F5 API Security Battlecard

carahsoft

Industry Trends and Federal Drivers

Increases in the use of API's within federal agencies to achieve automation and move into the DevOps cultural/space. While externally API's are being used for agency to agency information and data sharing.

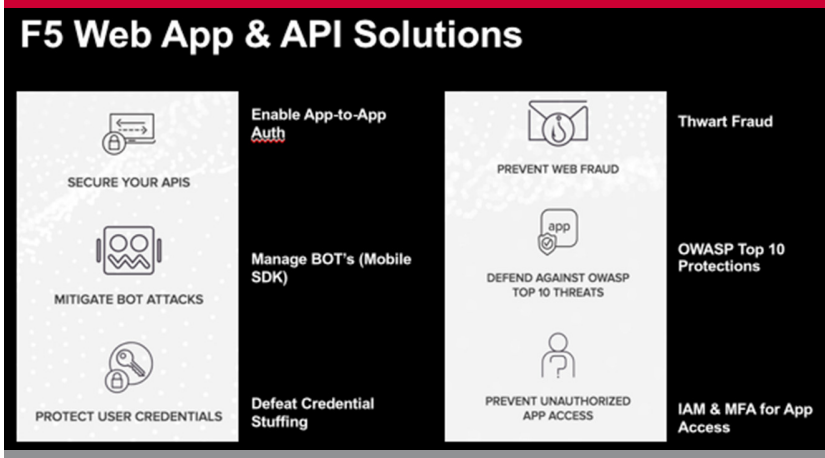
- High growth in REST API's. Using REST API's allow you to auto-provision virtual servers, automate backup intervals, and provide version control for workflows. REST API's use HTTP request to GET, PUT, POST, and DELETE data.
- Exponential Application Growth (Mobile, Cloud, & IoT)
- Rapid adoption of automation for in application development
- New security challenges around mobile & web applications and use
- These drivers stem from the growing trend towards speeding up app development through adopting architectures using DevOps, containers, and microservices, as well as supporting automation toolchains and frameworks. Ex: AWS Cloud Formation Templates

Problem Facing Customers

API are susceptible to the same vulnerabilities that traditional web applications have like:

- Denial of Service
- Web Application Vulnerabilities like SQL injection and XSS
- JSON Parser Crashing
- Man-In-The-Browser
- Session Hijacking
- Data Disclosure
- Key Disclosure or Certification Spoofing
- DNS Cache Poisoning

PUA Solution Overview



F5 provides superior API protections to address today's most dynamic threats. Helping customers verify the app to app authentication is always secure and available.

- Protect against app exploits
- App availability / performance
- Stop BOTS and DDoS / DoS
- Critical for Zero-Trust architecture
- App Auth / MFA enforcement

Probing Questions

- How are planning to protect your API's today?
- How do you protect your API gateway in the cloud?
- What is your plan for implementing API security architecture for mobile?
- Do you have an API architect / champion within your organization?
- Do you secure shared application information between agencies?
- What s/w modules are running on your BIG-IP's?

Elevator Discussion

As federal agencies looks to expand application services to you end users, Single Page Apps (SPA) are quickly becoming the standard interface to access these services through API calls. To secure access to these systems F5 can protect your network from automated and human hacking, by controlling access to your agency's resources, centrally controlling the OAuth access tokens and using F5 Advanced WAF to protect your systems from BOTS, application attacks and Denial of Service (DoS). F5 is your answer to defend against hackers trying to exploit your network though API calls.

Carahsoft Technology Corp. | 1860 Michael Faraday Drive, Suite 100 | Reston, VA 20190 | 877-95-F5GOV
f5@carahsoft.com | www.carahsoft.com/f5