CEQUENCE SECURITY

Protecting APIs from Automated Attacks

Driven by mobile device ubiquity and the move towards modular applications, organizations are using APIs to enable application business logic, facilitate integration with other system elements, and reduce development time. Unfortunately, APIs are a double edged sword, introducing an attack vector that is often times, left unprotected. According to Gartner, by 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the UI, up from 40% in 20191. There are multiple drivers behind the use of APIs as an attack vector.

› **APIs simplify automated attacks:** As shown in the Prying-Eye vulnerability discovered by Cequence Security in late 2019, bad actors can enumerate through web meeting IDs directly against the exposed API. If valid meetings are discovered without security enabled, the bad actor could join the meeting. By targeting the API instead of a web form, the bad actor is leveraging the same benefits of ease of use, efficiency and flexibility that APIs bring to the development community.

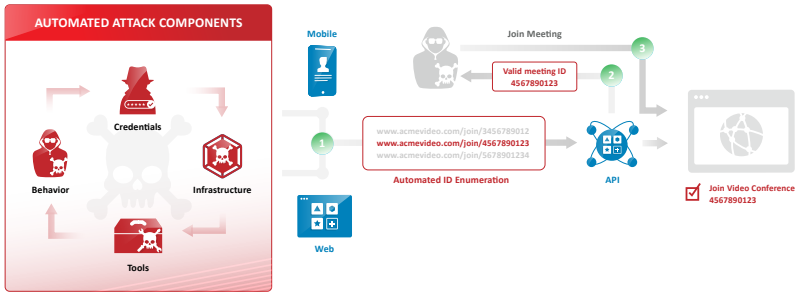


Image 1: Prying-Eye vulnerability allowed bad actors to discover and join valid web meetings through an enumeration attack across a set of exposed APIs.

› **Readily available API documentation:** Whether it's on your website, or on one of the many API repositories like programmableweb.com, GitHub, or SWAGGER, information on how the APIs work is readily available. In some cases, errors are made by the dev teams and API keys are published on GitHub, or in an Amazon S3 bucket, further exposing your application assets to attack.

› **Mobile apps use APIs heavily:** Decompiling a mobile app to discover the APIs in use represents another readily available source information for bad actors to use in an attack. In a financial services customer example, bad actors analyzed the mobile app, discovering and then using the login API to launch account takeover (credential stuffing) attacks. If an account takeover was successful, the bad actor would then would transfer funds to their own (fake) account using the OFX API – the financial services funds transfer protocol. Fortunately, the customer was able to block the attacks and stop the associated fraud or theft using Bot Defense.

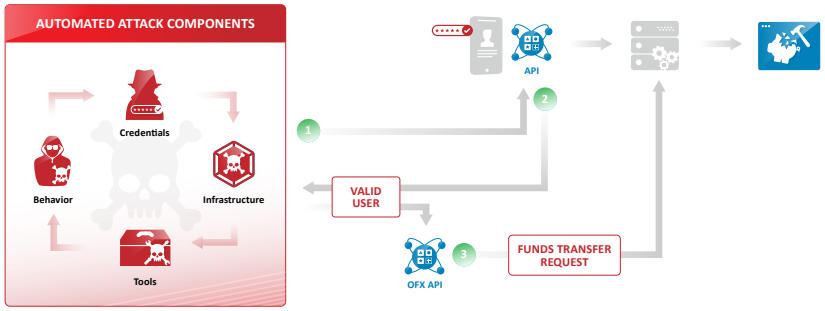


Image 2: Bad actors use mobile APIs as a means of automating account takeovers and if successful, commit fraud or theft.

Alternative Approaches to API Security

Researching API security will show that there are four distinct solution groups, each addressing specific challenges.

- **API Gateways:** the most mature and heavily populated category, these solutions focus heavily on visibility and control.
- **API Security:** largely populated with startups that find your APIs and protect them from vulnerabilities or data leakage.
- **Web Application Firewalls:** apply traditional web-based vulnerability exploit protection to APIs.
- **First Generation Bot Mitigation Vendors:** prevent automated attacks against web and mobile apps using JavaScript instrumentation and mobile SDKs to collect attack telemetry. Adding API security as an afterthought through a variety of approaches.

None of these solutions address the key requirements of complete visibility and consistent protection from automated attacks against APIs as well as web and mobile applications. In many cases, customers will use multiple offerings from the mix of API security providers.

How Bot Defense Protects APIs from Automated Attacks

The Cequence Application Security Platform (ASP) with Bot Defense uses an out-of-band, ML-based approach to protect the APIs supporting your public facing web and mobile applications from automated attacks and business logic abuse. The ASP is comprised of the following components:

- **CQAI** uses customizable machine-learning automation indicators to discover and analyze your public facing APIs, building an intuitive sitemap for complete visibility and to determine if the API activity is malicious or benign. CQAI findings are then used to enforce policy or exported via a REST-based API to an existing component of your security infrastructure.
- **Bot Defense** enforces mitigation policies based on CQAI findings with a range of response options including blocking, rate limiting, geo-fencing and deception.

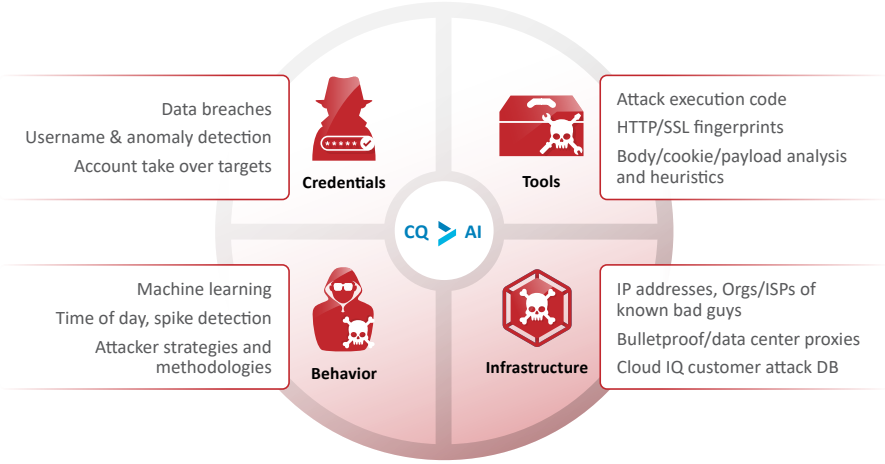
Bot Defense Features Features

Continuous Discovery and Visibility

The unique ML-based approach taken by CQAI discovers all the APIs that support your public facing web and mobile applications, automatically building an intuitive site map. Newly deployed APIs and other public-facing applications are automatically discovered and protected as they are deployed. Traditional prevention approaches that use JavaScript and mobile SDKs to collect the necessary telemetry are cumbersome to implement and provide inconsistent protection against attacks that target APIs directly.

Dynamic Machine Learning

CQAI determines the intent of each API-based transaction using more than 150 customizable ML-based automation indicators distributed across the Four Pillars of Detection: Credentials, Tools, Infrastructure and Behavior. Performed out-of-band, the CQAI analysis detects and prevents automated attacks targeting your APIs while simultaneously delivering two key benefits. Security is baked into your application workflow,



eliminating application JavaScript instrumentation and mobile SDK integration penalties such as deployment delays and slow page load times. The second benefit is consistent protection for exposed APIs, web and mobile applications and an opportunity to consolidate application security functions into a single platform.

Customizable Rules, Policies and Response Options

Complete application and attack visibility is translated into policies that enforce a positive security model – allowing what you want and denying all else. Automation indicators can be tailored to your environment to continually detect bot traffic as bad actors modify their behavior. Mitigation options include blocking, rate limiting, geo-fencing and deception; an alternative that allows you to mislead the attacker into believing that their attacks have been successful.

Open, Extensible Platform Integrates with Existing IT Infrastructure

As a means of improving your overall security posture, CQAI findings can be exported to your existing IT infrastructure such as another security device for enforcement, a SIEM, or a REST API endpoint for added analysis or correlation. The REST API also allows you to export the attack response results for post-mortem analysis and fine-tuning.

Flexible Deployment Options

Deployed in your data center, the cloud or as a SaaS offering, Bot Defense protects your APIs along with your web and mobile applications with a consistent attack protection, resulting in reduced operational burden associated with deploying multiple API security offerings while simultaneously improving your security posture.

[1] Gartner, API Security: What You Need to Do to Protect Your APIs, August 2019

CEQUENCE® SECURITY

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