7 things that Threat Intelligence Can Teach Us to Help Secure Small Businesses

Raymond Pompon

Ray Pompon

r.pompon@F5.com
@dunsany

Principal Threat Researcher Evangelist

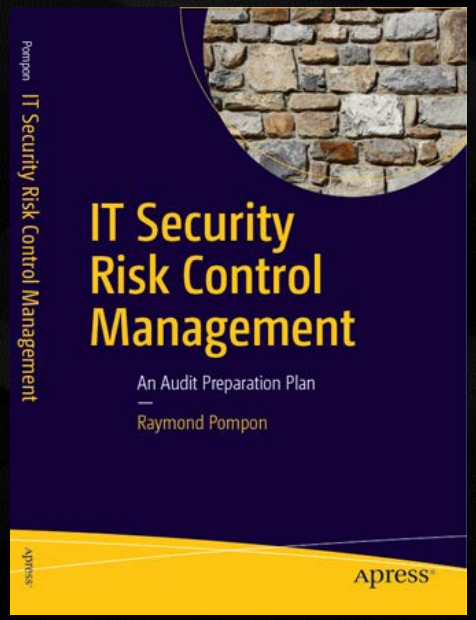
20+ years in InfoSec—CISSP

InfraGard Delaware board,
ISC^2 Delaware board,
Founder Seattle chapter of InfraGard

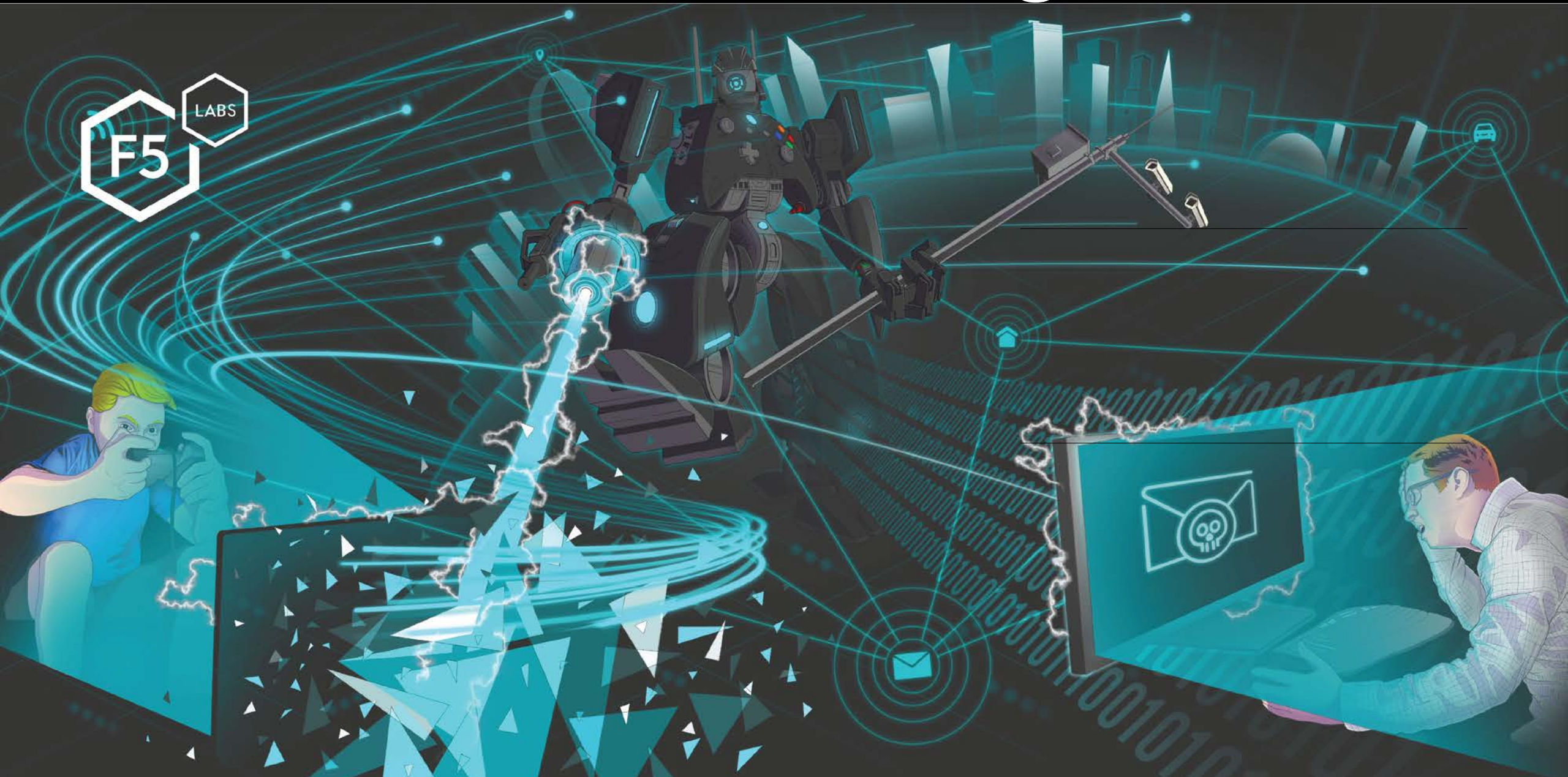
29 years in IT

Specialist in Compliance/Audit,
Web App Security, and
Network Security

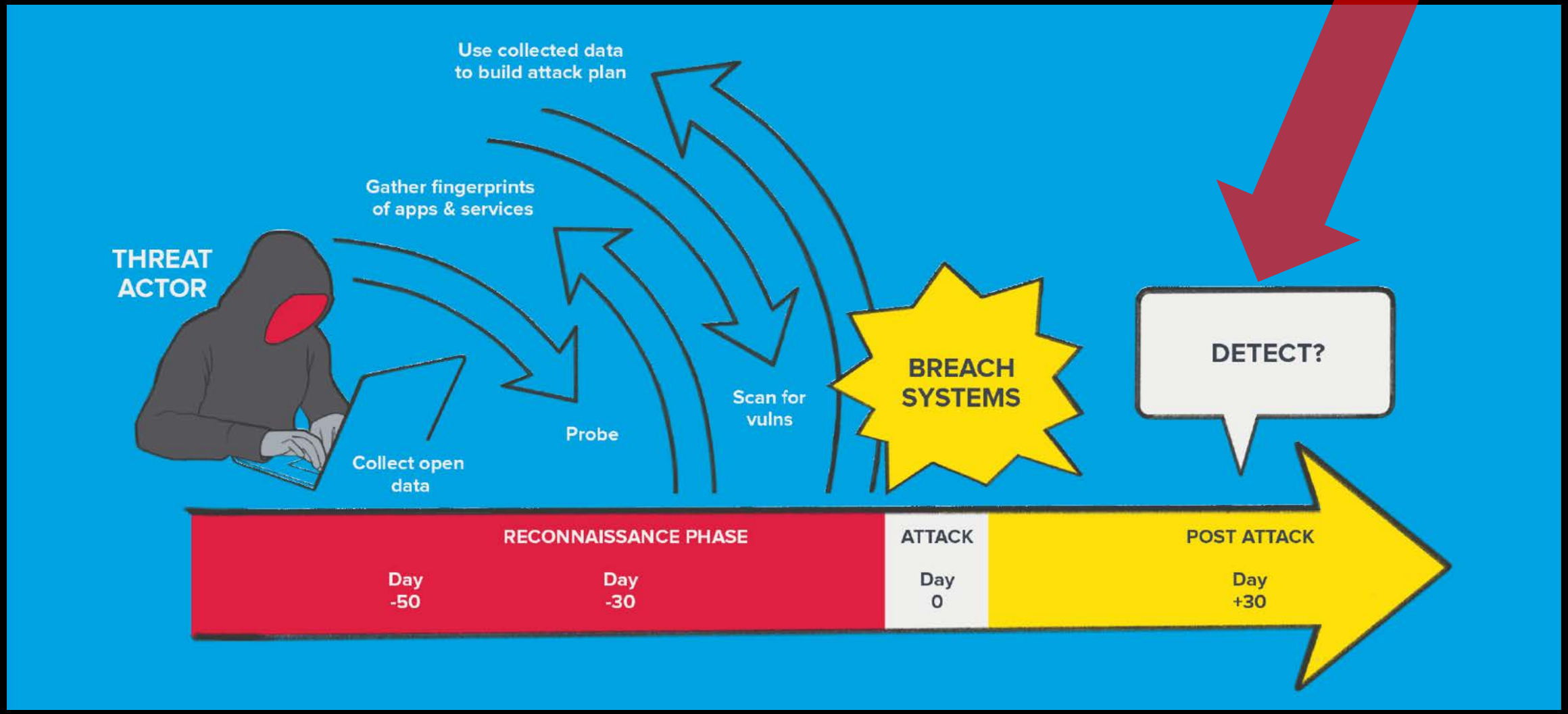
Author and Speaker



What is Threat Intelligence?

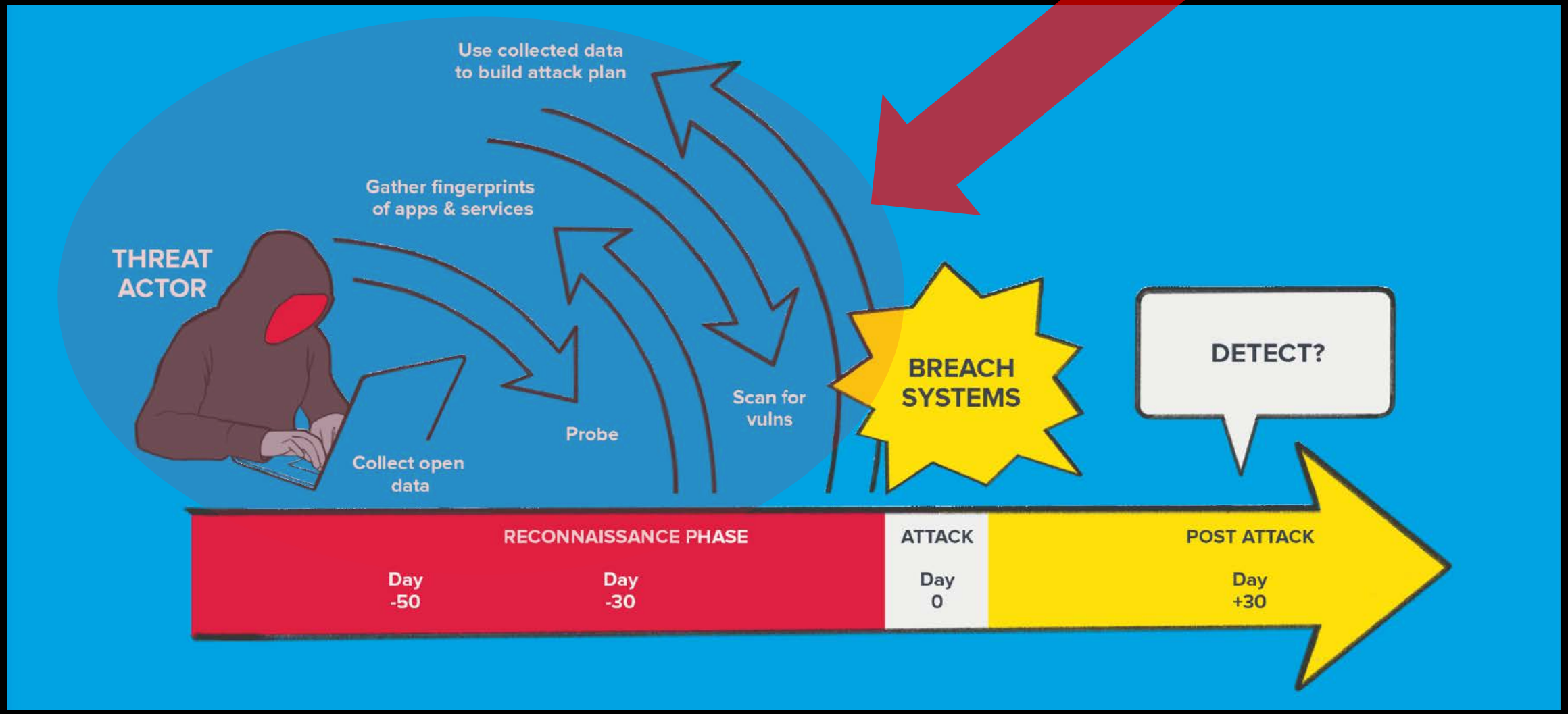


The attack timeline… when we usually detect



© 2017 F5 Networks

Threat intel looks for actions BEFORE attack



© 2017 F5 Networks

Questions to drive your intel efforts

What are the threats that I don't know about?

Where should I focus my attention?

What are my assets worth to attackers? How visible are they?

What useful, feasible decisions about these threats can I make?

© 2017 F5 Networks

How F5 Labs gathers Threat Intelligence

External Partners

- Cyentia
- WhiteHat Security
- Guest CISO's
- WebRoot
- Loryka
- Ponemon
- OPSwat
- Whatcom Cyber School Faculty
- UW Tacoma CyberSec Leadership

F5 Teams

- Security Operations Center
- PD Threat Research
- F5 Security Marketing
- Product Management
- Silverline
- F5 LABS
- F5 Security Incident Response Team
- Security Incident Response Team
- Sales Engineering
- Product Development
- IT Security
- Customer Reports
- Evangelists field reports

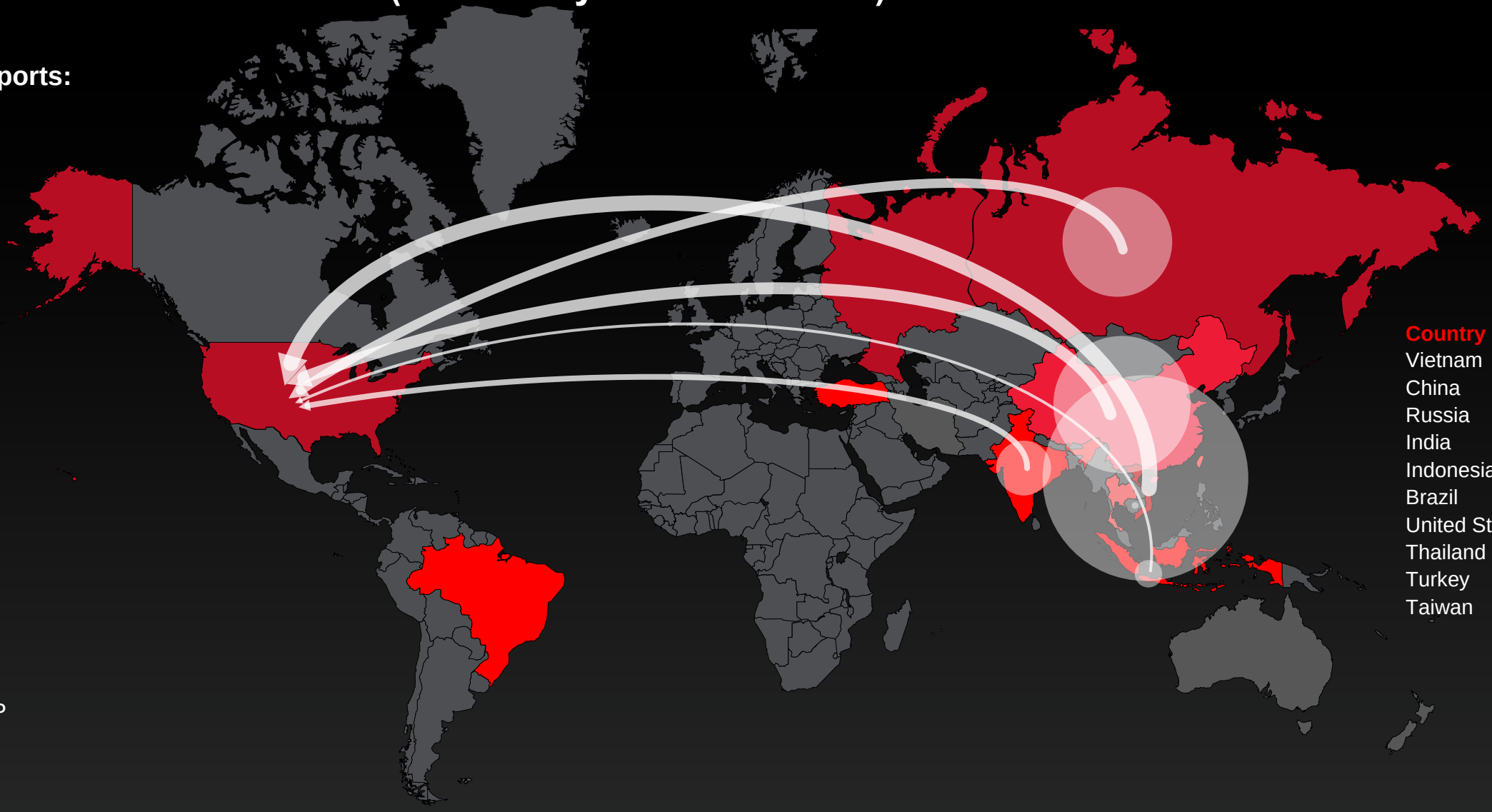
© 2018 F5 Networks

Attacks Targeting US

(last 90 days as of 3/1/2019)

Top 20 targeted ports:

Port	Service
445	SMB
22	SSH
80	HTTP
23	Telnet
3389	MS RDP
1433	MS SQL
8445	JSON RCP
81	HTTP
8080	HTTP
139	Netbios
5555	MS CRM
2323	Telnet
8291	Mikrotik
443	HTTPS
25	SMTP
3306	MySQL
8888	NewsEDGE Remote
5900	Framebuffer
21	FTP
8088	Radan HTTP

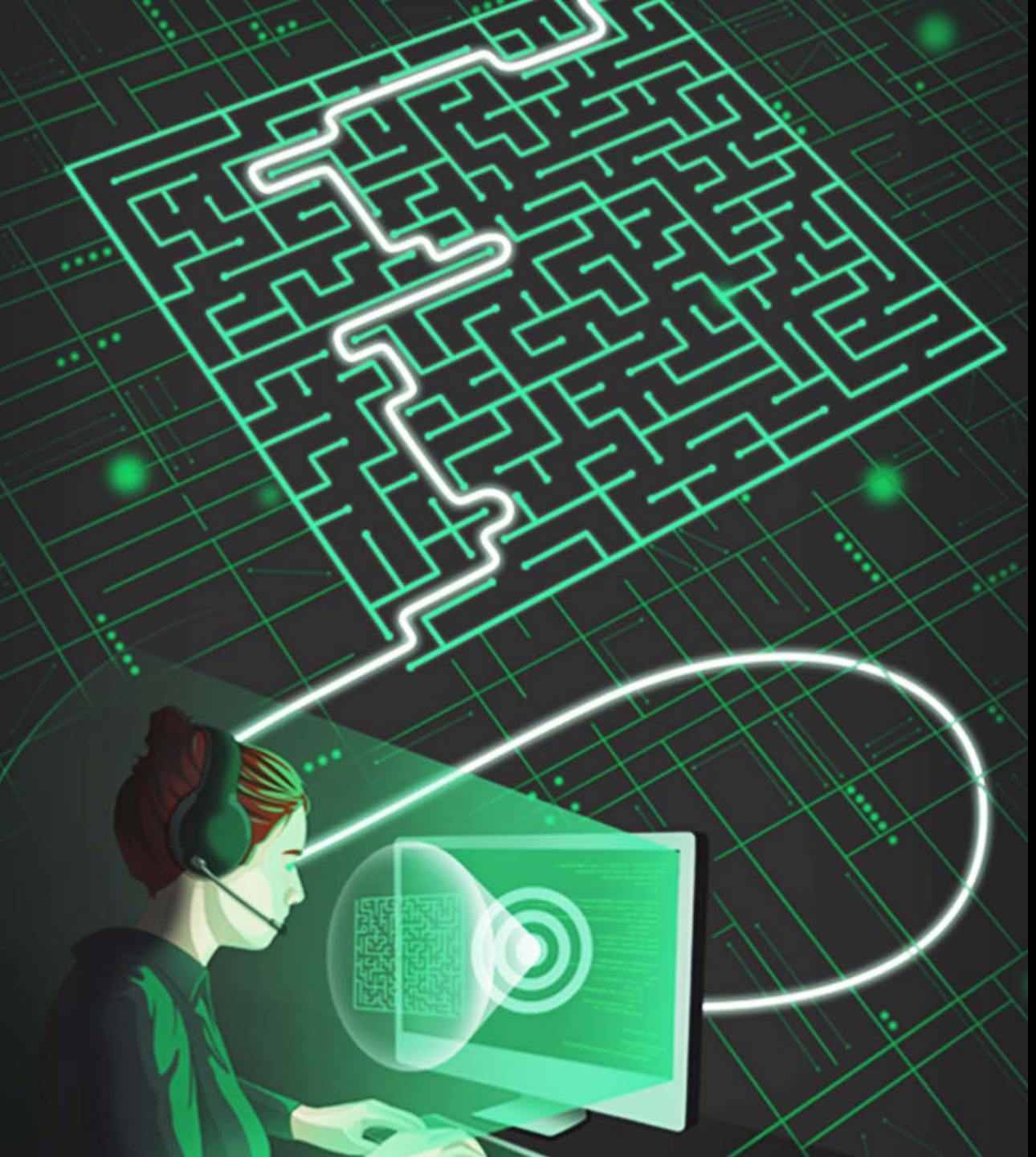


Country

Vietnam
China
Russia
India
Indonesia
Brazil
United States
Thailand
Turkey
Taiwan

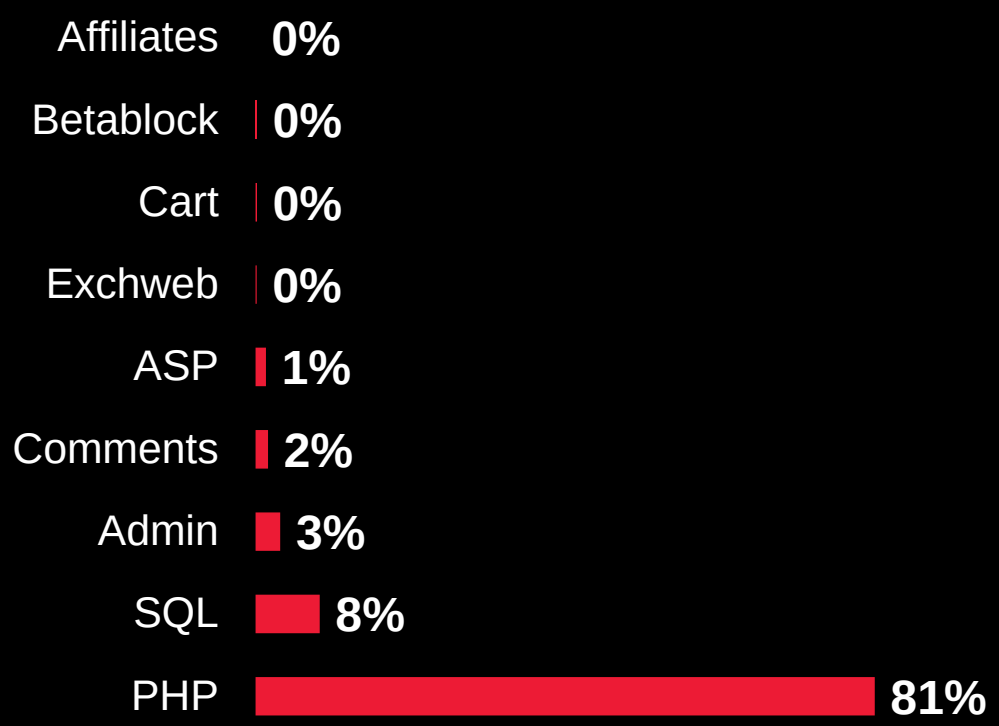
The 7 Things

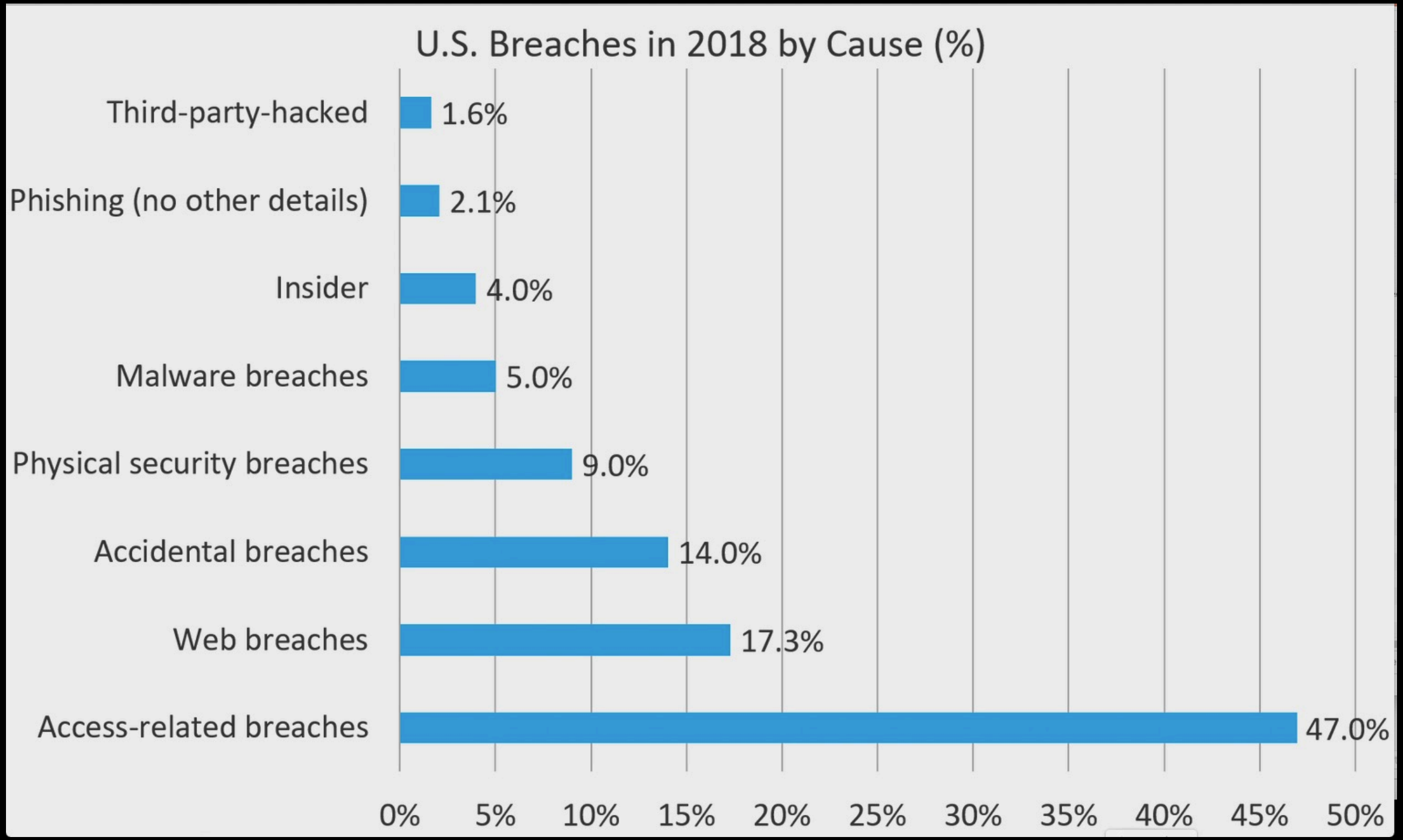
#1 Remember Web App Security



2018 Application Attacks

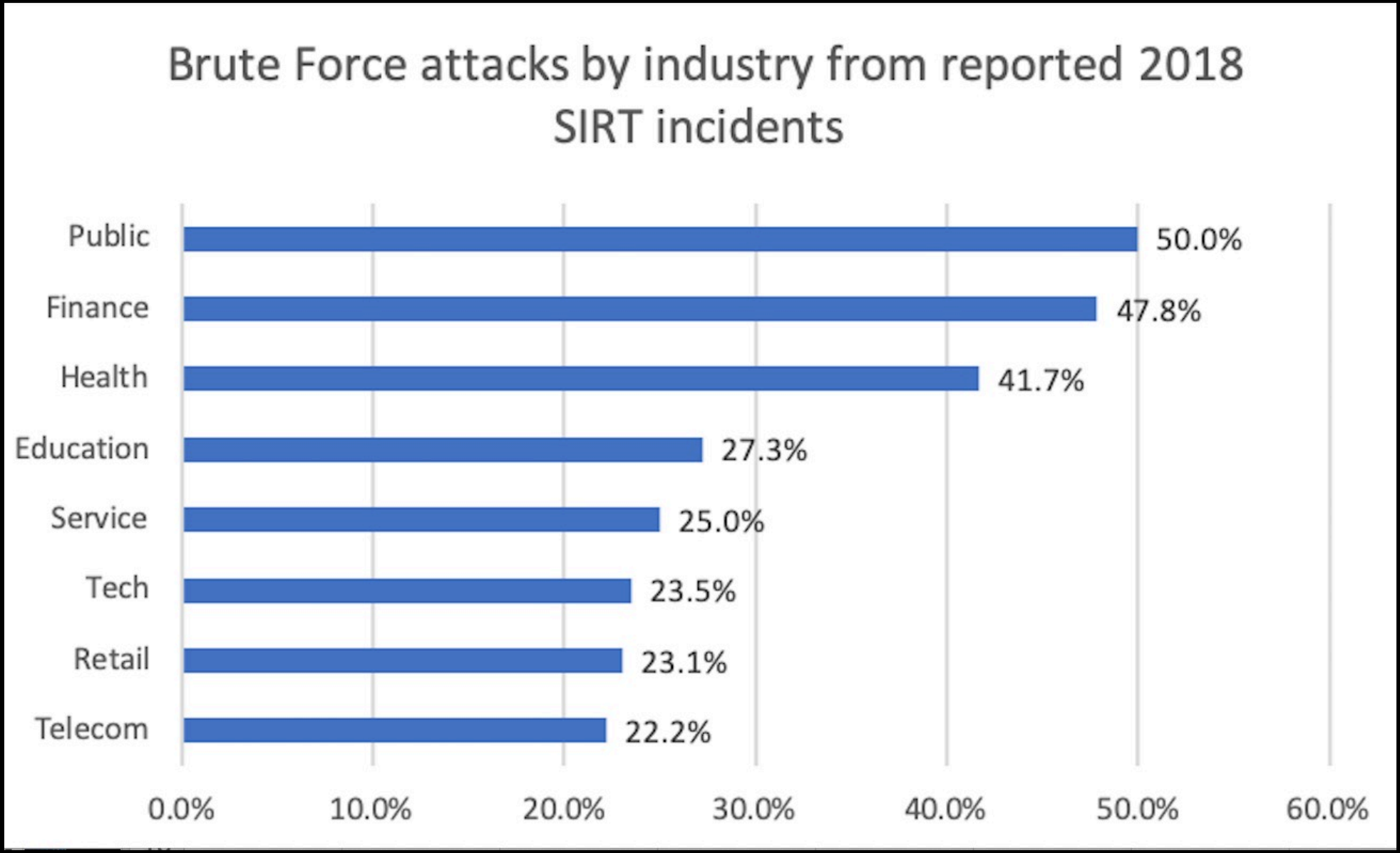
Injection → PHP




U.S. Breaches in 2018 by Cause (%)
Third-party-hacked
1.6%
Phishing (no other details)
2.1%
Insider
4.0%
Malware breaches
5.0%
Physical security breaches
9.0%
Accidental breaches
14.0%
Web breaches
17.3%
Access-related breaches
47.0%
0%
5%
10%
15%
20%
25%
30%
35%
40%
45%
50%

#2 Watch out for Credential Attacks

Brute force



Brute force attacks mitigated by the F5 SIRT, broken down by industry.

Credential Stuffing

In the last 8 years more than 7.1 billion identities have been exposed in data breaches

Nearly 3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more.

YAHOO! — **3 BILLION** accounts

myspace — **427 MILLION** accounts

Adobe — **150 MILLION** accounts

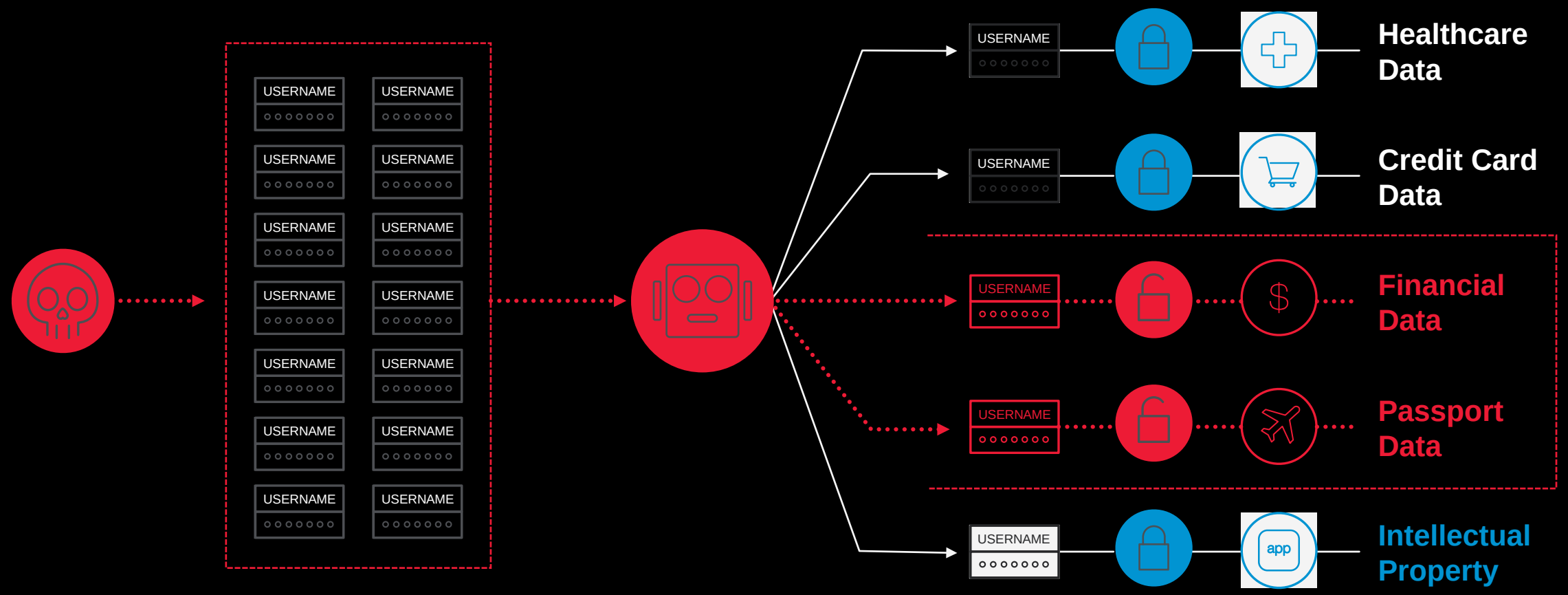
LinkedIn — **117 MILLION** accounts

Dropbox — **70 MILLION** accounts

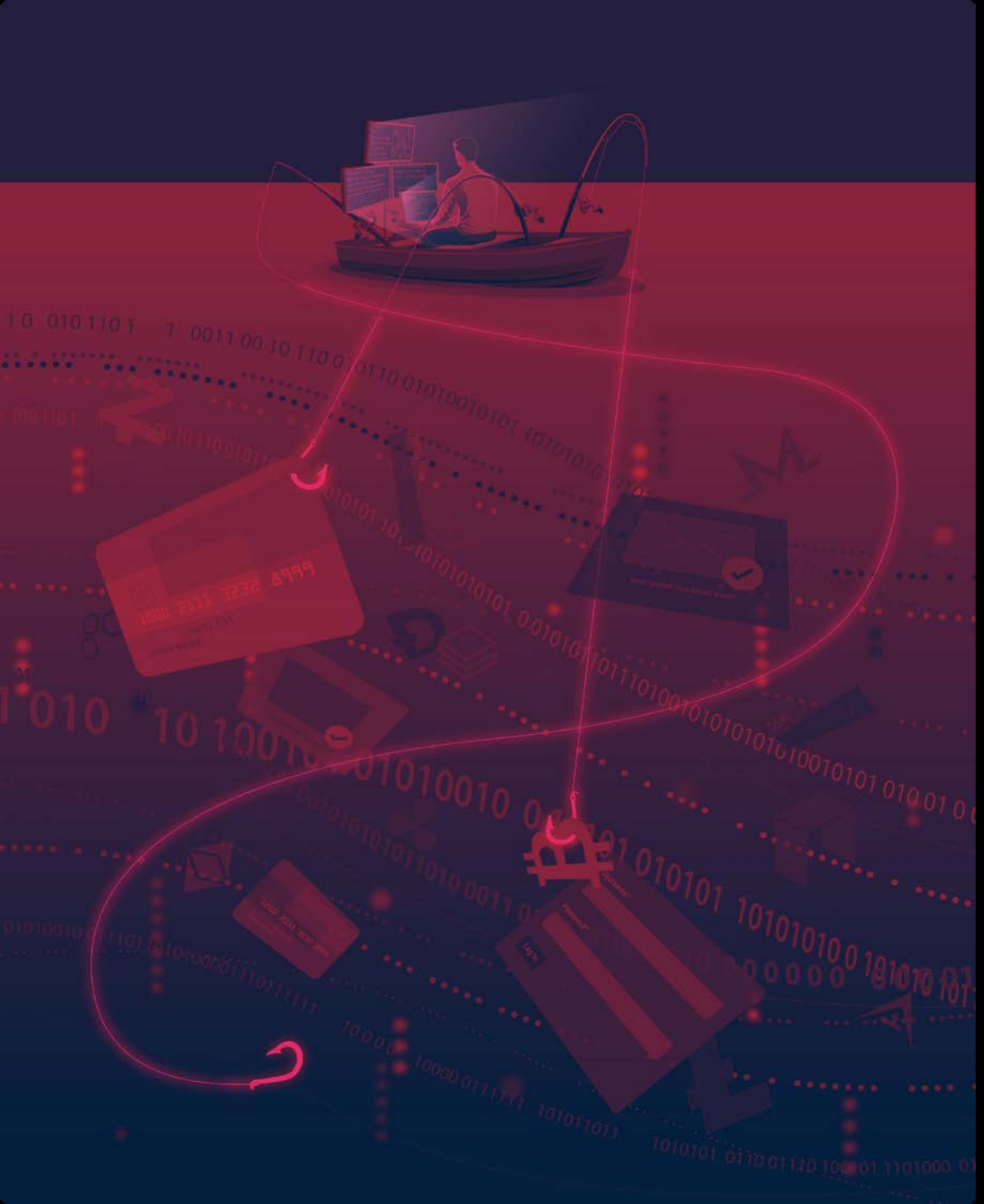
1. Symantec Internet Security Threat Report, April 2017
2. https://www.entrepreneur.com/article/246902#

© 2018 F5 Networks

Credential Stuffing

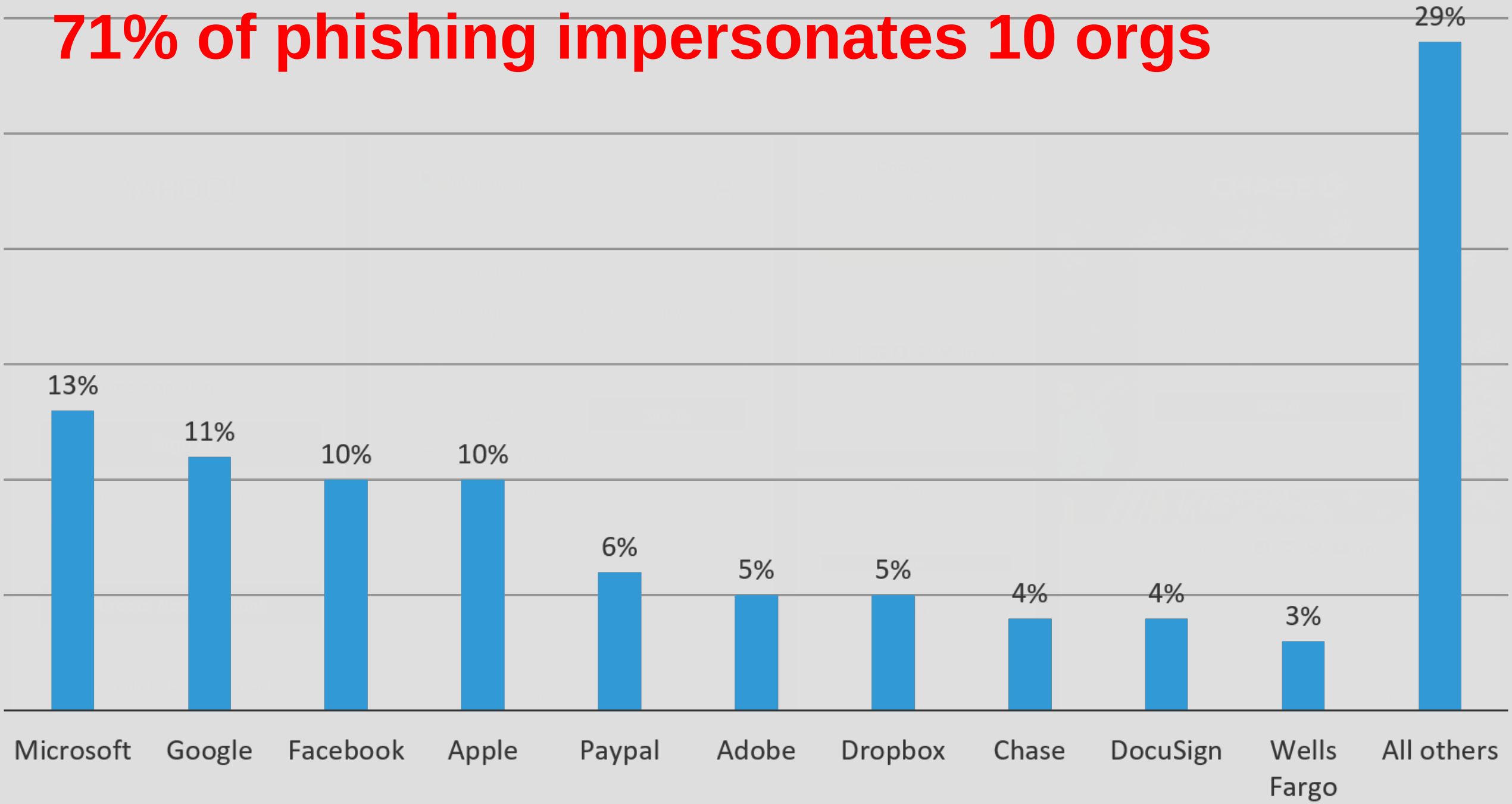


© 2018 F5 Networks



#3
Lots of Phishing

71% of phishing impersonates 10 orgs



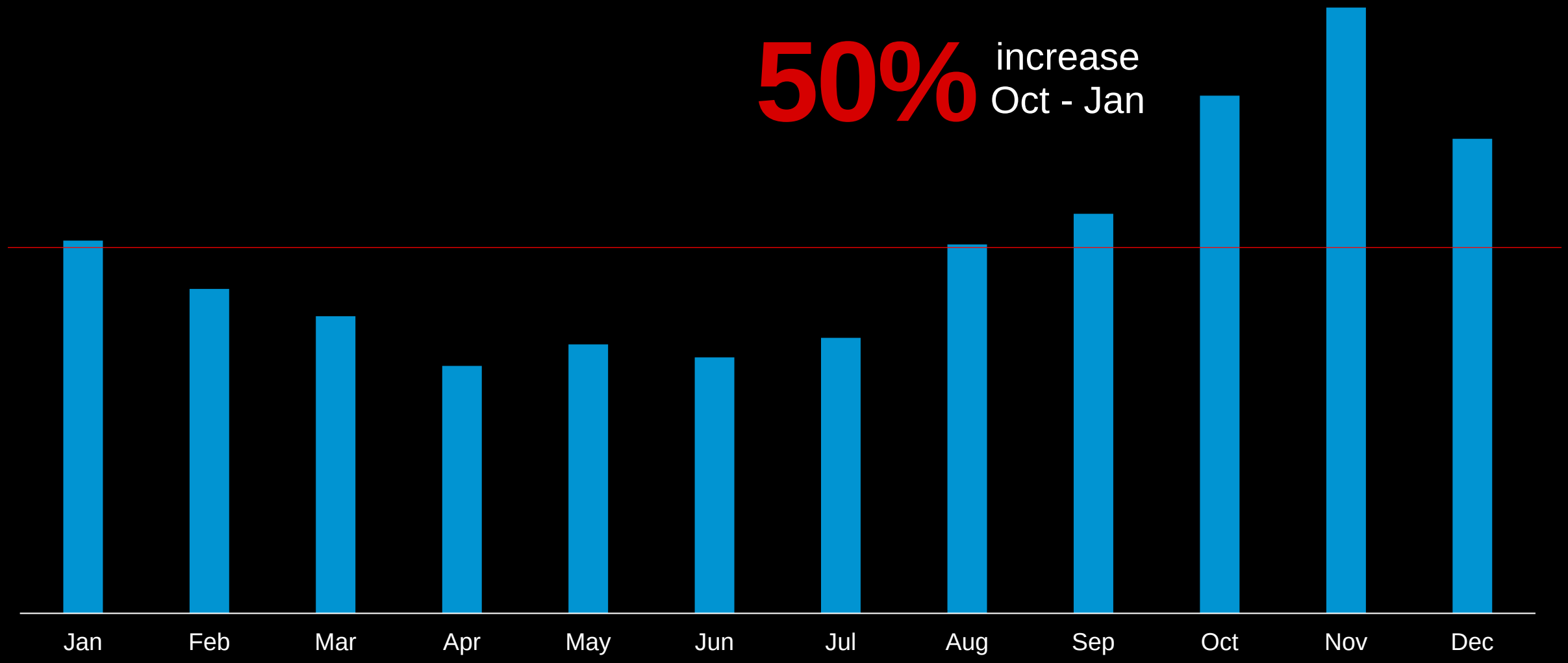
Phishing Kits

```
:: Disclaimer: Developers assume no liability and are not    ::
:: responsible for any misuse or damage caused by BlackEye.  ::
:: Only use for educational purporses!!                      ::

:: Attacking targets without mutual consent is illegal!      ::

[01] Instagram      [17] IGFollowers    [33] Custom     BLACKEYE  v1.1
[02] Facebook       [18] eBay
[03] Snapchat       [19] Pinterest
[04] Twitter        [20] CryptoCurrency
[05] Github         [21] Verizon
[06] Google         [22] DropBox
[07] Spotify        [23] Adobe ID
[08] Netflix        [24] Shopify
[09] PayPal         [25] Messenger
[10] Origin         [26] GitLab
[11] Steam          [27] Twitch
[12] Yahoo          [28] MySpace
[13] Linkedin       [29] Badoo
[14] Protonmail     [30] VK
[15] Wordpress      [31] Yandex
[16] Microsoft      [32] devianART
```

```
CODED BY:  @thelinuxchoice
UPGRADED BY: @suljot_gjoka

[*] Choose an option: 2
[*] Put your local IP (Default 192.168.1.19):
[*] Starting php server...
[*] Send this link to the Victim: 192.168.1.19
[*] Waiting victim open the link ...
```

© 2019 F5 Networks

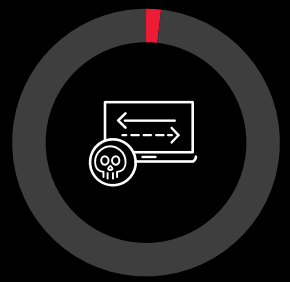
Phishing & Fraud Season Starts in October



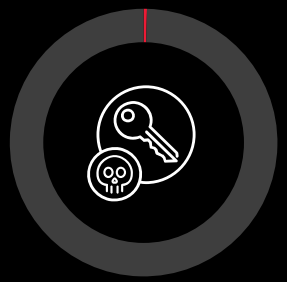
#4 Business Email Compromise is big

Access Attacks Broken down

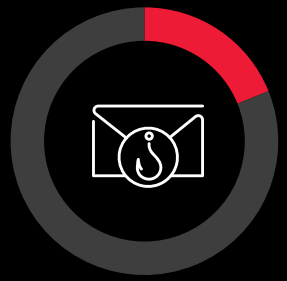
20.1%
Email cited as cause



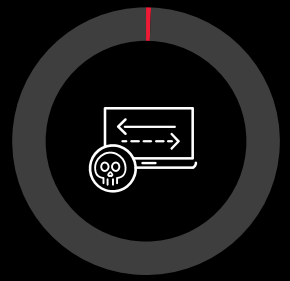
1.8%
Access cred stuffing



0.4%
Access brute

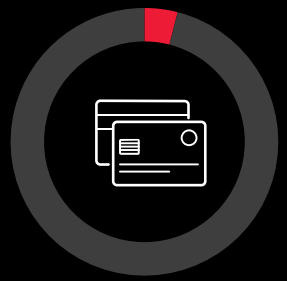


18.9%
Phishing gain access to email

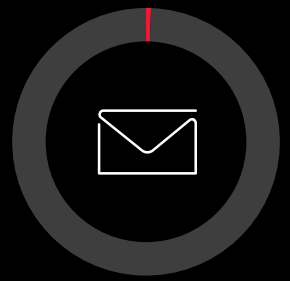


0.6%
Phishing creds stolen

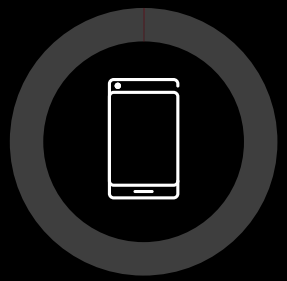
0.4%
Access stolen from third party



4.0%
Access creds stolen

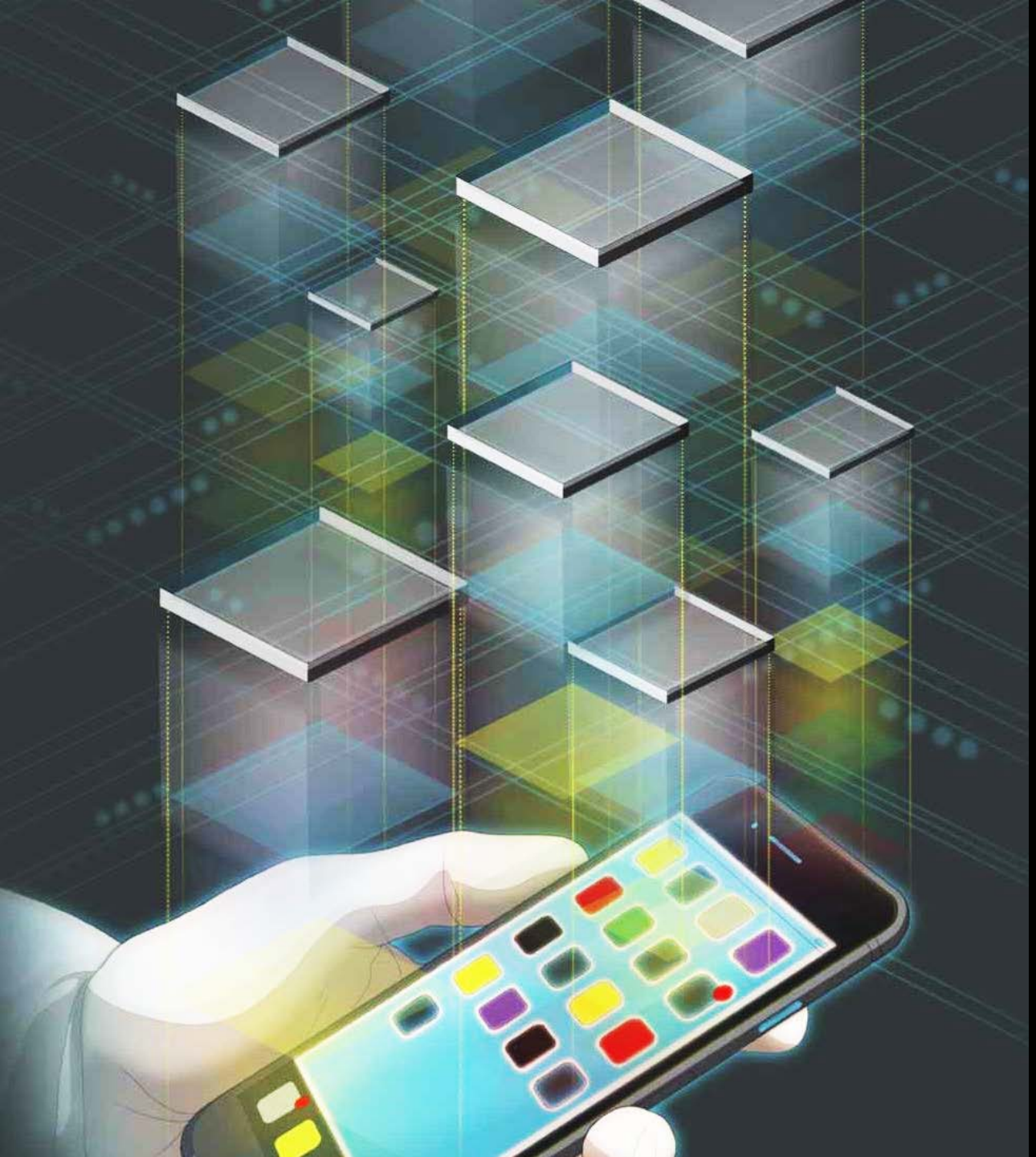


0.6%
Social engineer email



0.1%
Social engineer phone

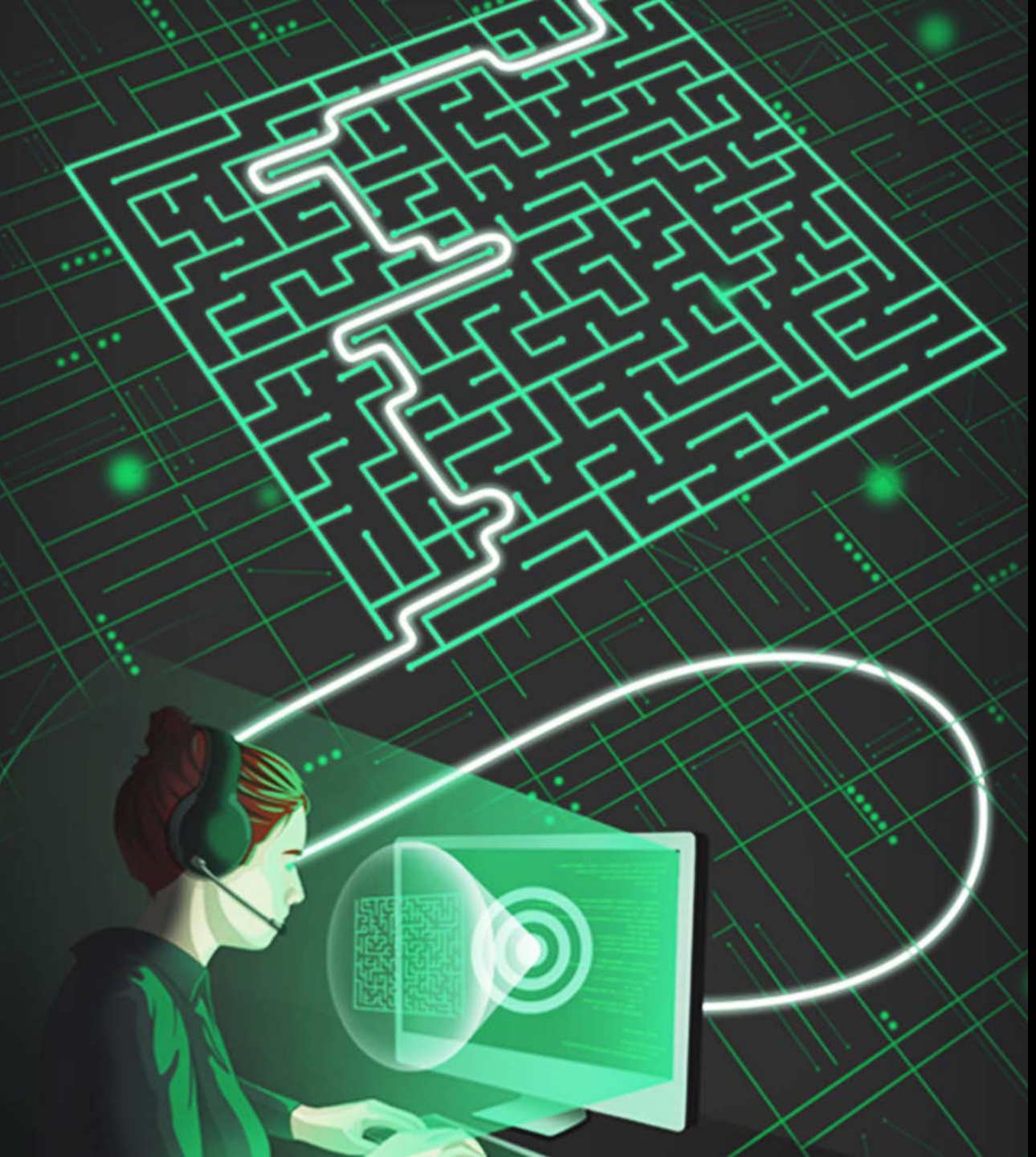
© 2019 F5 Networks



Fraud is powered by Email

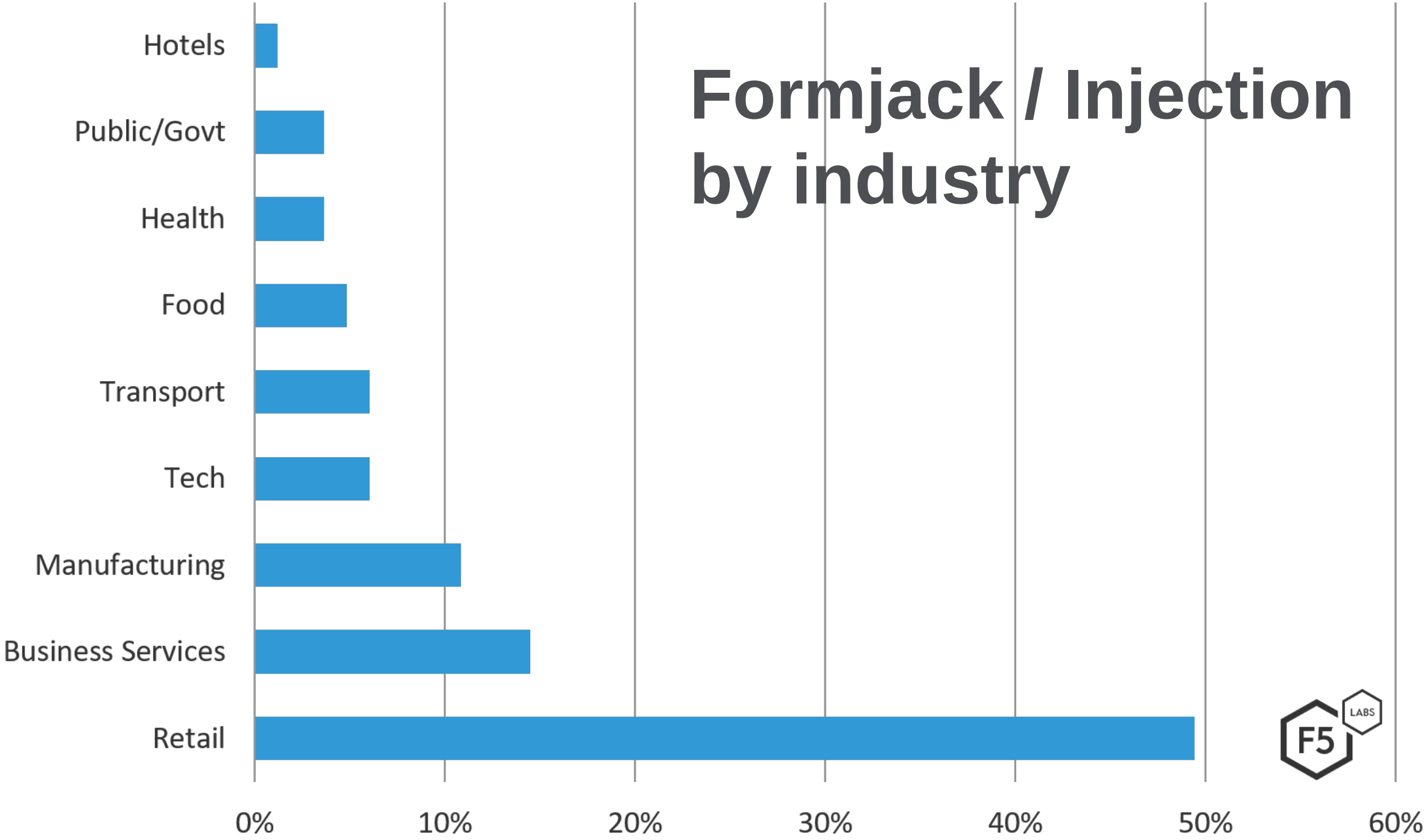
Email is directly attributed as a factor in over a **third** of all breach reports

Four percent of the email hacking cases noted that attackers used a stolen mailbox to phish others within the organization.

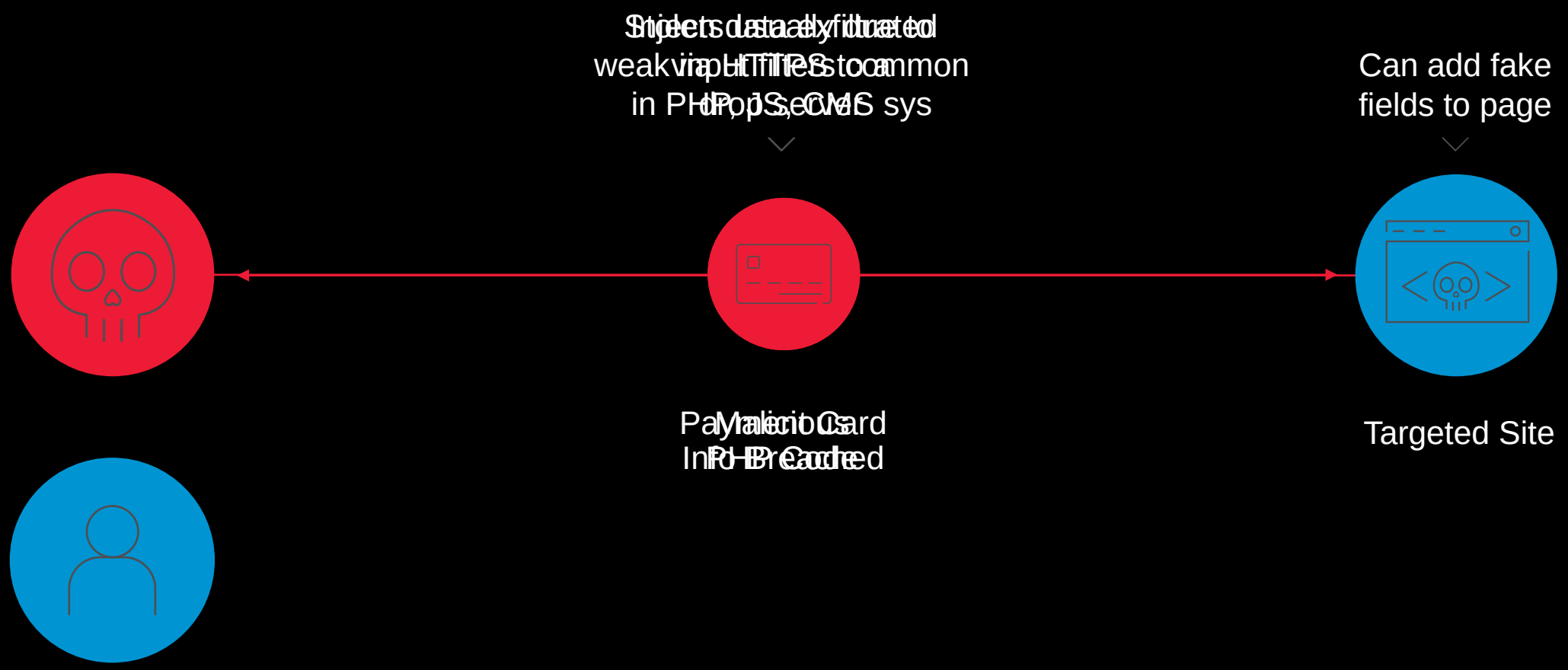


#5
Web Payment card Formjack Injections

Formjack / Injection by industry



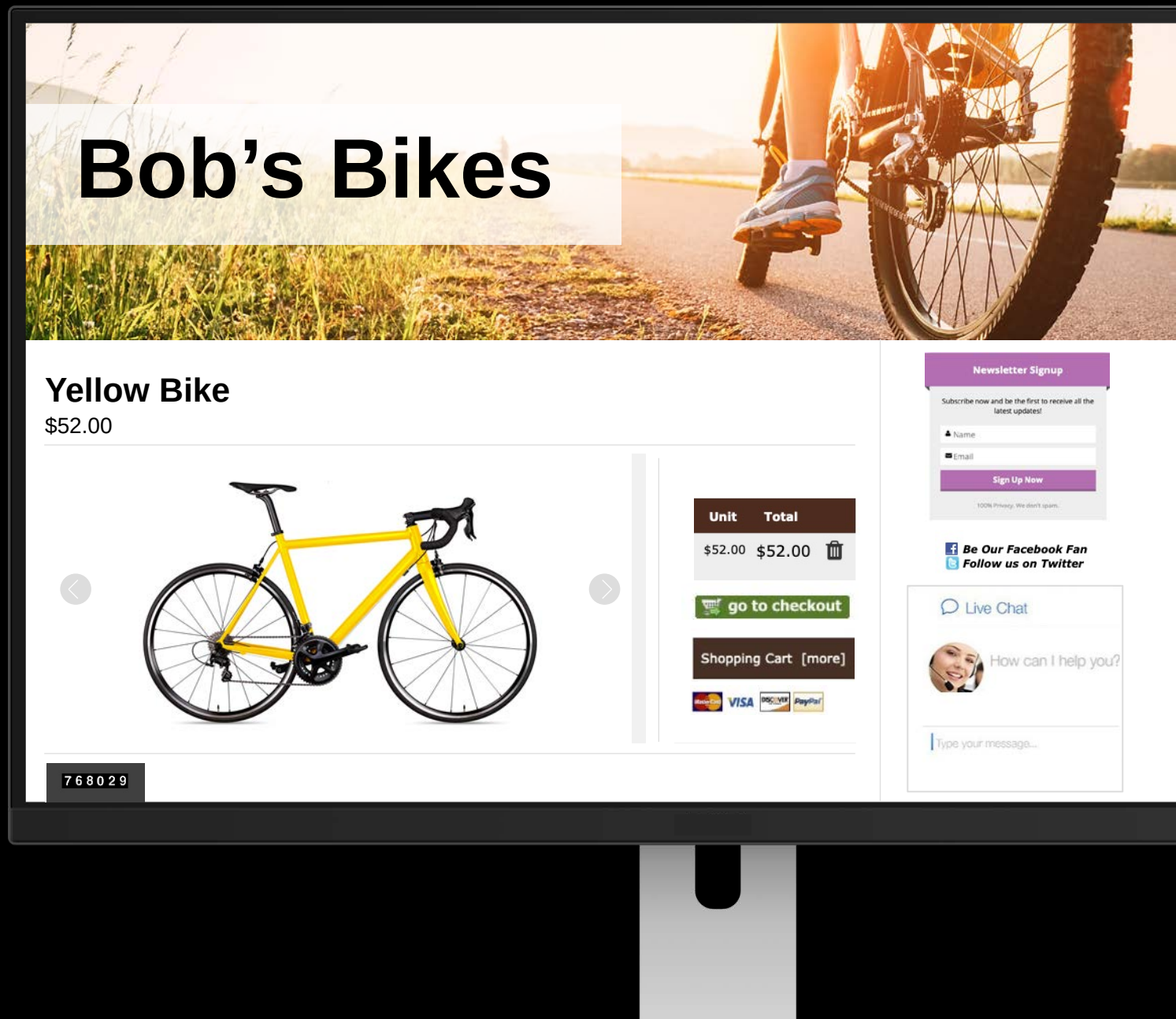
Card Stealing Web Injects



© 2018 F5 Networks

A typical shopping site

Third party widgets/content



All linked off main app site but hosted elsewhere…

#6 Ransomware Everywhere

© 2018 F5 Networks

Ransomware entry vectors

Email delivered malware:

- Malicious attachments
- Lures to download ransomware
- Lures to booby-trapped sites (drive-by browser exploits)

Self-propagating:

- Weak File Shares (SMB)
- Well-known exploits
- Stolen privileges from earlier infection

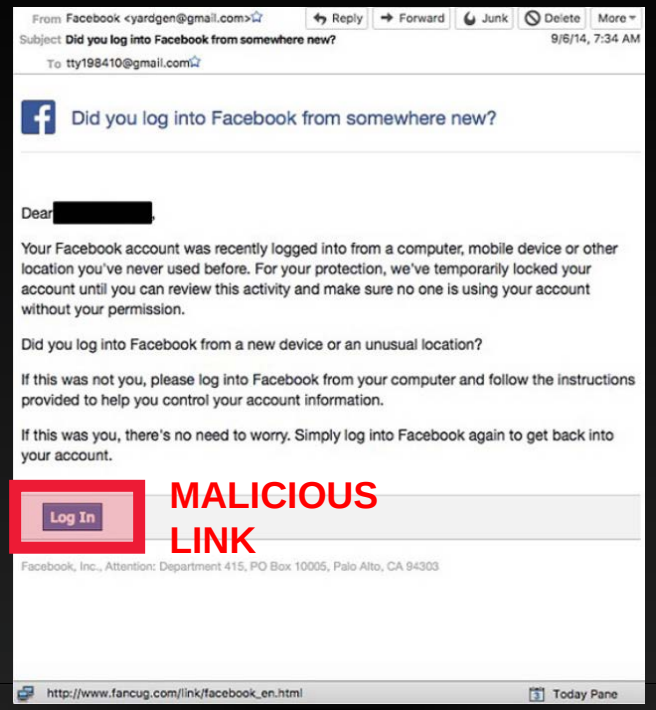
Credential Attack:

- Default credentials
- Credential stuffing
- Password spray

Malicious Web Link vs Attachment

3x

Phishing emails are **3 times more** likely to have a malicious link than a malicious attachment.



From Facebook <yardgen@gmail.com>
Reply | Forward | Junk | Delete | More
Subject Did you log into Facebook from somewhere new?
9/6/14, 7:34 AM
To tty198410@gmail.com

Did you log into Facebook from somewhere new?

Dear [redacted],

Your Facebook account was recently logged into from a computer, mobile device or other location you've never used before. For your protection, we've temporarily locked your account until you can review this activity and make sure no one is using your account without your permission.

Did you log into Facebook from a new device or an unusual location?

If this was not you, please log into Facebook from your computer and follow the instructions provided to help you control your account information.

If this was you, there's no need to worry. Simply log into Facebook again to get back into your account.

Log In

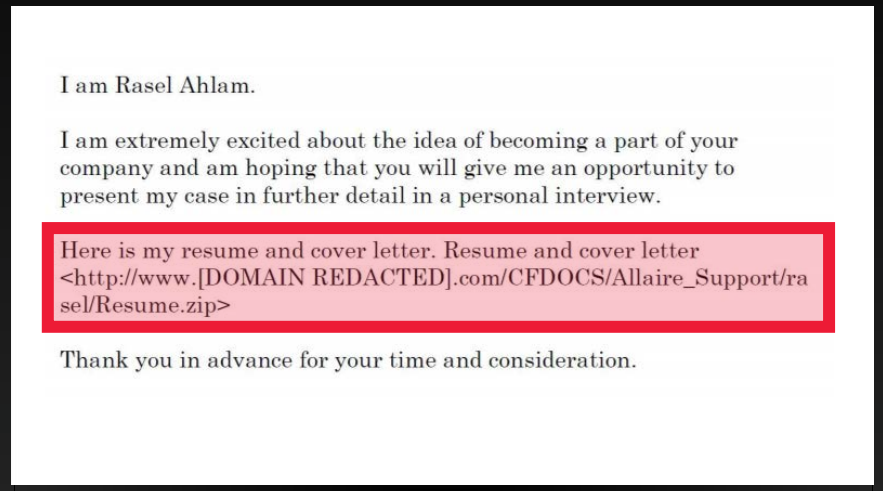
Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

http://www.fancug.com/link/facebook_en.html
Today Pane

MALICIOUS LINK

Email sent from North Korean ATP in Sony compromise.

MALICIOUS FILE



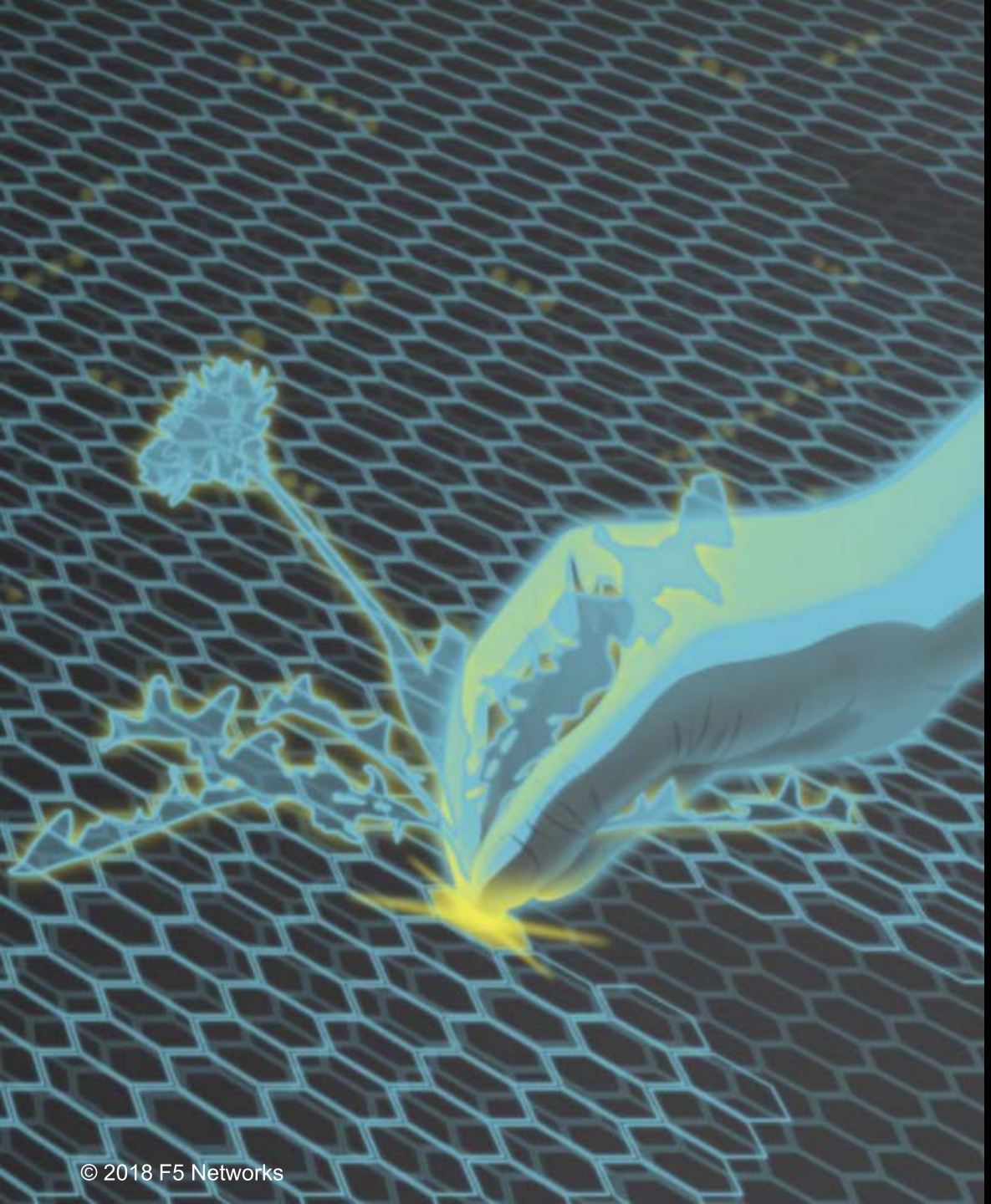
I am Rasel Ahlam.

I am extremely excited about the idea of becoming a part of your company and am hoping that you will give me an opportunity to present my case in further detail in a personal interview.

Here is my resume and cover letter. Resume and cover letter <http://www.[DOMAIN REDACTED].com/CFDOCS/Allaire_Support/rasel/Resume.zip>

Thank you in advance for your time and consideration.

Email sent from North Korean APT related to Bangladesh Bank heist.

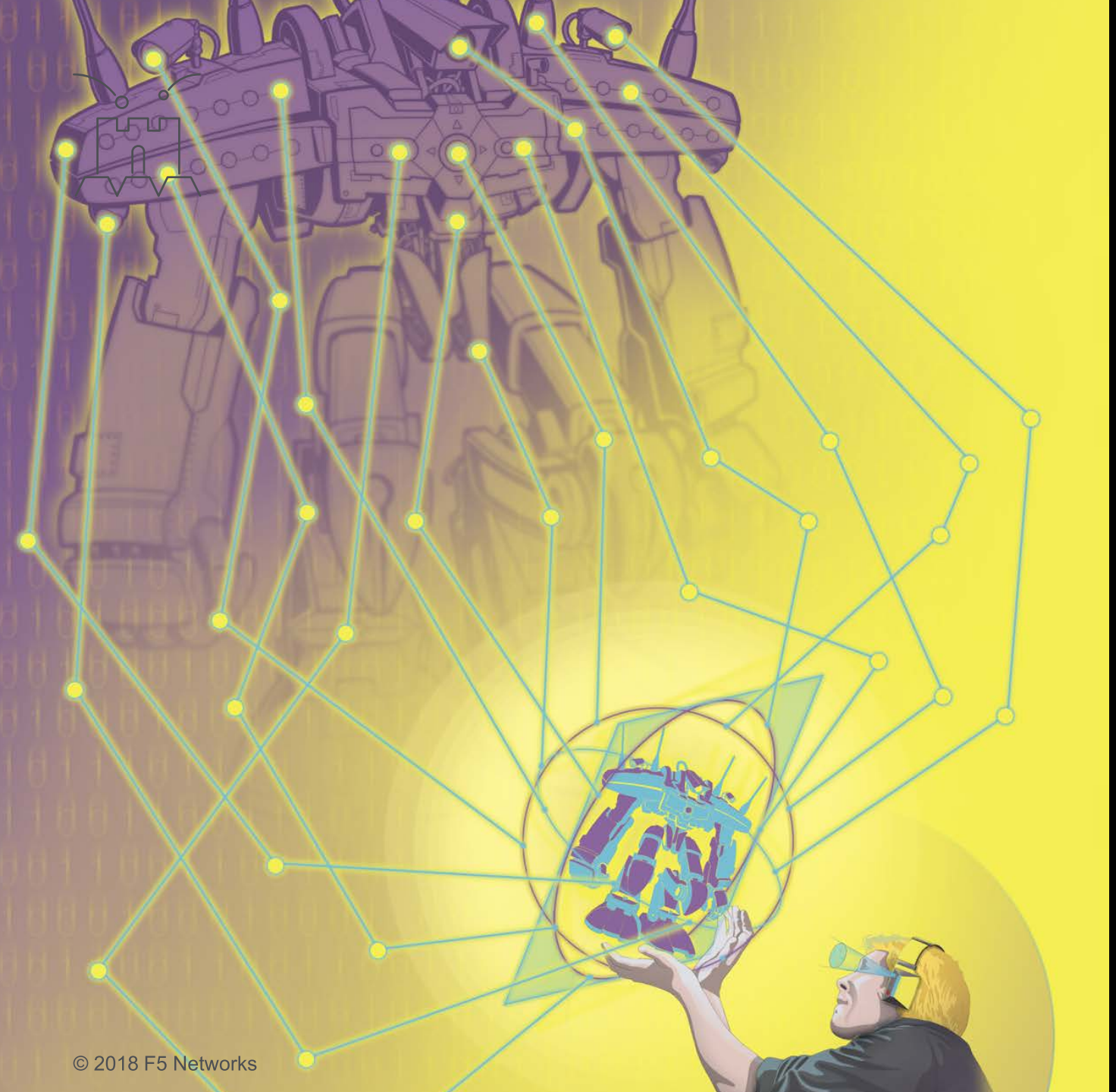


Attackers Hide Malware in Encryption

70% of all Internet traffic is encrypted

68% of malware phones home over port 443

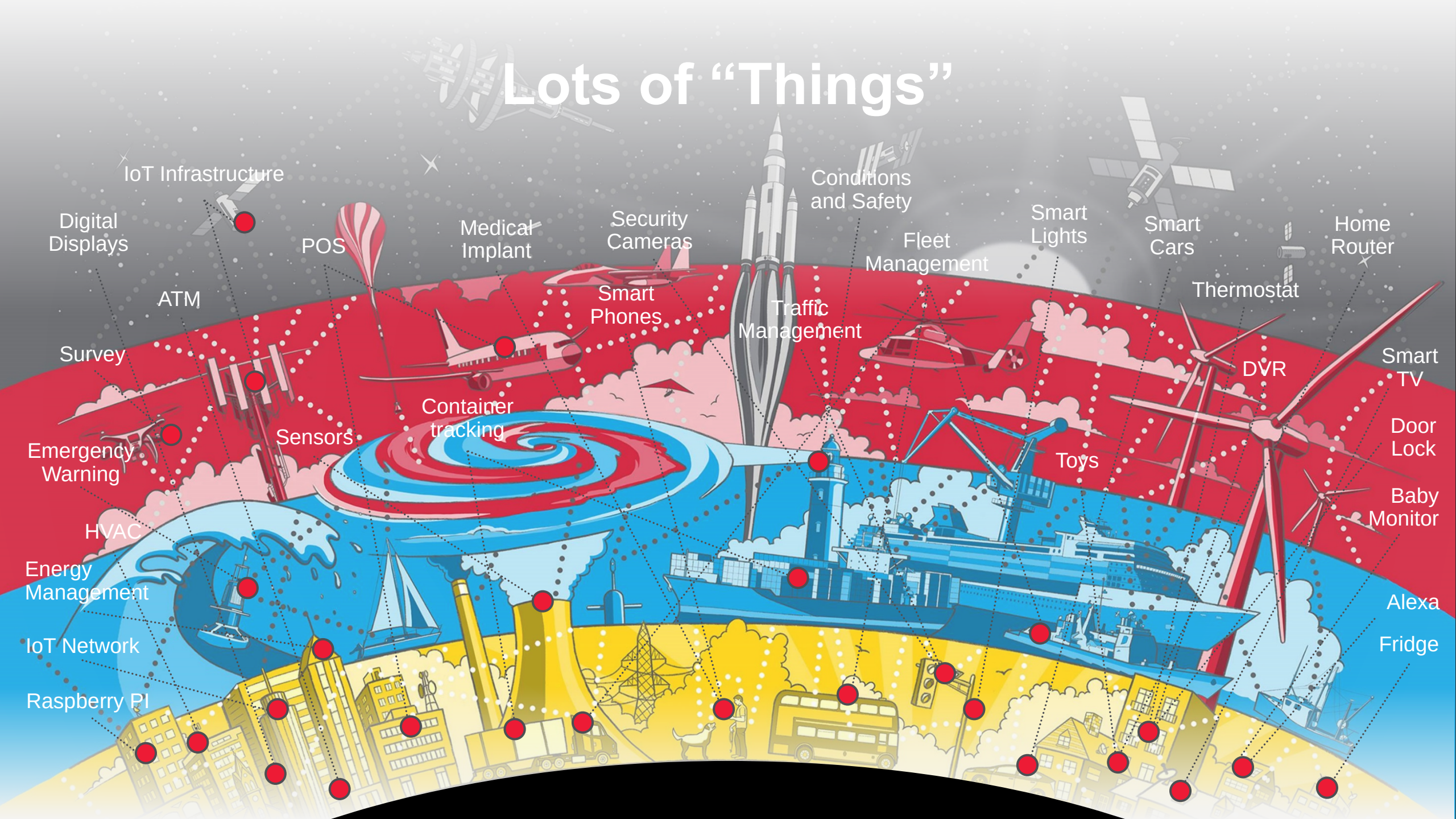
© 2018 F5 Networks



#7 Internet Of Things devices are easily hacked

© 2018 F5 Networks

Lots of “Things”



Common IoT Set Up

Port Forwarding Video

The following video gives an overview and explanation to the following questions. What is port forwarding? How does port forwarding work?

Port forwarding is a f
to devices on an IP (
a surveillance DVR, you will configure your router to forward incoming Internet requests on the port that the DVR uses to be routed / forwarded to the DVR. This enables you to access your DVR remotely over the Internet. The below network diagram illustrates a typical home or business network setup that includes a surveillance DVR. The diagram would be the same for an IP camera. Simply replace the below surveillance DVR in the diagram with an IP camera and all of the concepts are exactly the same.

DLink Port Forwarding Setup (Virtual Server)

DLink port forwarding, also known as virtual server, allows you to configure inbound Internet connections to your router to be routed to specific devices on the network. In the context of CCTV cameras and surveillance systems, your router is configured to forward requests to your surveillance DVR (standalone or Geovision) or directly to IP cameras. The IP address that your router assigns to your DVR is an internal IP address (LAN) that normally can not be accessed from outside of your local network. This is why port forwarding setup is needed.

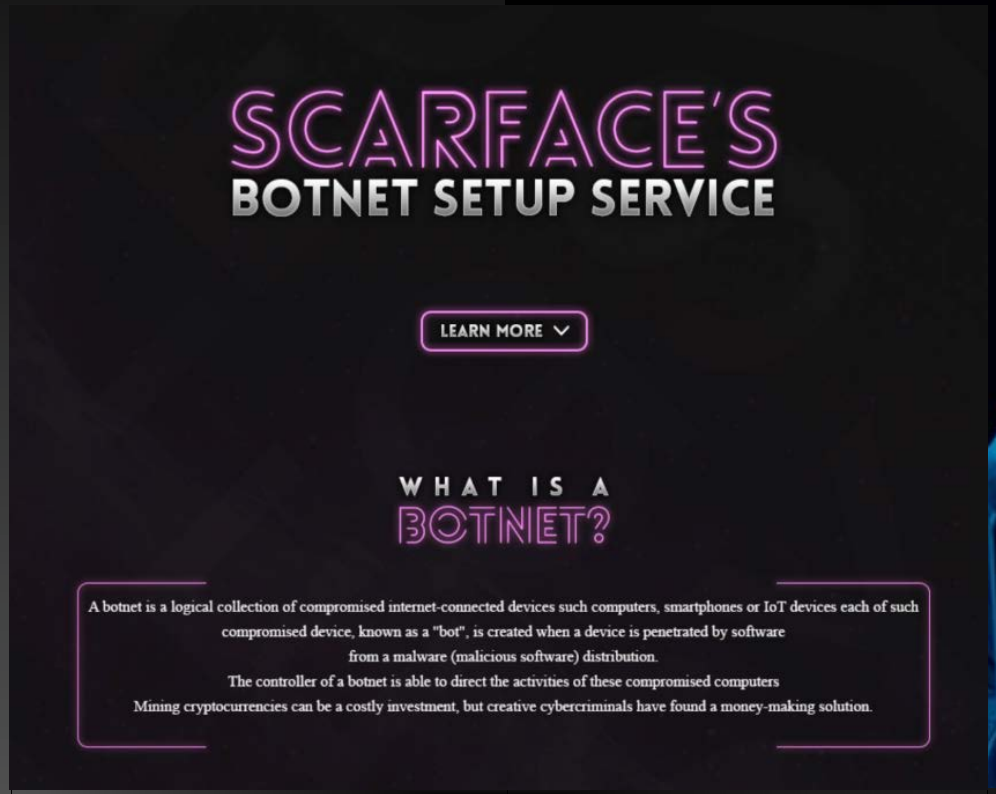
1. Open your D-Link router's control panel by going to the IP address http://192.168.0.1/ in a web browser. You will be prompt for a password. If you did not setup a password on your router, the **dlink default password** is blank. Enter admin for the username and leave the password blank.

Coffee machines scanning our honeypot


```
{ "_id" : { "protocol" : "http", "timestamp" : { "$date" : "2018-07-
19T20:31:04.000-0700" }, "source_ip" : "185.112.249.24", "session_http" : {
"request" : { "body" : "", "header" : [ [ "accept", "*/*" ], [ "user-agent",
"Keurig K575 Coffee Maker" ] ], "verb" : "GET", "path" : "/" } },
"source_port" : 56946, "destination_port" : 80, }

{ "_id" : { "protocol" : "http", "timestamp" : { "$date" : "2018-07-
23T12:16:41.000-0700" }, "source_ip" : "185.112.249.24", "session_http" : {
"request" : { "body" : "", "header" : [ [ "accept", "*/*" ], [ "user-agent",
"Keurig K575 Coffee Maker" ] ], "verb" : "GET", "path" : "/" } },
"source_port" : 49180, "destination_port" : 80, }

{ "_id" : { "protocol" : "http", "timestamp" : { "$date" : "2018-07-
25T10:04:52.000-0700" }, "source_ip" : "185.112.249.24", "session_http" : {
"request" : { "body" : "", "header" : [ [ "accept", "*/*" ], [ "user-agent",
"Keurig K575 Coffee Maker" ] ], "verb" : "GET", "path" : "/" } },
"source_port" : 40755, "destination_port" : 80, }

{ "_id" : { "protocol" : "http", "timestamp" : { "$date" : "2018-07-
25T10:14:46.000-0700" }, "source_ip" : "185.112.249.24", "session_http" : {
"request" : { "body" : "", "header" : [ [ "accept", "*/*" ], [ "user-agent",
"Keurig K575 Coffee Maker" ] ], "verb" : "GET", "path" : "/" } },
"source_port" : 40755, "destination_port" : 80, }

{ "_id" : {"protocol" : "http", "timestamp" : { "$date" : "2018-07-
28T06:29:53.000-0700" }, "source_ip" : "185.112.249.28", "session_http" : {
"request" : { "body" : "", "header" : [ [ "accept", "*/*" ], [ "user-agent",
"Keurig K575 Coffee Maker" ] ], "verb" : "GET", "path" : "/" } },
"source_port" : 50225, "destination_port" : 80, }
```

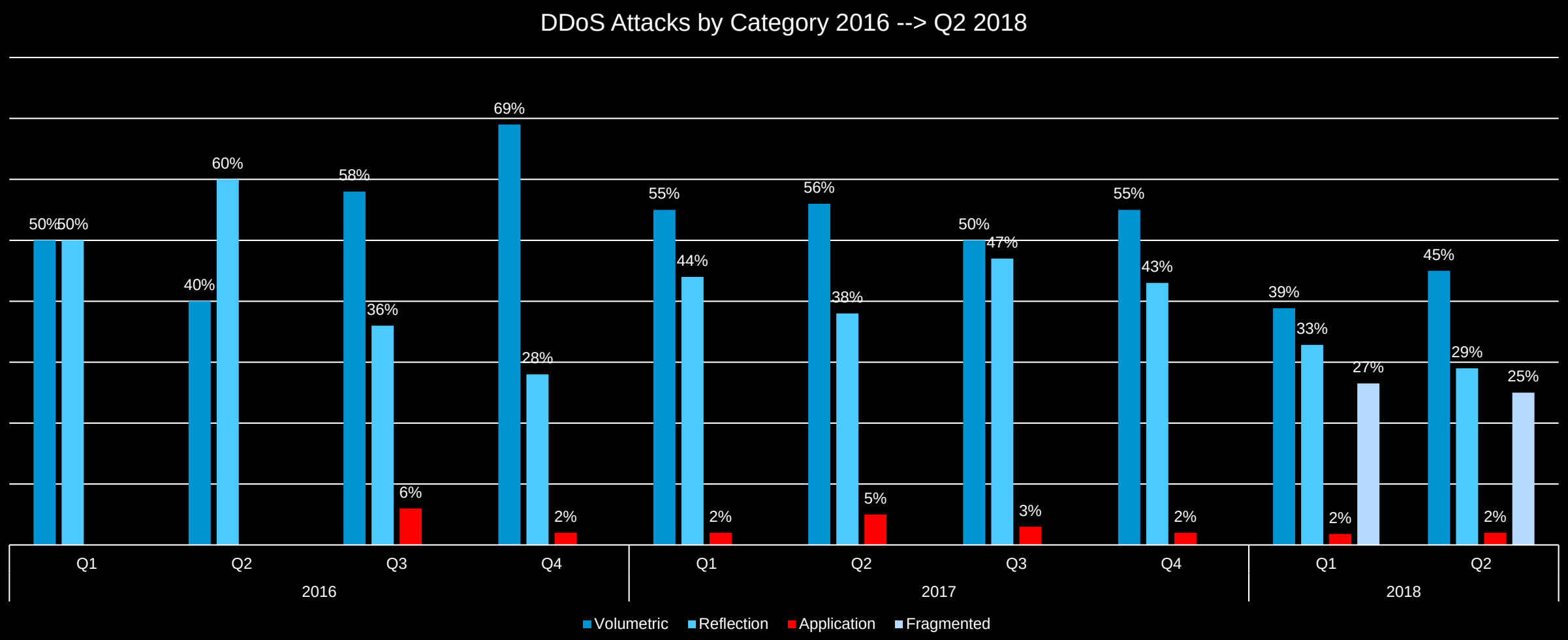
RFC2324: Hyper Text Coffee Pot Control Protocol

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

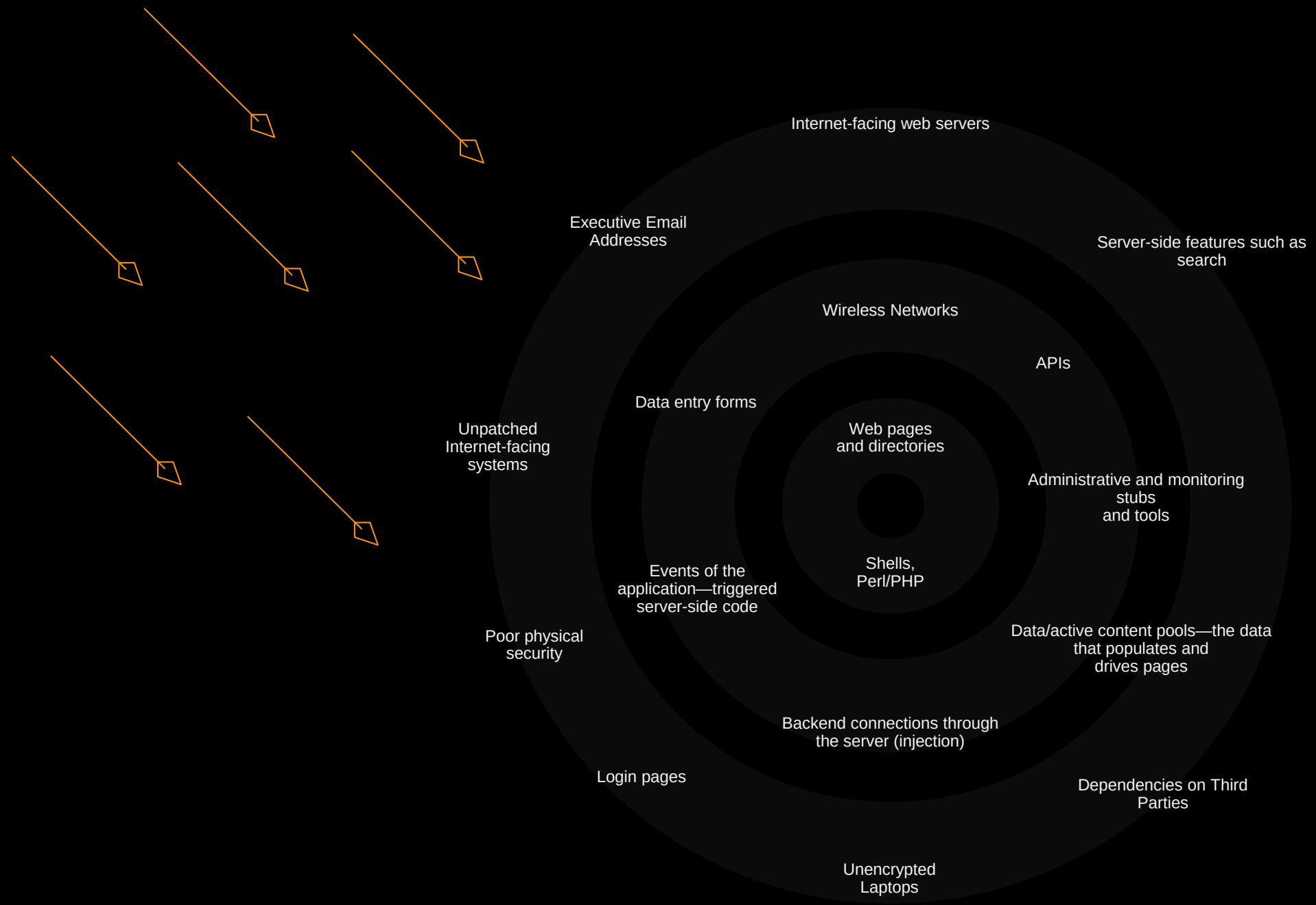
DDoS Attacks By Category (SOC-Mitigated)



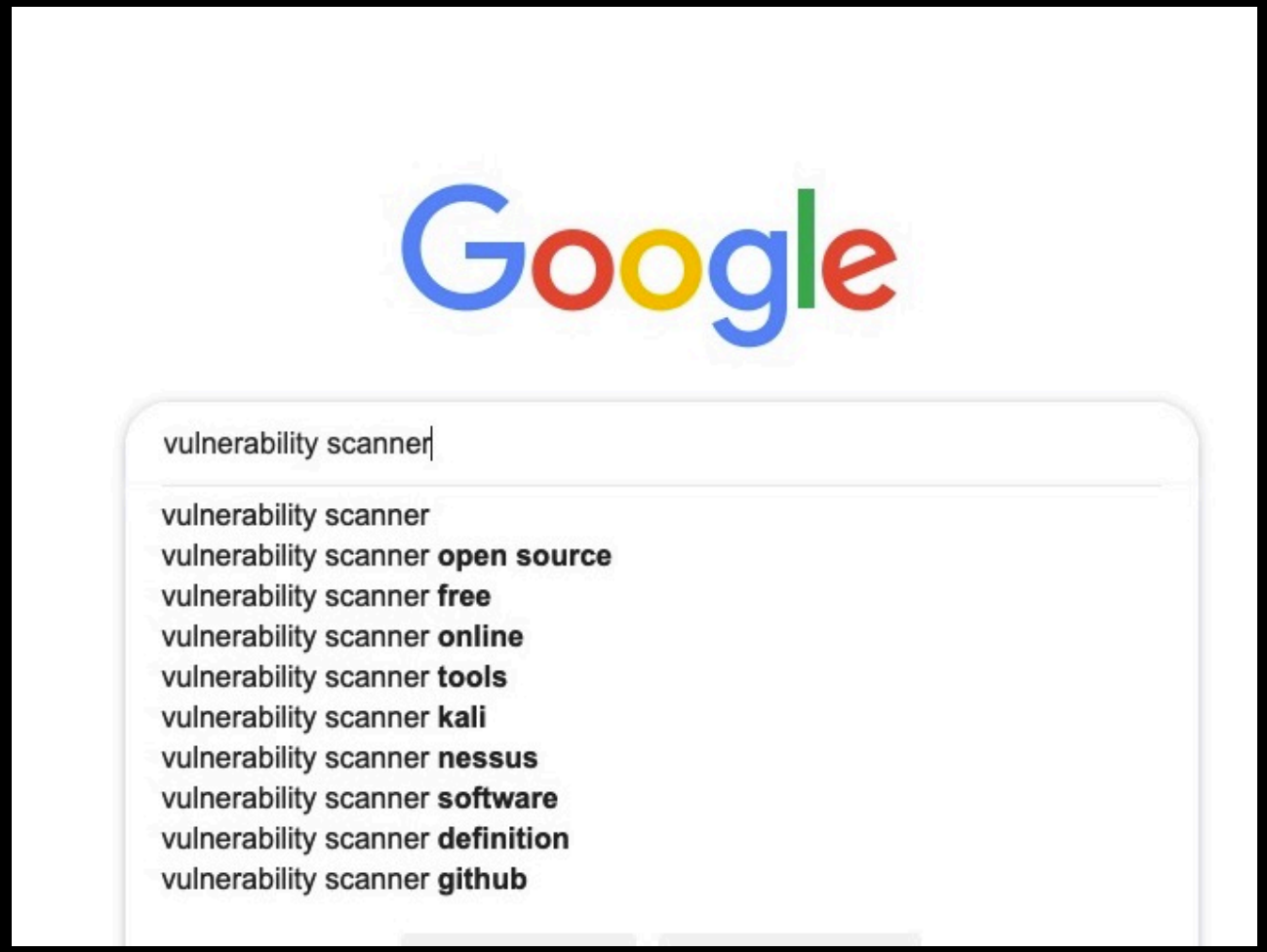
© 2016 F5 Networks

Data informs Defense

Reduce Your Attack Surface



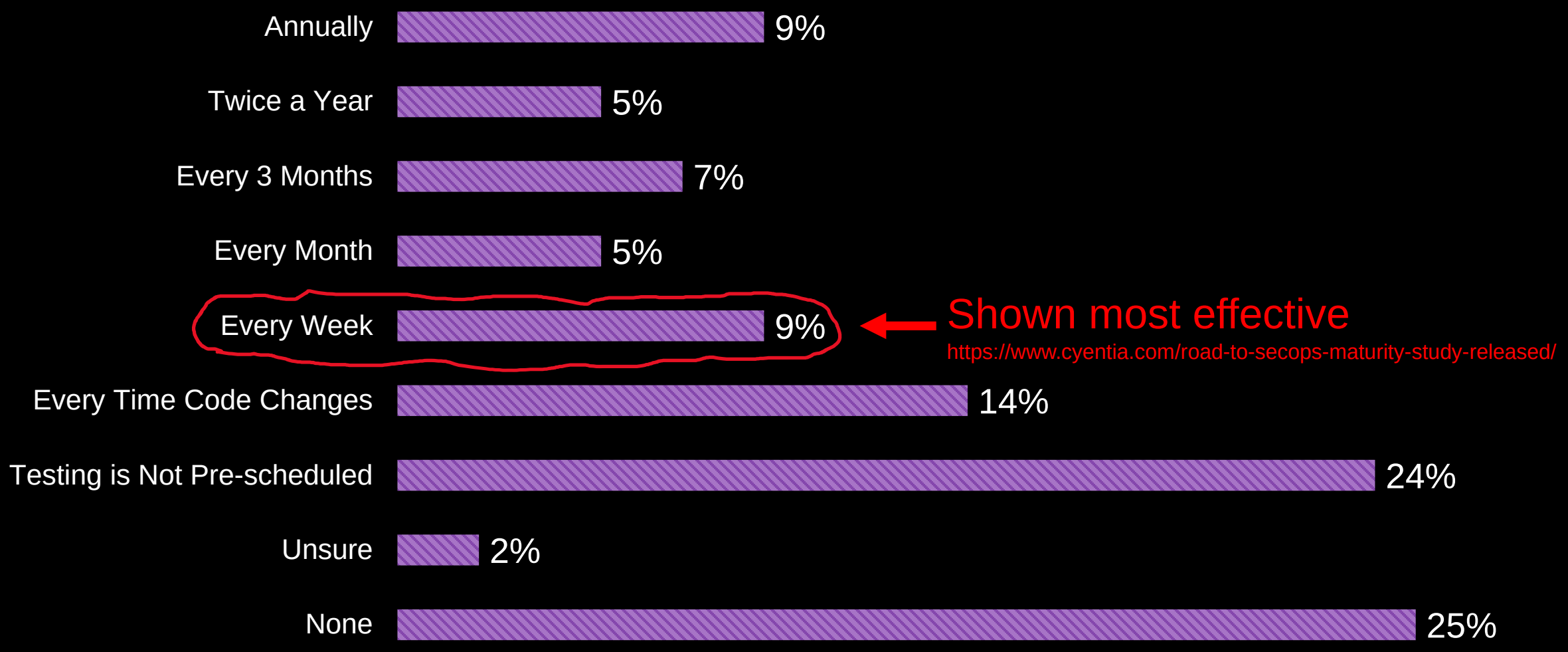
Reduce Your Attack Surface



At least know what problems you might have

© 2018 F5 Networks

App Scanning Frequency



2018 F5 App Protect Report Survey

© 2018 F5 Networks

Basic phishing defense

Filter email for executable attachments

© 2018 F5 Networks

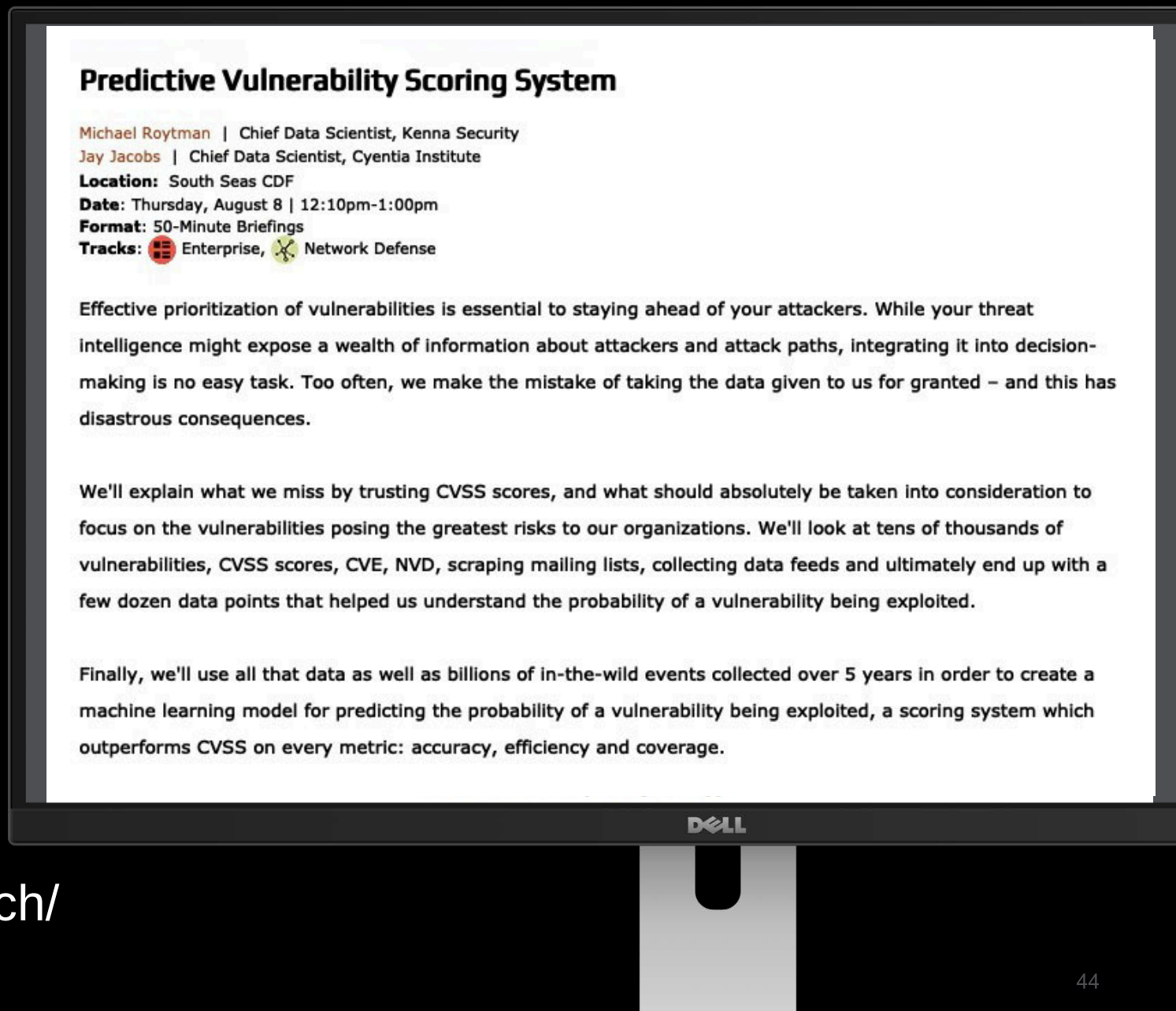
Basic phishing defense

Disable Macros to prevent macro attachments

© 2018 F5 Networks

Over 210k critical vulnerabilities

But vulnerabilities with published exploits have 1 in 3 chance of getting used by attackers



Predictive Vulnerability Scoring System

Michael Roytman | Chief Data Scientist, Kenna Security
Jay Jacobs | Chief Data Scientist, Cyentia Institute
Location: South Seas CDF
Date: Thursday, August 8 | 12:10pm-1:00pm
Format: 50-Minute Briefings
Tracks: Enterprise, Network Defense

Effective prioritization of vulnerabilities is essential to staying ahead of your attackers. While your threat intelligence might expose a wealth of information about attackers and attack paths, integrating it into decision-making is no easy task. Too often, we make the mistake of taking the data given to us for granted – and this has disastrous consequences.

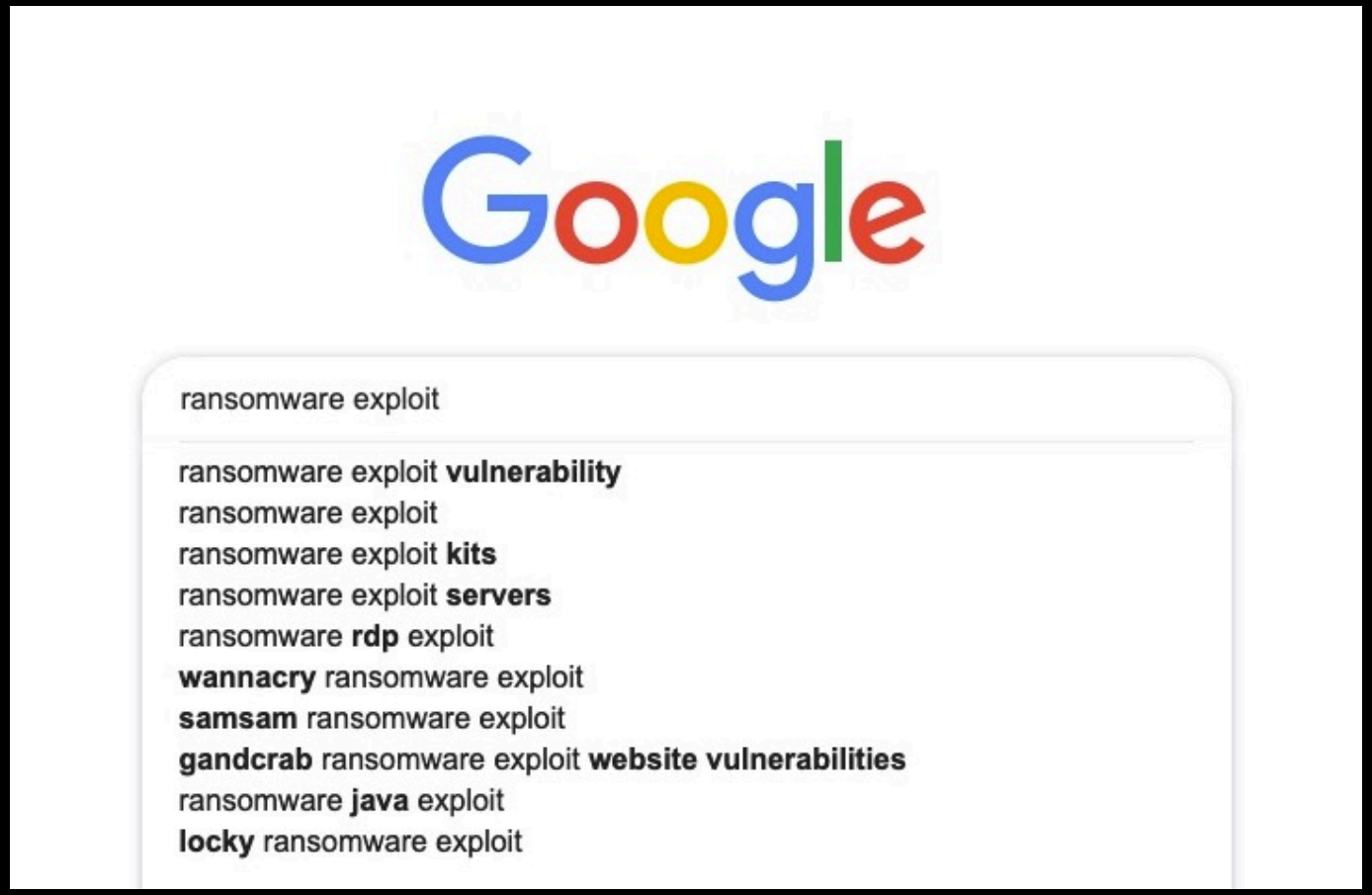
We'll explain what we miss by trusting CVSS scores, and what should absolutely be taken into consideration to focus on the vulnerabilities posing the greatest risks to our organizations. We'll look at tens of thousands of vulnerabilities, CVSS scores, CVE, NVD, scraping mailing lists, collecting data feeds and ultimately end up with a few dozen data points that helped us understand the probability of a vulnerability being exploited.

Finally, we'll use all that data as well as billions of in-the-wild events collected over 5 years in order to create a machine learning model for predicting the probability of a vulnerability being exploited, a scoring system which outperforms CVSS on every metric: accuracy, efficiency and coverage.

https://www.cyentia.com/research/

© 2018 F5 Networks

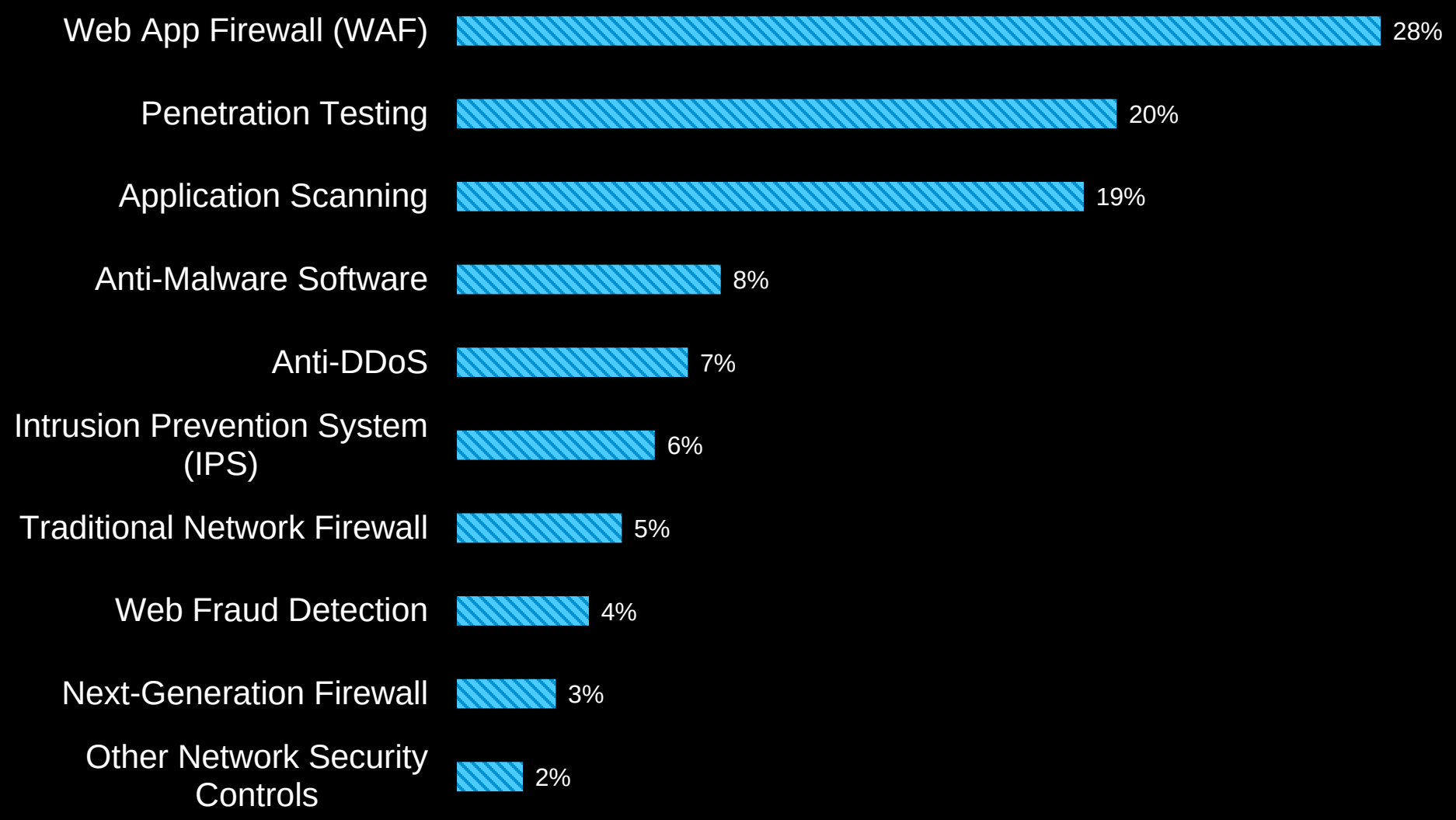
Patching



Prioritize your patching to what attackers are using

© 2018 F5 Networks

Select Flexible and Integrated Defense Tools



Defenses in Use, F5 2018 App Protect Report Survey

© 2018 F5 Networks

Training Reduces Phishing Success!

33%

Phishing success **without** training.

13%

Phishing success **with** training.

Application Protection Research Series

We focus on applications because your adversaries focus on applications.

Applications have become the focal point of the Internet, the workhorses behind organizations of all types. Attackers have figured this out, and they target applications more than anything else (besides people). This research series ties together trends and data from a number of perspectives to give an overall picture of the application security threat landscape.

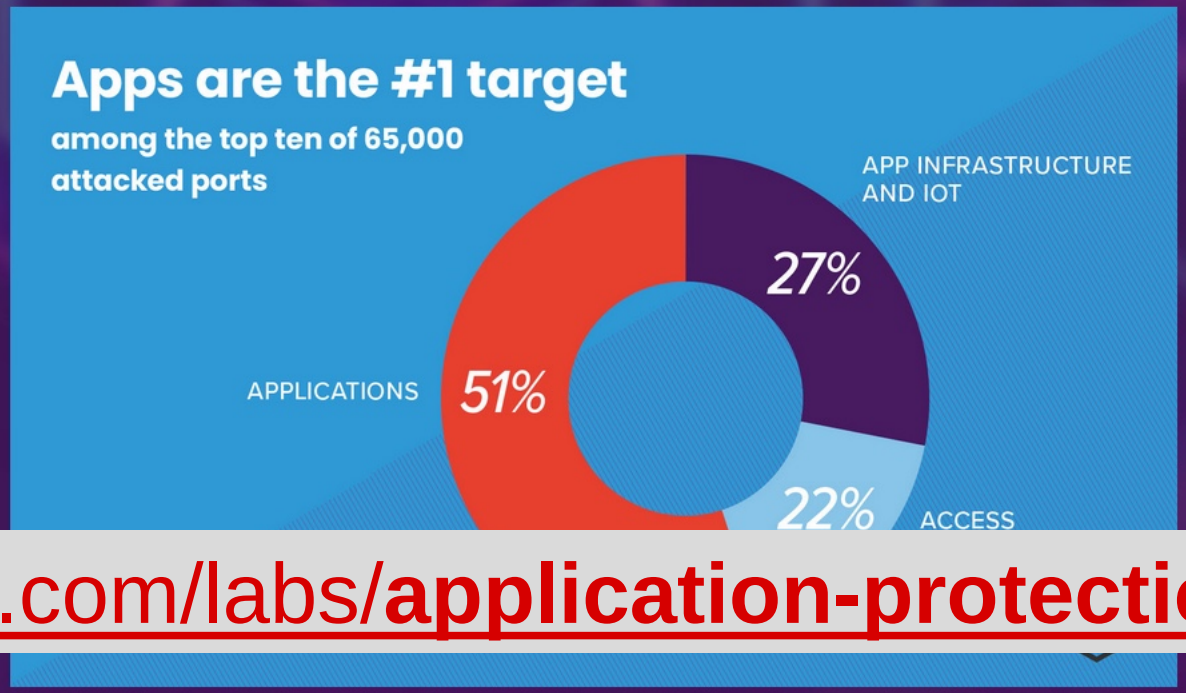
July 22, 2019

INTRO EPISODE

2019 Application Protection Series

Why Application Security?

Find out why we care so much about application security, how applications have grown into the weird beasts that they are today, and how our work fits into the bigger picture of securing and running an application.



https://www.f5.com/labs/**application-protection**

F5Labs.com

Stay Up to Date by Following Us!

Tell us what you want to read about – or write for us!

Twitter

LinkedIn

Email Updates (1 / week)

RSS

© 2016 F5 Networks