Anatomy of the attack:

1. Attacker picks targets carefully, doing extensive research across available resources such as social media or web presence.
2. Attacker crafts a phishing message designed to appear legitimate, such as pretending to be a colleague and referencing a topical situation, such as a recent company party that the attacker learned of online.
3. The victim is compelled to enter credentials by appealing to his or her emotions, such as a curiosity to see photos from the party behind a fake login page.
4. The attacker uses the credentials from the high-value target to access sensitive data or execute the next stage of their attack.

Attack #3

Credential stuffing



Credential stuffing is a form of brute force attack that takes advantage of our struggle to select unique passwords across our various accounts. This is hardly surprising when you consider that the average American internet user has 150 online accounts requiring a password. Yet many of us have had account credentials compromised as part of a data breach (have you checked yours recently?).

Attackers leveraging credential stuffing will use these compromised credentials on several other websites to test if the login details are re-used. And they often are: 73% of passwords are duplicates, according to the TeleSign 2016 Consumer Account Security Report.

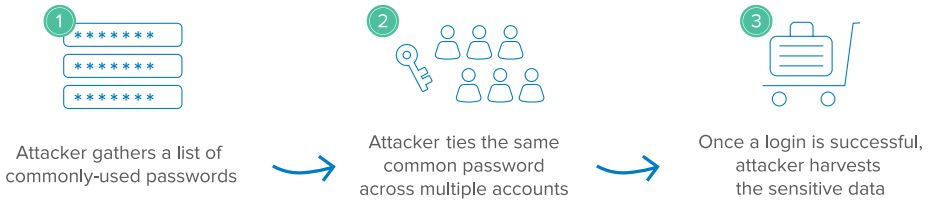
These types of attacks can be done at scale by bots, leading to a higher likelihood of these attacks affecting your organization. According to a recent report from Akamai, "more than 40% of global log-in attempts are malicious thanks to bot-driven credential stuffing attacks".

Anatomy of the attack:

1. Attacker acquires credentials from a website breach or password dump site.
2. Automated tools are used to test credentials across a variety of different sites.
3. When a successful login occurs, attacker harvests the sensitive data or executes the next stage of their breach.

Attack #4

Password spraying



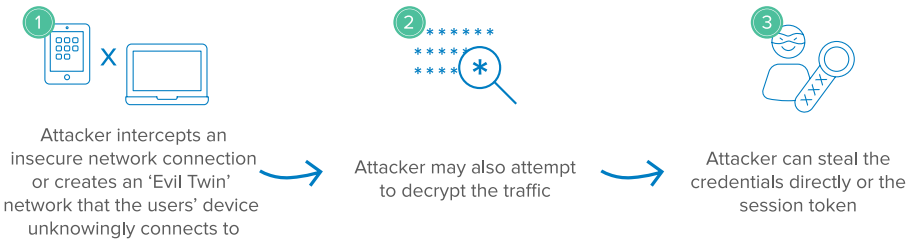
Password spraying is another form of brute force attack whereby an attacker takes advantage of our tendency to rely on common passwords such as "password1" (which according to Pwned Passwords has appeared in a data breach over 2.3 million times!).

Anatomy of the attack:

1. Attacker uses a small list of commonly-used passwords that match the complexity policy of the domain.
2. Instead of trying multiple passwords for one user, the attacker uses the same common password across many different accounts which helps avoid detection.
3. Once the attacker encounters a successful login, the attacker harvests the sensitive data or executes the next stage of their breach.

Attack #5

Man-in-the-Middle (MitM) attacks



A MitM attack on an organization is a highly targeted attack that can result in a full take of credentials and data-in-transit if executed correctly. After intercepting a network connection, an attacker can also take advantage of "session hijacking" that compromises the web session by stealing the session token.

Anatomy of the attack

1. Attacker intercepts a network connection, often by leveraging tools to mimic a legitimate wifi access point (such as Starbucks Wifi).
2. If data is encrypted, attacker may attempt to decrypt data by tricking the user into installing a malicious certificate or other technique.
3. If attack is successful before the initial authentication, the credentials may be stolen as the attacker is monitoring all the user inputs.
4. Alternatively, the attacker steals the session token and is able to authenticate into the account and execute the next stage of their breach.

How Multi-Factor Authentication (MFA) can prevent these identity attacks

As the identity becomes the new security perimeter, organizations that take an identity-driven approach to security are finding that these attacks are able to be prevented without impacting user experience.

While it's certainly important to educate employees of these identity attacks and implement best security practices like data encryption and certificate pinning, implementing MFA across your apps will significantly reduce the risk of successful attacks.

MFA prevents phishing attacks by requiring a second factor to access sensitive corporate data, such as a lightweight push to the user's mobile device for authentication. This means that even if an attacker has your credentials, they still will not be able to be authenticated into the app. MFA therefore also prevents credential stuffing and password spraying since stolen or weak credentials are not sufficient to gain access. If MFA is paired with modern identity solutions, organizations can also set policies against the use of compromised or common passwords that leave employees vulnerable to these attacks.

Minimizing MFA prompts should also be a key consideration, and by implementing modern Adaptive MFA, the second factor challenges are only surfaced under more risky scenarios, such as when the login occurs off the corporate network.

Moreover, organizations can apply especially strict MFA policies for business-critical apps or privileged users, providing an effective layer of defense against spear-phishing attacks.

Finally, MFA can prevent man-in-the-middle attacks by ensuring that if credentials are stolen in transit, a second factor is still required to access the account. Even more sophisticated attacks that attempt to steal a one-time password as part of the attack can be prevented by leveraging more secure authenticators like a U2F security key.

In light of these identity risks, NIST has recommended organizations implement MFA as part of their Digital Identity Guidelines.

Check out our product page to learn more about implementing Adaptive Multi-factor Authentication vwith Okta and how we can help prevent identity attacks on your organization.

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work. www.okta.com