CEQUENCE

Solution Brief

Protecting Financial Services APIs From Automated Attacks

Driven by the move towards modular applications and mobile device ubiquity, the financial services industry (banks, credit unions, credit card, and financial technology) were early API adopters as a means of engaging users with equal efficiency through a mobile app or a browser while fostering a vast 3rd-party ecosystem. The reason for the early adoption is simple – APIs provide speed and flexibility for developers. Validating that APIs are the development tool of choice, the Cequence CQ Prime Threat Research team found that 14.4 billion or 70% of the 21.1 billion application requests analyzed during the second-half, 2021 were API-based. In the same time period, the research team found that 80% of mitigated traffic was API-based, a finding that confirms the notion that attackers love APIs as much as developers.

Financial Services Targeted by API-based Account Takeovers

Industry research by BCG Digital states that financial services organizations are 300 times as likely as other companies to be targeted by a cyberattack. Attackers view the assets held and programs provided by the financial services industry as highly coveted targets, using a variety of techniques to execute account takeovers (ATOs) against APIs that often result in theft or fraud:

Shadow and zombie APIs

Attackers will use open source tools to find and attack shadow or zombie APIs that are unknown, unmanaged, and un-secured. Shadow APIs are a rapidly growing problem, as documented by Gartner who state that by 2025 less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools. This industry statistic is further validated by the Cequence CQ Prime Threat Research Team finding that roughly 30%, or 5 billion of the 16.7 billion attacks mitigated in the first-half 2022 targeted unknown, unmanaged, and un-secured APIs, commonly referred to as shadow, or zombie APIs.

Exploit API coding errors

Alternatively, analysis may uncover and exploit API coding errors that expose too much data, provide access to sensitive data, or allow unfettered access to user data.

Target perfectly coded APIs

Attackers analyze perfectly coded APIs to understand how they work, then use commercially available attack tools combined with the billions of readily available stolen credentials to launch automated high-volume attacks.

ATOs impact many different business groups including security, fraud, compliance, IT infrastructure, PR, and marketing. For EACH compromised account, the financial impact ranges from $290 (Juniper Research) and nine hours of investigative work to $311 (Federal Trade Commission).

Traditional API Security for Financial Services Falls Short

Many organizations turn to first-generation bot detection vendors to address automated attacks against their APIs with limited success due to the client-based (JavaScript and mobile SDKs) approach used by the bot management vendors. The client-less nature of APIs means that first-generation bot solutions have limited access to telemetry data and other information needed to determine if the intent of a transaction is malicious or not. Without this capability, policy enforcement and visibility become inconsistent across all of an organization's application endpoints – web, mobile, and, most critically, supporting APIs.

Compounding the ineffectiveness of bot detection offerings is the fact that security teams lack the visibility and defense capabilities they need to reduce the risks introduced by the explosive use of APIs. Many organizations believe that compliance with PCI or SOC 2 and a shift-left, DevOps approach is sufficient to protect APIs. The problem with these strategies is that they have no way to uncover all the (shadow, or zombie) APIs and API vulnerabilities without knowing where to look. Even if all APIs are discovered and known, attackers can still leverage seemingly legitimate transactions to steal data or commit fraud. Traditional approaches that use WAFs or API gateways depend on easily evadable detection, lack the real-time ability to discern good from bad API activity and are reliant on static, least common denominator protection spread across multiple technology components.

Solution: Cequence Unified API Protection

The Cequence Unified API Protection solution takes a comprehensive approach to securing financial services APIs by addressing each of the six phases of the API security lifecycle. Using a full-spectrum approach ensures that all your APIs are discovered, analyzed for hidden risks, and protected from automated threats and vulnerability exploits.

Outside-in discovery

Viewing an organization's API attack surface from a threat actor perspective to know the unknown.

Inside-out inventory

Performing a comprehensive API inventory, including all existing APIs and connections.

Compliance monitoring

Keeping APIs in compliance with specifications such as the OpenAPI framework, standards including OWASP API top 10 and regulations including PCI to ensure high API coding quality, consistency, and governance.

Threat detection

Continuously scanning for threats, including subtle business logic abuses and malicious activity that has not yet been observed.

Threat prevention

Employing countermeasures such as alerts, real-time blocking and even deception, without the need for added third-party data security tools.

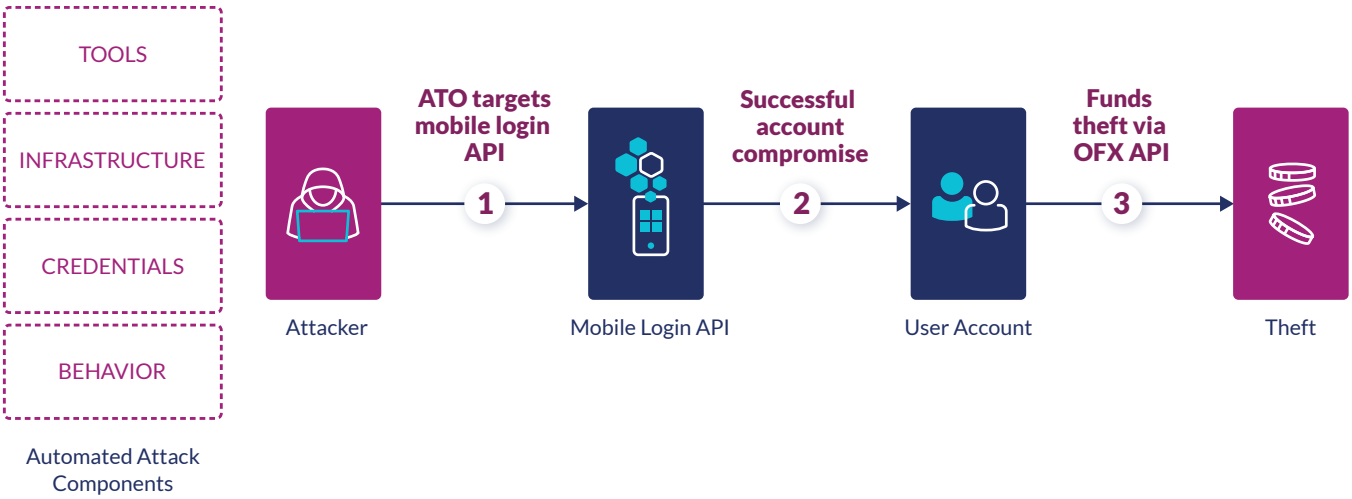
Ongoing API testing

Integrating API protection into development, which shifts API security left within the organization, so risky code doesn't go live.

Unified API Protection is different from fragmented or incomplete API protection offerings because it's a methodology designed to account for multiple types of risk, across every phase of the API protection lifecycle.

Customer Spotlight: Fortune 100 Financial Services Company

At a Fortune 100 financial services organization attackers analyzed the mobile application to fully understand how the login API worked. They then used known tools, malicious infrastructure and readily available (stolen) credentials to launch a sophsitcated ATO campaign. When they met resistance, the attackers quickly modified behaviors to continue their onslaught. If a malicious login attempt was successful, they would proceed to transfer funds to their own (fake) account using the OFX API, the financial services industry standard fund transfer protocol. Faced with mounting fraud, customer dissatisfaction and an API first development methodology, the customer turned to the Cequence Unified API Protection solution to stop the attacks.



The Cequence UAP detects ATOs using an advanced ML-based analytics engine that automatically discovers API, web and mobile application endpoints to build an intuitive site map for visibility and policy-based protection. Predefined policies based on the largest API threat database available dynamically determines the intent of each transaction request. If malicious activity is detected, the customer was able to natively enable mitigation policies using multiple response options such as blocking, rate limiting or deception. The agentless, ML-based approach of the UAP helped them achieve the following results:

- Significantly reduce their organization's API attack surface
- Prevent patterns of misuse that led to fraud and user dissatisfaction
- Protect newly deployed APIs and web apps automatically
- Unify protection for public-facing web, mobile and API-based applications

Today, the customer is using Cequence UAP to protect more than 50 public-facing applications, preventing fraud and theft associated with ATOs.

Get an Attacker's View into Your Organization

CEQUENCE
100 S. Murphy Avenue, Suite 300, Sunnyvale, CA 94086 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai
© 2023 Cequence Security, Inc. All rights reserved.