TLP: WHITE

6 Quick Wins for Detection and Protection to Fight ATO

Account Take Over (ATO) attacks remain one of the most persistent threats to the R-CISC community. ATO continues to be highly successful as a result of large data breaches that provide information threat actors need to conduct reconnaissance and ATO attacks on a massive scale. Successful data breaches are flooding the market with compromised username/password combinations, which threat actors continually use to test (and compromise) additional accounts across the retail industry. Analysis from cybersecurity firm Shape Security indicated that 90% of the login attempts made at online retailers' websites were hackers using stolen data.

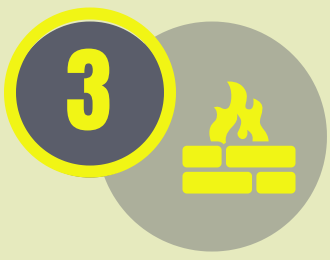
As part of the R-CISC's 2018 Holiday Guidance effort, the Fraud Working Group has outlined six quick wins for detection and prevention of ATO.

Security for Account Creation

- Validate new account creation with an authorization code emailed to user after a new account is created (limits fraudulently created accounts, however, if email account is compromised, this step will be ineffective.)
- Alert on new account creation by emailing user when a new account is created with an email address
- Require strong passwords (8-12 alpha-numerics and special characters, minimum)

Security for Account log-in page

- Limit validating verbiage by not displaying "incorrect password" or "email is not associated with an account" when incorrect UN/PW combo entered (may alert attackers of a valid account/email)
- Limit account session log-ins (force log-out of old session if new session is established)
- Inside Account or Wallet
  - Mask full payment card numbers (gift card, credit card, loyalty card) and account numbers
  - Temporarily block IP addresses that log in to multiple accounts simultaneously
  - Flag/review accounts accessed from multiple IP address geolocation within minutes of each other
  - For mobile applications, employ token-based access with a mobile application gateway to encrypt and tokenize communication
  - Employ password integrity by integrating a service to check if a password has previously appeared in a breach. Restrict positive matches or advise user that password may be insecure



Security for Account Activity

- Require reentering of full credit card numbers and passwords when a new shipping address is used
- Define acceptable user behavior by auditing normal login behavior activity based upon rate limit/policy for acceptable behavior, then restrict access for accounts above a defined threshold
- Analyze and define normal customer activity around security controls in place, and alert on traffic that defers from this workflow:
  - Deny certain user actions if customer profile cannot be validated through known fingerprint (i.e., IP address, session ID, browser information, user-agent)
  - Deny direct API access if you expect customer traffic to go through Content Delivery Networks (CDN)
  - Create custom web application firewall signatures around known suspicious/malicious activity and block all TOR traffic
  - Implement rate limiting via web application firewall

4 Security at the Checkout page

- Confirm all orders with a validation email sent to customer
- Require full password reentry at checkout for high-dollar orders or if stored shipping address changes
- Require verification of CVV2 for credit card purchases; don't allow null or wrong entries to be approved
- Deny purchase of gift cards with another gift card (activity enables money laundering)
- Limit unverified customer actions by removing "guest checkout" option

5 Considerations for Detection Control

- Employ rate-limiting access to APIs depending upon expected traffic. APIs should never allow traffic above 1.5x-2x the expected amount of traffic. Depending upon determined threshold value, calculate the average amount of typical customer traffic to a specific API or website feature on a 30- to 90-day dataset
- Identify business logic flaws using penetration testing activities such as:
  - Detecting sensitive APIs while bypassing authentication
  - Finding encrypted information within packet, due to logic error or poor header hygiene
  - Exposing logic flaws that allow bypass of security controls
  - Highlighting possible abuse of sensitive APIs

6 Awareness, Education and Collaboration

- Establish close relationships between CTI/Security and Fraud. All teams can benefit from sharing of knowledge
- Add ATO-specific information to FAQ pages to augment customer awareness
- Develop an incident response process for analysts to execute, and ensure that they are prepared in the event of an incident
- Develop a framework for tracking ATO tactics (and identifying campaigns) for future/ongoing analysis; continually revisit/update with detection and response teams
- Work with information sharing organizations like the R-CISC to disseminate pertinent information around TTPs for incoming ATO attacks

Failing to prevent ATO attacks creates risk to customers' accounts and data privacy, as well as impacting revenue and brand reputation. ATO attacks are becoming increasingly frequent and sophisticated, as criminals adapt methods in attempts to outmaneuver corporate fraud prevention activities. Use these tips to better protect your organization.

About the Retail Cyber Intelligence Sharing Center

The R-CISC is the trusted cybersecurity community for retailers, consumer products, grocers, hotels, gaming, restaurants and cybersecurity industry partners worldwide. The R-CISC supports its member base, representing more than $1 trillion in annual revenue, by serving as the conduit for collaboration, threat and best practice sharing, and cooperation. Through building and sustaining valuable programs, partnerships, products and opportunities, the R-CISC enables its members to build their trust-based relationships, strategic knowledge and tactical capabilities. For more information on R-CISC membership and benefits, visit us at our home page https://r-cisc.org.