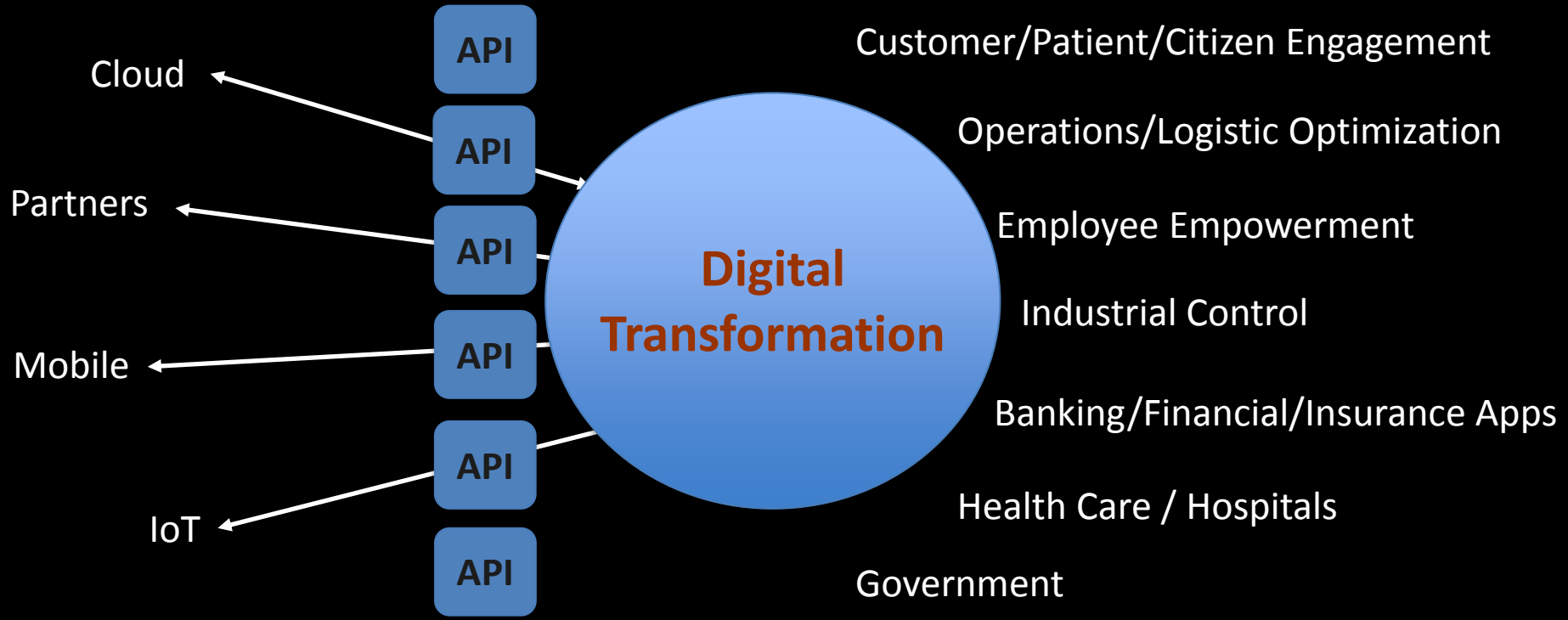
API Security: The Past, Present, and Future

Bernard Harguindeguy

Founder and CEO Elastic Beam

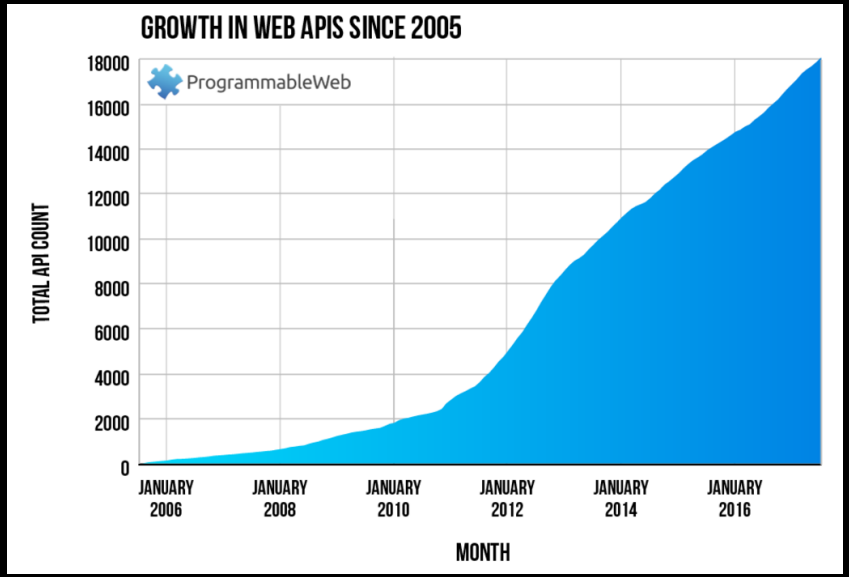
- CEO of Elastic Beam – API cyber security
- CEO of GreenBorder – Browser security company acquired by Google – Solution → Chrome
- CEO of WorldTalk (NASDAQ) – security company acquired by Tumbleweed – co-invented S/MIME
- Board of Sygate Technologies – desktop security company sold to Symantec – leading desktop fwl
- Chairman of BorderWare – network appliance security company sold to WatchGuard
- EVP/GM Critical Path Identity Management Business

APIs Are the Building Blocks for Digital Transformation



APIs Are an Emerging Vulnerability

Public API Growth



Source: ProgrammableWeb website

"To put perspective on how difficult API security is, **pretty much every major Internet company has had API security problems."** – ProgrammableWeb 2017

"... individuals obtained access to high-profile **Instagram** users'... **by exploiting a bug in an Instagram API**" – Instagram statement

Private photos belonging to several celebrities … were shared on the Internet after hackers allegedly **penetrated an Apple API**" – ProgrammableWeb 2015

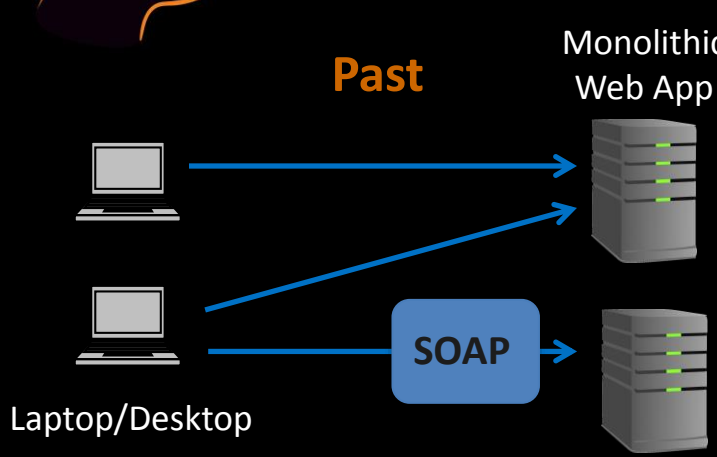
"100,000 taxpayers victims of the latest data breach … with **automated, brute force probe using IRS's public API** ..." – Forbes 2015

Facebook, Snapchat, Cisco, Symantec, Verizon, PayPal, Apple, McDonald's, …

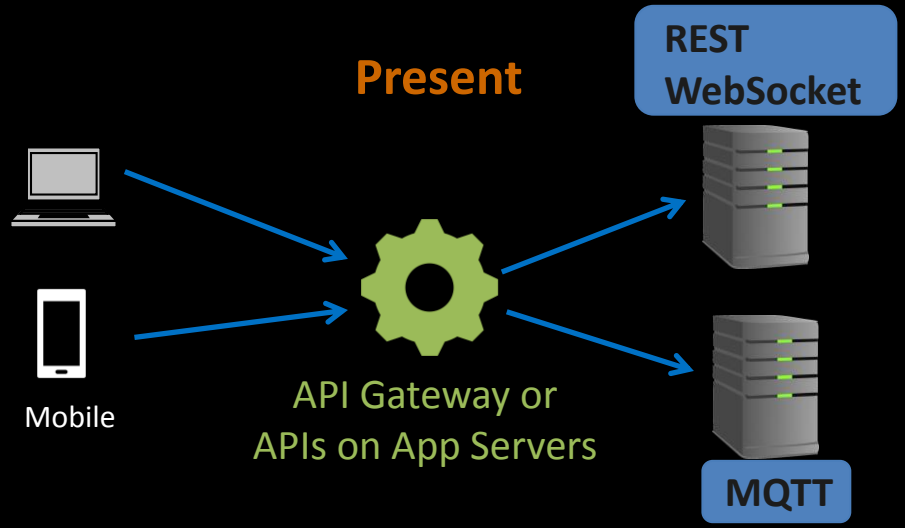
API Breach Impact

- Client and Patient accounts taken over
- Data breaches – safeguard customer records, private data, photos, …
- Fraud for banks, retailers, payment processors, …
- Industrial control systems taken hostage or worse …
- Services shut down or disrupted
- *Cloud / DC performance problems and costly ops snafus*

How Did We Get to Where We Are Today?



- Internal users
- SOA and SOAP APIs
- Ad hoc Control
- No/Basic Login to each API
- Cookies



- **External** and internal facing
- API services with centralized control
- OAuth2, stronger authentication
- Single Sign-on
- Tokens, API Keys, Cookies

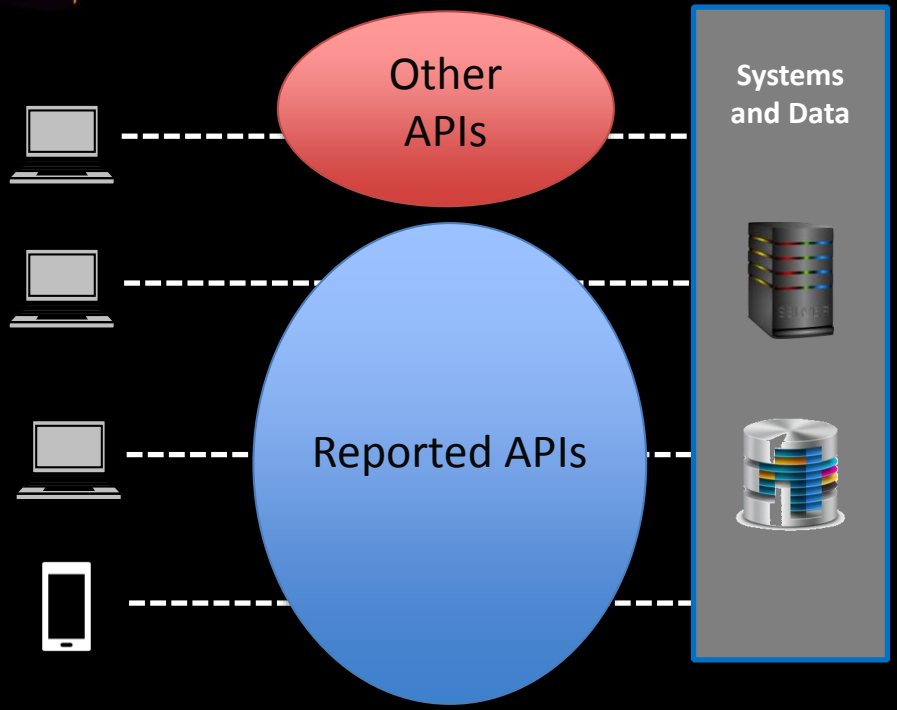
Today's API Security Gaps

Attacks on data, applications, and systems are not detected or blocked!

Post-Login Attacks	**Data, Application, System Attacks** APTs, Data exfiltration, deletion,…
	API/Layer 7 DDoS Attacks Compromise API services Access
Pre-Login Attacks	**Authentication Service Attacks** Credential stuffing, Fuzzing, Stolen cookies and tokens
Foundational API Security	**Access Control** Tokens, Authentication, Authorization
	Rate Limiting Client throttling, quotas
	Network Privacy SSL/TLS

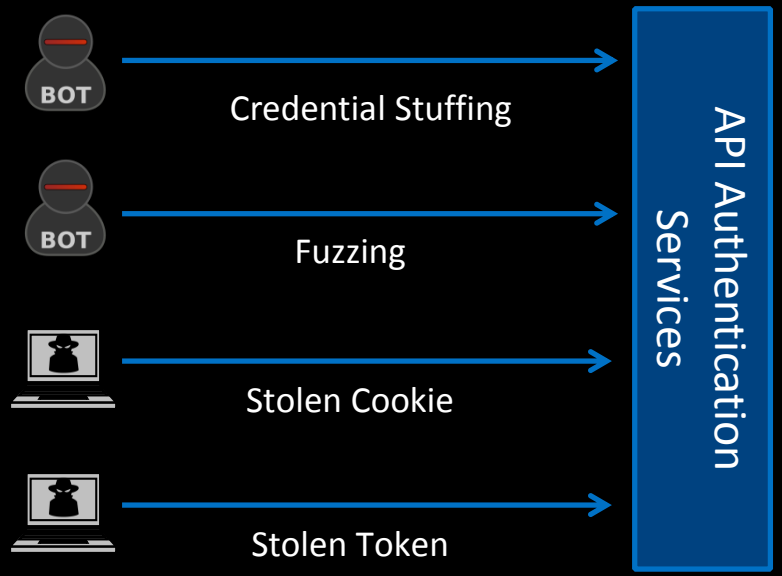
- Foundational API security no longer enough to protect against cyberattacks
- API Cyber Security requirements
  - Knowing about all APIs
  - Login/Identity attack detection
  - Cyberattacks on data, apps, systems
  - API-specific DDoS attacks protection
  - Deep reporting on all API traffic

Knowing About all APIs



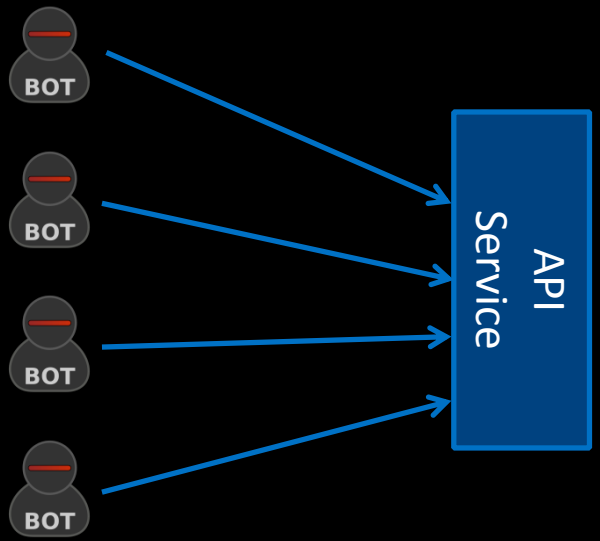
- Complete visibility to all API services
- DevOps reported APIs
- APIs not reported/not published

Attacks on API Authentication Services



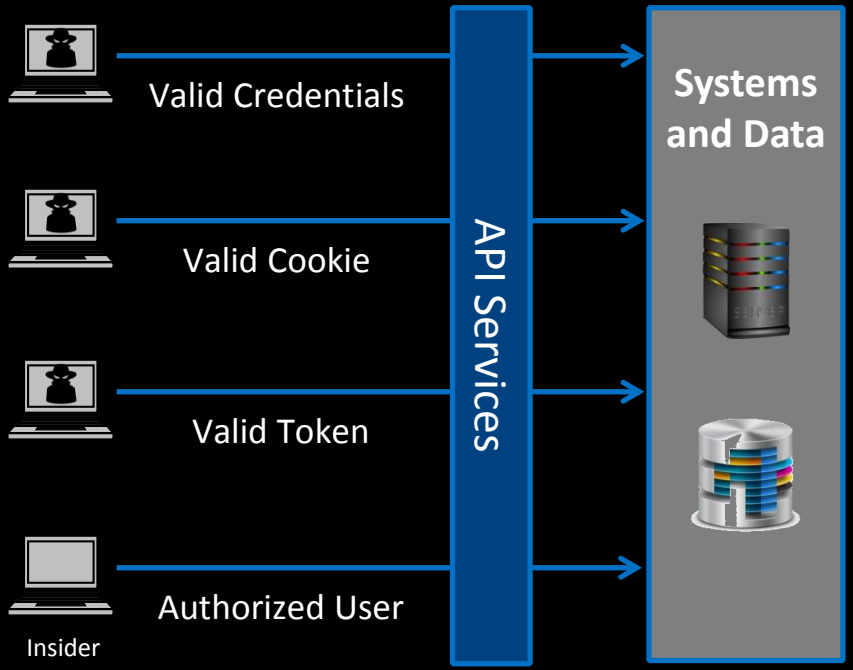
- Examples:
  - Automated credential guessing consumes resources and leads to compromised accounts
  - Replay attacks probe for application vulnerabilities to gain backdoor access
  - Stolen identifiers provide a hacker a vehicle to piggyback on authorized sessions
- Difficult to detect most in real-time

API/Layer 7 DoS/DDoS Attacks



- Different from Layer 3/4 DDoS which overwhelms network
- Clients keep activity below rate limits by intelligently adapting
- Attack examples:
  - DoS attack on API memory to disable the service
  - Multiple client distributed attack to disrupt login services
  - DDoS attack on cookie management service
- Intelligent algorithm needed to identify API DoS/DDoS attacks

Authorized User Attacks

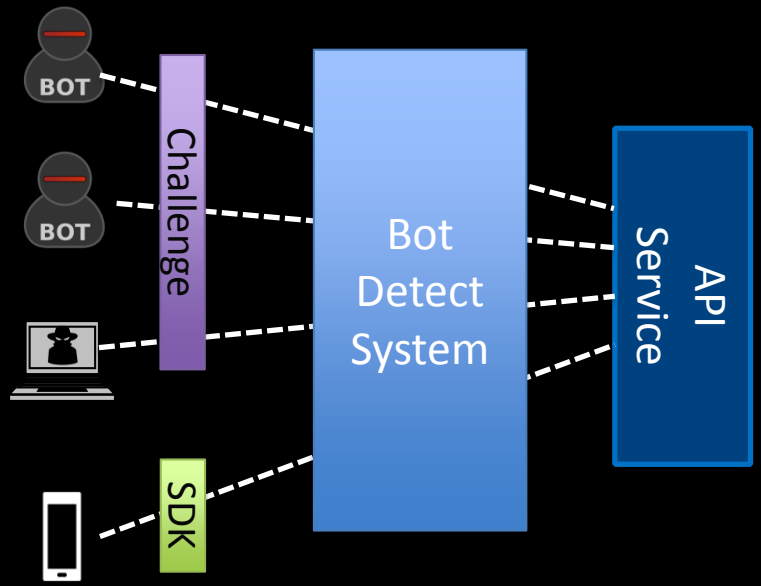


- With compromised credentials look like authorized clients – could be an insider also
- Attack examples:
  - Data exfiltration
  - Data manipulation or deletion
  - Account take over
  - Control system attacks
  - Line of business application attacks
- Most difficult to detect – must understand normal user behavior or specific attack pattern

How to Stop API Attacks

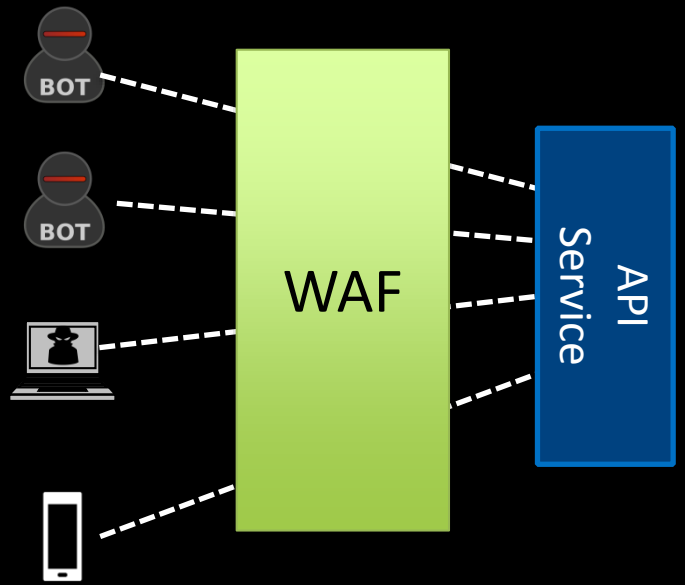
- Start with proper API security testing
- Try to use automated lines of defenses
  - User Behavior / Client Validation (pre login)
  - Vulnerability protection and attack signatures (pre/post login)
  - Traffic Behavior (pre/post login)
  - Application Behavior (post login)

User Behavior / Client Validation



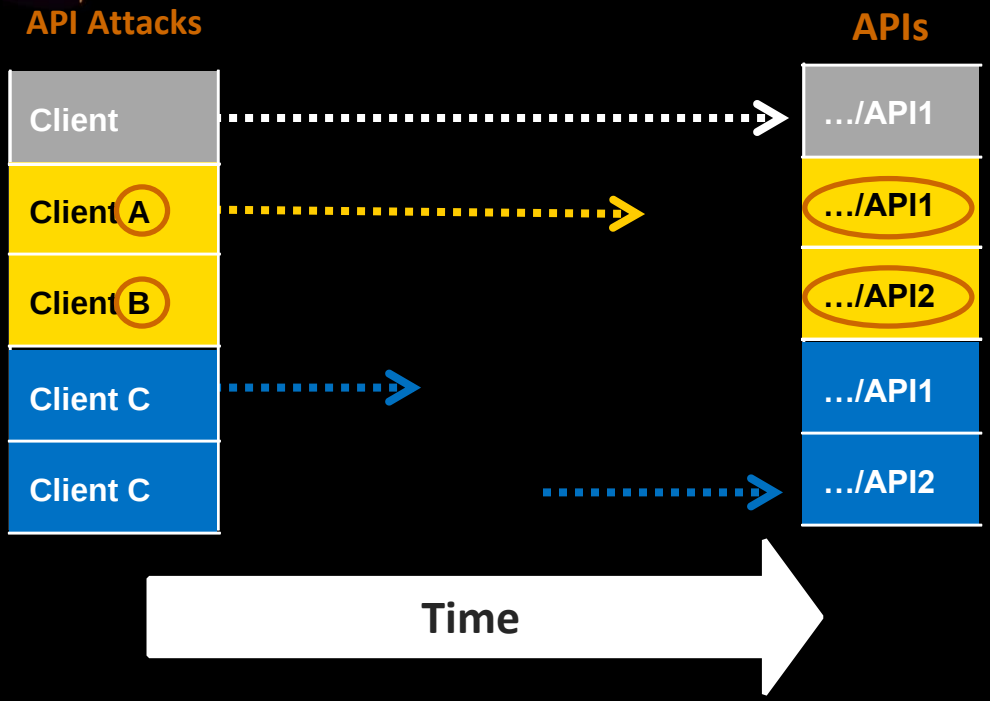
- Inline Protection for Login Service
- Validate client using device type techniques
  - BOT/Browser – challenges to test client validity
  - Mobile device – SDK to fingerprint client app
- Login activity analysis – Login traffic patterns, Geolocation, Time of Day, etc.

Vulnerability Protection and Attack Signature



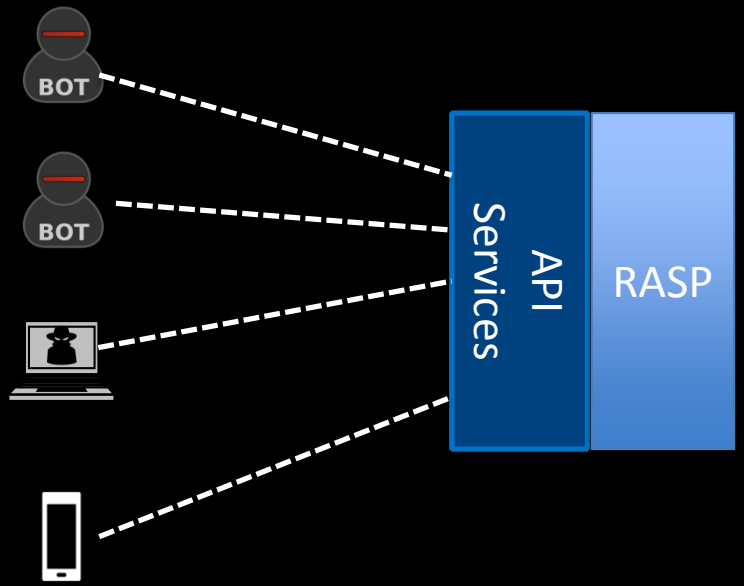
- Real-time analysis for attacks including OWASP Top 10
  - CMD injection, SQL Injection, …
  - Cross-site scripting, …
  - Addressing known vulnerabilities
  - API Attacks recently added to OWASP list
- Custom rule support for specific attack detection – e.g. invalid fields
- Relies on known vulnerabilities, attack signatures and attack patterns

API Traffic Behavior



- Analyze API activity against normal use
- Detect attacks based on behavior and not just user-defined rules
- Identify probing activity
- Monitor excessive error activity
- Etc.

Application Code Behavior

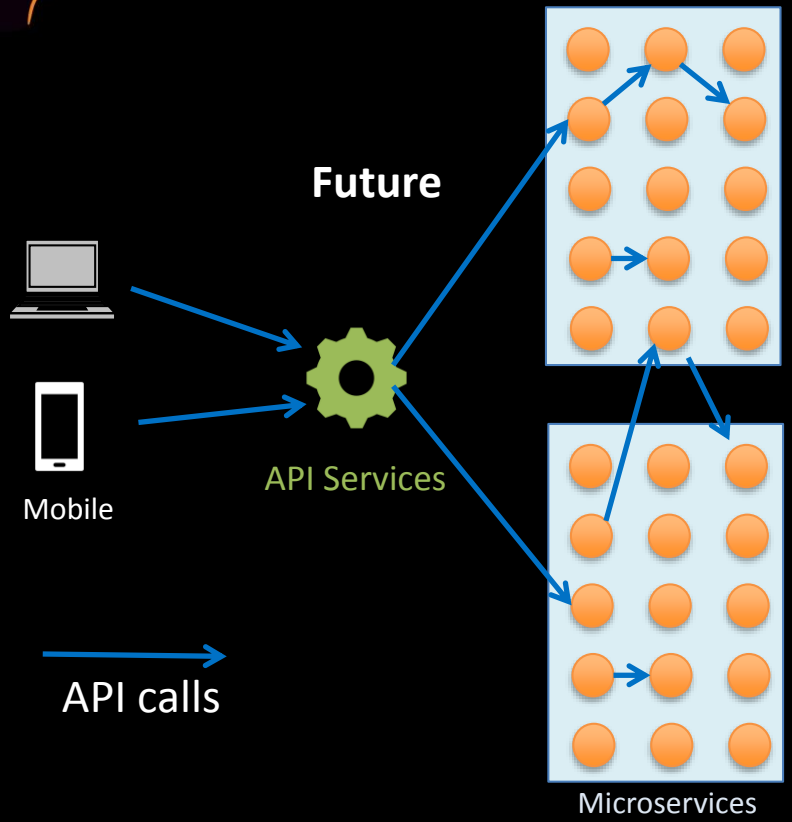


- Integrates with code libraries to protect applications
- Intercepts run time calls when harmful activity is detected
- Always active
- Last line of defense – attack in server at that moment but will capture valuable attack information as well

How to Stop API Attacks

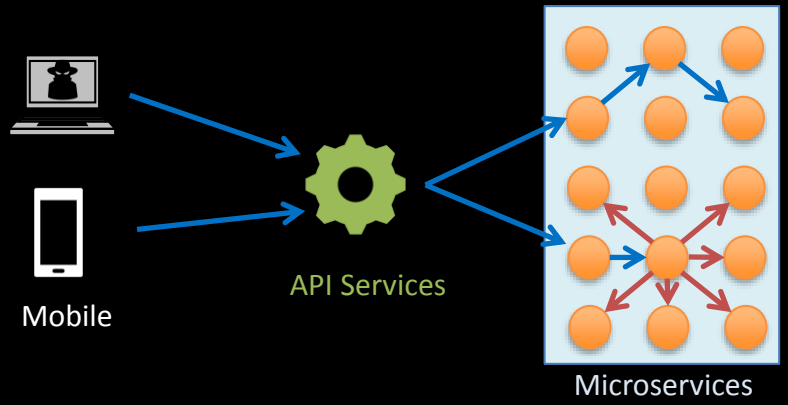
- API Security is hard
- Automated lines of defenses
  - User Behavior / Client Validation (pre login)
  - Vulnerability protection and attack signatures (pre/post login)
  - Traffic Behavior (pre/post login)
  - Application Behavior (post login)

What will API Ecosystems Look Like in the Future?



- API Services for Perimeter Control
- Microservices with APIs communication
- Distributed control and validation

DDoS with Cascading Requests



- Simple request generates many backend requests
- Inbound client activity below rate limits
- Netflix at 2017 DefCon Security Conference described attack; released open-source test

Some Guidance / Best Practices

1. Test APIs for security – “think like a hacker”
2. Continuous security mindset a must
3. **Automated security** scans/tests/monitoring
4. Deploy a strong authentication system
5. Utilize flow control and TLS (https) encryption
6. Prevent app servers from sending error messages with system traces
7. Don’t register internal API names in public DNS
8. Perform periodic reviews of all API access to identify abnormalities

Bernard Harguindeguy

Elastic Beam

Email: bernard@elasticbeam.com

Thank You!