RAPID7

A Field Guide to Measuring Internet Exposure

With Industry Examples from the Fortune 500

Bob Rudis

SecureWorld Boston • March 28, 2019

About Me

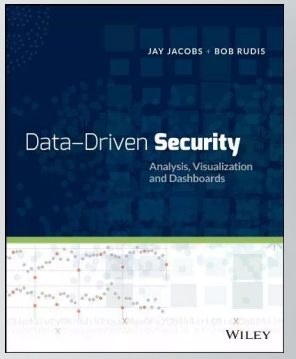
i.e. some reasons why my point of view might be interesting/useful

@hrbrmstr
research@rapid7.com
bob@rud.is
http://rud.is/

30+ Years in Cybersecurity
(20+ in Fortune 50 global organizations)

Former team lead for the **Verizon Data Breach Investigations Report**

Co-author of one of the 1st books on “doing data science” in Cybersecurity
(**Data-Driven Security**)

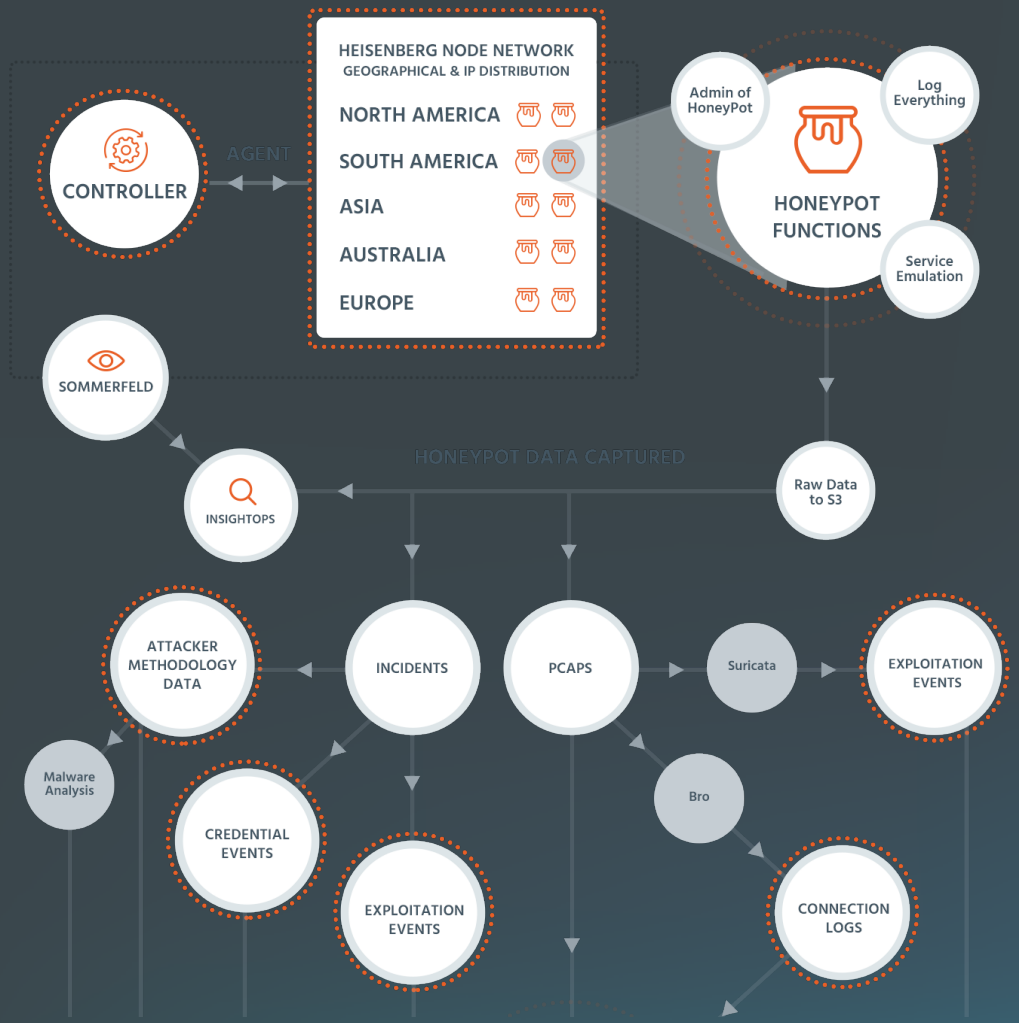


Over a petabyte of planetary-scale internet telemetry data analyzed daily

90+ R packages with a focus on cybersecurity/internet telemetry

Planetary Scale Research Platforms

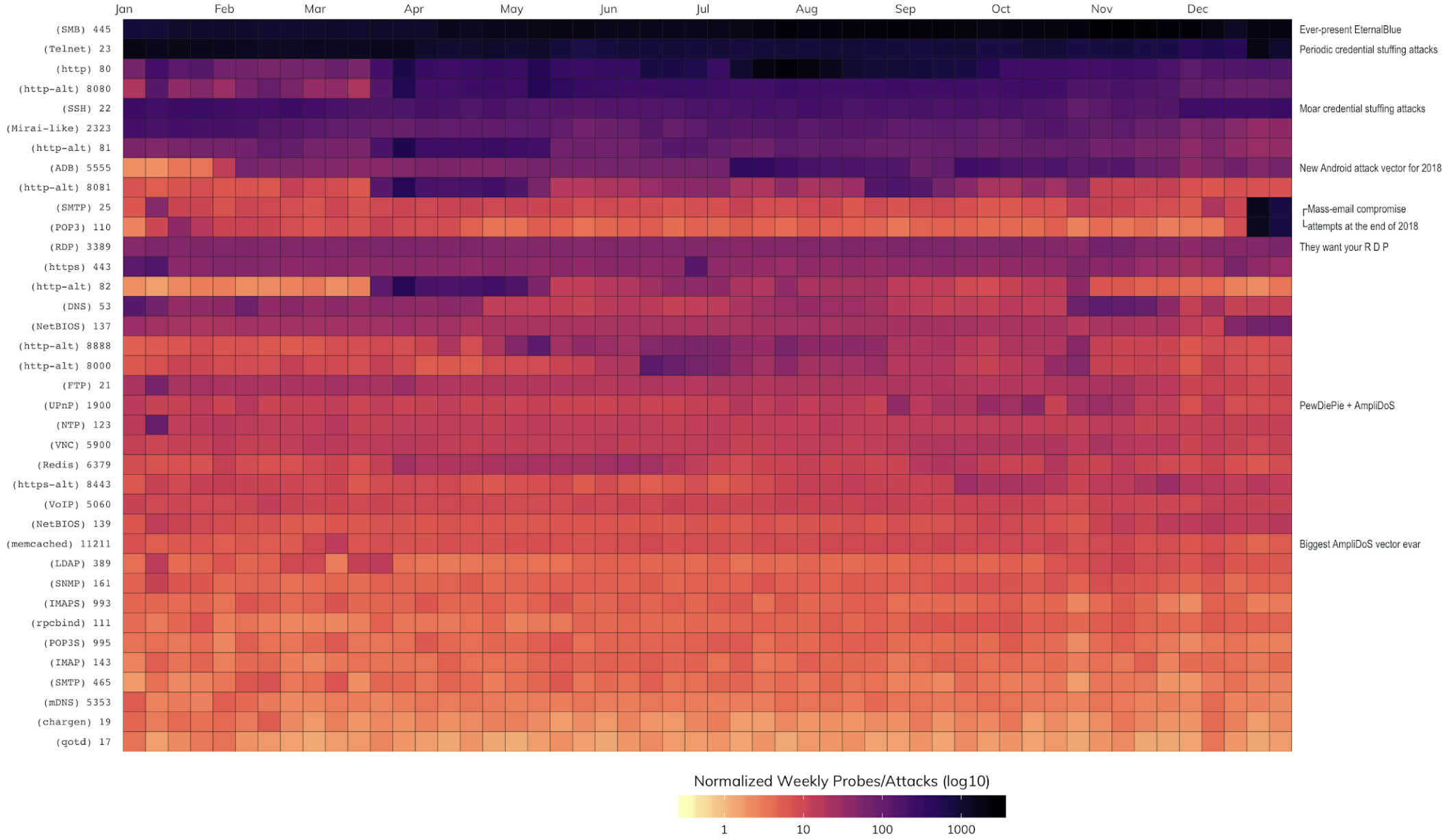
Planetary Scale Research Platforms : Heisenberg



- Passive internet telemetry collector made up of a centrally managed, globally distributed network of over 240 low-to-medium interaction honeypots.
- Tracks attacker campaigns, techniques and captures all interactions and payloads.
- Sits at the core of Rapid7's machine learning-based Early Warning System which tracks changes to behavior on all ports and protocols.
- Provides essential data to regional CERTs to help address critical/systemic configuration exposure.

2018 Attack Map

Each square is filled by according to the number of normalized (per-sensor) unique probes/attacks. Port/protocol ordered by highest activity to lowest.



2018 Attack Map

Each square is filled by according to the number of normalized (per-sensor) unique probes/attacks. Port/protocol ordered by highest activity to lowest.

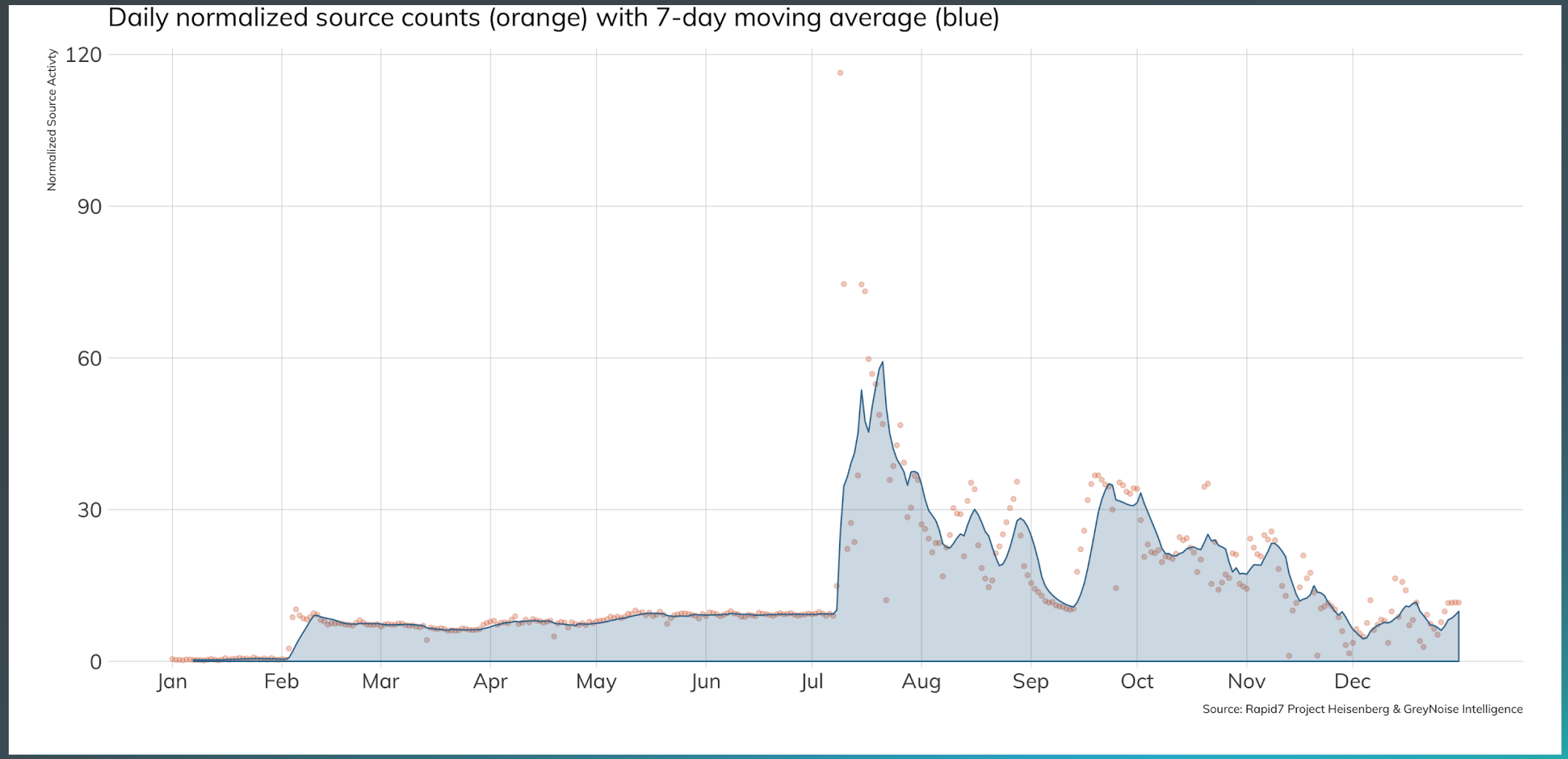
Each row tells a different story, often more than one.

We've selected a few & you can read

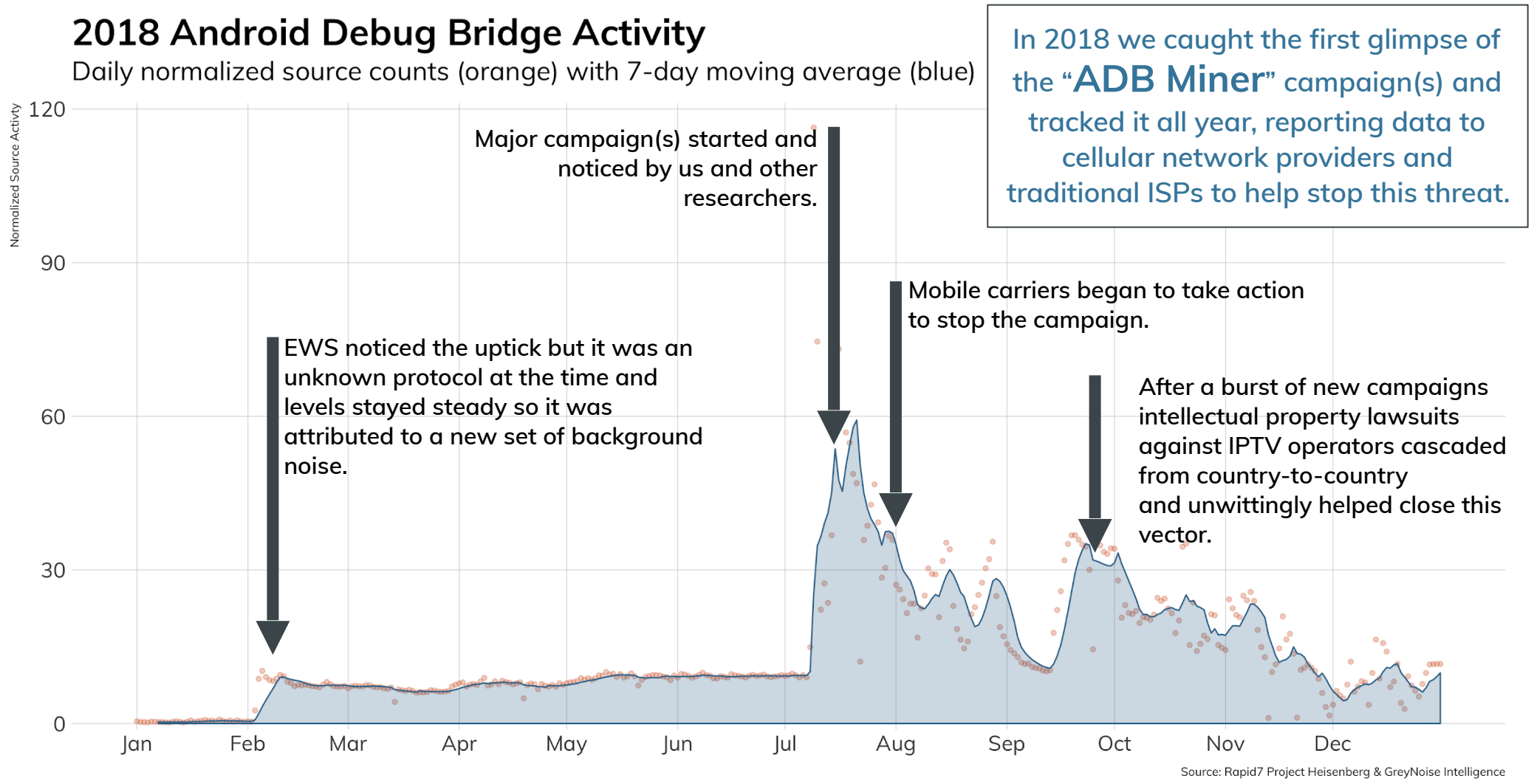
Rapid7's 2018 Q4 Threat Report

to explore a high-resolution version of this heatmap & corresponding time series charts that provide a full picture of opportunistic attacker activity for 2018.

Planetary Scale Research Platforms : Heisenberg

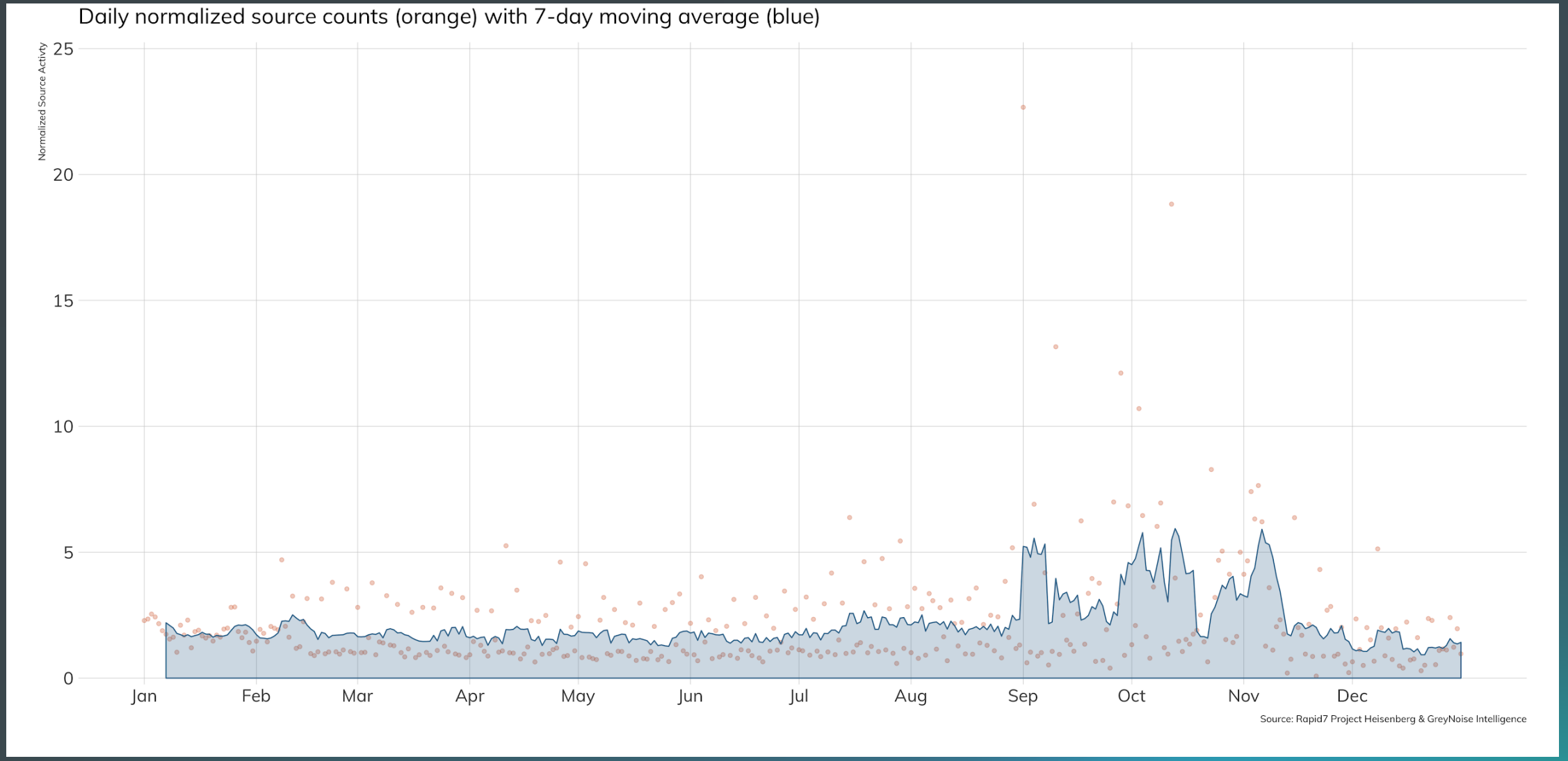


Planetary Scale Research Platforms : Heisenberg

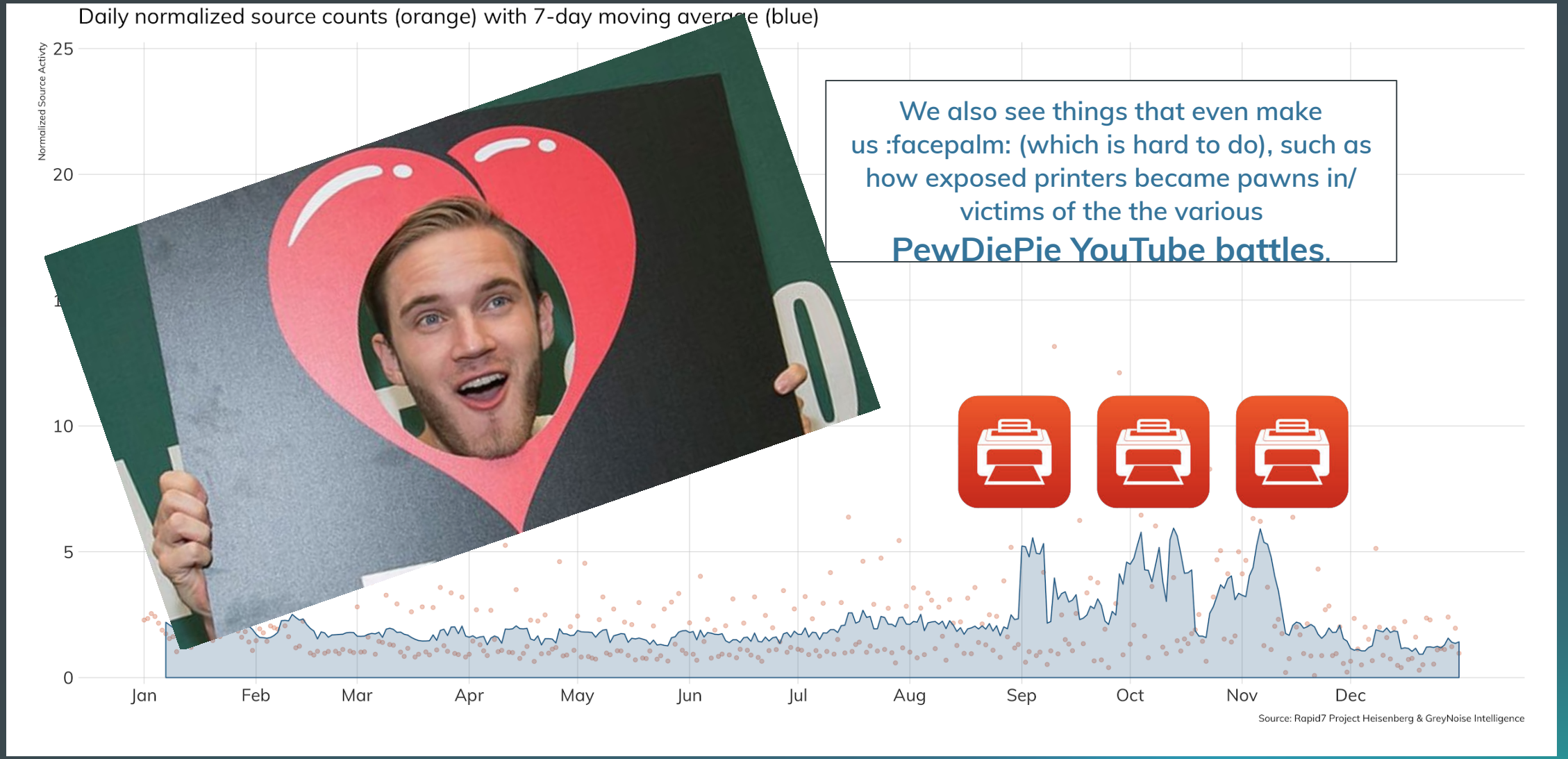


In 2018 we caught the first glimpse of the "**ADB Miner**" campaign(s) and tracked it all year, reporting data to cellular network providers and traditional ISPs to help stop this threat.

Planetary Scale Research Platforms : Heisenberg



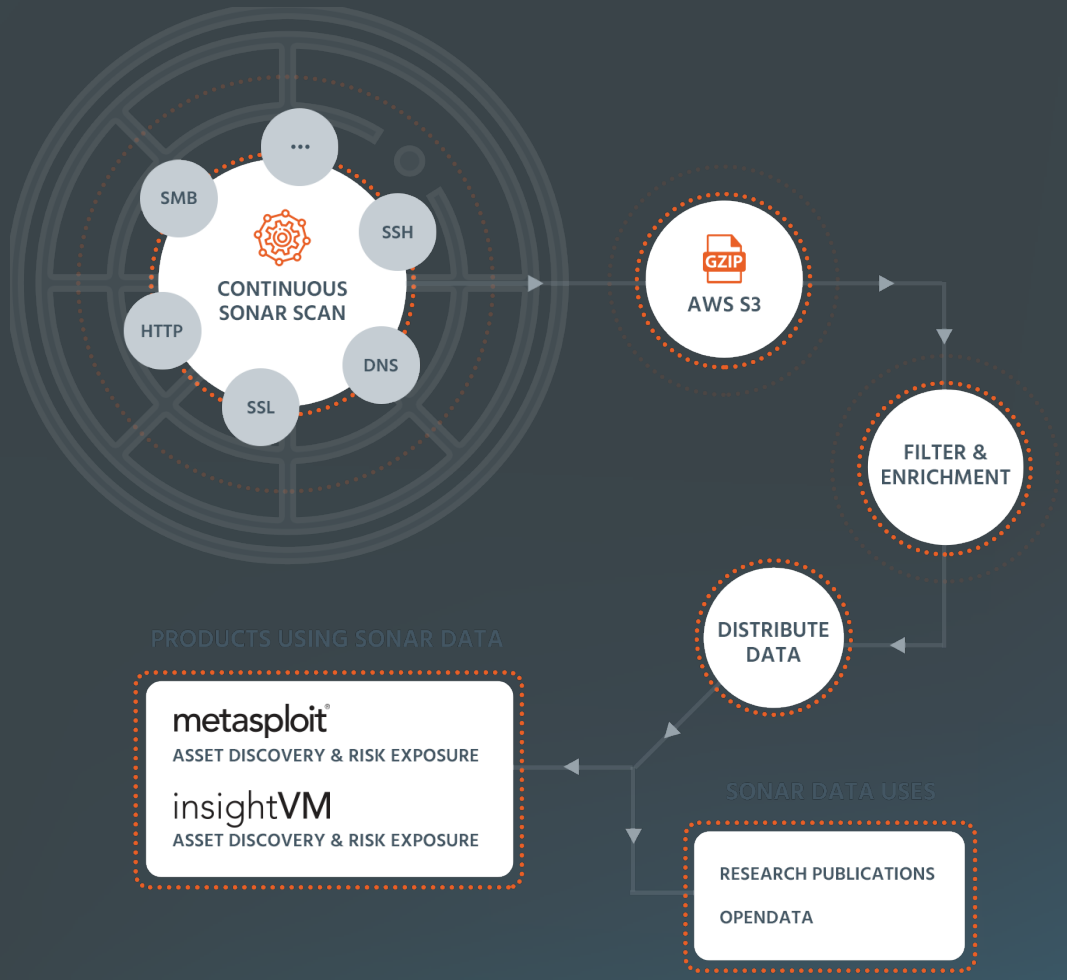
Planetary Scale Research Platforms : Heisenberg



We also see things that even make us :facepalm: (which is hard to do), such as how exposed printers became pawns in/ victims of the the various **PewDiePie YouTube battles**.

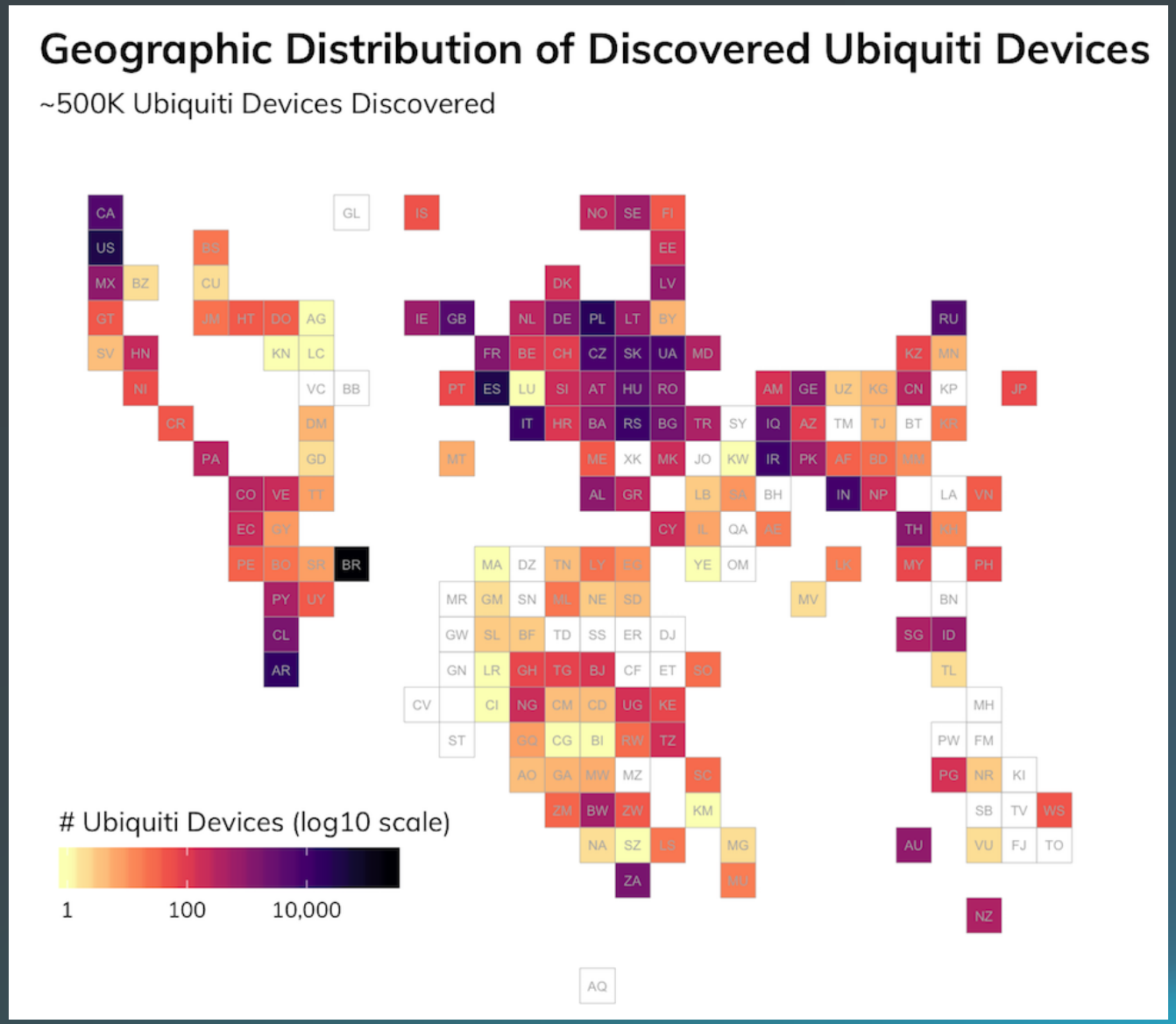
RAPID7

Planetary Scale Research Platforms : Sonar



- Active internet telemetry collector — scanning, certificates, DNS lookups.
- Over 200 monthly scans across over 50 ports/ protocols. Everything from HTTP captures to custom-crafted MQTT, ADB, CoAP, Ubiquiti Discovery & other scans.
- Over 60 billion DNS lookups every two weeks with dedicated prefix scans (e.g. _dmarc, _mta-sts) and 2 years of historical data available for Rapid7 IR & Research teams.
- Available for free to organizations and qualified researchers via opendata.rapid7.com

Planetary Scale Research Platforms : Sonar



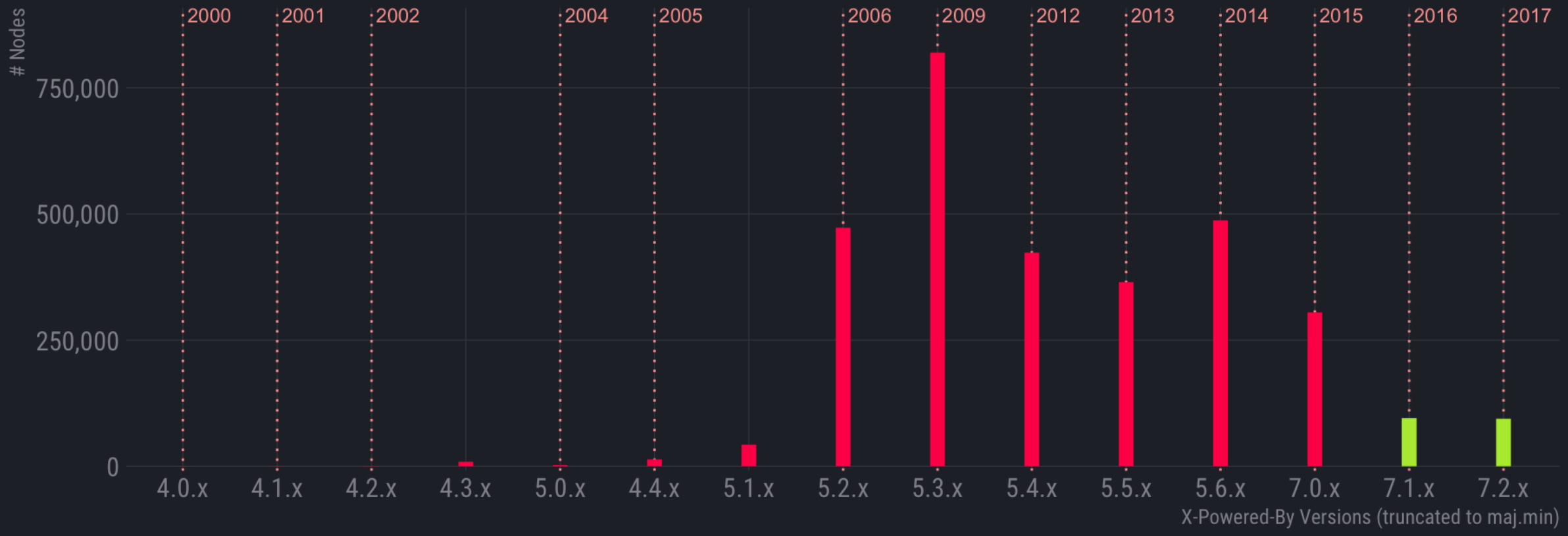
Our custom study for exposed devices responding to Ubiquiti Discovery — which pick up even one-off custom firmware version strings — probes helped eradicate 90% of exposed nodes in Brazil due to our partnership with CERT.br

All of these nodes are being used in active ~3.5x amplification DDoS campaigns.

RAPID7

~2.9 Million 'Powered By' PHP Web Sites Have No Official Support After Jan 1 2019

X Axis Ordered By First maj.min Version Release Date; Markers show release year of maj.min.x;
Chart only includes valid PHP version strings from 4.x to 7.x

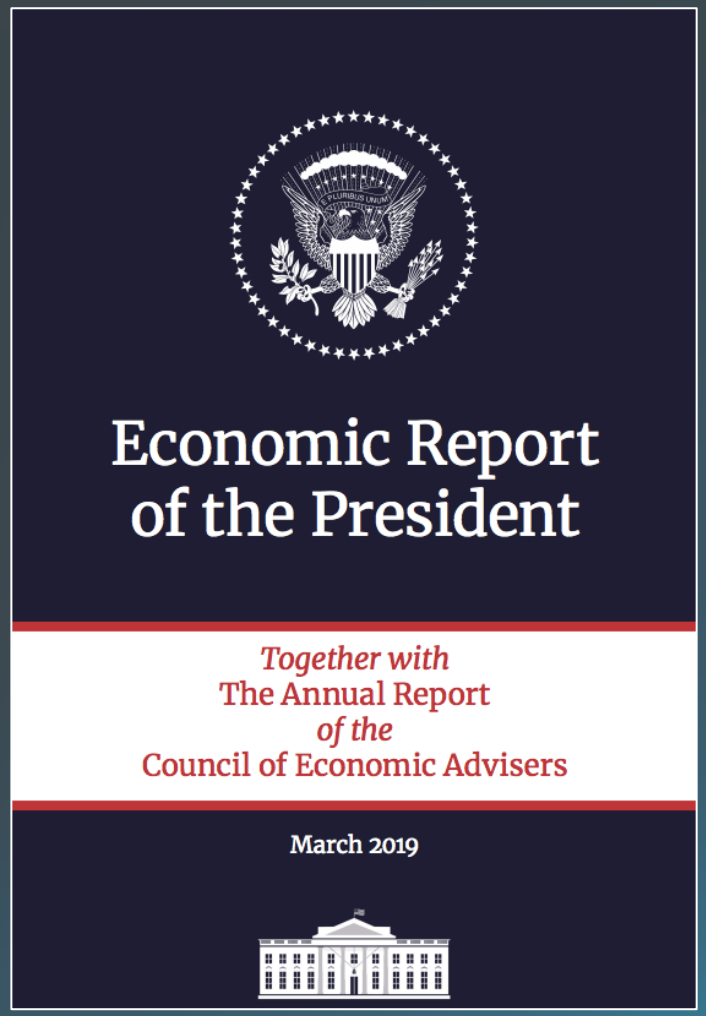


We use recog (github.com/rapid7/recog) at-scale to identify tech stacks.
Nearly 3 million PHP users are going to face serious attacks in 2019.

RAPID7

Putting Research Into Action

https://r-7.co/2U6EHkw



https://www.whitehouse.gov/wp-content/uploads/2019/03/ERP-2019.pdf

Find us on pages 365:368 in "*Potential Vulnerabilities by Industry*"

The Tremendous Trump: Retromastered Edition

Written by

Brian Denham

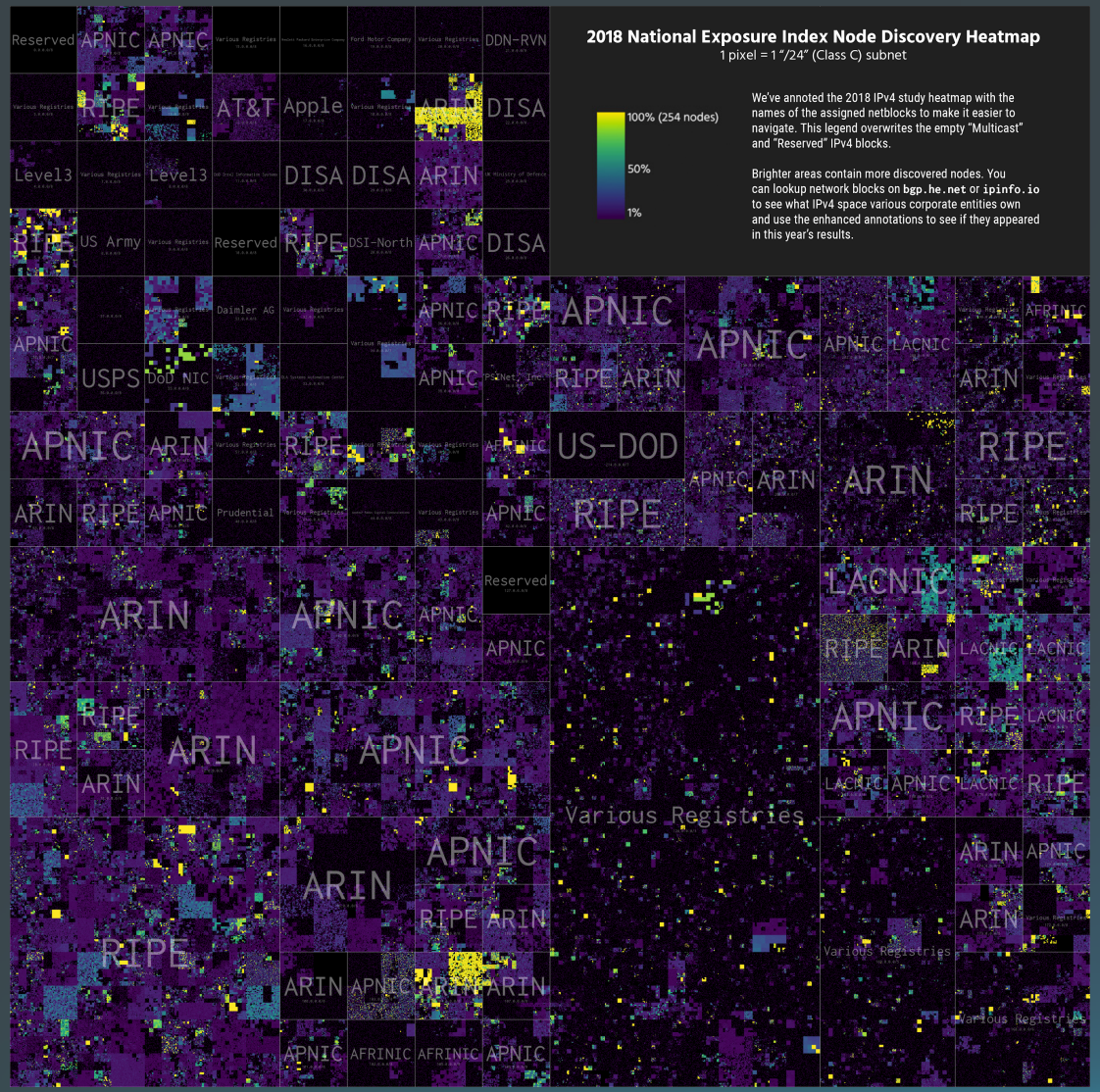
Alfred Perez

Art by

Brian Denham

Ben Dunn

Fortune 500 ICE → What We Measured



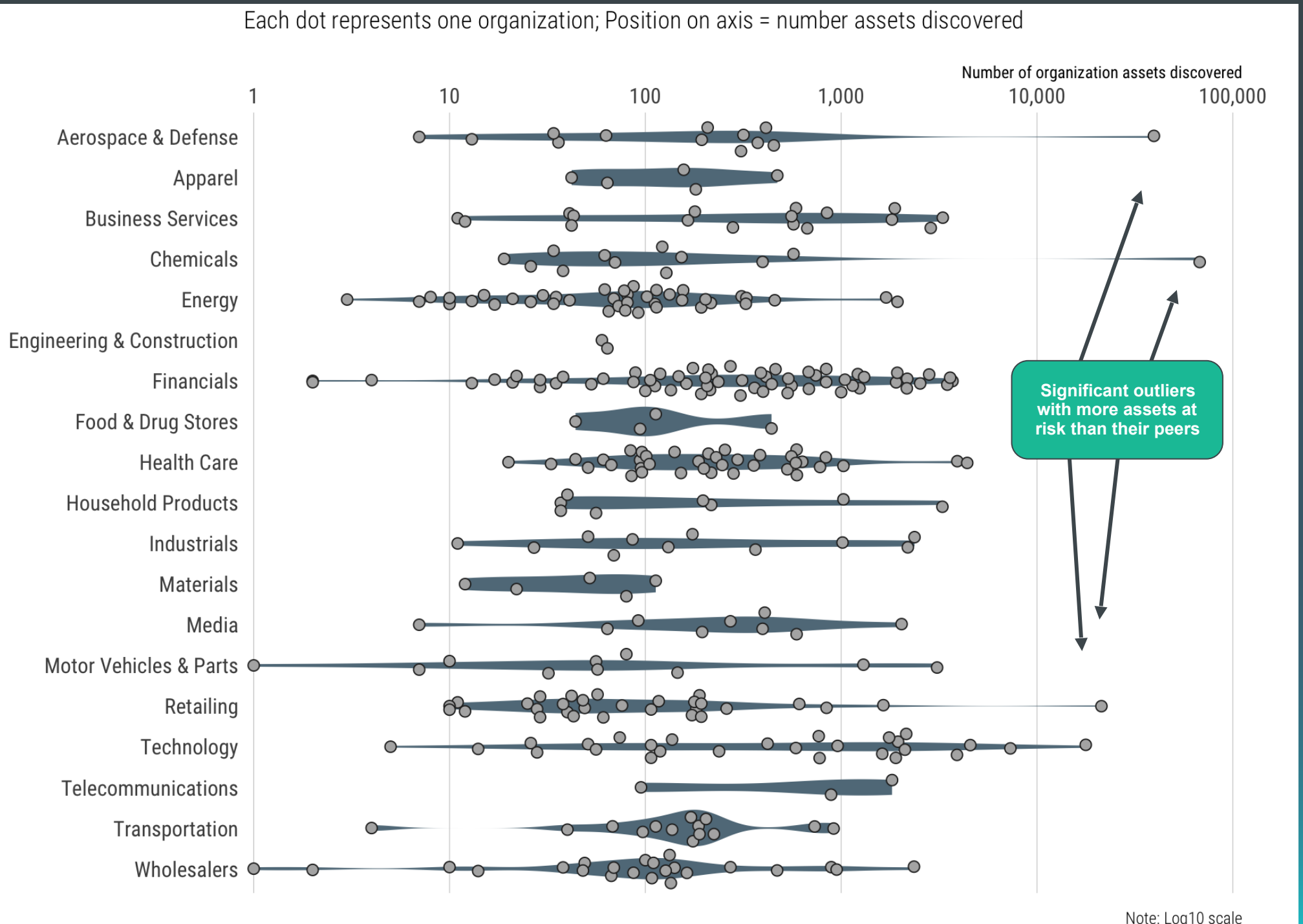
- **Overall attack surface**

Fortune 500 ICE → Overall Attack Surface

How many

servers / **routers** / **devices**

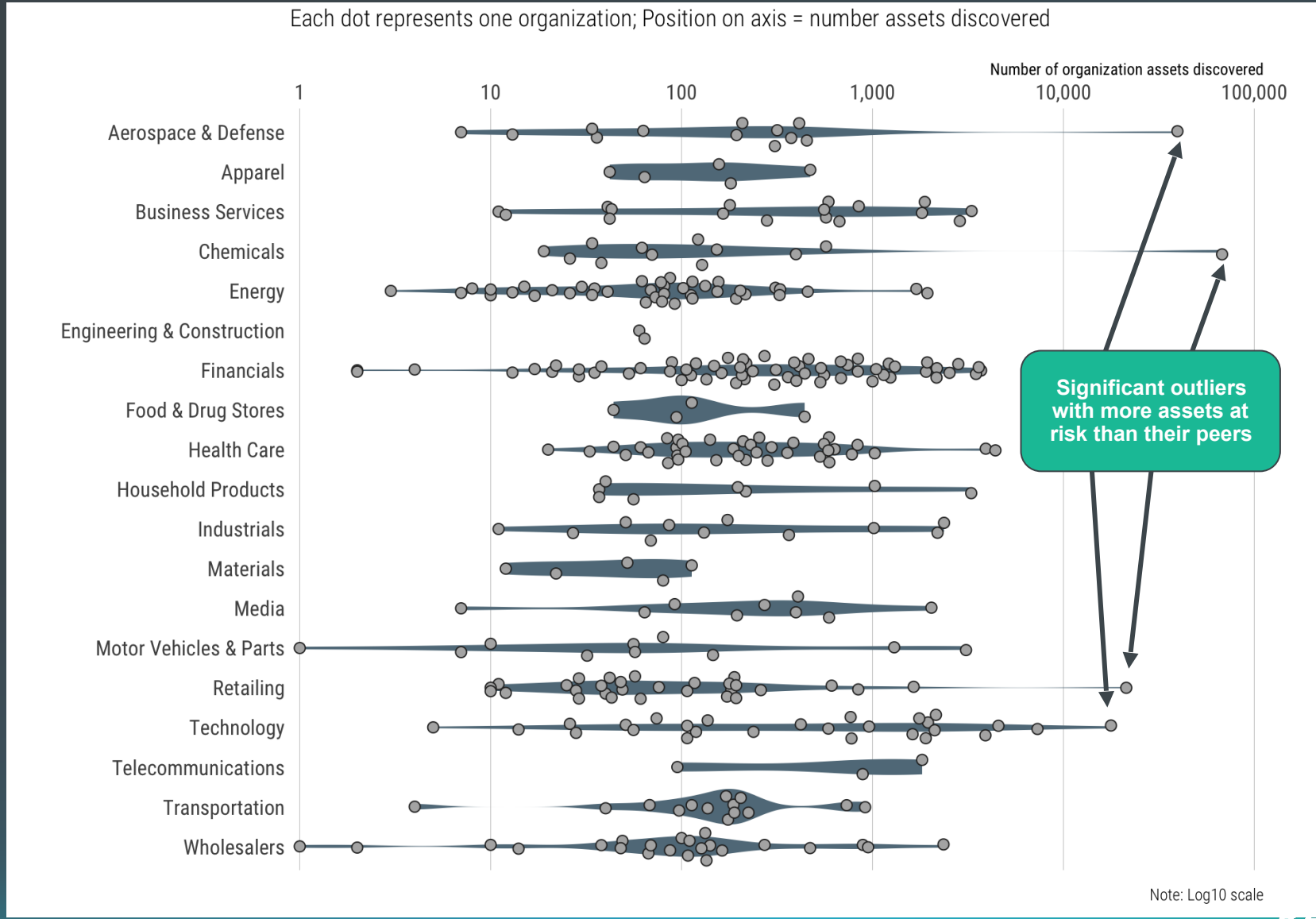
do Fortune 500 organizations have on the public internet?


Each dot represents one organization; Position on axis = number assets discovered
Number of organization assets discovered
1
10
100
1,000
10,000
100,000
Aerospace & Defense
Apparel
Business Services
Chemicals
Energy
Engineering & Construction
Financials
Food & Drug Stores
Health Care
Household Products
Industrials
Materials
Media
Motor Vehicles & Parts
Retailing
Technology
Telecommunications
Transportation
Wholesalers
Significant outliers with more assets at risk than their peers
Note: Log10 scale

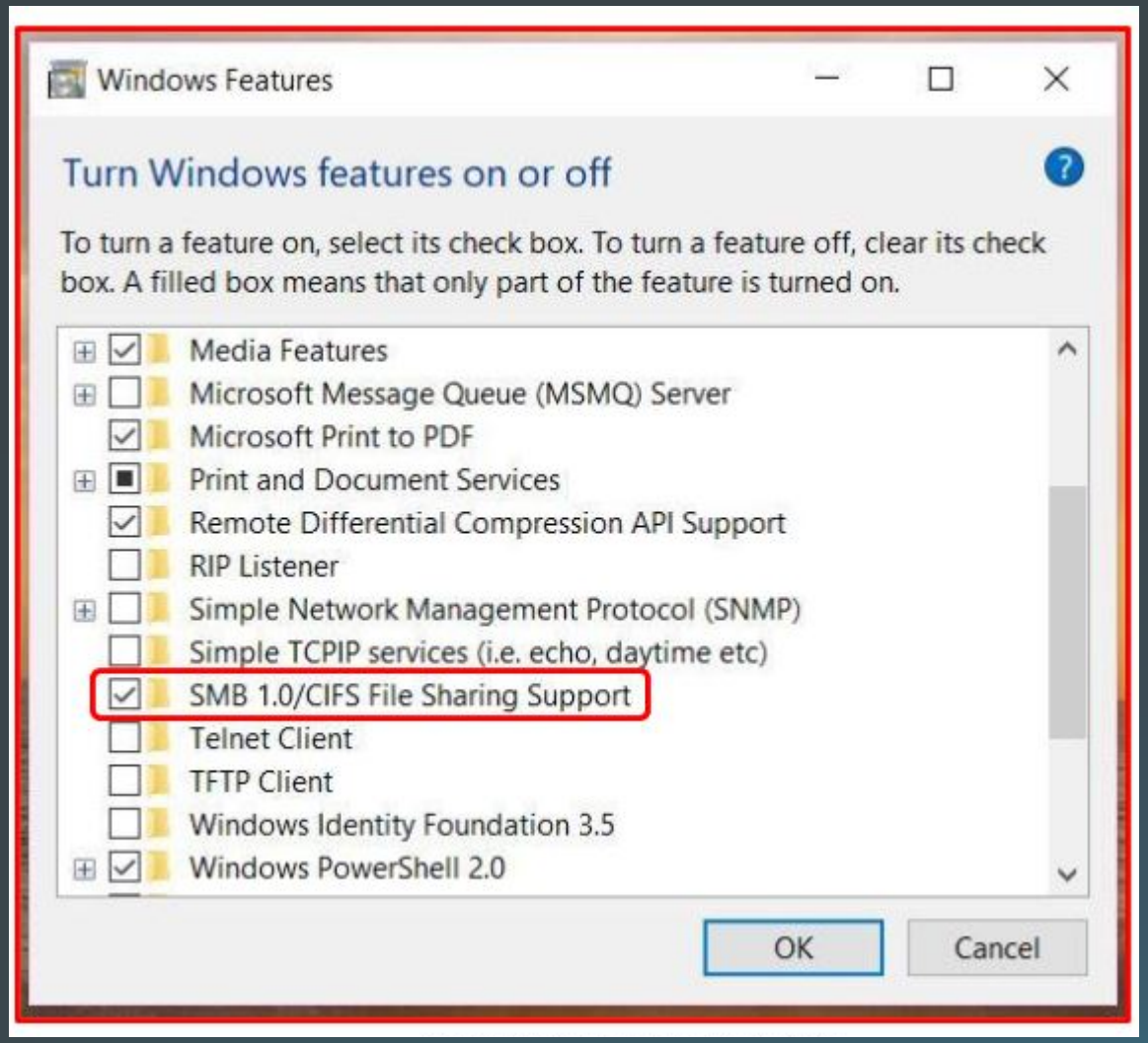
Fortune 500 ICE → Overall Attack Surface

Core takeaway:

Counts vary dramatically in & across industries but **the "average" F500 organization presents 500 services that attackers can probe & attack at-will.**



Fortune 500 ICE → What We Measured



- Overall attack surface
- **Presence of dangerous/ insecure services**

Fortune 500 ICE → Dangerous/Insecure Services

Weaknesses in Windows File Sharing protocol (**SMB**) spawned the WannaCry and NotPetya outbreaks in 2017/2018.

This protocol/service presents a clear and present danger to any organization that exposes it to the public internet.

STATEMENTS & RELEASES

Statement from the Press Secretary

FOREIGN POLICY | Issued on: February 15, 2018

★ ★ ★

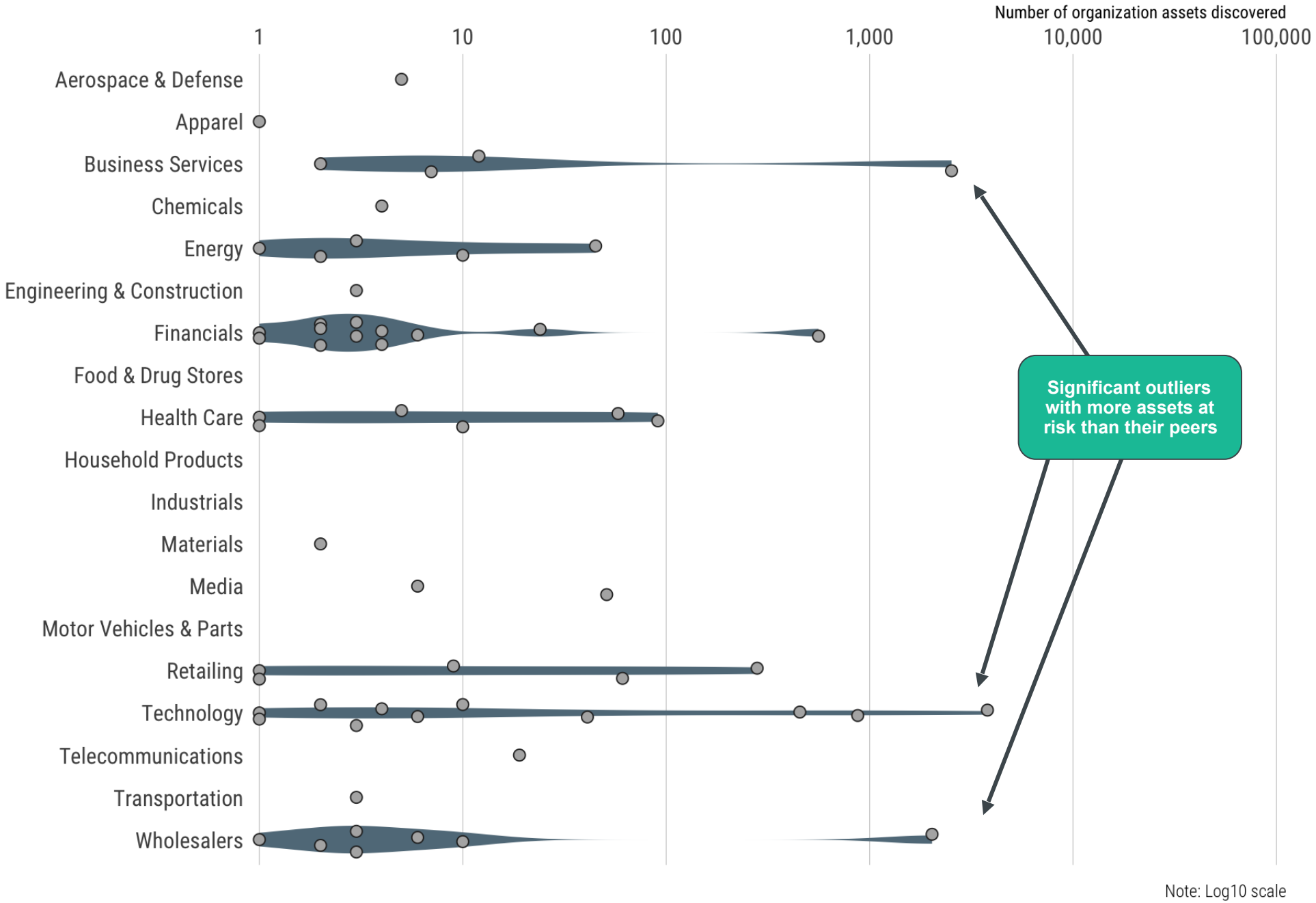
In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.

The attack, dubbed “NotPetya,” quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin’s ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia’s involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.

The White House

★ ★ ★

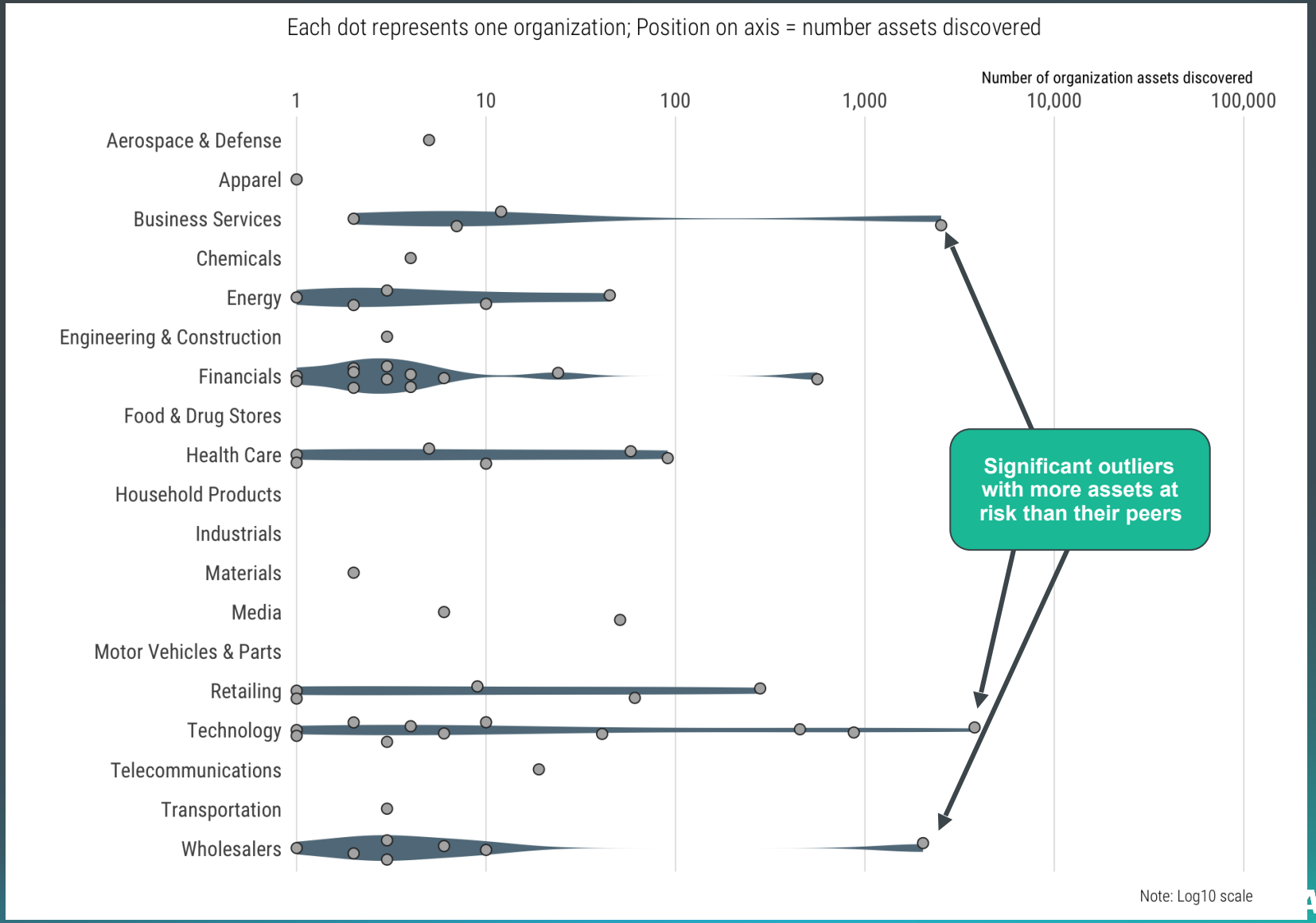
Each dot represents one organization; Position on axis = number assets discovered



Fortune 500 ICE → Dangerous/Insecure Services

Core takeaway:

Despite the dangers of exposing SMB to the public internet **15 out of 21 industry sectors have members** exposing at least one SMB server with an average of 10 SMB servers being exposed especially in Financial Services and Wholsesalers.

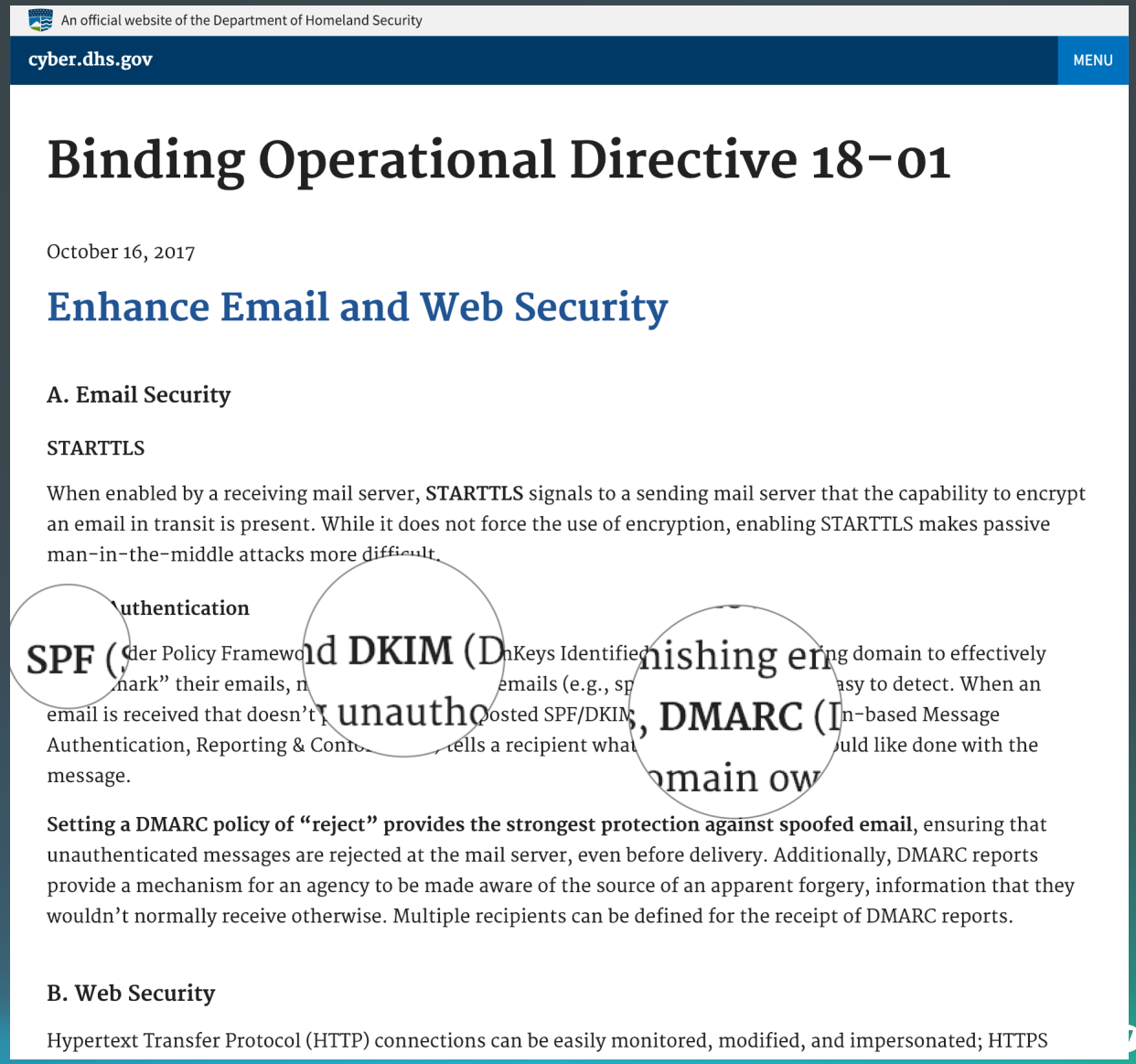


Fortune 500 ICE → What We Measured

- Overall attack surface
- Presence of dangerous/ insecure services
- **Phishing defense posture**

Fortune 500 ICE → Phishing Defense Posture

In 2017 DHS recognized the importance of a strong phishing defense based on modern email authentication configuration standards.



An official website of the Department of Homeland Security

cyber.dhs.gov MENU

Binding Operational Directive 18-01

October 16, 2017

Enhance Email and Web Security

A. Email Security

STARTTLS

When enabled by a receiving mail server, **STARTTLS** signals to a sending mail server that the capability to encrypt an email in transit is present. While it does not force the use of encryption, enabling STARTTLS makes passive man-in-the-middle attacks more difficult.

uthentication

SPF (

d DKIM (D

nishing em

unautho

, DMARC (I

omain ow

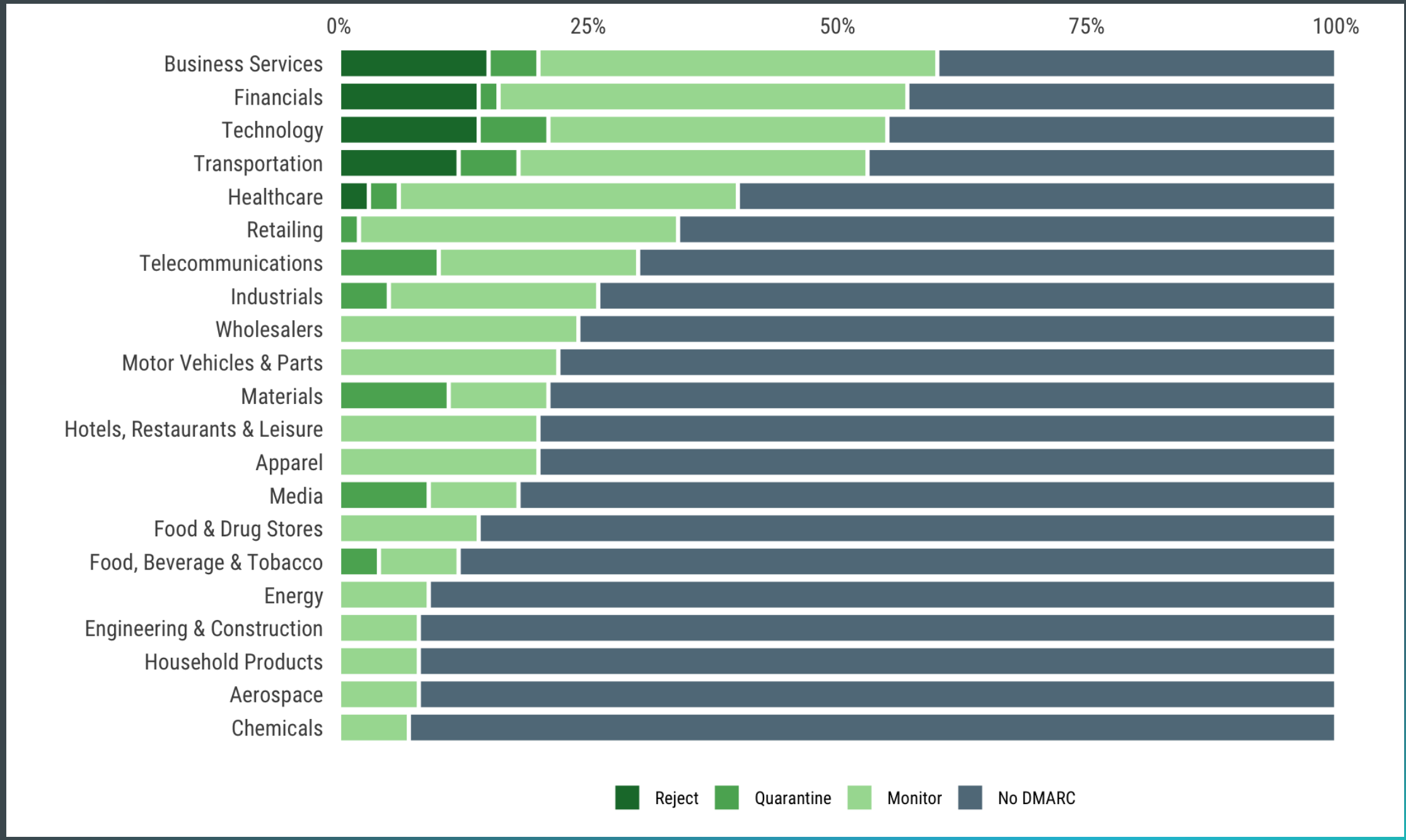
der Policy Framewo nKeys Identified ng domain to effectively hark" their emails, n emails (e.g., sp asy to detect. When an email is received that doesn't p osted SPF/DKIM n-based Message Authentication, Reporting & Conf ells a recipient what uld like done with the message.

Setting a DMARC policy of "reject" provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an agency to be made aware of the source of an apparent forgery, information that they wouldn't normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.

B. Web Security

Hypertext Transfer Protocol (HTTP) connections can be easily monitored, modified, and impersonated; HTTPS

(2017) Fortune 500 DMARC Implementation Status (August, 2018)



RAPID7

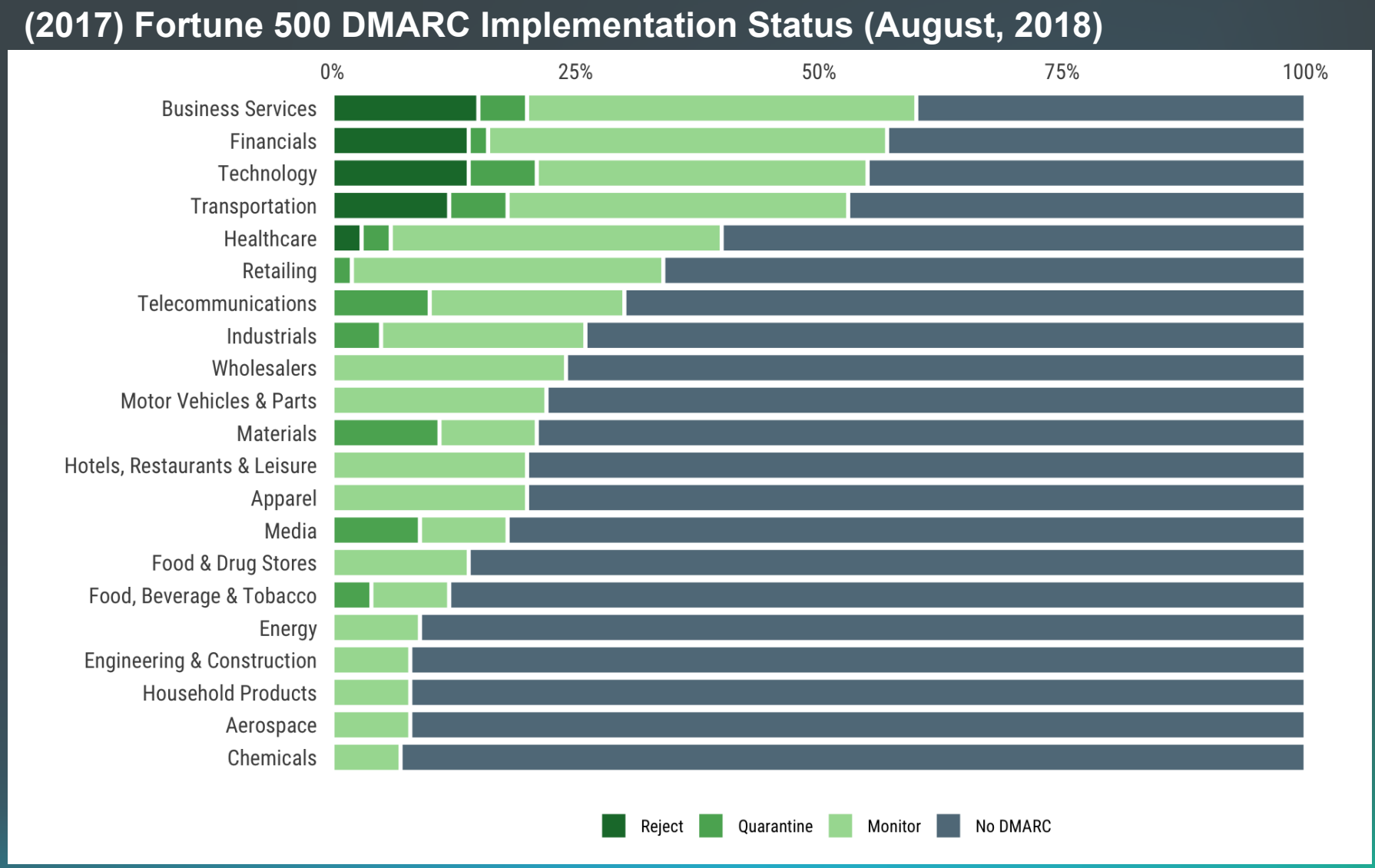
Fortune 500 ICE → Phishing Defense Posture

Core takeaway:

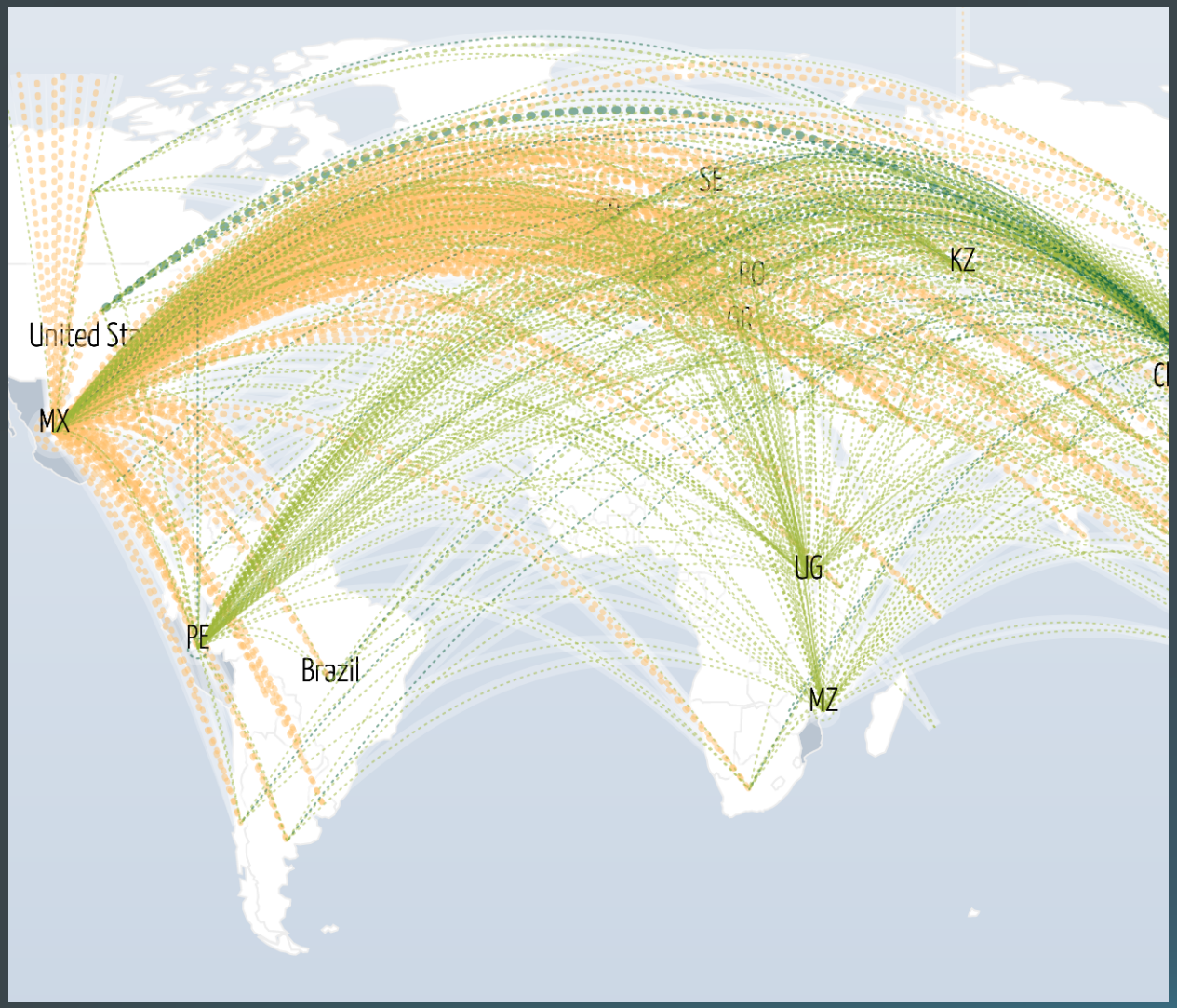
Phishing is the #1 way attackers gain a foothold in organizations;

DMARC in “reject” or “quarantine” mode is one of the most effective ways of reducing phishing attacks and spam.

DMARC usage in the F500 is seriously lacking.



Fortune 500 ICE → What We Measured

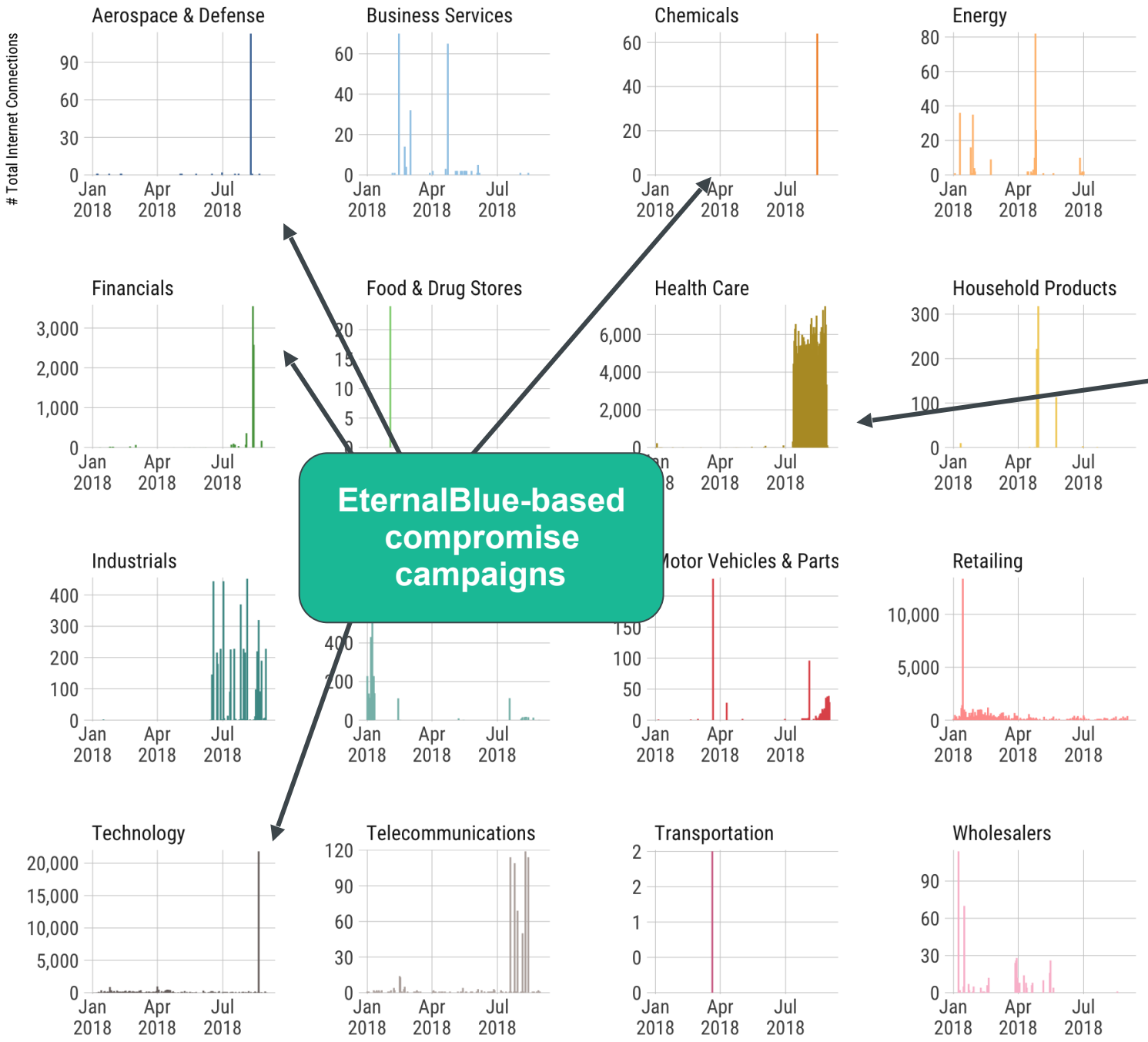


- Overall attack surface
- Presence of dangerous/ insecure services
- Phishing defense posture
- **Evidence of System Compromise**

Fortune 500 ICE → Evidence of System Compromise

"Information Security Continuous Monitoring" (ISCM) has been a fundamental component of DHS proactive defense strategies for nearly a decade now.

A core component of CDM is knowing what's happening on and from your network.


Total Internet Connections
Aerospace & Defense
Business Services
Chemicals
Energy
Financials
Food & Drug Stores
Health Care
Household Products
Industrials
Motor Vehicles & Parts
Retailing
Technology
Telecommunications
Transportation
Wholesalers
Jan 2018
Apr 2018
Jul 2018
EternalBlue-based compromise campaigns
One healthcare organization with multiple systems participating in DNS amplification attacks.

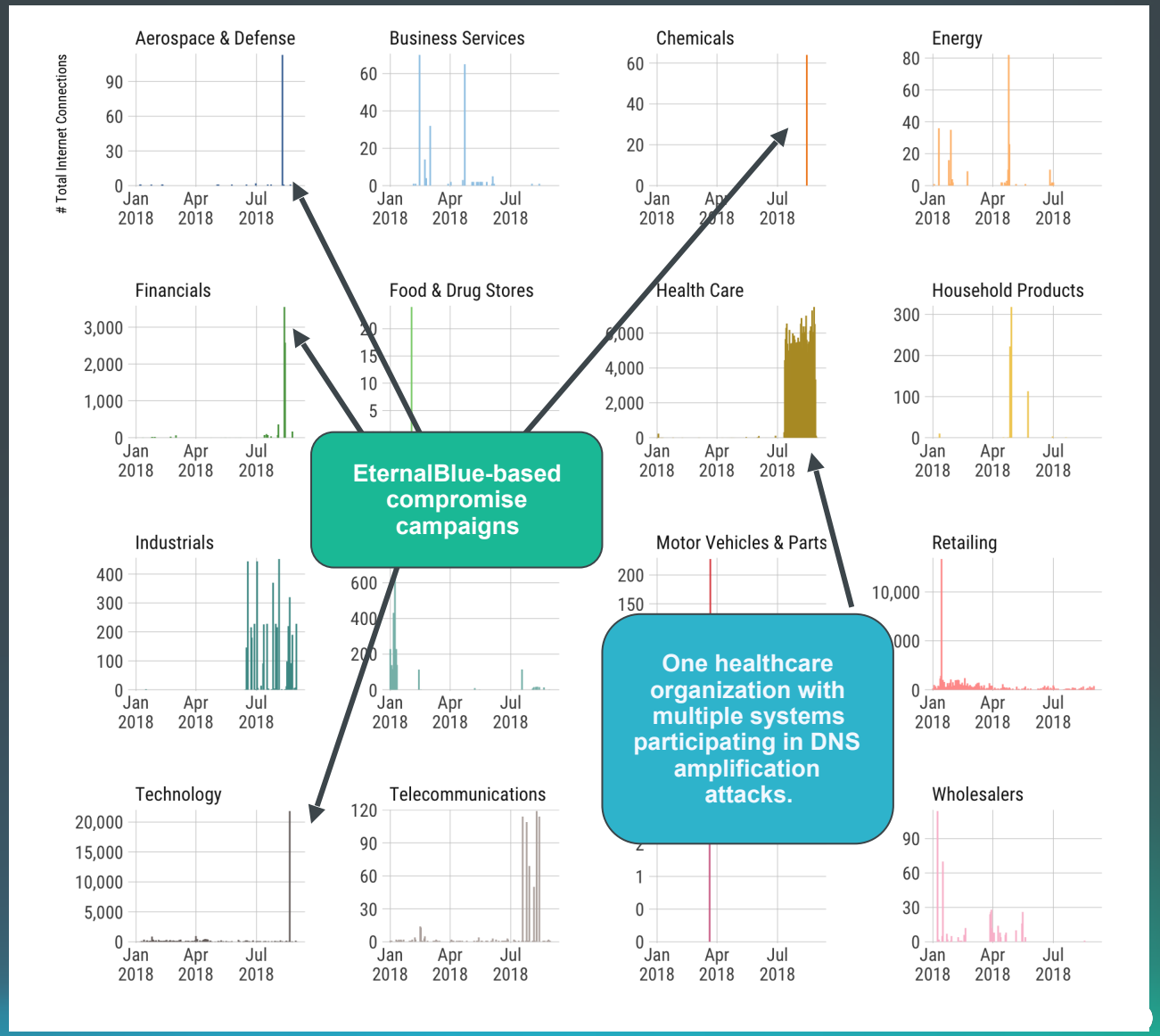
Fortune 500 ICE → Evidence of System Compromise

Core takeaway:

<u>This chart should be blank.</u>

Every F500 sector had at least one member with one or more compromises or serious service misconfigurations since January 2018.

Rapid7 tracked instances of EternalBlue-based compromise attempts coming from F500 networks as well as **F500 members unknowingly participating in amplification Denial of Service attacks**.



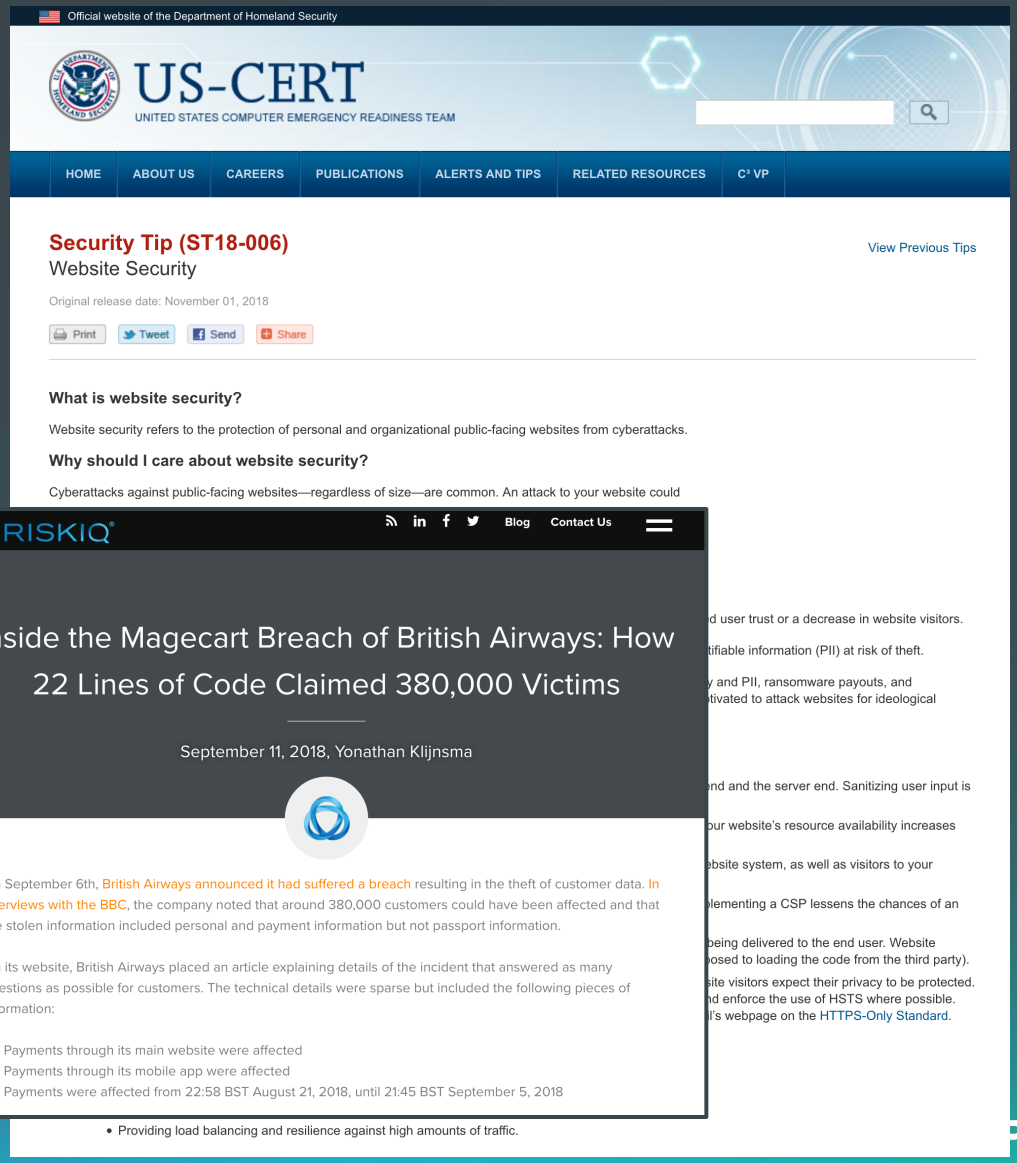
Fortune 500 ICE → What We Measured

- Overall attack surface
- Presence of dangerous/insecure services
- Phishing defense posture
- Evidence of System Compromise
- **Weak public-facing configurations & third-party risks**

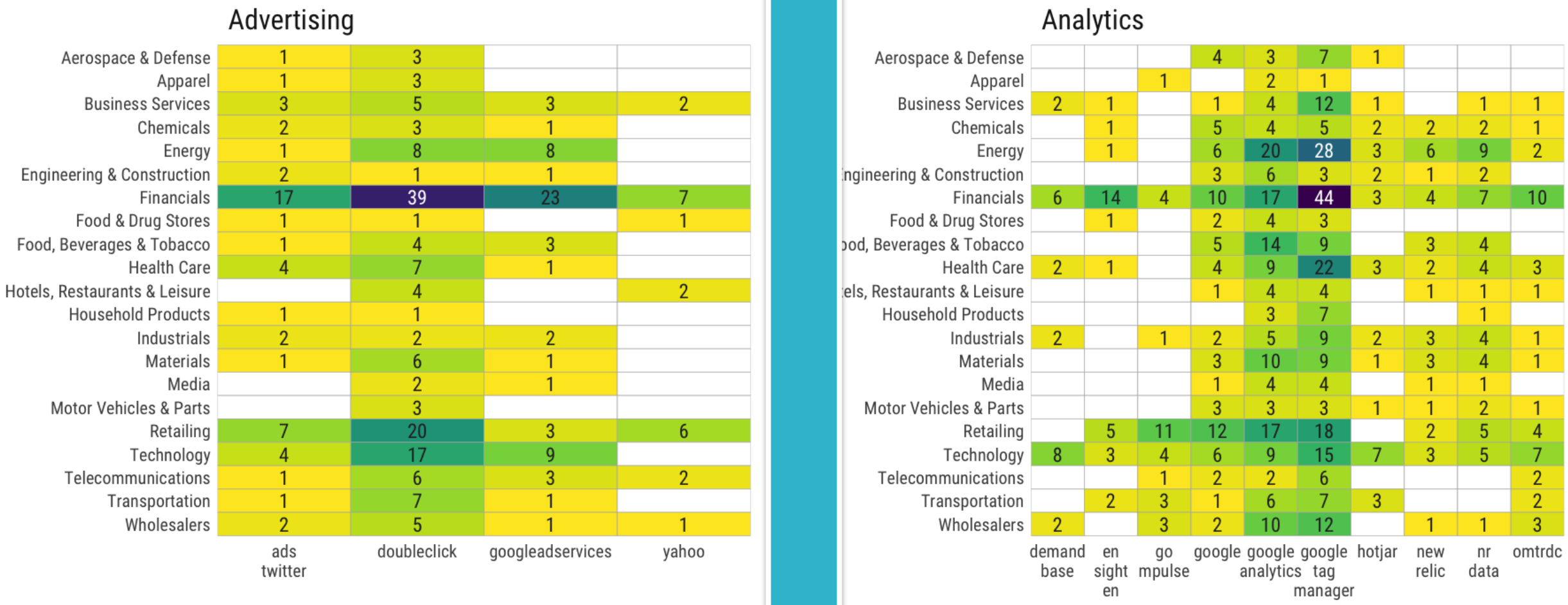
Fortune 500 ICE → Weak Configs/Third-party Risk

US-CERT has provided updated guidance on foundational best practices for web site security.

Magecart attacker groups have been leveraging weak configurations in organization dependencies on third-party resources to steal PII and payment card data.



SHARED RISK


Advertising
Aerospace & Defense 1 3
Apparel 1 3
Business Services 3 5 3 2
Chemicals 2 3 1
Energy 1 8 8
Engineering & Construction 2 1 1
Financials 17 39 23 7
Food & Drug Stores 1 1 1
Food, Beverages & Tobacco 1 4 3
Health Care 4 7 1
Hotels, Restaurants & Leisure 4 2
Household Products 1 1
Industrials 2 2 2
Materials 1 6 1
Media 2 1
Motor Vehicles & Parts 3
Retailing 7 20 3 6
Technology 4 17 9
Telecommunications 1 6 3 2
Transportation 1 7 1
Wholesalers 2 5 1 1
ads
twitter
doubleclick
googleadservices
yahoo
Analytics
Aerospace & Defense 4 3 7 1
Apparel 1 2 1
Business Services 2 1 1 4 12 1 1 1
Chemicals 1 5 4 5 2 2 2 1
Energy 1 6 20 28 3 6 9 2
ngineering & Construction 3 6 3 2 1 2
Financials 6 14 4 10 17 44 3 4 7 10
Food & Drug Stores 1 2 4 3
ood, Beverages & Tobacco 5 14 9 3 4
Health Care 2 1 4 9 22 3 2 4 3
els, Restaurants & Leisure 1 4 4 1 1 1
Household Products 3 7 1
Industrials 2 1 2 5 9 2 3 4 1
Materials 3 10 9 1 3 4 1
Media 1 4 4 1 1
Motor Vehicles & Parts 3 3 3 1 1 2 1
Retailing 5 11 12 17 18 2 5 4
Technology 8 3 4 6 9 15 7 3 5 7
Telecommunications 1 2 2 6 2
Transportation 2 3 1 6 7 3 2
Wholesalers 2 3 2 10 12 1 1 3
demand
base
en
sight
en
go
mpulse
google
google
analytics
google
tag
manager
hotjar
new
relic
nr
data
omtrdc

SHARED RISK

Content Delivery Network

	adobedtm	en25	jquery	tiqcdn	typekit	youtube	ytimg
Aerospace & Defense	1		1			5	
Apparel	1		1	1			
Business Services	4	1		3	2	6	2
Chemicals	1	1	1		1	5	2
Energy	2	3	4	1	3	2	
Engineering & Construction	2	1	2	1	2		
Financials	15	10	1	9	5	7	4
Food & Drug Stores			2		1		
Food, Beverages & Tobacco	2		2	3	2	3	3
Health Care	10	2	2	1	5	12	6
Hotels, Restaurants & Leisure	4				3		
Household Products	2		3		1	2	
Industrials	2	3	1	2		3	
Materials	1	1	2		4	3	
Media			1		3	2	2
Motor Vehicles & Parts	1		2			2	
Retailing	4		4	6	3	3	2
Technology	14	7	2	7	1	5	2
Telecommunications	4			2		2	2
Transportation	3	1		4			
Wholesalers	5	1	1	1	3	2	1

Social

	facebook	linkedin	twitter
Aerospace & Defense	5	6	4
Apparel	3		1
Business Services	8	8	4
Chemicals	3	2	2
Energy	14	5	2
ngineering & Construction	3	2	3
Financials	45	27	26
Food & Drug Stores	3	1	3
od, Beverages & Tobacco	6	3	3
Health Care	12	4	9
els, Restaurants & Leisure	1		1
Household Products	3	2	2
Industrials	4	5	2
Materials	8	4	1
Media	2		
Motor Vehicles & Parts	4	1	
Retailing	25		10
Technology	14	12	7
Telecommunications	6		1
Transportation	8	4	1
Wholesalers	5	4	5

Fortune 500 ICE → Evidence of System Compromise

Core takeaway:

Every sector & almost every F500 organization **relies on and uses untrusted third-party JavaScript code** for their primary domain & often uses those same resources for their partner/customer web apps.

The chart also shows a **massive interdependency across sectors** and organizations, meaning an attacker can compromise a single third-party resource and compromise nearly all of the Fortune 500 websites.

Summary of Key Findings

- Exposed attack surface averages 500 servers/devices per organization, up to more than 2,500 for many.
- On average, a min. of 5–10 known exploitable systems deployed and exposed.
- Two thirds of Fortune 500 organizations have weak or nonexistent anti-phishing defenses.

Summary of Key Findings

- Across all industries, exposure of DNS metadata and cloud service provider info.
- Indicators of malware compromises observed in all sectors.
  - Technology, Retailing, and Telecommunications sectors showing daily signs of ongoing compromise.
  - Compromises range from company resources being co-opted into amplification denial-of-service attacks to signs of EternalBlue-based campaigns similar to WannaCry and NotPetya.

Recommendations

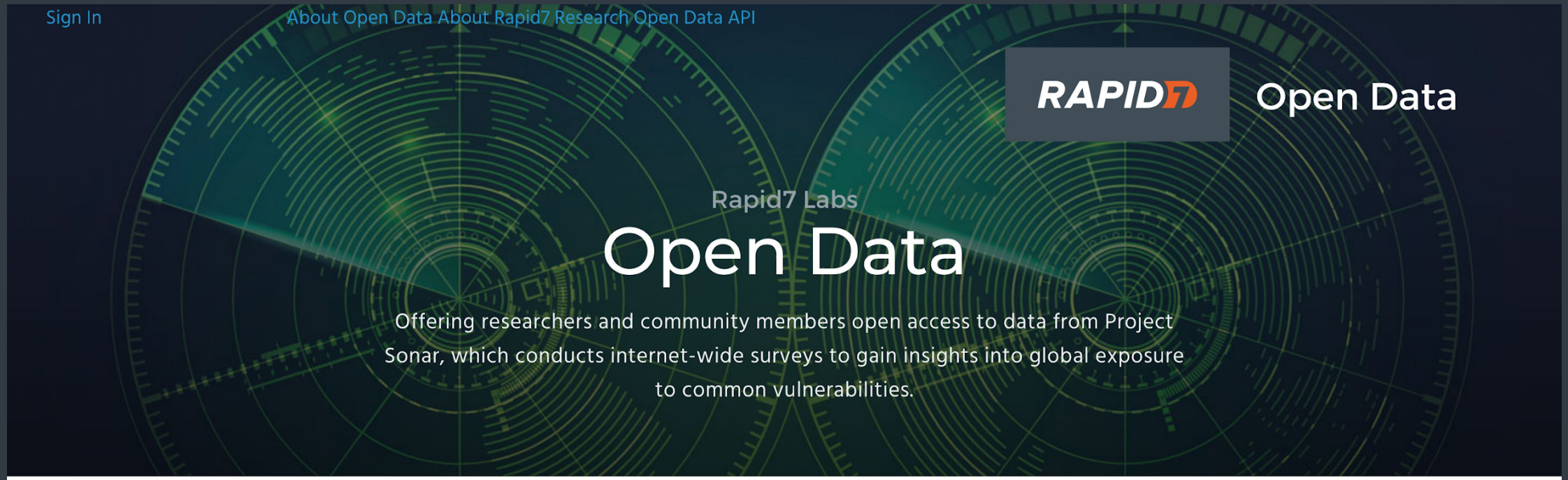
Fortune 500 ICE: Recommendations

- Organizations should adopt U.S. Federal standards & guidance for:
  - **Domain Name System (DNS)** configuration and maintenance
  - **Email safety & security** configurations
  - **Web site security and safety** configurations
  - **Continuous monitoring**

Fortune 500 ICE: Recommendations

- Organizations should also remove all internet-connected Windows File Sharing (SMB) servers and use more secure configurations for other, non-web services

Your Turn



All Datasets

DATASETS: 13 FILES: 7,284

Forward DNS (FDNS)

DNS 'ANY', 'A', 'AAAA', 'TXT', 'MX', and 'CNAME' responses for known forward DNS names

Reverse DNS (RDNS)

DNS IPv4 PTR responses

HTTP GET Responses

Responses to HTTP/1.1 GET requests against various HTTP ports

HTTPS GET Responses

Responses to HTTP/1.1 GET requests against various HTTPS ports

opendata.rapid7.com

RAPID7

Rapid7 FDNS ANY Dataset

computer security | cyber security | analytics | internet

Description

Subset of FDNS ANY queries against domain names produced by Rapid7 Project Sonar, made available in s3. More information on the schema can be found at Rapid7's Open Data website.

Update Frequency

Monthly

License

Non-commercial (NC) - Free for non-commercial purposes. For commercial use, contact research@rapid7.com. Full terms: https://opendata.rapid7.com/about/#terms

Documentation

https://opendata.rapid7.com/

Contact

research@rapid7.com

Usage Examples

- Creating a Project Sonar FDNS API with AWS by Evan Perotti at SecurityRiskAdvisors
- How to Conduct DNS Reconnaissance for $.02 Using Rapid7 Open Data and AWS by Shan Sikdar at Rapid7

Resources on AWS

Description
FDNS ANY Gzip-compressed parquet files following a HIVE partitioning model, with a 90-day retention period. This dataset represents the data returned for a name when an ANY query is issued. Data is partitioned by date=YYYYMM which is the year-month that the FDNS ANY study was launched.

Resource type
S3 Bucket

Amazon Resource Name (ARN)
`arn:aws:s3:::rapid7-opendata/fdns/any/v1/`

AWS Region
`us-east-1`

Description
New FDNS parquet dataset announcements

Resource type
SNS Topic

Amazon Resource Name (ARN)
`arn:aws:sns:us-east-1:740874647437:s3-event-notification-new-aws-pds-dataset`

AWS Region
`us-east-1`

Thank you!

For more on Rapid7 research, please visit:

https://www.rapid7.com/research/

Bob Rudis • Chief Data Scientist

research@rapid7.com

RAPID7