aircall

Account Takeover White Paper

Last Modified: April 18 2023

Introduction

In the digital age, even simple tasks like checking your bank account, scheduling a doctor's appointment, or logging into your favorite website can now lead to an Account Takeover.

Account Takeover (ATO) is a type of online fraud where a person steals someone else's login credentials (like username and password) to gain access to their online account without their permission. Once the attacker has control of the account, they can view personal information, perform unauthorized actions, and cause harm to the account owner.

This white paper aims to provide an analysis of ATO, including the various attack methods used by hackers, the impact of ATOs on businesses, best practices to prevent ATOs, how we prevent and detect account takeovers at Aircall, and provide information on how customers can get help if they suspect their account has been taken over.

Common Tactics Used in Account Takeover

Typical attacks that cybercriminals use in order to take over an account include credential stuffing, password cracking, password spraying, and social engineering. The last one, social engineering, is the most prevalent type of attack on the internet. Social engineering relies on human vulnerabilities, allowing attackers to exploit their trust rather than exploiting information systems.

The most common way that an attacker will mount a social engineering attack is by using phishing. With a phishing email, the victim is lured into revealing their credentials to the attacker. Depending on the type of resource that those credentials were protecting, the victim may consequently give the attacker access to personal information or even financial resources.

Credential stuffing is an attack related to the exploitation of information systems. The attacker uses the victim's credentials previously obtained from a data breach to access other vulnerable information systems. People tend to use the same password across different internet services, which increases the likelihood that a breached password will work on the service where the attacker is trying to take over the victim's account.

Password cracking and password spraying are attacks that exploit humans as well as the design of information systems. Humans tend to use simple passwords that are easy to guess, but the system should be designed to prevent them from using simple passwords. With password-cracking techniques, the attacker tries different combinations of passwords in an automated way. Their success will depend on the simplicity of the password.

Password spraying exploits the probability that, on a big group of users, there will be at least several that are using simple passwords. Therefore, the attacker tries several very simple passwords (such as Password, Password123 or Password123!) in combination with many usernames. Both password spraying and password cracking can be prevented by forcing users to use complex passwords at account creation.

Account Takeover Detection and Protection at Aircall

As account takeover (ATO) attempts become more sophisticated, detecting them is an ongoing challenge that requires Aircall to adapt our security measures frequently.

The two common techniques we use to detect ATO are anomaly detection and behavioral analysis, which we complement with Threat Intelligence. In this section, we will explore these methods in more detail, including their strengths and limitations.

Anomaly detection is a method of detecting unusual activity within a user's account. It involves monitoring a user's behavior and looking for patterns that deviate from the norm. For example, if a user suddenly logs in from a different location or device than usual, this could trigger an alert that their account has been compromised. However, this method can be challenging because it requires a baseline of what is considered "normal" behavior, and it can be difficult to distinguish between legitimate and malicious activity.

Behavioral analysis is a more sophisticated version of anomaly detection that involves monitoring user behavior over time to build a profile of their typical actions. This method looks at a variety of factors, such as the user's location, device, and time of day, to create a baseline for what is considered normal behavior. Any deviation from this baseline can trigger an alert. Behavioral analysis can be more effective than anomaly detection alone.

Threat Intelligence involves monitoring for known threats and patterns of behavior associated with ATO. This can be done by analyzing data from external sources, such as threat intelligence feeds.

Our behavioral and anomaly detection systems monitor user activity for unusual patterns that may indicate a potential attack, whereas IP monitoring allows us to detect various types of brute force attacks, including vertical, horizontal, and diagonal attacks. By analyzing login attempts and tracking IP locations and reputations, we can identify and block malicious login attempts from unknown or suspicious IP addresses.

To fully strengthen our security measures, Aircall also monitors login attempts from countries that are not typically associated with a user's account. This enables us to identify suspicious activity and block any unauthorized access.

In addition, we track the amount of resources (such as minutes or messages) and usage (such as calls or messages to suspicious countries) by each customer.
This consumption tracking allows us to identify unusual spikes in usage, which may indicate a potential security breach.
By detecting anomalies in resource consumption and usage patterns, we can take action to prevent unauthorized access before it becomes a significant problem.

Finally, Aircall uses a Web Application Firewall to analyse incoming web traffic and block any malicious requests or activity. The WAF provides an additional layer of protection against ATO attempts that may exploit vulnerabilities in Aircall's web application.

By implementing these measures, Aircall ensures the security of our customers' accounts and protects against ATO attempts.

Shared Responsibility

While we take steps to secure our systems and provide our customers with tools and resources to protect their accounts, there are also steps that our customers should take to reduce their risk of ATO.

One of the most important steps that customers can take is to use strong unique passwords for their accounts. Passwords that are easy to guess or reuse across multiple accounts can be easily cracked by hackers, giving them access to sensitive information. We encourage our customers to create passwords that are at least 12 characters long and include a mix of upper and lowercase letters, numbers, and special characters.

This article provides further information on how adding just one more character to a password can greatly increase its security. This is important because weak and reused passwords are one of the most common ways that hackers gain access to accounts.

Our roadmap for the year includes prioritizing the implementation of multifactor authentication (MFA) for our customers. MFA will provide with an additional layer of security to our customers accounts by requiring a second form of verification, which will reduce the **possibility of an account takeover by 99%.**

With the recent SAML rollout, our customers can now use their default authentication platforms to manage the Aircall application just like their other productivity tools. This means that they can apply their preferred security measures to ensure secure access to Aircall.

Customers should also be wary of **phishing emails** or text messages that ask for sensitive information or direct them to click on a link. These are phishing emails often designed to look like legitimate requests but are actually attempts to steal login credentials or other personal information.

Using public Wi-Fi should also be avoided, as these networks can be easily hacked, putting your sensitive information at risk. Instead, use a secure network or a personal hotspot when accessing sensitive accounts.

Finally, we want our customers to understand that if their account is compromised due to a weak password or falling victim to a phishing scam, we are not responsible for any resulting damage or loss.

Legal Obligations

An account takeover is not considered a security or data breach for Aircall. As explained before, this is a shared responsibility and will not affect the availability, data integrity or reliability of our application.

As per our terms of use, we are not responsible if the breach is caused by the customer's failure to maintain the confidentiality of their login details. And we can charge the customer the cost of remediation or their login details due to their failure to safeguard Customer's Login Details **(section 3.4 of our terms of use).**

While we take many steps to assist customers in securing their accounts, it is ultimately their responsibility to take measures that prevent ATO.

We believe that by working together for account security, we can help ensure that our customers' personal and sensitive information remains safe and secure.

How to contact us

At Aircall, we take security very seriously and understand that security is a major concern for our customers. If you suspect that your account has been compromised or you are experiencing any security-related issues, we strongly recommend that you contact our support team immediately.

submit a support ticket through our **online portal** and provide us detailed information about your security concern. This allows our team to thoroughly review your issue before responding.