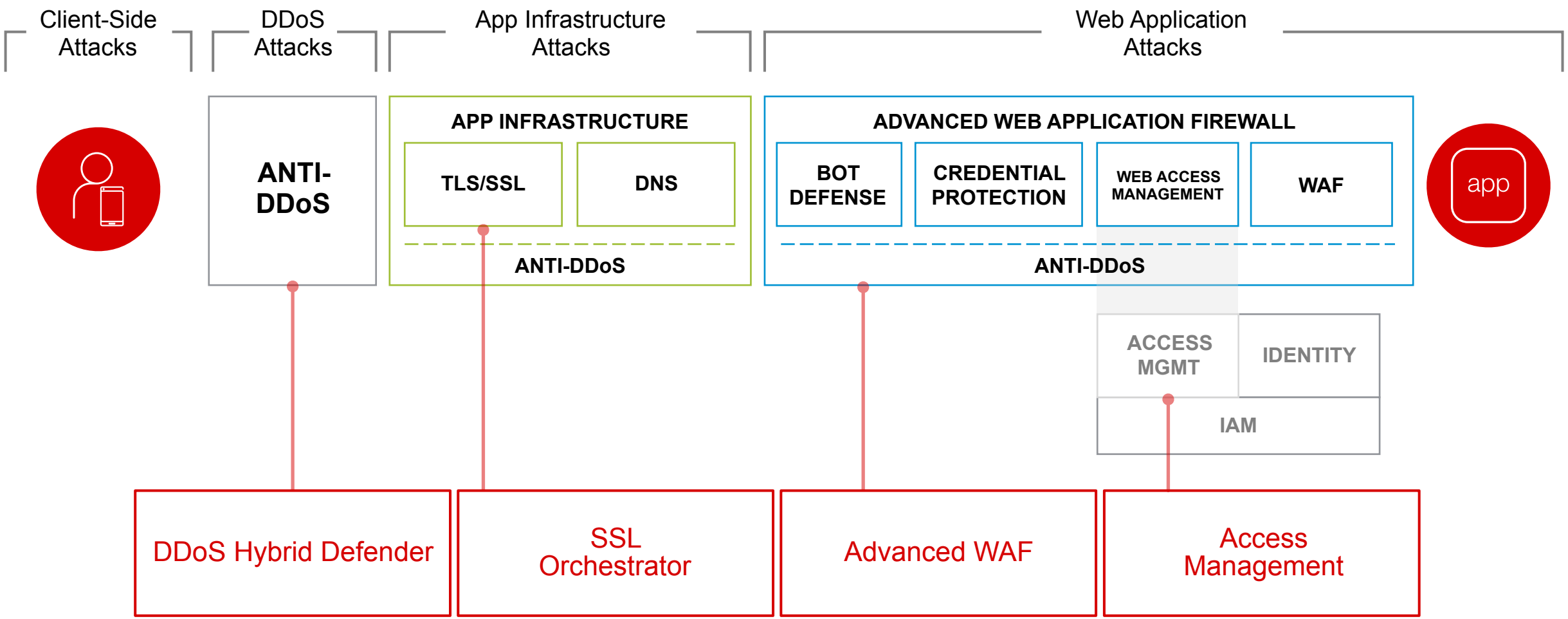
Zabezpečení Webových portálů kritických služeb

FILIP KOLÁŘ
F5 NETWORKS ČESKÁ REPULIKA
F.KOLAR@F5.COM

Bezpečnostní koncept aplikační ochrany F5



Zákazníci v ČR – více než 100 instalací

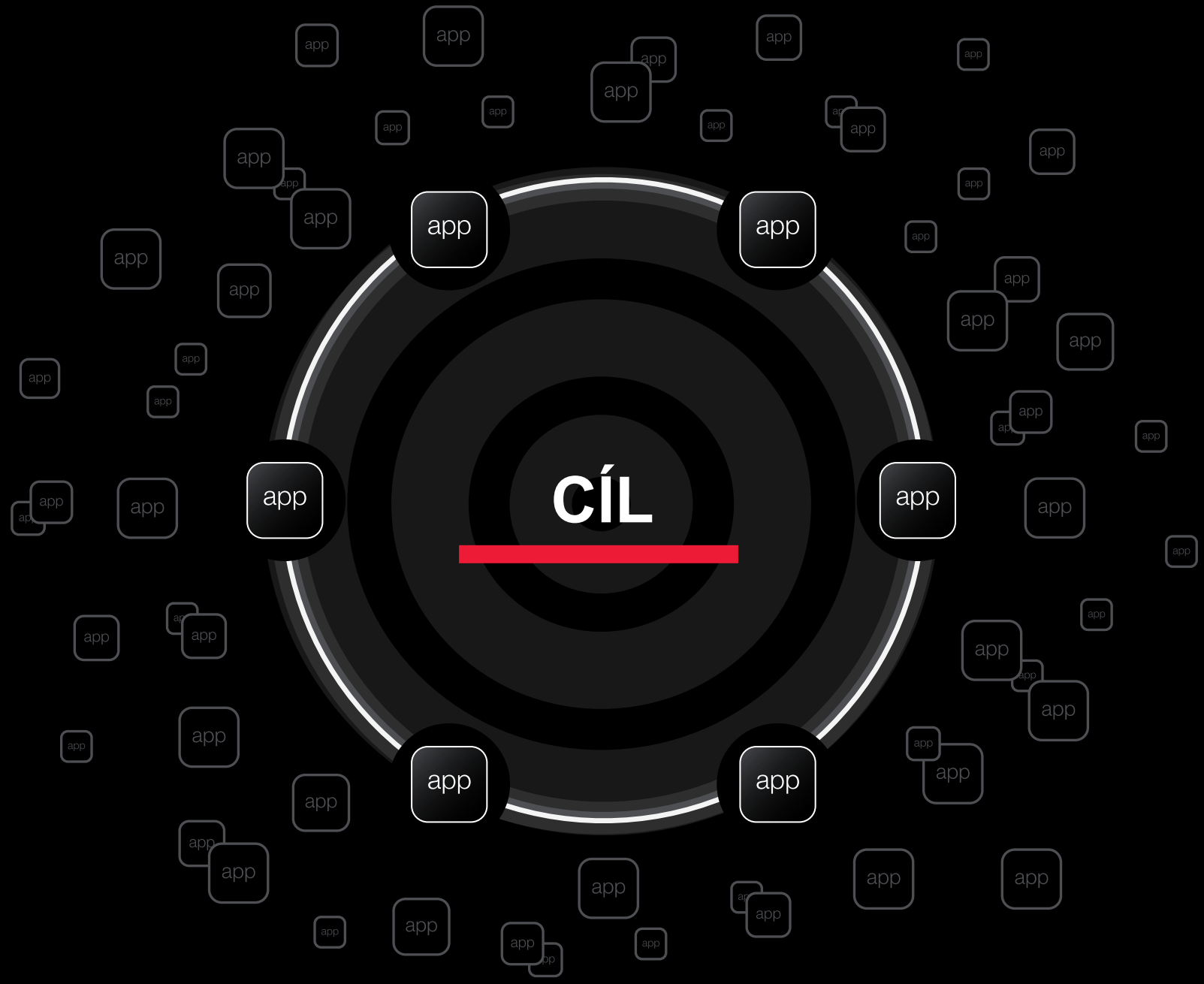
- Finance – Největší banky, nebankovní sektor, platební brány
- Komerční sektor – Sázkové kanceláře, “utility“, …
- Operátoři – Telco, ISP, poskytovatelé „manageovaných“ služeb
- Státní správa a podniky - Ministerstva, kraje, velké státní podniky

APLIKACE JSOU

Důvodem, proč lidé používají Internet

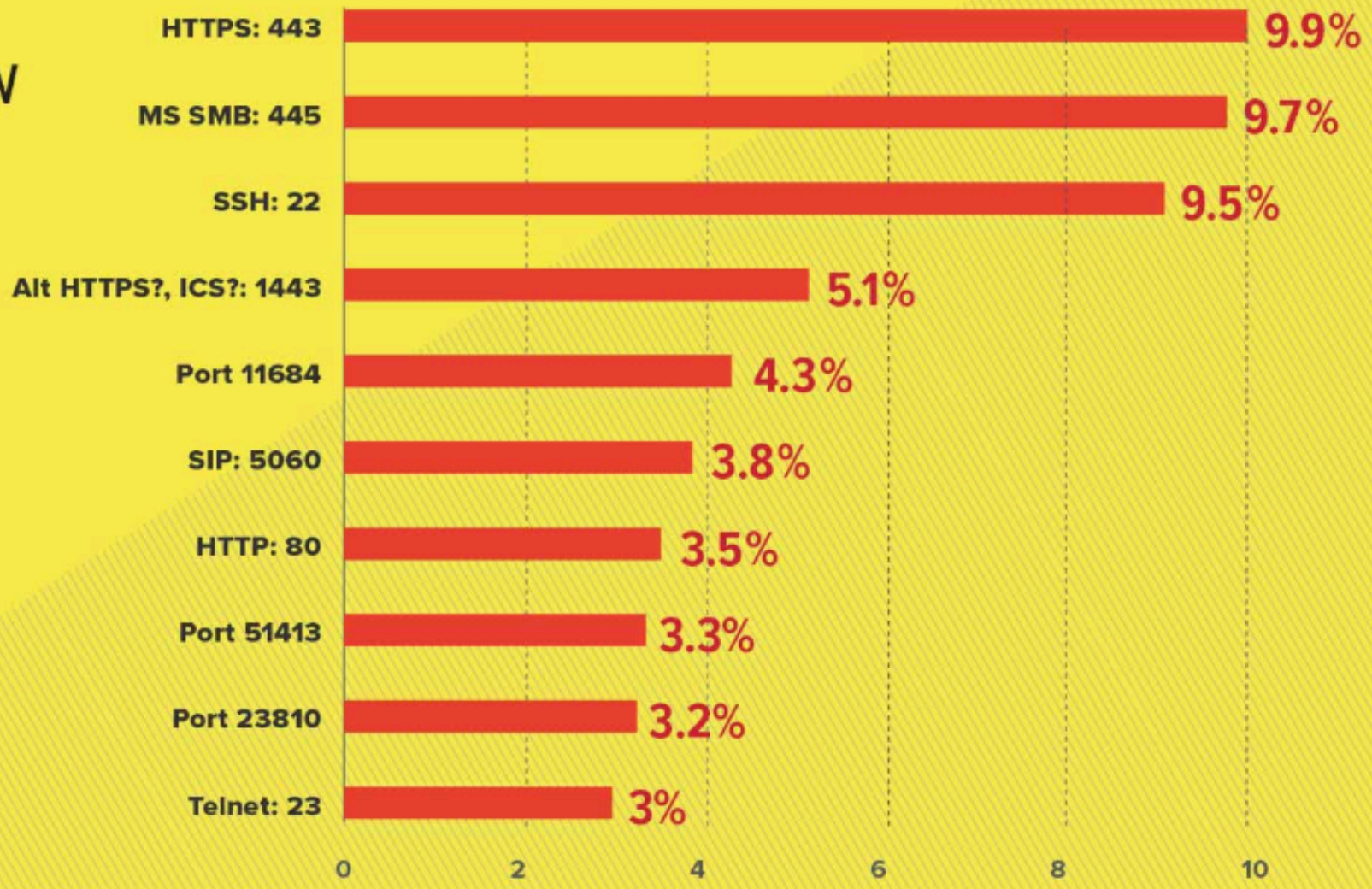
Váš business

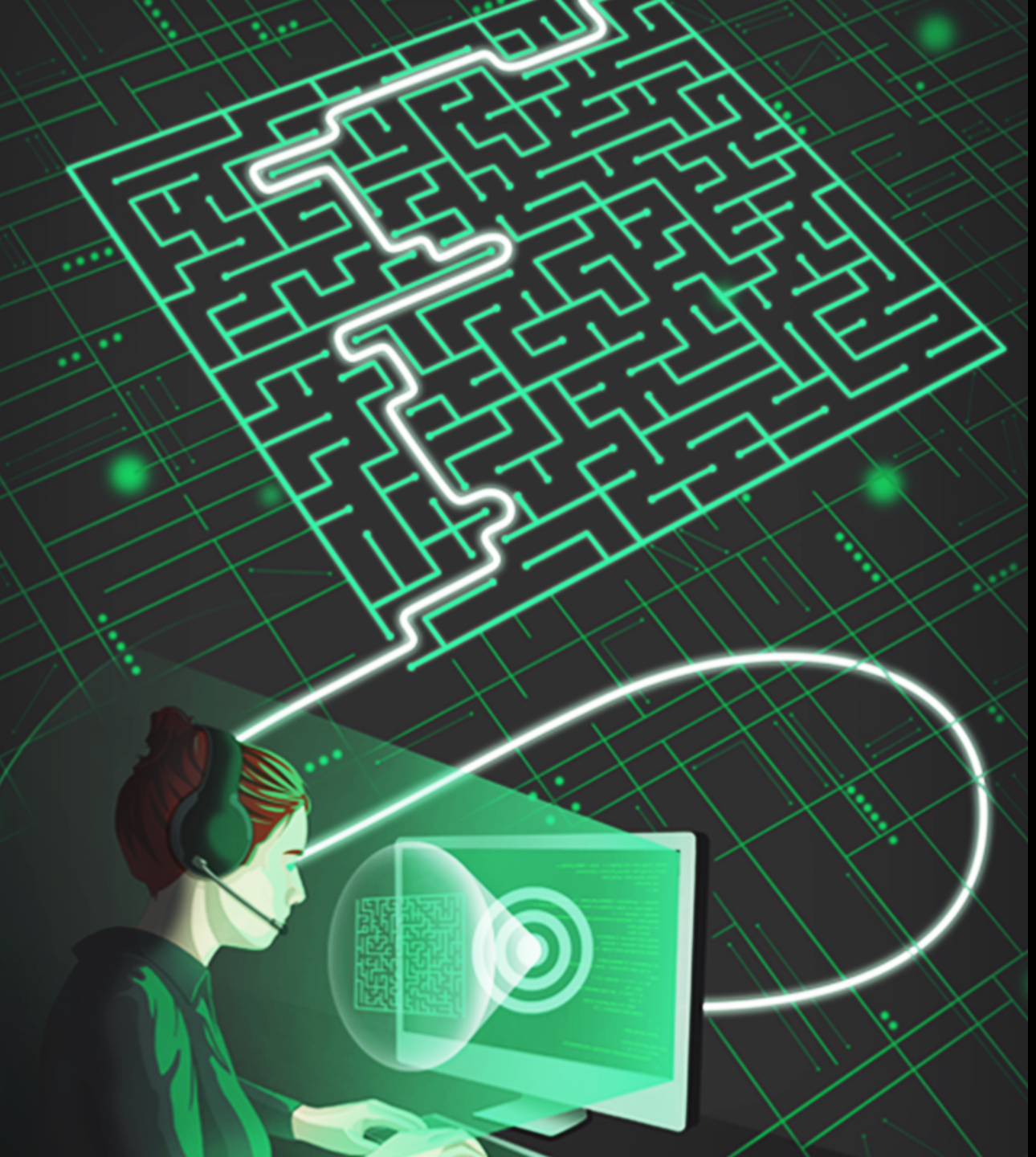
Gateway k Vašim DATŮM



Apps are the #1 attack target

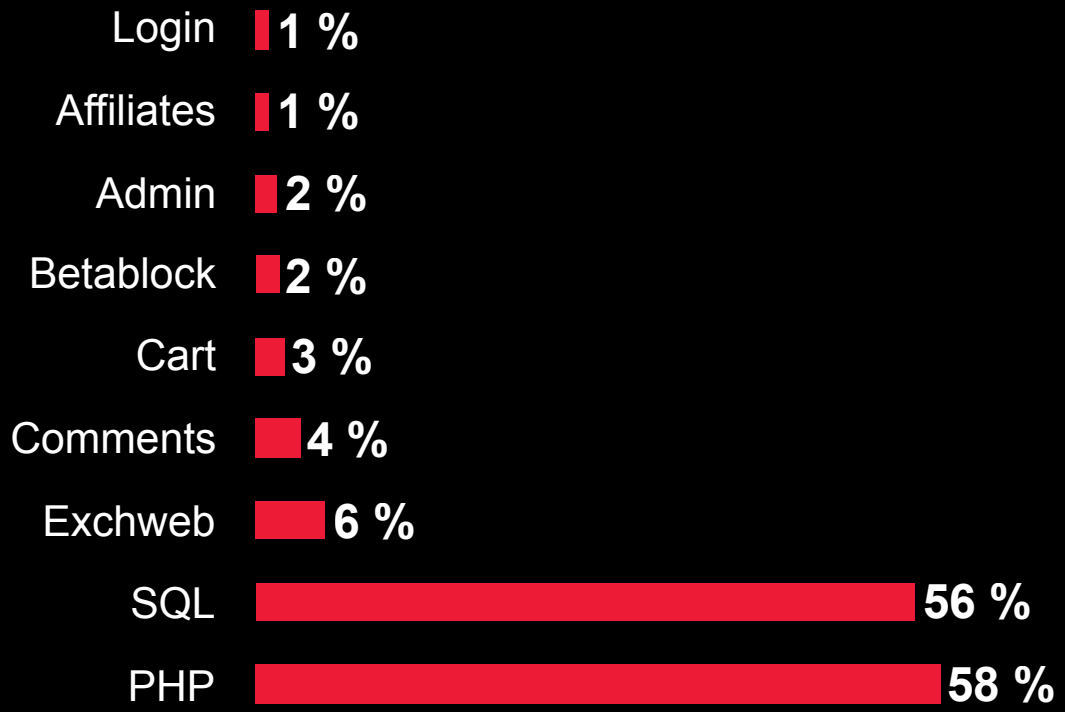
2018 ATTACKS BY TOP 10 DESTINATION PORTS





Aplikační útoky

Injection → PHP & SQL

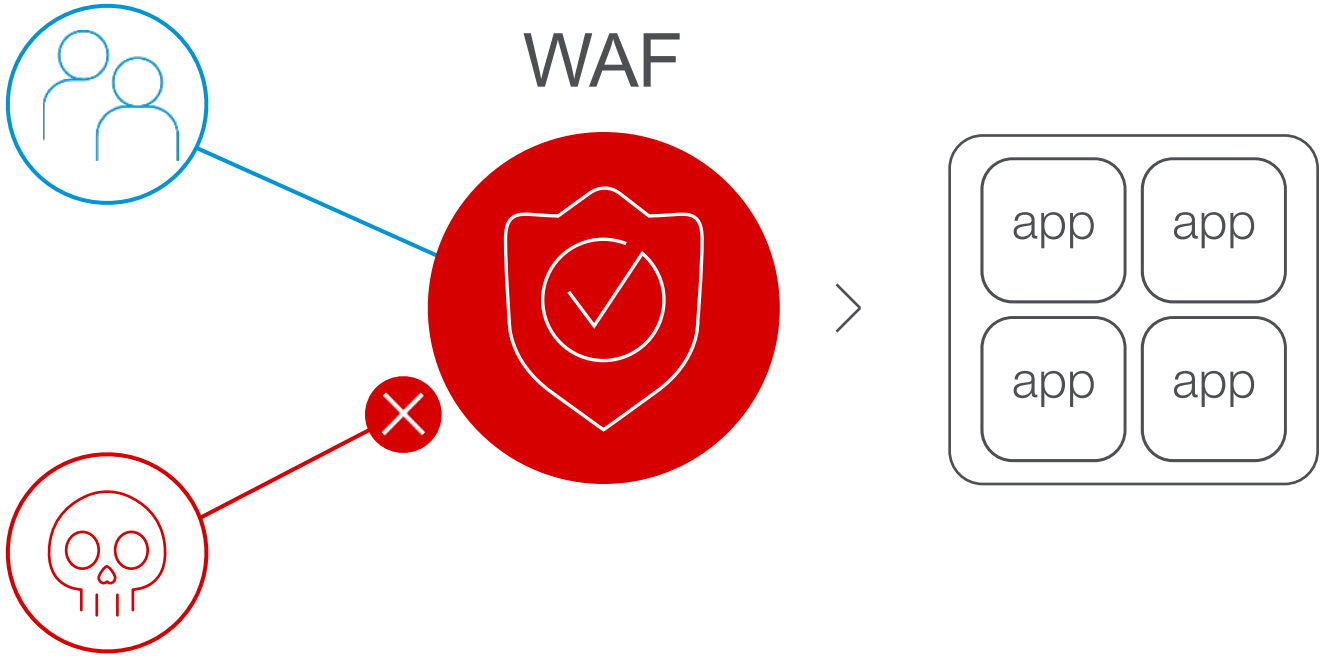


Útoky na webové aplikace analyzuje a reportuje nezávislé združení OWASP

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Injection…

Chráníte vaše aplikace proti zranitelnostem OWASP?



- Zranitelnosti
- Aktivní útoky
- Compliance

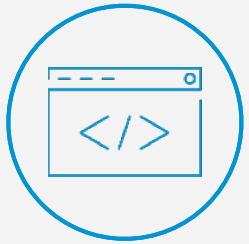
Web Aplikační FW...

	Network/Next Gen Firewall	*IPS*	*WAF*
Known Web Worms	Limited	✓	✓
Unknown Web Worms	X	Limited	✓
Known Web Vulnerabilities	Limited	Partial	✓
Unknown Web Vulnerabilities	X	Limited	✓
Illegal Access to Web-server files	Limited	Limited	✓
Forceful Browsing	X	X	✓
File/Directory Enumerations	X	Limited	✓
Buffer Overflow	Limited	Limited	✓
Cross-Site Scripting	Limited	Limited	✓
SQL/OS Injection	Limited	Limited	✓
Cookie Poisoning	X	X	✓
Hidden-Field Manipulation	X	X	✓
Parameter Tampering	X	X	✓
Layer 7 DoS Attacks	Limited	X	✓
Brute Force Login Attacks	Limited	X	✓
App. Security and Acceleration	X	X	✓
Credential Stuffing	X	X	✓
Password Field obfuscation	X	X	✓
BotNet protection	Limited	X	

Tradiční WAF

OWASP
Top 10

Inspekce
SSL/TLS

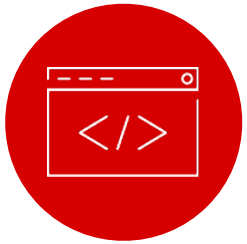


Skriptování

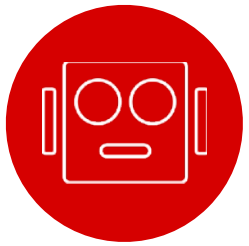
Pokročilá WAF

OWASP
Top 10

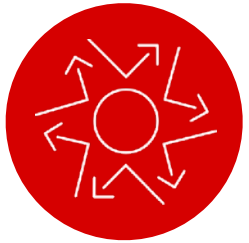
Inspekce
SSL/TLS



Skriptování

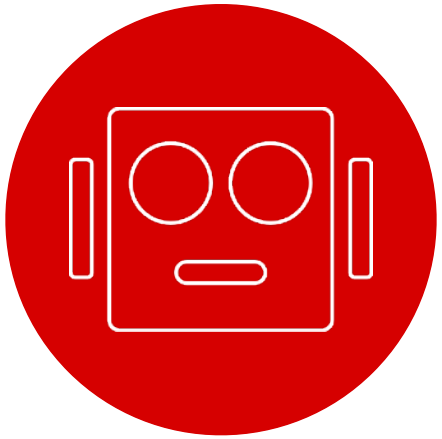


Proaktivní
Bot ochrana



Ochrana proti
aplikačním DoS
útokům

Ochrana
”Credentials”



Automatizované Útoky

Rozmach BOTů?

52%

Internetového provozu
je automatizováno

http://bit.ly/2FOtjA6

POVOLENO

98.6M identifikovaných botů


Botnet

Vzpoura BOTů!

73%

Prolomení webových aplikací za pomocí BOTů

98.6M identifikovaných botů

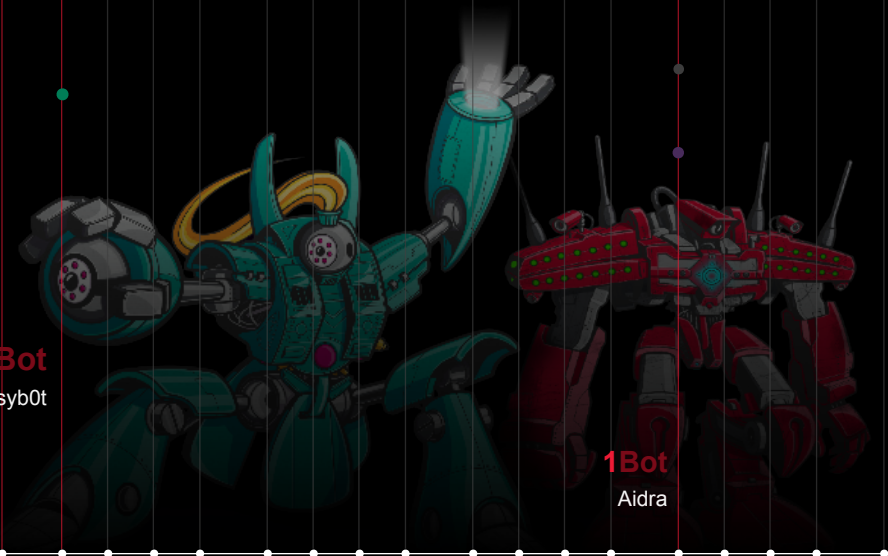
30% are bad

Expanze zlých botnetů nastala v posledních 3 letech

Affected Devices

74% Discovered in last 2 years

- CCTV
- DVRs
- SOHO routers
- iOS
- WAPs
- Set-Top Boxes
- Media Center
- ICS
- Android
- IP Cameras
- Wireless Chipsets
- NVR Surveillance
- VoIP Devices
- Cable Modems
- Busybox Platforms
- Smart TVs



1Bot
Psyb0t

1Bot
Hydra

1Bot
Aidra

1Bot
Moon

2Bots
Darlloz
Marcher

1Bot
Gafgyt
Family

4Bots
Hajime
Trickbot
IRC Telnet
Annie

1Bot
Crash override

1Bot
Remaiten

3Bots
Mirai
BigBrother
Rediation

1Bot
Brickerbot

3Bots
Satori Fam
Amnesia
Persirai

2Bots
WireX
Reaper

6Bots
Masuta
PureMasuta
Hide 'N Seek
JenX
OMG
DoubleDoor

7Bots
SORA
OWARI
UPnPProxy
OMNI
RoamingMantis
Wicked
VPNFilter

2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

Útočné vektory nalezené v botnetech

Červeně – útočné vektory objevené F5 Labs v provozu botnetů

Client-Side Attacks

- Malware
- Ransomware
- Man-in-the-browser
- Session hijacking
- Cross-site request forgery
- Cross-site scripting

App Infrastructure Attacks

- Man-in-the-middle
- Key disclosure
- Eavesdropping
- DNS cache poisoning
- DNS spoofing
- DNS hijacking
- Protocol abuse
- Dictionary attacks

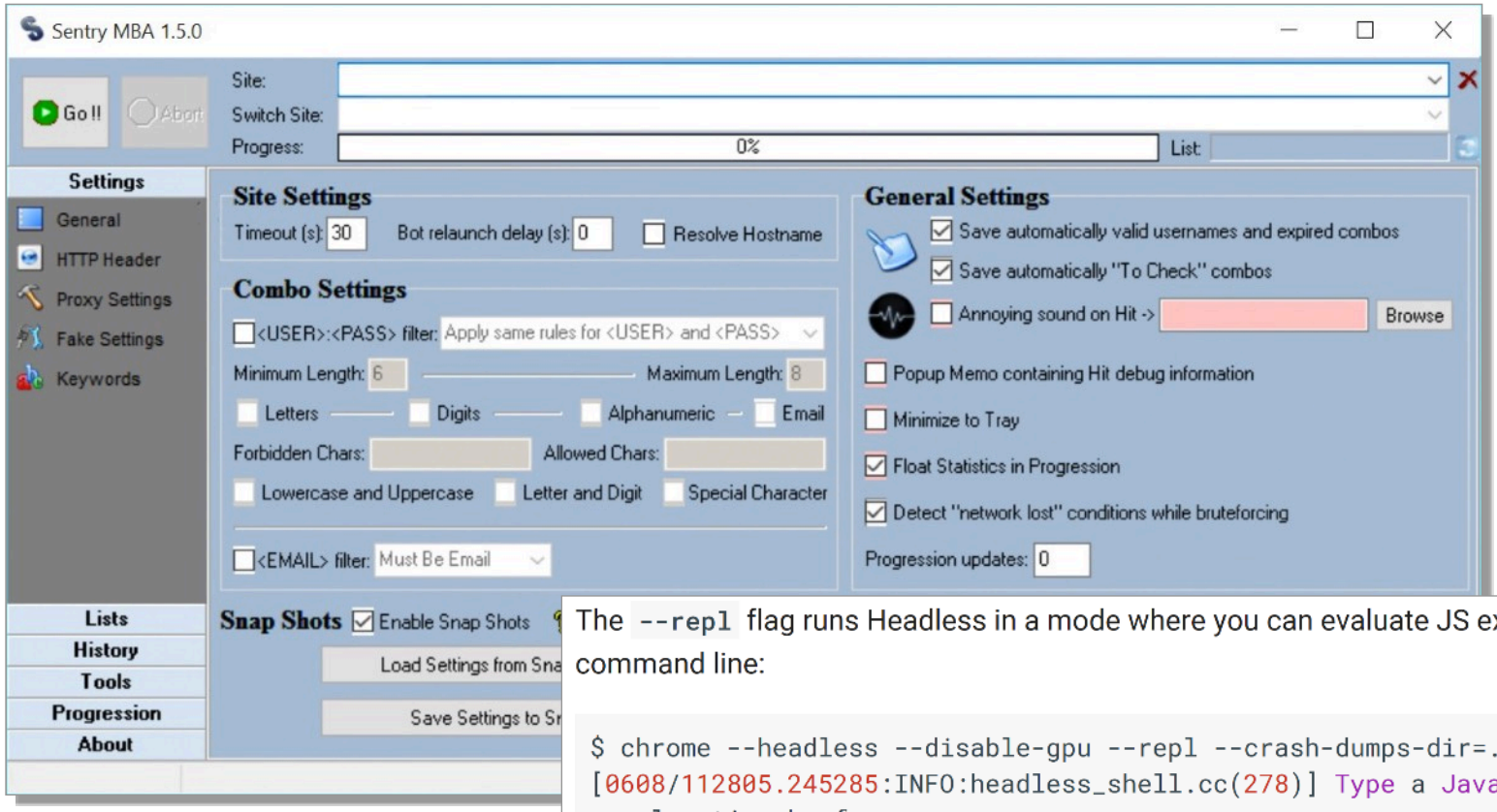
DDoS Attacks

- SYN, UDP, and HTTP floods
- SSL renegotiation
- DNS amplication
- Heavy URL

Web Application Attacks

- API attacks
- Cross-site scripting
- Injection
- Cross-site request forgery
- Malware
- Cryptominig
- Man-in-the-middle
- Credential theft
- Credential stuffing
- Phishing
- Certificate spoofing

BOTi, kteří simulují skutečného uživatele



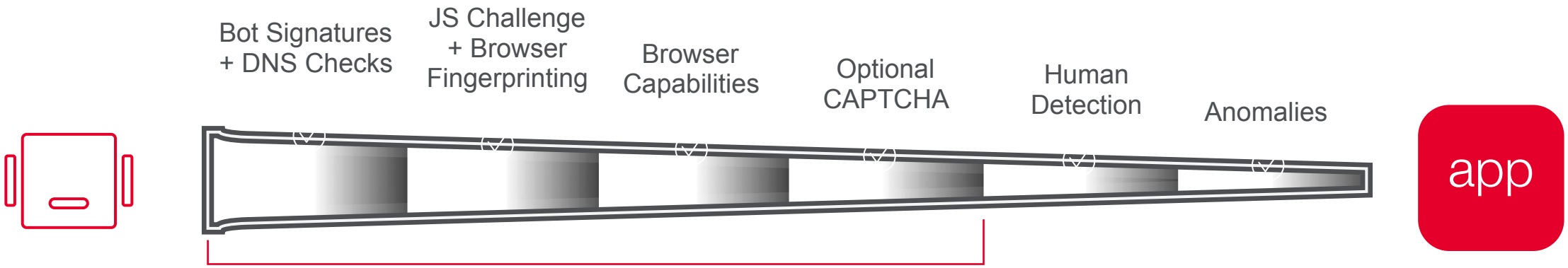
Sentry MBA

Headless Chrome

The `--repl` flag runs Headless in a mode where you can evaluate JS expressions in the browser, right from the command line:

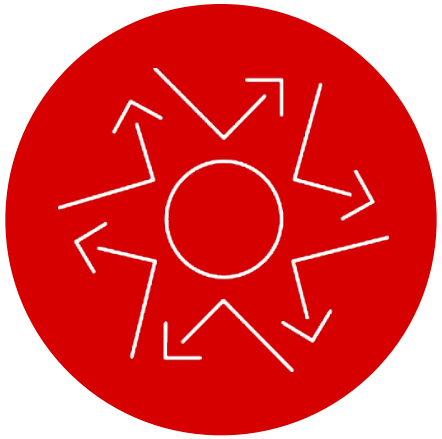
```
$ chrome --headless --disable-gpu --repl --crash-dumps-dir=./tmp https://www.chromestatus.com/
[0608/112805.245285:INFO:headless_shell.cc(278)] Type a Javascript expression to evaluate or "quit" t
>>> location.href
{"result":{"type":"string","value":"https://www.chromestatus.com/features"}}
>>> quit
$
```

Jak ochranu proti botům řeší F5?



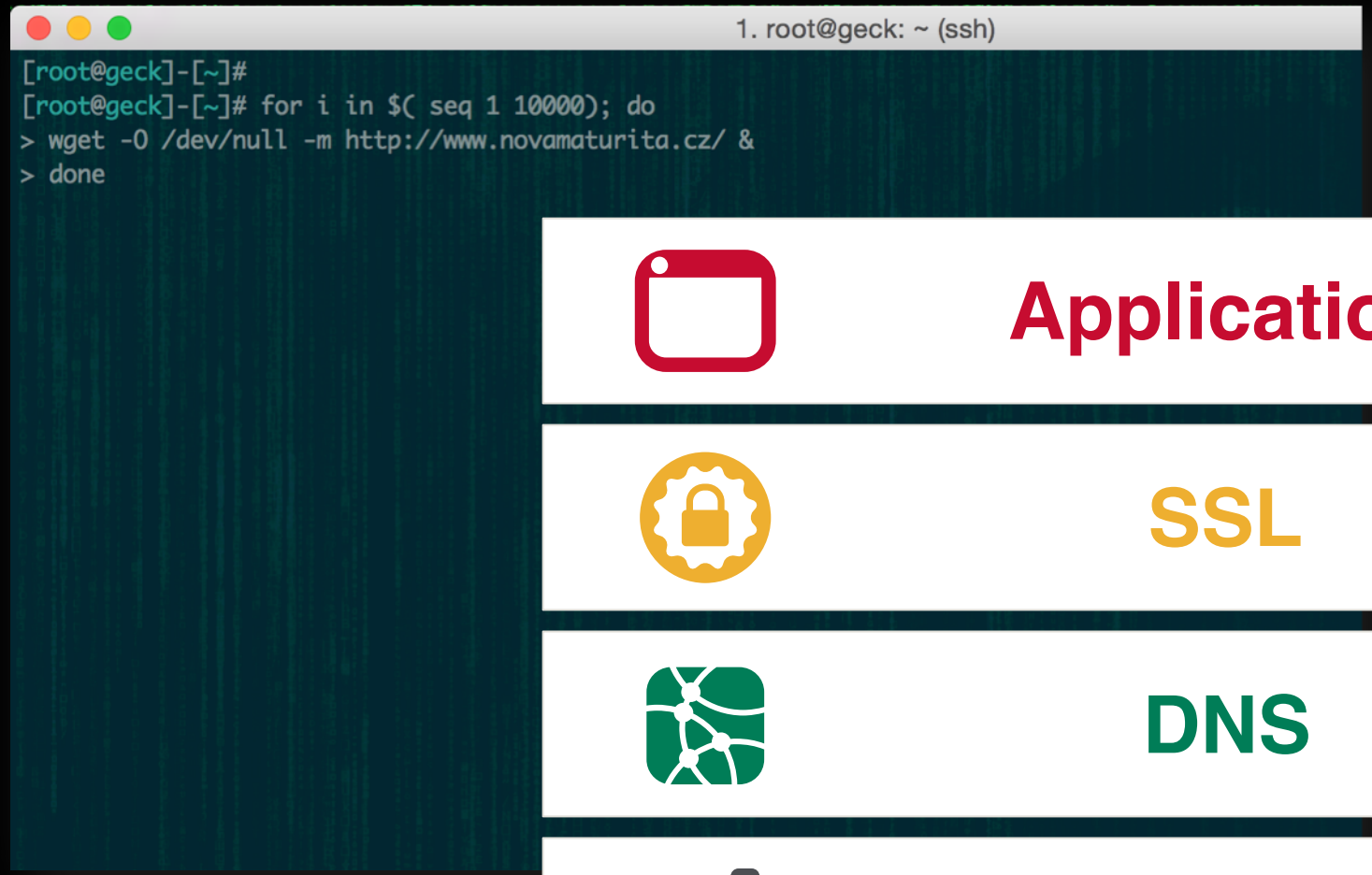
Provoz by se neměl dostat na server


I'm not a robot
reCAPTCHA
Privacy - Terms



Aplikační Denial-of-Service

L7 DoS není složitá věc!



22Mbps

26Gbps

Přesná detekce pomocí Behaviorální Analýzy

1 **Strojové učení**

F5 learns normal traffic baselines

2 **Dynamické Signatury**

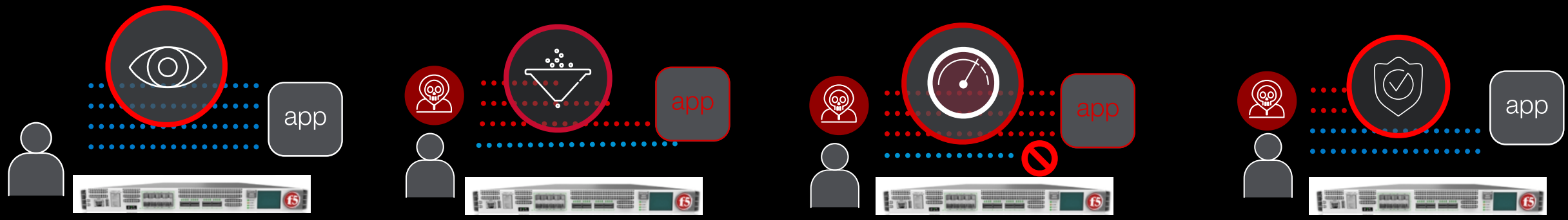
F5 identifies bad traffic and bad actors

3 **Stress Monitoring**

F5 detects abnormal application stress

4 **Mitigace útoků**

F5 shuns bad traffic automatically



Krádež uživatelských přístupů

';--have i been pwned?

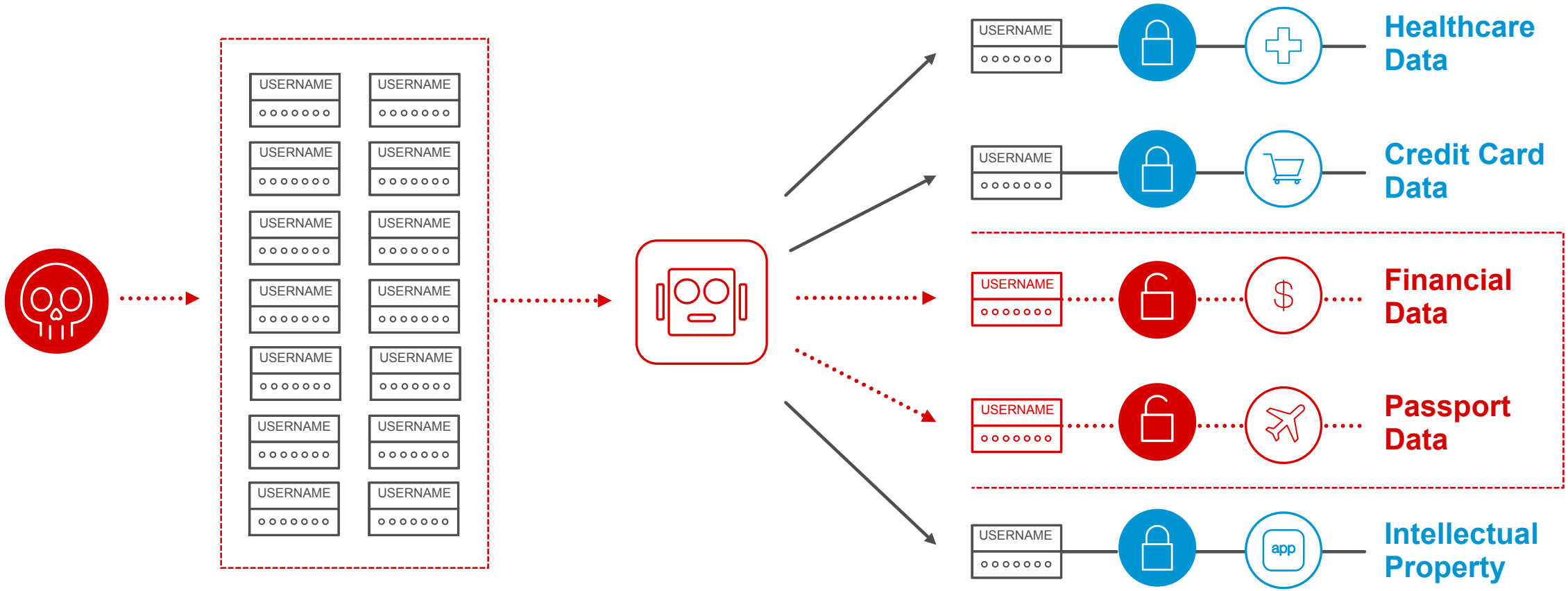
Check if you have an account that has been compromised in a data breach

fil.kolar@gmail.com pwned?

Oh no — pwned!

Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

Jak funguje útok typu ”Credential Stuffing”



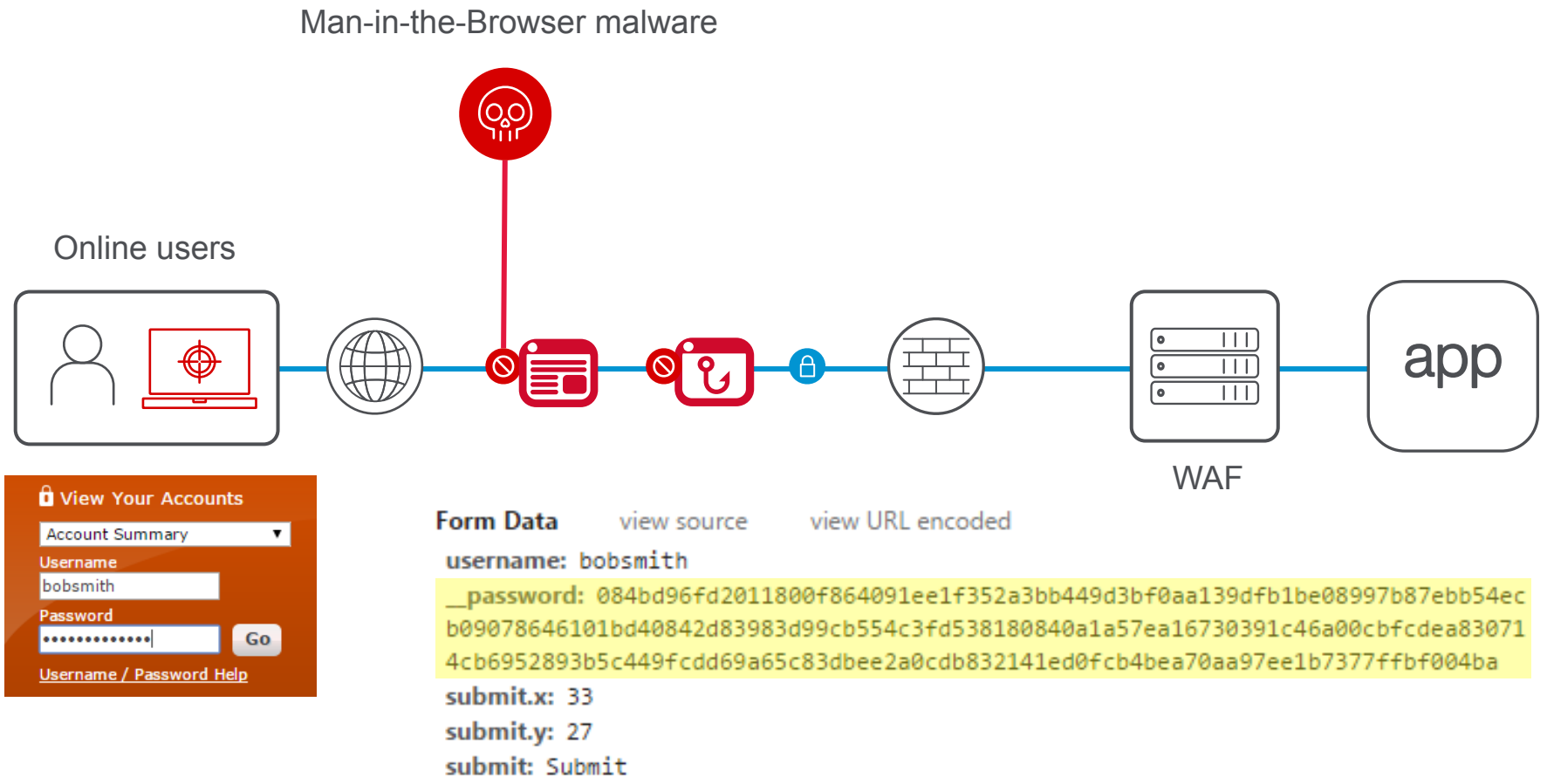
Krádež credentials pomocí malwaru: jak se chránit

PROBLEM

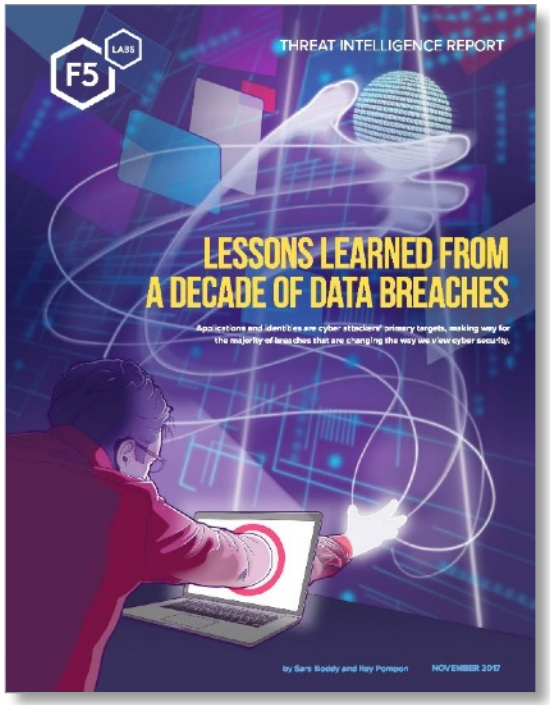
Malware

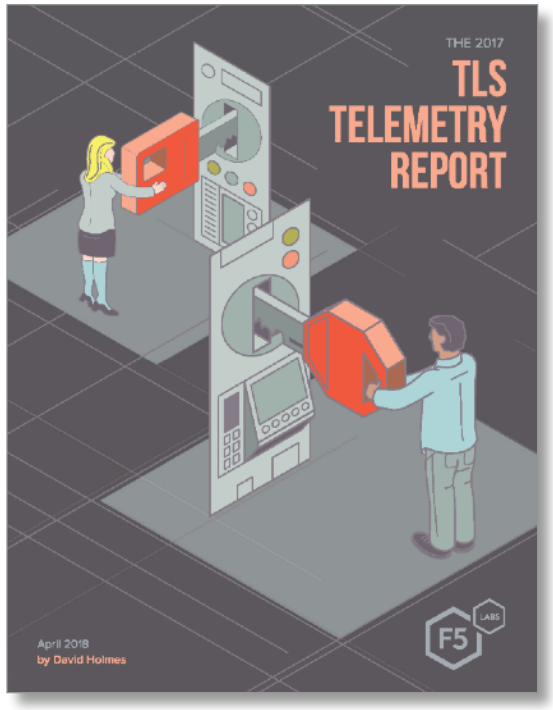
SOLUTION

App-layer encryption



F5 Labs Reports





WE MAKE APPS

FASTER. SMARTER. SAFER.

f.kolar@f5.com
r.gibala@f5.com