# Advanced WAF para amenazas avanzadas

Carlos Valencia – Sr Systems Engineer

# Do you…

…have a public facing web property?

…have a high-sensitivity web property?

…contend with bots and unwanted automation?

…have compliance obligations?

…have difficult to upgrade software stacks?

…have legacy web applications?

…need zero day breathing room?

…want to reduce your development time-to-market?

If you answered YES
to any of the above…

**WAF
might be for
you!**

# Security Policy vs. Security Reality

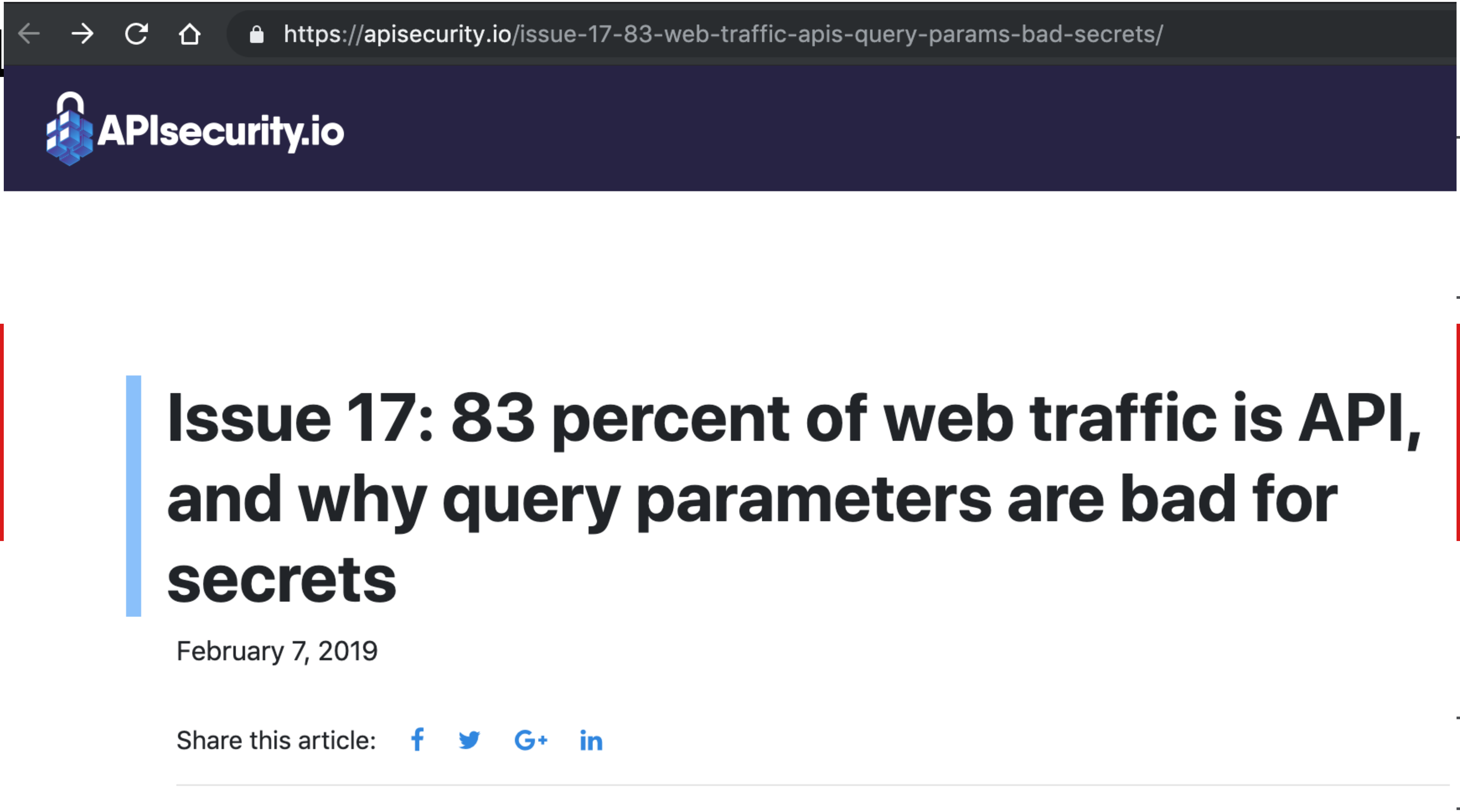
## Is security policy being enforced? Is it enforceable?

- What you bargained for isn't always what you get.

# Security Policy vs. Security Reality

## Is security policy being enforced? Is it enforceable?

- **What you bargained for isn't always what you get.**
- **Delivered state will likely deteriorate over time.**
  - Things change
  - Security controls often fall victim to troubleshooting as a necessity

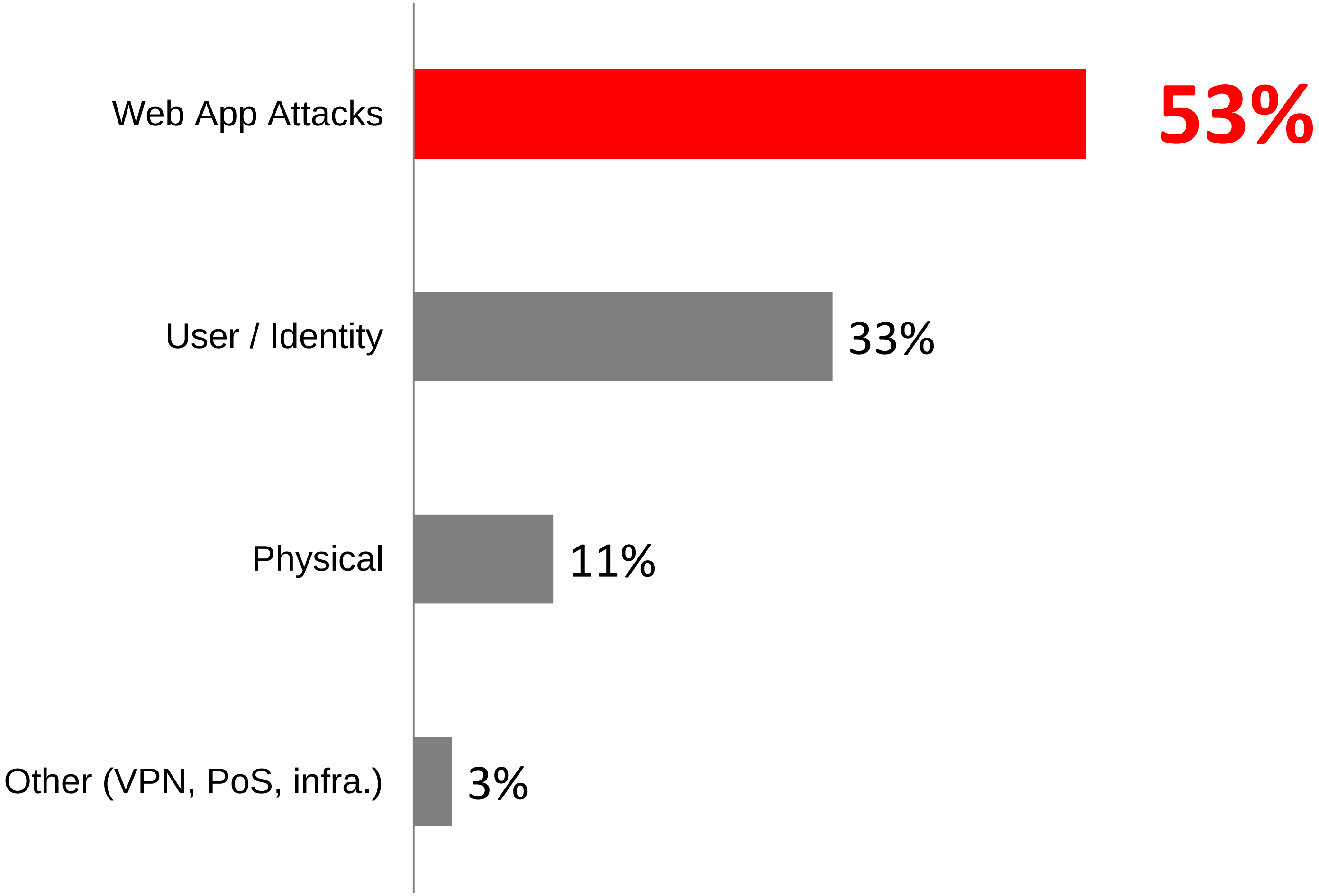


https://apisecurity.io/issue-17-83-web-traffic-apis-query-params-bad-secrets/

# Issue 17: 83 percent of web traffic is API, and why query parameters are bad for secrets

February 7, 2019

# Web App Attacks Are the #1 Single Source Entry Point of Successful Data Breaches…



# Traditional WAF Protections

## Traditional WAF

**OWASP Top 10** ▸ Protections against well known attack vectors

**Regulatory Compliance** ▸ Provides coverage as a compensating control

**Blacklisting** ▸ Filtering of known bad requests (signatures)

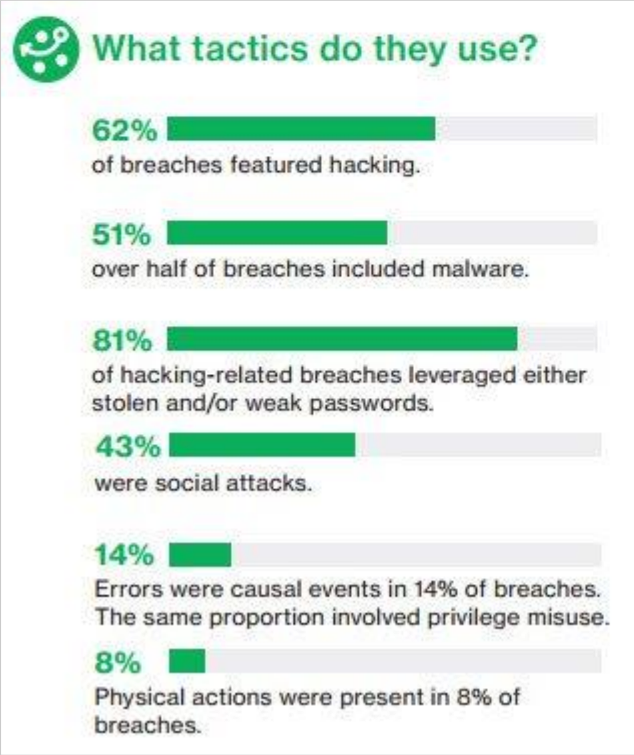
Does not take into account evolving attack vectors

(L7 DDoS, Intellectual Property Theft, Bot Fraud, etc.)

# F5 Advanced WAF Solution

# Password-Stealing Malware is a Key Tool for Cybercriminals

Figu



## What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

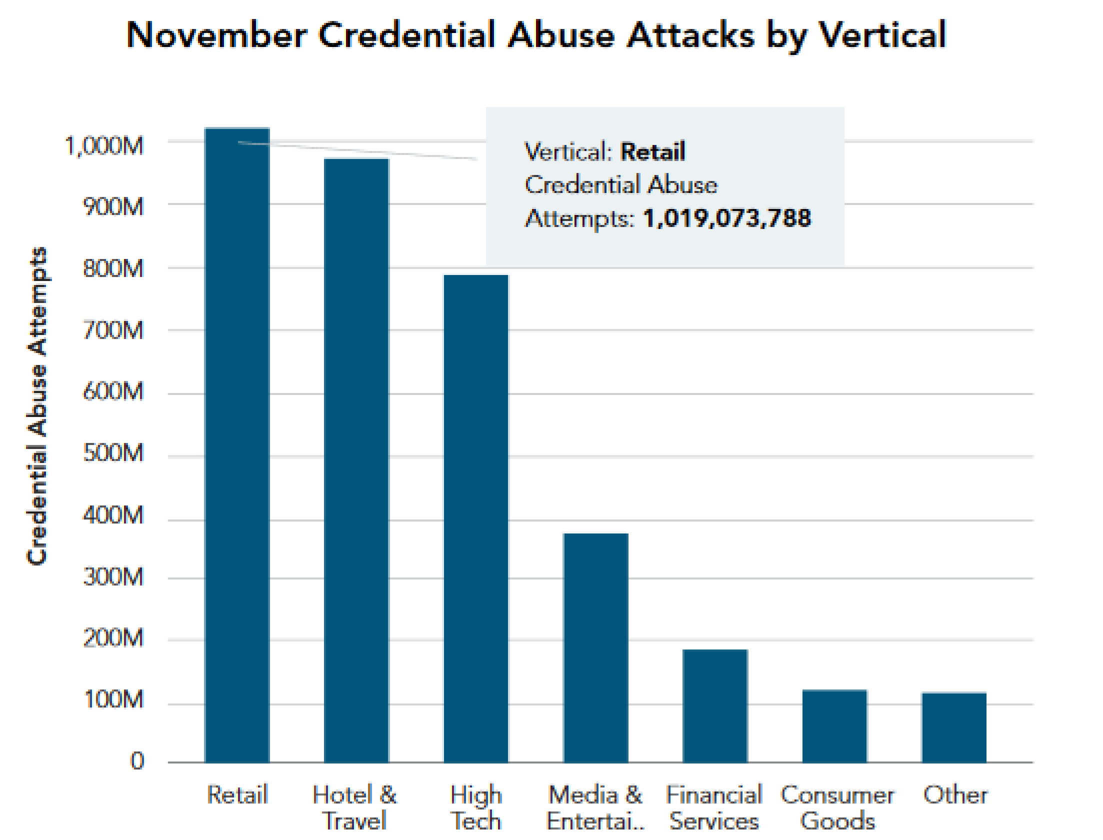


Figure 4-3: The retail vertical tops the chart with over a billion credential abuse attempts

**McAfee Labs Threats Report**
June 2017

This report was researched and written by:

Christiaan Beek
Diwakar Dinkar
Yashashree Gund
German Lancioni
Niamh Minihane
Francisca Moreno

Malware evasion tec

Hiding in plain sight: of steganography

The growing danger

Threats Statistics 69

ls

of stealing 26K

curity

ws Talks Academic About Me

## Vector

ities. We employ antivirus software to detect malware that exploits vulnerabilities. We have automatic patching systems to fix vulnerabilities. We debate whether the FBI should be permitted to introduce vulnerabilities in our software so it can get access to systems with a warrant. This is all important, but what's missing is a recognition that software vulnerabilities aren't the most common attack vector: credential stealing is.

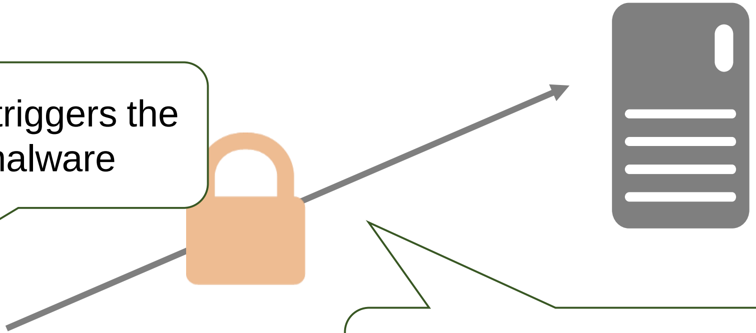
# How do we stop this?

- #1 is Protect Passwords
- F5 DataSafe application layer encryption

- #2 is Protect the Web Application
- Brute Force Login Protection, IP Intelligence and Anti-Bot Mobile SDK
- Credential Stuffing Subscription, Threat Campaigns and Centralized DeviceID

- #3 is Properly Managing Access
- Use APM for MFA and Federation

# What is Credential / Form Grabbing?

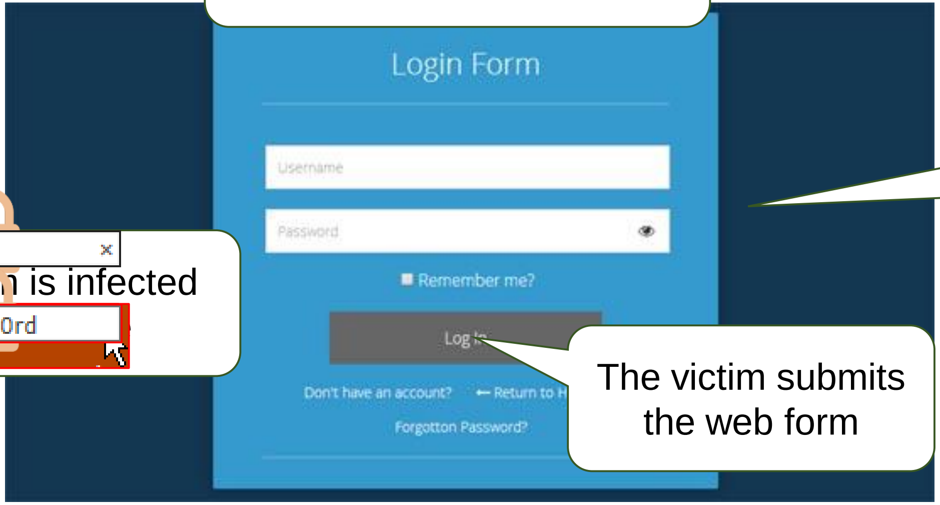


This triggers the malware

Victim

The victim makes a secure connection to a web site

The information is encrypted and sent to the web server



The victim enters data into the web form

The information is also sent to the drop zone in clear text

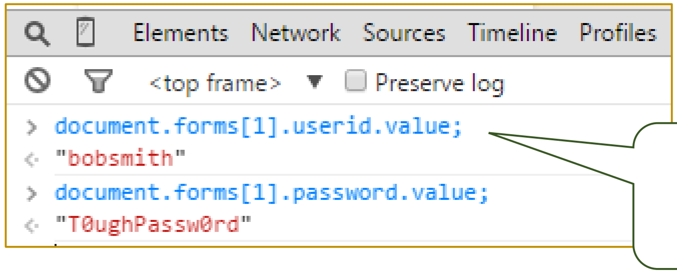
bobsmith

The victim is infected

ToughPassw0rd

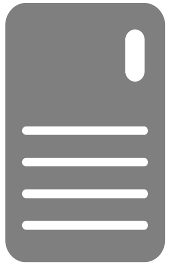
The victim submits the web form

Attacker

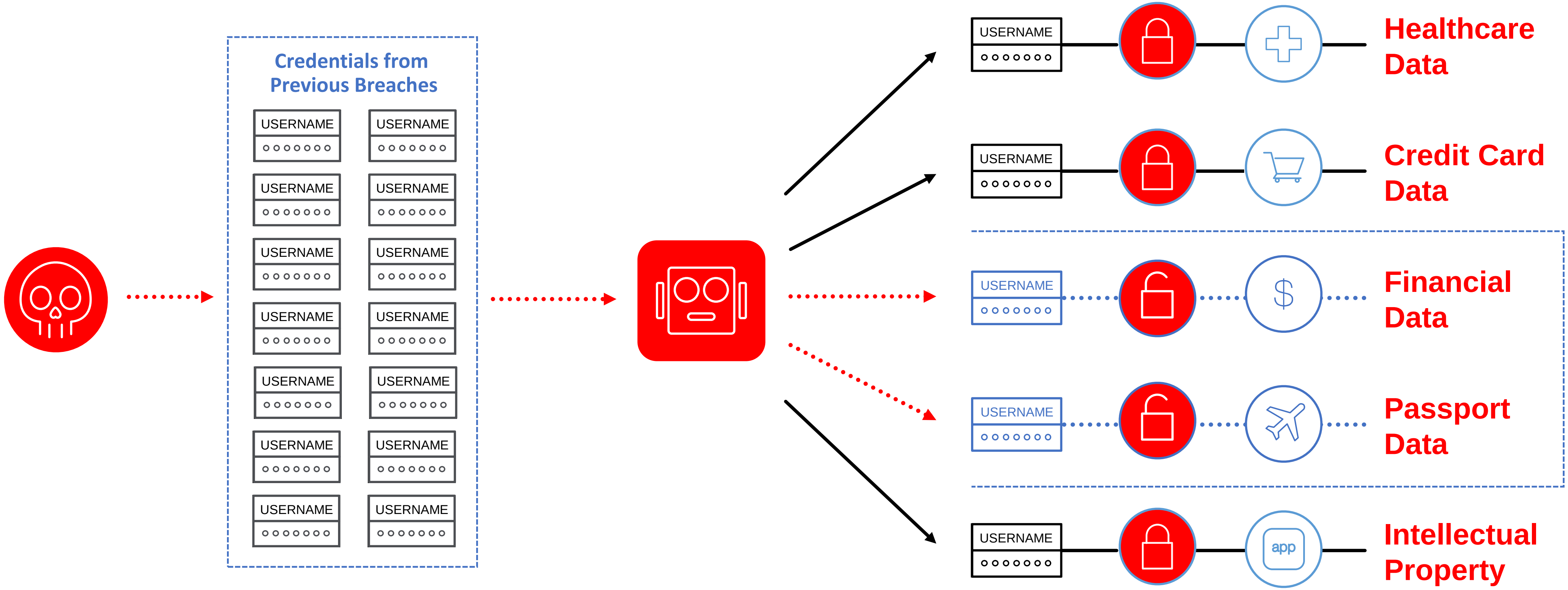


```
> document.forms[1].userid.value;
< "bobsmith"
> document.forms[1].password.value;
< "T0ughPassw0rd"
```

This content can be stolen by the malware



# How Credential Stuffing Works



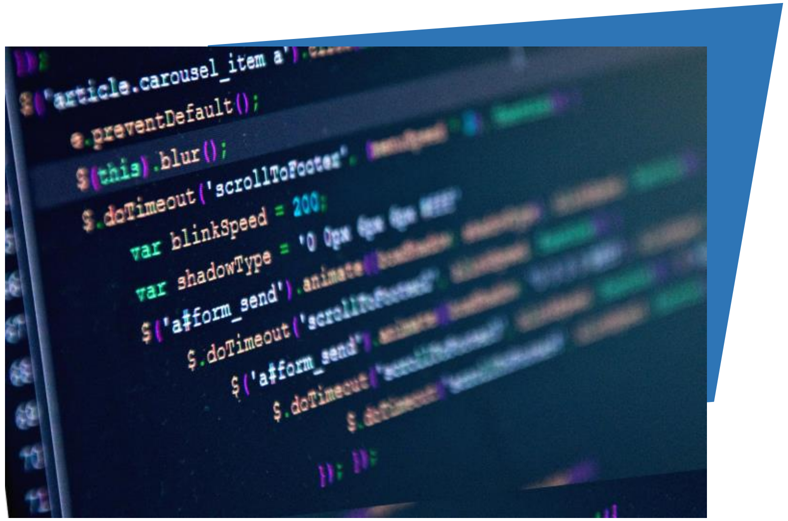
# Application Layer Encryption

Username = averagejoe
Password = 85Mustang

Username = 4TTFEQmlebq47+1s+AlykmQc9+A7quLctkKA/rC2CGo=
Password = J+4OfaGXwPqVCuDmOb9kY8Ama/P6AVxOSSfeCtGnAJI=

# HTML Field Obfuscation (HFO)

- Protects against malicious scripts that seek out form elements before HFO runs.
- Adds fake form fields to further confuse attackers.
- Dynamically changes field names on a frequent interval.



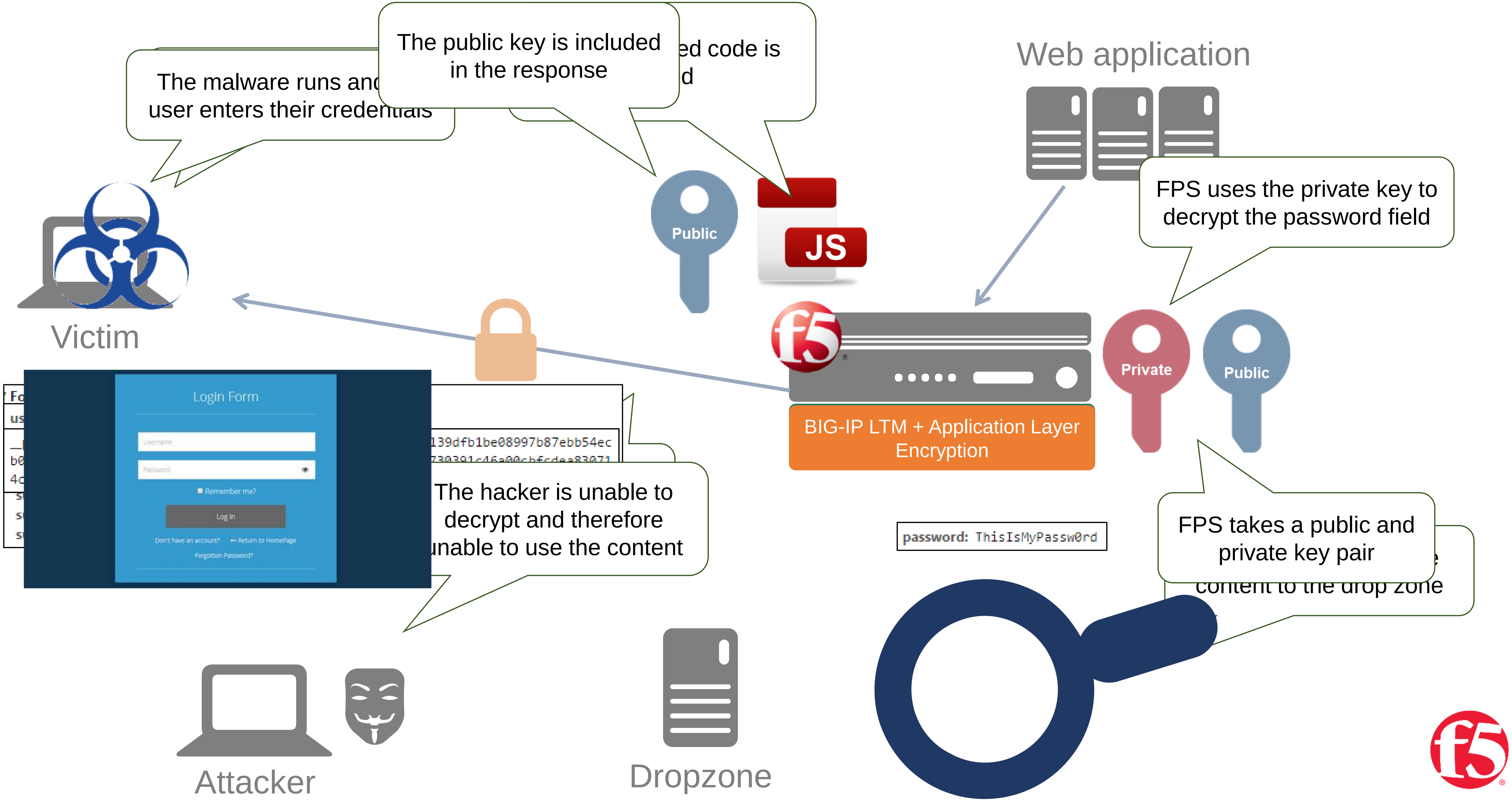
```
$('article.carousel_item a')
  e.preventDefault();
  $(this).blur();
  $.doTimeout('scrollToFooter',
    var blinkSpeed = 200;
    var shadowType = '0 0px
    $('a#form_send').animate
      $.doTimeout('scrollToFooter
        $('a#form_send')
          $.doTimeout(
    }); });
```

**Obscures visibility and slows down attackers**

Username = averagejoe
Password = 85Mustang

NikwQH38GADKDm4ShuYKw0t6KYLSnGyMElRpctLOFF8= = 4TTFEQmlebq47+1s+AlykmQc9+A7quLctkKA/rC2CGo=
ILdDJKaLSiopyvRjNw+V3V3NKTL4mFUeTL7alr+Swjk= = J+4OfaGXwPqVCuDmOb9kY8Ama/P6AVxOSSfeCtGnAJI=

# How DataSafe Uses Encryption to Protect Confidential Data?



The malware runs and user enters their credentials

The public key is included in the response

ed code is
d

FPS uses the private key to decrypt the password field

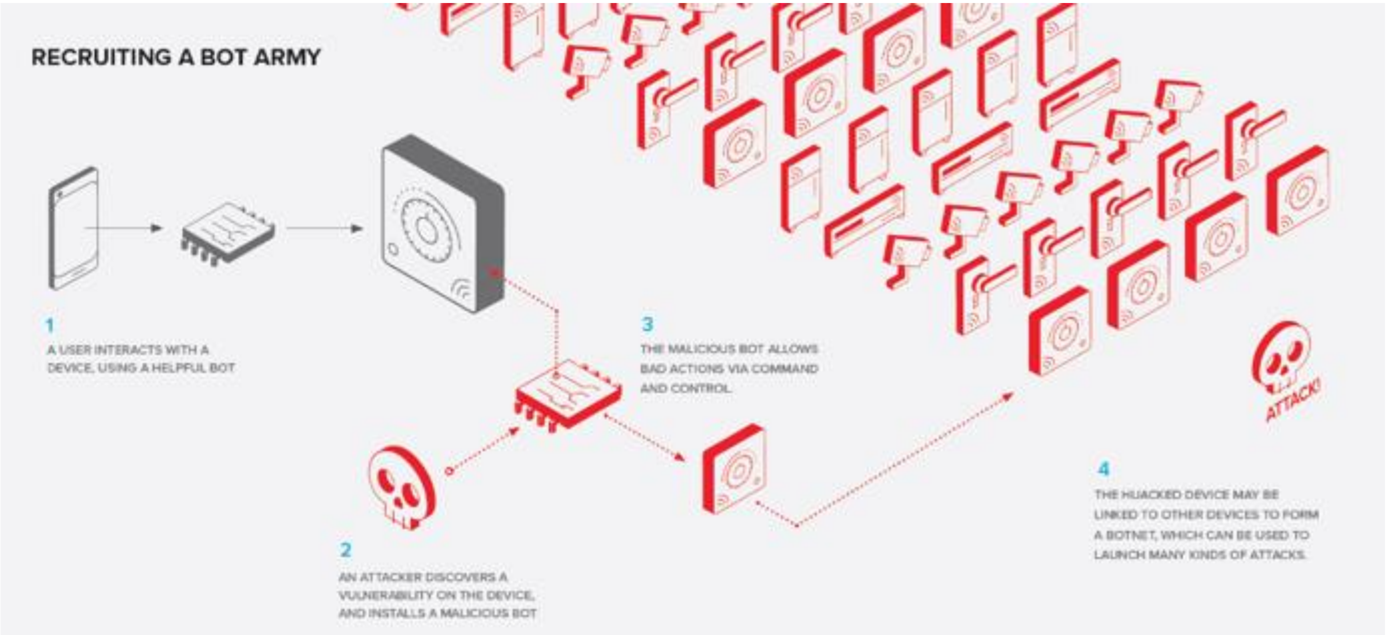
BIG-IP LTM + Application Layer Encryption

FPS takes a public and private key pair

e
content to the drop zone

The hacker is unable to decrypt and therefore unable to use the content

# Proactive Bot Defense


RECRUITING A BOT ARMY
1
A USER INTERACTS WITH A DEVICE, USING A HELPFUL BOT
2
AN ATTACKER DISCOVERS A VULNERABILITY ON THE DEVICE, AND INSTALLS A MALICIOUS BOT
3
THE MALICIOUS BOT ALLOWS BAD ACTIONS VIA COMMAND AND CONTROL
4
THE HIJACKED DEVICE MAY BE LINKED TO OTHER DEVICES TO FORM A BOTNET, WHICH CAN BE USED TO LAUNCH MANY KINDS OF ATTACKS
ATTACK!

Half of Internet traffic comes from bots

30% is malicious

## web attacks

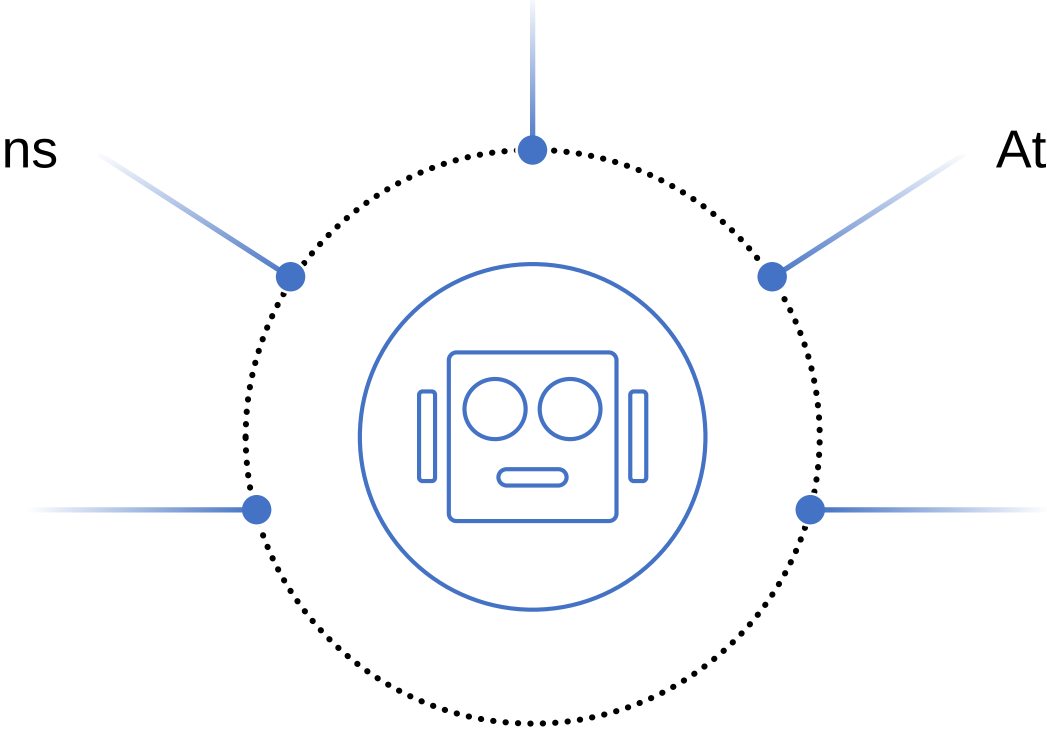
77% of web app attacks were the targets of botnet activity

## account takeover

Total account takeover losses reached $2.3B in 2016

Vulnerability Scanning
Web Scraping
Denial of Service

# What Do Malicious Bots Do?



Gain unauthorized access to accounts

Tamper with transactions

Attack web and mobile apps

Infect users with malware

Launch Denial of Service

**There are millions of bots**

# Advanced Bot Detection

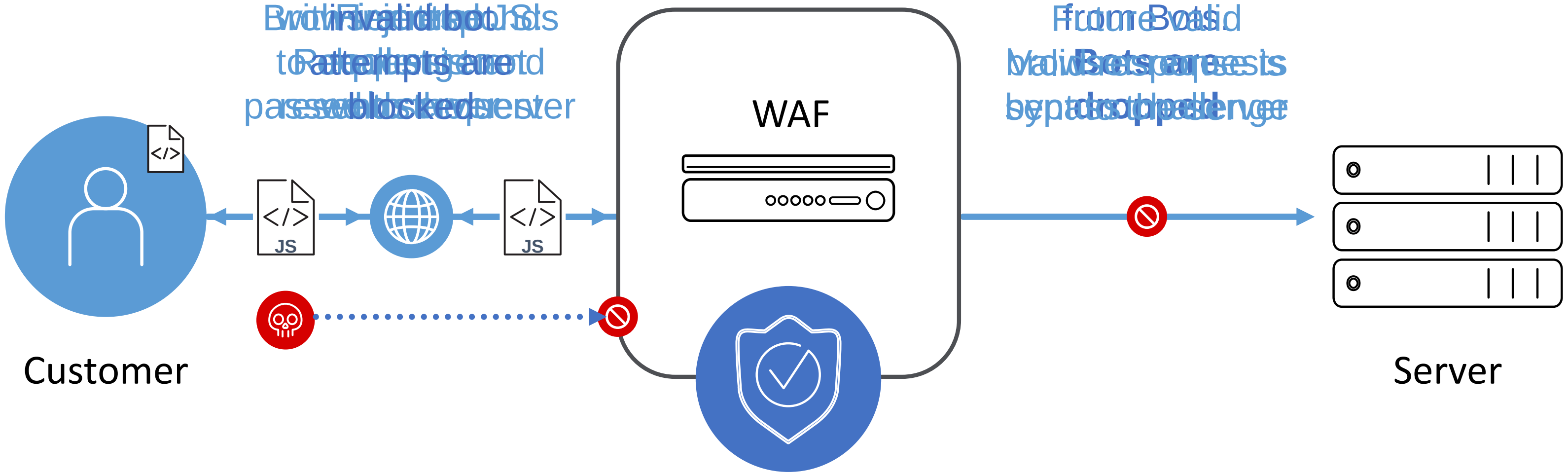
## Legitimate Browser Verification

Continuous invalid bot attempts are blocked

No challenge response from Bots

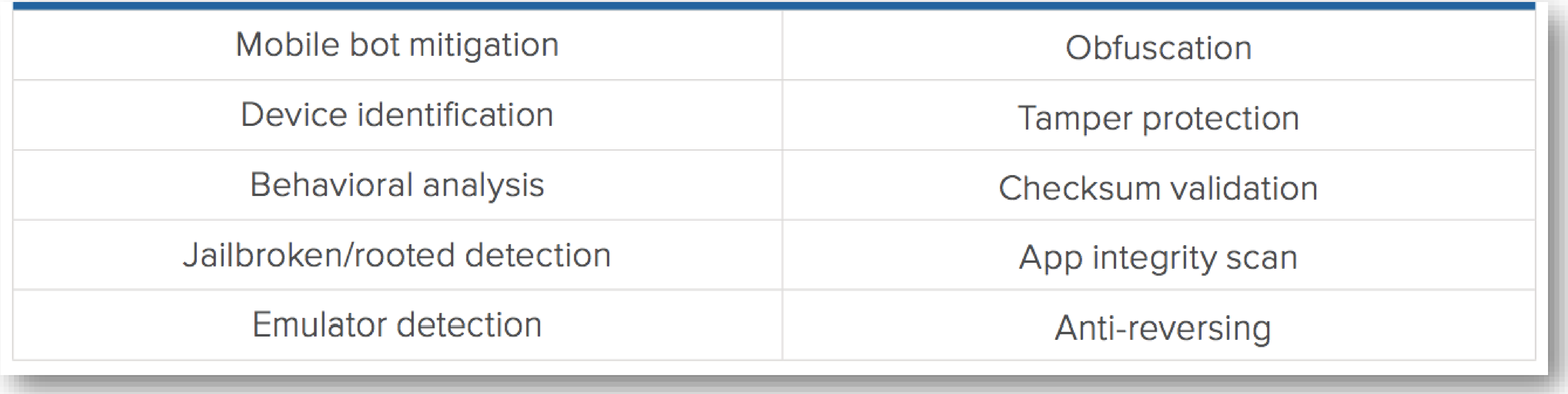
Bots are dropped

Future valid requests bypass challenge



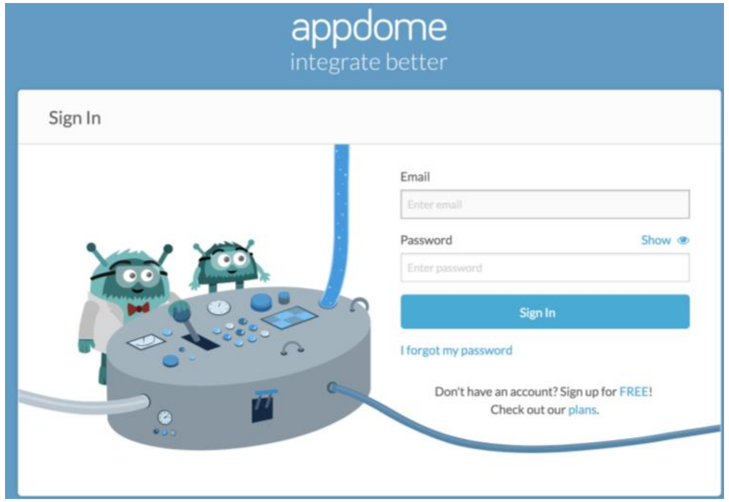
WAF verifies response authenticity.
Cookie is signed, time stamped,
and finger printed.

# F5 Anti-Bot Mobile SDK

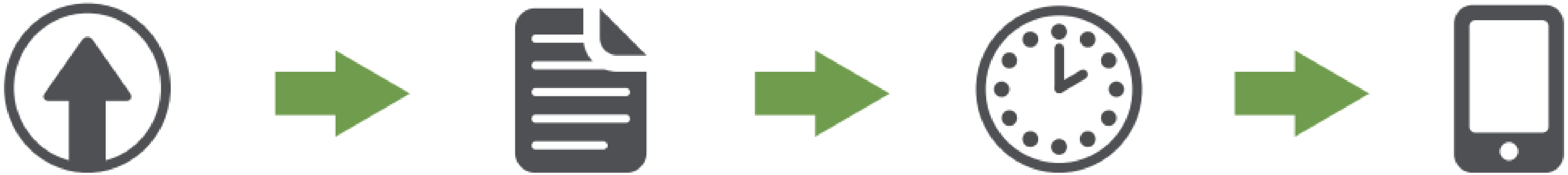


| | |
|---|---|
| Mobile bot mitigation | Obfuscation |
| Device identification | Tamper protection |
| Behavioral analysis | Checksum validation |
| Jailbroken/rooted detection | App integrity scan |
| Emulator detection | Anti-reversing |

# Fuse the Mobile App



Don't have an account? Sign up for FREE!
Check out our plans.



Upload post-build
.ipa or .apk
to Appdome.

Select the mobile
service SDKs
to integrate
(e.g.: F5 Anti-Bot
Mobile SDK).

Click
**Fuse My App**
and in minutes...

Distribute via
your app platform
of choice.

APPLICATION PROTECTION

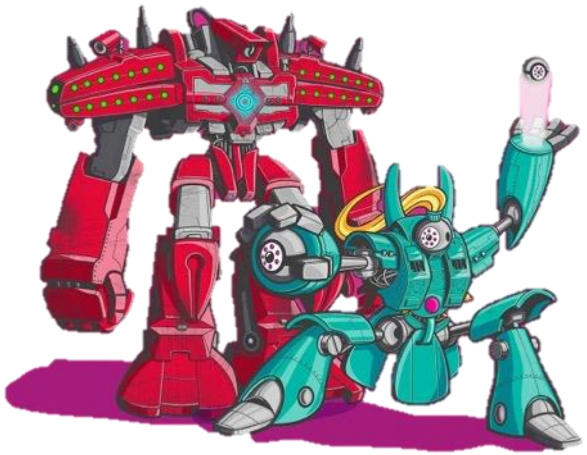
# ADVANCED WAF

PROACTIVE BOT DEFENSE

APP-LAYER ENCRYPTION

ANTI-BOT MOBILE SDK

BEHAVIORAL DDOS



f5®