Customer Account Takeover Detection and Response

A technical paper prepared for presentation at SCTE TechExpo24

Stuart Keener
Associate Vice President, Cybersecurity
Cox Communications
stuart.keener@cox.com

Jacob Prosser
Director, Cybersecurity
Cox Communications
jacob.prosser@cox.com

Table of Contents

Title **Page Number**

1. Introduction

Account takeover is a form of identity theft where a threat actor gains unauthorized access to online accounts using stolen credentials. As of 2023, 29% of American adults had experienced a form of account takeover[1].

Account takeover affects business and personal accounts, causing different types of harm and requiring different methods for detection, containment, and response. A business account is issued by a company, for use by employees, contractors, or business partners when conducting businesses activities, such as administering servers or selling products. The business account is terminated when its assignee is no longer associated with the business. Personal accounts are registered by a customer to be used for personal activities such as purchasing or utilizing a company's products or services. Credential reuse, which occurs when the same username and password are used across multiple companies' systems, is common because it does not require the account holder to remember multiple passwords.

This paper focuses on Customer Account Takeover (CATO) where a personal account used by a customer when interacting digitally with a business is taken over by a threat actor. The business can take actions to protect the customer's account by identifying suspicious activity through ingestion of multiple signals, relying on predefined baselines, and user behavior analysis to determine if a customer's account is compromised. Methods to respond to a customer account takeover will also be explored with considerations based on the business' industry.

2. CATO Risk and Impact

CATO has real-world negative impacts that affect the customers and businesses.

2.1. Customers

Once a threat actor has access to a customer's digital account, they can steal personal information, make unauthorized changes, commit fraud, or carry out other malicious activities. They often establish persistence by adding their contact method (e.g. a phone number or email address) for account recovery. They may also change the second authentication factor to lock out the customer and other threat actors that may also hold the compromised login credentials.

CATO impact is not restricted to digital interactions. Often, a threat actor garners sufficient information to extend the attack to customer call centers. If the threat actor is brazen and the end result enticing, the attack can sometimes be extended to in-person retail store interactions as well. For example, threat actors could modify authorized pick-up individuals to pick up high-end televisions from a home theater retail store.

CATO can also affect life and safety aspects of a customer, for example, modifying authorized users for childcare interactions and interacting with home security systems.

2.2. Businesses

Businesses suffer negative consequences of their customers' accounts being taken over. This can occur through losses such as monetary refunds for products fraudulently purchased and shipped, service credit for abuse of a product, and increase in operating expense to remediate the compromise through customer support calls and internal technology actions. Businesses can also experience loss of trust in the customer relationship even if the customer was the cause of the compromised login credentials.

3. CATO Objectives

CATO occurs through initial account access and then modification and abuse of the access.

3.1. Initial Account Access

Initial account access generally occurs when a threat actor acquires login credentials, often through phishing emails, social engineering, malware on customer computer, and data breaches where a customer has reused login credentials.

While multi-factor authentication is a preventative measure, the additional factors can be phished by threat actors using specialized tools or social engineering tactics. For example, a threat actor may call a customer saying that they are a business representative. While on the phone with the customer, the threat actor could leverage a "forgot password" function on a business' website to trigger the sending of a one-time passcode to a customer's phone via SMS. The threat actor would then ask the customer to read back the code to the threat actor for security purposes. If the threat actor can obtain this code, they would then type it into the business' website and complete the password reset, ultimately resulting in CATO.

3.2. Account Modification And Abuse

As previously described, modification and abuse of the customer's digital account is a common objective of threat actors performing CATO. While the types of modifications and abuse are dependent upon the products and digital features implemented by the business, the threat actor is often focused on monetary gain or harm to the customer and/or business through monetary transfers, reputational harm, or disruption. Monetary gain is often accomplished through fraudulent purchases or direct currency transfers. Reputational harm of the customer could occur if private conversations or browsing history is exposed publicly or fabricated communications are sent from a customer's account. This could occur through a disparaging message being sent from a student to other students or professors. Disruption can also occur through modification of services. For example, a threat actor could disconnect a utility to antagonize a foe.

4. CATO Detection And Response

CATO detection and response is the process of identifying and responding to the compromise of a customer's digital account. Response includes containment and remediation.

To detect CATO, businesses can monitor their own systems for suspicious user activity against a normal baseline, often called user behavioral analytics. They can also look outside their own systems by monitoring for customer login credential leaks on the internet.

Remediation is a combination of containment of the threat actor, customer notification, and preventative measures either recommended or enforced.

4.1. Detection

4.1.1. User Behavioral Analytics

Humans are creatures of habit and will generally act in the same manner from one digital session to another. For example, they may generally log in from the same computer or consistently log in during waking hours. Also, certain actions are abnormal, such as password changes occurring multiple times in a day or multiple days in a row. This often indicates a customer and a threat actor battling for control of a digital account.

Through a period of monitoring and analyzing customer digital interactions, a baseline can be created to only alert for CATO when a deviation occurs from the baseline. Alerting based on a single deviation could result in a false positive. To increase the fidelity of a CATO alert, the CATO detection system might calculate a risk score based on the deviations. Once a certain risk threshold is reached, an alert for CATO would be generated. A login from a known threat IP address could be enough to reach a risk threshold, for example, but the risk scores of a password change, entering a new shipping address, and a login from a new IP address summed together could reach the risk threshold of detecting and alerting for CATO. Data lakes and automated searches can be created to support these detections and risk scoring.

More advanced and technical analysis can be done on the customer's digital interactions such as keystroke speed, mouse movements, and touchscreen motions. This type of analysis requires advanced technology solutions but can also detect more sophisticated attacks where malware is being used to source the login directly from the customer's device. That malware technique would avoid detection by less sophisticated detection methods based on IP address.

4.1.2. Leaked Login Credentials

Customers will often reuse their email address and password for login to multiple websites. While a business can't stop another business from being breached and losing stored login credentials, a business can, directly or through a third party, monitor the internet for leaked credentials where the email address or username match a registered customer account. After a business detects a leaked credential of one of their customers, they can perform a targeted validation of the password to determine if the leaked password matches their systems, putting the customer's digital account at risk.

4.2. Response

Response is composed of containment and remediation. Containment means stopping and eradicating the threat actor. Remediation is reversing and remediating the malicious actions of the threat actor.

4.2.1. Containment

Upon alerting for CATO, an investigation should occur to determine if the alert is a false or true positive. If a false positive, consider how to tune the detection thresholds to increase the fidelity. If a true positive, containment steps should be taken to stop and eradicate the threat actor. A common approach is to systematically revoke all session tokens associated to the customer's digital account and perform a login credential reset (e.g., change password, remove recently added contact methods). Depending upon the business, a notation can be made to the customer account, alerting customer support agents of potential threat actor activity when interacting with the customer account via telephone, chat, or in-person.

4.2.2. Remediation

Remediation actions will vary based on the dwell time of the threat actor and functions available to them during the CATO event. Initial access timestamps and eradication timestamps should be recorded to assist in distinguishing between legitimate and malicious account actions as many times the threat actor and the real customer are both using the account in parallel.

The business must decide which malicious changes they will revert and whether the customer will be responsible for taking any remediation actions themself. The root cause of the CATO alert can be used as a deciding factor for which entity will identify and revert changes. While optional, notification to the customer is recommended so they are aware of actions that have been taken by the business and any further remediation actions that they may need to take. Awareness of the situation also allows the customer to be on heightened alert for additional threat actor activity.

5. CATO Prevention

While prevention strategies are outside the scope of this paper, there are multiple strategies businesses can consider requiring before CATO occurs or as a remediation step. Some examples include enforcing multi-factor authentication, only allowing logins from specific locations such as countries where the business operates, and out-of-band confirmation of high-risk transactions.

6. Conclusion

Customer Account Takeover is prevalent and executed by threat actors for reasons that depend on the products and/or services offered by the business where the customer account is registered. Businesses can take steps to detect and respond to attacks on their customers' digital accounts, thereby protecting the customer and the business from monetary, reputational, operational risks and impacts.

Abbreviations

CATO	Customer Account Takeover
IP	Internet Protocol

Bibliography & References

Include an annotated bibliography of key resources providing additional background information on your topic.

1. Security.org https://www.security.org/digital-safety/account-takeover-annual-report/
2. https://abnormalsecurity.com/blog/account-takeover-statistics