TLP: REDACTED FROM GREEN TO WHITE

THE ANATOMY OF ACCOUNT TAKEOVER

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY ISAC

INTRODUCTION

PURPOSE OF PUBLICATION

The purpose of this publication is to inform members of the RH-ISAC community of the evolving account takeover (ATO) threat by presenting a holistic overview and including best practices of detection and response. Our intent is to share member experiences, lessons learned and to support an ongoing Fraud Committee within the RH-ISAC for combating ATO.

THREAT

Account takeover (ATO) attacks are one of the top threats to the RH-ISAC community. ATO is defined as the unauthorized access and control of a legitimate user's account. With such control, an unauthorized user may change account credentials and lock out the legitimate user, or change notification methods and priorities so that they are unable to receive notifications of activity on their account. This may result in additional fraudulent activity for the user, as well as reputational damage, loss of consumer confidence and billions of dollars per year in lost revenue.

ATO is an attractive threat vector for cybercriminals since a typical user has several personal and business accounts. Once an account is compromised, it provides easy access to an existing digital identity or the ability to create a fraudulent one. With multiple accounts across eCommerce, financial and social platforms, threat actors have more opportunity to take over these accounts and expose personal information on criminal markets.

Accounts and related passwords may actually be more valuable to a threat actor than a compromised credit card as they can be used to create new accounts, impersonate real customers and steal goods and services. Despite multiple warnings and publications, an analysis by the Virginia Tech's Department of Computer Science shows (The Next Domino to Fall: Empirical Analysis of User Passwords Across Online Services) that more than half of the internet users continue to use the same passwords on various accounts. Often times, legitimate user accounts and password credentials remain in place longer than credit cards, which are more easily cancelled than accounts created with email addresses. Additionally, detection of this fraudulent activity is difficult and is further complicated by expanding business models and emerging trends that create new ways for threat actors to monetize stolen accounts.

Like so many other types of fraud, ATO is increasingly committed at scale by bots. In fact, according to Akamai's "State of the Internet Security" report, more than 40 percent of online login attempts are attackers trying to invade accounts. Hackers write scripts that test various combinations of stolen usernames plus potential passwords across multiple websites and apps, until they find a way in. This is called credential stuffing. These brute-force attacks are helping fraudsters move as quickly as possible and focus on maximizing the value of each successful ATO.

IMPACT ON A LARGE SCALE

Large data breaches provide threat actors with the information necessary to conduct reconnaissance and attacks on a massive scale, resulting in a rise of ATO attacks. According to the Identity Theft Resource Center, there have been 1,244 breaches identified in 2018, which have exposed more than 446 million records. In a 2018 identity fraud trends report from Javalin Strategy, ATO has tripled in the past year, reaching a four-year high and resulting in losses of $5.1 billion. Data breaches exposed 1.68 billion non-sensitive records in addition to nearly 446.5 million sensitive records exposed. In an article on Information Security Timelines and Statistics, researchers report that 17 percent of all attacks were attributed to ATO, or account hijacking. Case in point is the massive "collection" data breaches considered to be the largest data dumps in history with 773 million email addresses and 22 million passwords released with Collection #1 and three times as many unique records (2.2 billion usernames and passwords) with Collection #2-5. This unprecedented volume of leaked credentials is currently and will likely continue to fuel credential checking and ATO attacks. The availability of this data on torrent sites for free download is lowering the barriers to entry for even the most unskilled hackers to partake in this criminal enterprise.

Retail & Hospitality

Since January 2018, at least 17 retail and hospitality companies were compromised and likely had account information stolen from them. The 2018 Credential Spill Report from cybersecurity firm Shape Security showed that 91 percent of the login attempts made on online retailers' websites were hackers using stolen data. This startling statistic speaks to the unique challenges that retail and hospitality organizations face with balancing the need to secure their websites while maintaining minimal friction for customers who wish to shop online.

Here are the top 10 biggest data breaches of 2018:

10. Panera, 37 million records breached, disclosed April 2018
9. Newegg, 50 million records breached, disclosed September 2018
8. ElasticSearch, 82 million records breached, disclosed November 2018
7. Facebook, 87 million records breached, disclosed September 2018
6. MyHeritage, 92 million records breached, disclosed June 2018
5. Quora, 100 million records breached, disclosed December 2018
4. Under Armour/MyFitnessPal, 150 million records breached, February 2018
3. Exactis, 340 million records breached, disclosed June 2018
2. Starwood-Marriott, 500 million records breached, disclosed September 2018
1. Aadhaar, 1.1 billion records breached, disclosed January 2018

Threat actors exploit exposed records from breaches in the deep and dark web (DDW). Underground forums provide marketplaces where threat actors can maintain lucrative businesses by selling customer account login information in bulk, account-checking tools and frameworks, configuration files and proxy services. Several inexpensive and easy-to-use account checking kits are also in circulation. These methods and means allow even the most unsophisticated of threat actors to enter into the profitable business of conducting ATO attacks.

Table 3: Cost of Credential Stuffing in Retail

TOTAL COST OF CREDENTIAL STUFFING PER DAY	**$16,450,000**	**A3*B*C**
TOTAL COST PER MONTH	$493,500,000	
TOTAL COST PER YEAR	$6,004,250,000	
A1) Total number of attacks per day across US Industry	131,455,382	The average number of malicious login attempts per day
A2) Average Credential Stuffing Success Rate	0.50%	The proportion of credential stuffing attacks that result in a successful login, i.e., the attacker used credentials that were valid on the target site.
A3) Average # of ATOs (Account Takeovers) Per Day	657,277	**A1*A2**
B) Average Cost of Fraudulently Purchased Merchandise	$50	There are a number of ways for fraudsters to monetize a retail ATO. For this analysis, we assumed that the fraudster used stored value in the account to fraudulently purchase merchandise.
C) Percentage of Fraud Success	50%	The estimated proportion of fraudulent purchases that are not detected by internal fraud resources. Third party research finds that typical fraud success rates range between 20% to 67%

Screenshot of 'Cost of Credential Stuffing in Retail' from Shape Security's 2018 Credential Spill Report

The hospitality industry experiences a similar cost of ATO attacks, with cybercriminals targeting emerging technology for loyalty and rewards program members. In the competitive marketplace of hospitality, the potential impact to brand loyalty is a major threat. According to the Credential Spill Report, an estimated 82 percent of login requests for hotels and hospitality online markets are attributed to credential stuffing. To better fit the needs of the customer, hotels have incorporated the use of mobile applications to streamline user experience during booking, check-in and even as a substitute for room keys. But this has significantly increased the attack potential for hospitality.

Tactics, Techniques & Procedures (TTPs)

The success of an ATO attack depends on the successful targeting of real user accounts and the unauthorized access to valuable information like financial data. To obtain legitimate user credentials, adversaries may use a myriad of tactics and attack vectors including:

- **Phishing:** targeted cyber attack sent via email attempting to lure account owner to reveal personally identifiable information (PII)
- **Social Engineering:** methodology for misleading individuals to reveal sensitive/confidential information via phone, email or in-store
- **Credential Stuffing:** using a list of stolen credentials to gain unauthorized access to user accounts
- **Brute-forcing:** submitting and systematically checking many potential passwords in an attempt to crack password codes
- **Session Hijacking:** accessing unauthorized access to a valid user session in an attempt to exploit information
- **Exploiting Vulnerabilities:** finding specific web application flaws to gain access to customer database

THREAT ACTORS: PROFILES, METHODS & MONETIZATION

ATO Threat Actors

ATO is a highly persistent threat with attacks varying in sophistication depending on the adversary conducting the attacks. In general, however, ATO threat actors can be placed into two categories: casual, opportunistic threat actors and sophisticated threat actors.

Casual, Opportunistic Or Low-Skilled Actors

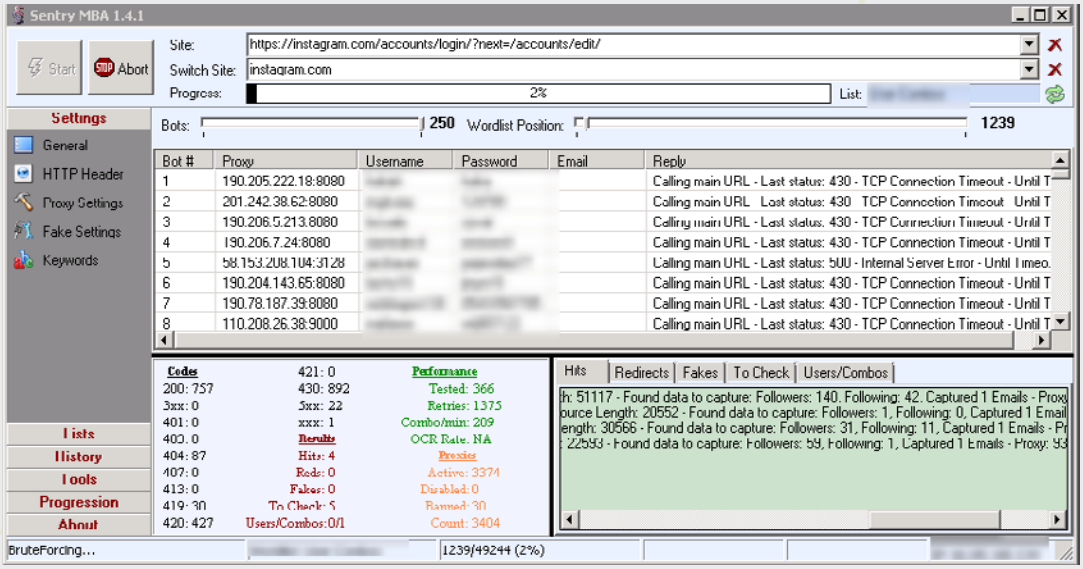
The threat actors that fall into the "casual" bucket are generally low-skilled, with activity that is often noisy and easily detected. They have little technical skill and typically use off-the-shelf tools or techniques developed by other more sophisticated cybercriminals. Consequently, these actors are generally unable to respond to mitigation and real-time blocks, and typically move on to other targets or are unaware of their lack of success. Much of the discussions in underground cybercriminal forums involving ATO is conducted by these casual actors, often openly discussing their activity and attempting to monetize stolen access.

Methods

One method often used by opportunistic actors is "brute-force" attacks. These attacks are a trial-and-error method of matching usernames to passwords, and are often conducted using one of two techniques: using multiple passwords tested against a single account in rapid succession or by checking different username and password combinations against multiple accounts. Brute-force tools can be configured on the fly, or can use a configuration file, often referred to as a "config," which manages the settings for the tool, determines which target will be attacked, the conditions for success and failure, and how the attack will be conducted. The config file allows the attacker to incorporate proxy IP addresses to carry out the attacks, and allows for cybercriminals to adjust the timing of each attack to further disguise the traffic to appear legitimate.

SentryMBA

An extremely common tool used by casual actors to conduct brute-force attacks is SentryMBA. It is a brute-forcing and account-checking tool that can defeat CAPTCHA. It is highly customizable with many readily available configuration packages for numerous targets that allow unsophisticated actors to conduct one-click attacks. Most SentryMBA users are unable to develop the packages themselves and rely on a far smaller number of configuration developers. When a successful configuration or tool for a particular target is released broadly, an attack can increase in scale extremely quickly — up to tens of millions of attempts within hours.

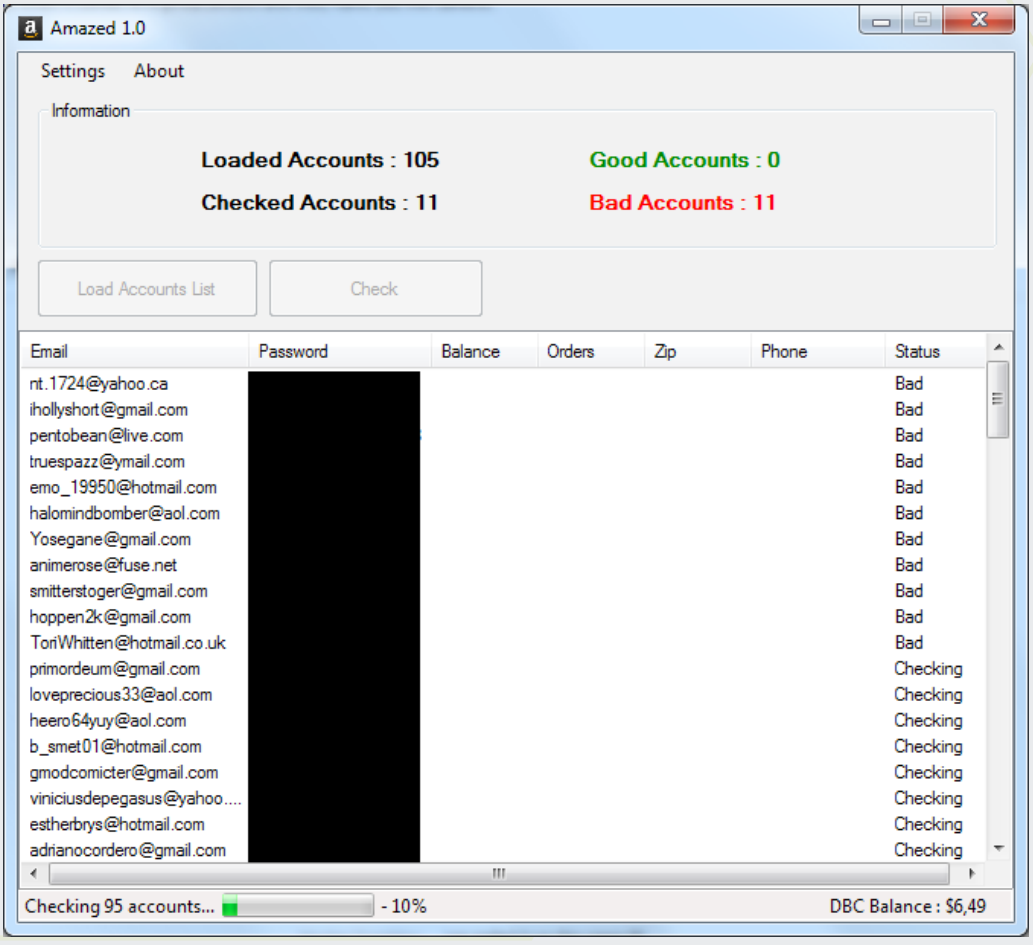


Screenshot of SentryMBA attack in progress. Source: http://imgur.com/cJ2vqeV

Automated tools allow cybercriminals to rapidly conduct thousands of attacks, and can increase effectiveness by incorporating proxies to avoid simple IP blocking technologies. Most security policies limit failed login attempts for a single user before locking the account, though the use of username and password combo lists usually only tries to log each user once, making account lockout and notification of fraudulent activity to the victim unlikely. Network monitoring, such as Splunk and ArcSight, can often detect this activity, which would normally appear as a surge of failed login attempts. When valid username and password combinations are used, these services are not likely to trigger suspicious activity because they will appear to be a regular user login. Successful logins resulting from an attack are then virtually indistinguishable from normal user login activity, making it difficult to detect and defend against.

Casual cybercriminals also use more simplified versions of brute-forcing tools commonly referred to as "account checkers" that provide ATO capabilities. Account checkers can be stand-alone or web-based, and also leverage lists of usernames and passwords. Unlike the more robust programs, account checkers verify if accounts are valid at a specific site or service, such as any retailer with an eCommerce presence. Cybercriminals can obtain and use account checkers in much the same way as other brute-forcing tools, but some authors have incorporated subscription and pay-per-use models that allow criminals to use the account checker as a service rather than as a stand-alone product. This provides the cybercriminal user with a continuously updated product while providing the author with a continuous source of revenue.

While the total number of ATO actors is unknown, the vast majority are in the casual or opportunistic category. Based on the targets chosen and discussion topics (video streaming, gaming and pornographic sites), it is likely that most casual ATO actors are teenagers and young men.



Screenshot of Amazed 1.0 attack in progress. Source: http://imgur.com/0c5Kboe

Sophisticated ATO Actors

ATO actors that are more persistent and able to circumvent mitigation and prevention methods fall into the "sophisticated" ATO actor bucket, and generally possess significantly higher skills. These actors often develop custom tools and scripts, and their activity is much harder to detect, as they often will rate limit their activity (low and slow) to evade detection. Sophisticated actors are far more persistent and continuously modify their attacks in response to blocks and other mitigation techniques, sometimes within hours. Some advanced actors may participate in forum discussions to sell or respond to commissions for custom-developed tools, but the most sophisticated actors monetize privately and do not participate in the forum discussions or sell their tools.

Methods

Sophisticated ATO actors use configs they specially develop for specific targets, and have conducted reconnaissance to fully understand their targets, uncover what controls may be in place on the website, and prepare to combat mitigation controls put in place. Albeit crafty and more sophisticated in nature, most of these attacks can easily be mitigated once their TTPs are identified. Their persistence is what makes them a tougher adversary.

The most sophisticated ATO actors attempt to simulate legitimate customer traffic using custom configurations of browser emulation technology and sometimes entire virtual machines, which can respond effectively to a variety of device profiling mitigation techniques. This infrastructure requires substantially more technical skills to set up and operate compared to a casual actor running SentryMBA.

Sophisticated ATO actors also are extremely good at hijacking legitimate accounts for use in fraud or further ATO activity. For a variety of reasons, account and session hijacking may be the most difficult type of ATO attack to prevent unless the website or application employs SSL throughout the process of browsing a site, not just for the login page. Whether through man-in-the-middle attacks or as the result of a direct compromise of a user's system, account hijacking allows a cybercriminal to harvest login credentials from the victim while remaining virtually invisible to the targeted website. Malware installed on the victim's system allows the cybercriminal to capture keystrokes to steal the victim's username and password, or capture session credentials and cookies that allow the cybercriminal to maintain the session after the victim closes their web browser. Hijacking an account allows the cybercriminal the ability to imitate a legitimate user without displaying the same signatures that would give away brute-force SQLi attacks.

Sophisticated ATO actors are a small fraction of the overall ATO actor population. Given the technical skill, persistence and patience, it is likely that the most sophisticated ATO actors are professional cybercriminals who have attacks running against multiple targets simultaneously and a consistent ability to monetize the acquired access.

Monetization

In the cybercriminal ecosystem, DDW forums and marketplaces represent the primary means by which products and services are bought and sold— including malware, access to compromised systems, login credentials, stolen credit cards and gift cards, PII, ATO tools, and refund services, among many others. The reasons for these transactions are as varied as the products and services themselves, but the endgame is the same – turn something stolen or acquired into money. The execution of these schemes, however, can be more problematic. Cybercriminals may have to transpose digital data onto physical cards, detect and defeat eCommerce fraud detection processes, or move purchased products between a retailer and the product's final buyer. Most cybercriminals do not have the resources to perform all of these steps without using services provided by other cybercriminals within the ecosystem. Such products and services on the DDW are evolving, as cybercriminals adapt to counter increasingly hardened targeted environments.

Monetization from ATO can occur at multiple phases, including, but not limited to: the sale of credential dumps, the sale of tools and services used to conduct ATO, the sale of target-specific configs used in brute-forcing tools such as Sentry MBA, the overall access to compromised accounts, the sale of credit cards or gift cards stolen from compromised accounts, and the sale of goods purchased from stored payment tender in compromised accounts.

Credit card fraud represents a pillar of the underground economy. The majority of DDW markets

are crowded by sellers that offer products and services to facilitate, streamline and industrialize this criminal practice. There is no end to how cybercriminals can monetize stolen or compromised credit cards – from selling the cards/numbers themselves, laundering money, paying bills, or the endless ways to spend the cards on fraudulent purchases – credit card fraud/sales is extremely lucrative for the successful cybercriminals involved.

The DDW has no shortage of forums that are full of dump shops, advertising a current stock of stolen credit cards or gift cards. Compromised payment data has become so prevalent on the dark web, that it has made it difficult to track, as many cybercriminals offering dumps are actually selling old or reused credit cards from other large dumps. Additionally, the ecosystem is a competitive consumer-facing marketplace where shops must cater to their customers by rotating their stock frequently to stay in business.

Cybercriminals monetize information stolen or discovered from ATO attacks either through conducting subsequent fraudulent activity themselves with the stolen information or by selling compromised accounts or payment data to other cybercriminals. ATO fraud includes using stolen accounts to purchase goods and services, including merchandise, technology services and gift cards. Gift cards are a common resource for cybercriminals due to their versatility: they can be used to purchase goods directly, sold to unsuspecting consumers or sold on legitimate gift card purchasing websites. Cybercriminals also use compromised accounts to purchase access to web servers and networks to expand their botnets, increasing their capabilities while minimizing the amount of personal funds they must invest.

In some cases, cybercriminals will obtain the tools and data to perform an attack and exploit the compromised accounts. In other cases, a cybercriminal will obtain combo lists from one dump and conduct the ATO attack to validate username and password combinations from that list against a particular website. Credentials determined to be valid are then resold on the market as “validated” combo lists for specific sites, serving as middlemen for other cybercriminals who then exploit the compromised accounts. Breaking up the processes between tool development, data extraction, data validation and final exploitation, cybercriminals are able to limit their involvement in the overall cybercriminal ecosystem, making it more difficult for law enforcement to identify and neutralize them. Additionally, the cybercriminal underground is so robust that relatively low-skilled cybercriminals are able to participate in the ecosystem. Low and even unskilled cybercriminals can buy the tools and information needed to conduct ATO attacks, or they can simply hire someone else to do it for them, as many of the same products sold in the cybercriminal underground are also sold as-a-service. While on the surface this may not seem much different from simply purchasing validated accounts, the as-a-service offerings allow for targeted exploitation rather than simply selecting accounts that are available. For example, a cybercriminal may hire “professional” cybercriminals to provide valid accounts for a major retailer, who would then perform the attack on the buyer’s behalf. Leveraging as-a-service offerings gives even unskilled cybercriminals the opportunity to attack high profile and hardened targets.

Cybercriminals monetize information from ATO attacks in a variety of ways:

- Subsequently conducting further fraudulent activity by:
    - Ordering goods or merchandise online or in-store with compromised customer account information to later resell or return in exchange for cash or gift cards
    - Purchasing gift cards to be delivered electronically
- Stealing gift cards and other payment data stored in an account to sell to other cybercriminals
- Acting as a reseller, selling compromised accounts or duplicate payment cards to other cybercriminals
- Redeeming customer rewards points for goods or services

From large-scale organized criminal operations operating out of Eastern Europe to local crime rings, resale of stolen or fraudulently purchased goods is a prime factor in the persistent targeting of retail and eCommerce customer accounts. Cybercriminals need

the ability and funds to acquire desirable goods, and pass to an intermediary, to reship products or pass to an aggregated reshipping service – often to less regulated overseas locations.

Reshipping operations are often highly organized criminal operations, resulting in billions lost collectively each year. Calculations estimate reshipping services abusing approximately $1.8 billion per year. Even lower level, localized reshipping activity using stolen credit cards and mules to deliver merchandise impacts retail organizations globally. The trend is only increasing, and will likely continue to grow based on high levels of recently observed activity.

Oversaturation of the market with stolen payment cards and account credentials, enhanced payment security measures, and increased fraud within cybercriminal offerings, reflect the declining value of most stolen payment data. While cybercriminal supply and demand and preferences change, many bad actors are turning their focus to more valuable targets, such as easily monetizable gift cards and stolen PII for the use of full identity theft.

Although this stolen payment card data remains a significant financial resource for cybercriminals, implementing point-to-point encryption (P2PE), EMV chip-enabled payment cards and other ATO mitigation tools used to more rapidly identify fraud are making it more difficult for cybercriminals to steal and use payment card data. As a result, retail and hospitality organizations with an online presence are seeing an increase in ATO attacks and card not present (CNP) fraud as cybercriminals turn to other activities to make up for lost financial resources. This was made evident when organizations in both Europe and Canada faced significant spikes in CNP fraud after implementing EMV technology.

BEST PRACTICES FOR ATO PREVENTION AND DETECTION

Threat actor ATO attacks differ based on their target's organizational infrastructure and end-points, and campaigns and characteristics shift as retail and hospitality organizations increase their monitoring, detection and prevention capabilities. No two attacks are the same, so organizations must thoughtfully select and deploy available and tested tools and techniques to increase their defenses against commonly seen ATO attempts.

PREVENTION METHODS

- Strong password
- Account validation at creation
- Limitation on error message information disclosure
- IP Blocking
- Limit exposure of sensitive information even after successful login
- Require more stringent re-authentication before allowing major account changes (address or email change)
- Behavioral account monitoring
- Require CVV2 at checkout
- Checkout page isolation

Account Creation

Once the account has been created, it should validated with an authorization code that is emailed to the new user upon creation. That new user will need to then validate their account by clicking on a unique URL generated within the email. This limits fraudulently created accounts; however, if the email account is compromised, this step will be ineffective. Companies can also alert on new account creation by emailing the user when a new account is created with an email address to ensure it is a legitimate account. Users should also be required to set up multifactor authentication using one-time codes sent to a customer's email, SMS or third-party multifactor authentication platform. The link or code provided should have a reasonable expiration time, between 30 minutes to an hour.

Password Policy

When a new account is created, organizations should require strong passwords. A strong password is 8-12 alpha-numeric and special characters at minimum. Increasing the complexity of password requirements

forces users to differenciate from previously used passwords, lowering the potential of password duplicates on other accounts held by that user. Retail and hospitality organizations can also prevent password reuse by recording password history and implementing a hard password usage dates, prompting password resets after a given amount of time has passed. Policies may also incorporate tools like Microsoft's Advance Threat Protection services or automated password checking against password checker services like 'Have I Been Pwned'.

Account Login

When a user attempts to login, limit any validated verbiage by not displaying 'incorrect password' or 'email is not associated with an account' when an incorrect username or password has been entered. This indicator alerts attackers that either the account or email is valid. You can also limit account session logins and force logout of old sessions if a new session is established. A lock-out policy can reduce attempted logins by an illegitimate user, and, when implemented, the customer should be emailed to alert that login attempts are being made.

Temporary blocking IP addresses that login to multiple accounts simultaneously or accounts that are accessed from multiple IP address geolocations will limit fraudulent activity. Another method is to employ token-based access to mobile application gateways that encrypts and tokenizes communication. Last, employ password integrity by integrating a service to check if a password has previously appeared in a breach. From there, organizations may restrict positive matches or advise customers that passwords may be insecure.

NOTE

One way to identify IP addresses or other indicators for ATO is to ingest from the RH-ISAC Vetted Enclave. This repository includes IOCs that have been shared by our members and vetted accordingly. The vetting process includes tagging for each indicator and a tag of ATO is added as well.

Account Monitoring

Once users have successfully logged into an account, there are several steps you can take to limit potential exposure of sensitive information. Examples include: mask full payment card numbers (gift card, credit card, loyalty card) so that full account numbers are not displayed, require re-entering of full credit card numbers and passwords when a new shipping address is used, or define acceptable user behavior by auditing normal login activity based on rate limit or standardized policy for acceptable behavior then restricting access for accounts above a defined threshold.

Account activity analysis helps organizations to define normal customer activity around security controls that are currently in place and alert on traffic that defers from a standard workflow including:

- Deny certain user actions if customer profile cannot be validated through known fingerprint (IP address, session ID, browser information, user-agent strings).
- Consider blocking account access if user browser blocks profiling attempts.
- Deny direct API access if you expect customer traffic to go through content delivery networks (CDNs).
- Create custom web application firewall signatures around known suspicious or malicious activity and block all TOR traffic.
- Implement rate limiting via web application firewalls.

Checkout Page

When a user is on the checkout page, there are several steps you can take to limit fraudulent activity: automated confirmation of orders with a validation email, requiring full password reentry at checkout for high-dollar orders, requiring verification of CVV2 for credit card purchases and not allowing null or wrong entries to be approved. To thwart money laundering attempts, deny purchase of gift cards with other gift cards and limit unverified customer actions by removing a 'guest checkout' option. Another defense strategy is to ensure checkout page is placed in a separate container to limit the potential avenues for exploiting a network or code-based weakness.

Detection

Threat intelligence teams should be constantly monitoring the internet and darknet for signs of branded gift cards, loyalty programs or customer information for sale. These teams can find ways into forums on the DDW and participate anonymously to obtain insights on data comprised to their brand. Often times, the information posted in these forums can assist threat intel teams in determining the root-cause of an attack, impact in terms of potential compromise, and in some cases even identify what customer accounts were compromised without having to buy anything from a threat actor. This information can help customer fraud teams who would follow internal processes to remediate the risk for the customer.

Some detection methods for retail and hospitality organizations include utilization of standard scripts to monitor abnormalities. Employ rate-limiting access to APIs depending upon expected traffic. In general, APIs should never allow traffic above 1.5 to 2x the expected amount of traffic. Depending upon determined threshold value, the average amount of typical customer traffic can be calculated to a specific API or website feature on a 30-to-90 day dataset.

Organizations can identify business logic flaws using penetration testing activities such as:

- Detecting sensitive APIs while bypassing authentication
- Finding encrypted information within a packet due to a logic error or poor header hygiene
- Exposing logic flaws that allow security control bypass
- Highlighting possible abuse of sensitive APIs

Sophisticated retail and hospitality cybersecurity teams may also employ behavioral analytics. Teams with dedicated data analysts can produce insights into the actions of customers' behaviors like logging in, checking card balance or status, moving products to shopping card, purchasing or changing account information. While this information is used by eCommerce teams to identify opportunities to optimize sales, it can also provide insight to abnormal customer behavior indicative of a sophisticated, low and slow ATO attack. By collecting specific key data on actions from customers, teams can develop trends and baseline normal behavior, and implement alerts or notifications to tactical teams when behavior deviates from these trends. For teams who do not have these dedicated resources or skillsets, they can leverage tools such as ThreatMetrix.

In addition, cybersecurity teams should implement security audits of digital teams and code verification cycles. Collaboration between digital, network and security teams helps to ensure business changes do not affect security controls downstream. Direct communication between these teams is critical once intelligence regarding successful ATO attacks is uncovered. This allows the customer fraud teams take action in a number of ways, including disabling the account; flagging the account for further monitoring; contacting customers via phone to notify of a potential breach; supplying data to analytics teams to understand the scope of fraud; and identifying where the accounts are being used at physical stores.

Incident Response And Remediation

Security incident response and remediation for ATO should align with a company's overall security process. Several standards for security incident response are:

- NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide)
- ISO/IEC 27035 (Information technology — Security techniques — Information security)

Each standard is focused on managing and reducing business risk. This section will utilize NIST SP 600-61 Revision 2 as a framework for a response and will be organized as follows:

1. Preparation
2. Detection & Analysis
3. Containment/Eradication & Recovery
4. Post-Incident Activity

Other standards are organized similarly. Minor modifications to align with other standards may be needed.

Preparation

As with technical controls, response process preparation is a key to reducing business risk. Preparation includes:

- Identifying and prioritizing areas for response
- Aligning with cybersecurity policy and regulations
- Defining roles and responsibilities

Identifying And Prioritizing Areas For Response

As previously stated, ATO is unauthorized access and control of a legitimate user's account. Each company may protect multiple types of accounts as well as the multiple methods that accounts may be accessed. Mapping these out is the first step to protection. Each type of account may have different levels of business risk. This may include:

- **Regulatory** – Such as payment card data and personal identifiable information handling
- **Fraudulent activity** – Products and services as well as potential theft or fraud against a customer
- **Reputational damage** – Such as impacts to brand perception
- **Loss of consumer confidence** – Perception of poor security may reduce consumer loyalty
- **Lost revenue** – Earnings before interest, tax, depreciation and amortization (EBITDA) may be directly impacted by other areas of business risk

Incident response processes should be aligned directly with the business risk. Response for accounts taken over with higher risk may require increased process and timeliness. Some activities, such as failed login attempts, are identified as only security events with no quantifiable business risk and have minimal or no response processes.

Aligning With Cybersecurity Policy and Regulations

ATO response processes must also align with company policy and external regulation and requirements. This reduces overall business risk of authorized access by ensuring consistency and proper execution of policy, regulation and requirements.

Defining Roles And Responsibilities

Response activities may include multiple departments within an organization. This includes compliance, legal, fraud and other applicable departments.

Each type of account should have identified which departments are responsible, accountable, consulted or informed on unauthorized activity. In addition, similar identification should be determined for external communication (both regulatory and direct consumer notification).

Detection and Analysis

Technical controls should be implemented to prevent unauthorized access. This reduces the urgency of prompt detection and analysis. Otherwise, the access may be identified as suspicious and requires analysis to confirm unauthorized access. Depending on a company's organization and sensitivity of account accessed, the team notified and investigating unauthorized access may vary. This could include the security operations center (SOC), incident response team, or even fraud/risk management. In some instances, the analysis and response may be automated, removing the need for human analysis.

Detection and notification can be implemented through multiple methods for monitoring various abnormal patterns, such as:

- Multiple accounts accessed from a single source
- Abnormal account behavior (such as through machine learning or other automated analysis)
- Successful access from a suspicious device or source (using previously collected observations and intelligence such as those for botnet activity)

Containment/Eradication and Recovery

Containment is gained by removing access to the account. This can be achieved by locking the account or implementing additional access prevention methods (including multifactor authentication, such as security questions or other methods of multifactor authentication).

Eradication and recovery are achieved by ensuring additional unauthorized access is prevented. This often occurs through the completion of the password reset process to change the credentials on the account.

Repeated unauthorized access to an individual account may be the result of a compromise on the account owner's device. Additional remediation on the compromised device may be needed to recover completely.

Any fraudulent activity or access of sensitive account information may require additional response and/or notification (depending on company policy and external regulations and requirements).

Post-Incident Activity

Retail and hospitality cybersecurity teams should conduct regular reviews of ATO remediation. This should consist of the following:

- Trends or other patterns
- Accounts of higher value to criminals (such as VIP)
- Efficacy of current processes

The goal of regular review is to develop new methods for prevention, efficiency in response and overall business risk reduction.

Teams may also consider writing reports. These reports provide an excutive overview of what happened, what was impacted, and what needs to be done so that a vulnerability or attack doesn't occur again. Recommendations should be defined, tracked and provided to teams for remediation. If an attack happens again, teams can resort back to the lessons-learned report to verify what recommendations were not applied.

RETAIL & HOSPITALITY ISAC

REDACTED MATERIAL

RECAP

ATO is an increasingly costly threat for retailers in the U.S. and worldwide. As education and awareness increases for cyber teams, customers and legitimate account owners, so does the capability and sophistication of cybercriminals. Key recommendations from the RH-ISAC include:

1. **Develop a plan and process:** Work across departments to audit each potential end-point for an attack and develop a tracking system based off of behaviors and technological indicators at each spot on the kill chain. Once you understand your vulnerabilities and which data is important, you can implement analytical tools for ATO, setup scripts to monitor common brute-forcing or account checking tools, and begin to establish a framework for how your organization tracks actors. Make incident responses plans proactively, and if and when an attack occurs, write up a lessons-learned report that can be referenced during future incidents.
2. **Adapt and adjust your methodology:** Protecting against ATO attacks is inherently reactive, so cyber intel and fraud teams must continually iterate and restructure tools and methods to increase barriers of protection and limit or eliminate monetization opportunities to deter reoccurring attacks. Focus on ways to disrupt attacker progress by looking at TTPs, mitigating low-level activities and observing exploit techniques. Act quickly to stop persistent attackers from pivoting, monitor your logs and remain vigilant.
3. **Utilize your network:** No two ATO attacks are the same, but sharing and collecting intelligence from retail and hospitality peers, law enforcement and organizations like the RH-ISAC can help increase organizational understanding, ownership and preparedness. Know your local FBI and DHS affiliates and establish a process for outreach. Ask questions to your peers in trust groups and circles and educate your cross-departmental teams on available resources.
4. **Ingest IOCs for ATO from the RH-ISAC vetted enclave:** Member-shared intelligence includes various indicators and tags that exist to identify those related to ATO. Ingestion into protection systems can be accomplished via API, TAXII, or direct CSV download. These indicators may also be ingested by MSSPs who manage protection systems for member organizations. Please contact the RH-ISAC Intel Team for further support.
5. **Join the RH-ISAC Fraud Committee:** Established in 2017, this is a member-led and member-driven group organized to focus efforts to demonstrably mitigate losses and the effect of fraud on customers by defining and targeting specific issues within the cyber-fraud space. Through the Fraud Committee, retail cybersecurity practitioners harness the insight of individual member contributors to produce outcomes that benefit the entire community by zeroing in on trending pain-points for the membership such as ATO.

For more information on the RH-ISAC, the Fraud Committee or how to get involved, reach out to membership@rhisac.org.