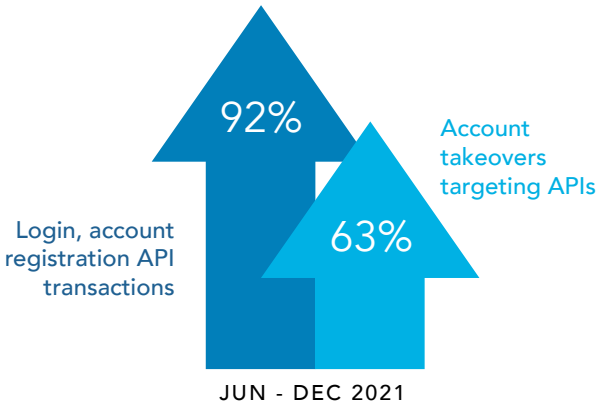
CEQUENCE SECURITY

The Account Takeover Cat-and-Mouse Game

ATO attacks are evolving. Jason Kent, hacker-in-residence at Cequence Security, discusses what new-style cyberattacks look like in the wild.

In an analysis of more than 21 billion application transactions analyzed by the Cequence Security Threat Research Team between June and December of last year, API-based account login and registration transactions increased by 92 percent to more than 850 million. Highlighting the fact that attackers love APIs just as much as developers, that same dataset showed account takeover (ATO) attacks on login APIs increased by 62 percent.

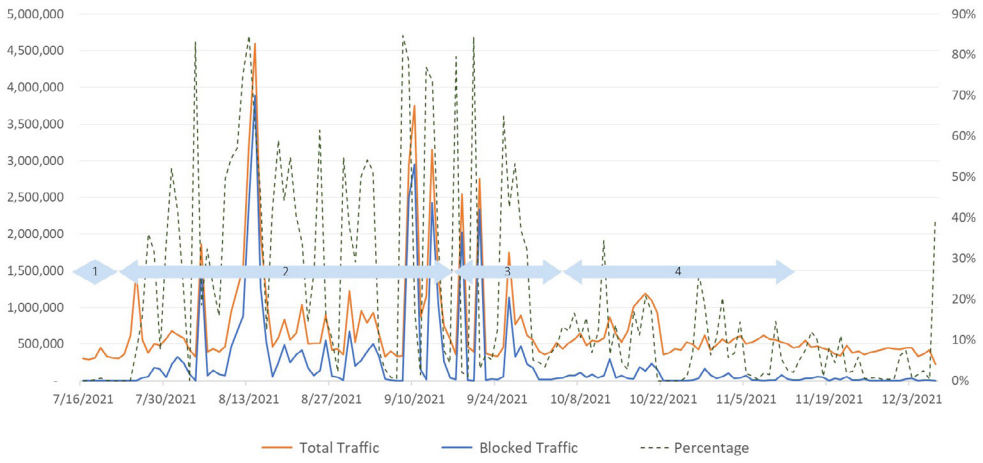


The initial impact of an ATO on an end user is to panic – they often get a message like, "you have received a password reset notification from your favorite retailer/social media/financial institution because your account has been compromised."

Being a victim of account takeover isn't very fun and causes one to want to stop doing business with the organization the account is for. The impact on the business is not only the potential loss of customers, but the impacts can be felt directly on the bottom line due to lost sales, infrastructure cost overruns and damage to the brand.

The Evolution of ATO Attack Techniques

ATO techniques have expanded beyond the commonly used hot-and-heavy, high-volume **credential stuffing**, to include methodical low-and-slow attacks using specific usernames and passwords.



These patterns are best exemplified in attacks on companies and individuals with a significant social presence (i.e., reviews, recommendations, etc.). For them, account takeovers are a persistent problem where the goal is to not necessarily steal from the compromised account, but to use it to amplify positive or negative information.

Between mid-July and late September 2021, one organization we examined experienced four distinct attack-defend cycles, outlined to the left.

Phase 1: ATO mitigation was enabled during the first week of July, resulting in an immediate impact. Bots disappeared – but only for about a week.

Phase 2: Bots returned with a vengeance beginning in late July, continuing for nearly two months with pedal to the metal, high-volume attacks consuming up to 80 percent of all login traffic. In this phase, the attackers continuously retooled their efforts every other day – looking for weaknesses in the defense. They also used hundreds of thousands of clean residential proxy IPs to distribute their actions and mask their identity and location.

Phase 3: In yet another attempt to hide in plain sight, during this phase, attackers shifted from high-volume to low-and-slow, mixing their evasive techniques. Attackers were seen reverse engineering good browser fingerprints and farming legitimate cookie profiles (both site-specific and common web tools like Google Analytics). For a period of more than three weeks, bot activity never exceeded 20 percent of overall traffic.

Phase 4: Bot activity has dropped to nearly an all-time low.

The patterns observed here have been seen previously in one form or another in other customer environments. Bots go quiet for a time period and they return with a vengeance. Monitoring bot forums confirms that botters often collaborate by sharing ideas, probing for unprotected vectors (like a deprecated API), all in preparation for the next attack. A successful defense requires continued vigilance, monitoring all types of endpoints – web, API and mobile, and collaboration between your peers and with your protection provider.

ATO is a problem that more and more organizations are facing as threat actors want to steal gift cards, access one-click purchasing and dominate hype-sales to buy and resell the inventory. As we have seen through this analysis, the pace and vigor are on the rise. All organizations that have an authenticated application should consider monitoring for ATO, and build mitigations to ensure their customer satisfaction remains high.

CEQUENCE® SECURITY

100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai