CEQUENCE™ SECURITY

Stopping Account Takeover Attacks with Cequence Security

Account Takeover Attacks are Easy, Automated, Widespread, and Successful

Bad actors using account takeover (ATO) attacks have an easy time of it – attack toolkits are readily available, attack infrastructure can be rented or owned, and new large sets of legitimate user credentials from previous attacks are made available regularly. Sticking these three components together has proven to be a successful recipe for gaining illegitimate access to user accounts at various online/web properties. Not only has it been made easy, but these attacks are increasing in sophistication. In response to some early attempts to defend applications – attackers now ensure that their infrastructure is appropriately sited and timed, their user agents look authentic, and their credential datasets are from the right geography. In many cases, these attackers have become sophisticated and specialized enough to sell the set of compromised accounts on the open market to attackers looking to harm that particular victim with another type of attack.

Existing Security Infrastructure Can't Stop ATO Attacks

ATO attacks "look" like regular network traffic – normal logins and application traffic – the same kind one might see from end users or legitimate automation from a business partner. So much of the traditional network security infrastructure – firewalls and IDS/IPS – is blind to ATO attacks. To a firewall, it looks like an allowed application login on the appropriate port. To an IDS or IPS, it is non-malicious traffic that doesn't exploit a known vulnerability. Many organizations adopted web application firewalls (WAFs) for a combination of compliance and security reasons. While WAFs take a closer look at application traffic, they are still doing it from a network perspective, and they are typically still looking for traffic that exploits a known vulnerability. They can be tuned for finer-grained inspection, but that usually proves to be more pain than most organizations are willing to undergo, and even with effort, WAFs will see most ATO attacks as "normal." Unfortunately, for many organizations, WAFs are simply compliance checkbox items. Finally, most "anti-bot" technologies are designed for a more recent past, assuming a browser-only application landscape (which is no longer the case) or requiring painful modification of the mobile app – ignoring the increasingly common avenue of risk that everything is converging on (the API).

What's Needed: A Solution That Sees the Application, the Attack, and Flexibly Mitigates

For many organizations, simply understanding the application attack surface is the first step. Surprisingly, many organizations may not even be aware of all the applications that have been deployed across their infrastructure. Even for a given application, the way a user or partner might access that business logic has proliferated – where browser-only was the norm in the past, many organizations have an API-first approach where mobile apps and browser-based apps are using the same API that IoT devices use. Second, a solution must be intelligent enough to distinguish the difference between ATO attacks and normal login activity – across all access methods (web browser, API, mobile app) – and be able to alert teams immediately when attacks are taking place. Third, a solution should be able to automatically stop attacks – either through its own mitigation capabilities or by working with surrounding infrastructure. Given that CAPTCHA has proven to stop legitimate users while only creating a moment-in-time speedbump for attackers, the solution must have other means of stopping attacks. Finally, integration flexibility is a requirement for most organizations – therefore, it must be deployable in a variety of environments (public/private cloud, virtualization, containers, etc.), with ease (no application changes). In summary, a solution must:

1. Understand attack surface – across browsers, mobile apps, and APIs
2. Understand and differentiate attacks vs. normal app traffic
3. Automatically stop and mitigate attacks
4. Be deployable across different infrastructures and app access methods

Cequence Application Security Platform Stops Account Takeover Attacks

With a flexible, software-only approach, Cequence discovers, detects, and defends. Cequence's Application Security Platform (ASP) first delivers visibility. Too many security teams don't have a clear picture of the resource they are protecting (the app) – components, access methods, locations, etc. Cequence enables security teams to have a complete, automated discovery of all applications in operation.

Cequence ASP spots ATO attacks. Cequence looks at application level behavior and applies machine learning and AI techniques to determine whether a particular application or API login attempt is a real user or an automated attempt. Cequence uses similar AI across all customers to understand bot behavior and the latest tricks attackers use to make their attacks look more like real logins. Thus, the Cequence Application Security Platform can identify ATO attacks when other security measures cannot. Specifically, Cequence looks at:

- **Behavior** – subtle inconsistencies in presentation vs. actions (how the traffic identifies itself vs. how it actually behaves), rates and response, sources and timing, and specific actions within the application or API
- **Network intelligence** – what's happening around the world – new attack or bot behaviors, new or changing attack infrastructure, newly known botnets
- **Specific to App/API** – learned or taught behavior specific to the app. Could be known good or known bad.

Cequence ASP stops ATO attacks. Depending on how enterprises deploy, Cequence enables in-solution mitigation of attacks (block, alert, or even misdirect to fool the attacker into thinking that they are being successful) or works with relevant security and application infrastructure (firewalls, load balancers, WAFs) to block attackers and their infrastructure. Furthermore, since Cequence has a native understanding of the application and its componentry, it can enable an accelerated response for teams to remediate any compromised accounts. In other words, it gives teams a list of compromised accounts to go fix.

Cequence Application Security Platform deploys in any environment. Cequence customers have deployed in traditional data centers, in public cloud and private cloud environments, across all sorts of virtualization and container infrastructure. Cequence provides a complete solution across all application access methods (web browser, API, mobile app) without time-consuming changes to the application or its infrastructure. Because Cequence decouples detection and mitigation, organizations can benefit from powerful analytics without inducing performance or response time issues for the application and infrastructure.

Cequence Provides Continuous Automated Defense Against a Continuous Threat – ATO Attacks

Due to the ease of implementation and the seemingly never-ending supply of user credentials from successful breaches, ATO will continue to be leveraged as a common attack technique. Organizations must implement and maintain a strong defense against ATO - one that understands apps and attacks, and integrates into enterprise applications, infrastructures, and operations. Cequence delivers.

Learn more about the Cequence Application Security Platform by visiting our website's resources section at cequence.ai/resources or schedule a demo at cequence.ai/demo.

CEQUENCE™ SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-408-978-3258 › info@cequence.ai › www.cequence.ai