WHAT IS ACCOUNT TAKEOVER AND HOW DOES IT HAPPEN

Account takeover is a form of online identity theft in which a cybercriminal illegally gains unauthorized access to an account belonging to someone else. The victim's account will be of value to the hacker because it either holds funds or access to products, services, or other stored value of some kind (such as sellable private information). This can happen in both a personal environment such as your personal email or accounts and it can happen in a work environment.

What is account takeover fraud?

Account takeover fraud is a type of cybercrime or identity theft where a malicious third party gains access to (or "takes over") an online account, such as an e-mail address, bank account, or social media profile.

What types of organizations are targets of ATO attacks?

Fraudulent account access to customer accounts has always been a concern for financial institutions, but today ATO attacks can affect any organization with a customer-facing login. As the 2021 Verizon DBIR notes, the most common threat actor motivation is financial. Cybercriminals usually look for the easiest way to make money, which currently involves the sale of private information, ransomware, or stealing cryptocurrency.

In other scenarios, the criminal's goal is to collect personally identifying information (PII). Private information is very valuable as it can be used to perpetrate identity theft in many ways: applying for lines of credit under the victim's name, committing insurance fraud, or obtaining credit card information are all popular. Personal information can also be used in phishing and spam campaigns to make the fraudulent communications more believable, and help criminals target their victims. These types of attacks often target healthcare, the public sector, and academic institutions.

What are the risks of account takeover?

ATO can be used as the entry-point for much larger attacks than personal, providing an initial foot-in-the-door for an attacker to leverage other vulnerabilities and compromise the entire system or network. This is often done by using the victim's computers for criminal activity or installing malware and ransomware. The consequences of this level of compromise can be immense as we've seen with the recent SolarWinds and Colonial Pipeline hacks, and their effects on the economy, government, and infrastructure.

How does account takeover happen?

The foundation for a successful account takeover is access to a user's account credentials. Here's how attackers usually compromise legitimate accounts:

Brute-force attacks. These include both password spraying (guessing common passwords for a given user) and credential stuffing (guessing full credential pairs). The attacker, usually through an automated

script, tries a username/password combination across many accounts until one works. These include so-called dictionary attacks, in which attackers use common passwords and dictionary terms to guess passwords.

Breach replay attack (also known as credential stuffing). It's a bad practice, but many people 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 (often an email address) and password is at risk.

Phishing. Old-fashioned credential phishing remains a highly effective way to get a victim's password. Without barriers like multi-factor authentication (MFA), stolen credentials lead to compromised accounts.

Malware attacks. Keyloggers, stealers, and other forms of malware can expose user credentials, giving attackers control of victims' accounts.

Attackers can also download cracked passwords from darknet markets to attempt ATO on the same user accounts on their target site.

How is an account takeover attack performed?

There are four steps in the lifecycle of an ATO attack:

*Cybercriminals know users commonly reuse the same password across different services; so obtaining stolen credentials is their first step. Due to data leaks and massive data breaches, billions of compromised credentials are traded and sold on the dark web and the public Internet.

*The next step for the attacker is to test the stolen credentials against the target service. These can be manual or automated attacks with bots using credential stuffing tactics. It is estimated that with these bots, they can access 3 to 8% of the accounts, depending on the target.

*Once the attacker has identified valid credentials for a user account, they can either fraudulently login to extract value for themselves or sell the working login to others.

*Often the data extracted from one account leads to more ATO and other forms of cyberattacks. For example, if an email account can be compromised with an ATO attack, the attacker can use it to reset passwords on other accounts and use tactics to defraud the victim's personal contacts.

Who is impacted by account takeover?

Everyone. For a victim, the impact may be as minimal as being locked out from their Netflix account for a week or two, but the global cost of cybercrime is projected to be USD 6 trillion in 2021. This cost is borne by some individuals more than others if they are victims of identity theft, but this cost in the global economy is felt by all of us in the loss and disruption of services during ransomware attacks to healthcare and infrastructure, and in the cost of digital products like streaming entertainment and social media, as companies must invest more and more to bolster their security postures.

Why is ATO hard to protect against?

Unlike other cyber attacks on an organization, ATO takes advantage of the weaknesses created by customers, which are more difficult to close. The security hurdles that can be imposed to protect employee accounts are can lead to abandonment if they are required of customers. Unfortunately, even when the customer may be to blame for unauthorized access to their account, the organization is still held responsible by customers, the media, and even in court.

How can you secure your business data against corporate account takeovers?

*Because ATO attacks rely heavily on the reuse of credentials exposed in 3rd party data breaches, an effective defense involves detecting logins using previously compromised credentials.

*Employee education is essential. Ensure employees are trained to recognize suspicious emails and phishing attempts Enforce good password habits and abolish re-use.

*Protect your online environment. Follow the principle of least privilege- each account should have only the minimum access required for proper functioning. Segment on-premise networks to prevent the spread of malware and reduce the fallout from network compromise. Keep software up to date. Make sure all systems are secured, especially cloud-based and internet-facing systems. Have employees use VPNs. Implement MFA systems.

*Pay attention to suspicious activity and react quickly. Employ hardware and software monitoring tools to the greatest extent possible. Implement continuous password monitoring for exposed credentials to enforce password hygiene and mitigate threats as they arise. Enzoic offers a solution to screen logins and works well with existing authentication system.

What is the difference between credential stuffing and account takeover?

Credential stuffing is a type of brute-force attack that relies on automated tools to attempt logins with large volumes of stolen usernames and passwords.

Account takeover is the unauthorized access of the account by a threat actor. As a result of successful credential stuffing, ATO can also be performed through phishing, password spraying, or many other vectors.