ONE MINUTE WHITEPAPER

The Anatomy of Account Takeover Attacks

Account takeover attacks (ATO) are cheap, easy, and increasingly common. Without proper protection these attacks can be devastating. Learn about system weak points and how to recognize an attack in progress.

Account Takeover Attacks Are a Growing Concern

Account takeover can happen to anyone. Ignoring the problem is no longer an option.

Increase in Account Takeover

44%

Of businesses have experienced targeted email-based attacks[1]

Overall Market Loss to ATO

$7B

Lost in attacks that resulted in a data breach

Average Victim Cost

$290

Lost in data breaches involving credential-stealing malware

Poor credentials and weak identity management are the root cause of account takeover. We took a look at how these attacks are executed and what organizations are doing to prevent them.

Stolen or Weak Passwords

81%

Of breaches leveraged stolen and/or weak passwords

Social Attacks

43%

Of attacks on social media accounts resulted in successful data breaches

Credential-Stealing Software

51%

Of data breaches involved credential-stealing malware

What Do Identity-Driven Account Takeover Attacks Look Like?

Credential Stuffing

73% of passwords are duplicates, according to the TeleSign 2016 Consumer Account Security Report.[2] This allows attackers to gain access to credentials from a source with lower security, and then brute-force access into other more secure systems, leveraging the security risk created by password reuse.

1. Attacker acquires credentials from website breach or password dump site
2. Attacker uses automated tools to test credentials across different sites
3. When a successful login occurs, attacker executes next stage of attack

Password Spraying

50+% of people use the top 25 most common passwords.[3] Attackers exploit this weakness by performing effective brute-force password attacks using a small list of passwords.

1. Attacker gathers a list of commonly-used passwords
2. Attacker tries the same common password across multiple accounts
3. Once a login is successful, attacker harvests sensitive data

Phishing

91% of successful cyber attacks involve phishing[4], a method of obtaining passwords using deceptive messages via channels such as email or SMS.

1. Attacker acquires emails and designs a phishing message
2. Attacker distributes phishing message and waits to see who enters credentials
3. Attacker uses stolen credentials to access sensitive data

Man-in-the-Middle (MitM) Attacks

Attackers intercept data in transit, resulting in credentials being captured and compromised.

1. Attacker intercepts a network connection
2. Attacker may also attempt to decrypt the traffic
3. Attacker can steal the credentials directly or steal the session token

Motivations for Account Takeover

Once an account has been successfully taken over, attackers can engage in a number of malicious activities.

1. Using stored financial instruments or loyalty points
2. Making high value purchases of digital goods
3. Spamming users and creating fake listings
4. Selling stolen credentials on the black market
5. Assuming the identity of the real user

Defending Against Account Takeover Attacks With Okta

Whether it's standard authentication, multi-factor authentication, or adaptive multi-factor authentication, learn how Okta is the best tool to defend against account takeover attacks.

Authentication

Authentication	Authentication & Password Policy	Password & Account Recovery

Okta Authentication enables strong authentication to prevent password misuse and weak passwords. Self-service and secure password reset capability secure all flows.

Adaptive Authentication

User Context	Application	Device
Network	Location	Threat

Okta Adaptive Multi-Factor Authentication (MFA) helps you to create intelligent policies based on login context that limit identity challenges to risky login attempts.

MFA

MFA	MFA Policy	Factor Management

Okta MFA allows you to deploy strong authentication at login or downstream in your application using a range of factors, or leverage pre-built WebAuthn support. Not only do widgets, SDKs, and Restful APIs make adding Adaptive MFA simple, but admin dashboards also make day-to-day management of users a seamless experience.

Learn about how Okta's Adaptive Multi-Factor Authentication can help protect you from account takeover attacks.

Sources

1 https://www.agari.com/email-security-blog/account-takeover-based-email-attacks-increased-by-126-percent/

2 https://www.okta.com/security-blog/2018/03/5-identity-attacks-that-exploit-your-broken-authentication/

3 https://keepersecurity.com/blog/2017/01/13/most-common-passwords-of-2016-research-study/

4 https://cofense.com/enterprise-phishing-susceptibility-report/