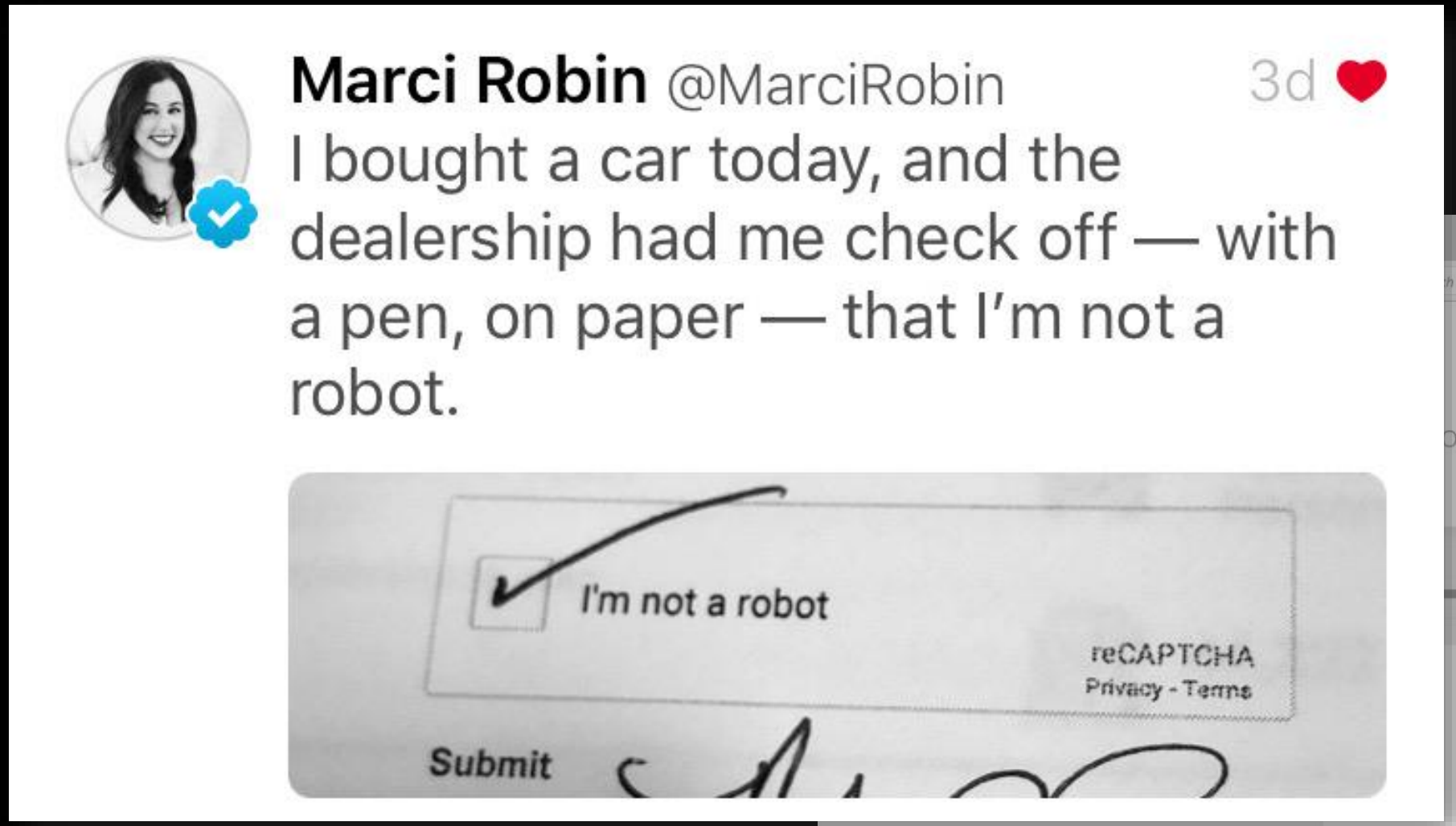
Sustainable WebApp Security

PRESENTED BY:

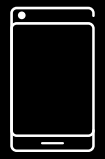
Luboš Klokner | F5 Networks | Sr. Systems Engineer

lubos@f5.com | +421 908 755152 | @lklokner



AppSec

Fiction vs. Reality



AppSec

Fiction vs. Reality

Modern

WebApp

AppSec

Fiction vs. Reality

Modern

WebApp

Threats

… and protections

AppSec: Guidance vs. Reality

Patch your S#1t!

(Except if the patch breaks your app)

Scan for vulns!

(Only if you like bad news)

Review your code!

(Because DEVs have lots of free time)

Use modern frameworks!

(But don’t touch that legacy apps)

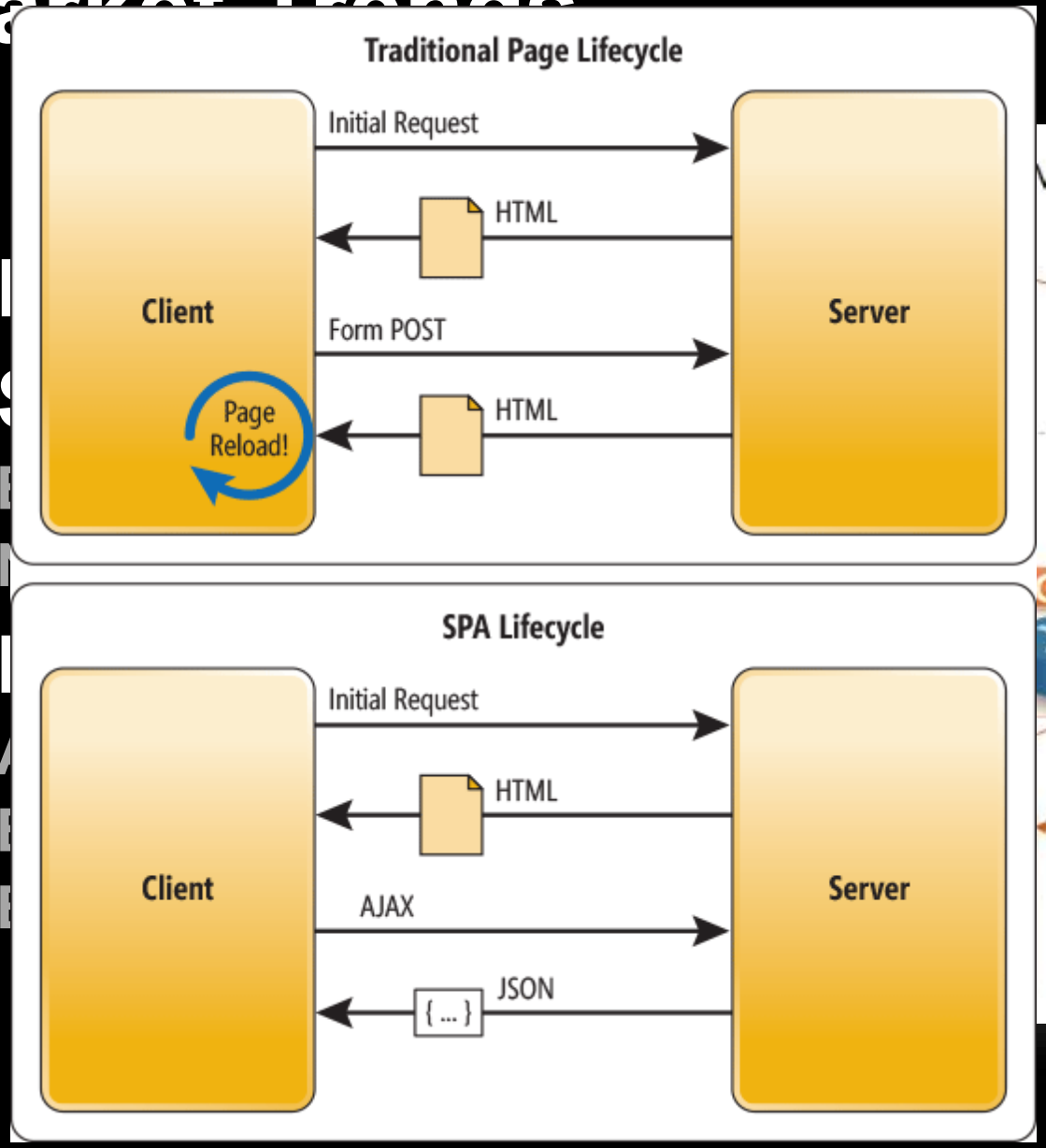
Application security is hard.

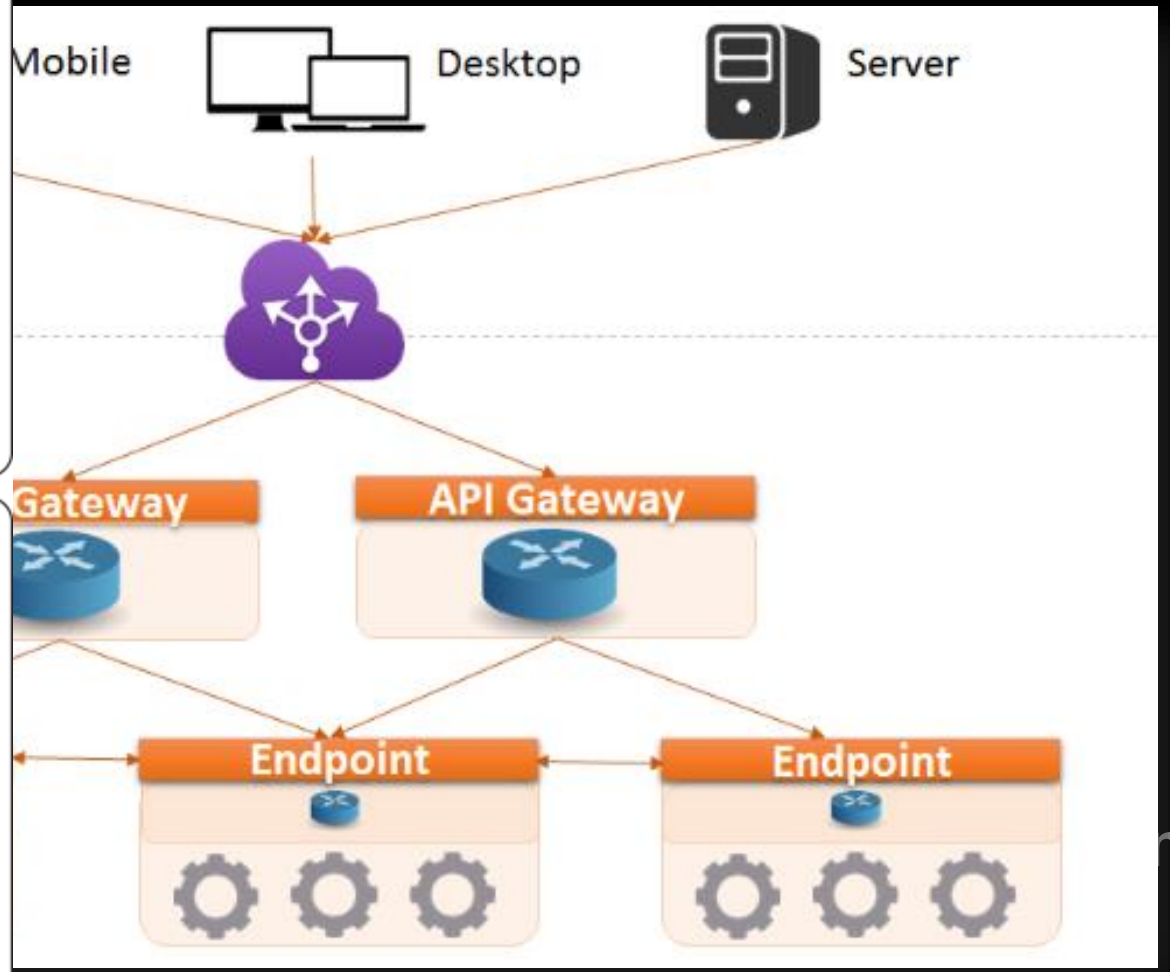
(But only if you focus on the apps)

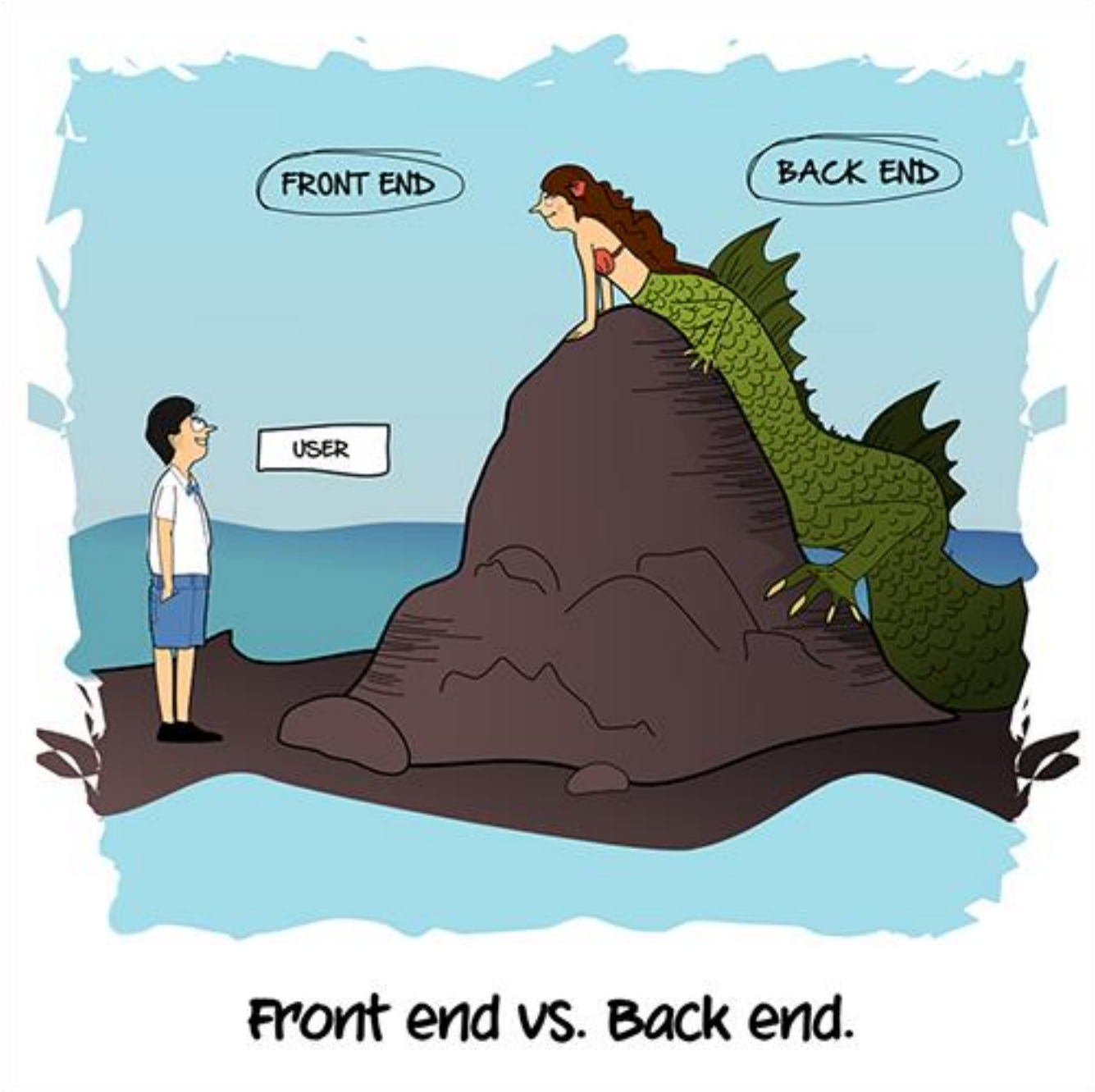
Modern Web Application

“…a web application that fits on a single page with the goal of providing a user experience similar to a desktop application”

Market Trends



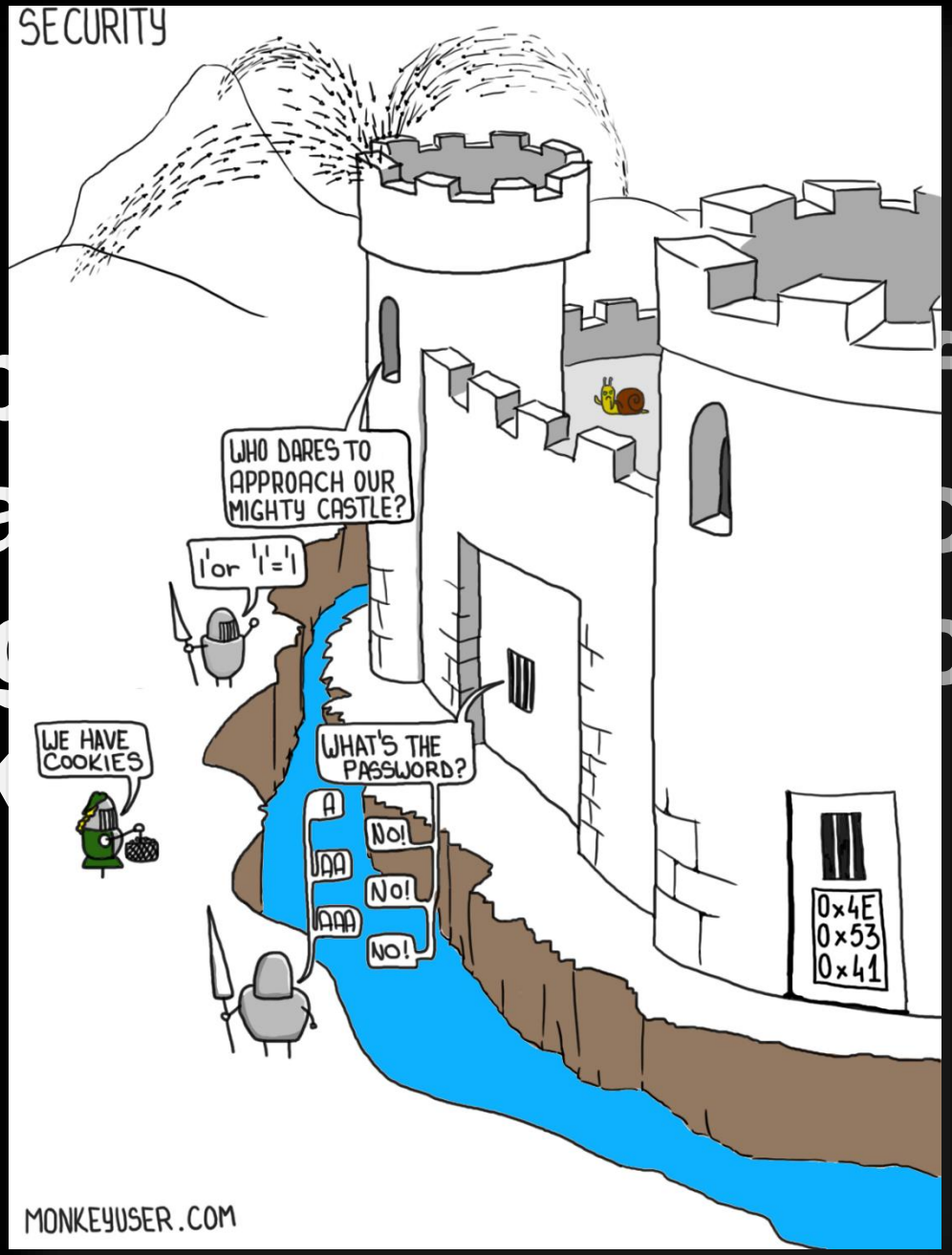




Source: comic.browserling.com

Threats and Protections

“…a web fits on a single pa of providing ce similar to a desk



Vectors of Attack

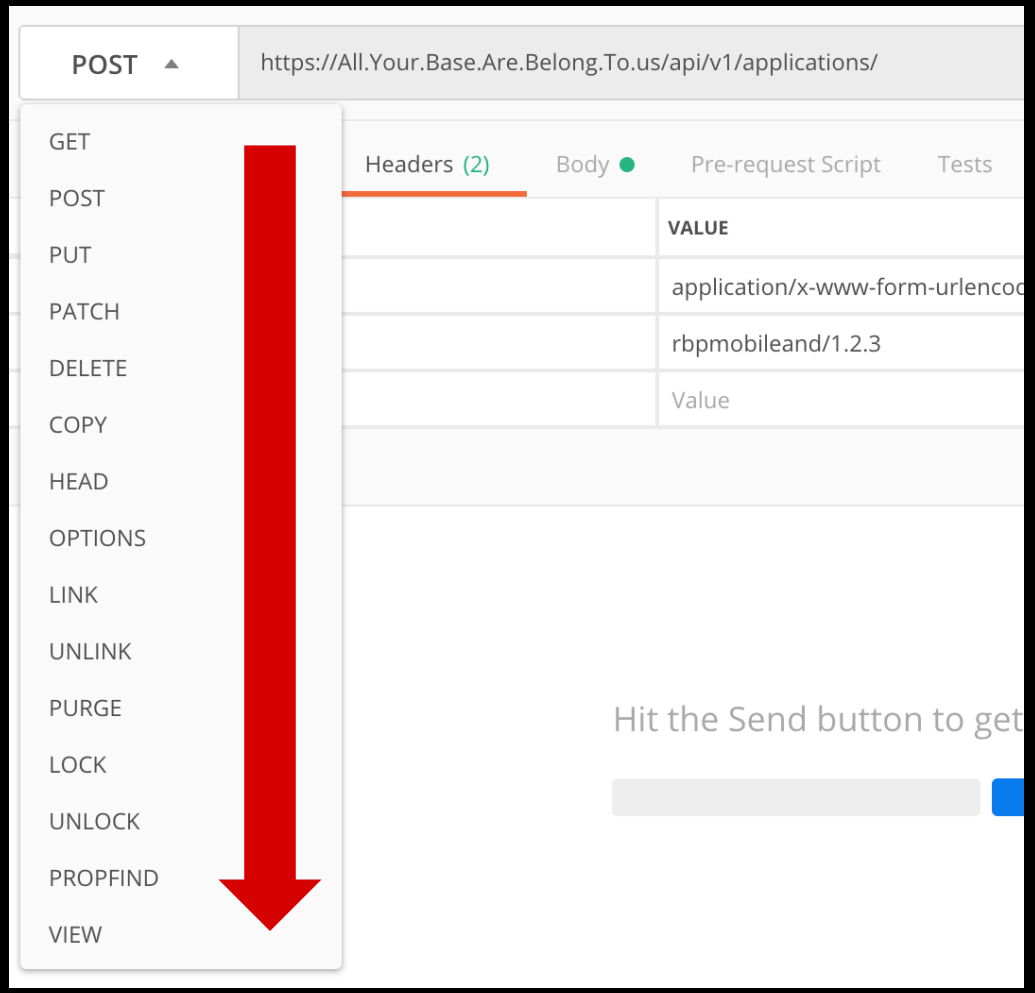
- Traditional Web Page

GET

POST

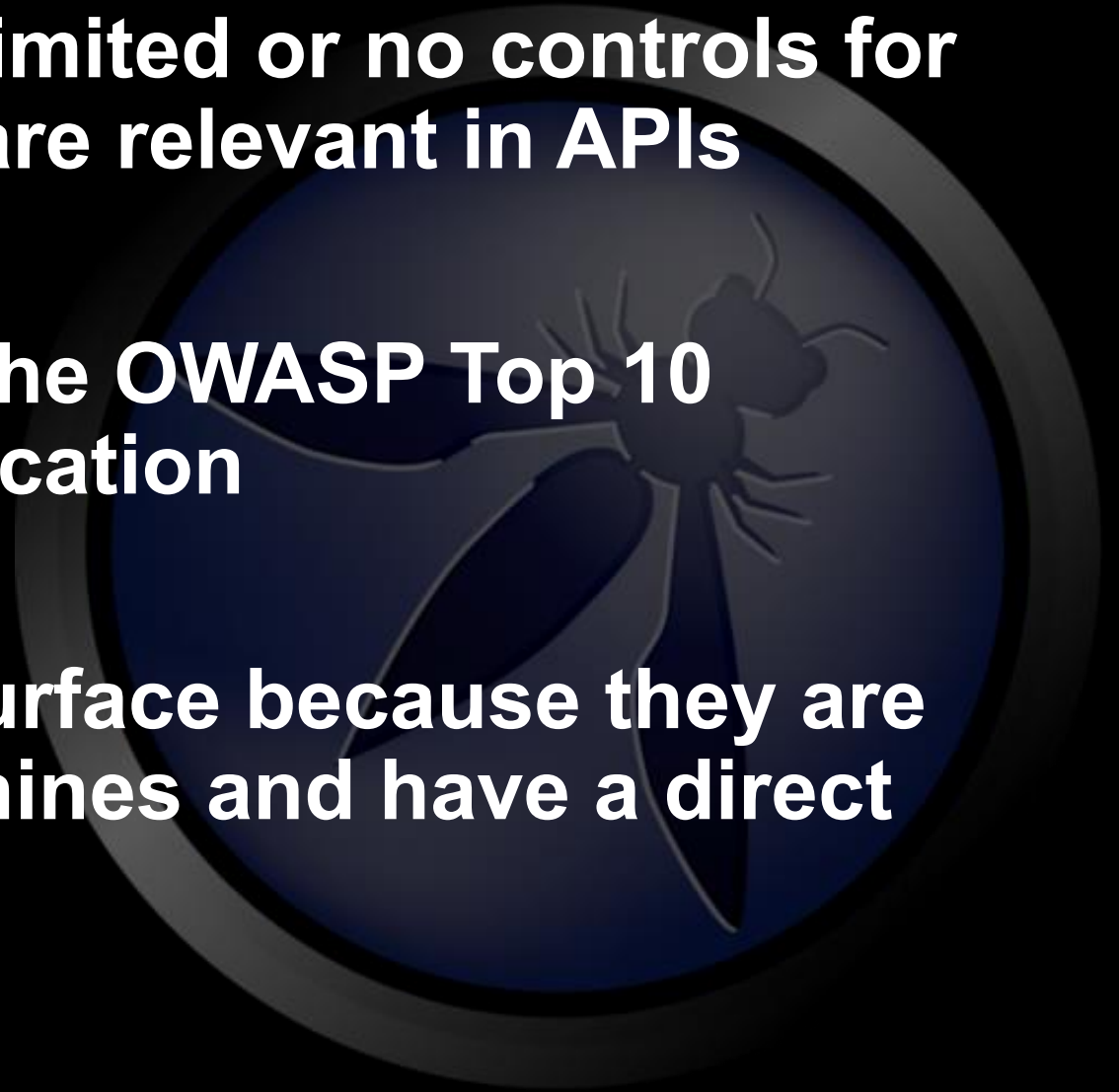
HEAD

- SPA/API Based App



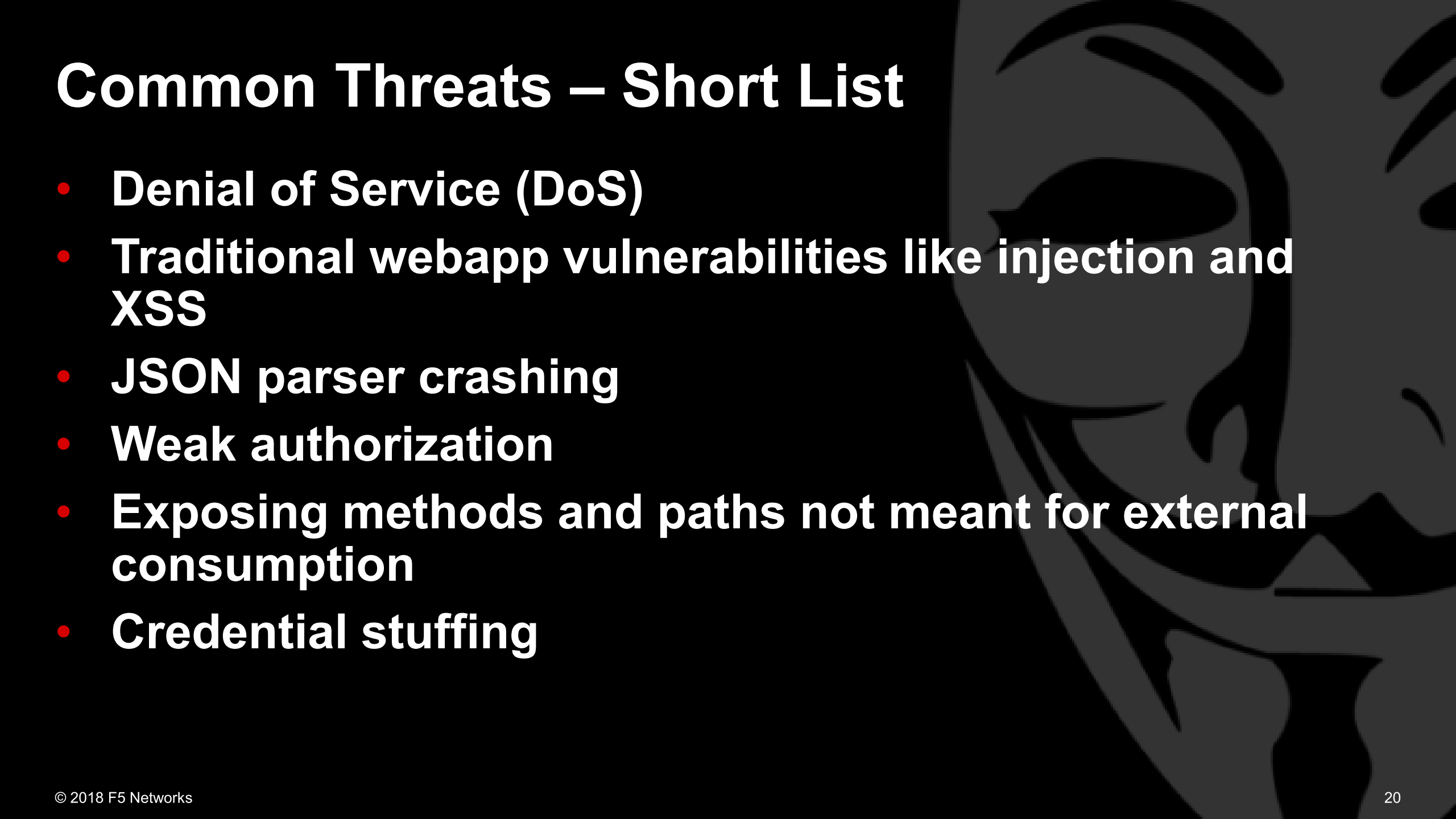
OWASP Top 10

- Most API Gateways provide limited or no controls for OWASP Top 10, all of which are relevant in APIs
- APIs are vulnerable to all of the OWASP Top 10 categories like any web application
- APIs are such a rich threat surface because they are designed to be used by machines and have a direct connection to the data



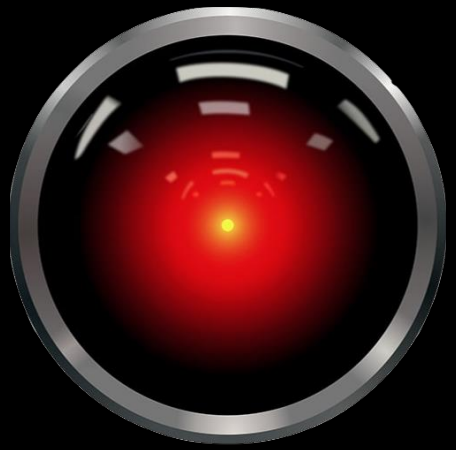
Common Threats – Short List

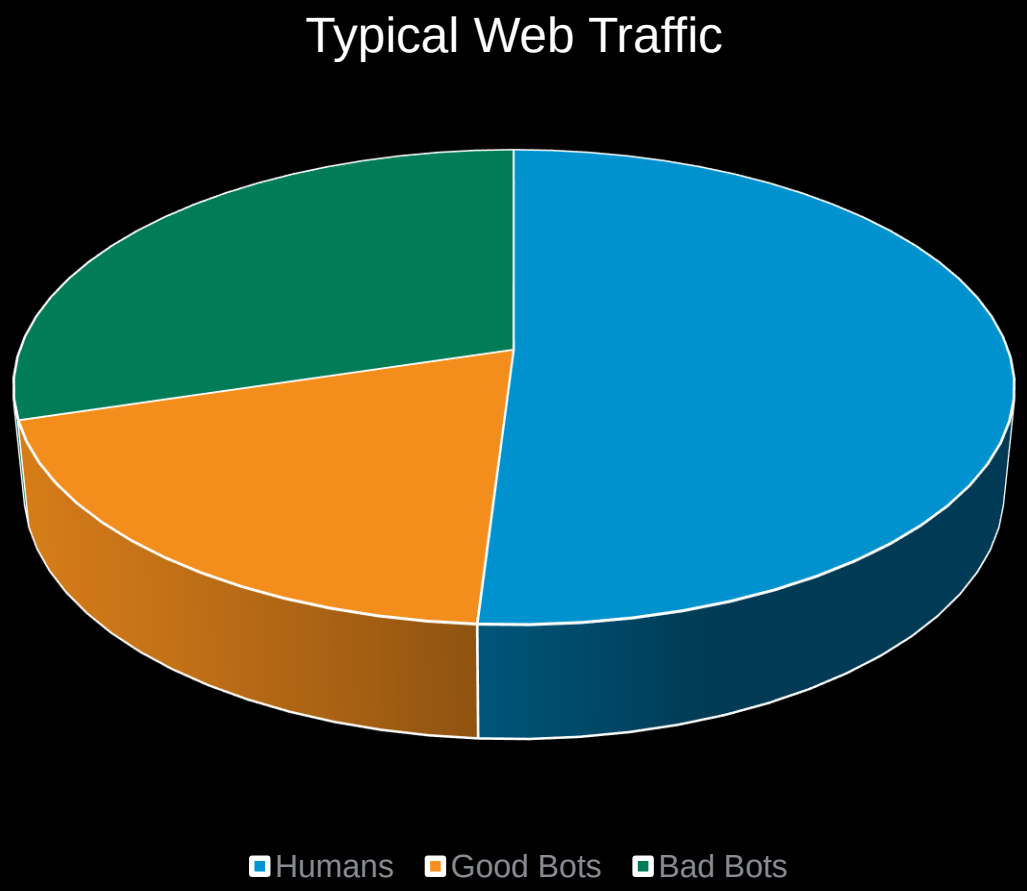
- Denial of Service (DoS)
- Traditional webapp vulnerabilities like injection and XSS
- JSON parser crashing
- Weak authorization
- Exposing methods and paths not meant for external consumption
- Credential stuffing



Automated Traffic Consumes 50% of Resources

- Roughly 50% of traffic is human
- About 20% is good bots
- Remaining 30% is malicious bots





https://www.incapsula.com/blog/bot-traffic-report-2015.html

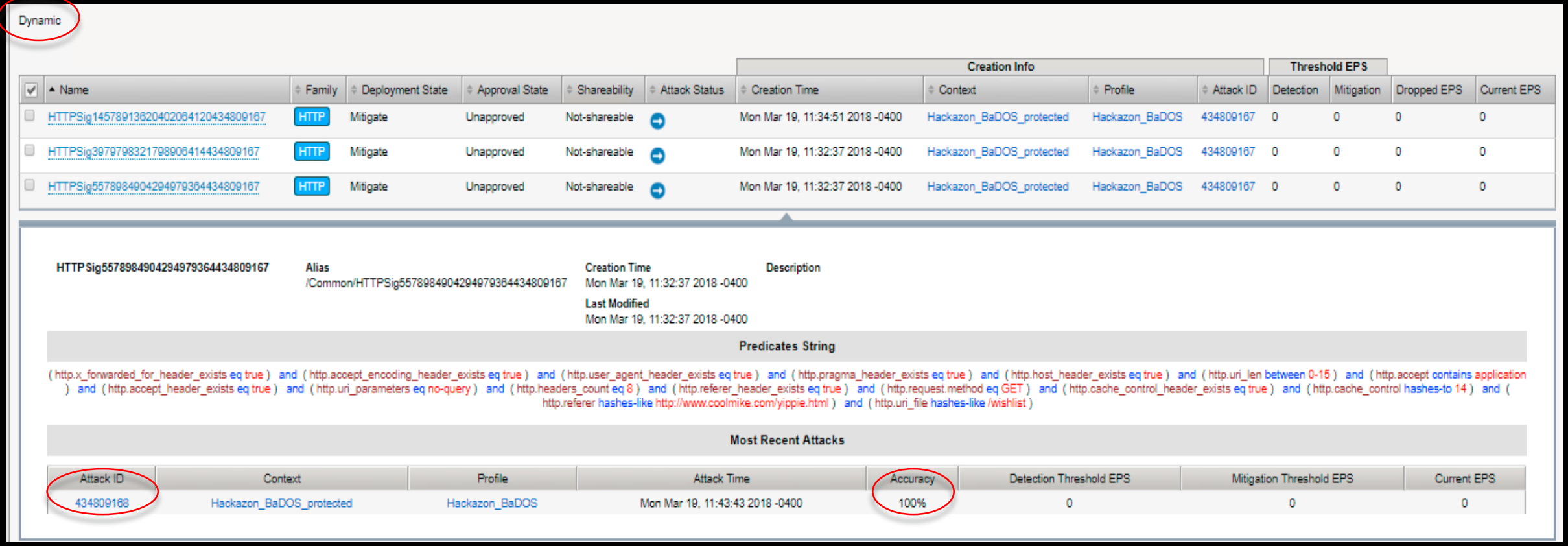
OWASP Top 20 Automated Threats

- OAT-020 Account Aggregation
- OAT-019 Account Creation
- OAT-003 Ad Fraud
- OAT-009 CAPTCHA Defeat
- OAT-010 Card Cracking
- OAT-001 Carding
- OAT-012 Cashing Out
- OAT-007 Credential Cracking
- OAT-008 Credential Stuffing
- OAT-021 Denial of Inventory
- OAT-015 Denial of Service
- OAT-006 Expediting
- OAT-004 Fingerprinting
- OAT-018 Footprinting
- OAT-005 Scalping
- OAT-011 Scraping
- OAT-016 Skewing
- OAT-013 Sniping
- OAT-017 Spamming
- OAT-002 Token Cracking
- OAT-014 Vulnerability Scanning

Threats and Protections

DDoS Attacks

DDoS Mitigation

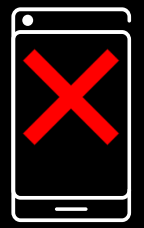


Antibot Mobile SDK

Bot Protection on Mobile?

- **F5 WAF relies on JavaScript for Proactive Bot Defense**

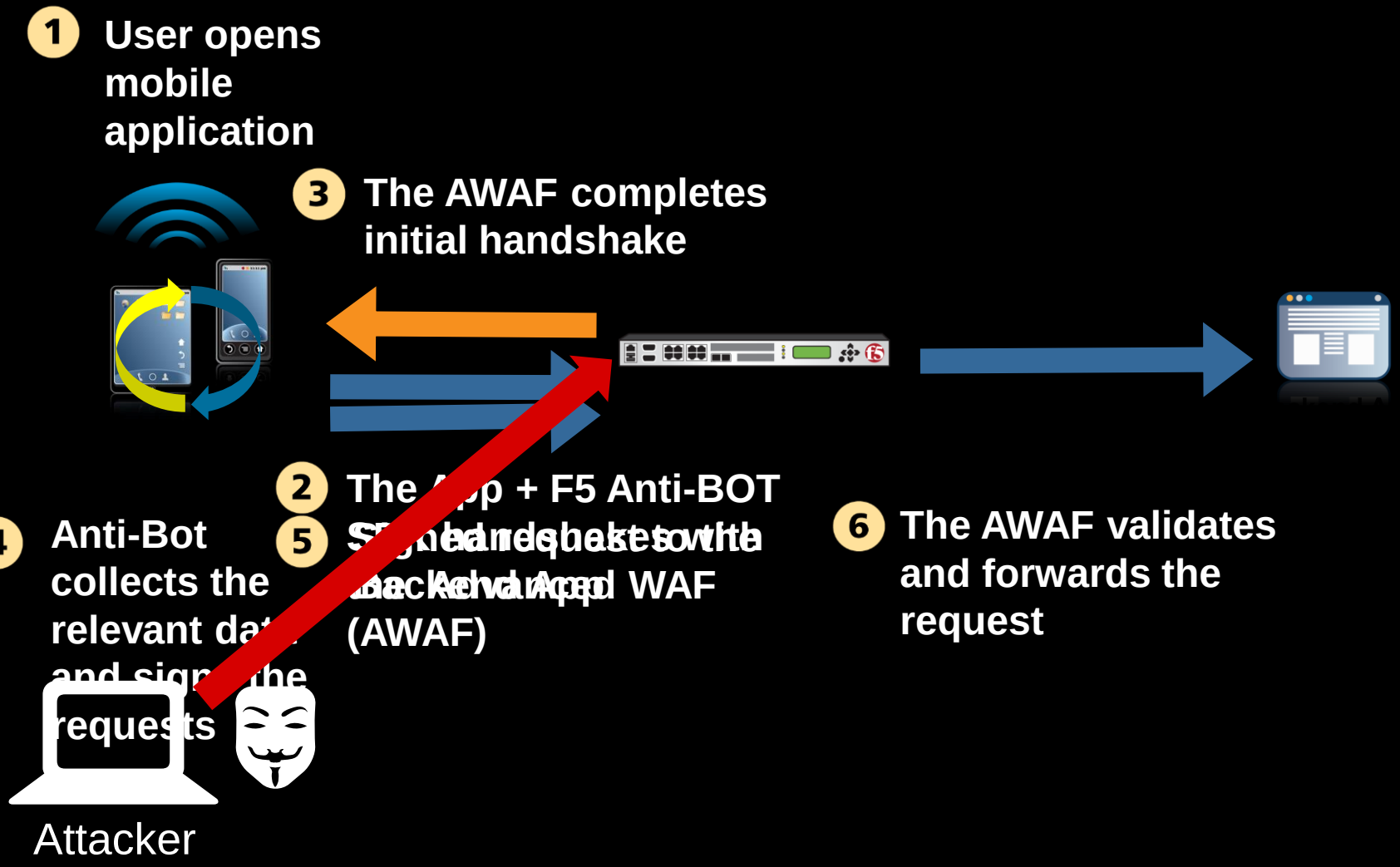
[Web]



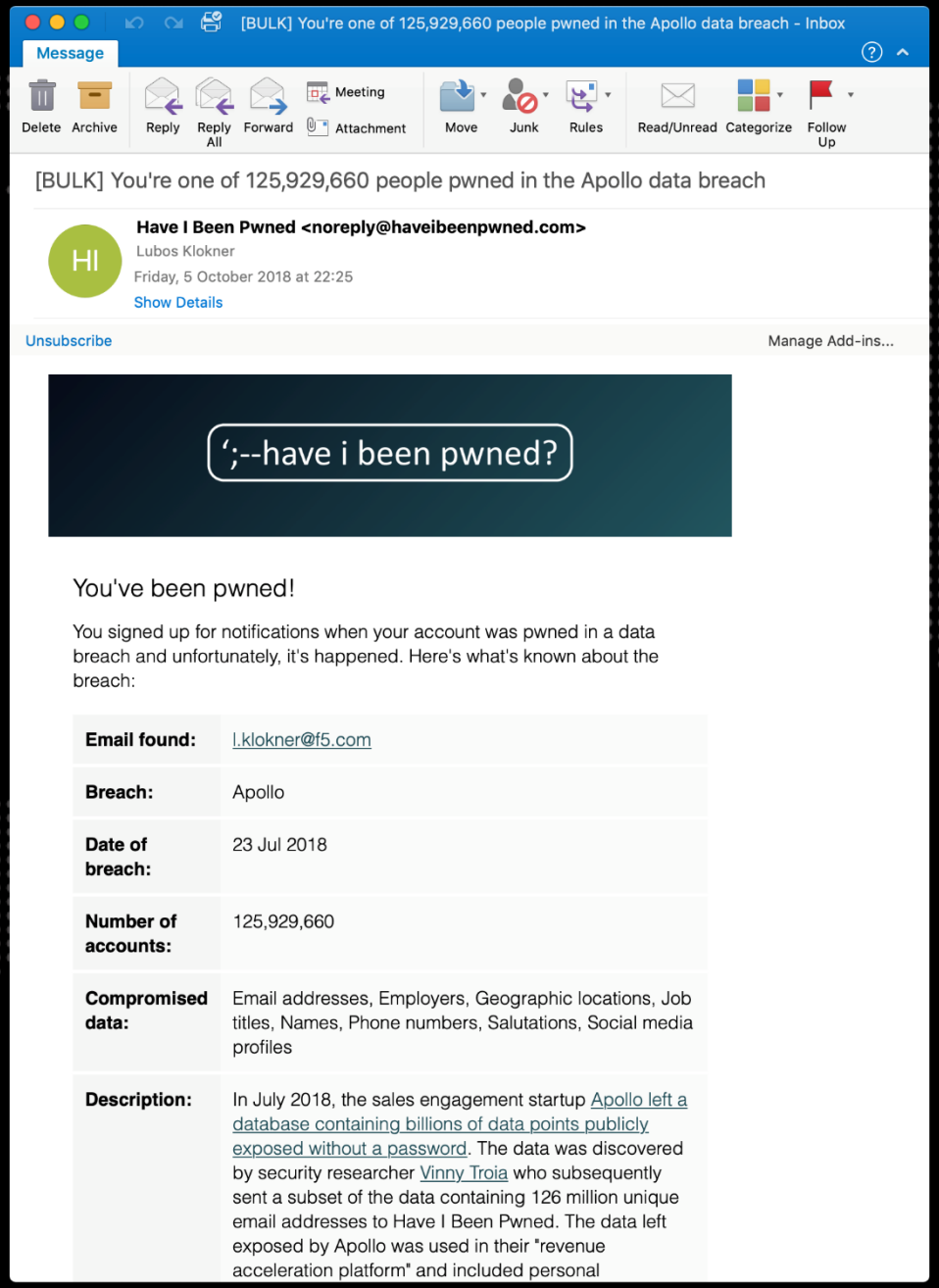
[Native]

- **Solution**
- Replicate JS functionality in an SDK that can be easily integrated into the native mobile app

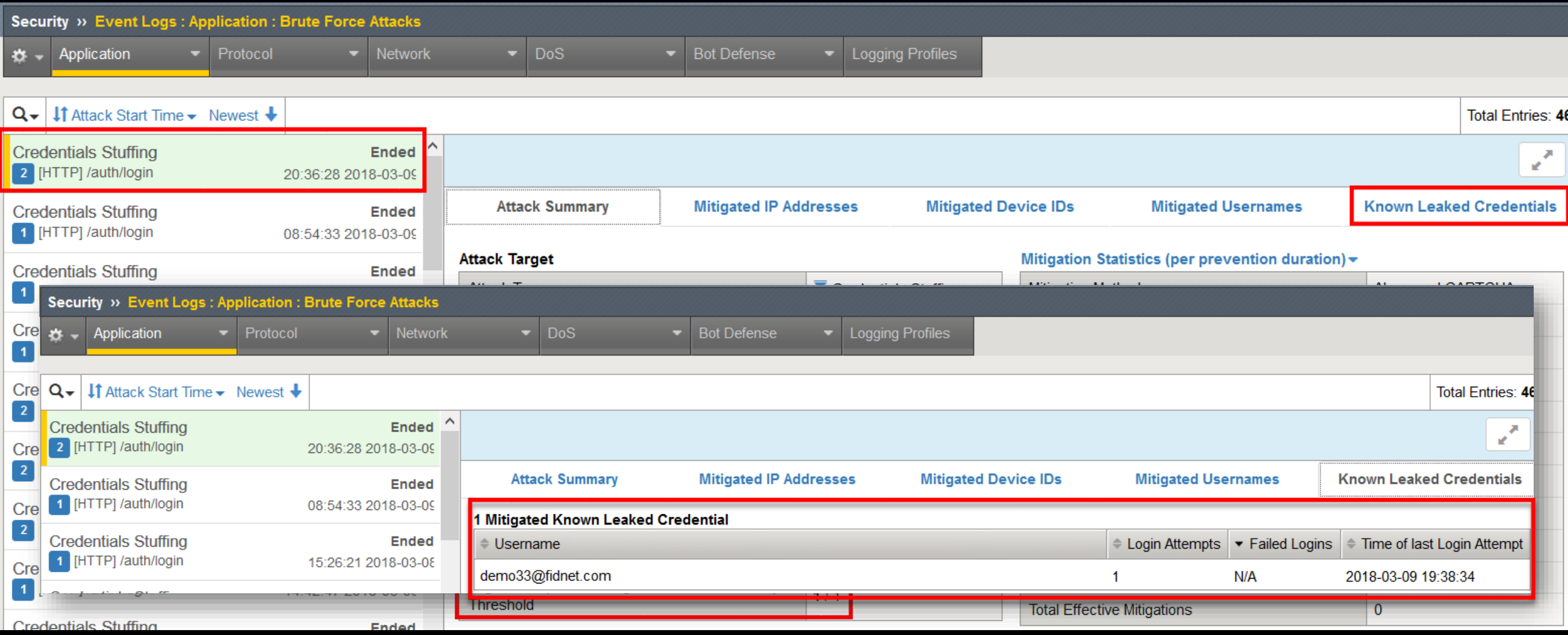
How Anti-Bot Works – High level



Credentials Stuffing

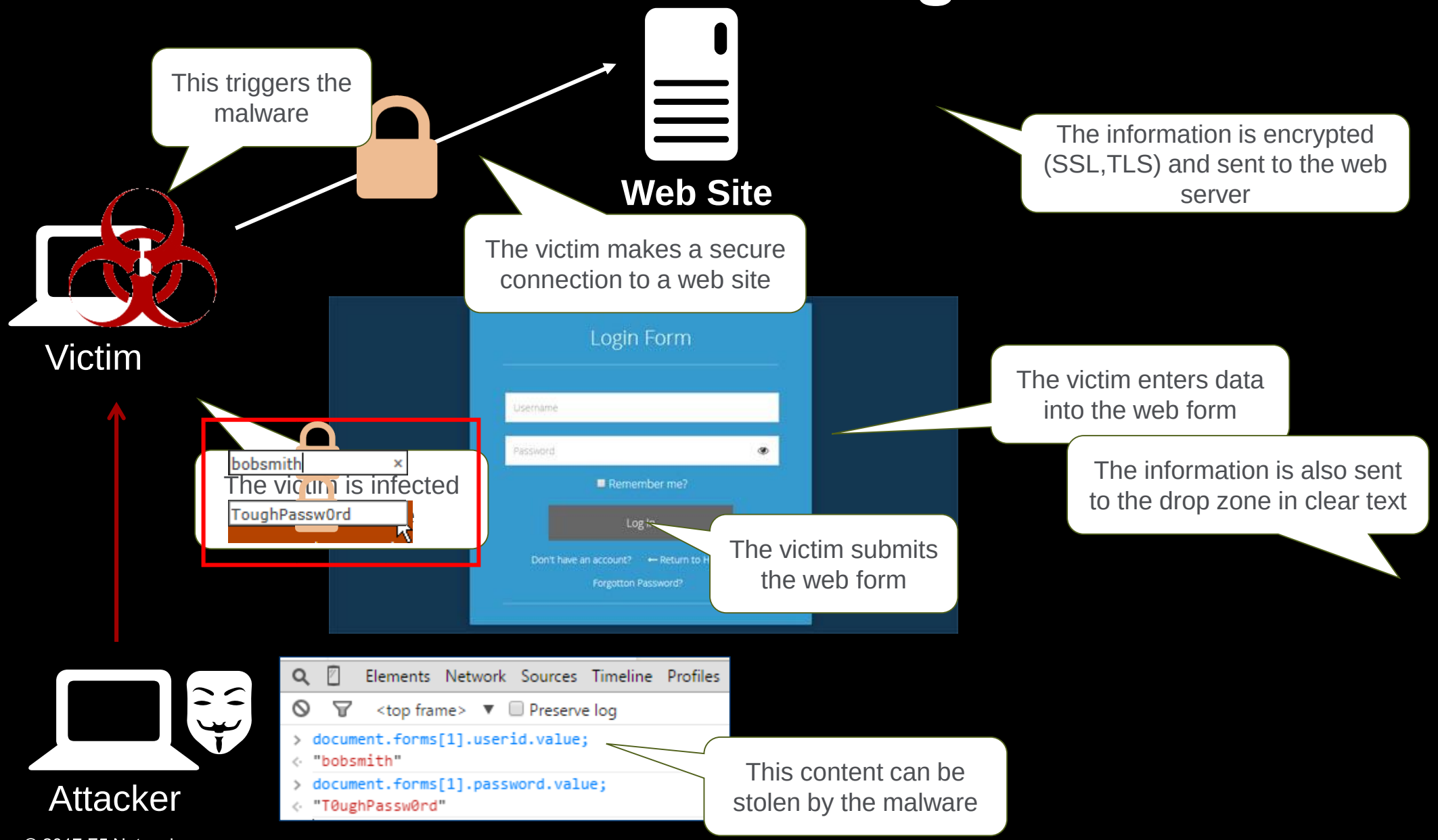


Credential Stuffing - Mitigation

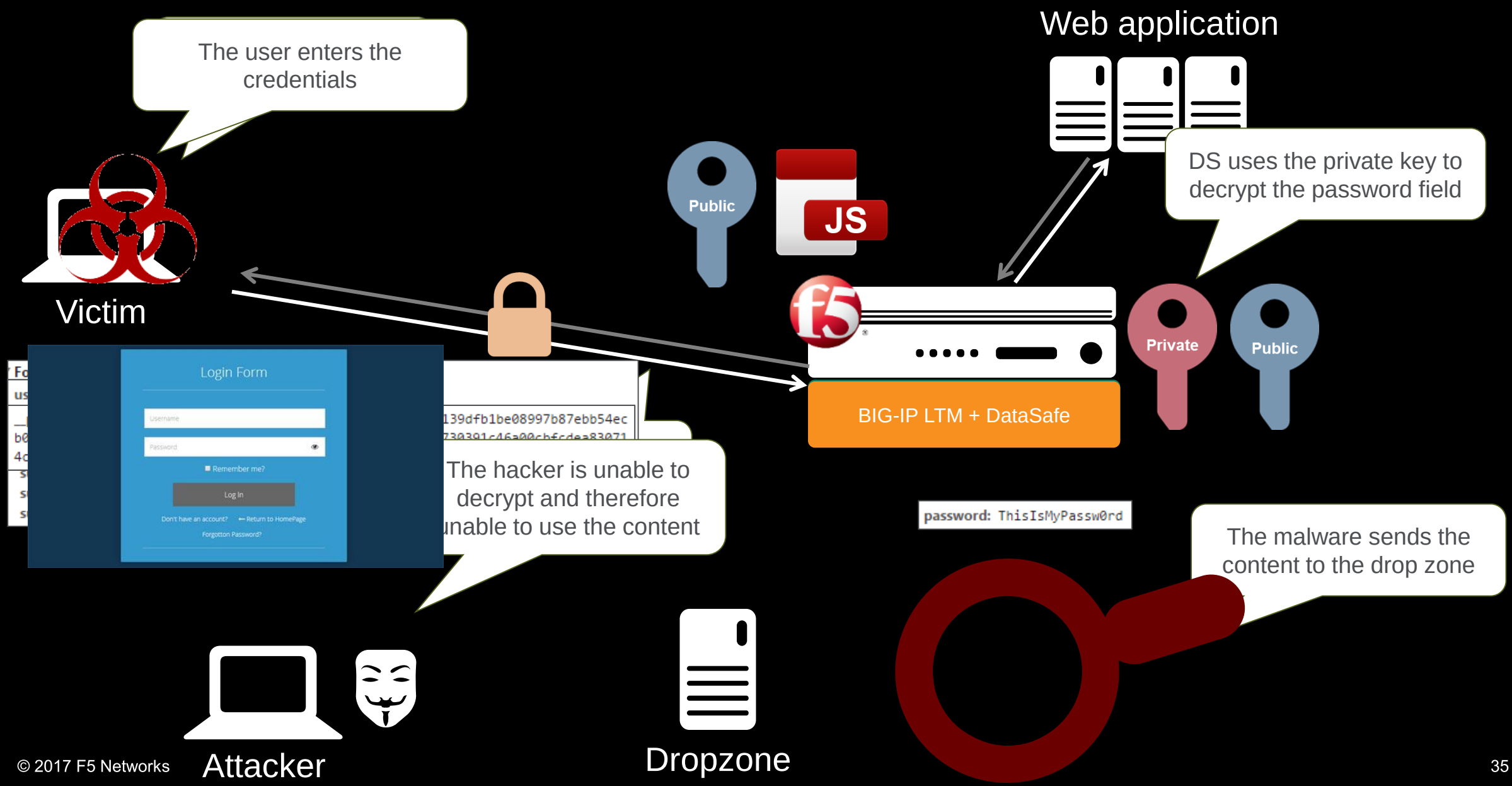


DataSafe

Credential / Form Grabbing



How DataSafe Uses App Layer Encryption to Protect Confidential Data



SOLUTIONS FOR AN APPLICATION WORLD