Digital Health Webinar June 2020

Using Threat Intelligence To Protect Digital Healthcare

PRESENTED BY:

F5 Networks

F5 Labs

Lancashire Teaching Hospitals NHS Foundation Trust

Neill Burton
Director, UK Channel
F5 sales

David Warburton
Senior Threat Research Evangelist
F5 Labs

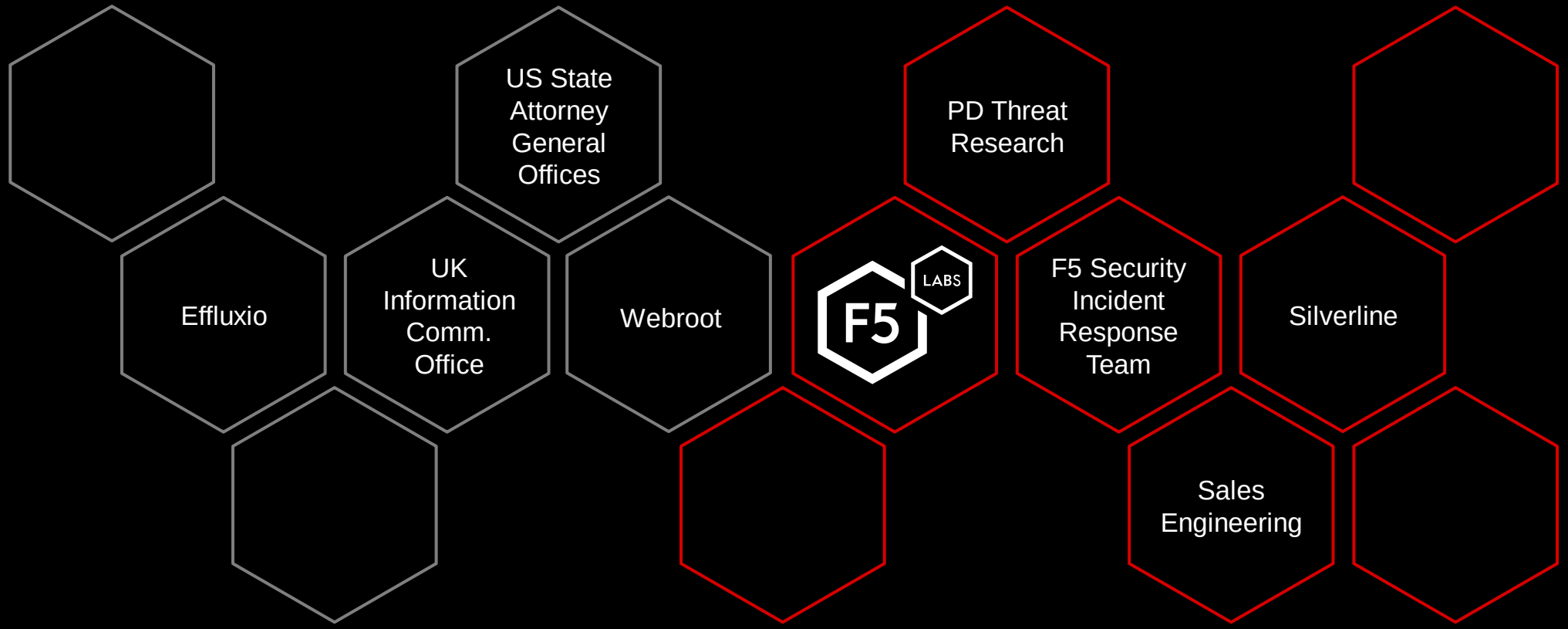
Saeed Umar
Head of Technical Services
Lancashire Teaching Hospitals
NHS Foundation Trust

Richard Harvey
Solutions Engineer
F5 sales

Security professionals researching threats and publishing intelligence, twice a week.

External Partners

F5 Teams



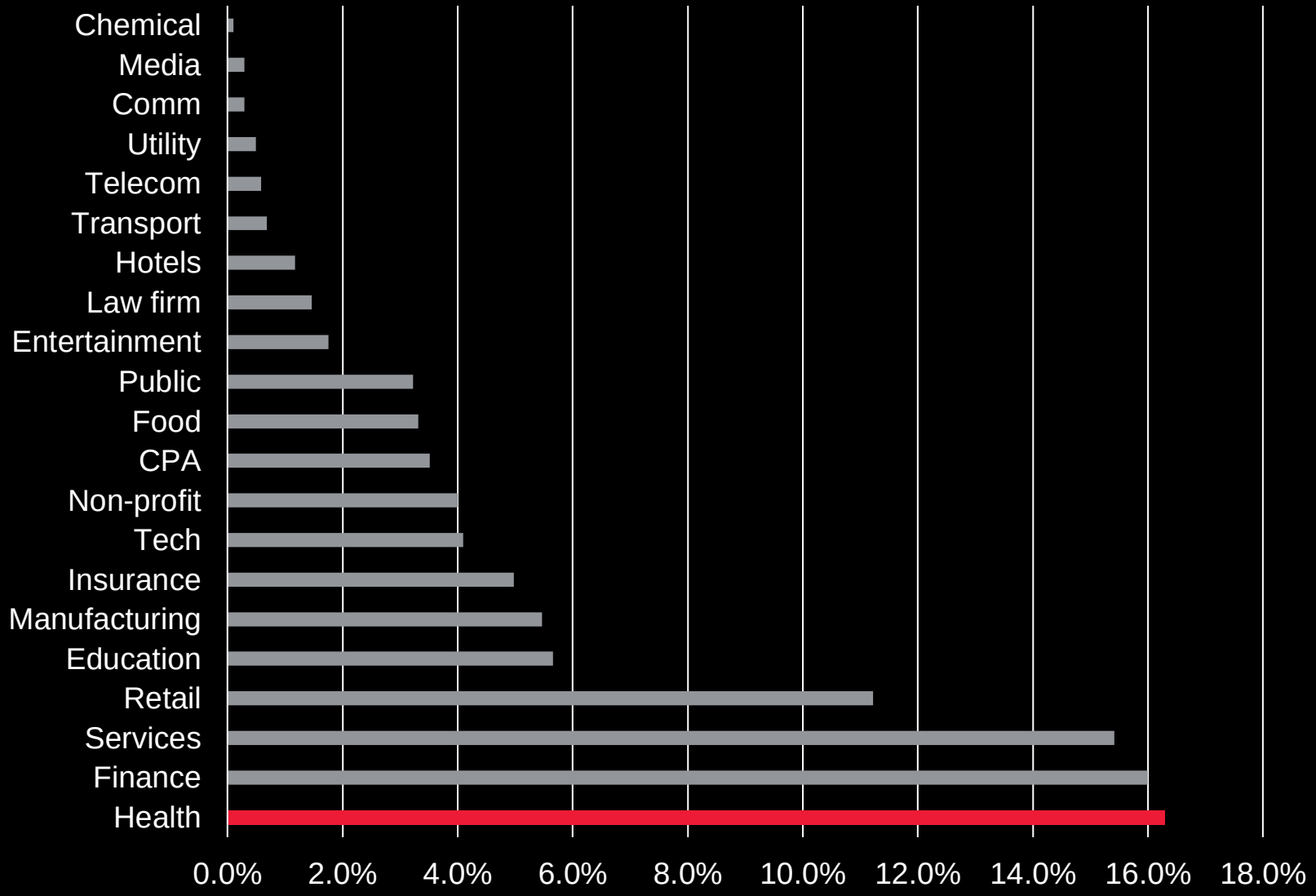
UK healthcare accounts for 18% of all breaches

ico.
Information Commissioner's Office

	Healthcare
2019 - 2020 Q4	16%
2019 - 2020 Q3	19%
2019 - 2020 Q2	20%
2019 - 2020 Q1	16%
2018 - 2019 Q4	16%

[1] ICO Data security incident trends

2019 US Breaches by Sector



Breach Analysis

State Attorney General

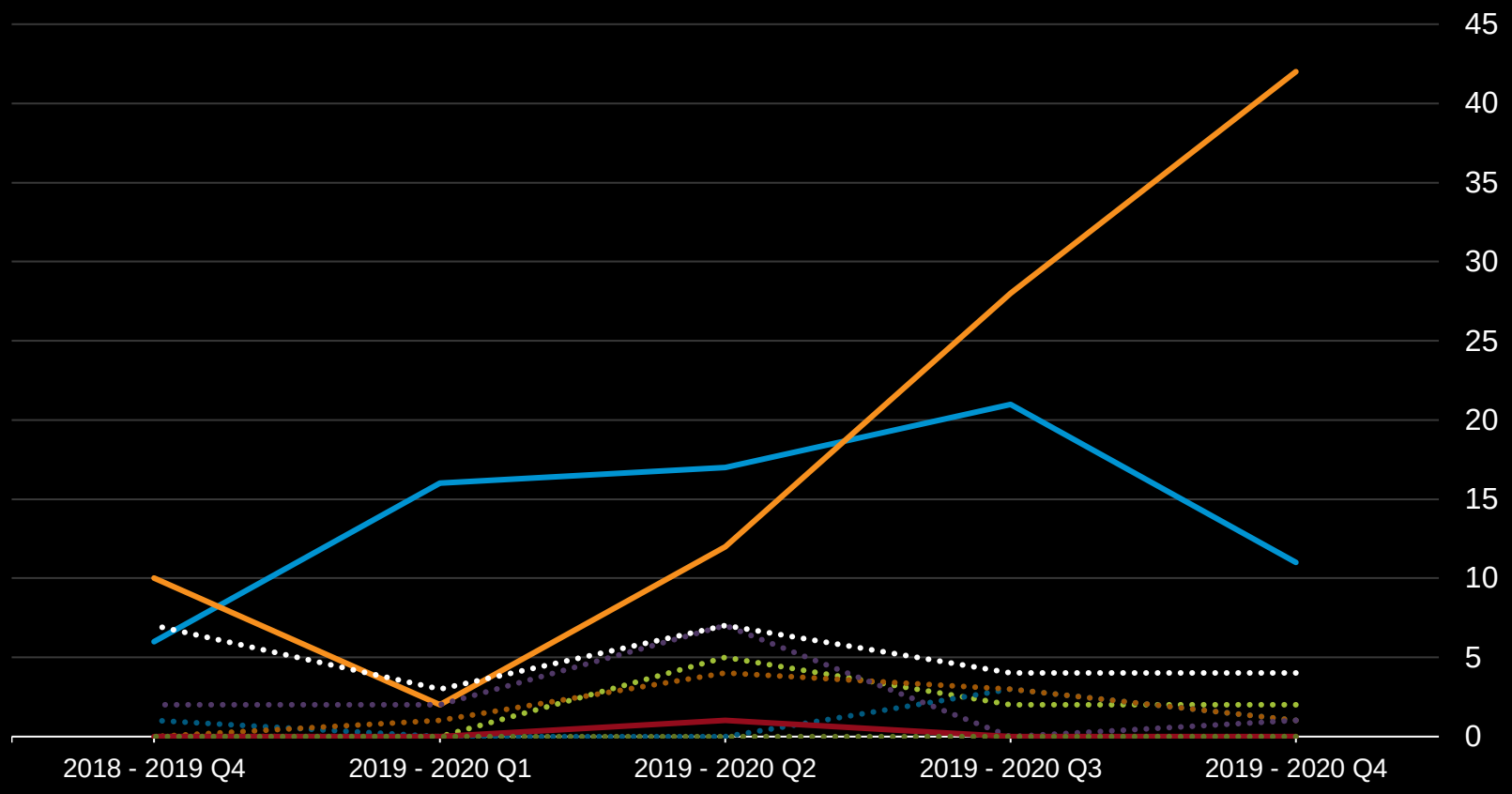
1025

Cases 2019

85%

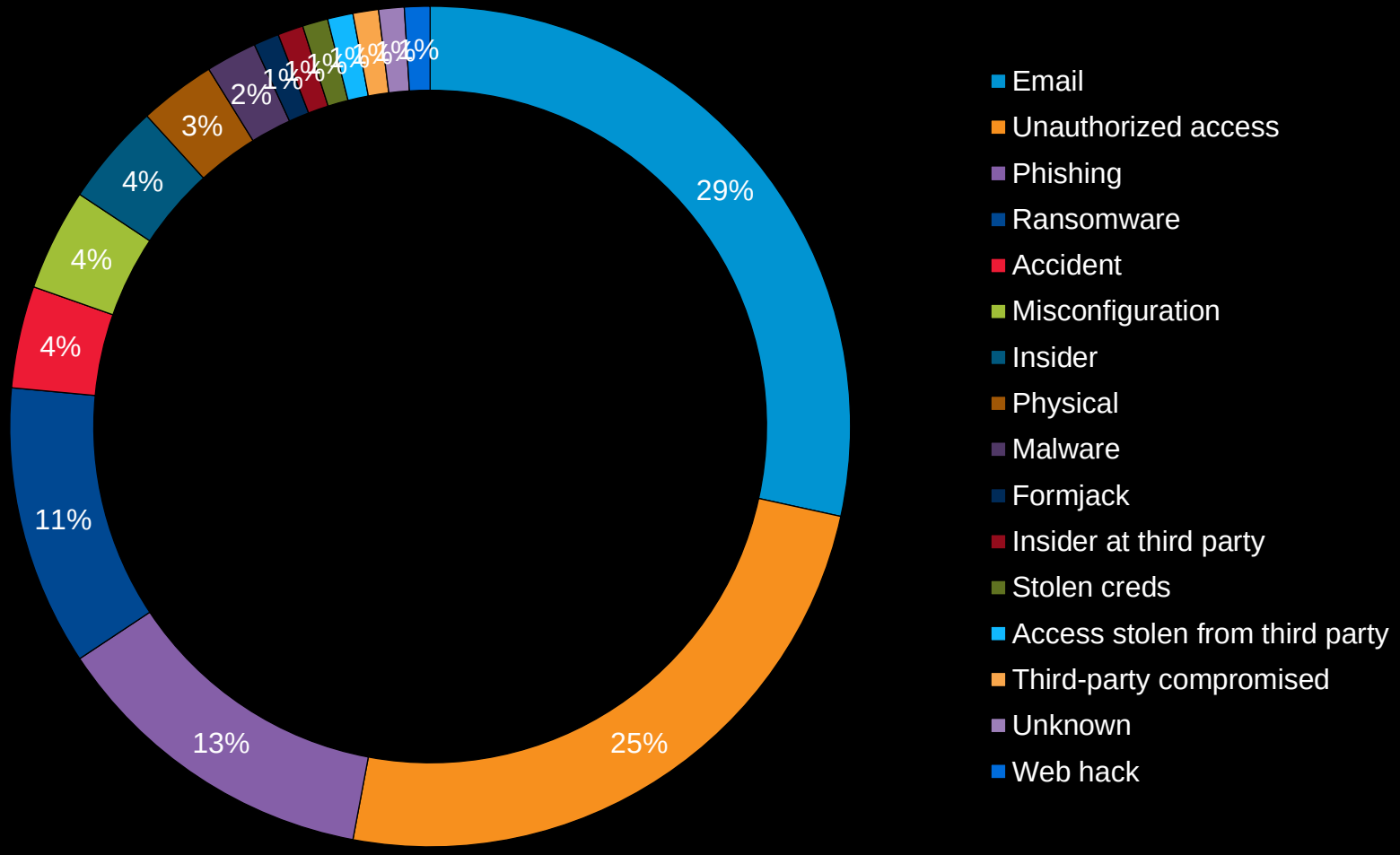
Had explanations

UK Healthcare breaches



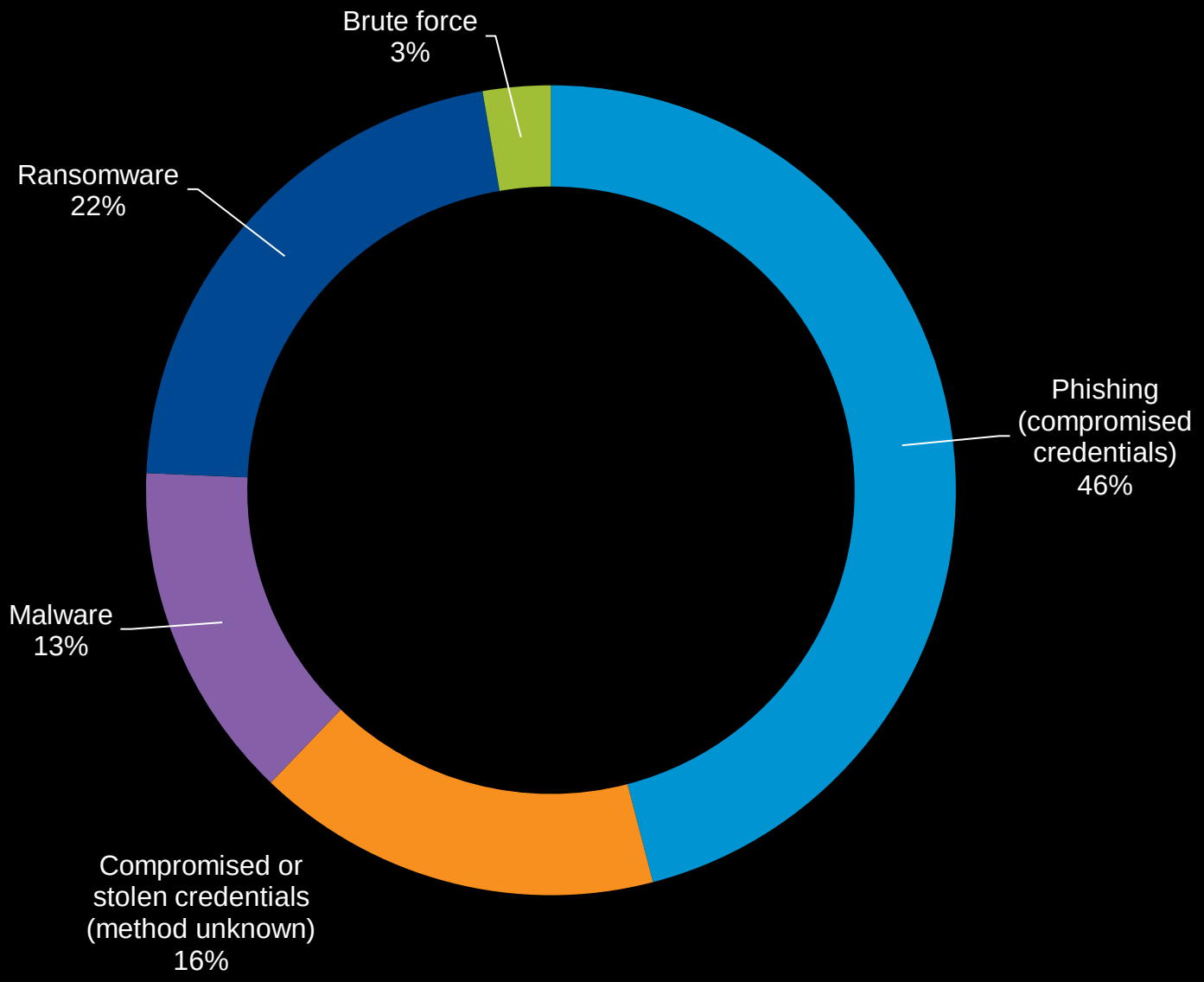
- Phishing
- Unauthorised access
- Data of wrong data subject shown in client portal
- Hardware/software misconfiguration
- Malware
- Other cyber incident
- Ransomware
- Brute Force
- Denial of service

2019 US Healthcare Breaches



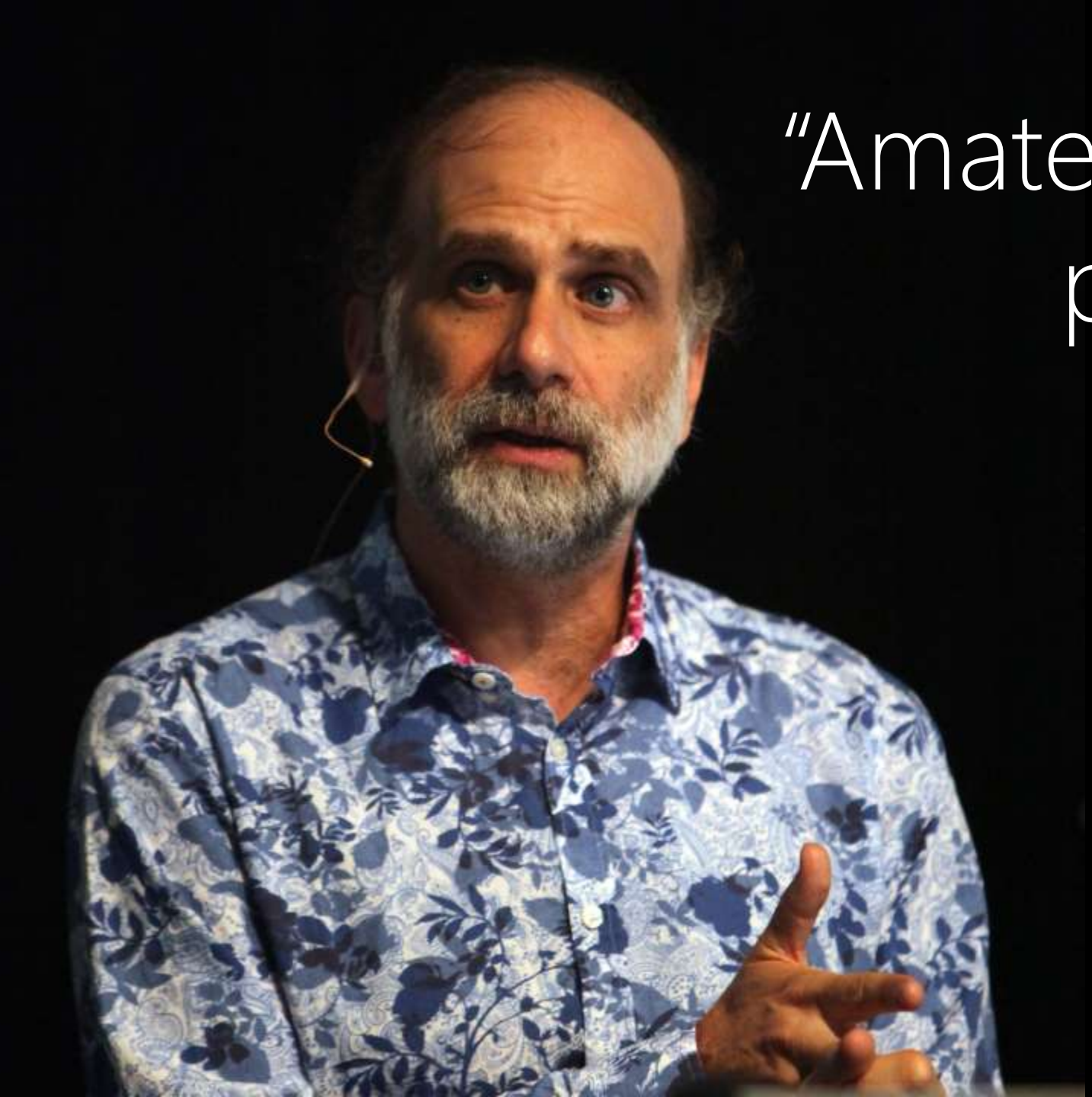
- Healthcare account for 16% of all breaches in US
- 42% social engineering
- Email and access account for 54%
- Insiders only 7 incidents

2019 Oz Healthcare Breaches



ACSC Australian Cyber Security Centre

- Healthcare top again with 22% of all breaches
- Phishing and use of compromised credentials account for majority of breaches
- Email inboxes contain sensitive personal data
- 54% of breaches were due to criminal and malicious activity



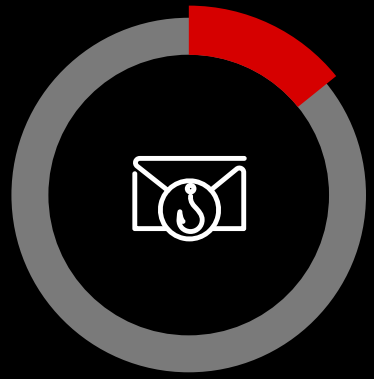
"Amateurs hack systems, professionals hack people"

- Bruce Schneier

2019 Access Attacks Broken Down

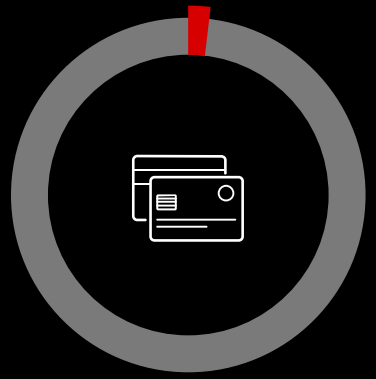
32.8%

Email cited as cause



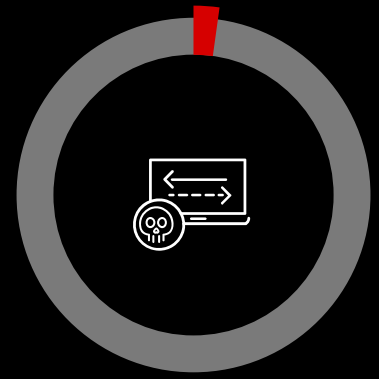
14.2%

Phishing gain access to email



1.9%

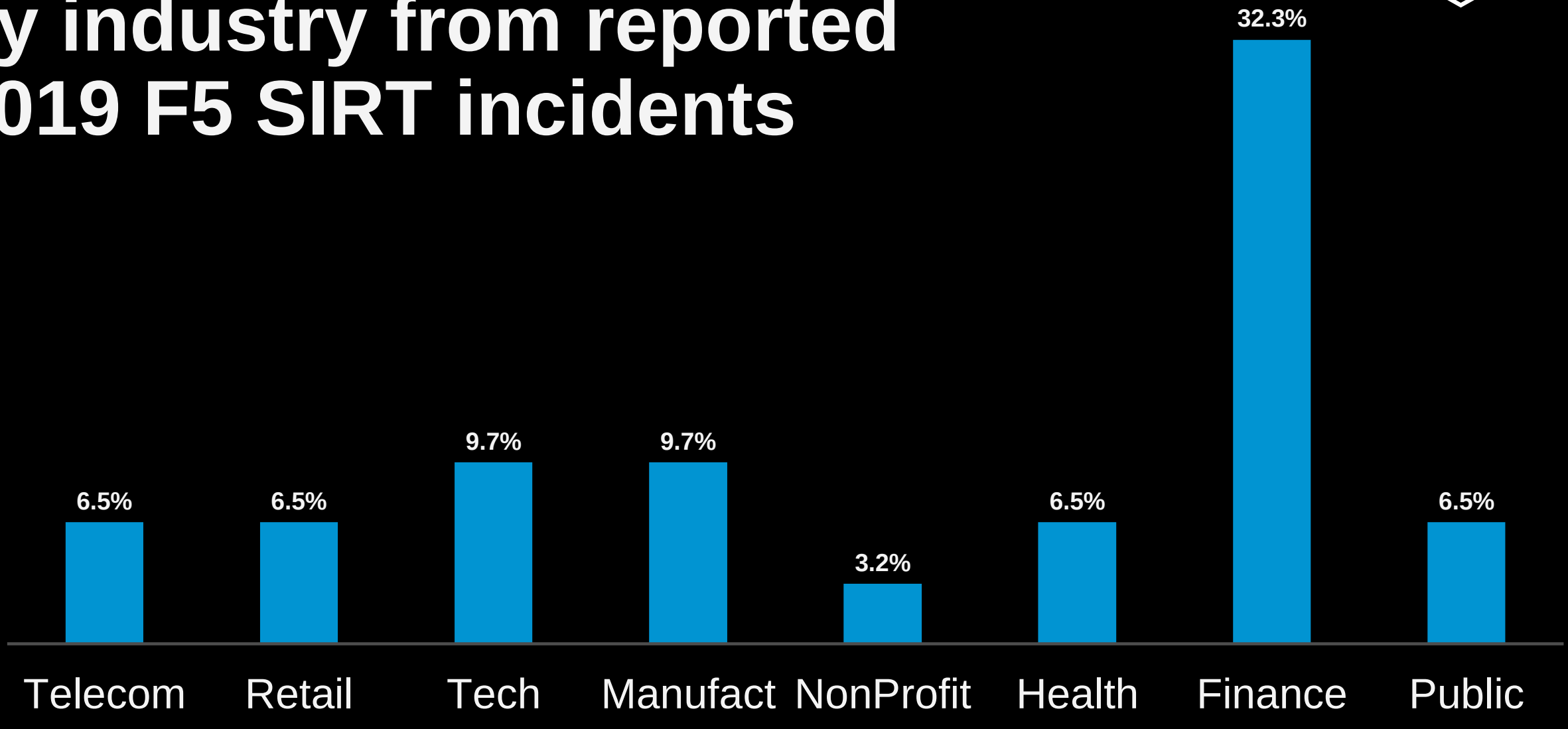
Access creds stolen



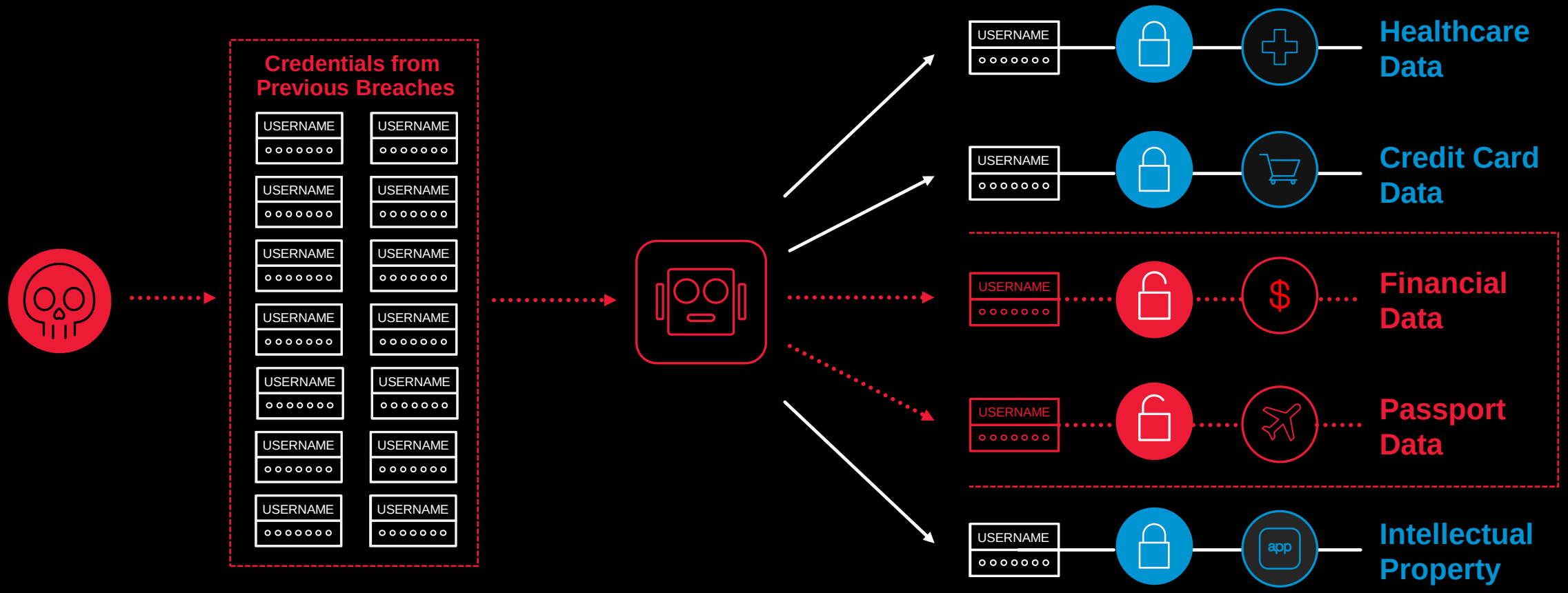
2.2%

Access cred stuffing and brute

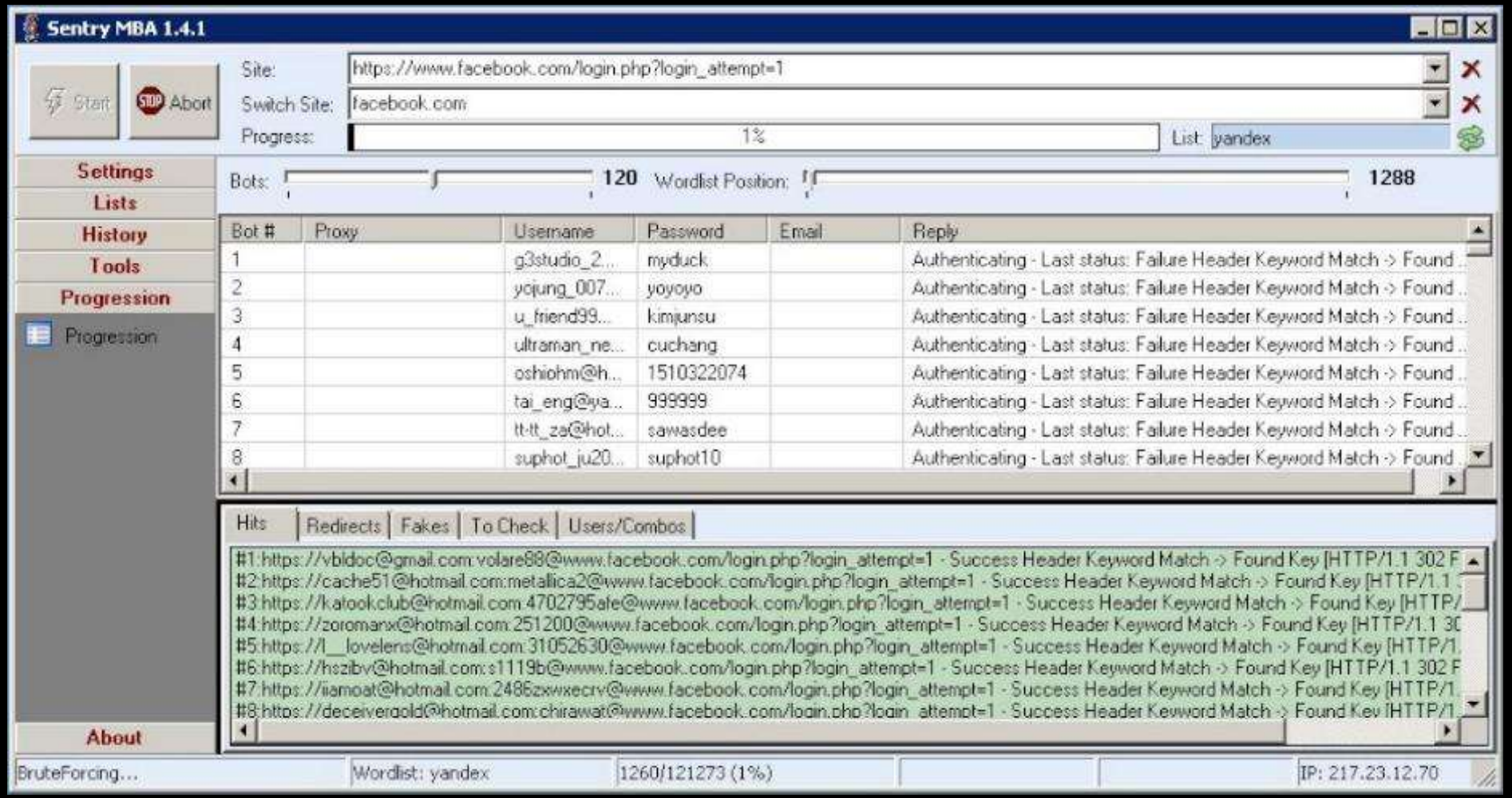
Brute Force attacks by industry from reported 2019 F5 SIRT incidents



Credential Stuffing



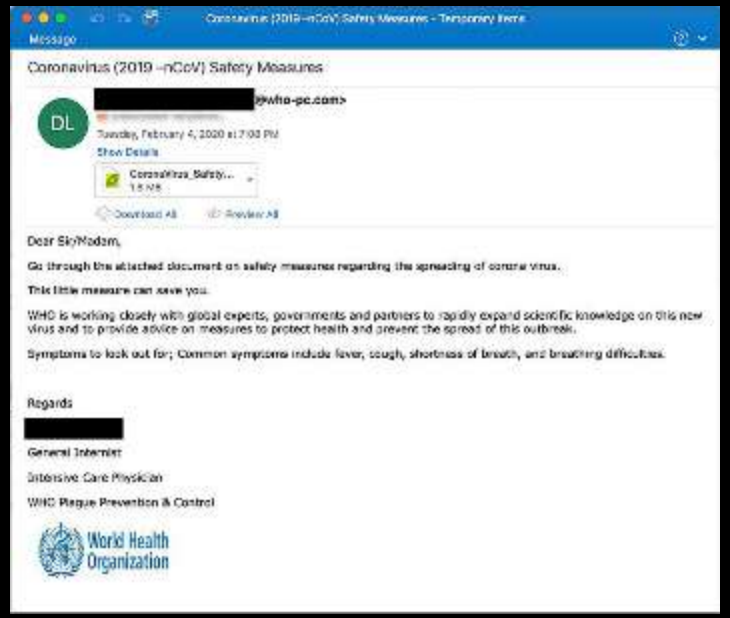
Credential Stuffing

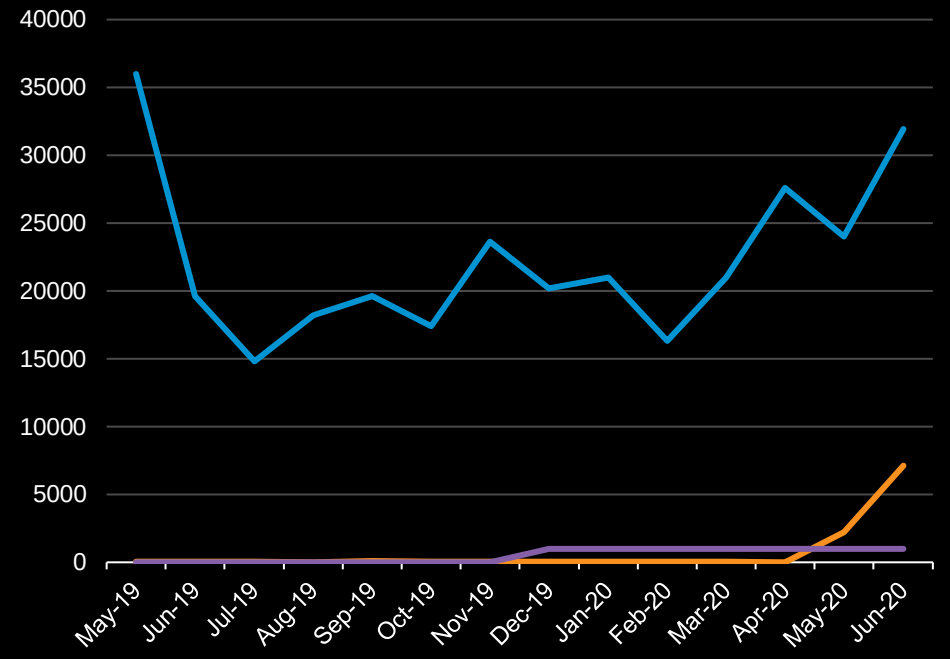


Threat Actors using COVID-19

Phishing Attacks Impersonating Health Authorities

- WHO
- Public Health Offices (CDC)
- Revenue Agencies
- Human Rights offices
- Charities
- Unicef
- WSJ
- FedEx





APTS **CYBERCRIME**

IoT Driving COVID Variants

2017

1TB

DEVICES

Softbank

2020

3B

*Excludes smartphones, tablets, and computers

IoT Driving COVID Variants

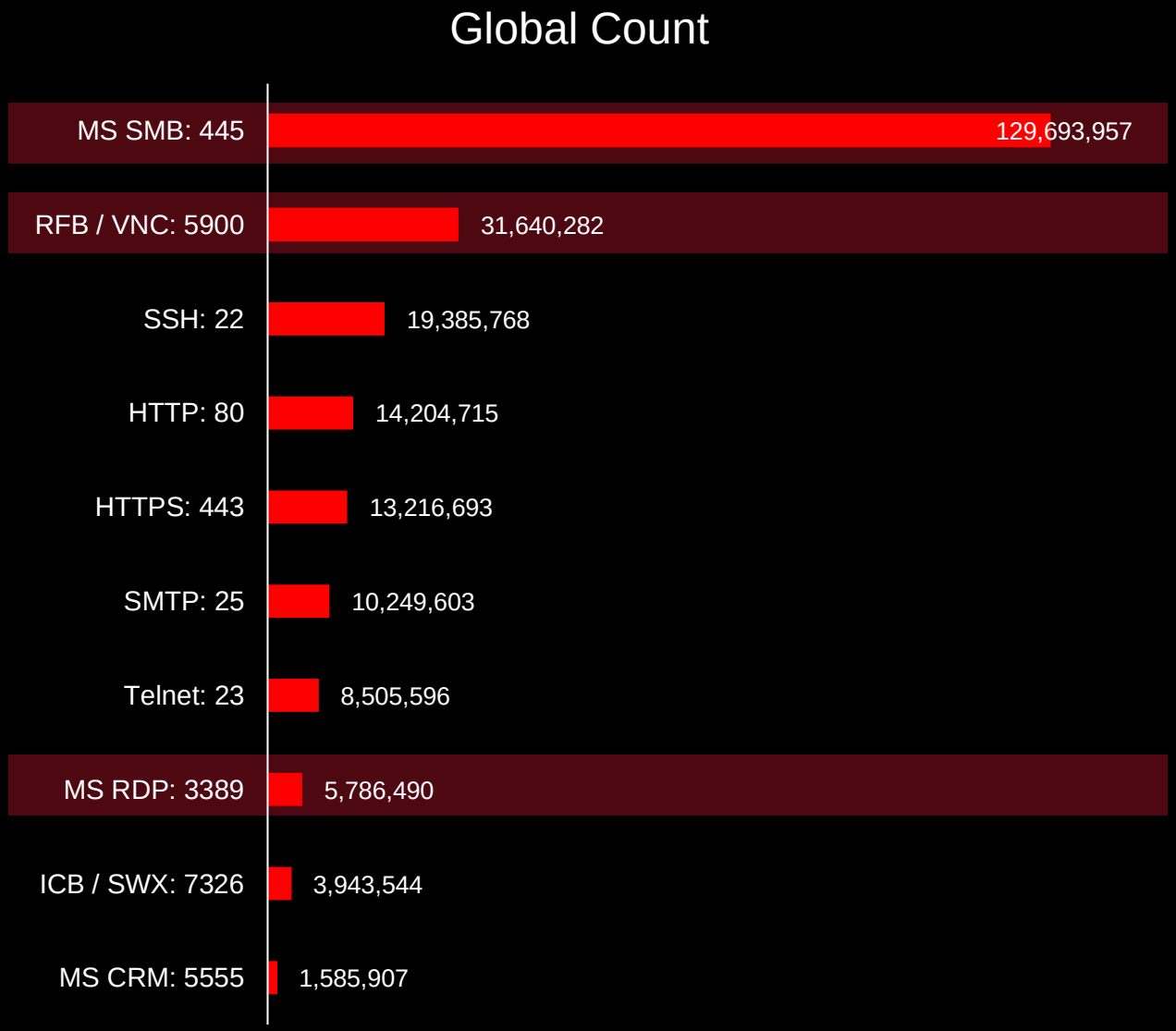
< 45 minutes

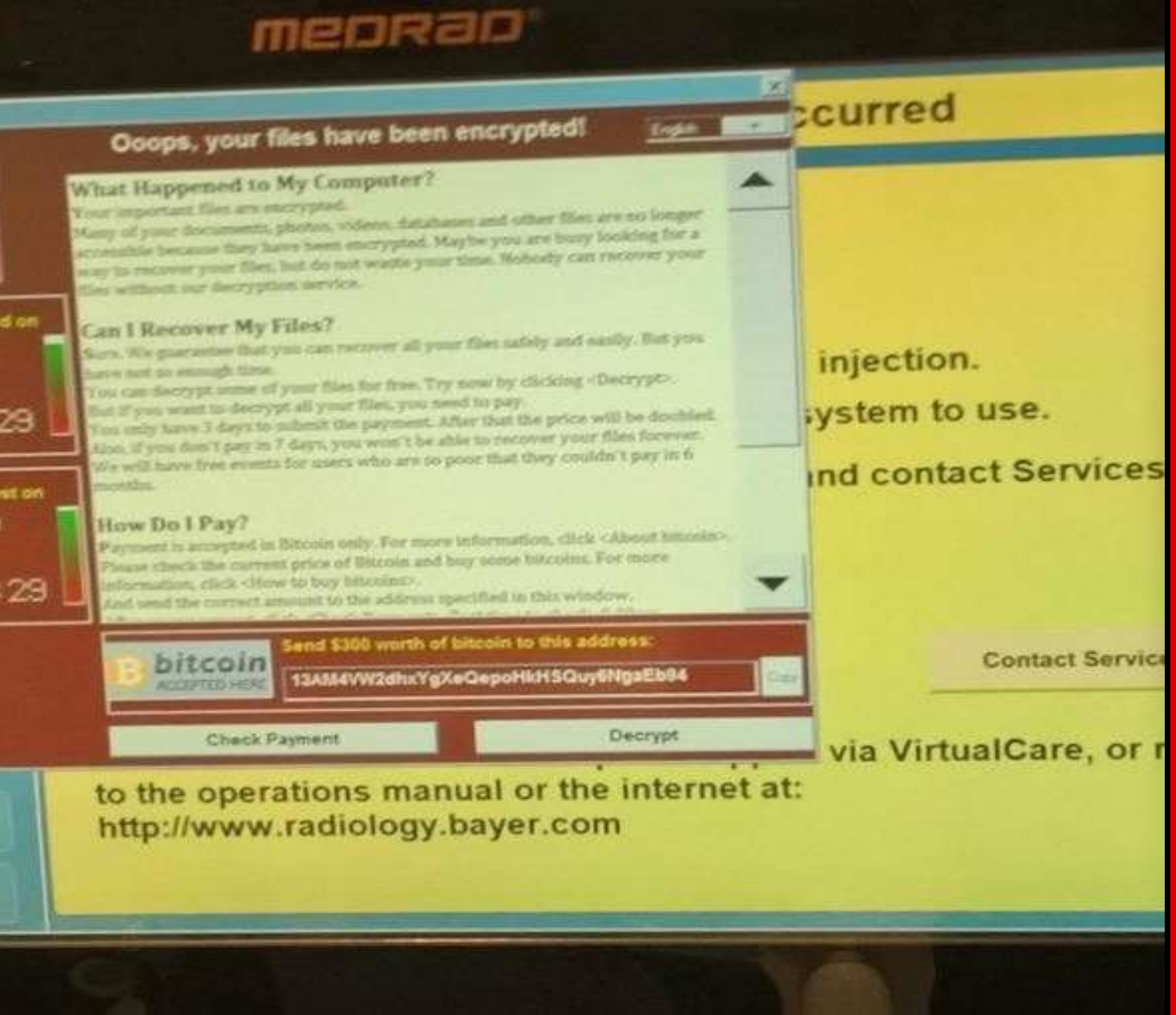
1. 3 mins
   Find source code (Pastebin search)
2. 30 mins
   Weaponize
3. 10 mins
   Validate everything is working properly

Various Bots and Bot Services for Hire

SERVICE	BITCOIN (Typical price range listed along with the highest listed price)	USD (Typical price range listed along with the highest listed price)
HACKING WEB SERVER (VPS OR HOSTING)	0.034 - 0.0449, 0.47	$220 - $500, $3,000
SETTING UP KEYLOGGER	0.0263	$170
DDOS (PRICES MAY VARY)	0.0534, 0.078 - 0.39	$350, $500 - $2,500
HACKING PERSONAL COMPUTER	0.0364, 0.044 - 0.55	$280, $500 - $3,500
HACKING CELL PHONES	0.047 - 0.093	$300 - $600
EMAIL HACKING	0.078 - 0.12	$500 - $800
SOCIAL MEDIA ACCOUNT HACKING	0.0352, 0.054 - 0.11	$230, $350 - $700
CHANGE SCHOOL GRADES	0.19 - 0.58	$1,200 - $3,750
FUD RANSOMWARE + DECRYPTER	12 MO / 0.14 6 MO / 0.076 1 MO / 0.019	12 MO / $900 6 MO / $490 1 MO / $120

Top Targeted Ports Q4 2019





WannaCry

- Wormed ransomware able to spread to connected devices
- Bayer MedRad device used to assist in MRI scans
- Radiography, mobile X-ray and mammography products from Siemens Healthineers

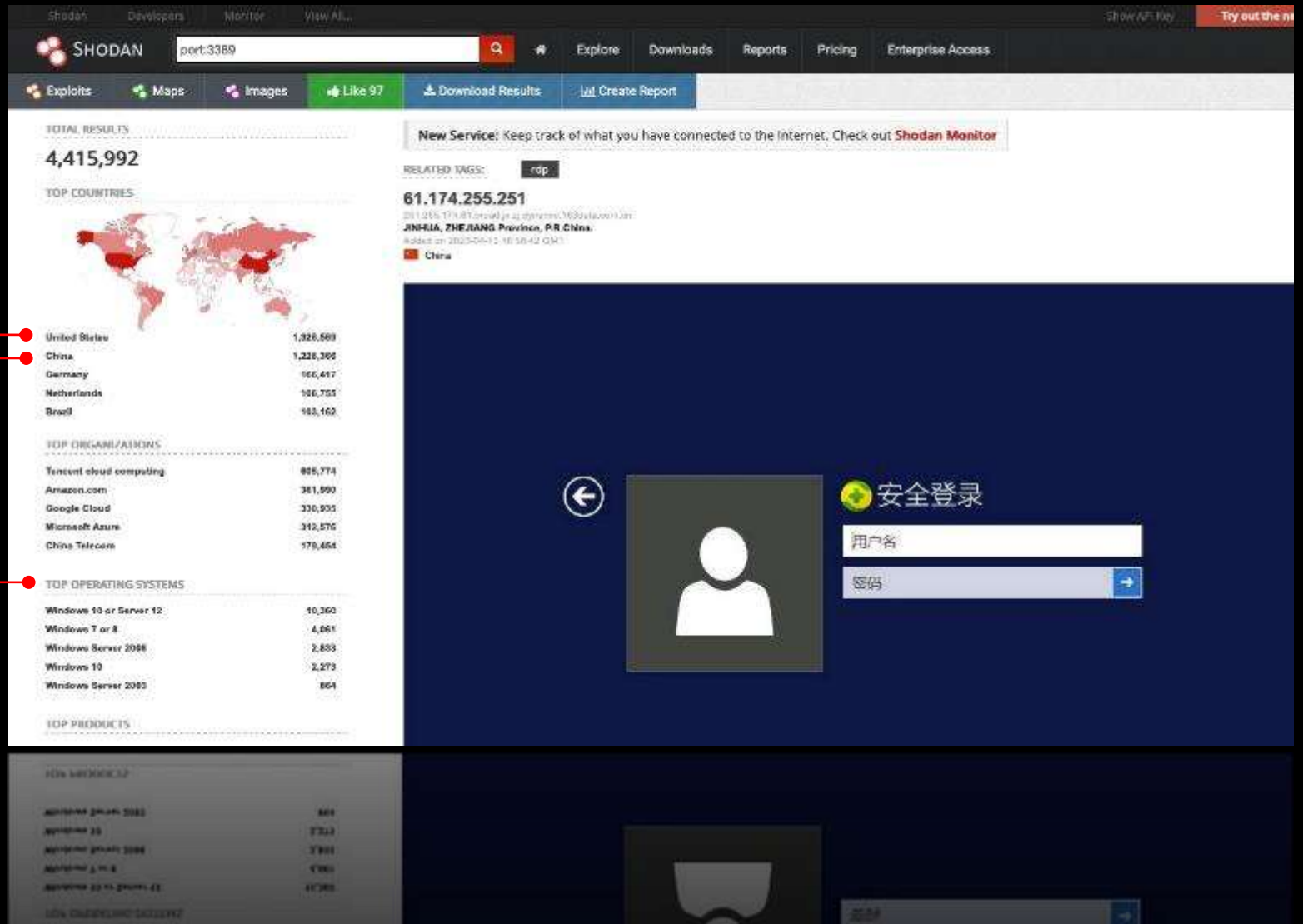
It’s not about you, it’s how you look.

If Shodan can find you…

US
AWS
Google Cloud
Azure

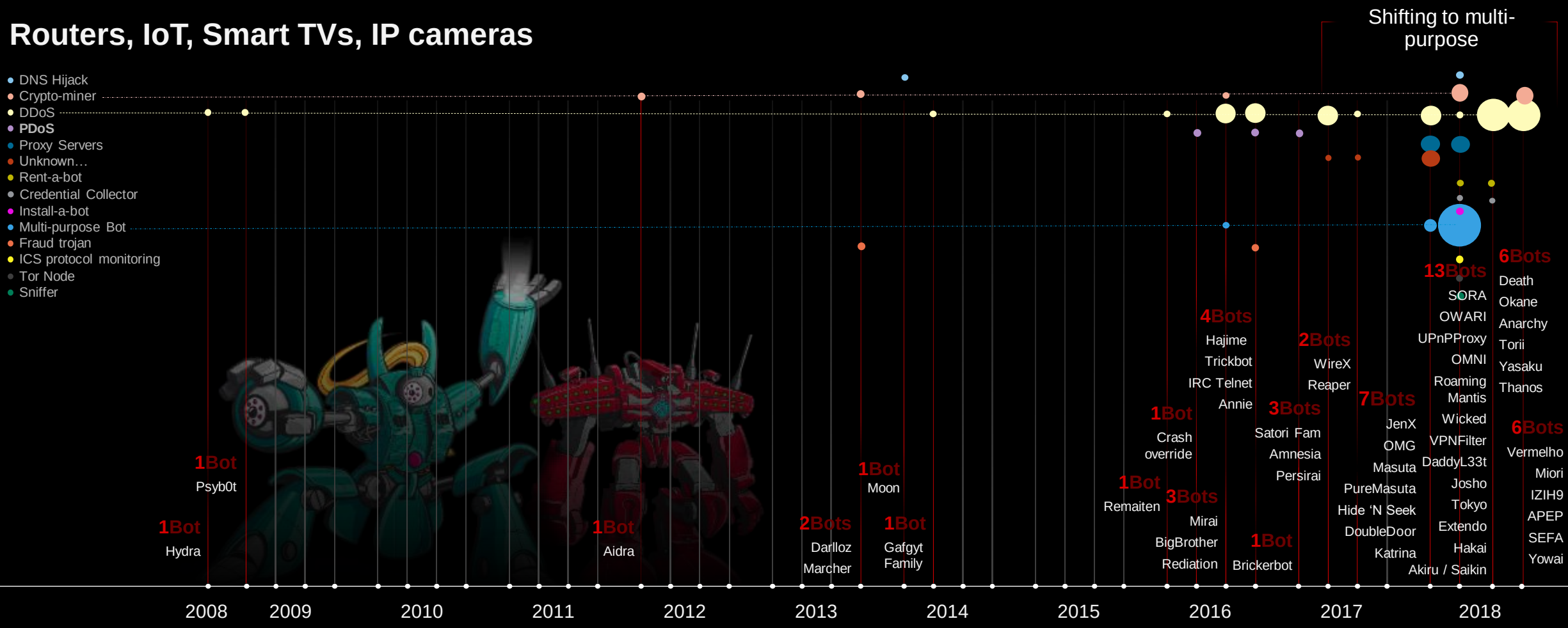
China
Tencent
China Telecom

Terminal Servers?
Shifted workloads to the cloud?

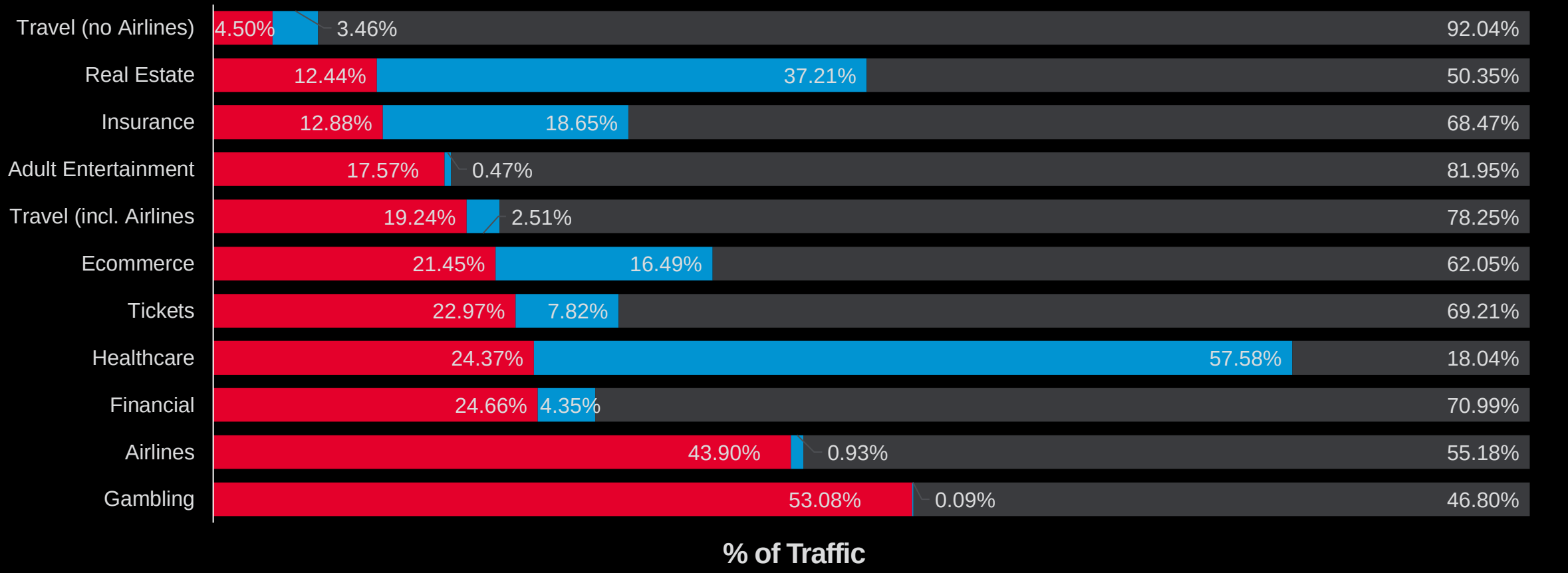


Bad Bots

Routers, IoT, Smart TVs, IP cameras



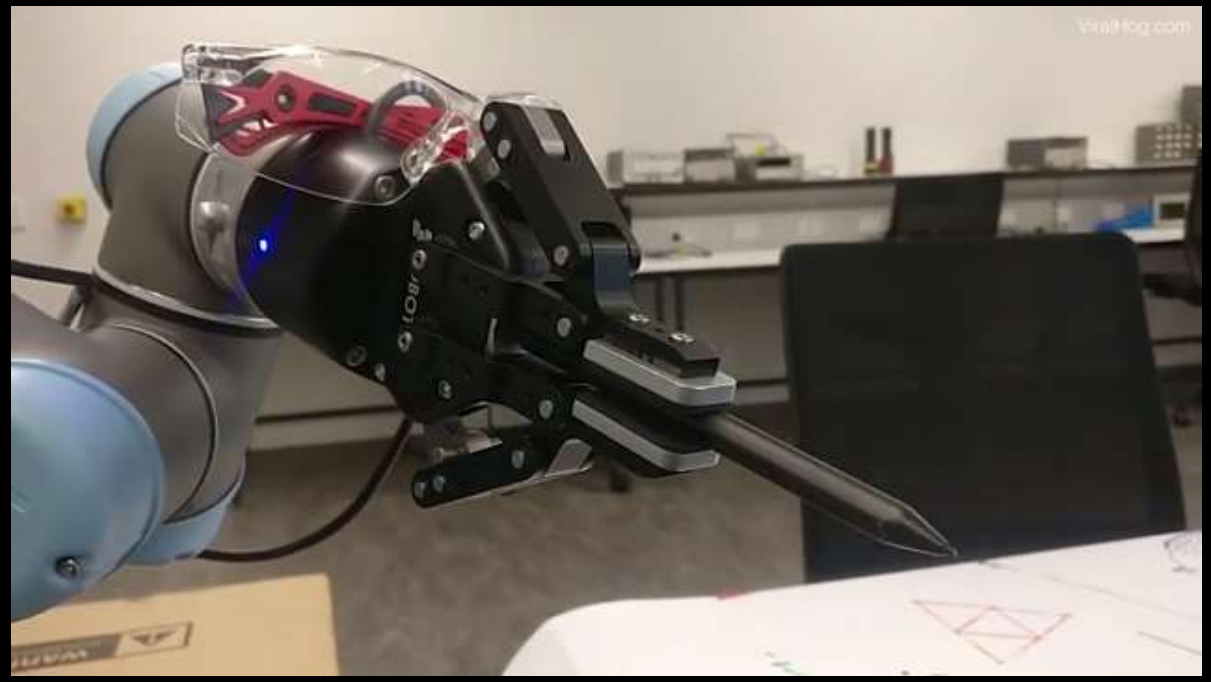
Bots by Industry

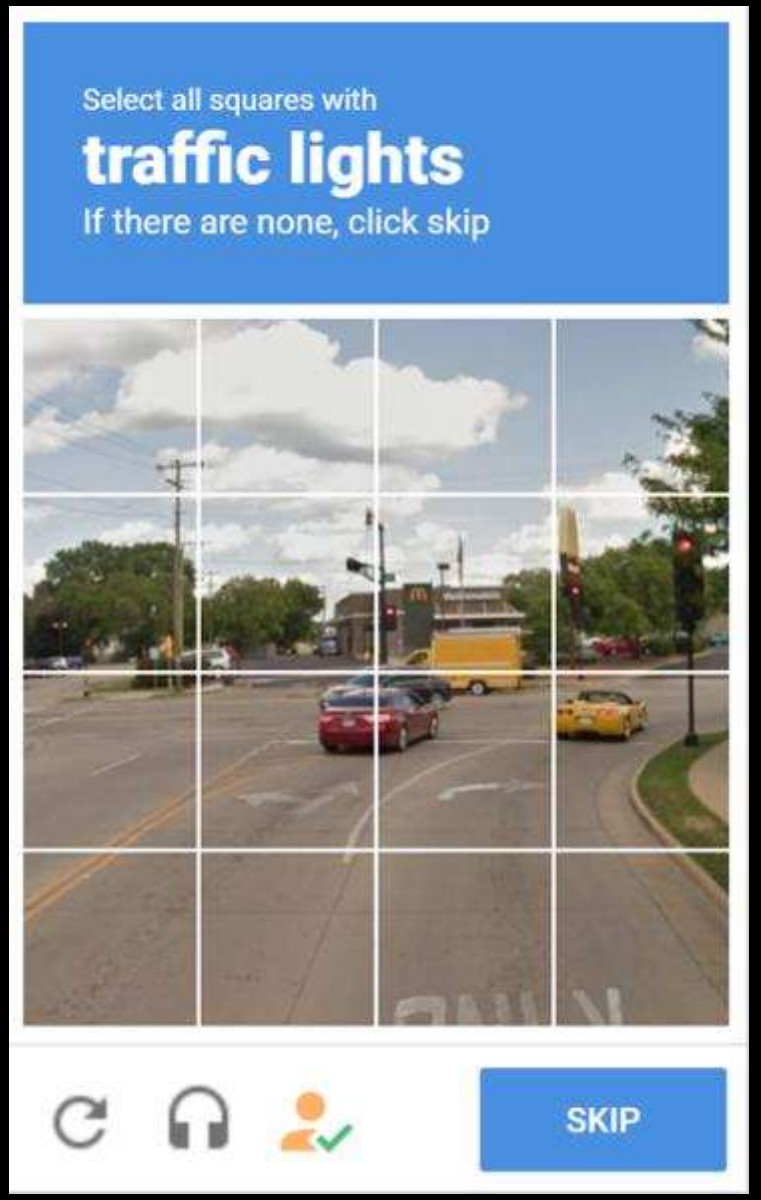


Source: GlobalDots Bad Bot Report 2018

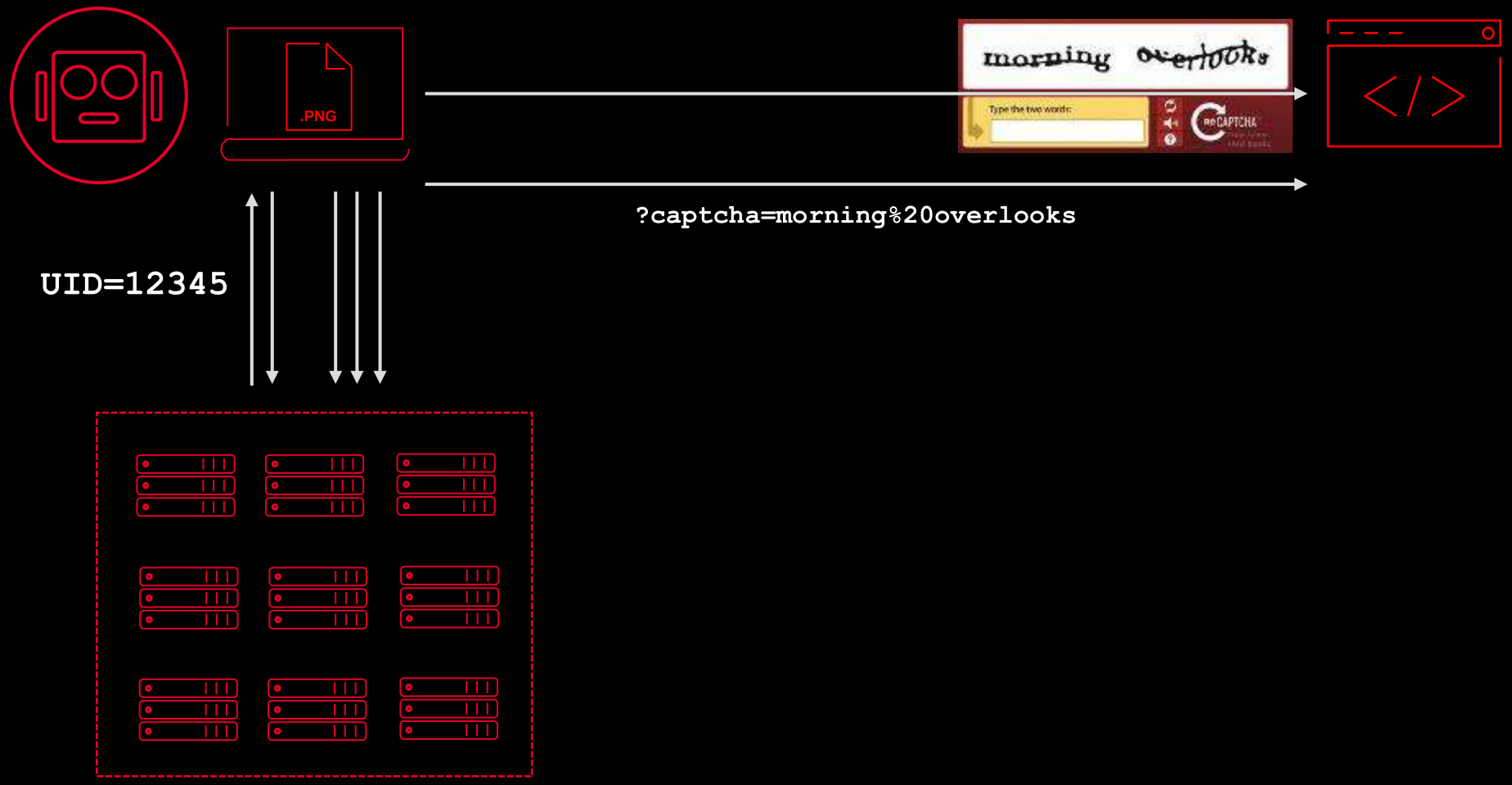
CAPTCHA


morning
overlooks
Type the two words:
reCAPTCHA
stop spam.
read books.




Select all squares with
traffic lights
If there are none, click skip
SKIP

Automated CAPTCHA Solvers



Architecture Changes Driven by Pandemic Response

Attacks go after easy targets

Rapid increase of remote access

Rapid expansion of unplanned remote access can introduce over privileged risks

Increased risk of pivoting attacks

Working “offline” drives more local PII storage

Allowing BYOD authentication to corp network

VPN exposure publicly up 33%

Lack of posture assessments with BYOD

Can’t secure internet connection of remote assets when split tunneling.

Exposing login to internet attracts brute force, cred stuffing and DoS attacks.

RDP (port 3389) exposure publicly up 41%

Publicly discoverable RDP hosts (in Shodan) are up 45% since Jan.

Exposing highly targeted ports publicly attracts brute force, cred stuffing and DoS attacks.

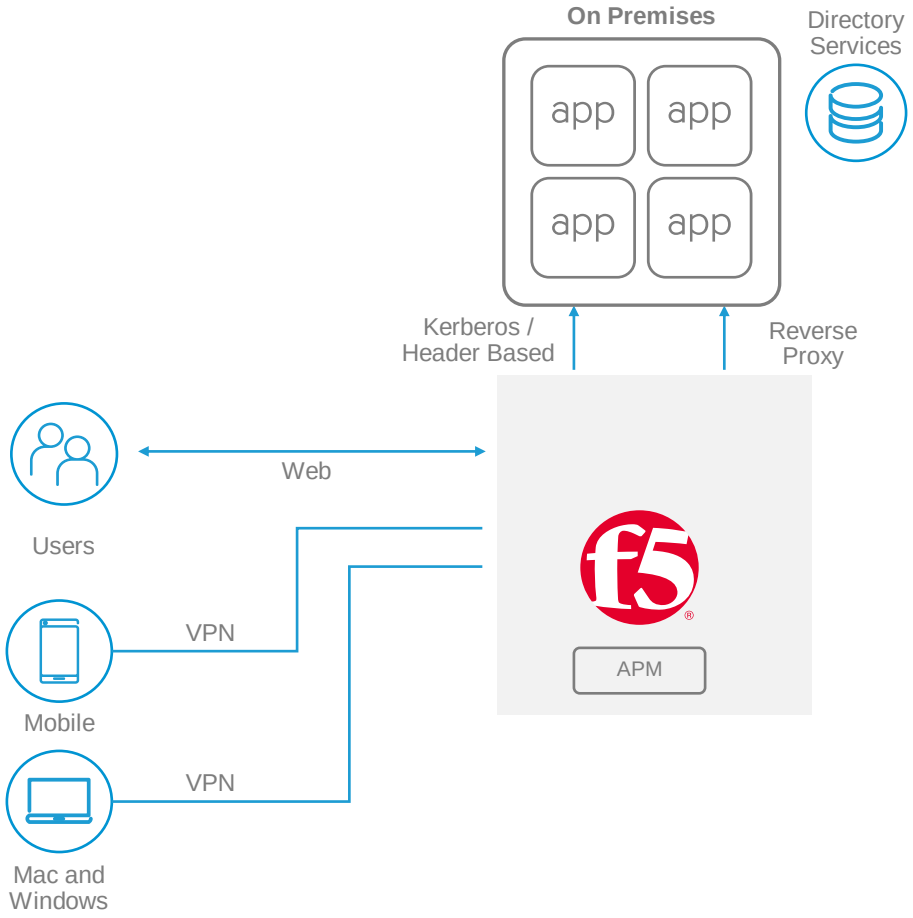
MFA is being disabled

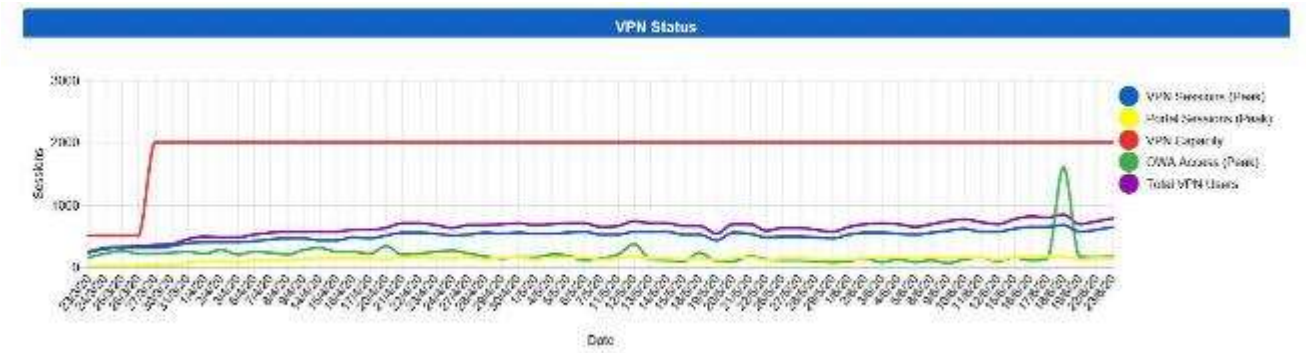
At a time when phishing campaigns are targeting consumers using corporate resources at home.

Rapid expansion of remote access while decreasing security controls

Lancs NHS Trust

Providing NHS services

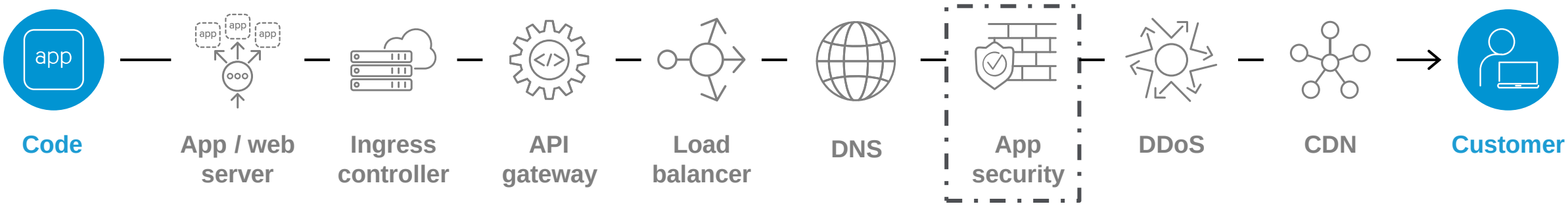


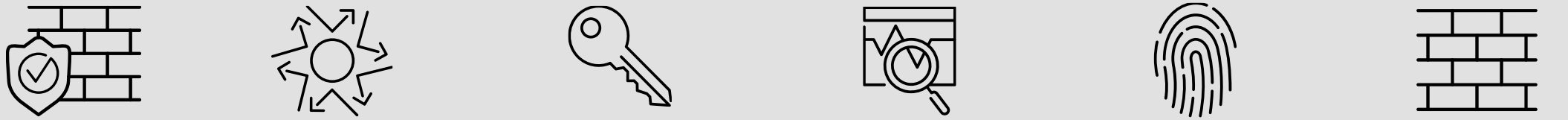


- Rapidly increase remote working
- Consolidated access to all applications
- Streamlined user experience

F5 Code to customer

END TO END APPLICATION SERVICES



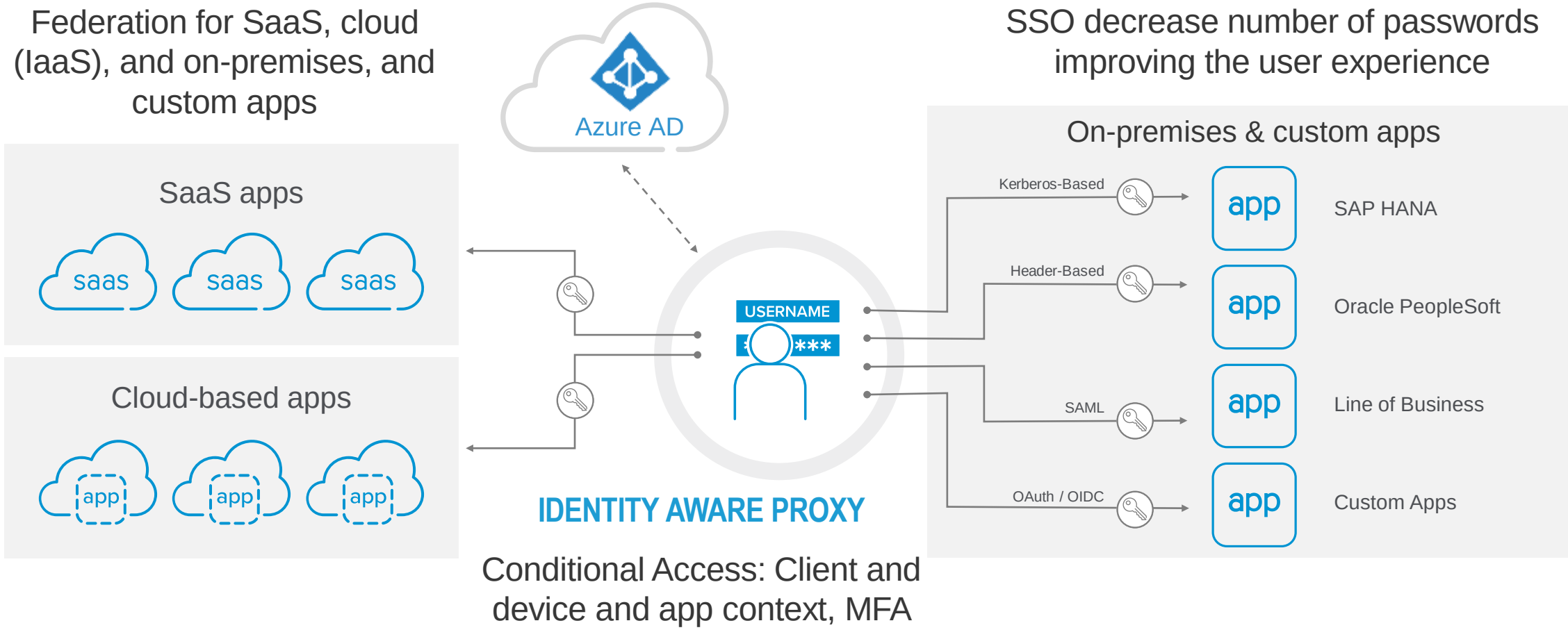


Simplifying application access

CONTEXT-AWARE POLICIES ENFORCE CONDITIONAL APP ACCESS

ACCESS ALL APPS

Federation for SaaS, cloud (IaaS), and on-premises, and custom apps



Conditional Access: Client and device and app context, MFA

SIMPLIFY AND SECURE

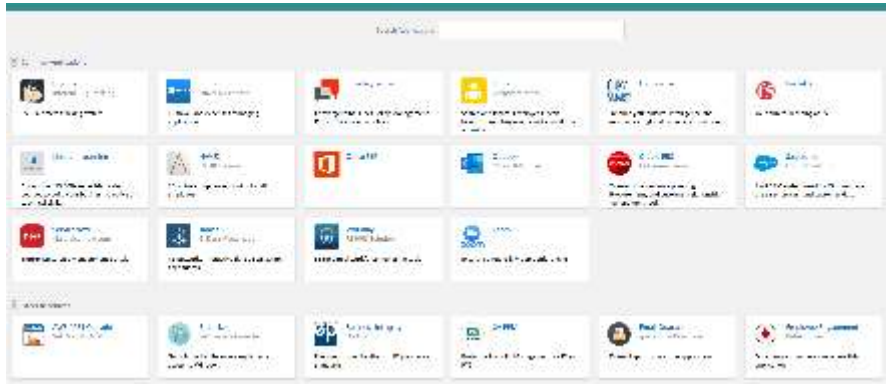
SSO decrease number of passwords improving the user experience

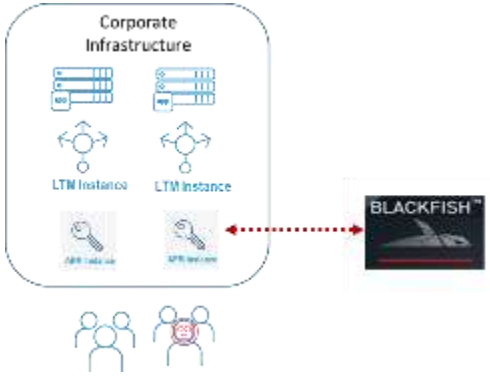
Has your credentials been compromised?

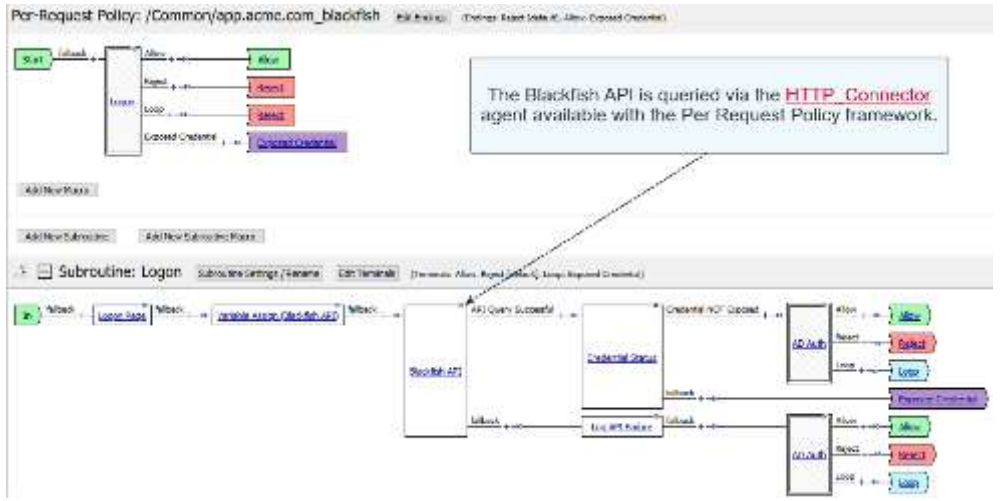
THE AVERAGE PERSON USES THE SAME CREDENTIALS FOR 4 ACCOUNTS

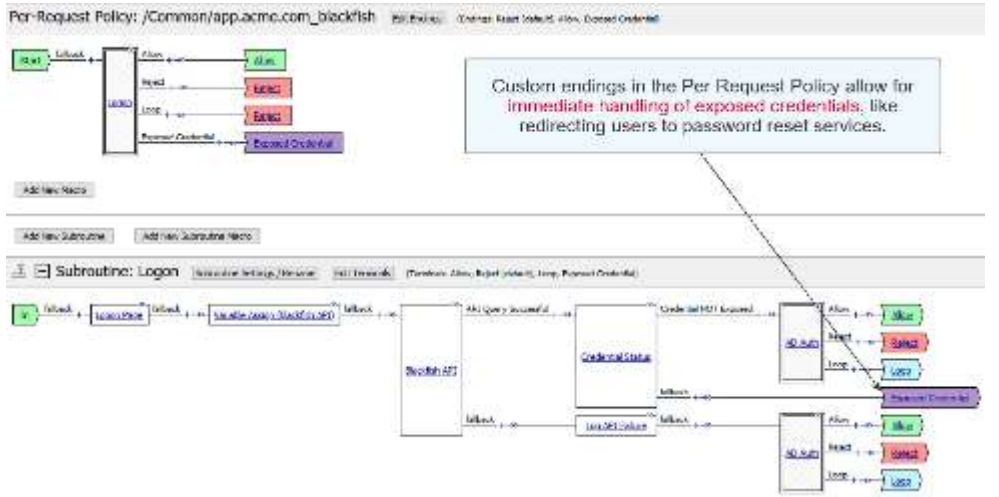
BlackFish

- Subscription service to validate if userID/password (hashed/encoded values) are known to be comprised
- Can integrate with remote access solutions such as F5 APM
- Can integrate using APIs to non F5 security devices



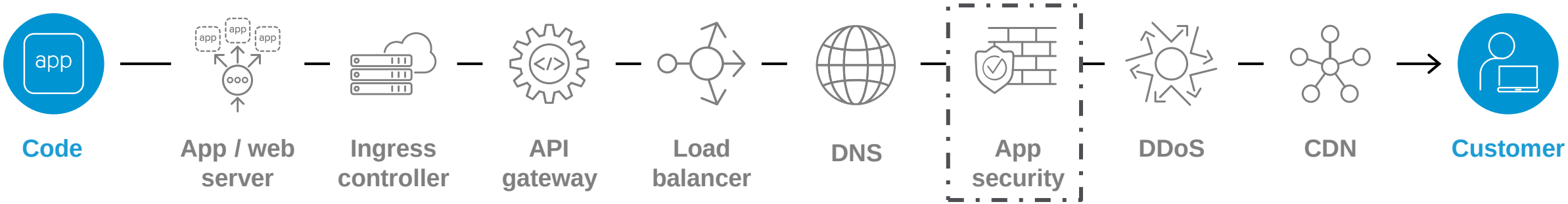






Who, What, Why – Protect your apps!

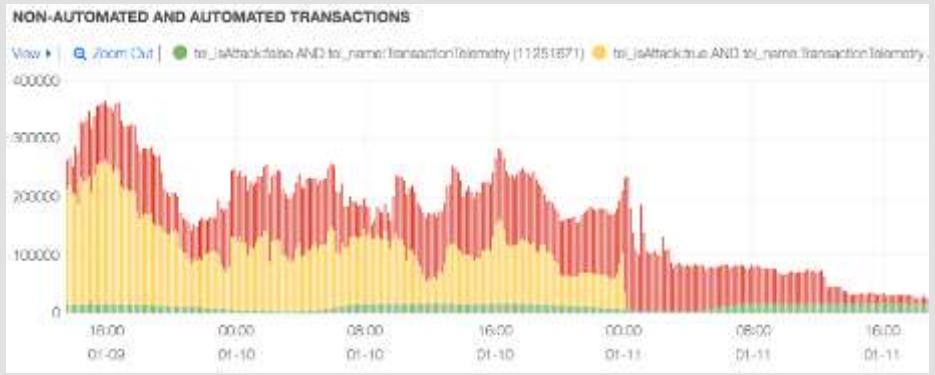
WEB APPLICATION FIREWALL AND SHAPE



WAF

Protecting application code from attacks

Shape



Protecting application logic from fraud

F5 Technology to Support Front line Services

HEALTHCARE, NON-PROFIT AND EDUCATION SERVICES

FREE SOFTWARE AND SERVICES TO HELP THOSE ON THE FRONT LINES

Healthcare, nonprofit, and educational organizations are taking heroic steps to keep us safe during this global crisis. We want to help keep *them* safe from security and technology challenges so they can stay focused on doing their essential work.

If you're in the healthcare, nonprofit, or educational sectors contact us for more details.

Request offer

Keep applications secure

Make sure applications used by remote employees or learn-from-home students are secure with a six-month free trial of Essential App Protect.

Handle increased demand

With exponentially more employees, students, and community partners needing to access your website, scale with one free year of NGINX Plus.

Scale quickly in the cloud

If you're having difficulty keeping up with increased app demand, enable load management in the cloud with up to six months of free BIG-IP Virtual Edition solutions on AWS and up to three months free on Microsoft Azure.

Protect access to apps and data

Keep employees productive and secure with a free 45-day BIG-IP trial, including Access Policy Manger (APM), or a 45-day capacity upgrade to APM. This offer is for nonprofit customers only.

Guard against cyberattacks

Protect your remote students or nonprofit, healthcare, and governmental workforce from targeted cyberattacks with free managed security services from Silverline. *

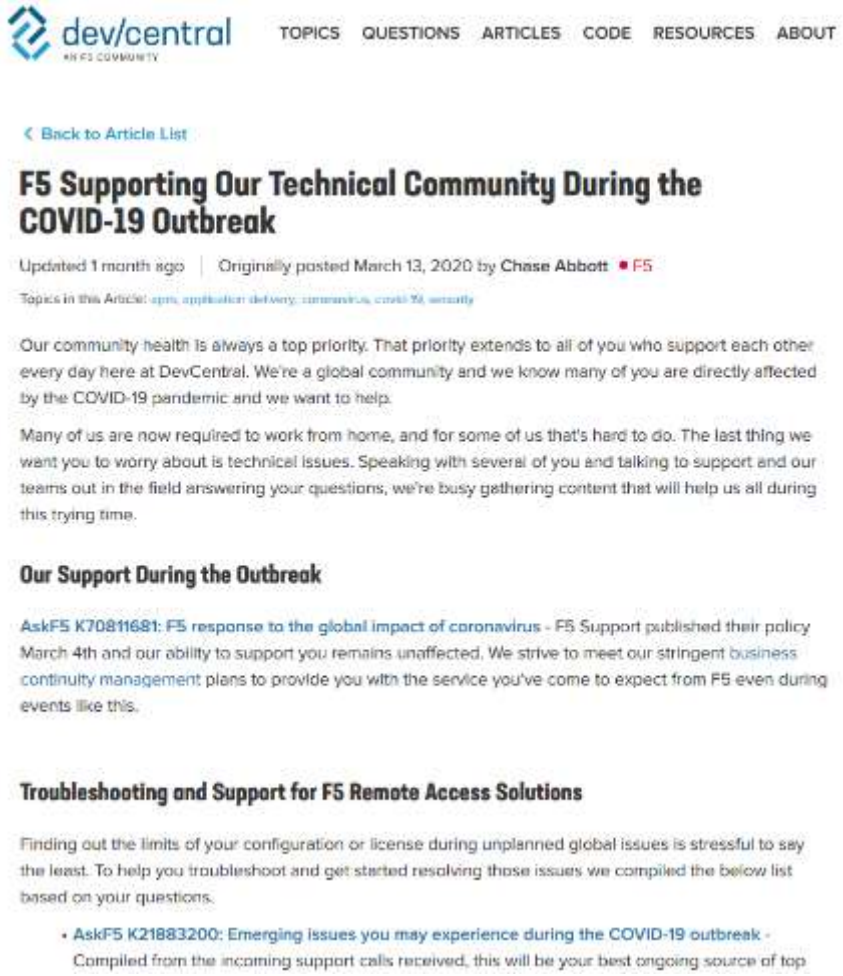
Get up to speed, fast

You're under pressure to set up secure, remote access ASAP. We're here to help. Get free guidance from F5 Professional Services for all BIG-IP APM products, plus free training and learning resources. *

* Case by case basis

Online Technical And Response Services

HTTPS://WWW.F5.COM/BUSINESS-CONTINUITY#RESOURCES



* Not just during Covid-19, available with any active support contract

Thank You