Industry Cyber Exposure Report: Fortune 500 & Quarterly Threat Report EMEA

Key Findings & Recommendations

Rapid7

Cyber Exposure for Fortune 500

Determining how many internet-connected technologies are publicly deployed by the Fortune 500, and examining their:

- Total attack surface
- Exposure to known common attack vectors
- Exposure/susceptibility to phishing attacks
- Evidence of infection of malware

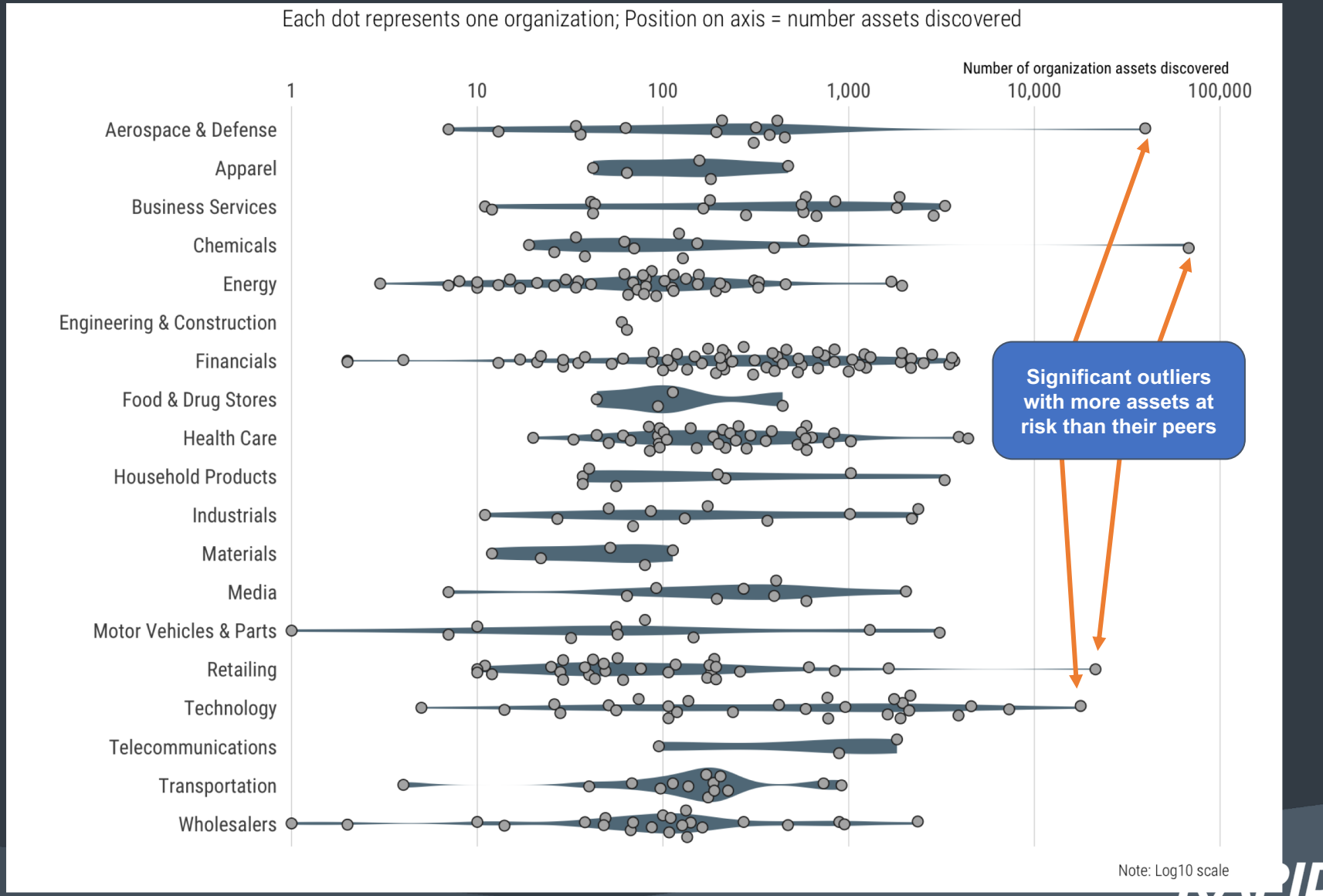
RAPID7

Key Findings

Fortune 500 ICE → Overall Attack Surface

Core takeaway:

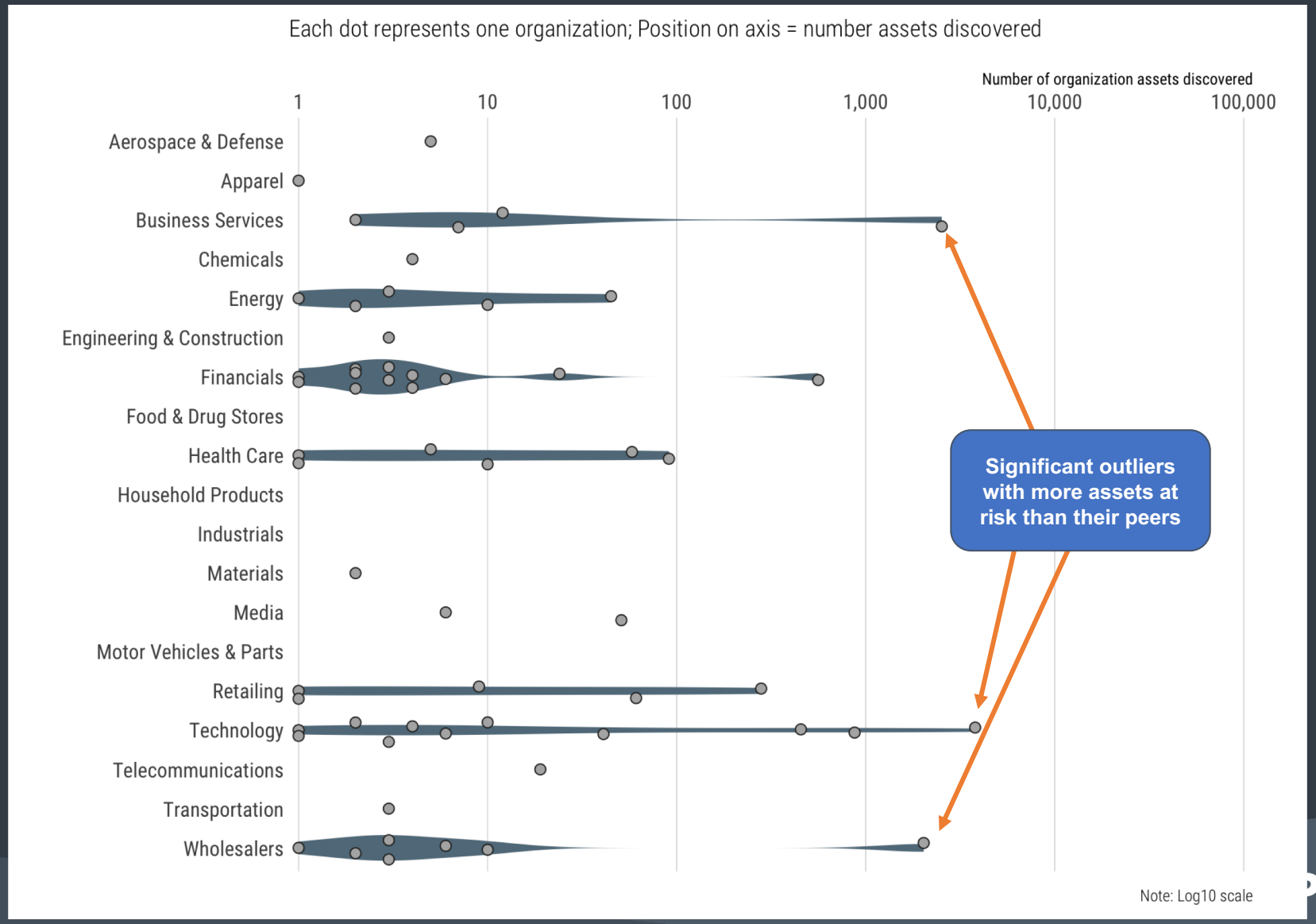
Counts vary dramatically in & across industries but the "average" F500 organization presents 500 services that attackers can probe & attack at-will.



Fortune 500 ICE → 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 Wholesalers.



Fortune 500 ICE → Phishing Defense Posture

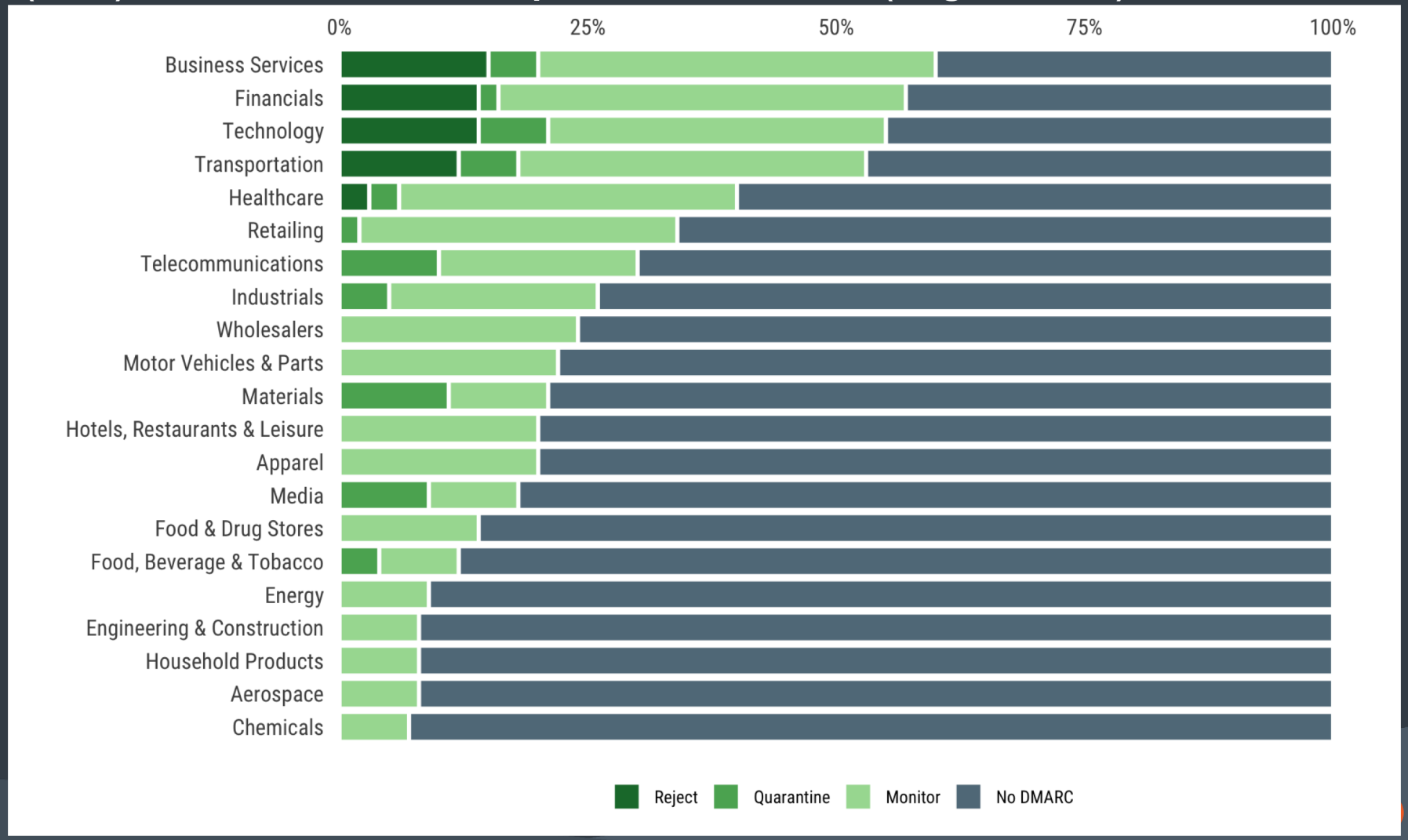
Core takeaway:

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.

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



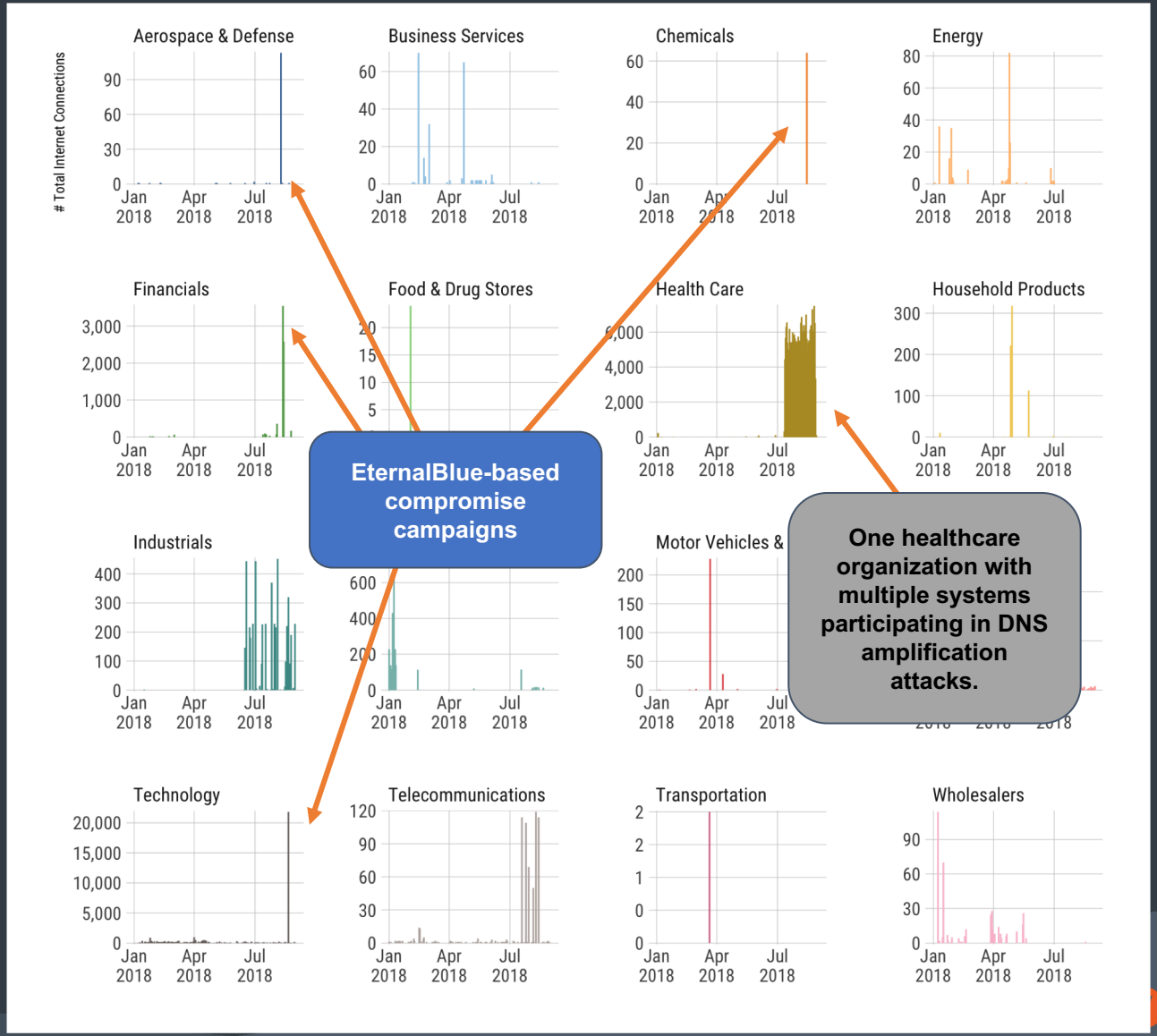
Fortune 500 ICE → Evidence of System Compromise

Core takeaway:

This chart should be blank.

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 → Use of Shared 3rd Party Services

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

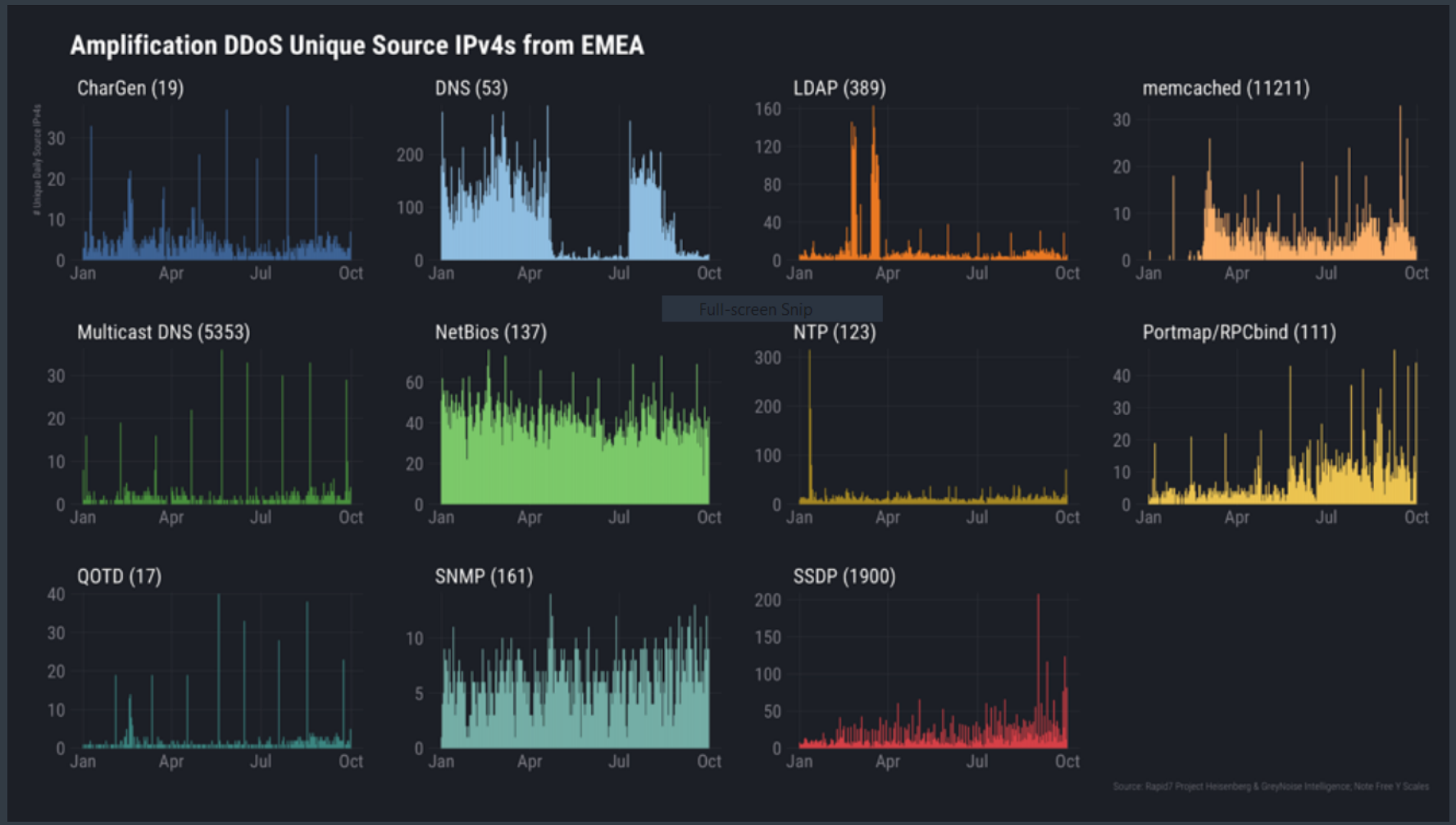
- Exposed attack surface averages 500 servers/devices per organization, up to more than 2,500 for many.
- On average, a min. of 5–10 known exploitable systems deployed and exposed.
- Two thirds of Fortune 500 organizations have weak or nonexistent anti-phishing defenses.
- Across all industries, exposure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

EMEA Data

Amplification DDoS from EMEA

Core takeaway:

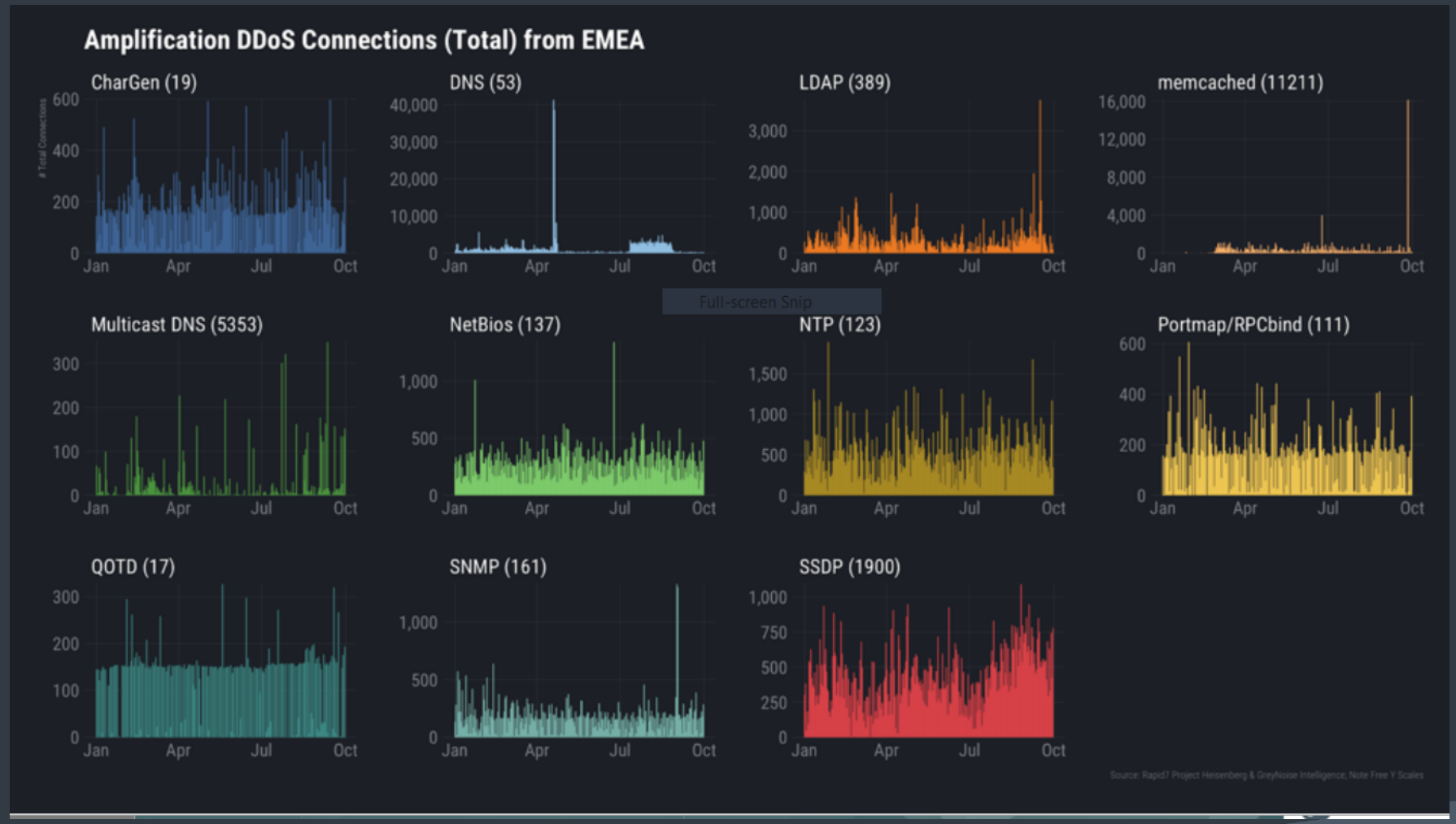
Counts vary dramatically in & across unique sources but the spikes show activity in services that attackers can probe & attack at-will.



Amplification DDoS – EMEA Total Connections

Core takeaway:

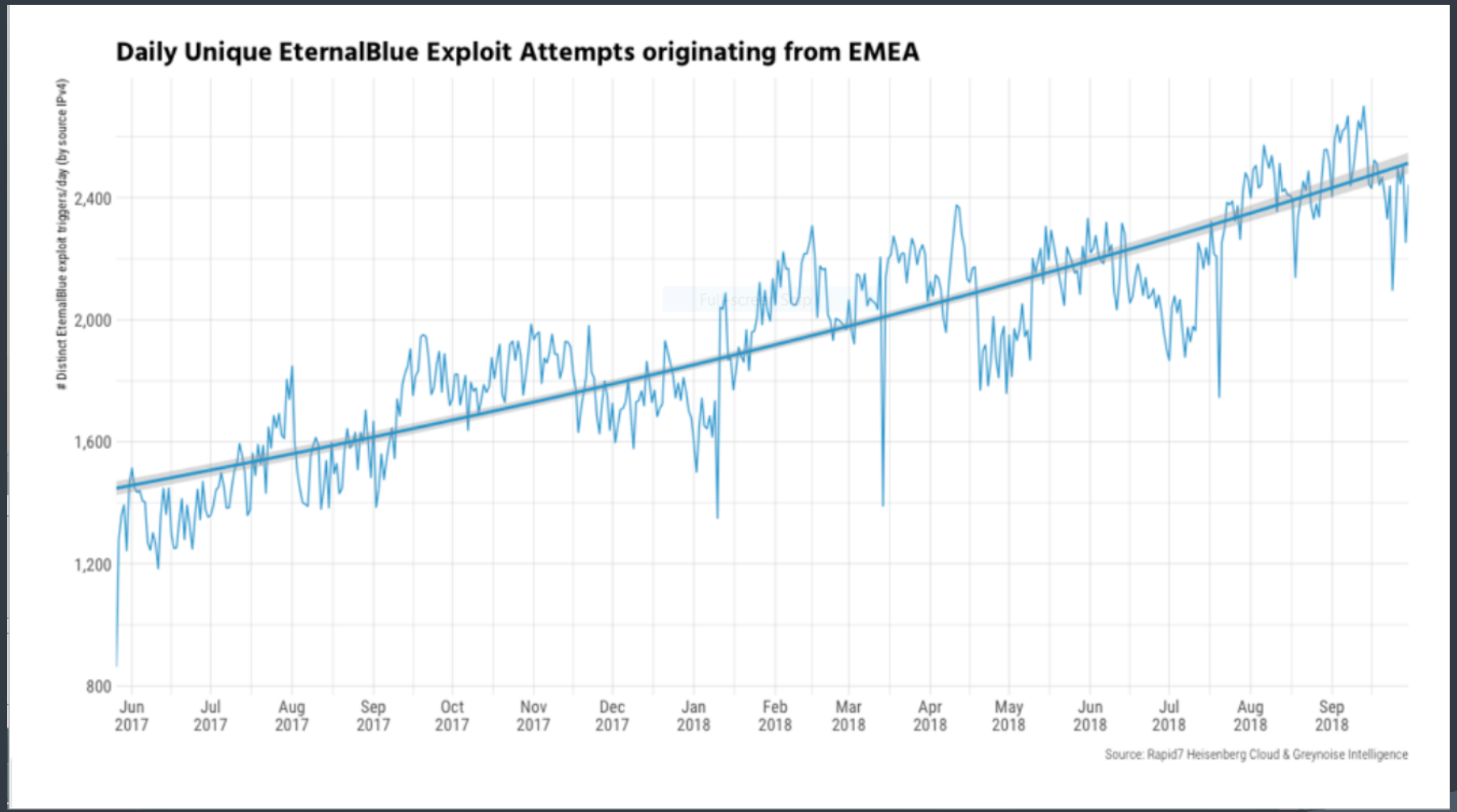
Counts vary dramatically in & across connections but the spikes show activity in services that attackers can probe & attack at-will.



Daily Unique EternalBlue Exploit Attempts from EMEA

Core takeaway:

The daily unique EternalBlue exploit attempts originating from EMEA are on the rise.

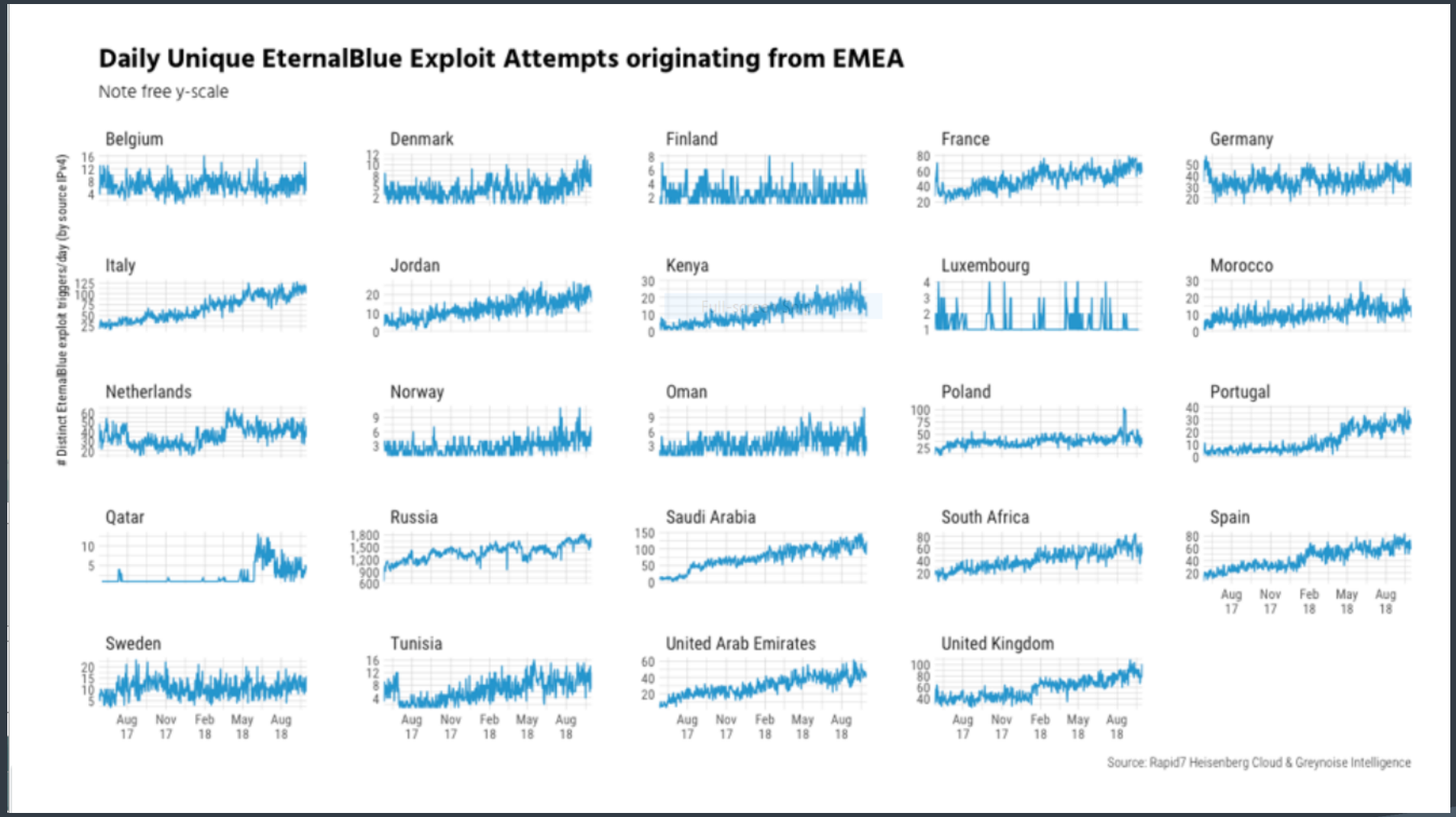


RAPID7

Daily Unique EternalBlue Exploit Attempts per region EMEA

Core takeaway:

The daily unique EternalBlue exploit attempts originating from EMEA are on the rise for specific countries and regions such as Russia, Saudi Arabia and the UK specifically.



Recommendations

EMEA: Recommendations

- Implement SPF
- Setup DKIM
- Enable DMARC in Monitor mode
- Plan to phase to Quarantine within 3 month's time
- Plan to phase to Reject within one month later

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

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**

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

Thank you!

For more on Rapid7 research, please visit:

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

- Michelle Martinez• Senior Threat Intelligence Analyst
- Kwan Lin • Senior Data Scientist
- Bob Rudis • Chief Data Scientist

Full-screen Snip

https://www.rapid7.com/info/threat-report/

RAPID7