Cyberlitica
Threat Intelligence Services

Account Takeover Defined

What is account takeover?

Account Takeover (known as ATO) is a type of identity theft where a bad actor gains unauthorized access to an account belonging to someone else.

What types of organization 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. ATO targets regularly include technology, retail, restaurants, online travel, and reward programs where a criminal tries to obtain products and services. In other scenarios, the criminal's goal is to collect personally identifying information (PII) to be used for other forms of fraud and identity theft. These types of attacks often target healthcare, public sector, and even academic institutions.

What is the business impact of ATO?

Losses from ATO and fraud cost businesses across all industries billions of dollars per year. According to Juniper Research, losses from fraudulent online transactions are expected to reach $25.6 billion in 2020. **These types of attacks also lead to the erosion of customer trust and harm to brand reputation**.

How is an Account Takeover attack performed?

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

1. 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 beaches, there are billions of compromised credentials being traded and sold on the dark web and public Internet.

2. 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.
3. 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.
4. Often the data extracted from one account leads to more ATO and other forms of cyber-attacks. 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 phishing tactics to defraud the victim's personal contacts.

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 organizations stop ATO attacks?

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. Cyberlitica offers 24x7x365 monitoring to help prevent ATO attacks from happening. For more info checkout: Cyberlitica.com or email us at info@cyberlitica.com