2020 NICER Report

Federal Trade Commission Briefing
On Rapid7's 2020 Internet Atlas

"America built the internet and shared it with the world; now we will do our part to secure and preserve cyberspace for future generations."[2]

"Information technology creates enormous value for the U.S. economy. However, it also exposes U.S. firms, the government sector, and private individuals to new risks that originate and are often effectuated entirely in cyberspace."[1]

"Cybersecurity is a common good. A firm with weak cybersecurity imposes negative externalities on its customers, employees, and other firms tied to it through partnerships and supply chain relations."[1]

[1] February 21 2018 Fighting Cybersecurity Threats to the Growing Economy
[2] September 20, 2018 Statement from the President Regarding the National Cyber Strategy

How we are able to measure exposure

- Internet-wide scanning (Project Sonar)
- Honeypots (Project Heisenberg)
- Unique visibility produces most comprehensive Internet survey
- Detailed methodology in NICER

NICER

National
I ndustry
Cloud
Exposure
Report

Top Takeaways

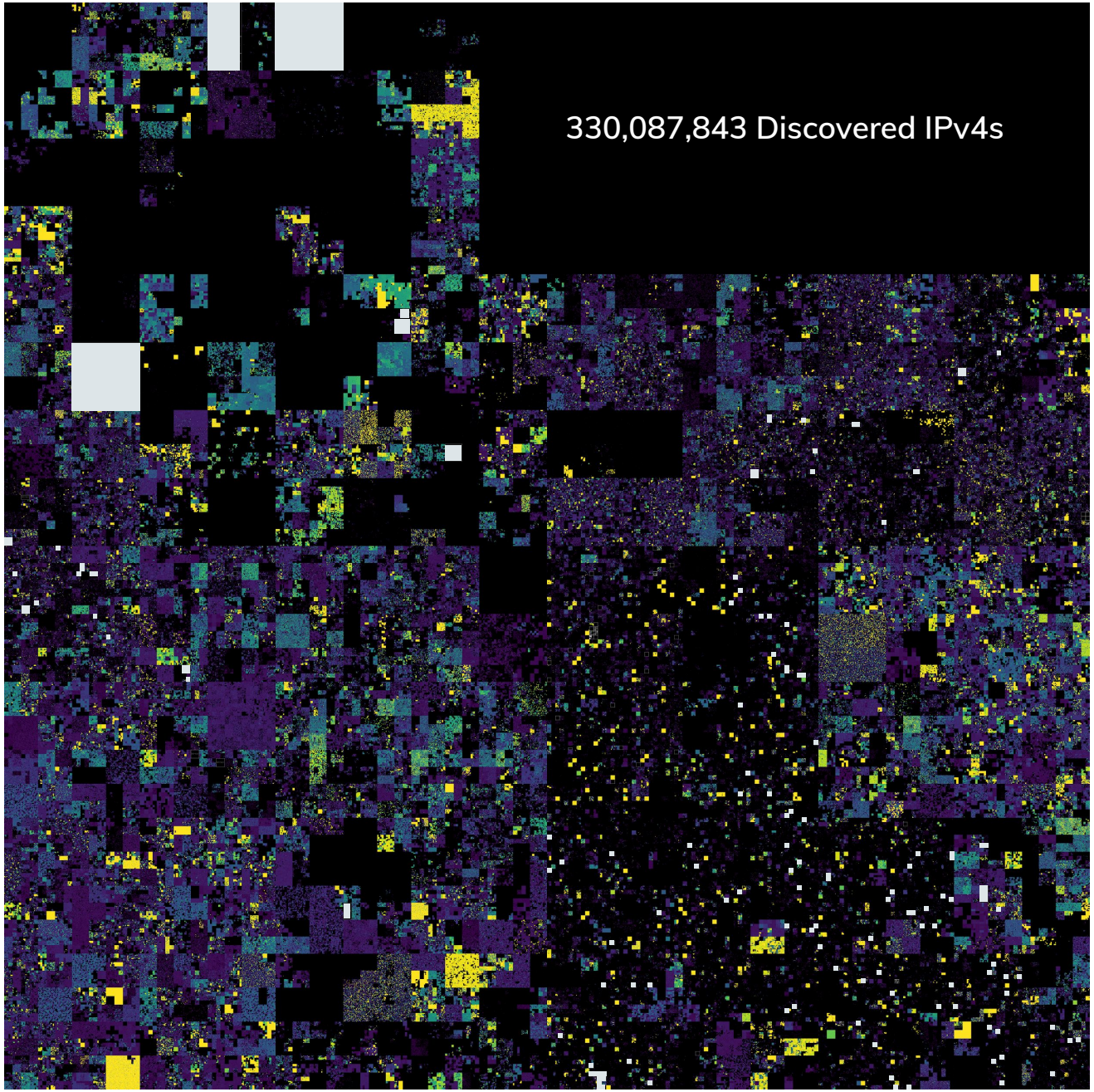
- The US🇺🇸 is the most exposed country. China🇨🇳 is second.
- Large scale exposure among big companies across all global industry sectors. **Telecom** and **Finance** most exposed.
- Millions of assets continue to offer dangerous services (though overall, dangerous service exposure is getting marginally better).
- Millions of assets are running un-updated software versions **vulnerable to exploitation.**
- ***<u>What should be done:</u> Reduce reliance on dangerous services and update those services that must be online.***

NICER

National Industry Cloud Exposure Report

"Security flaws that are publicly visible."

- Dangerous services vulnerable to attack (i.e., Microsoft Windows SMB, Telnet)
- Outdated, unpatched software vulnerable to old, known exploits
- Unencrypted protocols that reveal sensitive data (cleartext / plaintext)
- Originators and amplifiers of malicious traffic DoS/DDoS


330,087,843 Discovered IPv4s

NICER

National Industry Cloud Exposure Report

- High accuracy (~96.5%) of IPv4 attribution
- More IP space ∴ more exposure
- Dangerous services/configurations impact national security
- Rankings based on measuring IP prevalence, service exposure and “patchedness”

Rank	Country
1	**United States**
2	China
3	South Korea
4	United Kingdom
5	Germany
6	Brazil
7	Russia
8	Japan
9	Canada
10	Iran
11	Italy
12	Argentina
13	Taiwan
14	Australia
15	Spain
16	France
17	India

Rank	Country
18	Turkey
19	Hong Kong
20	Mexico
21	Vietnam
22	Netherlands
23	Egypt
24	Thailand
25	Ireland
26	Sweden
27	Indonesia
28	South Africa
29	Singapore
30	Poland
31	Colombia
32	Saudi Arabia
33	Venezuela
34	UAE

Rank	Country
35	Morocco
36	Portugal
37	Algeria
38	Austria
39	New Zealand
40	Romania
41	Ukraine
42	Switzerland
43	Chile
44	Malaysia
45	Norway
46	Tunisia
47	Belgium
48	Croatia
49	Hungary
50	Greece

Deep Dive: 🇺🇸 

Deep Dive: 🇺🇸 S

54,539,614 Servers / routers / devices found

Deep Dive: 🇺🇸 S

CVE Severity	Total Found
Low	5,773,581
Medium	7,671,842
High	**8,413,402**

Just under
8.5 million* high severity vulnerabilities
across those 54.5 million devices.

Deep Dive: 🇺🇸 S

191,314 Windows/Linux SMB Servers

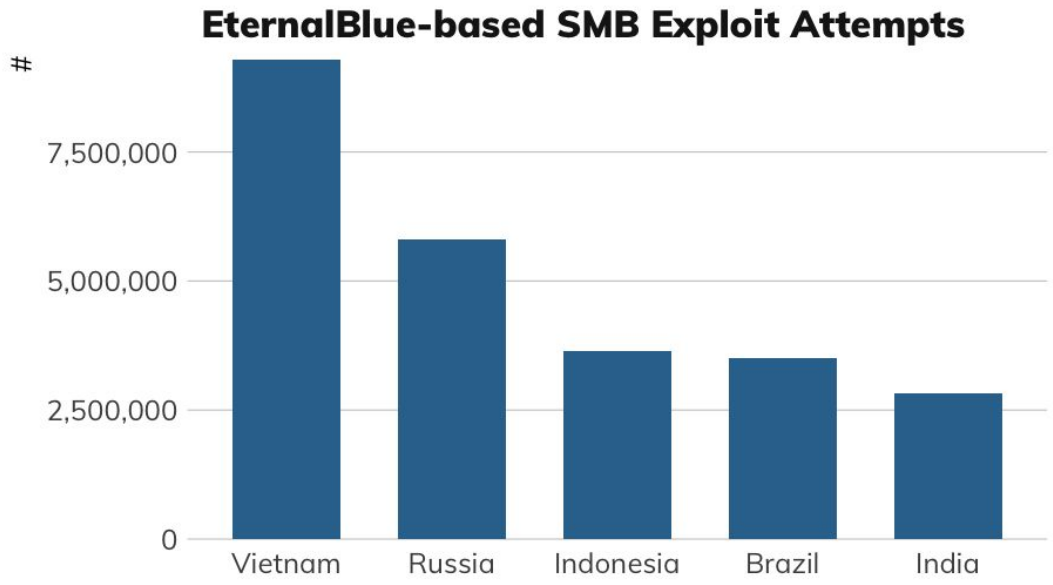
RAPID7

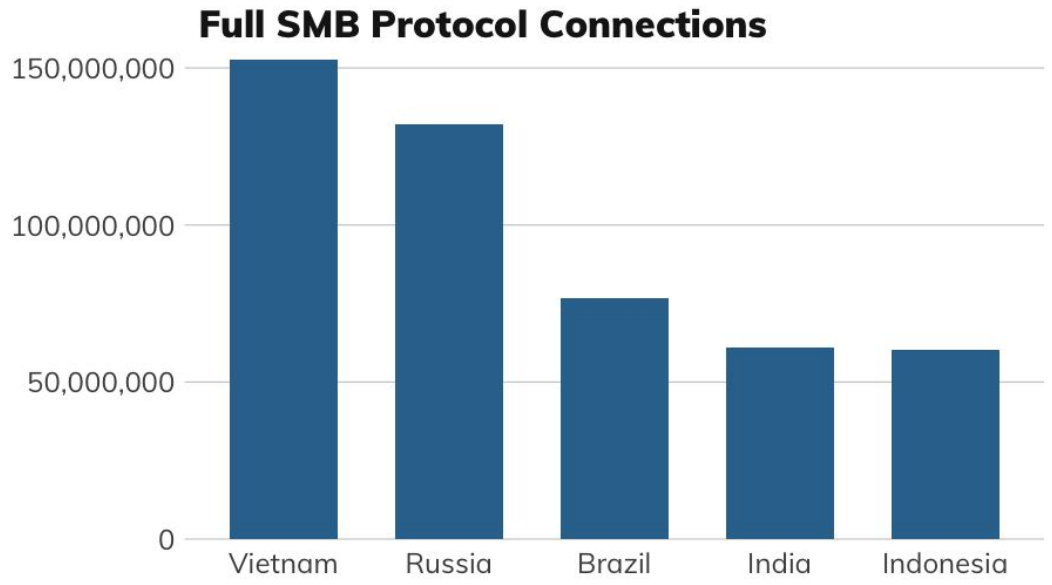
Deep Dive: 🇺🇸 S

191,314 Windows/Linux SMB Servers

Project Heisenberg Malicious SMB Activity by Source Country (April 2020)

Note free Y scales





Deep Dive: 🇺🇸 RDPS

921,828 Microsoft RDP Servers

Deep Dive: Citrix

921,828 Microsoft RDP Servers

23,433 Citrix ADC/Netscaler

70% patched

Alert (AA20-031A)

Detecting Citrix CVE-2019-19781

Deep Dive: DDoS

921,828 Microsoft RDP Servers

23,433 Citrix ADC/Netscaler

70% patched

Alert (AA20-031A)

Detecting Citrix CVE-2019-19781

21,491 Memcached

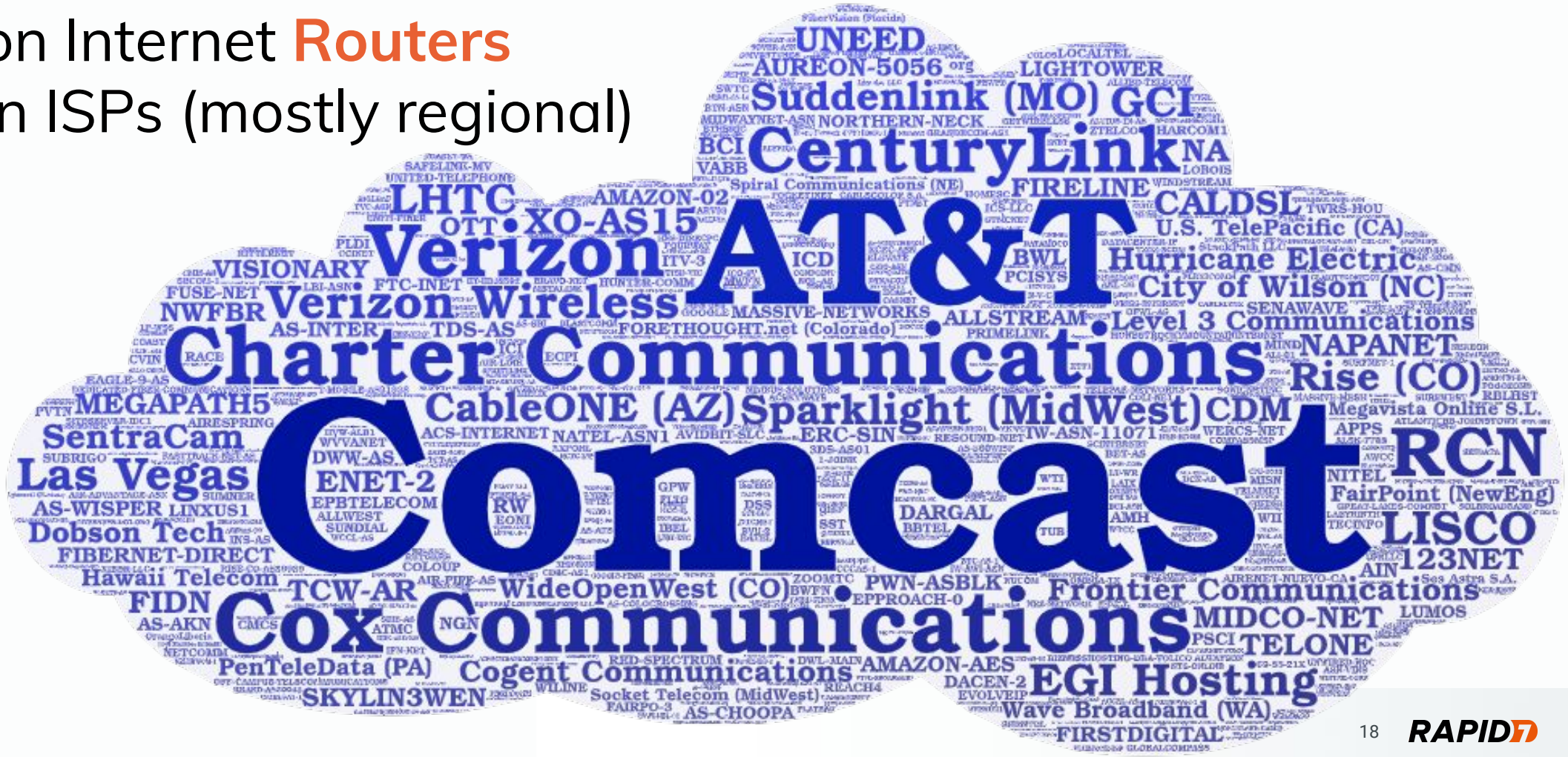
GitHub Survived the Biggest DDoS Attack Ever Recorded

Deep Dive: 🇺🇸 TelnetS

232,616 Telnet servers

>5,700 on Internet Routers

>500 in ISPs (mostly regional)



RAPID7

```
$ telnet 67.###.##.66
Trying 67.###.##.66...
Connected to 67.###.##.66.
Escape character is '^]'.

MikroTik v6.45.8
Login:
```

```
$ telnet 24.###.##.158
Trying 24.###.##.158...
Connected to 24.###.##.158.
Escape character is '^]'.

MikroTik v6.44.3 (stable)
Login:
```

```
$ telnet 216.###.##.141
Trying 216.###.##.141...
Connected to 216.###.##.141.
Escape character is '^]'.

MikroTik v6.42.3 (stable)
Login:
```

Blockchain & Cryptocurrency , Cybercrime , Endpoint Security

Cryptojackers Keep Hacking Unpatched MikroTik Routers

Vigilante Hacker Is Killing Unpatched Routers' Remote Administration Ability

Mathew J. Schwartz (euroinfosec) • October 19, 2018

FROM EXPOSURE TO TAKEOVER

The 15 billion stolen credentials allowing account takeovers

Authors: Digital Shadows Photon Research Team

digital shadows_

But, it’s bad everywhere...

Millions of assets using dangerous protocols...

Protocol	Port	2020
SMB	445	594,021
Telnet	23	2,830,759
rsync	873	208,882
POP3	110	4,335,533
SMTP	25	5,809,982
IMAP	143	4,049,427
SMTP	587	4,011,697
RDP	3389	3,979,356
POP3S	995	3,717,883
IMAPS	993	3,852,613
MS SQL Server	1434	98,771
SMTPS	465	3,497,791
DNS (Do53)	53	8,341,012
FTP	21	13,002,452
NTP	123	1,638,577
FTPS	990	460,054

...slowly getting better;

often due to nation state and/or ISP intervention.

Protocol	Port	2019	2020	Change	Percentage
SMB	445	709,715	594,021	-115,694	**-16.30%**
Telnet	23	3,250,417	2,830,759	-419,658	**-12.91%**
rsync	873	233,296	208,882	-24,414	**-10.46%**
POP3	110	4,818,758	4,335,533	-483,225	**-10.03%**
SMTP	25	6,439,139	5,809,982	-629,157	**-9.77%**
IMAP	143	4,296,778	4,049,427	-247,351	**-5.76%**
SMTP	587	4,220,184	4,011,697	-208,487	**-4.94%**
RDP	3389	4,171,666	3,979,356	-192,310	**-4.61%**
POP3S	995	3,887,033	3,717,883	-169,150	**-4.35%**
IMAPS	993	4,008,577	3,852,613	-155,964	-3.89%
MS SQL Server	1434	102,449	98,771	-3,678	-3.59%
SMTPS	465	3,592,678	3,497,791	-94,887	-2.64%
DNS (Do53)	53	8,498,166	8,341,012	-157,154	-1.85%
FTP	21	13,237,027	13,002,452	-234,575	-1.77%
NTP	123	1,653,599	1,638,577	-15,022	-0.91%
FTPS	990	443,299	460,054	16,755	3.78%
SSH	22	15,890,566	18,111,811	2,221,245	**13.98%**
DNS over TLS (DoT)	853	1,801	3,237	1,436	**79.73%**

Pandemic Effects on the Internet

What does pandemic mean for the internet?

Doom🌋 and gloom😿 predicted...

...but not observed 🔬!

Turns out the internet is resilient to biological viruses☣️.

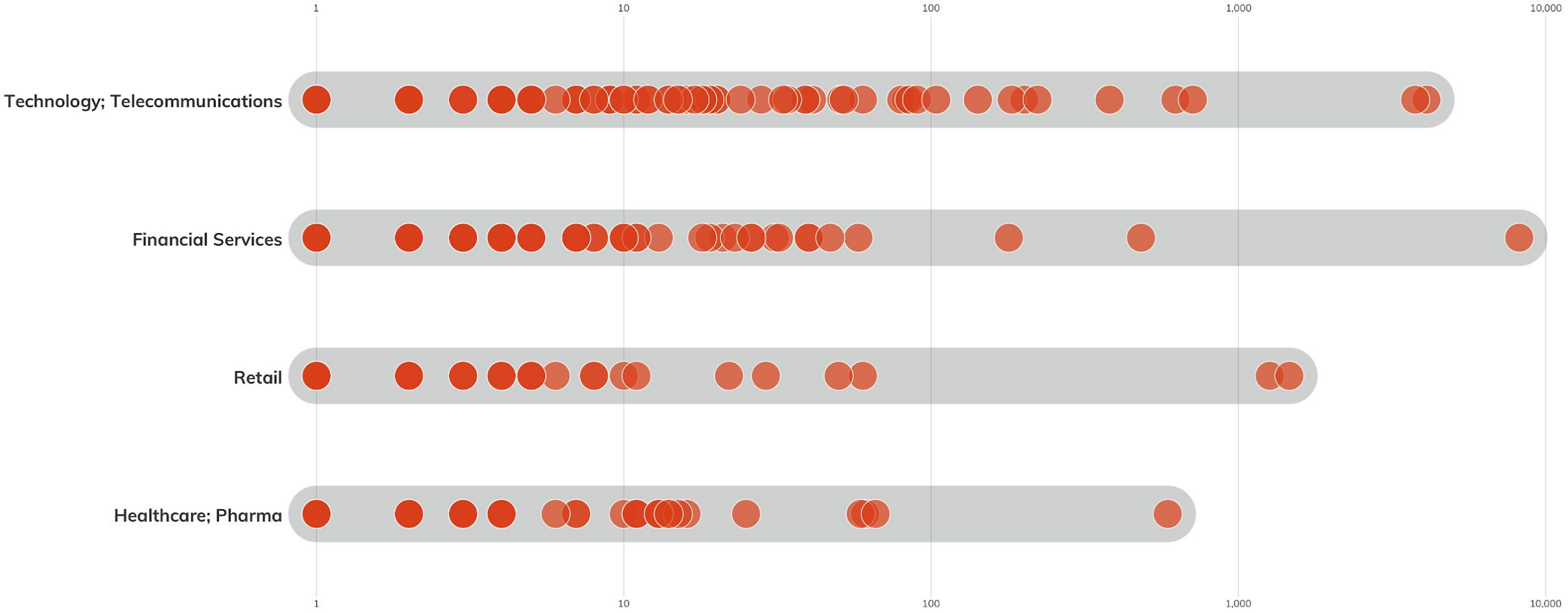
NICER

National Industry Cloud Exposure Report

The Rapid7 Industry 1500

- Exposure analysis of the best resourced public companies in the world.
- Focus on US, UK, Germany, Japan, and Australia
  - Fortune 500
  - FTSE 250
  - DB 350
  - Nikkei 225
  - ASX 200


1
10
100
1,000
10,000
Technology; Telecommunications
Financial Services
Retail
Healthcare; Pharma
Engineering; Construction; Industrials
Aerospace; Defense; Transportation
Business Services; Media
Energy; Utilities
Food; Beverages; Tobacco
Consumer
Materials; Mining
Transportation; Logistics
Wholesale
Motor Vehicles; Parts
Hotels; Restaurants; Leisure
Administrative; Professional
Real Estate
1
10
100
1,000
10,000
High Severity Vulnerabilities Across Industries



High Severity Vulnerabilities Across Industries (Top 4)

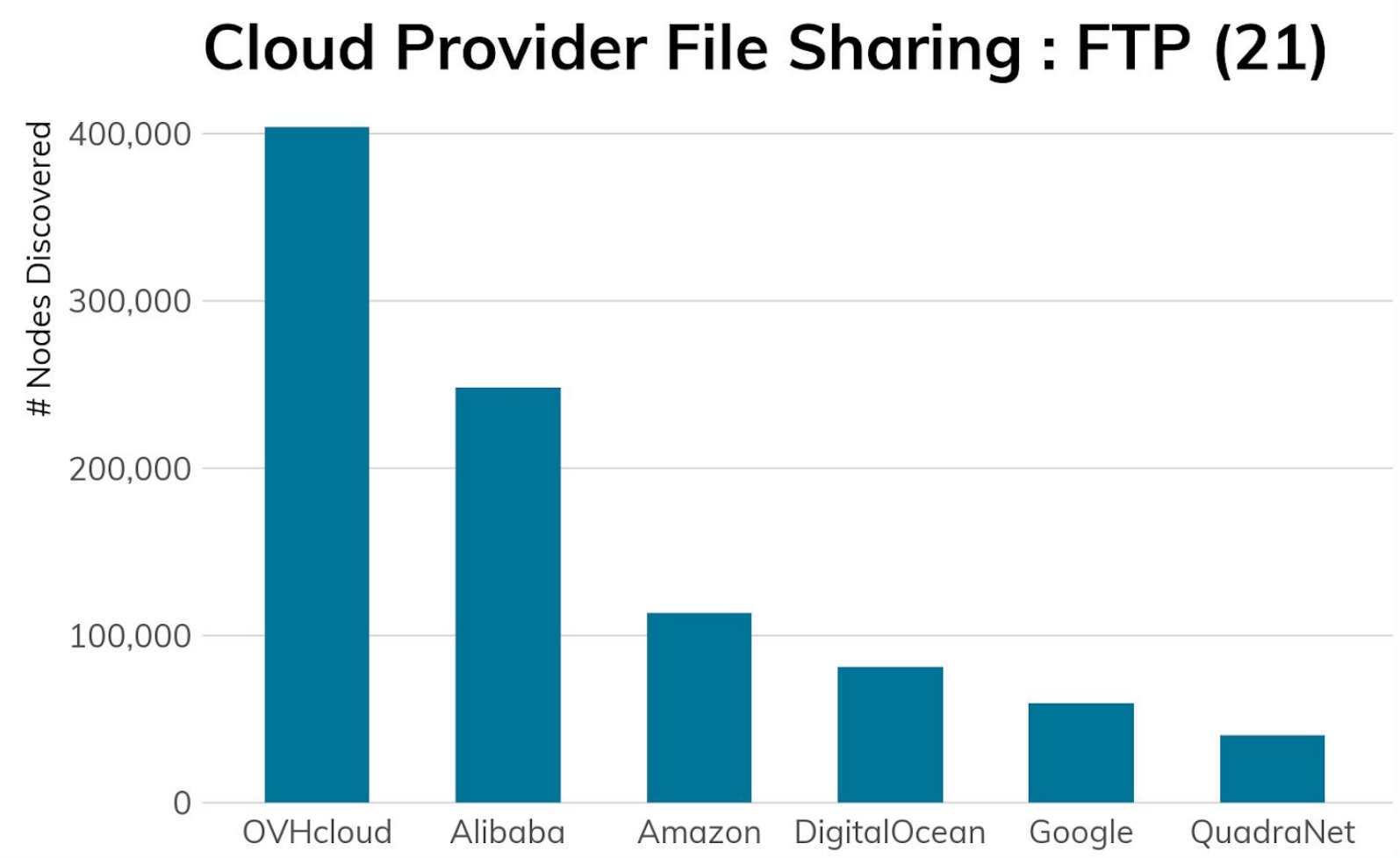
National Industry Cloud Exposure Report

The Myth of the Silver City

- How does "the Cloud" impact internet security?
- Paas and Iaas providers are proliferating
- Surely they're doing The Right Thing?

Example: Cleartext FTP in the Cloud?

- Symptom of "lift-and-shift"
- More secure alts exist
  - scp, ftps, rsync + ssh…
- PaaS could steer customers



Key Finding: Cryptographic Design

- *Key finding:* **Cleartext protocols are still the rule**, rather than the exception, on how information flows around the world. 42% more plaintext HTTP servers than HTTPS, 3 million databases awaiting insecure queries, and 2.9 million routers, switches, and servers accepting Telnet connections.
- *Why this is a problem:* Sensitive data is exposed in transit, and there's no guarantee of authenticity of the server, the client, or the data.
- *Key recommendation:* If it touches the internet, it should be encrypted. This goes for data, service identification, everything.

Key Finding: Service Deployment

- *Key finding:* **Millions of assets are exposing dangerous and insecure services** to the entire internet. There are still over 200,000 rsync servers, half a million SMB servers, three million MySQL servers, and many more across the spectrum, all directly exposed to internet-based attackers.
- *Why this is a problem:* Unregulated access to these services means unregulated opportunity for attack, either through credential stuffing or vulnerability exploitation.
- *Key recommendation:* Routinely scan your own network from the outside to keep tabs on what you're exposing. Expect attackers, regulators, and insurers to do the same.

Key Finding: Service Deployment... getting better

- *Key finding:* One bit of positive news was that we found the population of insecure services has gone down over the past year, with an average **13% decrease in exposed, dangerous services** such as SMB, Telnet, and rsync, crushing the doom-and-gloom predicted jump of newly exposed insecure services such as Telnet and SMB, despite the sudden shift to work-at-home for millions of people and the continued rise of Internet of Things (IoT) devices crowding residential networks.
- *Key recommendation:* Keep up the good work!

Key Finding: Console Access

- *Key finding:* We have discovered nearly **three million telnet servers still active** and available on the internet, and many of those are associated with core routing and switching gear. This is three million too many. While remote console access is a fundamental design goal of the internet, there is no reason to rely on and expose this ancient technology on the routers and switches.
- *Why this is a problem:* Offers external, across-the-globe attackers an opportunity to directly control and shape network traffic, and they're merely one good password guess away.
- *Key recommendation:* Telnet, SSH, RDP, and VNC should all enjoy at least one extra layer of security — either multifactor authentication, or available only in a VPN'ed environment.

Key Finding: Software Maintenance

- *Key finding:* **Millions of assets are not updated to the latest software versions.** Patch and update adoption continues to be slow, even for modern services with reports of active exploitation. This is particularly true in the areas of email handling and remote console access where, for example, 3.6 million SSH servers are sporting [vulnerable] versions between five and 14 years old.
- *Why this is a problem:* Unpatched and legacy software is vulnerable to known exploits.
- *Key recommendation:* Given that all software has bugs and patching is inevitable, enterprises should bake in regular patching windows and decommissioning schedules to their internet-facing infrastructure.

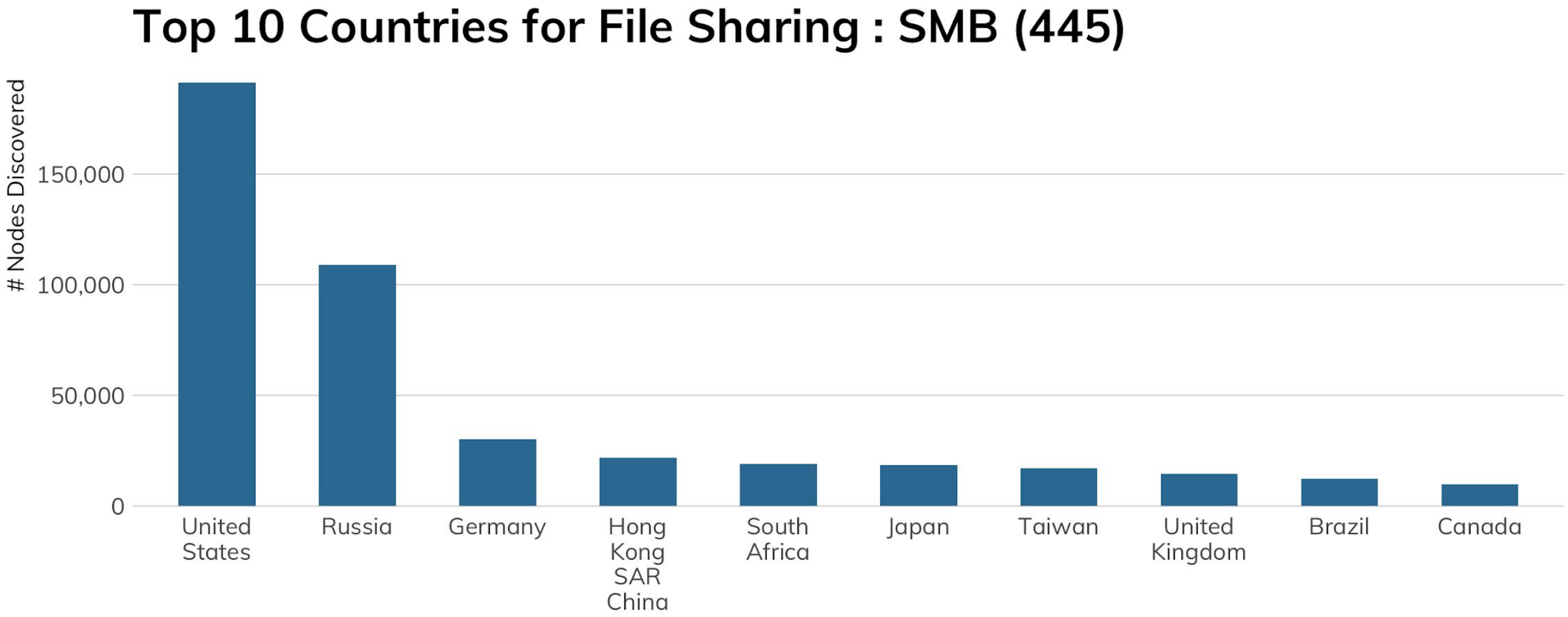
How to read NICER

Simplified Takeaways

TLDR

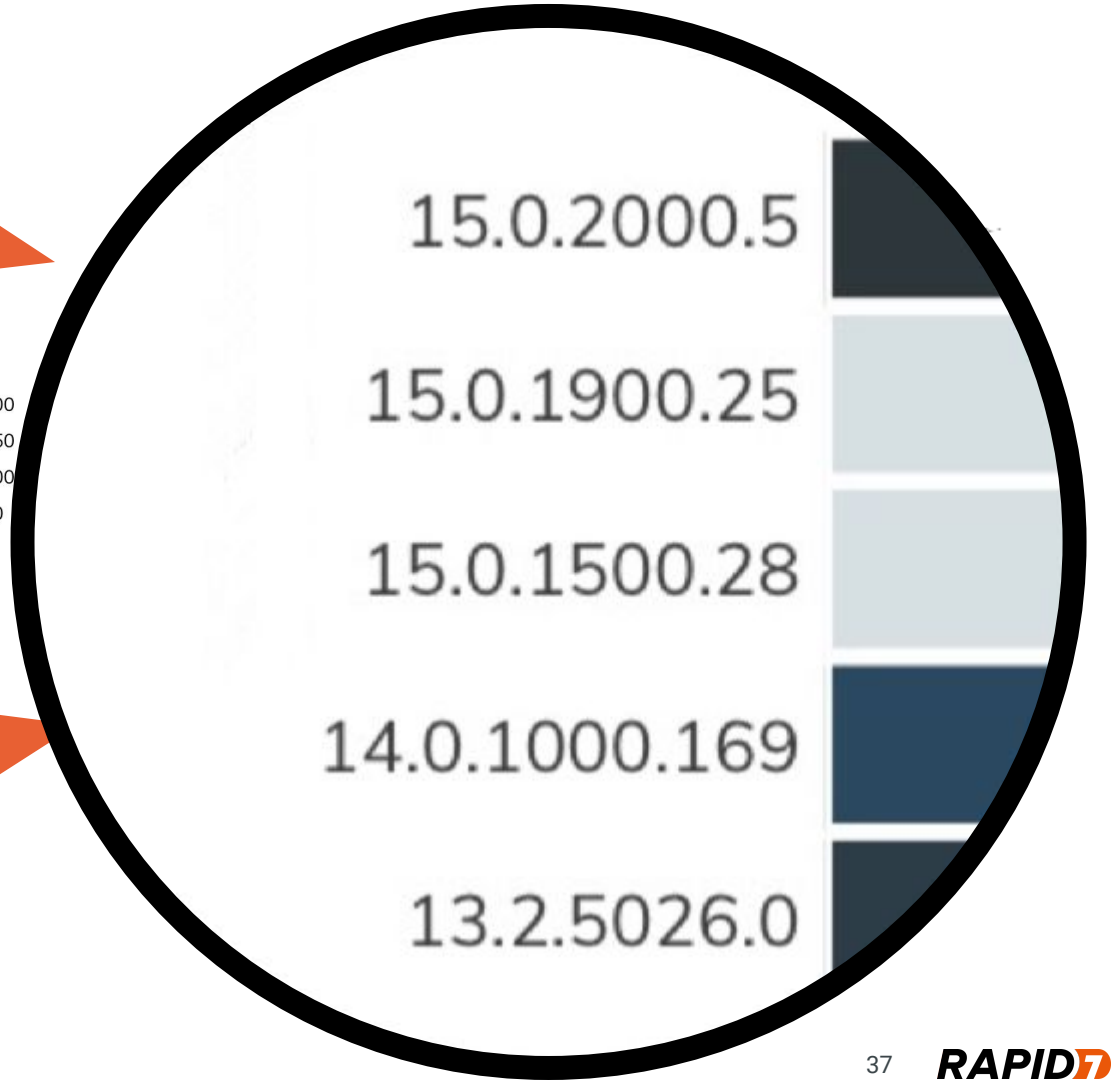
- WHAT IT IS: One of the oldest remote console applications in use today on the internet.
- HOW MANY: 2,829,555 discovered nodes
  389,528 (13.7%) have Recog fingerprints for 36 total service families
- VULNERABILITIES: Oddly, there are few remote code execution-style vulnerabilities, but plenty of default credentials and opportunities to eavesdrop on the same.
- ADVICE: Never, ever expose Telnet to the internet.
- ALTERNATIVES: SSH (Secure Shell) is the most straightforward alternative to Telnet, but consider the wisdom of exposing console access to the internet in the first place.
- GETTING: Better! There was a 13% reduction from 2019 exposure.

At-a-glance Comparisons



Range of MS SQL Server Versions Exposed in Turkish Hosting Providers

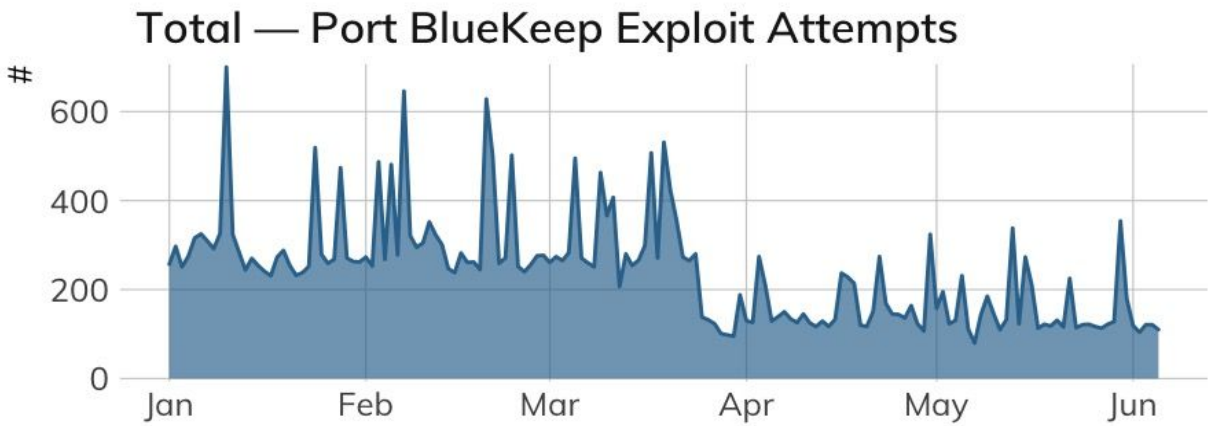
Methodology: Digging In Deep

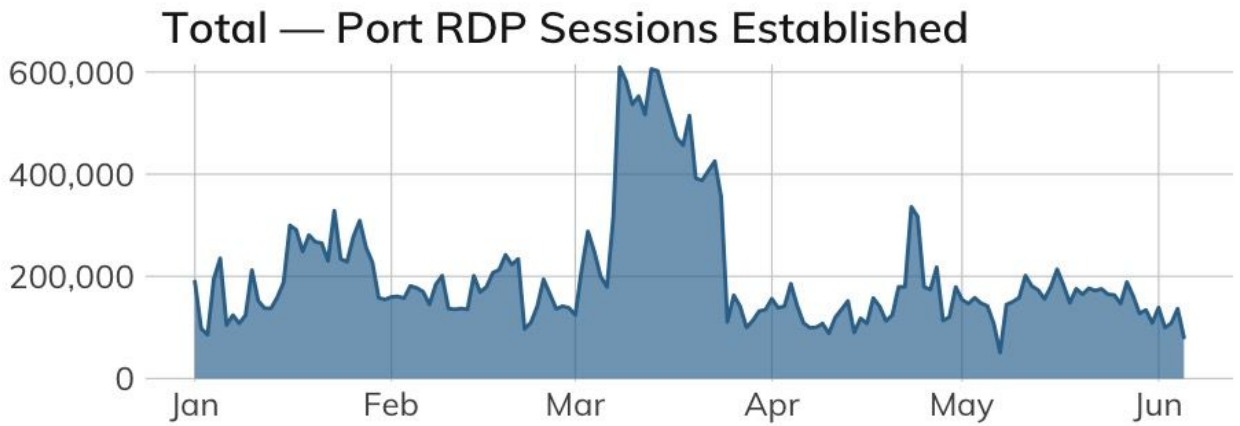


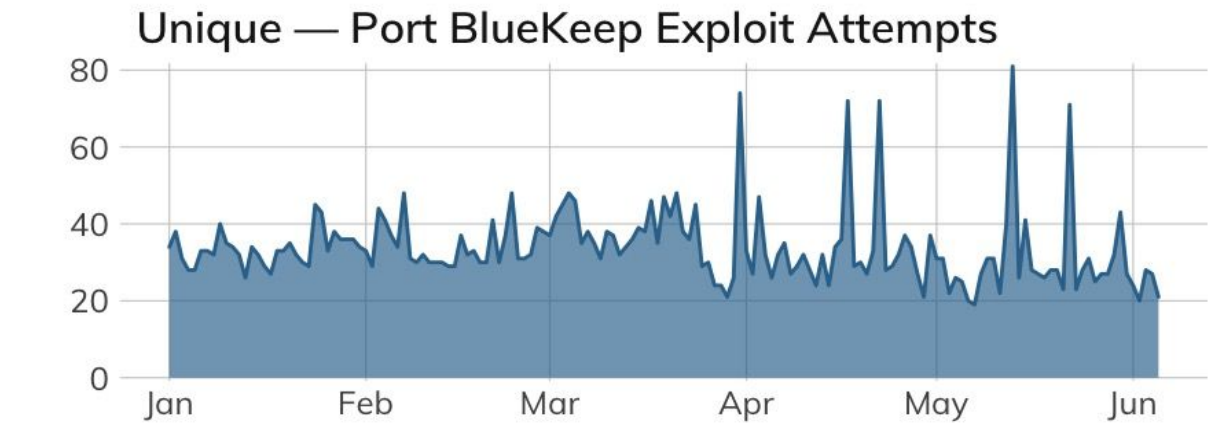
RAPID7

Not Just Scans

Project Heisenberg RDP Activity







Note free Y scales

Practical Guidance

Our Advice

IT and IT security teams should routinely review the costs involved in running their own on-premises mail infrastructure, in terms of not just money, but time and expertise. If at all possible, they should see about moving off to a professionally maintained email provider, like Outlook 365 or Google G Suite (which offer TLS-backed client mail services by default), and reap the benefits of uptime assurance and spam-scrubbing being Someone Else's Problem.

Cloud providers should, similarly, steer people away from maintaining their own email infrastructure, and gently encourage customers to investigate the sane and stable alternatives. At the very least, cloud provider documentation should clearly explain the differences between POP and IMAP and why you might not need one or the other, then guide customers toward TLS-wrapped client mail services.

Government cybersecurity agencies should advocate for strong encryption alternatives to the cleartext IMAP and POP protocols, and educate the public on the fact that POP and IMAP are often convenient backdoors to password testing, since they are rarely secured with multi-factor authentication.

Thank you!

How can we at Rapid7 help

secure and preserve cyberspace for future generations?

research@rapid7.com

rapid7.com/nicer