



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**

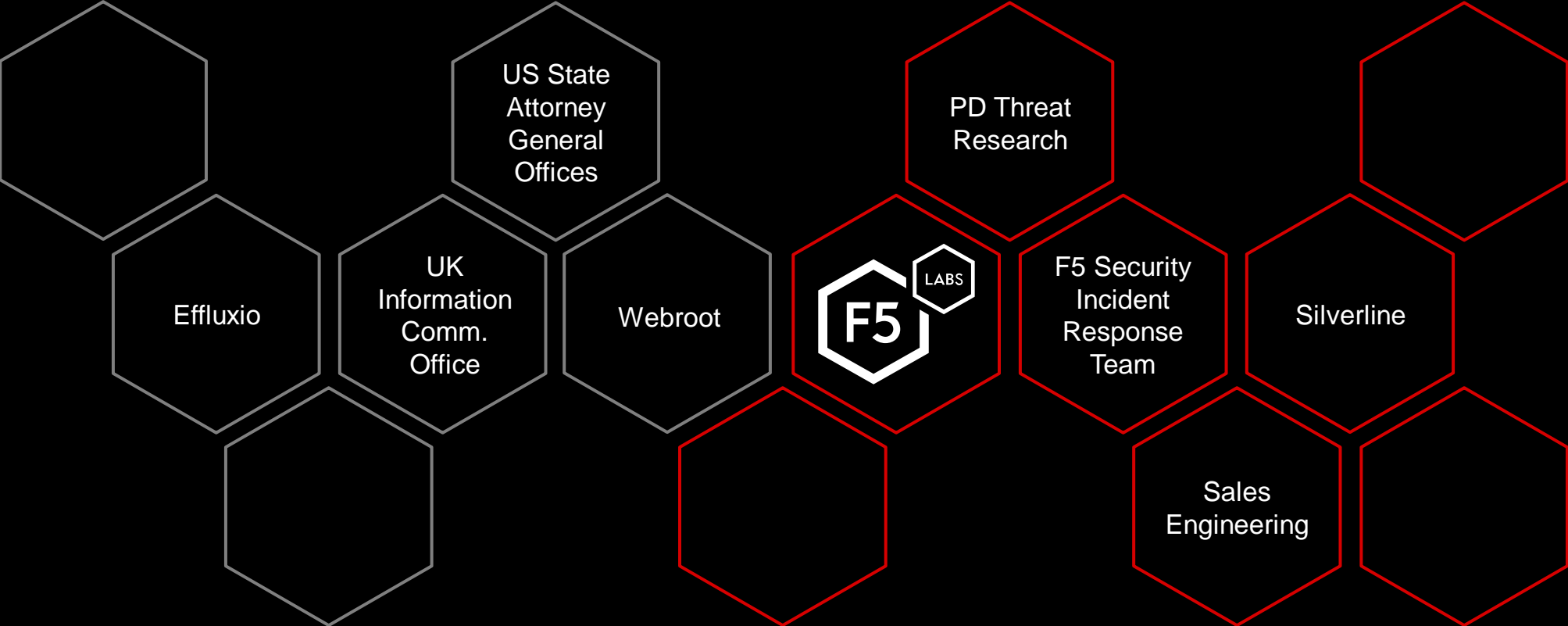
Solutions Engineer  
F5 sales



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

External Partners

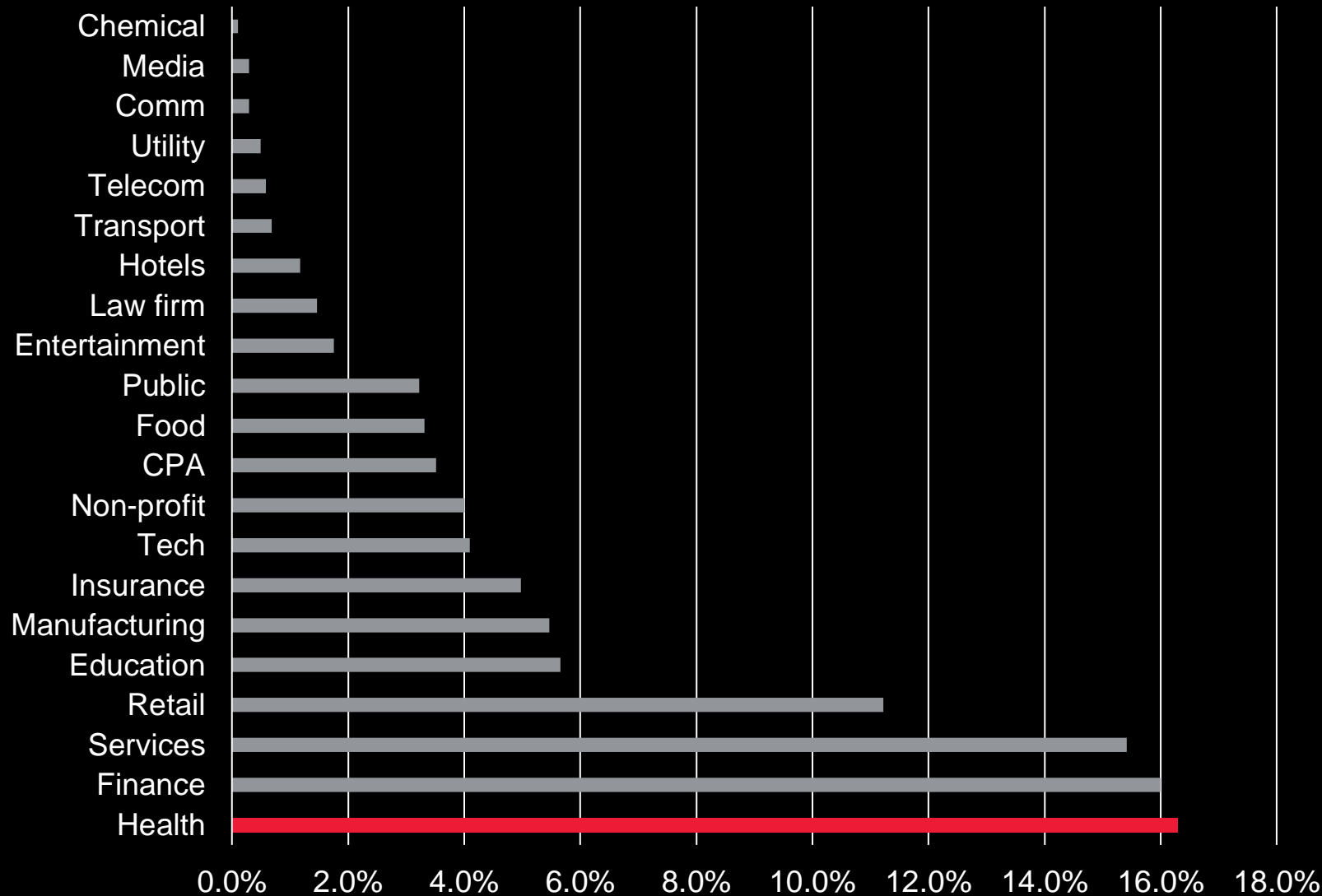
F5  
Teams



UK healthcare accounts  
for 18% of all breaches

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

# 2019 US Breaches by Sector



## Breach Analysis

State Attorney General

**1025**

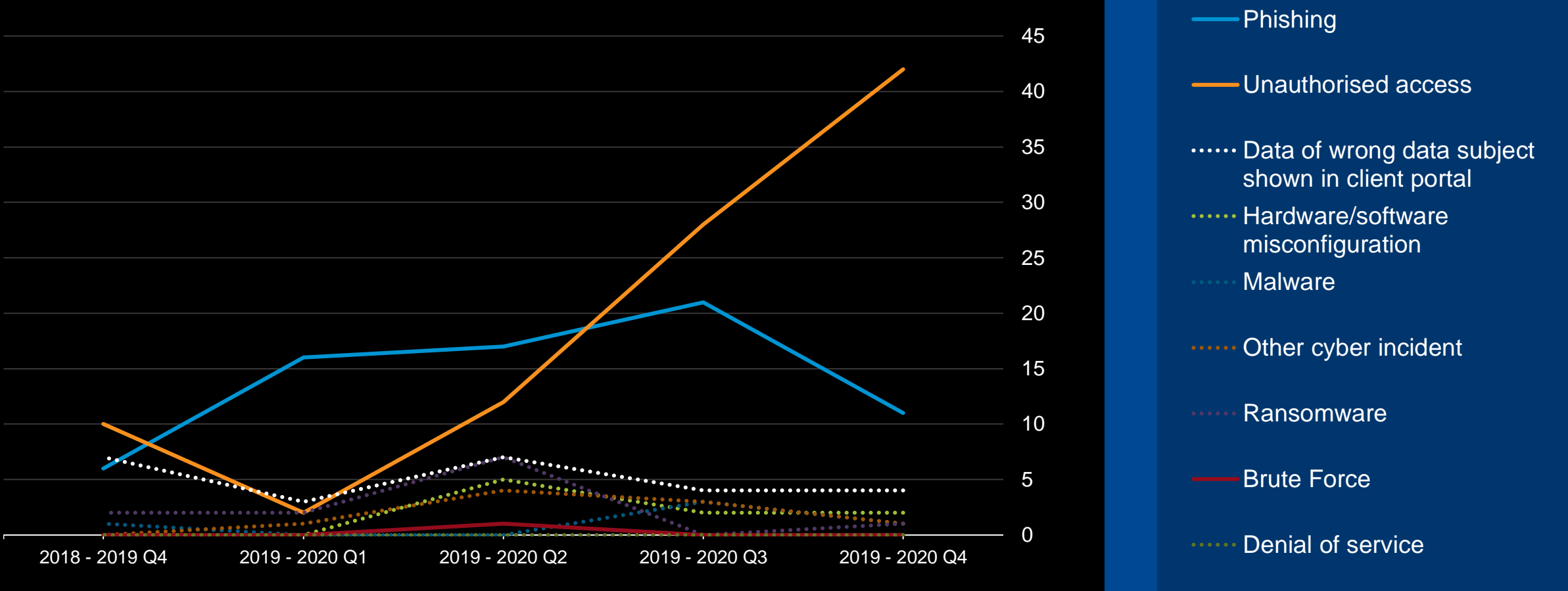
Cases 2019

**85%**

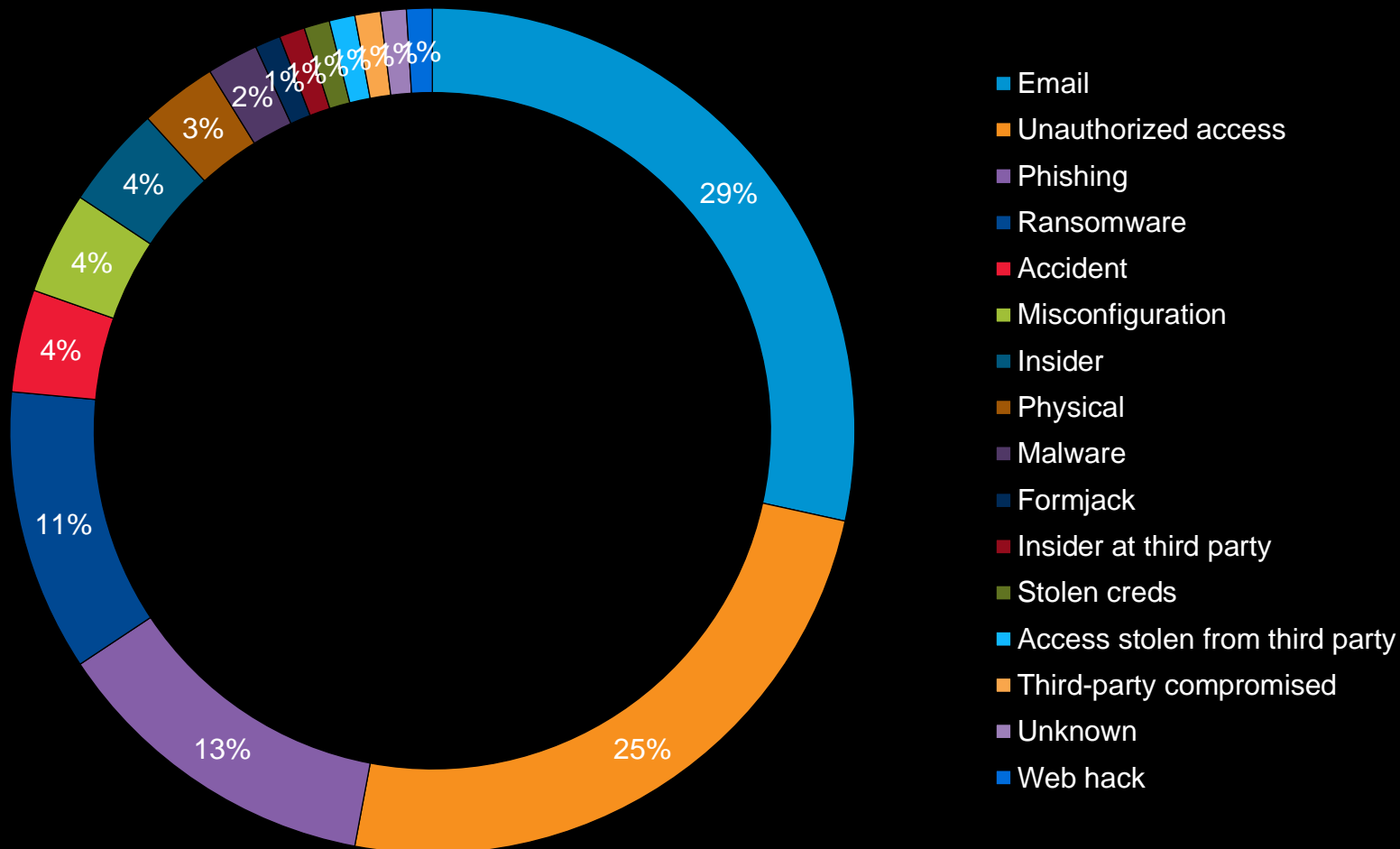
Had explanations



# UK Healthcare breaches

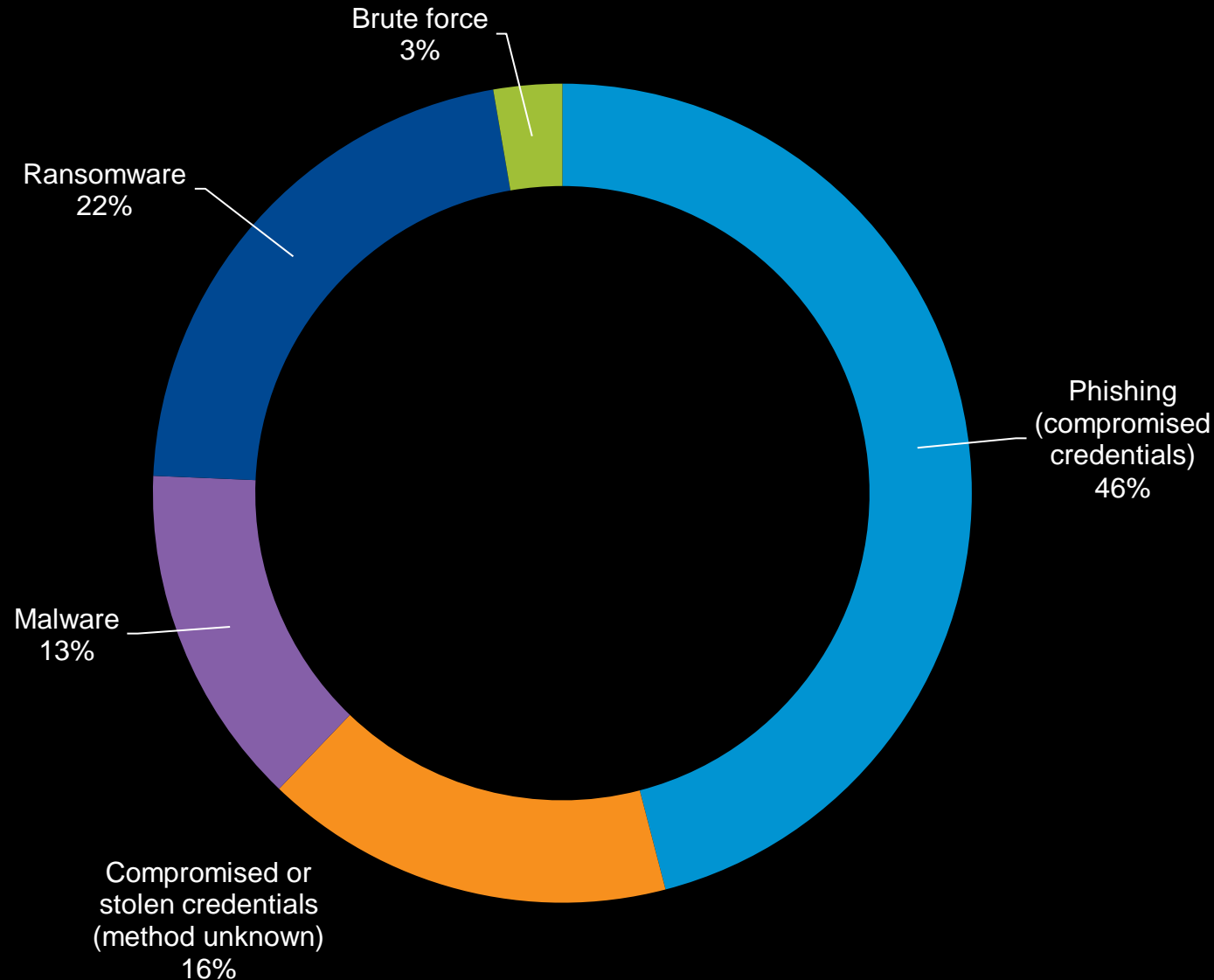


# 2019 US Healthcare Breaches



- 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



- 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



A man with a grey beard and hair, wearing a blue and white floral patterned shirt, is speaking. He has a small earpiece in his left ear and is gesturing with his right hand. The background is dark.

"Amateurs hack systems,  
professionals hack  
people"

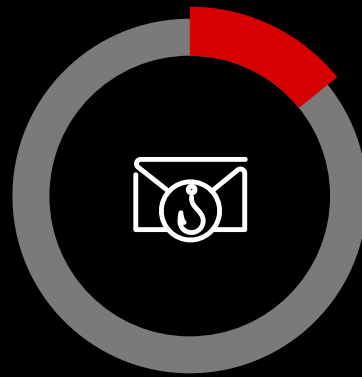
- Bruce Schneier

# 2019 Access Attacks Broken Down



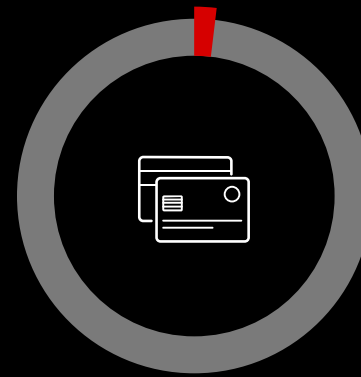
**32.8%**

Email cited  
as cause



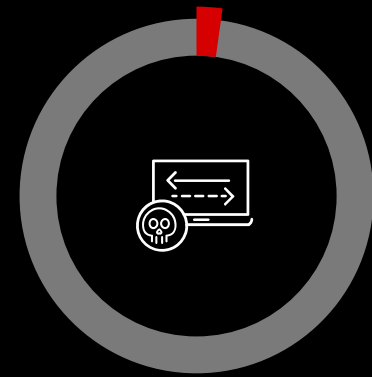
**14.2%**

Phishing gain  
access to email



**1.9%**

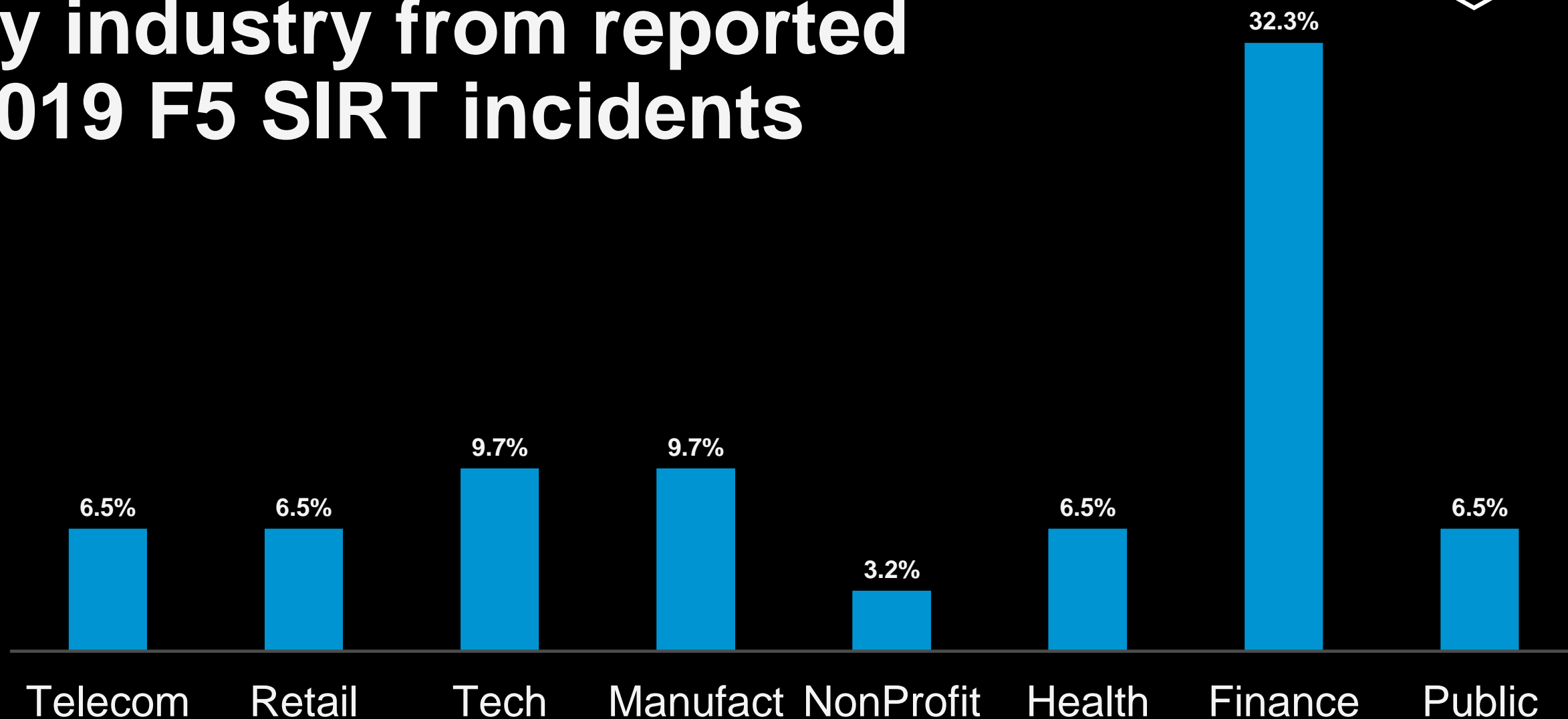
Access  
creds stolen



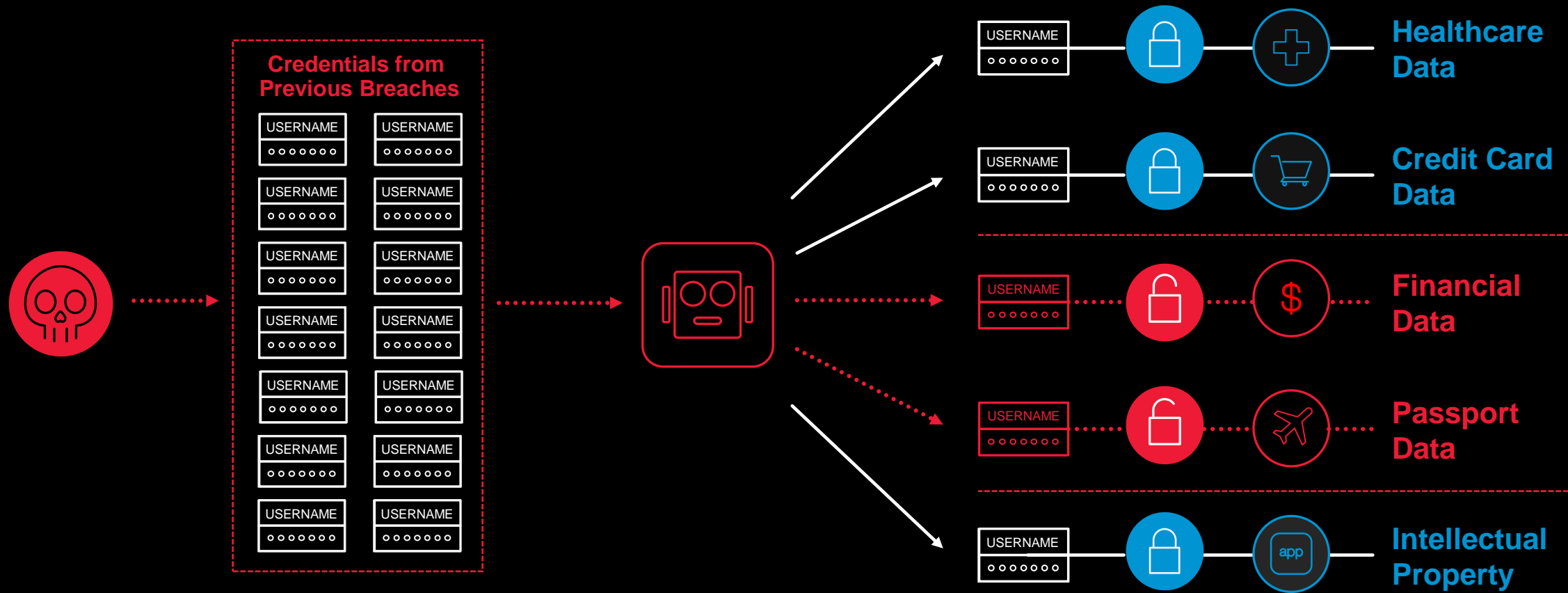
**2.2%**

Access cred  
stuffing and brute

# Brute Force attacks by industry from reported 2019 F5 SIRT incidents



# Credential Stuffing



# Credential Stuffing

The screenshot shows the Sentry MBA 1.4.1 application window. The interface includes a top bar with 'Start' and 'Abort' buttons, a 'Site' field set to 'https://www.facebook.com/login.php?login\_attempt=1', a 'Switch Site' field set to 'facebook.com', and a 'Progress' bar at 1%. Below this, there are fields for 'Bots' (120) and 'Wordlist Position' (1288). A table displays the progress of 8 bots, each with columns for Bot #, Proxy, Username, Password, Email, and Reply. The 'Reply' column shows 'Authenticating - Last status: Failure Header Keyword Match -> Found'. At the bottom, there is a 'Hits' tab showing a list of successful login attempts with details like IP address, email, and password. The status bar at the very bottom indicates 'BruteForcing...', 'Wordlist: yandex', '1260/121273 (1%)', and 'IP: 217.23.12.70'.

**Sentry MBA 1.4.1**

Site:  X  
Switch Site:  X  
Progress:  List:

Bots:  Wordlist Position:

Bot #	Proxy	Username	Password	Email	Reply
1		g3studio_2...	myduck		Authenticating - Last status: Failure Header Keyword Match -> Found
2		ycjung_007...	yoyoyo		Authenticating - Last status: Failure Header Keyword Match -> Found
3		u_friend99...	kimjunsu		Authenticating - Last status: Failure Header Keyword Match -> Found
4		ultraman_ne...	cuchang		Authenticating - Last status: Failure Header Keyword Match -> Found
5		oshiohm@h...	1510322074		Authenticating - Last status: Failure Header Keyword Match -> Found
6		tai_eng@ya...	999999		Authenticating - Last status: Failure Header Keyword Match -> Found
7		tt-tt_zs@hot...	sawasdee		Authenticating - Last status: Failure Header Keyword Match -> Found
8		suphot_ju20...	suphot10		Authenticating - Last status: Failure Header Keyword Match -> Found

Hits | Redirects | Fakes | To Check | Users/Combos

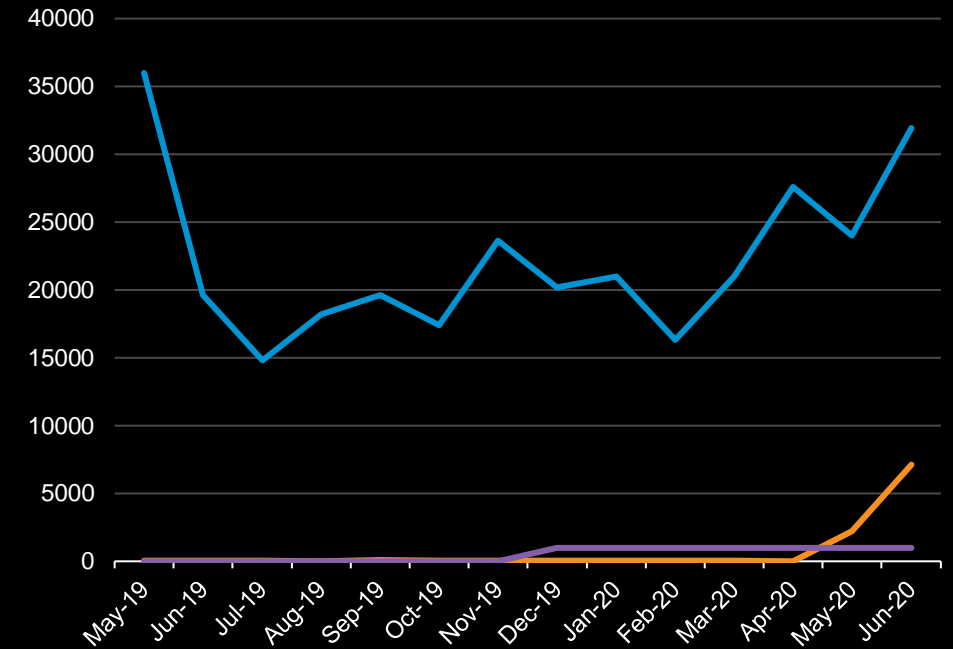
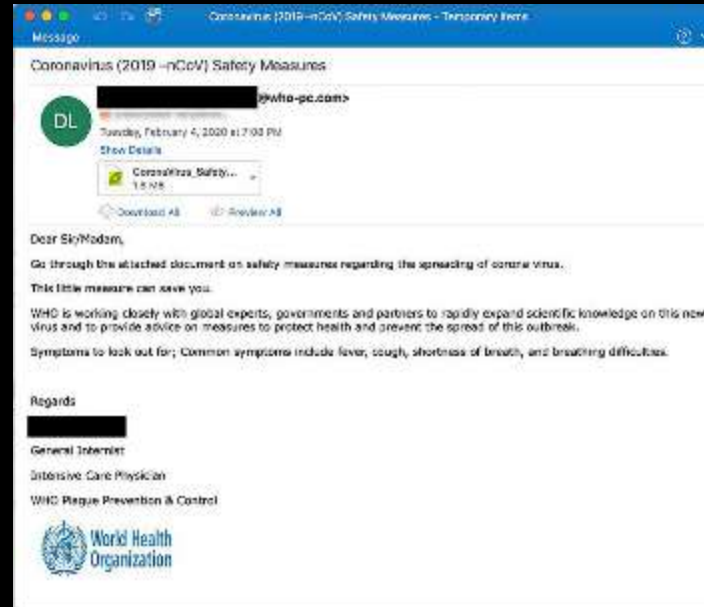
#1: https://vblidoc@gmail.com: volare88@www.facebook.com/login.php?login\_attempt=1 - Success Header Keyword Match -> Found Key [HTTP/1.1 302 F...]  
#2: https://cache51@hotmail.com: metalica2@www.facebook.com/login.php?login\_attempt=1 - Success Header Keyword Match -> Found Key [HTTP/1.1...]  
#3: https://katookclub@hotmail.com: 4702795ale@www.facebook.com/login.php?login\_attempt=1 - Success Header Keyword Match -> Found Key [HTTP/1...]  
#4: https://zoromanx@hotmail.com: 251200@www.facebook.com/login.php?login\_attempt=1 - Success Header Keyword Match -> Found Key [HTTP/1.1 30...]  
#5: https://i\_lovelens@hotmail.com: 31052630@www.facebook.com/login.php?login\_attempt=1 - Success Header Keyword Match -> Found Key [HTTP/1...]  
#6: https://hszibv@hotmail.com: s1119b@www.facebook.com/login.php?login\_attempt=1 - Success Header Keyword Match -> Found Key [HTTP/1.1 302 F...]  
#7: https://iismoat@hotmail.com: 2486zxwecrv@www.facebook.com/login.php?login\_attempt=1 - Success Header Keyword Match -> Found Key [HTTP/1...]  
#8: https://deceiverold@hotmail.com: chirawat@www.facebook.com/login.php?login\_attempt=1 - Success Header Keyword Match -> Found Key [HTTP/1...]

BruteForcing... Wordlist: yandex 1260/121273 (1%) IP: 217.23.12.70

# 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

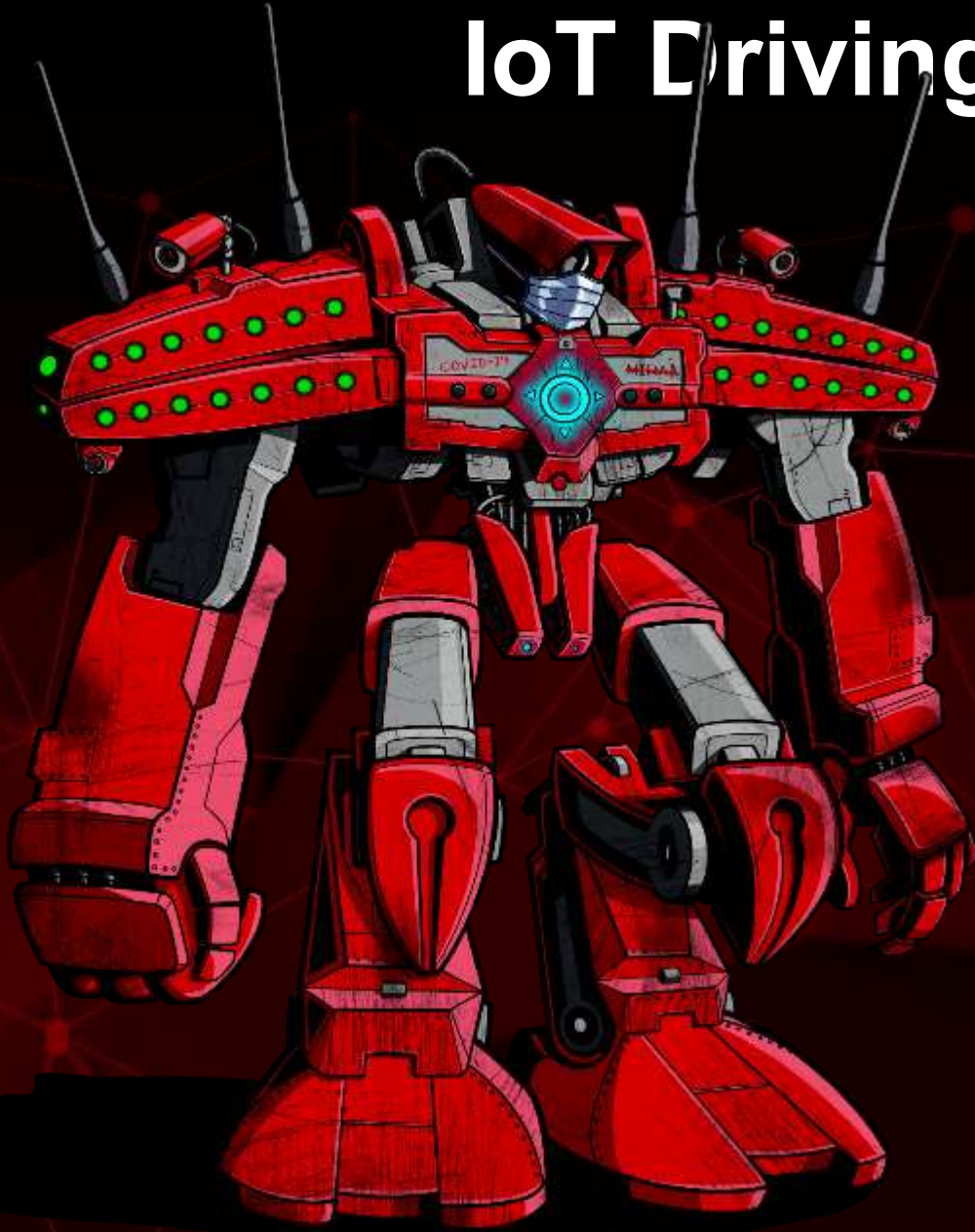
Phishing Attempts

Malware Attachments

Corona or Coronavirus



# IoT Driving COVID Variants



2017B  
DEVICES

Softbank

2026

\*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

## SCARFACE'S BOTNET SETUP SERVICE

LEARN MORE ▾

### WHAT IS A BOTNET?

A botnet is a logical collection of compromised internet-connected devices such as computers, smartphones or IoT devices each of such compromised device, known as a "bot", is created when a device is penetrated by software from a malware (malicious software) distribution.

The controller of a botnet is able to direct the activities of these compromised computers.

Mining cryptocurrencies can be a costly investment, but creative cybercriminals have found a money-making solution.



### SERVICE

HACKING WEB SERVER  
(VPS OR HOSTING)

SETTING UP KEYLOGGER

DDOS (PRICES MAY VARY)

HACKING PERSONAL COMPUTER

HACKING CELL PHONES

EMAIL HACKING

SOCIAL MEDIA ACCOUNT HACKING

CHANGE SCHOOL GRADES

FUD RANSOMWARE + DECRYPTER



### BITCOIN

(Typical price range listed along with the highest listed price)

0.034 - 0.0449, 0.47

0.0263

0.0534, 0.078 - 0.39

0.0364, 0.044 - 0.55

0.047 - 0.093

0.078 - 0.12

0.0352, 0.054 - 0.11

0.19 - 0.58

12 MO / 0.14

6 MO / 0.076

1 MO / 0.019



### USD

(Typical price range listed along with the highest listed price)

\$220 - \$500, \$3,000

\$170

\$350, \$500 - \$2,500

\$280, \$500 - \$3,500

\$300 - \$600

\$500 - \$800

\$230, \$350 - \$700

\$1,200 - \$3,750

12 MO / \$900

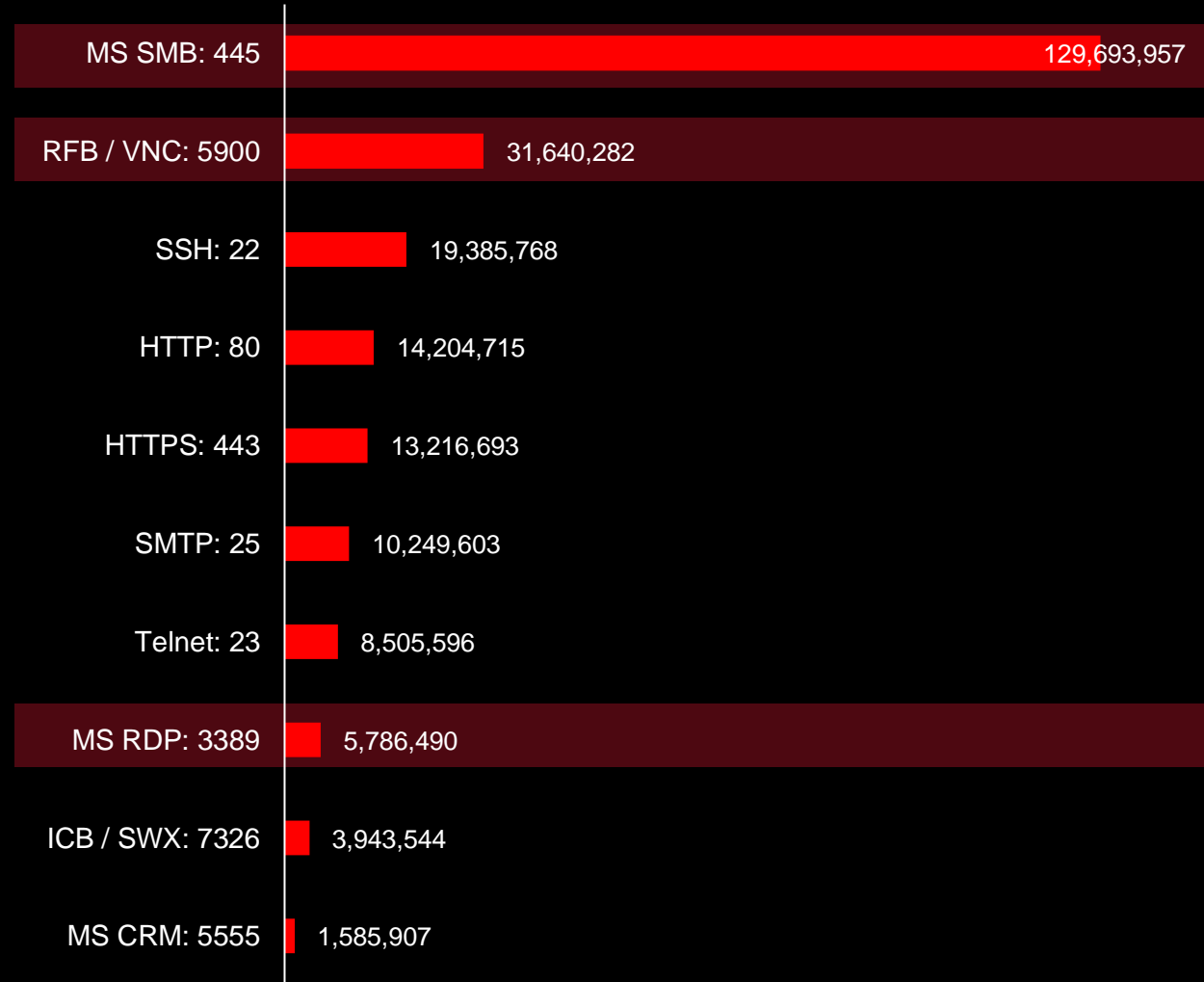
6 MO / \$490

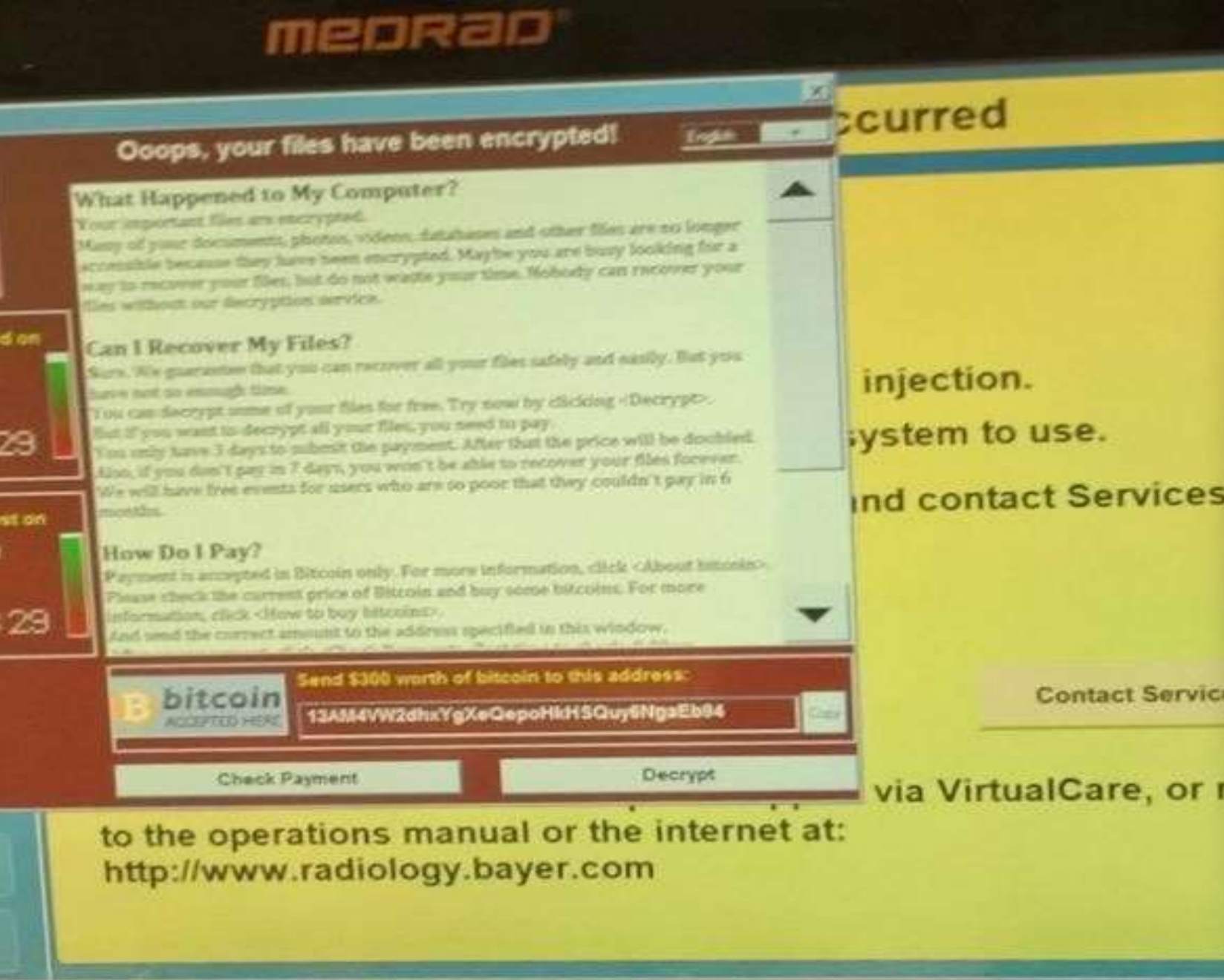
1 MO / \$120



# Top Targeted Ports Q4 2019

Global Count





# 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?

Shodan Developers Monitor View All... Show API Key Try out the new

SHODAN port:3389 Explore Downloads Reports Pricing Enterprise Access

Exploits Maps Images Like 97 Download Results Create Report

TOTAL RESULTS  
4,415,992

TOP COUNTRIES

Country	Count
United States	1,328,589
China	1,228,365
Germany	166,417
Netherlands	106,755
Brazil	103,162

TOP ORGANIZATIONS

Organization	Count
Tencent cloud computing	805,774
Amazon.com	381,590
Google Cloud	330,535
Microsoft Azure	312,576
China Telecom	178,464

TOP OPERATING SYSTEMS

Operating System	Count
Windows 10 or Server 12	10,360
Windows 7 or 8	4,661
Windows Server 2008	2,833
Windows 10	2,273
Windows Server 2003	864

TOP PRODUCTS

Product	Count
Windows Server 2003	864
Windows 7	7,722
Windows Server 2008	7,801
Windows 8.1	4,760
Windows 10 or Server 12	10,360

New Service! Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

RELATED TAGS: rdp

61.174.255.251  
201.125.174.81 (real) ip address: 168.144.11.11  
JIN-HUA, ZHEJIANG Province, P.R.China.  
Added on 2023-04-12 18:58:42 GMT  
China

安全登录

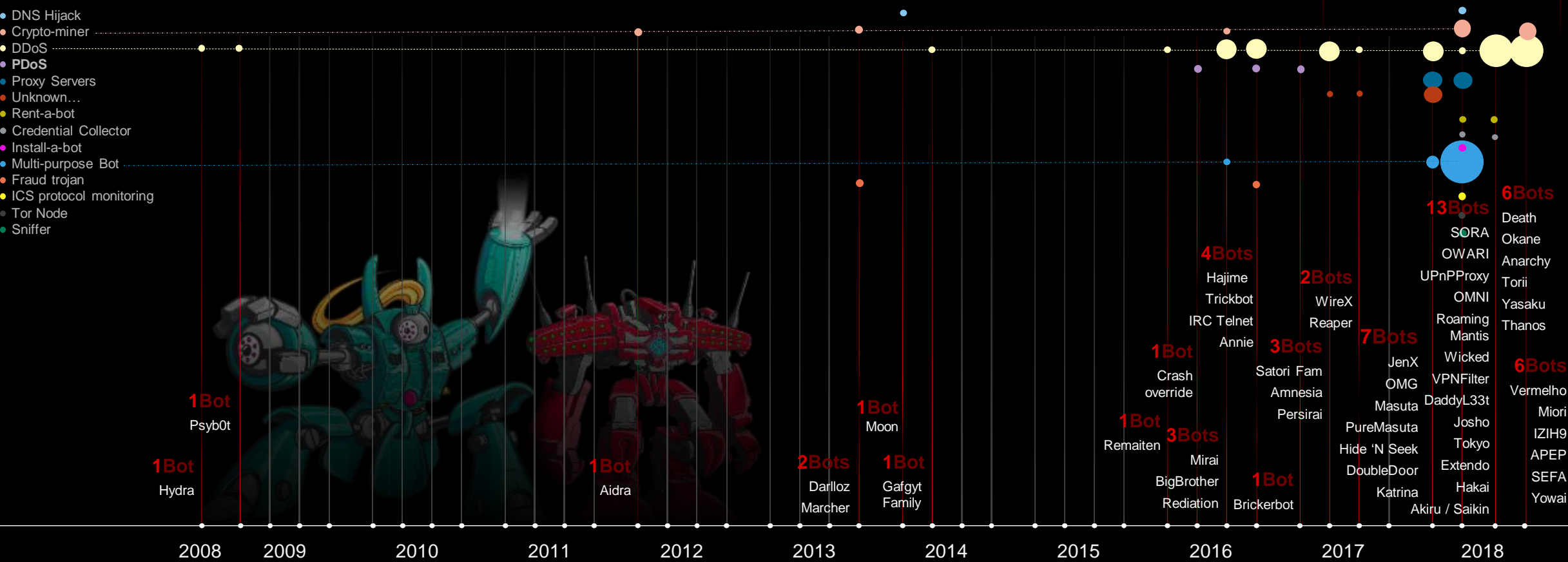
用户名

密码

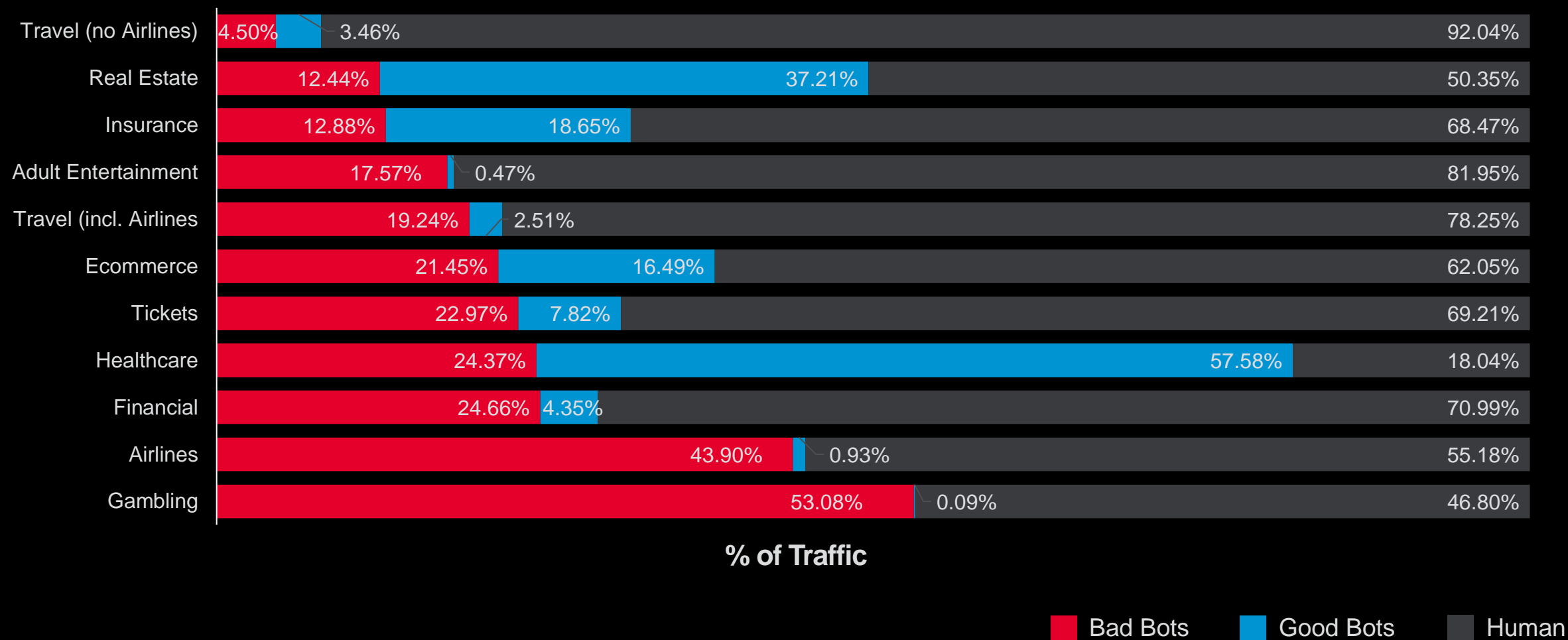


# Bad Bots

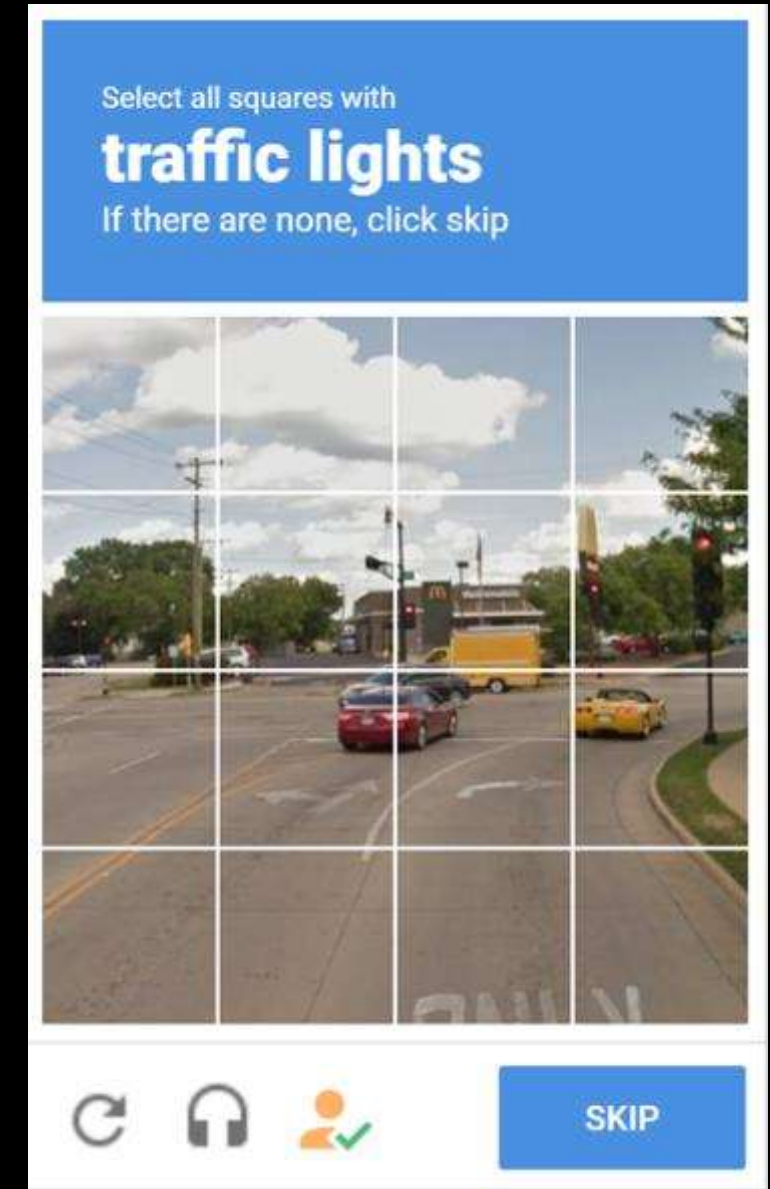
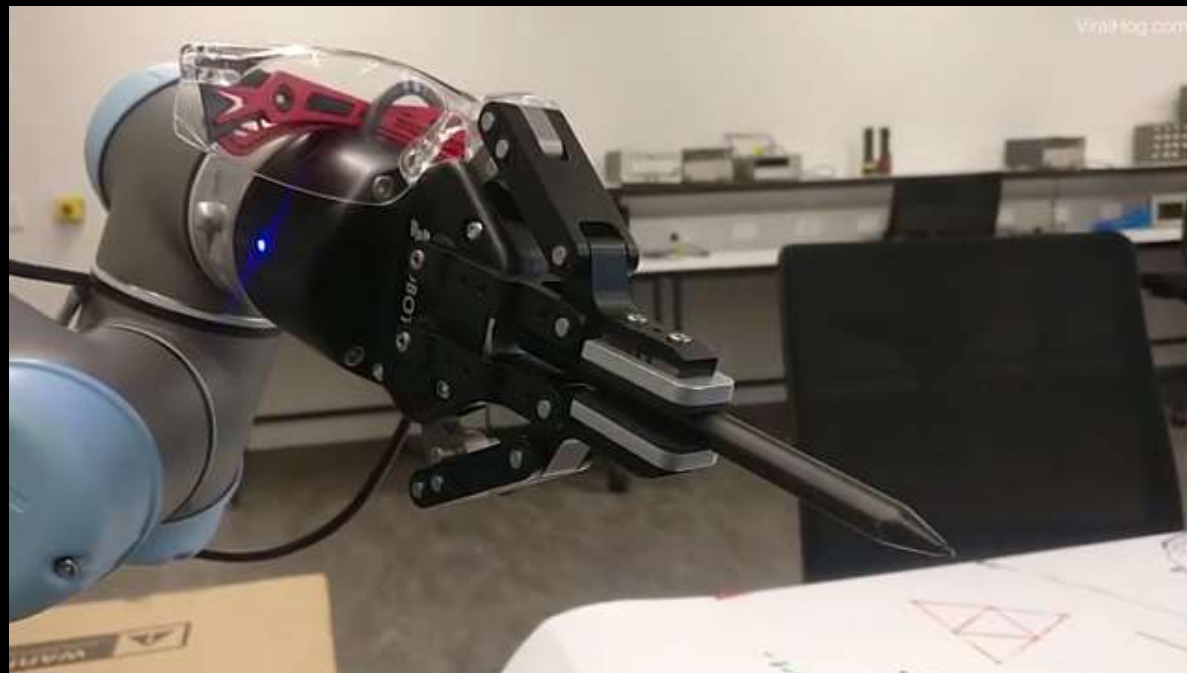
## Routers, IoT, Smart TVs, IP cameras



# Bots by Industry



# CAPTCHA



# 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.



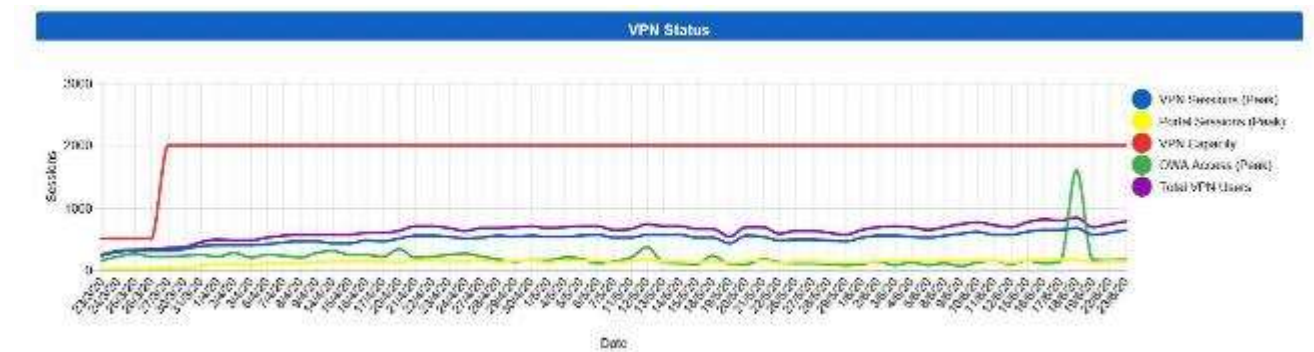
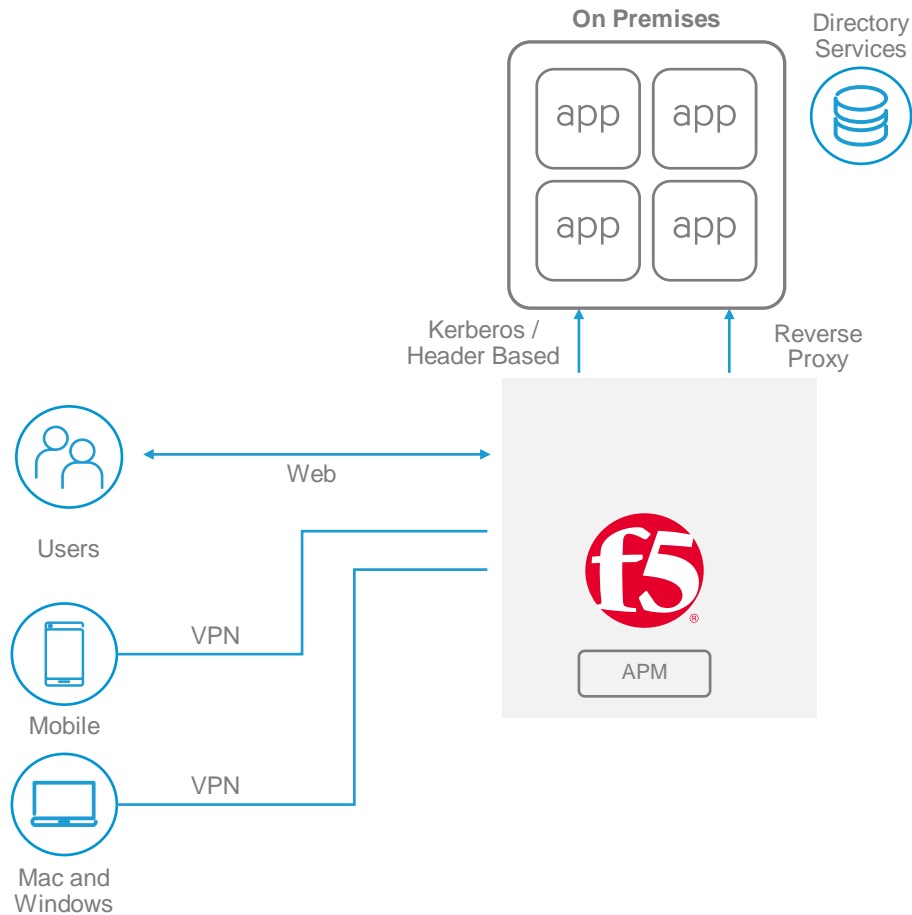
## MFA is being disabled

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

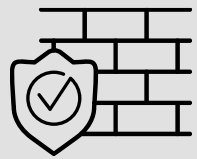
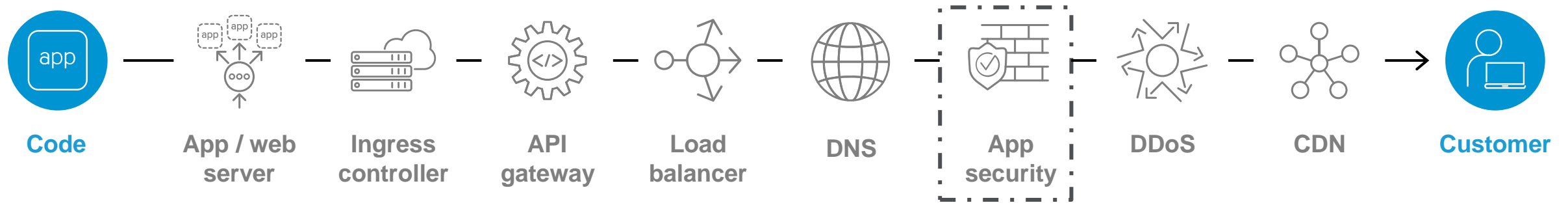


- Rapidly increase remote working
- Consolidated access to all applications
- Streamlined user experience

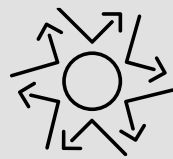


# F5 Code to customer

## END TO END APPLICATION SERVICES



**Web app  
firewall**



**DDoS +  
bot protection**



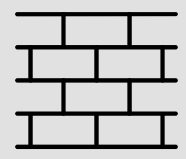
**Access  
management**



**SSL decryption  
& orchestration**



**Credential & anti-  
fraud protection**



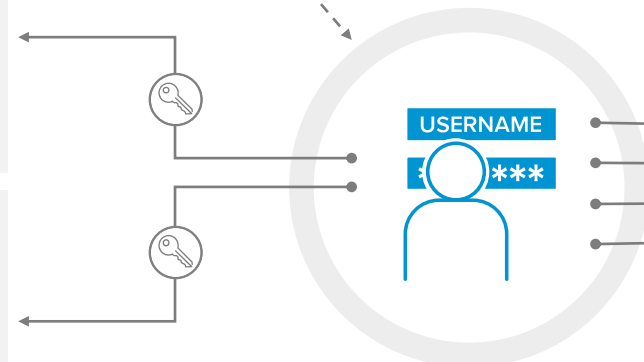
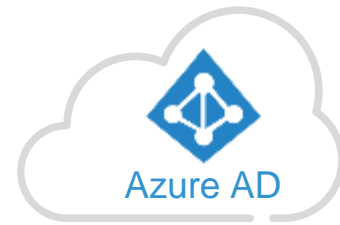
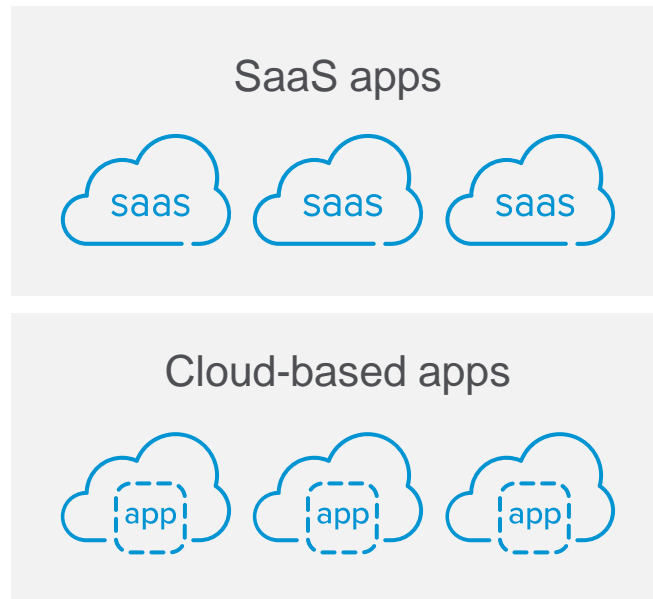
**L4 firewall  
including IPS**

# Simplifying application access

## CONTEXT-AWARE POLICIES ENFORCE CONDITIONAL APP ACCESS

### ACCESS ALL APPS

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

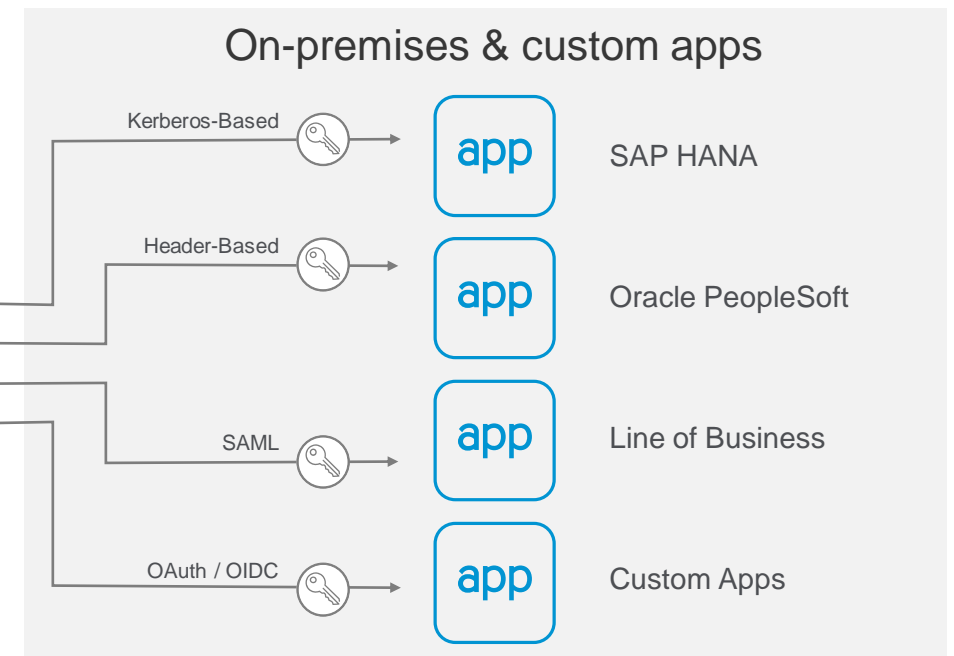


### IDENTITY AWARE PROXY

Conditional Access: Client and device and app context, MFA

### SIMPLIFY AND SECURE

SSO decrease number of passwords improving the user experience

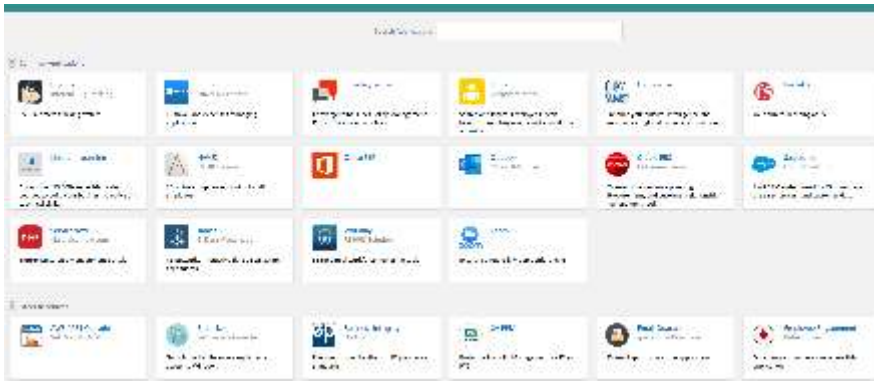
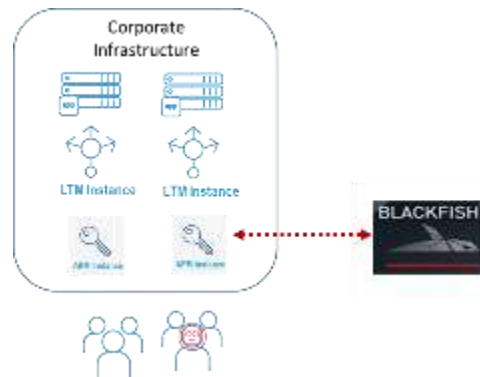
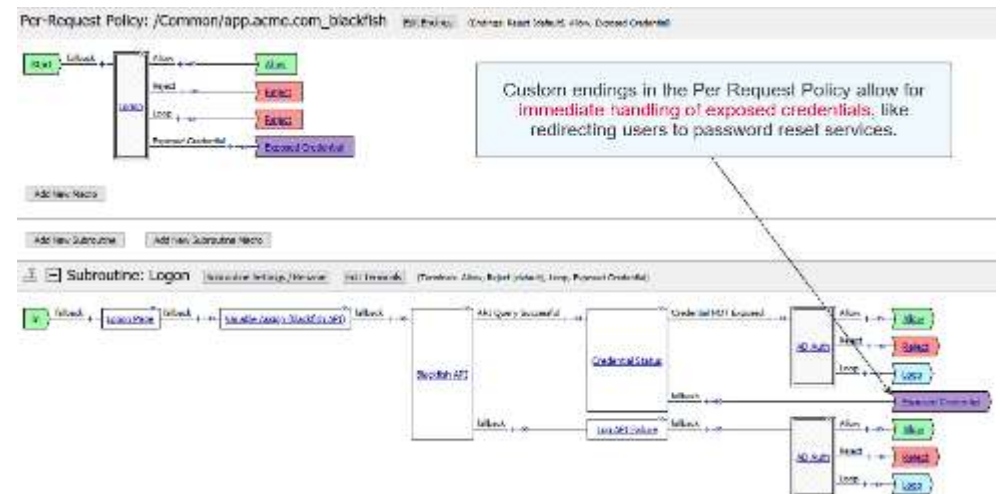
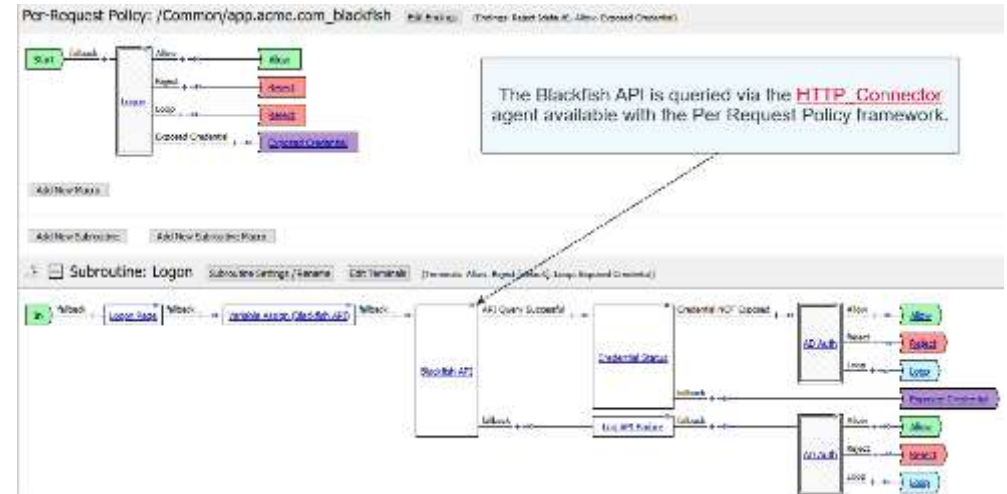


# Has your credentials been compromised?

THE AVERAGE PERSON USES THE SAME CREDENTIALS FOR 4 ACCOUNTS

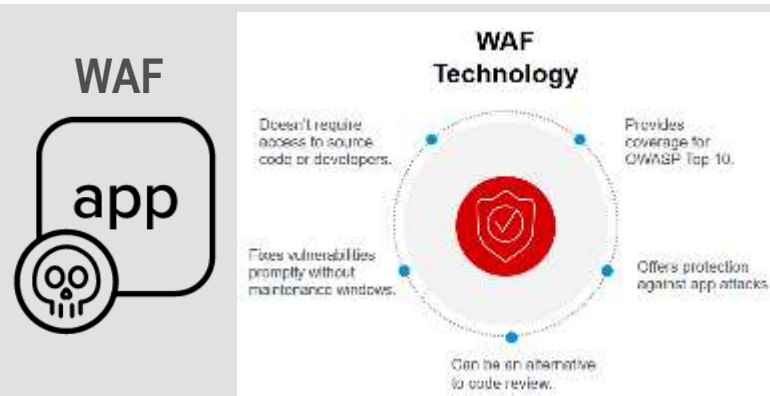
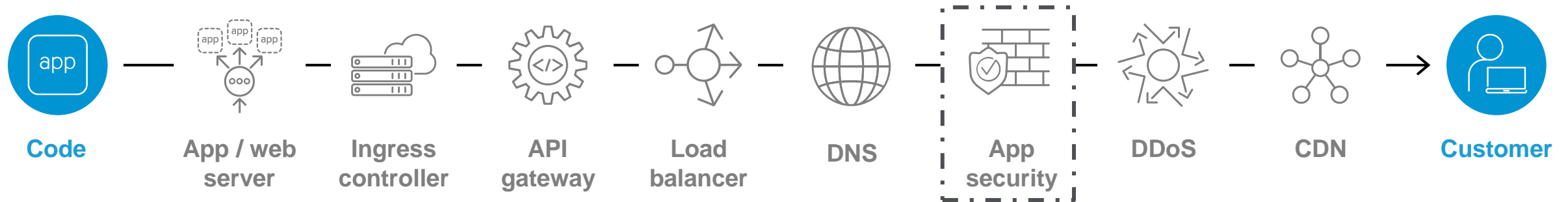
## BlackFish

- 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

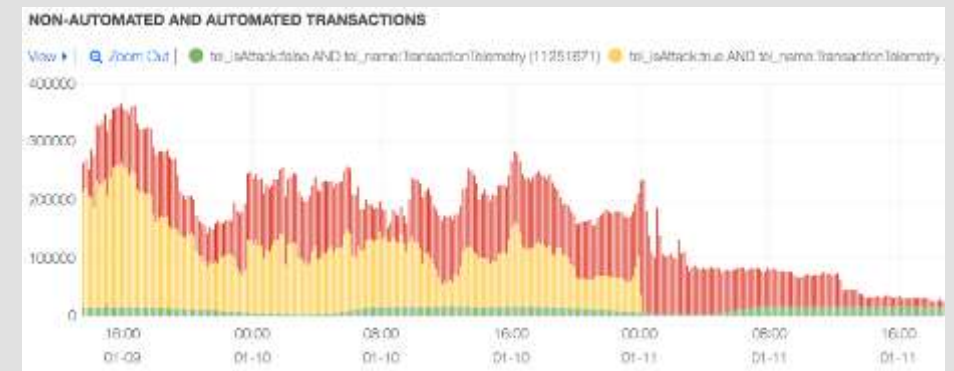
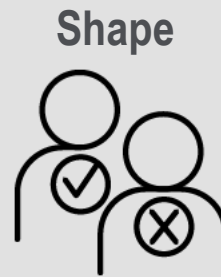


# Who, What, Why – Protect your apps!

## WEB APPLICATION FIREWALL AND SHAPE



Protecting application code from attacks



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.**

### 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.**

### Guard against cyberattacks

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

### Handle increased demand

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

### Protect access to apps and data

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

### 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](https://www.f5.com/business-continuity#resources)



TOPICS QUESTIONS ARTICLES CODE RESOURCES ABOUT

[← Back to Article List](#)

## F5 Supporting Our Technical Community During the COVID-19 Outbreak

Updated 1 month ago | Originally posted March 13, 2020 by Chase Abbott • F5

Topics in this Article: [apps](#), [application delivery](#), [coronavirus](#), [covid-19](#), [security](#)

Our community health is always a top priority. That priority extends to all of you who support each other every day here at DevCentral. We're a global community and we know many of you are directly affected by the COVID-19 pandemic and we want to help.

Many of us are now required to work from home, and for some of us that's hard to do. The last thing we want you to worry about is technical issues. Speaking with several of you and talking to support and our teams out in the field answering your questions, we're busy gathering content that will help us all during this trying time.

### Our Support During the Outbreak

**AskF5 K70811681: F5 response to the global impact of coronavirus** - F5 Support published their policy March 4th and our ability to support you remains unaffected. We strive to meet our stringent business continuity management plans to provide you with the service you've come to expect from F5 even during events like this.

### Troubleshooting and Support for F5 Remote Access Solutions

Finding out the limits of your configuration or license during unplanned global issues is stressful to say the least. To help you troubleshoot and get started resolving those issues we compiled the below list based on your questions.

- **AskF5 K21883200: Emerging issues you may experience during the COVID-19 outbreak** - Compiled from the incoming support calls received, this will be your best ongoing source of top



SOLUTIONS PRODUCTS CUSTOMERS **SERVICES** COMMUNITY PARTNERS COMPANY

EN



## Security Incident Response Team (SIRT)

Our security team, ready to help when you need us.

Are you under attack? For immediate help, call (888) 882-7335 or +1 (800) 11-275-435

[Contact F5 SIRT](#)

### SIRT BENEFITS

No matter how well you protect against security breaches, you also need a plan in place for when attacks break through. When security incidents occur, F5 SIRT will be there to help you.



#### MITIGATE ATTACKS

Mitigate attacks more efficiently with F5 global support



#### BLOCK UNAUTHORIZED ACCESS

Block unauthorized access to systems and data



#### PROTECT YOUR BUSINESS



#### RECOVER QUICKLY

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





# Thank You