
June 2019
The Business of Organised Cybercrime
Paul Dignan
Solutions Engineering Manager.
@SuperDiggers
f5.com/labs
WE MAKE APPS GO
FASTER.
SMARTER.
SAFER.


EUROPOL


NCA
National Crime Agency


F5
LABS


National Cyber
Security Centre
a part of GCHQ


TOP SECRET

Cyber Enabled Crime

Traditional crime amplified by the web

- Illegal markets
- Financial Fraud
- Sale of counterfeit goods
- Human trafficking
- Child sexual exploitation

Cyber Dependent Crime

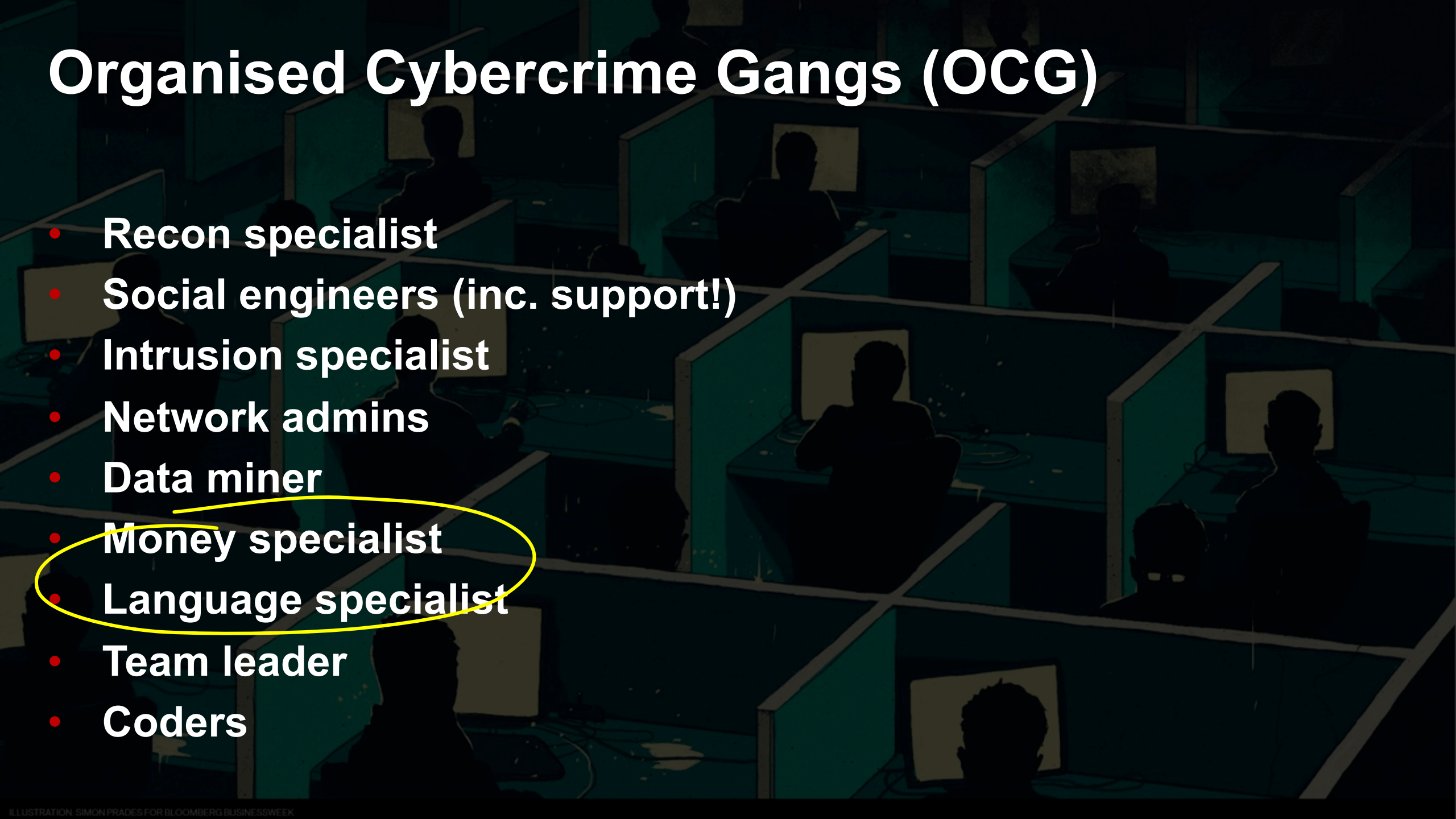
'High-tech' crime

- Ransomware
- Cryptojacking
- Cyber extortion
- Business email compromise (CEO fraud)

ILLUSTRATION: SIMON PRADES FOR BLOOMBERG BUSINESSWEEK

Organised Cybercrime Gangs (OCG)

- Recon specialist
- Social engineers (inc. support!)
- Intrusion specialist
- Network admins
- Data miner
- Money specialist
- Language specialist
- Team leader
- Coders



Organised Cybercrime Gangs (OCG)

- Recon specialist
- Intrusion specialist
- Social engineers (inc. support!)
- Network admins
- Data miner
- Money specialist
- Language specialist
- Team leader
- Coders

ILLUSTRATION: SIMON PRADES FOR BLOOMBERG BUSINESSWEEK

Crime-as-a-Service

[I have] ransomware. I am responsible for making the malware evade anti-virus software, you will be responsible for spreading it. (Looking for a highly-skilled partner to cooperate with).

The name of the ransomware is GandCrab.
[For more in-depth information,] please see the reporting from below.

https://www[.]hackeye.net/securitytetchnology/netsec/12140.aspx
https://www[.]hackeye[.]net/threatintelligence/12530.aspx
http://www[.]freebuf[.]com/column/162254.html

Searching for high-skilled [malware] spreaders.
[Profits will be split] 60 percent/40 percent
[If there are high profits then the split] will be raised to 70 percent/30 percent

You do not have to worry about malware coding, evading anti-virus systems and so on.
All you need to do is spread the malware.

ILLUSTRATION: SIMON PRADES FOR BLOOMBERG BUSINESSWEEK

Always follow the money…

Traditional

- Traditional fraud
- Tech Support scam
- **Banks:**
- Banking malware
- **Clients:**
- Banking trojans

Cryptocurrencies

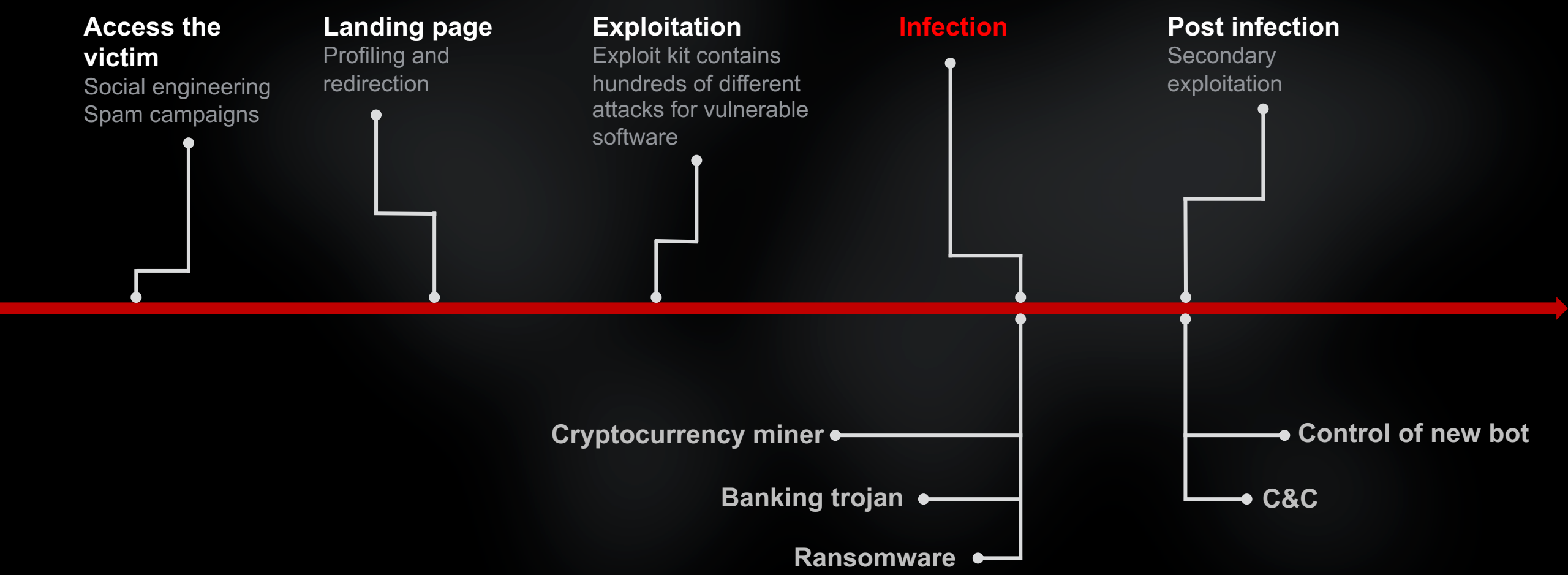
- **Ransomware**
- **Cryptojacking**
- Server side – app server
- Client side – web browser

Data

- **Theft**
- Credentials
- Personal Data
- **Resale**
- Intellectual Property
- Credentials

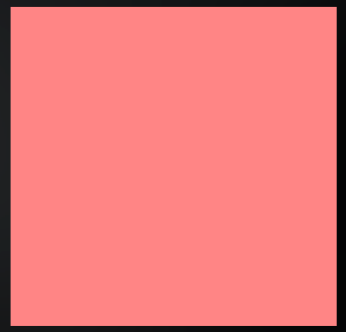
ILLUSTRATION: SIMON PRADES FOR BLOOMBERG BUSINESSWEEK

Exploit Kits



Changing Attack Methods

Exploit Kits



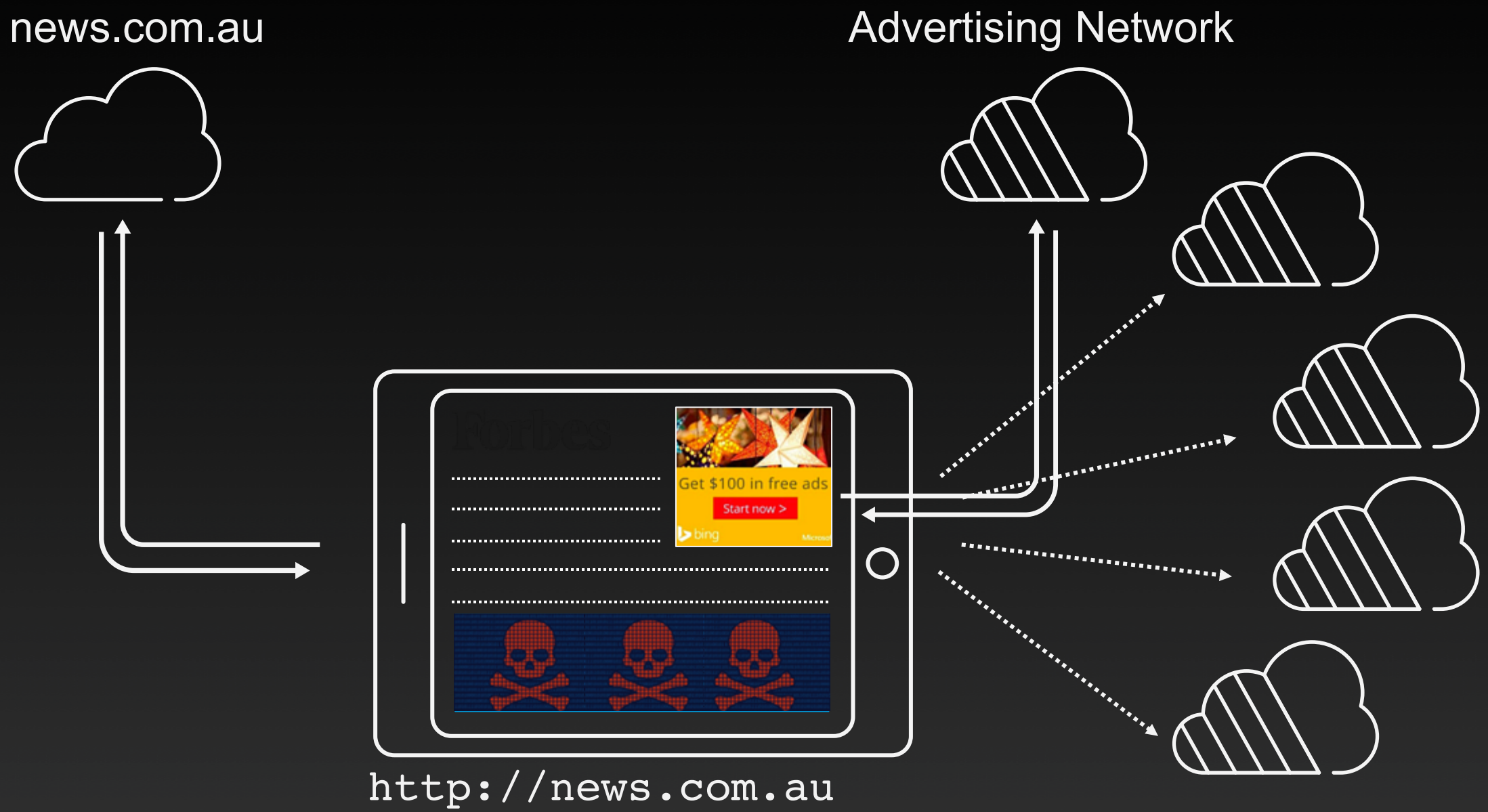
Web Injections

Software
supply-chain

Phishing
Credential stuffing
Brute force

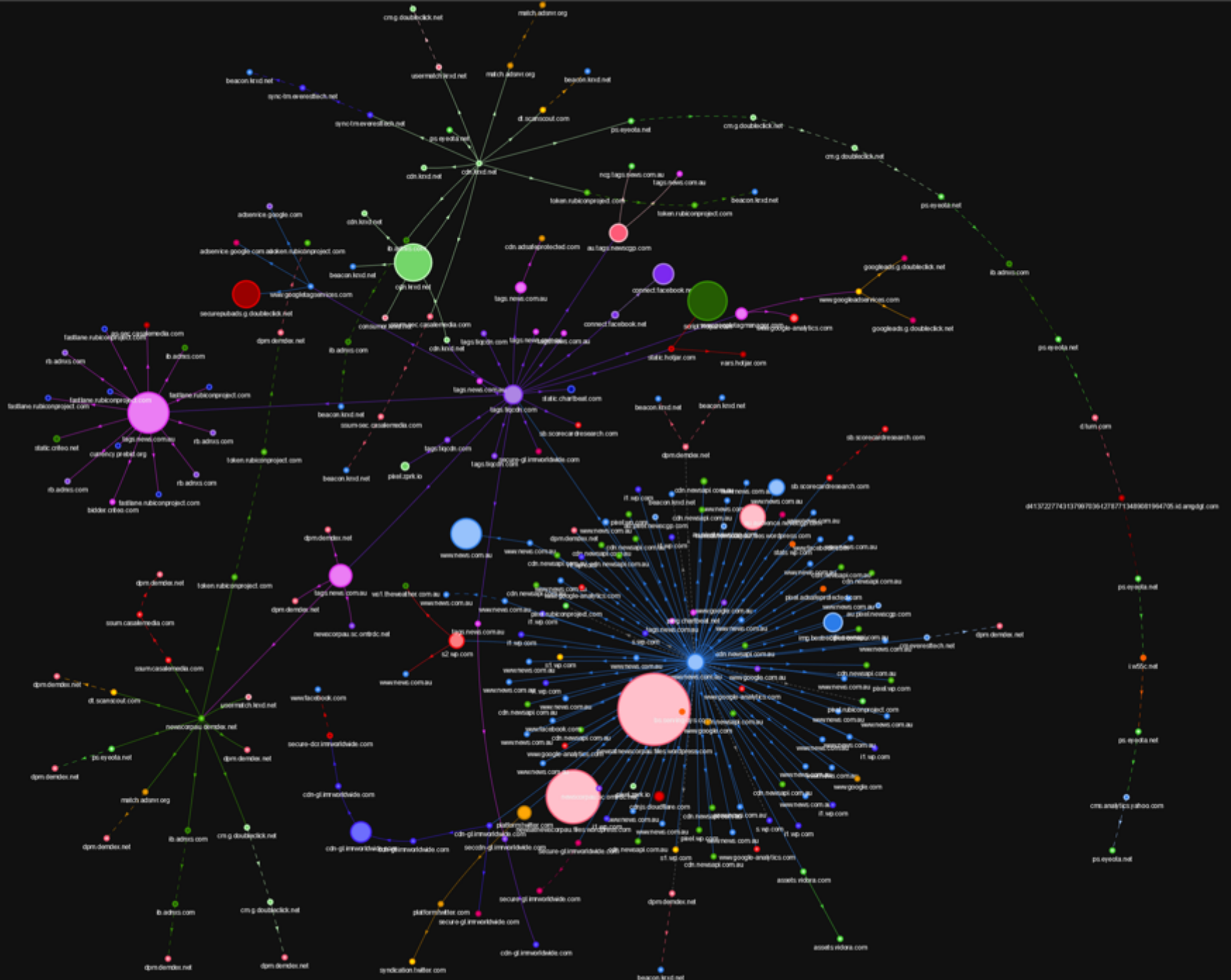
APP TIER

ACCESS TIER


news.com.au
Advertising Network
Get $100 in free ads
Start now >
bing
http://news.com.au

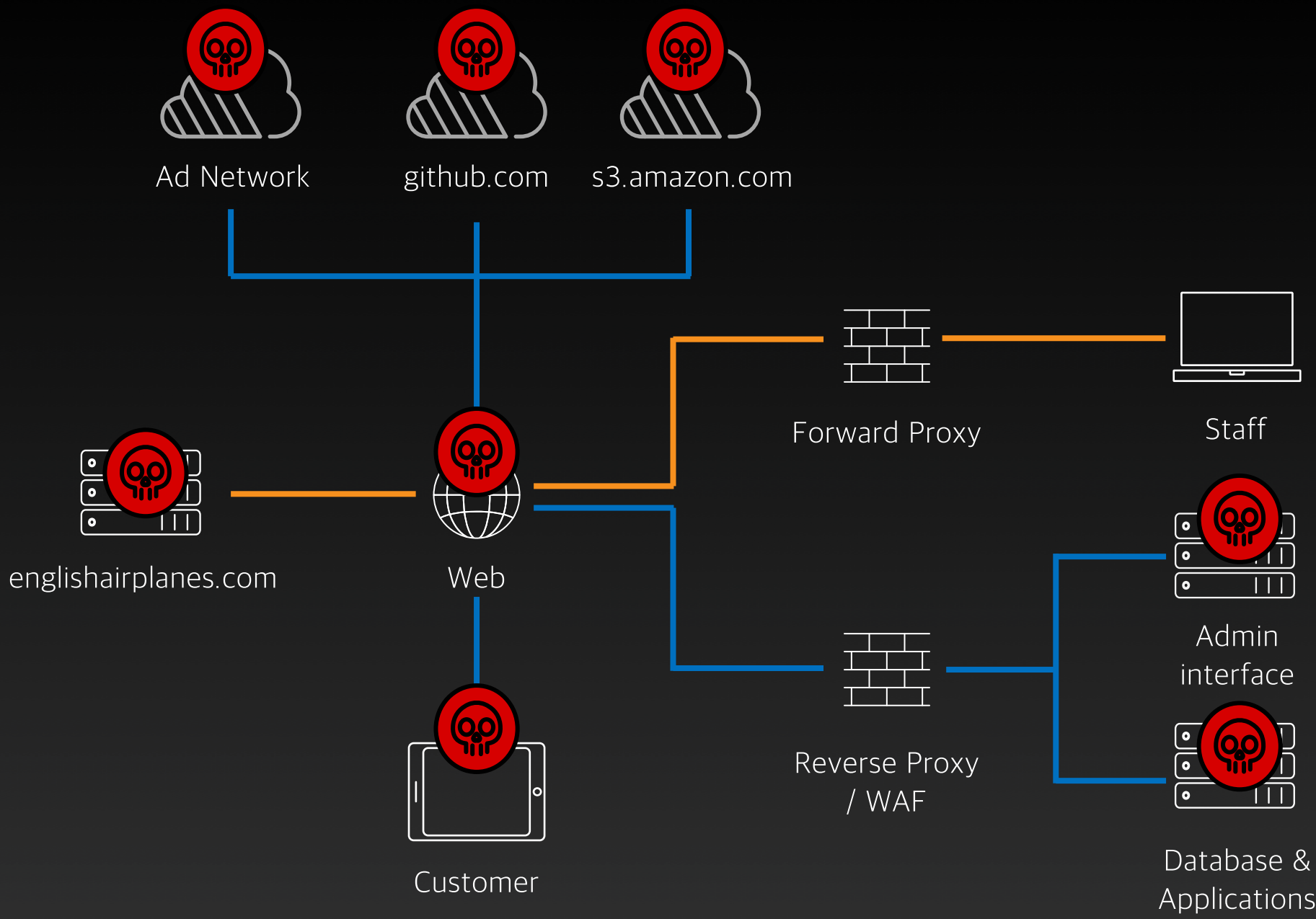
news.com.au

- 76 domains
- 73 third party



Injections

- Client (MITB, e.g. malware)
- Network (MITM of non-SSL/TLS traffic)
- Origin server
- 3rd party resource provider
- Admin interface of shopping cart software



In 2018

71% of web attacks

12% of all breaches

Payment cards stolen:

1,396,969

https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019--episode-3--web-injection-attacks

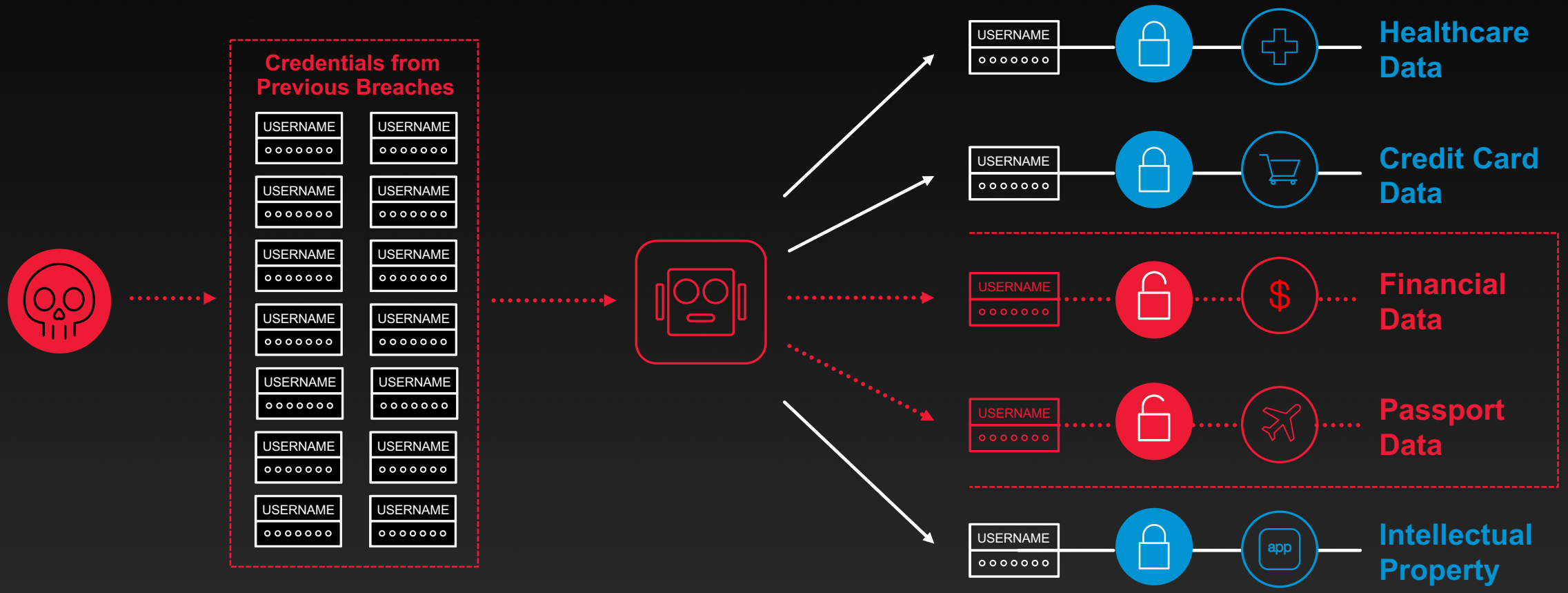
2018 Breaches in Retail, Tech and Manufacturing

#1 root cause:

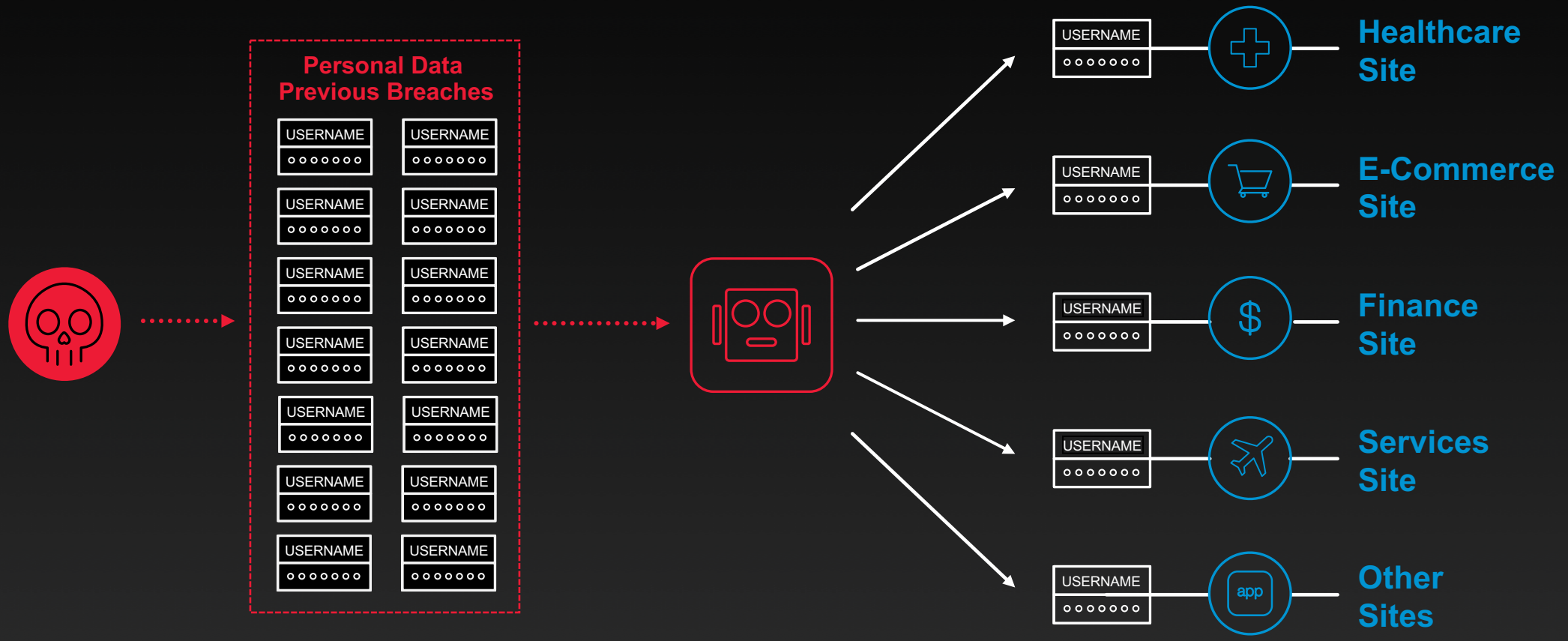
Magecart

https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019--episode-3--web-injection-attacks

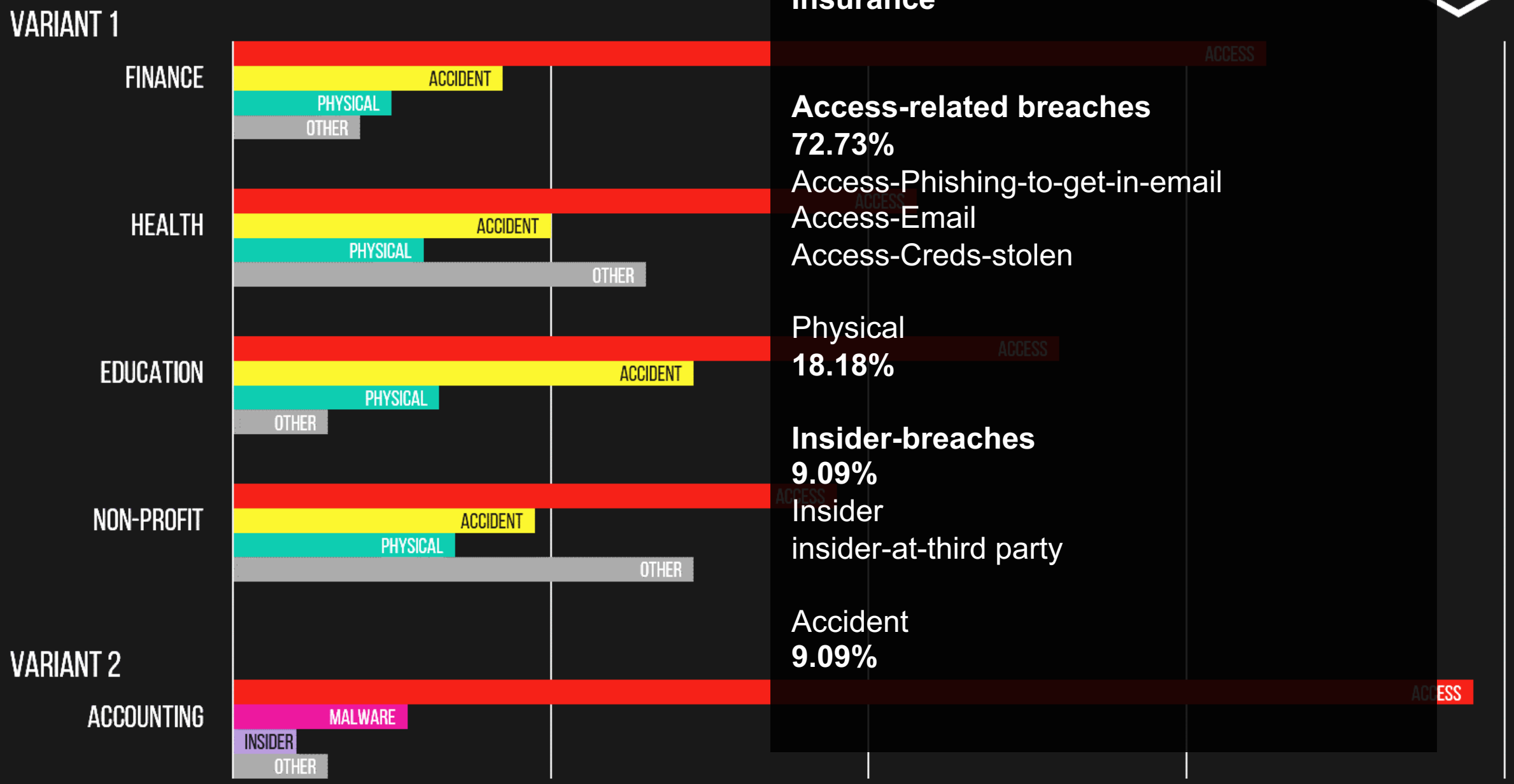
Credential Stuffing Attacks



New Account Creation Attacks



BREACH CAUSE PROFILES: PHISHING



Insurance

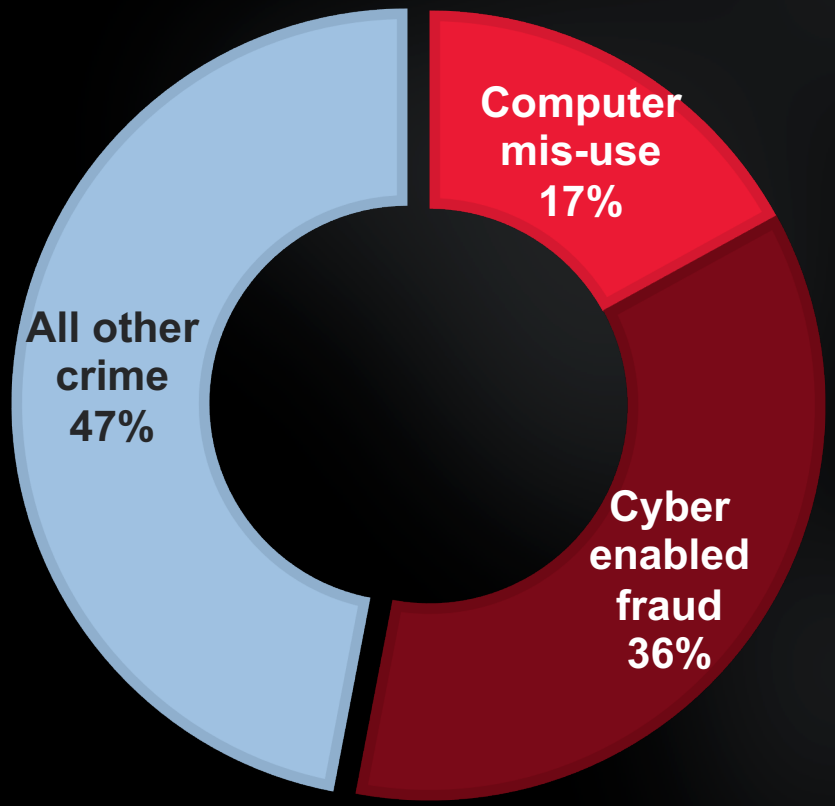
Access-related breaches
72.73%
Access-Phishing-to-get-in-email
Access-Email
Access-Creds-stolen

Physical
18.18%

Insider-breaches
9.09%
Insider
insider-at-third party

Accident
9.09%

UK (2016)



NCA Cybercrime Assessment 2016

Europe (2018)

Email threats

UK: attachments
Ireland: malicious URL
EU: Phishing
Spam: from France, Germany

Compromised IoT

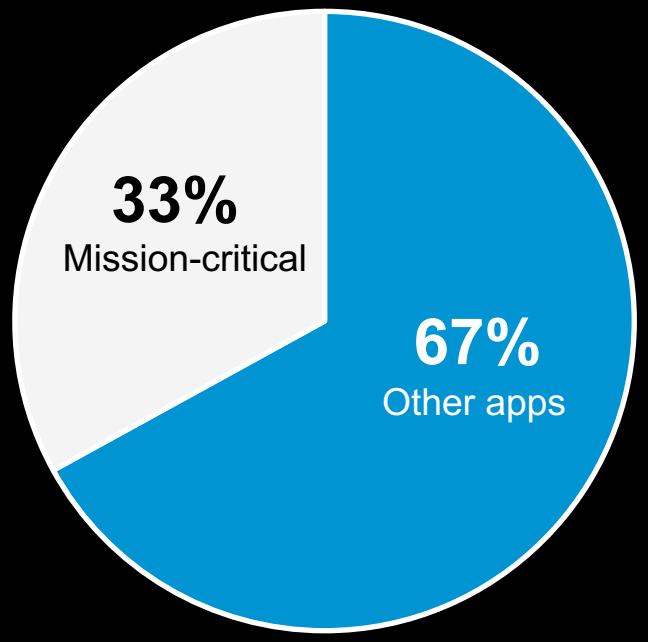
Payment Fraud

Europe vs Europe

Europol Internet Organised Threat Assessment 2018

Every Application Must Be Protected

NOT JUST THE MISSION-CRITICAL ONES



Large finance org

- Millions of customer records exfiltrated
- Billions in damages, market cap – CEO fired
- Entry point through a single compromised server

Casino operator

- Customer database taken
- Most lucrative customers at risk
- Entry point through a digital thermometer in the lobby aquarium

Thank You

1. Europol Internet Organised Crime Threat Assessment (2018)
   https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018
2. NCA Intelligence Assessment: Pathways Into Cyber Crime (2016)
   http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file
3. NCA Cyber Crime Assessment (2016)
   http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
4. CREST Identify, Intervene, Inspire (2015)
   https://www.crest-approved.org/wp-content/uploads/CREST_NCA_CyberCrimeReport.pdf
5. Globaldot Bad Bots Report (2018)
   https://www.globaldots.com/wordpress/wp-content/uploads/files/GlobalDots-2018-Bad-Bot-Report.pdf
6. F5 Labs Hunt for IoT Report (2018)
   https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot--multi-purpose-attack-thingbots-threaten-intern
7. NCSC Cyber Crime - Understanding the Online Business Model (2017)
   https://www.ncsc.gov.uk/news/ncsc-publishes-new-report-criminal-online-activity
8. Check Point Security Report (2019)
   https://blog.checkpoint.com/2019/03/04/check-points-2019-security-report/
9. ThreatMetrix H2 2018 Cybercrime Report
   https://www.threatmetrix.com/info/h2-2018-cybercrime-report/
10. F5 Labs SOC data


F5
LABS