How Can Cybercriminals Monetize Accounts?

Cybercriminals are always on the lookout for new ways to make money. One of the most common methods they use is account takeover attacks, which involve stealing usernames and passwords to gain access to accounts and then using them to steal money or personal information. This can include scenarios where cybercriminals have stolen personal details, such as credit card information, or even more dangerous scenarios where they have taken over someone else's accounts to commit identity theft.

How Can You Stop Account Takeover Attacks?

Account Takeover (ATO) is an attack in which cybercriminals gain unauthorized access to accounts. There are several ways to prevent ATO attacks, including using behavioral analysis and machine learning to detect anomalies and characteristics that indicate potential ATO activity. Additionally, HUMAN Bot Defender can help prevent ATO attacks by leveraging machine learning and behavioral analysis to detect and block suspicious activity.

What Are Account Takeover Attacks?

Account Takeover (ATO) attacks occur when cybercriminals gain unauthorized access to accounts. ATO attacks can be extremely difficult to detect because they often involve small numbers of login attempts that are scattered across different IP addresses. As a result, ATO attacks can go undetected for long periods of time, allowing cybercriminals to continue their activity without being noticed.

Why ATO Attacks Are So Difficult to Detect

ATO attacks are difficult to detect because they typically involve small numbers of login attempts that are spread across different IP addresses. This makes it very easy for attackers to launch a highly distributed campaign with bots that pretend to be legitimate users. Additionally, ATO attacks can go undetected for long periods of time, allowing cybercriminals to continue their activity without being noticed.

The Business Impact of ATO Attacks

ATO attacks can have a significant impact on businesses, causing financial losses and damage to customer trust. Studies have shown that businesses can lose up to 80% of their e-commerce revenue due to ATO attacks, and that this number can rise to 85% during times of peak bot traffic.

Learn more at www.humansecurity.com