



Sustainable WebApp Security

PRESENTED BY:

Luboš Klokner | F5 Networks | Sr. Systems Engineer

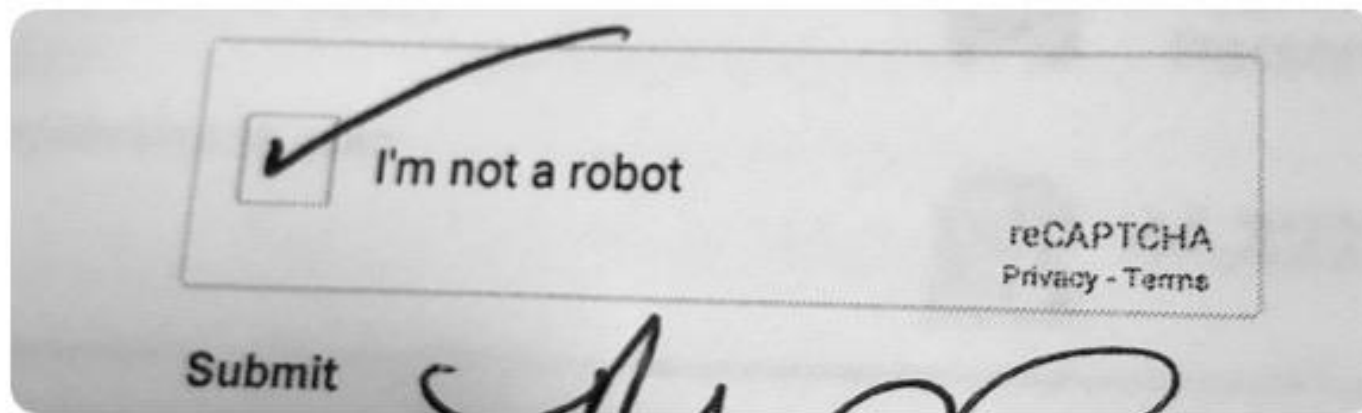
lubos@f5.com | +421 908 755152 | @lklokner



Marci Robin @MarciRobin

3d 

I bought a car today, and the dealership had me check off — with a pen, on paper — that I'm not a robot.





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.

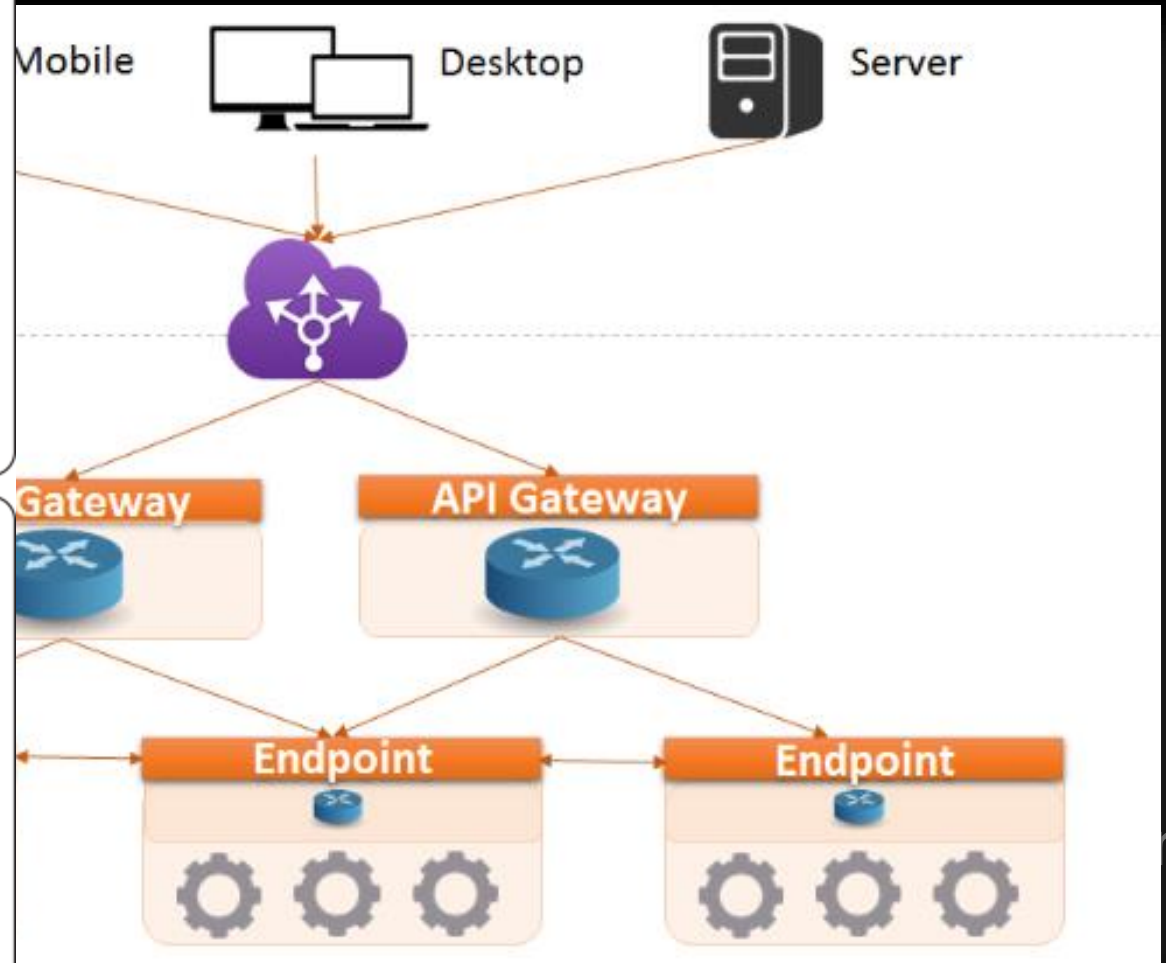
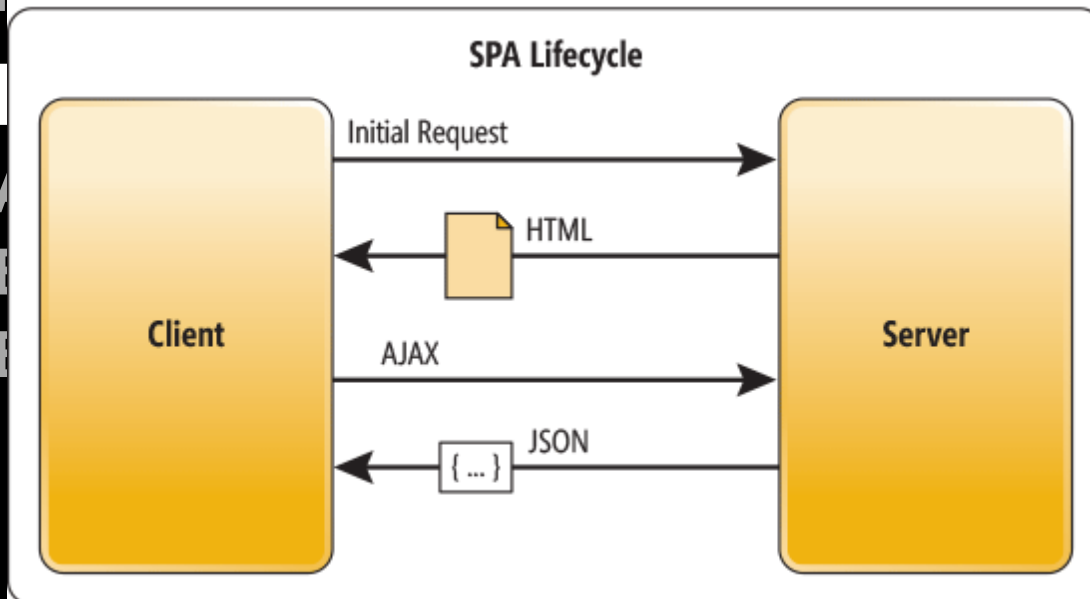
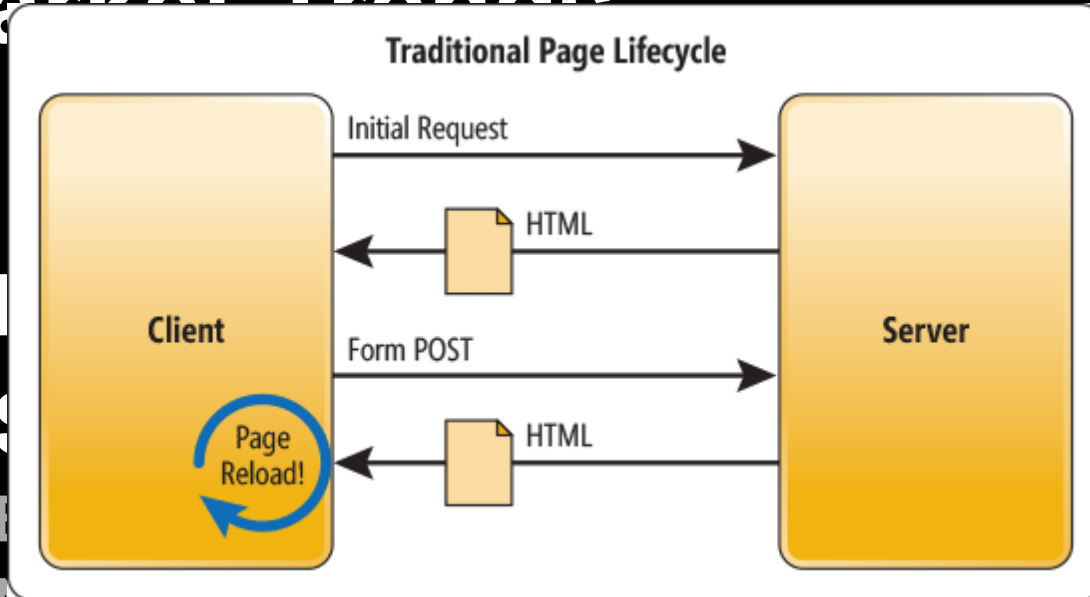
(But only if you focus on the apps)

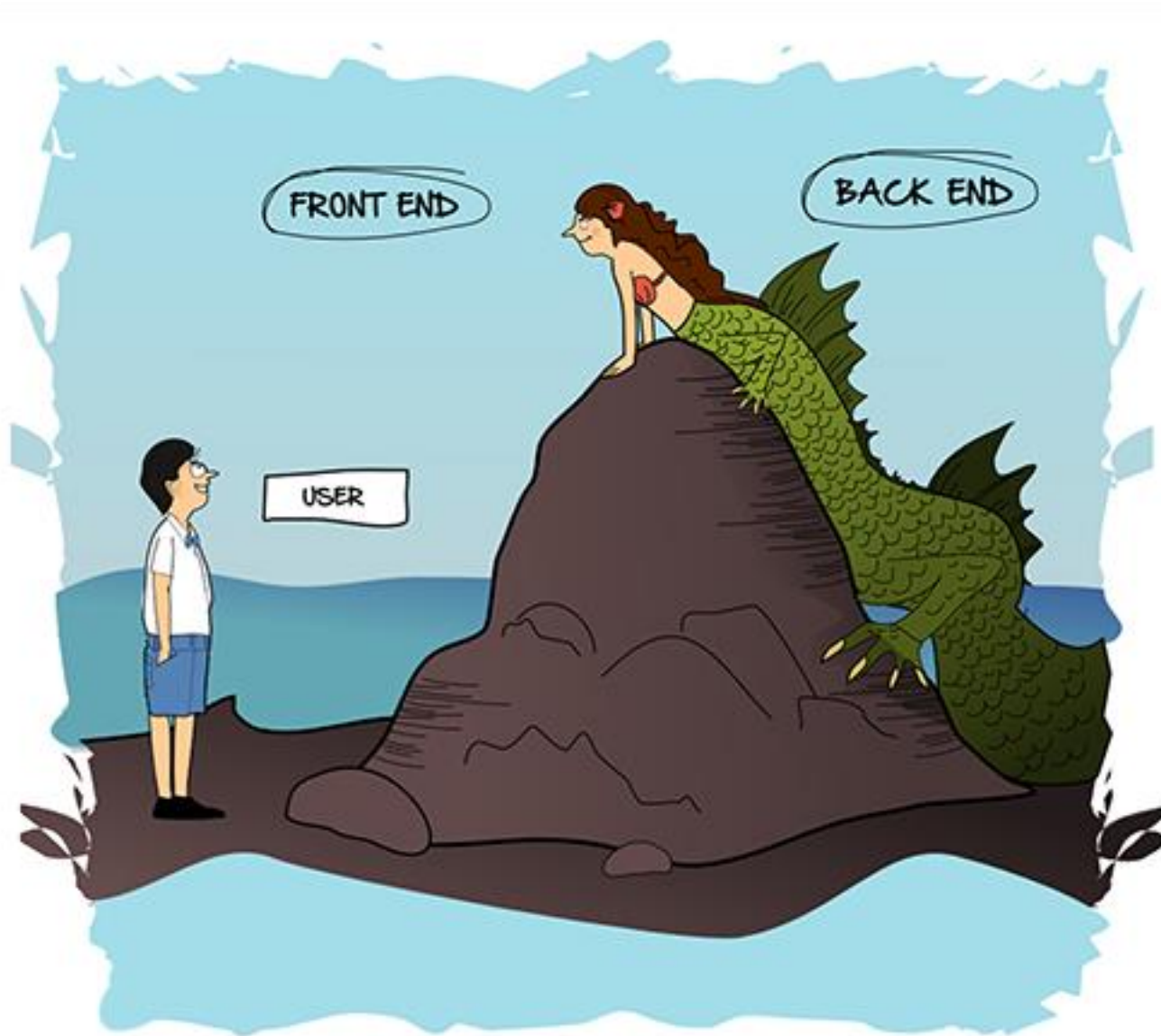
Modern Web Application



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

Market Trends





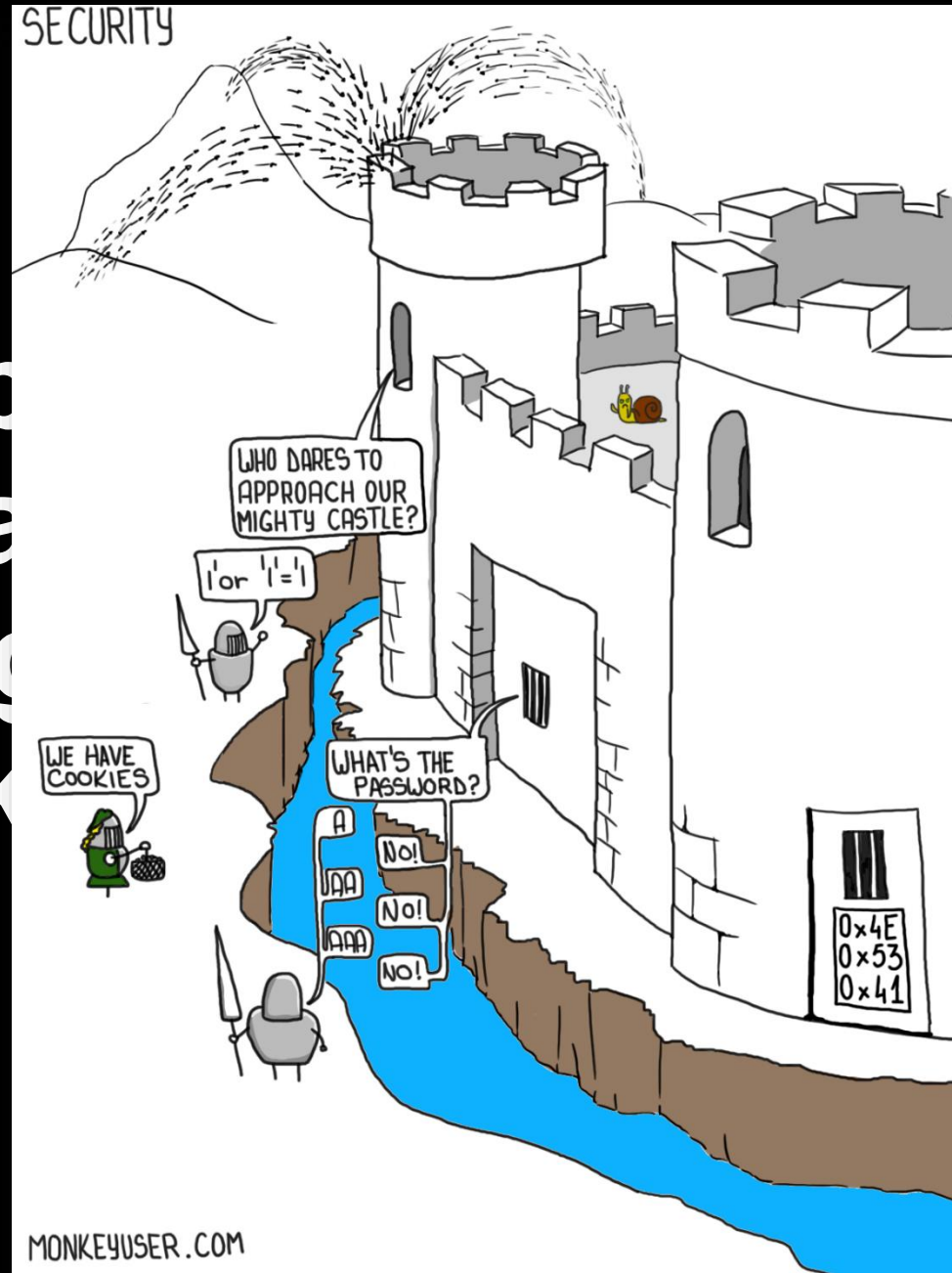
Front end vs. Back end.

Source: comic.browserling.com

Threats and Protections



“...a web
single pa
providing
to a desk



its on a
of
ce similar

Vectors of Attack

- Traditional Web Page

GET
POST
HEAD

- SPA/API Based App

POST <https://All.Your.Base.Are.Belong.To.us/api/v1/applications/>

GET
POST
PUT
PATCH
DELETE
COPY
HEAD
OPTIONS
LINK
UNLINK
PURGE
LOCK
UNLOCK
PROPFIND
VIEW

Headers (2) Body Pre-request Script Tests

	VALUE
	application/x-www-form-urlencoded
	rbpmobileand/1.2.3
	Value

Hit the Send button to get

OWASP Top 10

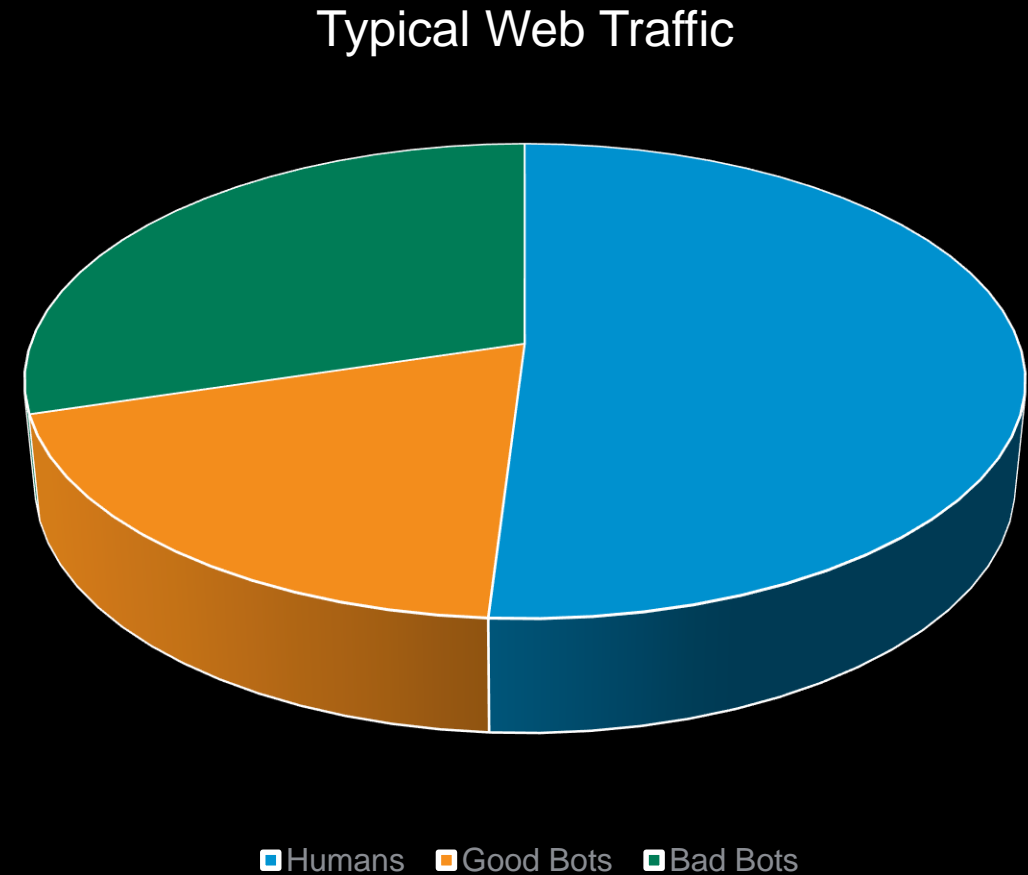
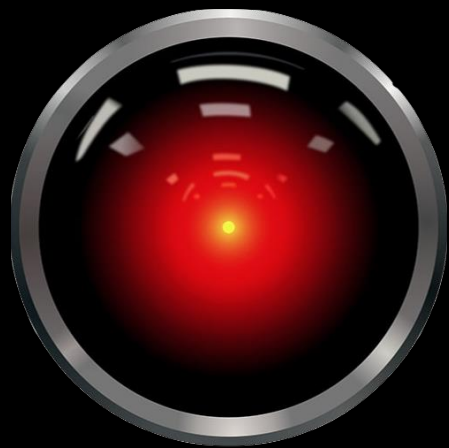
- **Most API Gateways provide limited or no controls for OWASP Top 10, all of which are relevant in APIs**
- **APIs are vulnerable to all of the OWASP Top 10 categories like any web application**
- **APIs are such a rich threat surface because they are designed to be used by machines and have a direct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



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**





Zone Kaiwei Ni factory
Sponsored

80% OFF
BLACK FRIDAY SALE



Shop Now

DDoS Attacks



DDoS Mitigation

Dynamic

Name	Family	Deployment State	Approval State	Shareability	Attack Status	Creation Info				Threshold EPS			
						Creation Time	Context	Profile	Attack ID	Detection	Mitigation	Dropped EPS	Current EPS
HTTPSig14578913620402064120434809167	HTTP	Mitigate	Unapproved	Not-shareable	→	Mon Mar 19, 11:34:51 2018 -0400	Hackazon_BaDOS_protected	Hackazon_BaDOS	434809167	0	0	0	0
HTTPSig3979798321798906414434809167	HTTP	Mitigate	Unapproved	Not-shareable	→	Mon Mar 19, 11:32:37 2018 -0400	Hackazon_BaDOS_protected	Hackazon_BaDOS	434809167	0	0	0	0
HTTPSig5578984904294979364434809167	HTTP	Mitigate	Unapproved	Not-shareable	→	Mon Mar 19, 11:32:37 2018 -0400	Hackazon_BaDOS_protected	Hackazon_BaDOS	434809167	0	0	0	0

HTTP Sig5578984904294979364434809167

Alias: /Common/HTTPSig5578984904294979364434809167
Creation Time: Mon Mar 19, 11:32:37 2018 -0400
Description:
Last Modified: Mon Mar 19, 11:32:37 2018 -0400

Predicates String

```
( http.x_forwarded_for_header_exists eq true ) and ( http.accept_encoding_header_exists eq true ) and ( http.user_agent_header_exists eq true ) and ( http.pragma_header_exists eq true ) and ( http.host_header_exists eq true ) and ( http.uri_len between 0-15 ) and ( http.accept contains application ) and ( http.accept_header_exists eq true ) and ( http.uri_parameters eq no-query ) and ( http.headers_count eq 8 ) and ( http.referer_header_exists eq true ) and ( http.request.method eq GET ) and ( http.cache_control_header_exists eq true ) and ( http.cache_control hashes-to 14 ) and ( http.referer hashes-like http://www.coolmike.com/yippie.html ) and ( http.uri_file hashes-like /wishlist )
```

Most Recent Attacks

Attack ID	Context	Profile	Attack Time	Accuracy	Detection Threshold EPS	Mitigation Threshold EPS	Current EPS
434809168	Hackazon_BaDOS_protected	Hackazon_BaDOS	Mon Mar 19, 11:43:43 2018 -0400	100%	0	0	0

Antibot Mobile SDK

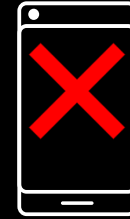


Bot Protection on Mobile?

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



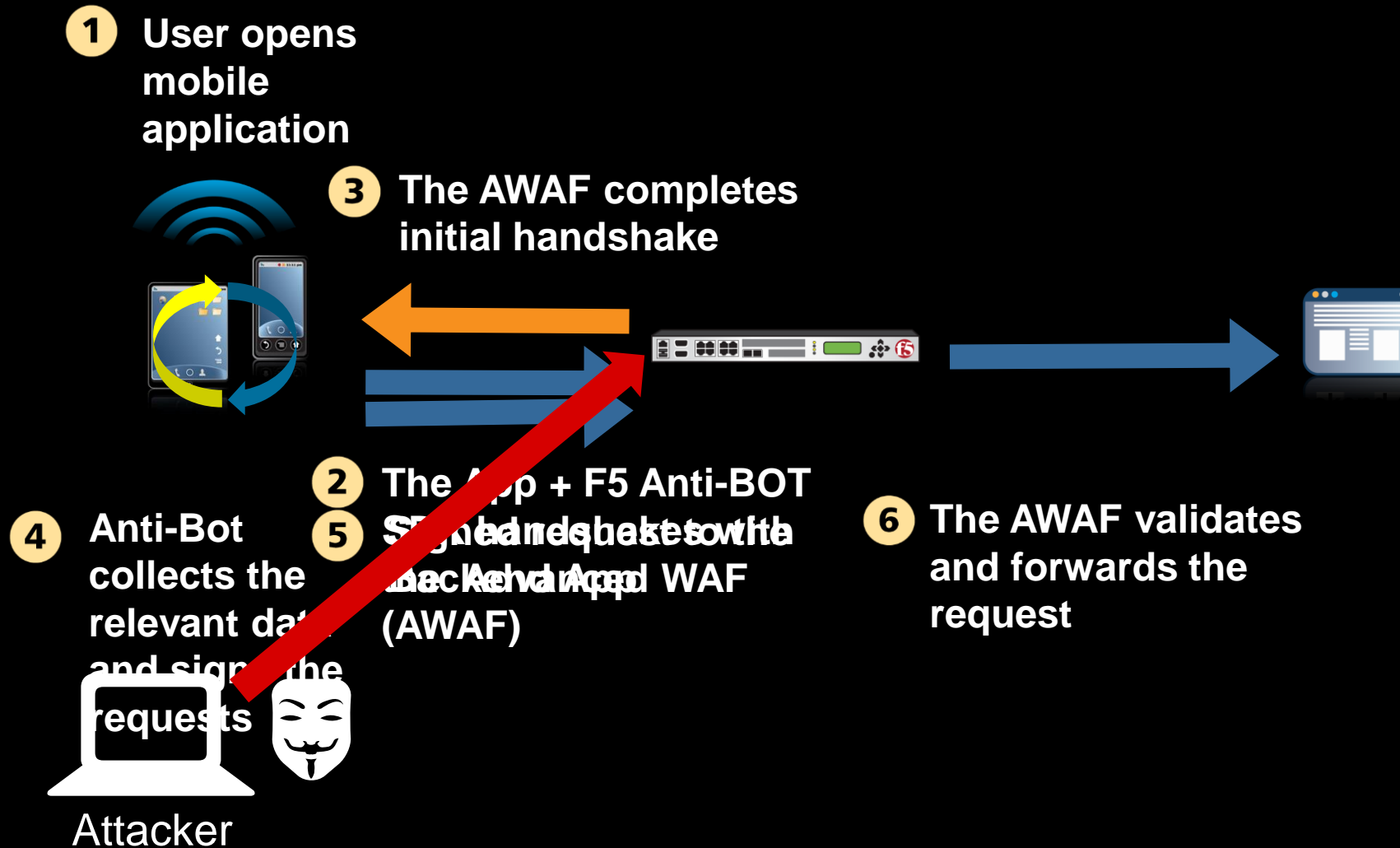
[Web]



[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



[BULK] You're one of 125,929,660 people pwned in the Apollo data breach - Inbox

Message

Delete Archive Reply Reply All Forward Attachment Meeting Move Junk Rules Read/Unread Categorize Follow Up

[BULK] You're one of 125,929,660 people pwned in the Apollo data breach

Have I Been Pwned <noreply@haveibeenpwned.com>
 Lubos Klokner
 Friday, 5 October 2018 at 22:25
[Show Details](#)

[Unsubscribe](#) [Manage Add-ins...](#)

';;--have i been pwned?'

You've been pwned!

You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Email found:	l.klokner@f5.com
Breach:	Apollo
Date of breach:	23 Jul 2018
Number of accounts:	125,929,660
Compromised data:	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles
Description:	In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password . The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal



Credential Stuffing - Mitigation

Security » Event Logs : Application : Brute Force Attacks

Application Protocol Network DoS Bot Defense Logging Profiles

Attack Start Time Newest Total Entries: 46

Attack ID	Attack Name	Status	Start Time	End Time	Attack Target	Mitigation Statistics (per prevention duration)
2	Credentials Stuffing [HTTP] /auth/login	Ended	20:36:28	2018-03-09		
1	Credentials Stuffing [HTTP] /auth/login	Ended	08:54:33	2018-03-09		
1	Credentials Stuffing [HTTP] /auth/login	Ended	08:54:33	2018-03-09		
2	Credentials Stuffing [HTTP] /auth/login	Ended	15:26:21	2018-03-09		
1	Credentials Stuffing [HTTP] /auth/login	Ended	15:26:21	2018-03-09		

Attack Summary Mitigated IP Addresses Mitigated Device IDs Mitigated Usernames **Known Leaked Credentials**

Attack Target Mitigation Statistics (per prevention duration)

Security » Event Logs : Application : Brute Force Attacks

Application Protocol Network DoS Bot Defense Logging Profiles

Attack Start Time Newest Total Entries: 46

Attack ID	Attack Name	Status	Start Time	End Time	Attack Target	Mitigation Statistics (per prevention duration)
2	Credentials Stuffing [HTTP] /auth/login	Ended	20:36:28	2018-03-09		
2	Credentials Stuffing [HTTP] /auth/login	Ended	08:54:33	2018-03-09		
2	Credentials Stuffing [HTTP] /auth/login	Ended	08:54:33	2018-03-09		
2	Credentials Stuffing [HTTP] /auth/login	Ended	15:26:21	2018-03-09		
1	Credentials Stuffing [HTTP] /auth/login	Ended	15:26:21	2018-03-09		

Attack Summary Mitigated IP Addresses Mitigated Device IDs Mitigated Usernames **Known Leaked Credentials**

1 Mitigated Known Leaked Credential

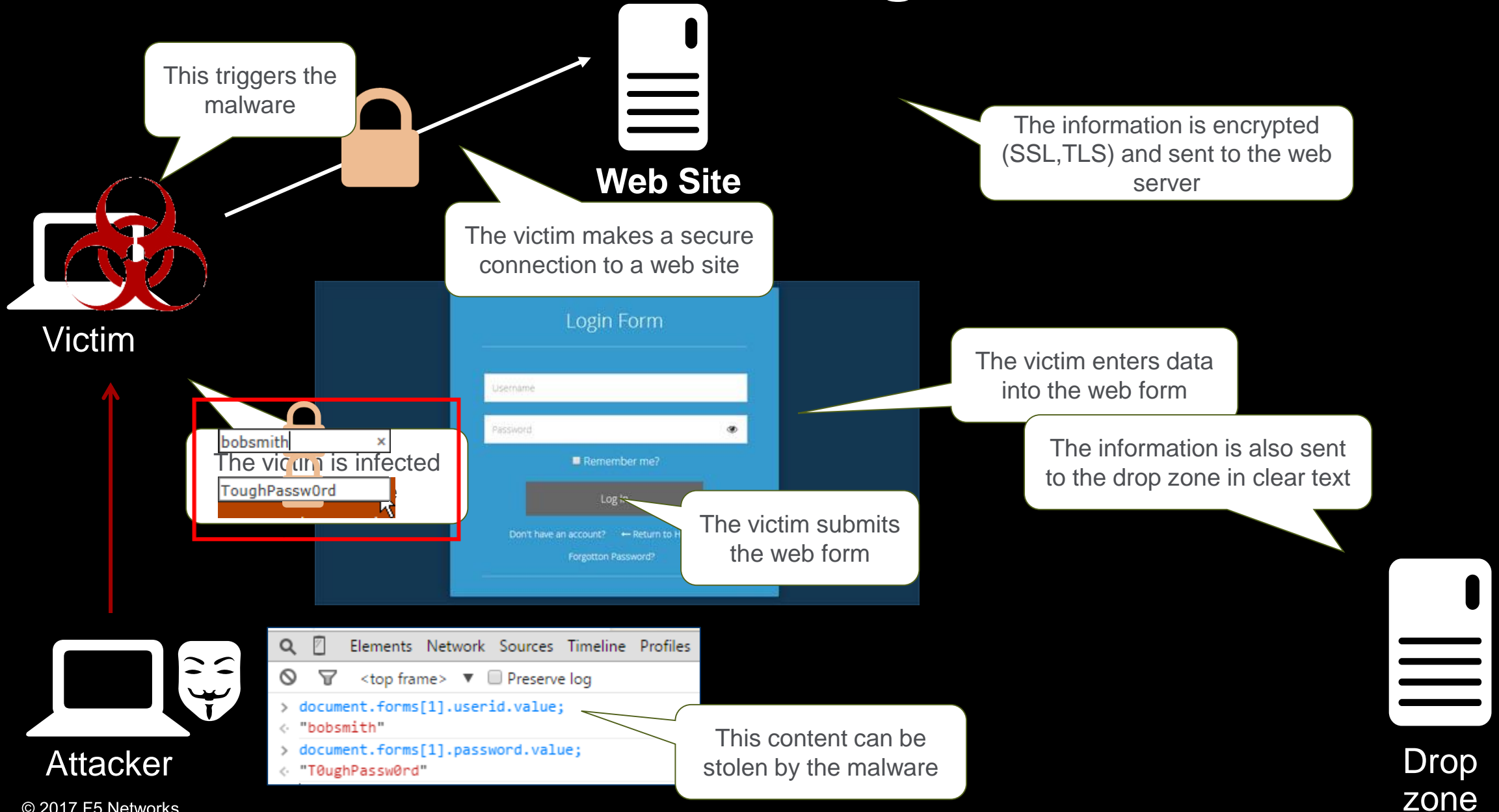
Username	Login Attempts	Failed Logins	Time of last Login Attempt
demo33@fidnet.com	1	N/A	2018-03-09 19:38:34

Threshold Total Effective Mitigations 0

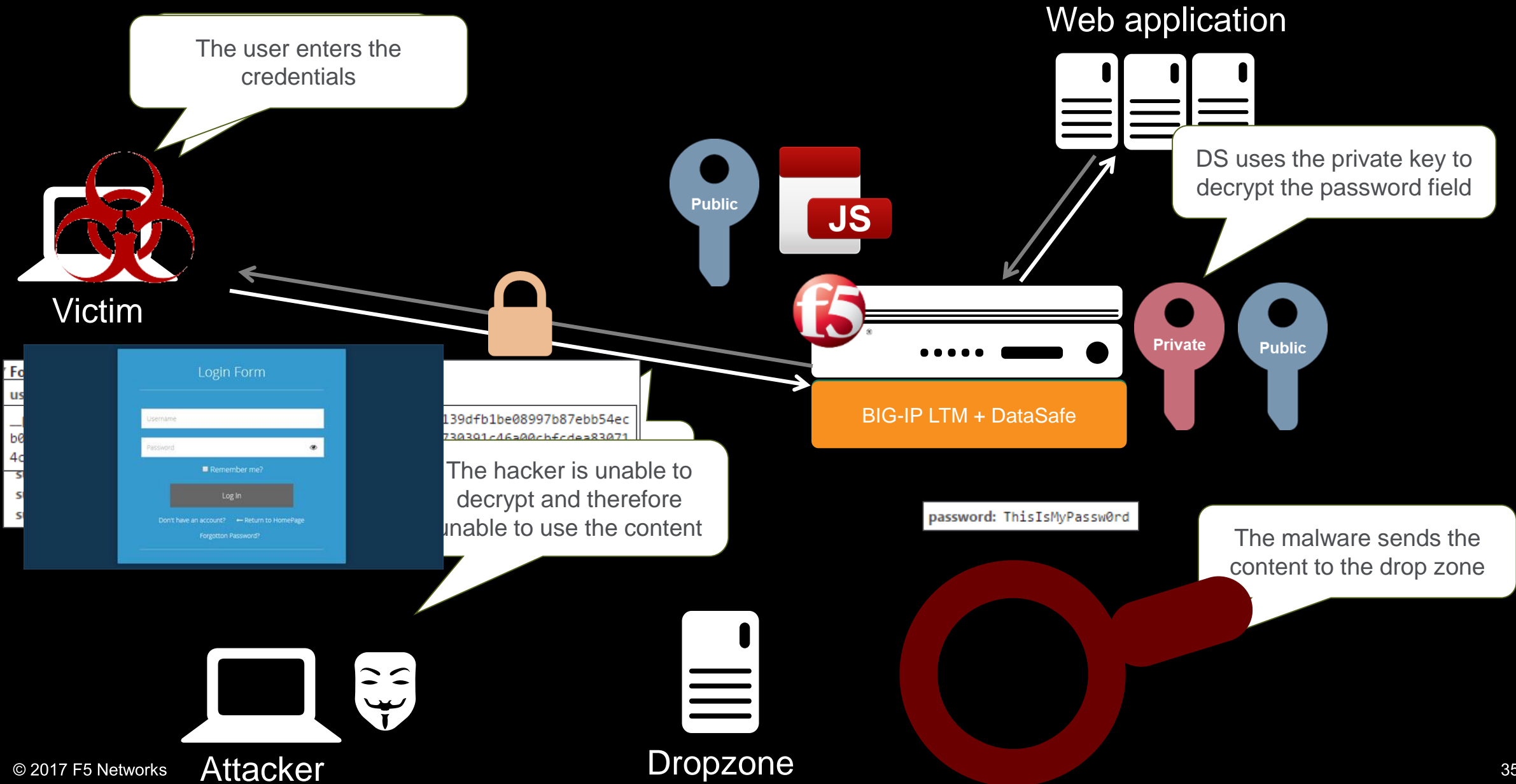
DataSafe



Credential / Form Grabbing



How DataSafe Uses App Layer Encryption to Protect Confidential Data





SOLUTIONS FOR AN APPLICATION WORLD