RAPID7

RESEARCH

# Industry Cyber-Exposure Report

## FTSE 250+

Rapid7 Labs

June 11, 2019

## TABLE OF CONTENTS

# Executive Summary

In the face of growing cybersecurity threats, it is increasingly important to measure the cost and concentration of "exposure," which we define here as weaknesses in the public-facing configuration of internet-connected services. Having an accurate view of the resilience of organisations and industries against cyber-attacks can facilitate more accurate cost models, help target efforts to reduce exposure to the industries that need it most, and enhance cooperative efforts between government and the private sector to better protect users and companies alike. Measurement of industry-level exposure can also inform working groups that share cybersecurity information and threat intelligence within their industry.

To understand current levels of exposure and resiliency in the United Kingdom, Rapid7 Labs measured the internet-facing security profiles of the FTSE 250[1] plus a handful of non-FTSE 250 members that meet certain size and revenue criteria[2] to ensure sufficient statistical coverage in each industry (this combined list of 253 companies will be referred to as the FTSE 250+ throughout the remainder of the report) during Q1 2019 for:

- Overall attack surface (the number of exposed servers/devices);
- Presence of dangerous or insecure services;
- Phishing defence posture;
- Weak public service and metadata configurations; and
- Joint third-party website dependency risks.

We believe this is the most comprehensive and accurate public report covering the real-world internet presence of a national economy to date. By measuring these specific areas of cybersecurity, we are able to zero-in on the most common problem areas in each of the surveyed industries and offer practical, specific defensive advice to each one.

An important factor to consider in the context of discovered weaknesses is that members of the FTSE 250+ list are well-resourced organisations that typically attract top talent in all aspects of the business, including information technology (IT) and security. The discovery of such widespread weaknesses in the exposed services of these leading organisations makes it likely that there is even greater exposure and risk in smaller organisations with fewer human and financial resources available for securing their public internet resources.

**Key findings include:**

- FTSE 250+ organisations, on average, expose a public attack surface of 35 servers/devices, with many companies exposing over 1,000 systems/devices.
- Of the appraised FTSE 250+ organisations, 231 (88%) have weak or nonexistent anti-phishing defences (i.e., DMARC) in the public email configuration of their primary email domains. This is the weakest anti-phishing showing of all the Rapid7 Industry Cyber-Exposure Reports (ICERs) to date.[3]
- SSL/TLS security is not enforced on the primary websites of 19% of FTSE 250+ organisations. This leaves visitors open to a wide array of common and potentially devastating attacks by adversaries in a position to modify web content as it is being transmitted.

[1] FTSE 250 list, https://www.londonstockexchange.com/exchange/prices-and-markets/stocks/indices/summary/summary-indices-constituents.html?index=MCX (Last accessed May 21, 2019)

[2] FTSE inclusion criteria, https://www.ftse.com/products/downloads/FTSE_UK_Index_Series.pdf (Last accessed May 21, 2019)

[3] This figure was 73% for the US-centric Fortune 500, and 68% in the Australasia-centric ASX 200.

- All industry sectors had at least one organisation with malware infections, with Administrative and Professional organisations showing monthly signs of regular compromise. Incidents across industries ranged from company resources being co-opted into denial-of-service (DoS) amplification attacks to signs of EternalBlue-based campaigns similar to WannaCry and NotPetya.
- Many organisations across industry sectors in the FTSE 250+ signal how many and which cloud service providers they use in their public domain name system (DNS) metadata, with 114 organisations using between two and seven cloud service providers. This information can be used to craft highly effective, targeted attacks, among other actions.
- Severely vulnerable services such as Telnet and Windows SMB file-sharing were present in only a few organisations, which is positive. However, most organisations in every sector had serious issues with patch/version management of business-critical internet-facing systems.

The details behind these findings are presented in the remainder of the report.

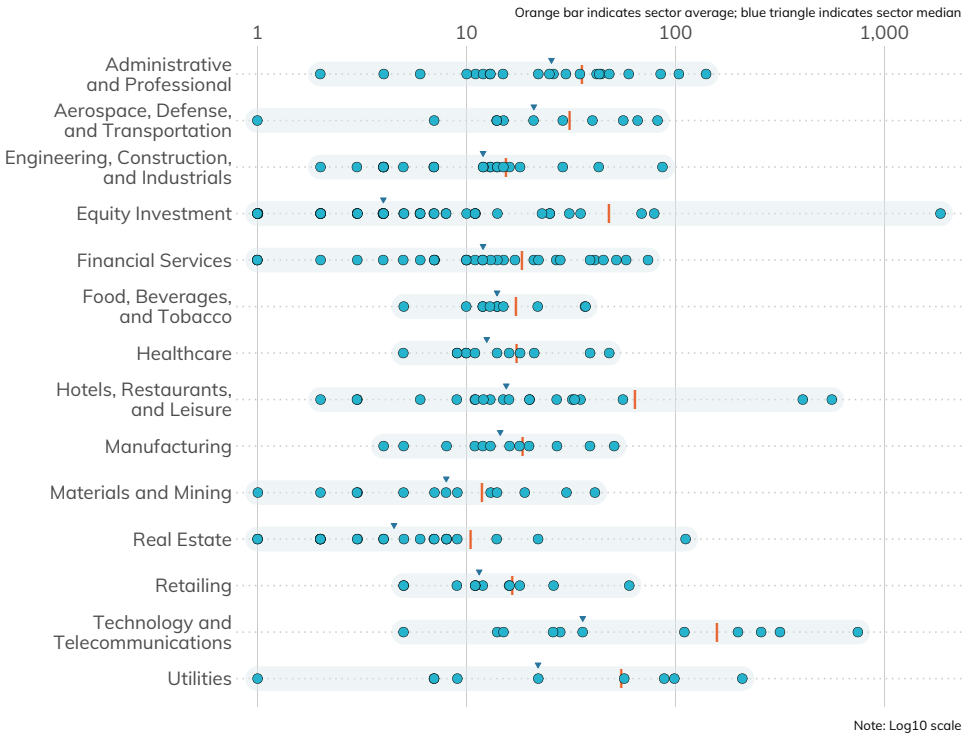
# Overview of Results

## Attack Surface by Sector

The **Methodology** section (pg. 27) details how Rapid7 uses Project Sonar[4] to scan the internet for exposed systems and devices. On average, each FTSE 250+ organisation exposes roughly 35 services. This number is neither good nor bad, but each exposed node increases the attack surface of an organisation, potentially boosting the opportunity for attackers to gain a foothold. To put it another way, each exposed server or device must be properly configured, managed, patched, and defended to reduce the risk of a cyber-attack. There is no rule to indicate when the number of exposed services tips the balance of risk, since many factors can influence how well an organisation can protect its internet-exposed resources. Still, the more exposed systems, the more opportunity attackers gain, regardless of defensive capabilities.

**Figure 1: Distribution of Discovered Organisation Asset Totals by Sector**

**Each dot represents one organisation; position on axis = number assets discovered.**




Taking a look at Figure 1, there are four outliers: one in Equity Investment, two in Hotels, Restaurants, and Leisure, and one in Technology and Communications. If your business processes do require increased levels of asset exposure (as it seems is the case for these four organisations), you must have commensurate vulnerability management, patching, and monitoring practices in place to facilitate a speedy response to discovered weaknesses or attempts by attackers to compromise your services. If your business processes are not the direct reason for this exposure and/or you do not have a well-oiled asset identification and configuration management process in place, working to reduce the surface area should be paramount, followed by plans to shore up those IT/security operational areas.

### Recommendation: Reduce Attack Surface

Organisations should strive to only expose systems and devices on the internet if they support business processes and must further ensure they have robust asset identification and configuration management processes in place to help avoid these systems becoming enterprise entry points for attackers.

[4] Rapid7, Project Sonar, https://www.rapid7.com/research/project-sonar (Last accessed May 21, 2019)

## Phishing Defence Capabilities

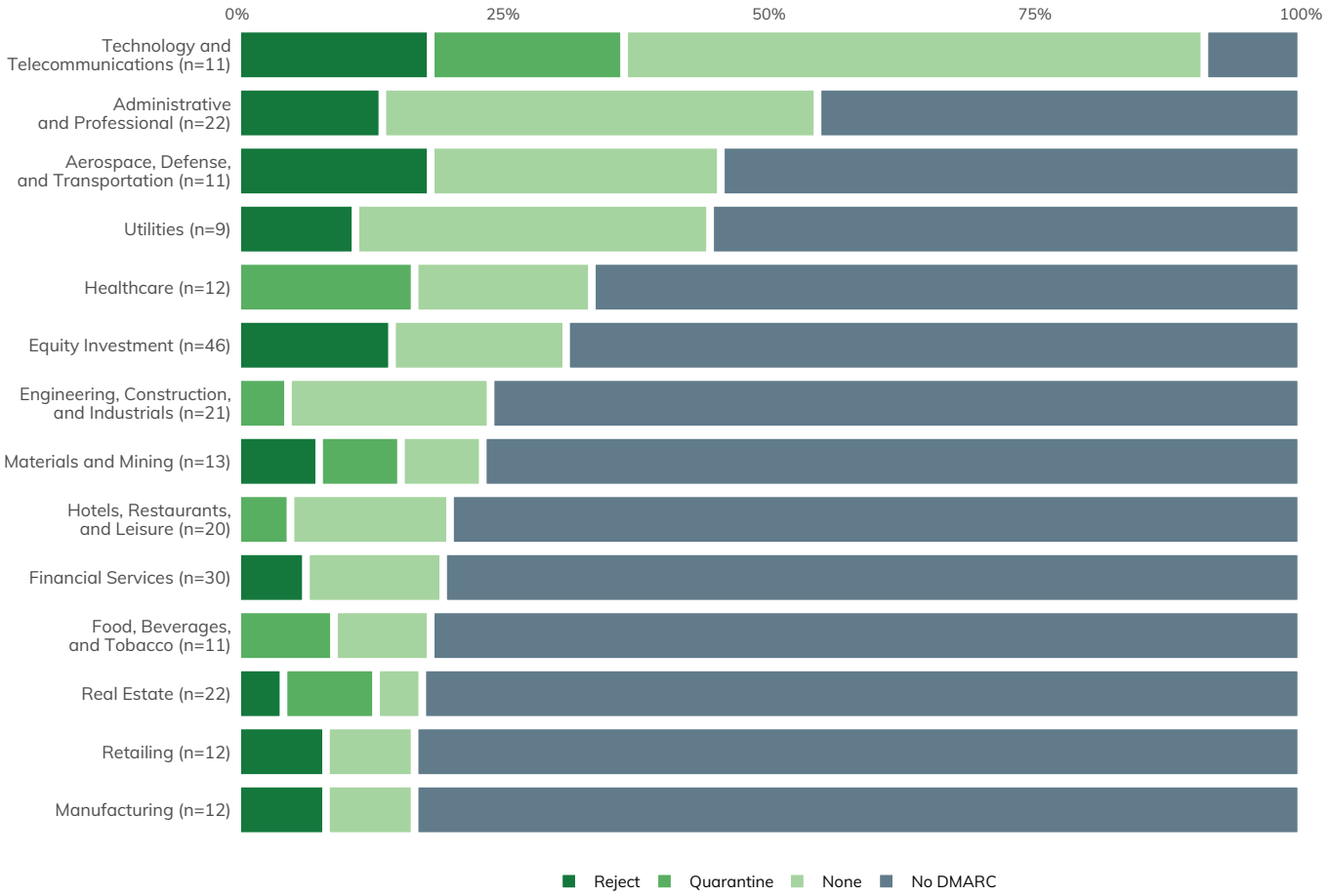
Phishing remains one of the most common cyber-attack vectors corporations face today. The Anti-Phishing Working Group (APWG), a cross-industry phishing watchdog group, collected a record-breaking quarter-million phishing reports in the third quarter of 2018.[5] Unfortunately, most organisations in the FTSE 250+ have not implemented a modern safeguard against phishing attacks.

As noted in the **Methodology** section (pg. 27), DNS records expose a means to identify how well an organisation has configured its email service for protection from spam and phishing through the analysis of Domain-based Message Authentication, Reporting and Conformance (DMARC) records.[6] DMARC enables organisations to:

- Signal that they are using email authentication to prove emails are not forged;
- Provide an email address to gather feedback about messages using their domain, legitimate or not; and
- Apply a policy to messages that fail authentication (one of "`none`", "`quarantine`", or "`reject`").

No DMARC records—or a DMARC record of "`none`"—means this first-line-of-defence protection from spam or phishing attacks is absent. However, a "`none`" record may be a signal that an organisation is on the path to email safety and is in the process of validating its DMARC configuration before enabling more active email defence measures.

**Figure 2: Email Safety Status of FTSE 250+ Primary Email Domains**




[5] Phishing Activity Trends Report, http://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf (Last accessed May 21, 2019)

[6] DMARC, https://dmarc.org (Last accessed May 21, 2019)

Properly configured DMARC records with "`quarantine`" or "`reject`" have active email defence measures in place. Figure 2 shows the percentage of DMARC adoption (by configuration category) of FTSE 250+ organisations within a given sector. Green indicates that organisations within that sector have either fully adopted and implemented DMARC or are on the path toward DMARC adoption. Unfortunately, the results indicate that the vast majority (70%) of the FTSE 250+ have not embraced modern email safety configurations, boosting their risk of phishing attacks. Several industry sectors have no organisations with DMARC configured to "`quarantine`" or "`reject`".

Since there is no direct scanning involved, DNS records are not impacted by the Project Sonar opt-out blacklist (described in the next section). Therefore, we can paint a more complete picture of the email safety configurations of the entire FTSE 250+ than we can with active scanning for vulnerable services. The **Further Work** section (pg. 31) outlines additional steps that can be used to increase the scope of the examination in order to paint a wider picture of email safety.

### Recommendation: Implement DMARC

DMARC controls have been available for several years and are supported by virtually all major email providers. Originally deployed as a mitigation against phishing attacks that target a company's external customers, DMARC also has the added benefit of making it much more difficult to spoof internal email addresses. Planning and deploying a properly restrictive DMARC configuration takes time[7], which is reflected in the three DMARC policy levels, but it's a time investment that can vastly improve a company's internal and external email security posture.

## Lack of SSL/TLS

The configuration of SSL/TLS has not been a factor in previous ICERs, as the organisations that made up the corpora for each of those studies all had primary web server configurations that ensured sessions were automatically upgraded to use SSL/TLS (i.e., "HTTPS") if the initial connection was made over plaintext HTTP.

Unfortunately, nearly 17% (42) of FTSE 250+ organisations do not auto-upgrade HTTP requests to HTTPS, which leaves visitors wide open to a vast array of person-in-the-middle attacks.[8] This is even more surprising since—at the time of publication—GDPR[9] still applied to all of these organisations.

### Recommendation: Enable HTTPS

This is an egregious configuration oversight that all impacted FTSE 250+ members should strive to remediate as soon as possible. HTTPS is the industry standard for all well-known domains, with some browsers labeling the cleartext HTTP protocol as "not secure."

## Evidence of System Compromise

Much of the data gathered for this report is through active scanning and DNS queries, but Rapid7 also maintains a global passive sensor network, Project Heisenberg.[10] The Heisenberg sensor network is described in detail in the **Methodology** section (pg. 27), but in short, the network is a collection of honeypots with unadvertised services such as HTTP/HTTPS, Telnet, SMB, and so on, where no legitimate internet traffic should be expected. Figure 3 shows the unique, daily connections with the Heisenberg sensor network for all organisations in a given sector. Ideally, this chart should be blank. However, the chart shows lapses in control across every sector in this data set.

[7] At CyberUK 2019, the UK's NCSC indicated that it can easily take up to 18 months to go from "No DMARC" to "reject" for organisations with complex or diverse email communications operations.

[8] Man-in-the-Middle (MITM) Attacks, https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/ (Last accessed May 21, 2019)

[9] General Data Protection Regulation (GDPR), https://www.rapid7.com/fundamentals/gdpr/ (Last accessed May 21, 2019)

[10] Rapid7 Project Heisenberg, https://www.rapid7.com/research/project-heisenberg/ (Last accessed May 21, 2019)

Figure 3: Daily Time Series of Unique Connections to Project Heisenberg

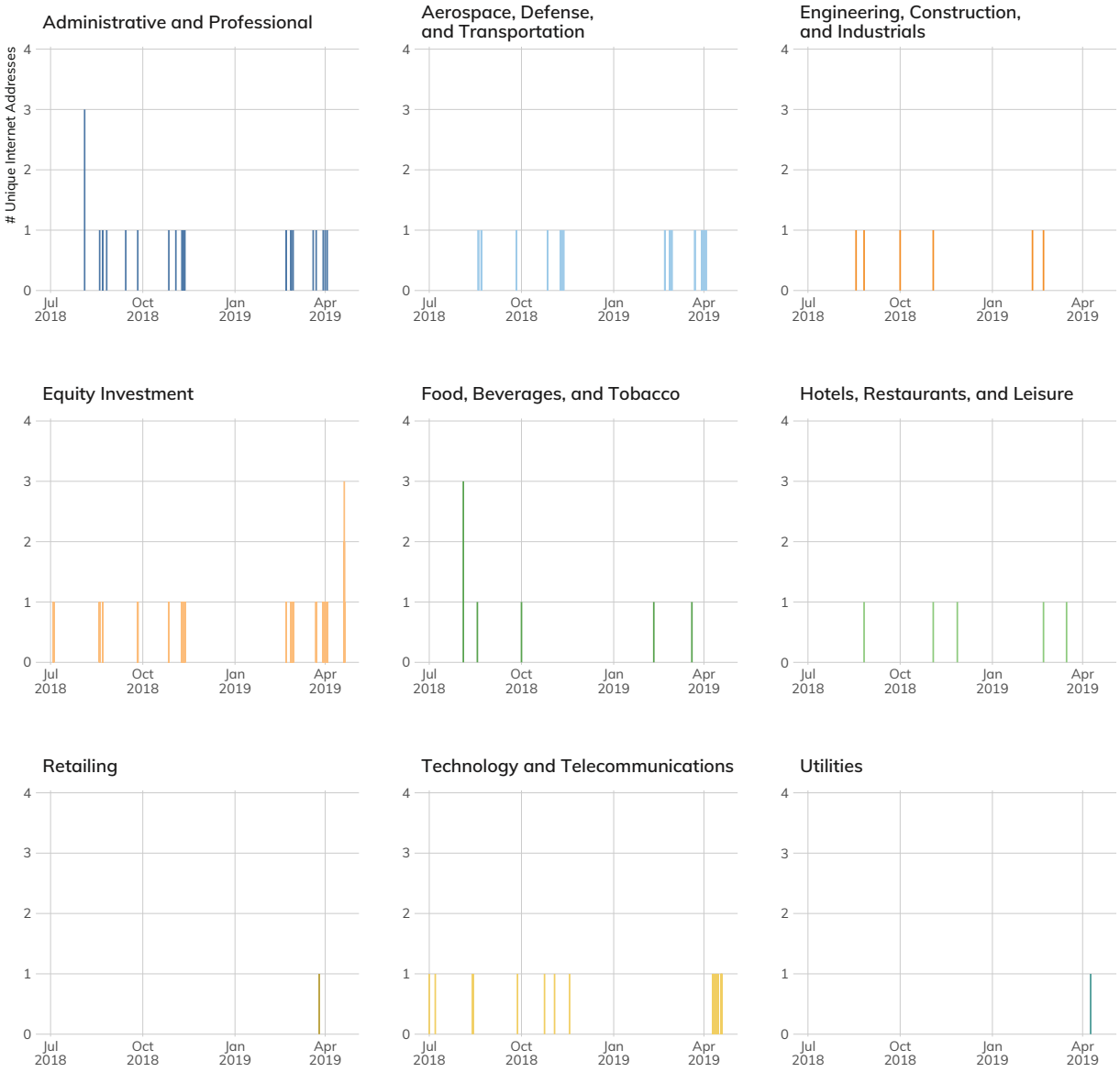
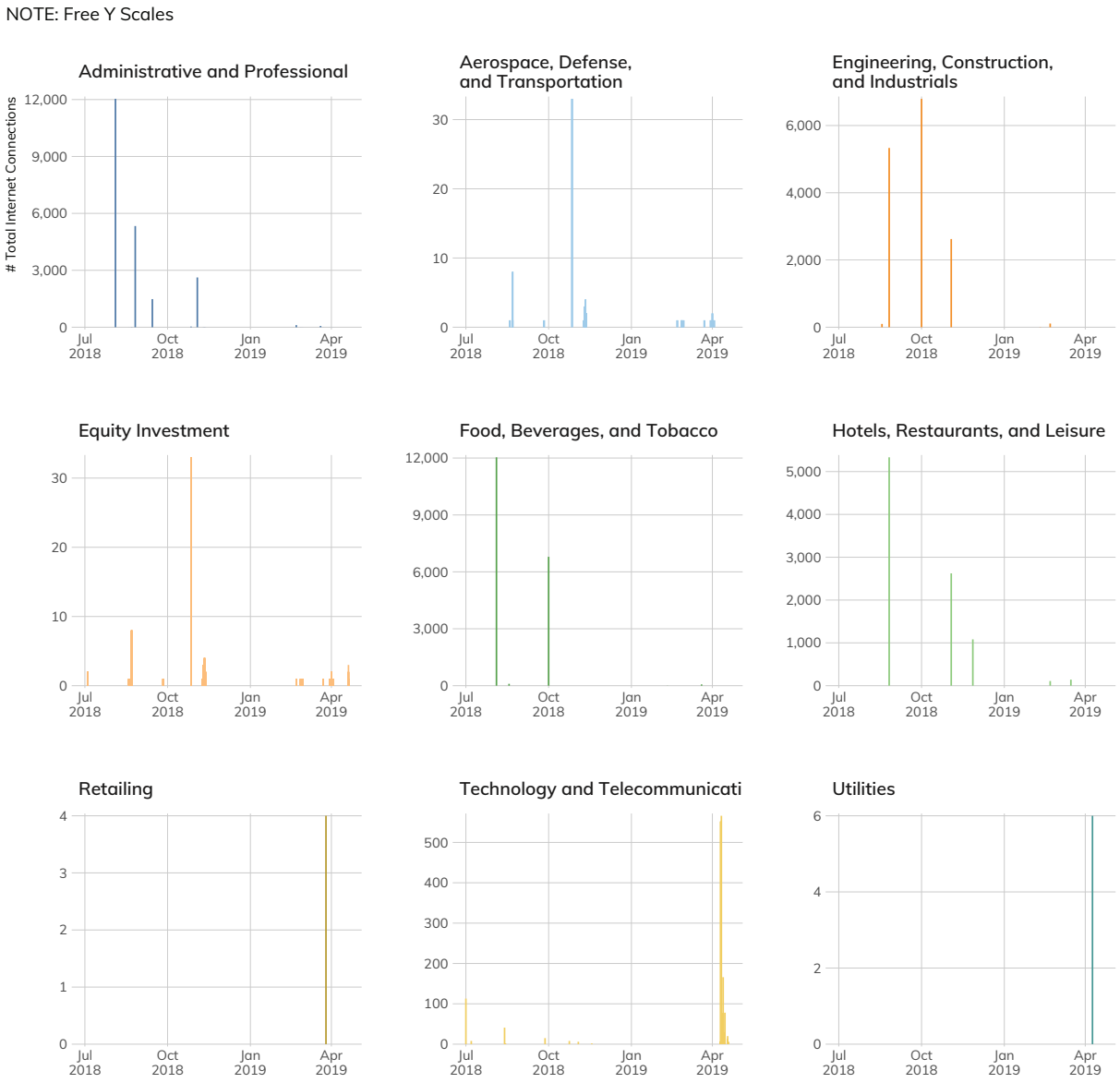


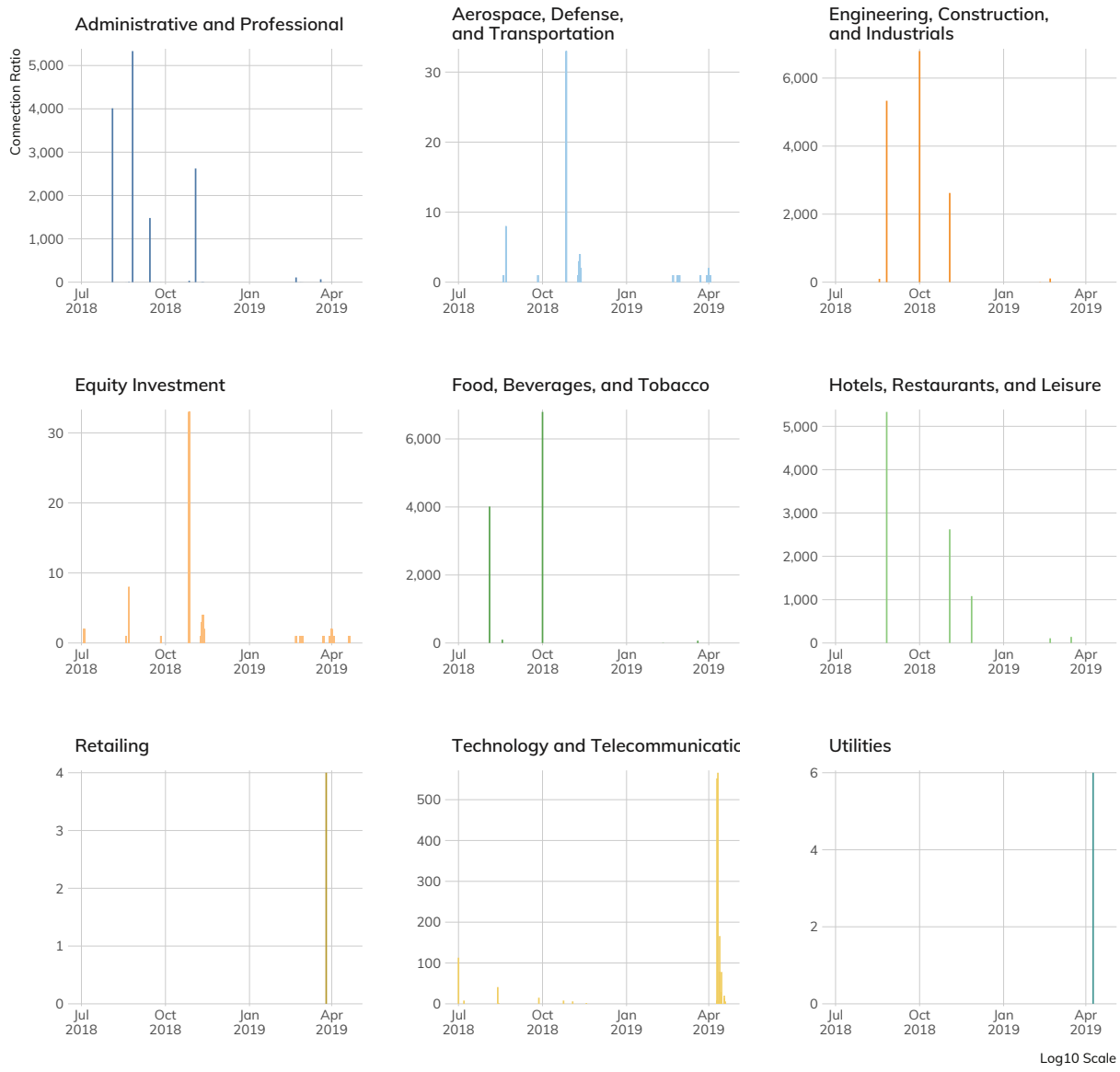

Figure 3 is handy to show presence, but we need another view to show volume. In contrast to the unique connection footprint view, Figure 4 shows the total daily connections to Project Heisenberg across organisations in the measured industry sectors. Note that the Y-axis is not uniform across the panels. This freescale lets us "zoom in" on each industry and more easily distinguish potential patterns and problems. We see that just because an industry has a small number of unique nodes connecting to Heisenberg sensors does not mean they are inactive. Larger volumes in this view could indicate a mass malware infection internal to an organisation (i.e., dozens, hundreds, or thousands of infected systems reaching out to the internet) or may be indicative of a few systems being co-opted into DoS campaigns.

**Figure 4: Daily Time Series of Total Connections to Project Heisenberg**




To further compare industries, we can combine the data from the previous two charts to complete the macro-exposure picture. Figure 5 shows the distribution of connection ratios (total connections in a day / unique sources in a day) by industry sector. Sectors with a greater number of points have organisations with more frequent gaps in configuration control or malware containment. Sectors with points further out on the axis also have gaps in monitoring as well as containment.

Figure 5: 2018 Heisenberg Connection Ratios

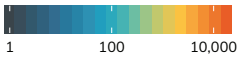



Some connections are more serious than others, and four of the top connection types to Heisenberg from organisations in this study are especially bad. As Figure 6 shows, throughout the first half of 2018, Heisenberg recorded daily connections that indicate multiple organisations were impacted by the following:

- Malware associated with SMB (i.e., WannaCry, WannaMine, and NotPetya);
- DNS DoS attacks;
- Mail access brute-forcing;
- Telnet/FTP/IMAP/LDAP cleartext credential brute-forcing; and
- SSH encrypted credential brute-forcing.

Figure 6: Signs of Malicious Activity per Sector

Total attacks by identified service (log10 scale)





## Recommendation: Keep an Eye on Egress Filters

Some level of honeypot traffic is to be expected; after all, the modern internet has plenty of opportunistic attackers seeking out low-hanging fruit. In the case of the observed misdirected traffic, networking mistakes can and do happen. With that said, traffic that is unambiguously sourced from the FTSE 250+ speaks to a lack of egress filtering from these organisations. Network administrators are accustomed to making sure connectivity is both smooth and uninterrupted and fixing things when connections fail. On the reverse side, though, their job is to also prevent errant and malicious traffic from leaving their domains. Outbound traffic rules should be regularly audited and tested, both from the data center and from deep inside the LAN, to ensure that a misconfiguration doesn't result in an accidental self-breach.

## Third-Party Risk Exposure

There is no question that the internet has become the backbone of international commerce in virtually every industry and locale. This interconnectedness means no organisation is an island, and it is a central reason why it is almost impossible to have a website, business process, or digital storefront without relying on some outside party. As a firm's digital footprint expands, the more the details of these third-party dependencies leak out through necessarily exposed metadata required to keep these services connected and operating smoothly.

An unfortunate result of this is that every organisation in the FTSE 250+ is vulnerable to targeted phishing attacks based on the third-party service metadata they expose in their DNS records. In addition, every FTSE 250+ organisation places itself and its website visitors at risk due to reliance on improperly configured third-party web services, with only five primary websites providing even a thin layer of third-party protection through the use of content security policies.[11]

When an organisation uses third-party resources to supplement its online assets, it takes on risks associated with those third-party resources. Vulnerable third-party resources can be used as a conduit to attack the first-party organisation. For example, in September 2018, security researchers noted that many sites are vulnerable to web-based credit card-skimming attacks due to their reliance on third-party content delivery networks (CDNs).[12] In another example, the Syrian Electronic Army used a compromised CDN in 2015 to take over a major news media outlet's web presence and use it to send custom push notifications to readers.[13]

For the purposes of this study, "third-party risk" exposure is defined as being present either when:

- A measured organisation is seen to be relying on resources from a third-party site when building its own websites and applications; or
- A measured organisation exposes which third-party services it actively uses by leaving potentially sensitive artifacts in its published metadata.

The **Methodology** section (pg. 27) outlines how attributes of third-party risk are collected and analysed. Figure 7 shows the breakdown by general categories of resource: advertising-oriented, site analytics, sourced from a CDN, or incorporating code from social network sites such as Facebook and Twitter.

In Figure 7, heatmap cells are coloured by an index score in which the number of discovered third-party resources in that sector is divided by the total number of industries in that sector. This normalises the amount so that over-represented sectors (such as Equity Investment) aren't being penalised for having more representation in the FTSE 250+ list. The number on top represents the number of resources, and the parenthetical value is the index score.

Some of these third-party services are likely resilient to cyber-attacks and do not meaningfully contribute to the first-party organisation's degree of exposure. For example, it is unlikely that Google would be sufficiently breached as to be an unwitting conduit for malicious activity to client organisations. However, widespread common exposure for third-party services such as DoubleClick—which has regular occurrences of malicious ads in its network—does increase the shared risk across the sectors.

[11] Content Security Policies, https://content-security-policy.com/ (Last accessed May 21, 2019)

[12] Kevin Beaumont, "Magecart—new tactics leading to massive unreported fraud," DoublePulsar, Sept. 19, 2018, https://doublepulsar.com/magecart-new-tactics-leading-to-massive-unreported-fraud-5211c9883dea (Last accessed May 21, 2019)

[13] Thu Pham, "Malicious Hackers Take Over Media Sites via Content Delivery Network Providers," Duo Security, May 19, 2015, https://duo.com/blog/malicious-hackers-take-over-media-sites-via-content-delivery-providers (Last accessed May 21, 2019)

## Figure 7: Third-Party JavaScript Execution by Industry and Service Type

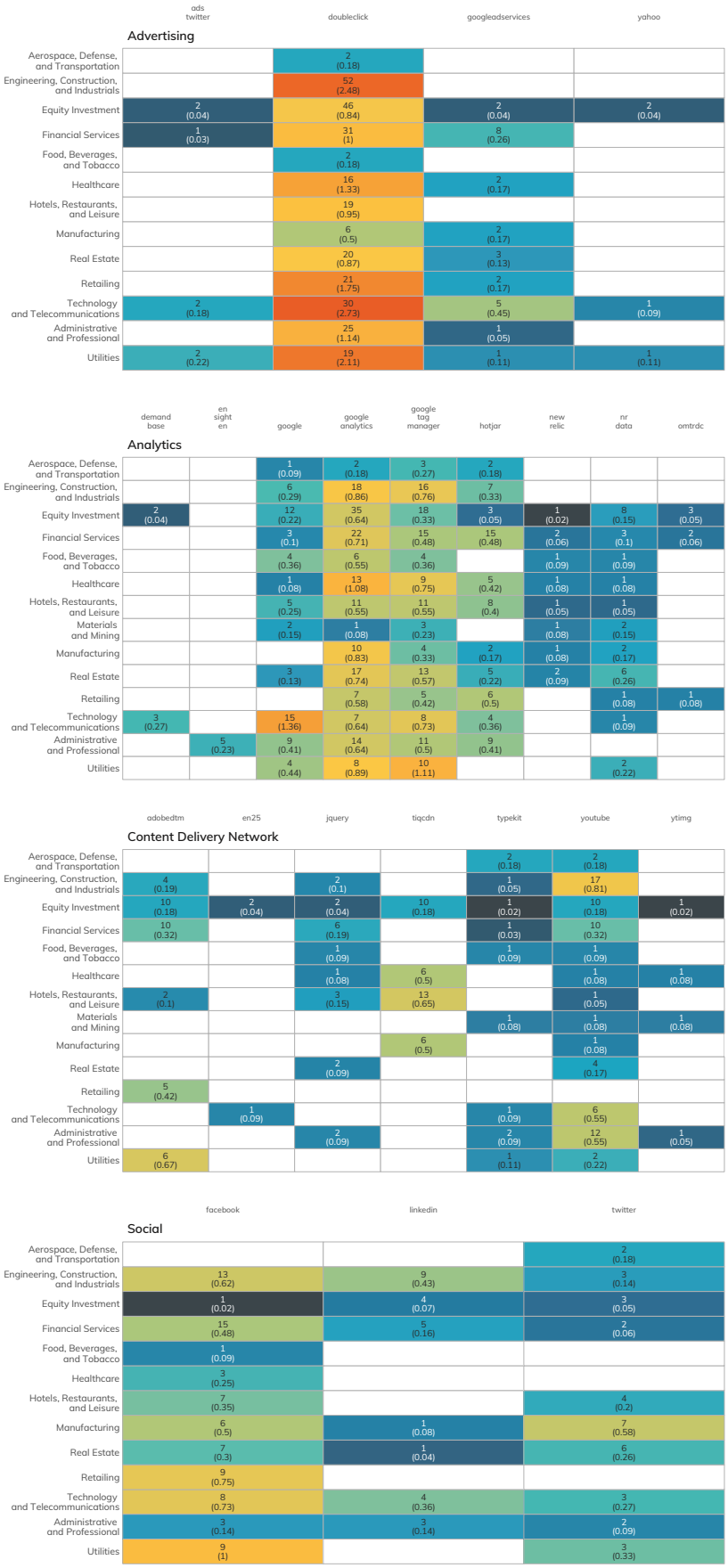


Figure 8 focuses attention on the latter component of third-party exposure: detecting the use of vendor applications/cloud services.

**Figure 8: Third-Party App/Cloud Usage Exposure via DNS Metadata**

| | Adobe | Atlassian | Cisco | Docusign | Dropbox | Facebook | Global Sign | Google Apps | HIBP | Office 365 |
|---|---|---|---|---|---|---|---|---|---|---|
| Aerospace, Defense, and Transportation | | 2 (0.18) | 2 (0.18) | | | | | 5 (0.45) | | 8 (0.73) |
| Administrative and Professional | | 3 (0.14) | | 2 (0.09) | | 2 (0.09) | 5 (0.23) | 10 (0.45) | 2 (0.09) | 18 (0.82) |
| Engineering, Construction, and Industrials | | | | | | 1 (0.05) | 2 (0.1) | 4 (0.19) | | 15 (0.71) |
| Equity Investment | 14 (0.25) | 3 (0.05) | | 15 (0.27) | | 3 (0.05) | 4 (0.07) | 9 (0.16) | 1 (0.02) | 33 (0.6) |
| Financial Services | 4 (0.13) | 1 (0.03) | | | 1 (0.03) | 4 (0.13) | 4 (0.13) | 10 (0.32) | 1 (0.03) | 23 (0.74) |
| Food, Beverages, and Tobacco | | 1 (0.09) | | 1 (0.09) | | 1 (0.09) | 2 (0.18) | 4 (0.36) | | 8 (0.73) |
| Healthcare | | 1 (0.08) | | 1 (0.08) | | 1 (0.08) | 1 (0.08) | 1 (0.08) | 1 (0.08) | 9 (0.75) |
| Hotels, Restaurants, and Leisure | 3 (0.15) | 4 (0.2) | 2 (0.1) | | | 1 (0.05) | 6 (0.3) | 12 (0.6) | 2 (0.1) | 16 (0.8) |
| Materials and Mining | 1 (0.08) | | | | | | | 1 (0.08) | | 4 (0.31) |
| Manufacturing | 1 (0.08) | | | | | | | 2 (0.17) | | 4 (0.33) |
| Real Estate | 1 (0.04) | 2 (0.09) | | | 1 (0.04) | 1 (0.04) | 2 (0.09) | 5 (0.22) | | 16 (0.7) |
| Retailing | 1 (0.08) | 1 (0.08) | | | 1 (0.08) | 1 (0.08) | 3 (0.25) | 8 (0.67) | | 6 (0.5) |
| Utilities | 2 (0.22) | | | | | 1 (0.11) | 3 (0.33) | 4 (0.44) | | 7 (0.78) |
| Technology and Telecommunications | 1 (0.09) | 2 (0.18) | 1 (0.09) | | | 2 (0.18) | 2 (0.18) | 7 (0.64) | | 10 (0.91) |

In addition to providing the connection address for names such as <www.rapid7.com>, DNS records can identify secure email configurations, as detailed in the **Phishing Defence Capabilities** section (pg. 8). DNS records can also reveal which third-party providers an organisation uses for everything from application development to cloud hosting environments to file-sharing and more.

One way these services are exposed is through the use of verification information stored in free-form TXT records. To illustrate, Table 1 shows a sample of DNS TXT records for rapid7.com:

Table 1: Rapid7 DNS TXT Records Sample

| DNS RECORD KEY | DNS TXT RECORD VALUE |
|---|---|
| rapid7.com. | smartsheet-site-validation.rapi d7.com=wfJFw8OnJ0WwBCBDP7NuqH |
| rapid7.com. | MS=ms93061892 |
| rapid7.com. | atlassian-domain-verification=+ Mx+hFjC77glTvA7K9Tp/5x7LvbyawRYOe ZpkXhE/Xys/xciI66aaIgyQQAD88E7 |
| rapid7.com. | citrix-verification-code=3d0b36 42-a1b3-4cf3-8616-c9fb8cd0c2da |

- "**smartsheet-site-validation**" signals that Rapid7 uses SmartSheet, a cloud spreadsheet service.
- "**atlassian-domain-verification**" signals that Rapid7 uses cloud-based services by Atlassian, a provider of popular software development tools and platforms.
- "**citrix-verification-code**" signals that Rapid7 uses services offered by Citrix.

Rapid7 researchers used Project Sonar DNS collection data to examine the TXT records of the FTSE 250+ organisations in this study. Only well-known domain names were used (expanding on this effort to use additional domains is covered in the **Further Work** section (pg. 31)), and Figure 8 only focuses on the most prevalent or well-known third-party services.

It may come as no surprise that every industry sector uses Microsoft Office 365, and it is highly unlikely that Microsoft is going to fall prey to a non-nation-state attack that would enable Office 365 to be a malicious gateway into organisations. There is a high prevalence of Google Apps across the FTSE 250+ as well, plus a fairly well-populated use of all the other resources of interest. It is worth mentioning that this is the first ICER corpus where more than one organisation was keen enough to utilise the Have I Been Pwnd (HIBP)[14] service, which provides visibility into stolen credentials potentially in use by employees of an organisation. Taking an interest in this service is a sign of potential improved security maturity in these organisations, provided they are using it as part of regular incident response workflows.

If organisations begin to stray from established and resilient service providers, they boost their risk of successful phishing and other types of attacks by observant, capable attackers who simply need to make a handful of DNS queries to create a list of targets.

## Recommendation: Reduce Third-Party Risk Exposure

These findings may not seem like major risks when reviewed individually. In truth, many of these "validation" records are only required once and can be removed after the initial validation has occurred. These records prove that one is the true owner of a given domain since in theory, only the true owner can add, modify, or delete DNS entries. If one were to look at those records in aggregate, it might be possible to find a common, shared third-party service in use by a large number of organisations or a boutique service provider used by only a handful of organisations. These may be high-value targets for malicious actors that seek to compromise multiple organisations, making resiliency of these third-party services all the more important.

[14] HIBP, https://haveibeenpwned.com/ (Last accessed May 21, 2019)

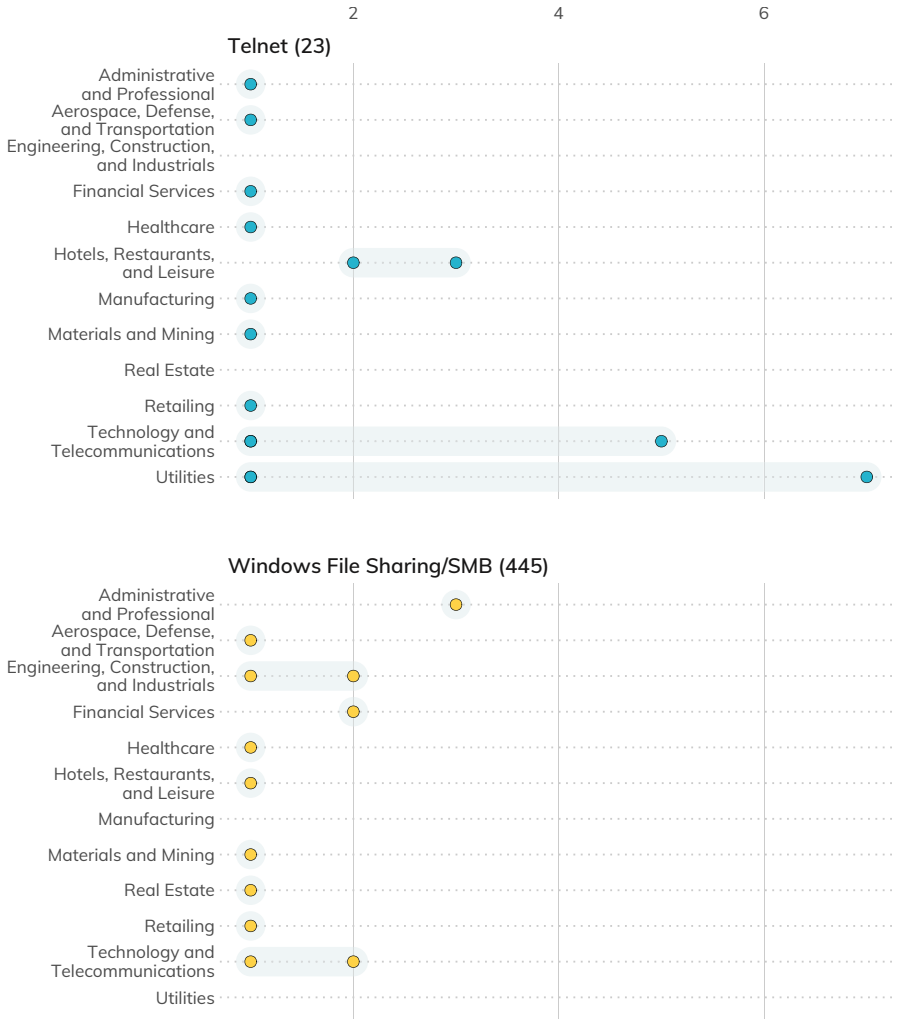
## Inappropriate Services: SMB and Telnet

The type of service being exposed has a direct impact on the severity of exposure (i.e., some services are less "safe" than others). Figure 9 shows that organisations in the FTSE 250+ are not immune to attacks that target these two critically vulnerable services: Telnet and Windows file-sharing.

One service in particular, Server Message Block (SMB), is one of the most dangerous services for a system to expose. SMB is an all-in-one file-sharing and remote administration protocol, usually associated with Windows, that has been an attractive target for attackers and researchers alike for decades. MS03-049 in 2003, MS08-067 (Conficker) in 2008, and MS17-010 (EternalBlue) in 2017 all arose from the complexity of this protocol and its central nature to Windows networking.[15] Recently, vulnerabilities in the SMB service were at the heart of the WannaCry and NotPetya attacks, which crippled networks and caused significant outages to critical business processes that cost many companies millions of dollars in lost revenue.[16]

**Figure 9: Distribution of Organisations Exposing Telnet/Windows File-Sharing (SMB) Services**

**Each dot represents one organisation; position on axis = number assets discovered.**




Telnet exposure creates risks similar to SMB exposure. Telnet dates back to the early days of the internet, with the official "modern" standard dating back to 1983.[17] Telnet is a cleartext protocol that is used to directly log in to servers and network equipment, usually to issue commands and run scripts directly at the operating system level of the device. Telnet services have a history of vulnerabilities and exposures that put organisations at risk of credential theft, passive and active eavesdropping, and remote code execution. The cleartext nature of the protocol means that an attacker in the proper network position can read any usernames, passwords, or data being transmitted—and endpoints with weak, default, or eavesdropped passwords can be hijacked to run malicious code directly by the operating system.

The singular positive takeaway is that most sectors have only one member organisation exposing Telnet or SMB. While a total absence of Telnet and SMB on today's internet would be ideal, the FTSE 250+ has far less SMB/Telnet exposure, both in absolute and relative terms, than the Fortune 500.[18]

[15] Rapid7, National Exposure Index 2018, "Inappropriate Services," pg. 14, Jun. 7, 2018, https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf (Last accessed May 21, 2019)

[16] Bob Rudis, "No More Tears? WannaCry, One Year Later," Rapid7, May 14, 2018, https://blog.rapid7.com/2018/05/14/no-more-tears-wannacry (Last accessed May 21, 2019)

[17] J. Postel and J. Reynolds, Telnet Protocol Specification, Internet Engineering Task Force, May 1983, https://tools.ietf.org/html/rfc854 (Last accessed May 21, 2019)

[18] Rapid7, Industry Cyber-Exposure Report: Fortune 500, pgs. 13–14, Dec. 11, 2018, https://www.rapid7.com/info/industry-cyber-exposure-report-fortune-500 (Last accessed May 21, 2019)

### Recommendation: Eliminate Public-Facing SMB and Telnet

Though the presence of these services—especially Windows SMB— is extremely small among FTSE 250+ organisations, there is no safe way to expose SMB services to the public internet. In light of this, Microsoft has made efforts to reduce SMB exposure for normal desktop and laptop clients. For example, current Microsoft documentation explicitly recommends blocking SMB on an internet perimeter firewall, and Windows 10 desktops automatically firewall access to port 445 by default.[19] Even exposing one asset with SMB running could end up spreading (or re-spreading) WannaCry, NotPetya, or modern variants across an entire organisation.

There is also no technical or practical justification for running a Telnet service today. It has been superseded by the Secure Shell (SSH) Transport Layer Protocol, which provides encryption-in-transport and encourages the use of digital certificates when authenticating connections.[20] If a device is truly incapable of running SSH rather than Telnet due to a lack of local computing resources, that device is simply too insecure by design to expose to the public internet, regardless of the reasoning for staying with a 40-year-old un-encryptable protocol. Of note, not close to half (80) of the FTSE 250+ expose SSH services without exposing any Telnet services, so it seems there has been some acknowledgement of the strengths of this protocol.

## Older, Unpatched Web Service Exposure

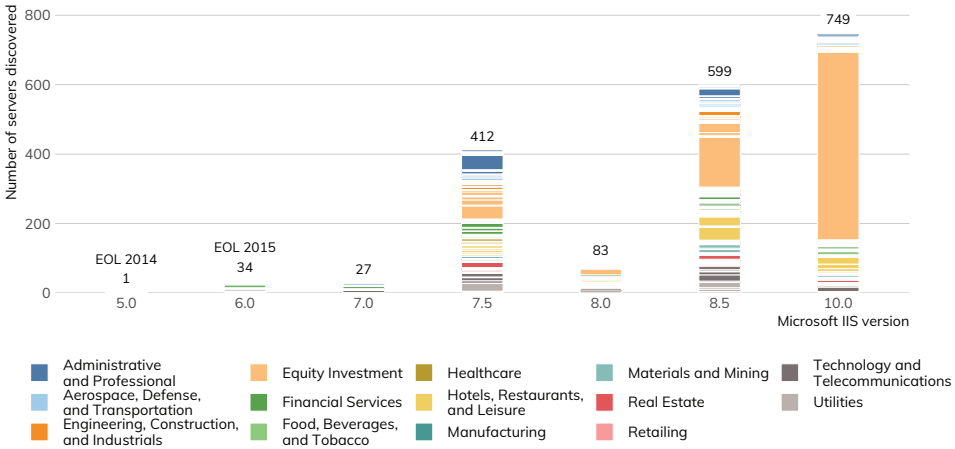
Keeping internet services configured, patched, and running supported versions of operating systems and internet-facing applications can go a long way toward thwarting attackers. Failure to use updated software versions puts organisations at greater risk of attack through known vulnerabilities. Unfortunately, most organisations in the FTSE 250+ are running older and often unsupported versions of the three most prolific web servers: Microsoft's Internet Information Services (IIS), Apache HTTPD, and nginx.

### Microsoft IIS

Microsoft's IIS was the second most popular web server on the internet in February 2019, according to Netcraft.[21] This is no surprise, as IIS is usually found in enterprise settings due to software licensing agreements and large organisations' continued reliance on Microsoft technologies. Figure 10 shows Project Sonar discovered 1,905 IIS servers with attributable version numbers in 194 organisations spanning all 14 FTSE sectors.

**Figure 10: Microsoft IIS Version Distribution**

**Each coloured segment represents a different organisation**




[19] Microsoft, Guidelines for blocking specific firewall ports to prevent SMB traffic from leaving the corporate environment, Aug. 31, 2016, https://support.microsoft.com/en-us/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic (Last accessed May 21, 2019)

[20] T. Ylonen and C. Lonvick, The Secure Shell (SSH) Transport Layer Protocol, The Internet Society, January 2006, https://tools.ietf.org/html/rfc4253 (Last accessed May 21, 2019)

[21] Netcraft March 2019 Web Server Survey, https://news.netcraft.com/archives/2019/02/28/february-2019-web-server-survey.html (Last accessed May 21, 2019)

Table 2 shows 28% of FTSE 250+ organisations maintain a single version of IIS, with nearly 25% running over three separate versions. This version diversity and the discovery of end-of-life IIS versions increases defence and management complexity and further increases the likelihood of down-version IIS servers becoming an intrusion conduit for attackers.

**Table 2: FTSE 250+ Microsoft IIS Version Diversity**

| NUMBER OF IIS VERSIONS MAINTAINED | NUMBER OF ORGANISATIONS | PERCENTAGE OF FTSE 250+ |
|---|---|---|
| 1 | 72 | 28% |
| 2 | 64 | 26% |
| 3 | 37 | 14% |
| 4 | 12 | 4% |
| 5 | 9 | 4% |

## Apache HTTPD

The web server version picture is a bit more complex when we look at Apache. Figure 11 shows that Project Sonar discovered 549 attributed Apache servers with 37 distinct version numbers in 84 organisations spanning all 14 FTSE sectors. Table 3 shows a majority of organisations only expose a single version of Apache HTTPD, but nearly 8% of them expose three or more distinct versions—which, again, increases the management complexity.

**Figure 11: Apache HTTPD Version Distribution**

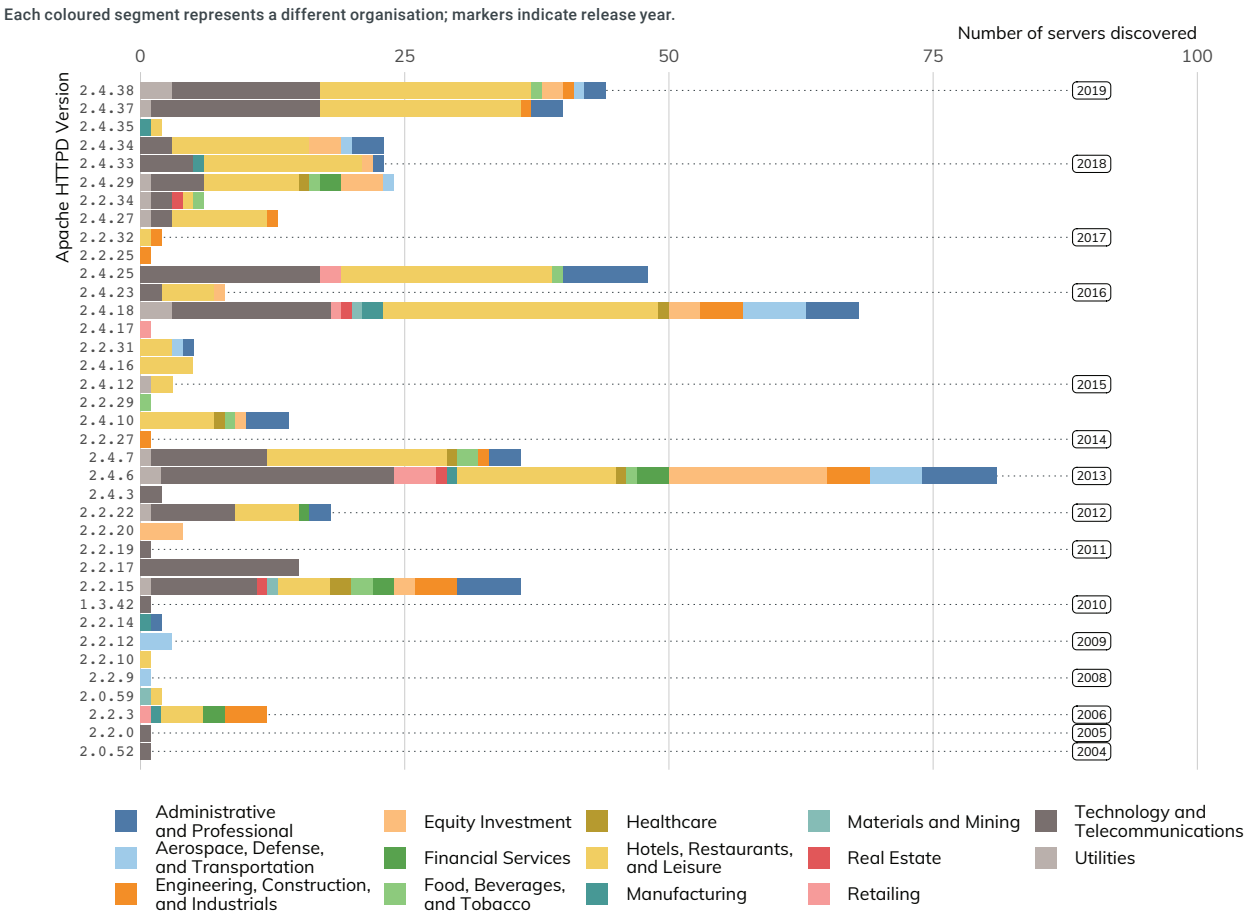


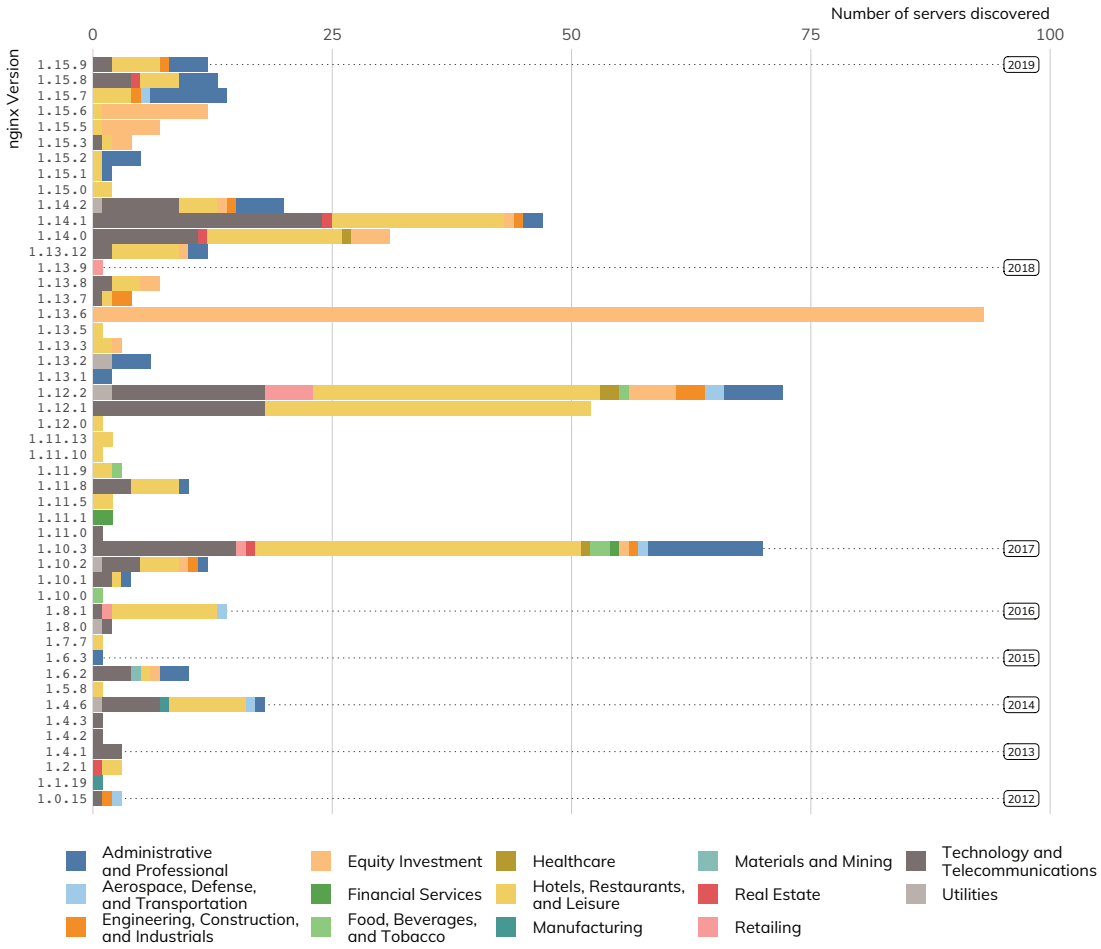
Table 3: FTSE 250+ Apache HTTPD Version Diversity

| NUMBER OF APACHE HTTPD VERSIONS MAINTAINED | NUMBER OF ORGANISATIONS | PERCENTAGE OF FTSE 250+ |
|---|---|---|
| 1 | 47 | 18% |
| 2 | 18 | 8% |
| 3 | 7 | 2% |
| 4 | 2 | <1% |
| 5 | 1 | <1% |
| 6 | 2 | <1% |
| 7 | 3 | 2% |
| 9 | 1 | <1% |
| 10 | 1 | <1% |
| 13 | 1 | <1% |
| 17 | 1 | <1% |

While the software version diversity alone is disconcerting, the fact that most discovered versions are well over a year old is an indicator organisations aren't keeping Apache installations up-to-date. Unlike IIS, organisations must use a third-party vulnerability management tool to catalog and identify the version and patch levels of Apache servers. The Apache Foundation regularly releases new versions to add features, fix problems, and patch security issues. Also, because Apache HTTPD is open source, attackers have full access to the source code and can more easily discover flaws and develop exploits.

Figure 12: nginx Version Distribution

Each coloured segment represents a different organisation; markers indicate release year.




## nginx

The nginx web server may come in third in the February 2019 Netcraft survey, but it's No. 1 for the number of distinct versions Project Sonar discovered among the FTSE 250+ (48). Figure 12 shows that 590 nginx servers were found in 66 organisations spanning all 14 FTSE sectors.

Table 4 is similar to the Apache findings, with many organisations running a single version but far too many running three or more.

Table 4: FTSE 250+ nginx Version Diversity

| NUMBER OF NGINX VERSIONS MAINTAINED | NUMBER OF ORGANISATIONS | PERCENTAGE OF FTSE 250+ |
|---|---|---|
| 1 | 39 | 16% |
| 2 | 11 | 4% |
| 3 | 5 | 2% |
| 4 | 1 | <1% |
| 5 | 1 | <1% |
| 6 | 3 | 2% |
| 8 | 1 | <1% |
| 10 | 1 | <1% |
| 11 | 1 | <1% |
| 14 | 1 | <1% |
| 17 | 1 | <1% |
| 29 | 1 | <1% |

While one could argue that maintaining the security posture of multiple versions of a single web server platforms is well within the capabilities of mature operations teams, there are added complexities when more than one vendor's technology is in play. For the FTSE 250+, nearly half the organisations maintain two or more different internet-facing web server vendor technologies (Table 5). The combined vendor and version diversity substantially increases the risk of overlooking configuration weaknesses that potential attackers are more than ready to find and exploit.

Table 5: FTSE 250+ Combined Vendor Diversity

| NUMBER OF COMBINED VERSIONS MAINTAINED | NUMBER OF ORGANISATIONS | PERCENTAGE OF FTSE 250+ |
|---|---|---|
| 1 | 116 | 46% |
| 2 | 69 | 28% |
| 3 | 30 | 12% |

## Recommendation: Strive for Version Consistency

The need to patch and maintain servers may sound trivial and obvious, but scheduling change control and orchestrating outages of what may be core services can be a complex undertaking in large organisations. Though this task can be tedious, it's vital that organisations keep an up-to-date inventory of what they're exposing and work with their business and application teams to ensure they are using supported and patched versions of software.

# Conclusions

The methodology outlined in this report describes several ways, based on openly available internet connections, to measure the exposure of specific organisations and industry sectors to certain cybersecurity risks. To reiterate, while far from a complete picture of the organisations' overall cybersecurity posture, the results of this research indicate significant levels of exposure among FTSE 250+ companies:

- Companies in the FTSE 250+ expose an average of 35 servers/devices, with four companies exposing near or over 1,000 systems/devices. More systems equals more exposure to opportunistic and targeted attacks.
- An overwhelming majority (88%) of FTSE 250+ companies do not use enhanced email safety configurations, creating a greater risk of phishing attacks. To reduce exposure, organisations should evaluate and strengthen their DMARC configuration settings.
- FTSE 250+ organisations in every sector had serious issues with patch/version management of business-critical internet-facing systems. It is vital that organisations make configuration and patch management of internet-facing systems a top priority to avoid exploitation of known vulnerabilities in outdated software.
- Nearly 20% of FTSE 250+ organisations do not require the use of HTTPS on their primary domains, putting visitors at serious risk for person-in-the-middle attacks.
- Dozens of exposed third-party services are shared among the FTSE 250+ organisations, creating a greater risk that a vulnerability in a shared third party can lead to the compromise of multiple organisations. Organisations should ensure their third-party service providers are taking appropriate steps to strengthen their own security, as well as use tools such as subresource integrity signatures when sourcing these services to help reduce the likelihood of shared compromise.
- Critically weak services such as Telnet and Windows file-sharing had only a light presence in the FTSE 250+ corpus, but they were present. Each instance creates a greater risk of susceptibility to exploitation of SMB vulnerabilities. To reduce exposure, organisations should close port 445 whenever possible and migrate from Telnet to SSH.

Because FTSE 250+ organisations typically have substantial resources and access to excellent technical expertise, the findings suggest that the severity of exposure may be greater for the many thousands of organisations smaller than those in the FTSE 250+. The digital ecosystem could benefit from an ongoing conversation with key stakeholders on the reasons for this continued exposure, along with steps to mitigate the cybersecurity risks it poses.

# Measuring Industry Exposure: Methodology Overview

This report documents findings regarding organisations' exposure to certain cybersecurity risks using data made available through interactions with public-facing systems over the internet. That data was then used to quantify the exposure of members of the UK-based FTS 250 plus outliers, with results aggregated by industry sector. Measuring exposure at this level can help target cyber-risk reduction efforts, improve cybersecurity information-sharing within industry sectors, and build awareness of practices organisations can undertake to avoid future exposure.

Since 2016, Rapid7 has annually measured and reported on the exposure of specific countries to certain cybersecurity risks.[22] With this information, we engage country-level Computer Emergency Response Teams (CERTs) to analyse the exposure in more detail and support action to reduce their overt exposure of critical services. To generate these reports, Rapid7 uses our internet-wide scanning platform, Project Sonar,[23] and our passive sensor network, Project Heisenberg,[24] to determine whether online assets are advertising vulnerable internet services or making suspicious outbound connections. We then aggregate the results at the nation-state level.

Aggregating the exposure data at the nation-state level is relatively straightforward. We use high-quality, regularly updated databases that match country location to internet addresses, with over 98% accuracy.[25] However, it takes additional effort to measure exposure at a deeper level. More robust exposure measurement of specific organisations is possible by analysing the dedicated internet address space that those organisations own and use as part of their business operations. After matching organisations to internet addresses, exposure to certain cybersecurity risks can be quantified through publicly available data obtained with active scans and passive sensors. This section details the steps involved in the following:

- Attributing internet addresses and primary internet domain names to FTSE 250+ organisations;
- Using Project Sonar's active scan data to identify exposure to vulnerable services and systems within the internet address space attributed to these organisations;
- Enhancing this exposure measurement by identifying the frequency and nature of interactions from this attributed internet address space with Rapid7's Project Heisenberg global passive sensor network; and
- Supplementing these direct exposure measurement with inferred exposure. To do this, we analysed "metadata" from organisations' attributed internet address space, such as email "safety" configurations stored in internet DNS records, and detectable operating system and application version information.

The measurements can be broken down into three primary areas, each of which is covered in the following sections:

- **Inferential measurements** using public DNS records, the most significant of which is the measurement of an organisation's defences against phishing attacks;
- **Active measurements** using Rapid7's Project Sonar, which includes measuring both the presence of public-facing systems and services as well as the content those systems and services expose; and
- **Passive measurements** using Rapid7's Project Heisenberg, which records when systems from an organisation's network contact this honeypot collection and what actions they were trying to perform during these connections.

[22] Rapid7, National Exposure Index, June 7, 2018, https://www.rapid7.com/info/national-exposure-index (last accessed Feb. 12, 2019).

[23] Rapid7, Project Sonar, https://www.rapid7.com/research/project-sonar (last accessed Feb. 12, 2019).

[24] Rapid7, Project Heisenberg, https://www.rapid7.com/research/project-heisenberg (last accessed Feb. 12, 2019).

[25] MaxMind, https://www.maxmind.com (last accessed Feb. 12, 2019).

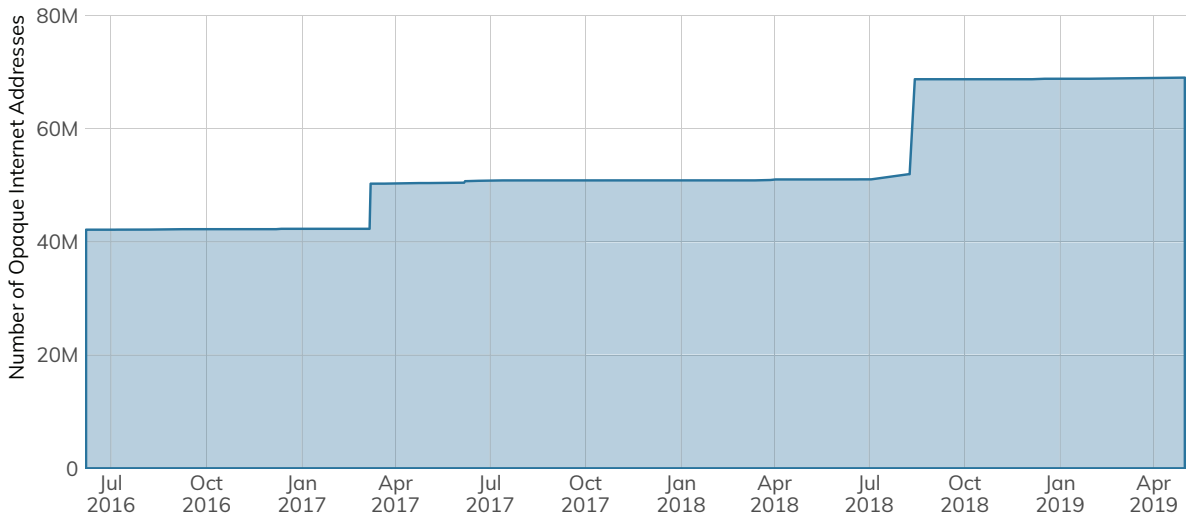
## Active Measurements with Project Sonar

Project Sonar scans the internet across a wide array of services. A "service" could mean a web server, mail server, file server, database server, network equipment, or even cameras, along with many other types of servers that listen for requests over the internet. When a service on a given internet address responds positively to a probe, the positive result is recorded along with the response data. Depending on the service being scanned, this response data can include detailed version and configuration information of the scanned service.

Rapid7 adheres to the legal restrictions associated with internet scanning. As a result, the probes performed by Project Sonar never involve the use of credentials, exploits for known vulnerabilities, or payloads that may cause harm to the service being probed, no matter how obvious or well-known those passwords or exploits may be. While this places some limits on what we can scan and the types of service metadata we can retrieve, we can still capture a wide array of useful information.

A further, self-imposed restriction comes as a result of Rapid7's "opt-out" process. Organisations may request that Rapid7 exempt specific internet address ranges from Project Sonar scans. Rapid7 obliges these requests and places the address range onto a blacklist that is restricted from the scanning process (Figure 13).

**Figure 13: Rapid7 Project Sonar Blacklist Growth**




Unlike the 2018 ICER for the Fortune 500 corpus, there were no networks present on the opt-out blacklist from any organisation in the Q1 2019 FTSE 250+ list.[26]

## Passive Measurements with Project Heisenberg

Rapid7's Project Heisenberg is, at heart, nearly 250 unadvertised systems hosting a variety of fake services, such as HTTP, SMB, SSH, and many others. These honeypots are closely monitored for unsolicited connections but do nothing to attract or entice those connections. Other than internet-wide scanning research, there are no legitimate reasons for an organisation to connect with the Heisenberg sensor network, so any recorded activity in Heisenberg is a high-quality indicator that an organisation does not have control of its outbound connections—which further suggests either malicious activity or misconfigured service traffic coming from the organisation. In essence, if there is any contact with Heisenberg, there is some type of exposure occurring in that organisation.

[26] Rapid7, Industry Cyber-Exposure Report: Fortune 500, pgs. 10–11, Dec. 11, 2018, https://www.rapid7.com/info/industry-cyber-exposure-report-fortune-500 (Last accessed May 21, 2019)

## Measuring Web Server Third-Party Risk

To get an idea of third-party risk when exposing web servers/service to the internet, we can examine the resources each web page loads when the page is loaded into a web browser. Project Sonar can perform this task at scale by controlling a virtual web browser, visiting the pages of the well-known domains of the organisations in the study, and capturing all the activity as each site loads resources.

These websites load a great quantity of third-party resources, so the complete list would be difficult to visualise and comprehend. The resultant list was pared down to only the most prevalent third-party resources used across the target study list.

# Further Work

The processes and procedures used for the exposure analyses in this report are the initial steps at communicating the overall "cyber-health" of industries based on a subset of possible internet telemetry measurements. Possible measurement deficiencies have been identified and will be addressed in this section.

## Improving Entity Internet Asset Attribution

The most common Internet Protocol (IP) address space (version 4, IPv4) is fully exhausted, meaning there are no "spare" blocks of IP addresses to assign an entity. However, organisations that currently do own IPv4 address space are not utilising said space to capacity. The scarcity of this finite resource has resulted in the creation of a marketplace in which IPv4 space can be bought and sold.[27] While some long-standing organisations have sold portions of their IPv4 address space blocks to other parties, some retain ownership and manage the leasing of this space to others on their own. This practice results in attribution errors, which are especially vexing when corporate address space is leased in a non-attributable way to third-party hosting providers and/or cloud providers.

For this report, Rapid7 researchers initially used a manual processes for both preliminary attribution attempts, as well as identification of attribution anomalies, by comparing address space utilisation and service composition with that of known hosting and cloud service providers. As noted in the **Methodology** section (pg. 27), this approach was enhanced using directly attributable resources from organisations' DNS records and inferring organisation-owned IPv4 space from these records. Further work will be performed to shore up IP space attribution and automate this classification, which will enable filtering out hosting and cloud service provider blocks at scale.

Note especially that this combination of RIPE-attributed owned IPv4 space and DNS record resource attribution approach differs from that of Rapid7's inaugural Fortune 500 ICER in 2018 and ASX 200 ICER in 2019.

## Avoiding Opt-Out Opacity

Research work like this report depends on continuous, light-touch scanning like the kind provided by Rapid7's Project Sonar, so if enough organisations decide to opt out of these scans, the internet research community will undoubtedly suffer. There are two future paths that can reduce the impact of the Project Sonar "opt-out" list opacity issue. As a responsible internet citizen, Rapid7 keeps the opt-out list process in place, but it may be possible to augment current processes and have the opt-out be an annual process whereby organisations may re-acknowledge their desire to have their IPv4 space remain on the opt-out list. This would provide an opportunity to restate the advantages of allowing Project Sonar scans, reduce the size of the opt-out list, and preserve the statistical integrity of the surveys.

The second path is to just expand the sample size to cover more industry participants regardless of where their headquarters are. To this end, there are other notable organisation lists—e.g., Inc. 5000, S&P 500, ASX 200—that can be mined to significantly expand the sample sizes in each industry and reduce the size of the opaque IPv4 address space to (perhaps) less than 1%. The previously noted attribution accuracy and expansion enhancements are key components to ensuring the validity and efficacy of this expansion process.

[27] IPv4 Brokers, ARIN IPv4 Market Prices & Transfer Statistics, https://ipv4brokers.net/arin-ipv4-prices-transfer-statistics/ (Last accessed May 21, 2019)

## Utilising More DNS Records

The email safety analyses utilised the well-known DNS domains of the organisations on the FTSE 250+ list. Most of those corporations have subsidiaries and brands, each with their own set of DNS domains and these brand-domains were used to enhance the coverage of the exposure analysis. Further work will be performed to develop a machine learning-based web-crawling and data-mining process to identify these additional domains and incorporate the data associated with them into the analysis framework used in this report.

## Expanding Resource Safety Evaluation

The further work to discover additional domain names will have a direct impact on the email safety analyses used for this report. Furthermore, this report only looked at one aspect of email safety, DMARC. There are additional resource records that describe other email safety configurations, such as Sender Policy Framework (SPF), which further helps reduce spam and prevents attackers from misusing email domains. This will be included in future analyses.

Other types of DNS records (i.e., non-email-related ones) also communicate other types of both exposure and safety. That information will also be explored for inclusion in future analyses.

## Third-Party Dependency/Risk Analyses

Finally, by analysing the overall configuration of an organisation's DNS records, discovering how an organisation's IPv4 networks are routed on the internet, enumerating which third-party resources an organisation relies upon in its web and web application services, and other indirect, public measurements, it is possible to report on both the potential fragility of an organisation's overall internet presence and provide exposure views of third-party dependencies across all organisations.

# Study Methodology

## Why the FTSE 250+

Aggregating exposure for specific UK industry sectors poses a unique problem. First, IP address space is fairly expansive. IPv4 alone supports over 4.2 billion addresses (a portion of which are not assignable), without taking into consideration the exponentially more massive IPv6 space. These addresses are assigned to various governments, companies, and service providers around the world. Second, with the onset of dynamic infrastructure (the cloud), it is increasingly common for companies to lease IP address space from other companies to host their services. This makes traditional methods of attributing IP addresses to particular organisations (such as by using the WHOIS lookup tool) incomplete, since the owner of the IP address may not be the owner of the service evaluated for exposure.

Instead of attributing IP addresses to companies and filtering by FTSE 250+ industries, we focus on the Q1 2019 FTSE 250+ as a representative sample, from which we attribute and filter global IP address space and services hosted on dynamic infrastructure.

The Q1 2019 FTSE 250+ list was chosen for many reasons. First, it is a diverse list (see Table 6) chosen using well-established criteria for selecting firms for inclusion. When revenues are combined, the composite list equates to approximately 12% of the UK GDP, with aggregate employment reaching over 10 million individuals globally. Furthermore, over 50% of these organisations are incorporated in the UK, enabling the creation of a UK-centric view of exposure and the development of potential economic impact models.

**Table 6: FTSE 250+ Constituents Summary**

| INDUSTRY SECTOR | NUMBER OF ORGANISATIONS |
|---|---|
| Administrative and Professional | 22 |
| Aerospace, Defence, and Transportation | 11 |
| Engineering, Construction, and Industrials | 21 |
| Equity Investment | 55 |
| Financial Services | 31 |
| Food, Beverages, and Tobacco | 11 |
| Healthcare | 12 |
| Hotels, Restaurants, and Leisure | 20 |
| Manufacturing | 12 |
| Materials and Mining | 13 |
| Real Estate | 23 |
| Retailing | 12 |
| Technology and Telecommunications | 11 |
| Utilities | 9 |

Constituents in this study that are not in the official FTSE 250 include:

**Table 7: ICER Organisations Not in Official FTSE 250**

| NAME OF ORGANISATION | ANNUAL REVENUE |
|---|---|
| Arla Foods | €10.3 billion |
| Associated British Foods | €1.54 billion |
| BMI Healthcare | €1 billion |
| British Gas | €31 billion |
| E.ON Group | €42 billion |
| EDF Energy | €9.2 billion |
| HCA Healthcare | €10 billion |
| Müller UK & Ireland | €2.1 billion |
| Nuffield Health | €1.04 billion |
| Ramsay Health (Forbes Global 2000 company) | €5.8 billion |
| Scottish Power | €5.9 billion |
| Spire Health | €1.07 billion |
| SSE | €33 billion |

Furthermore, JP Morgan and Fidelity Investments are parent firms for a total of nine members of the official FTSE 250 and have only been counted once in any tabulations in this report. The resultant total number of organisations profiled is therefore 253.

Finally, FTSE 250+ member organisations attract and employ top talent at every level. This includes internal and external network and systems management personnel, as well as highly skilled and experienced application development and operations staff. Many of these organisations have representatives on committees who provide leadership and governance of groups that develop IT and internet standards—a large number of these organisations have been incorporated for over 20 years and were early adopters of internet technologies. In other words, if there are exposure issues in this group of organisations, it may signal that exposure conditions are even more substantial in companies that do not have similar stature.

## Organisation Internet Asset and Metadata Attribution Methodology

The Internet Assigned Numbers Authority (IANA) coordinates the governance of key elements that enable smooth operation of the internet.[28] Two key governance elements relevant to the process of attribution include internet address space (or "IP" addresses) and domain names (the system that helps turns web addresses such as http://www.example.com/ into internet addresses so systems can connect to internet resources).

[28] Internet Assigned Numbers Authority, https://www.iana.org/ (Last accessed May 21, 2019)

## Attributing Internet Address Space to an Organisation

IANA delegates the management of internet address space to a small number of global and regional internet registries. These registries further delegate blocks of internet addresses and coordinate the metadata associated with these assignments to national and "local" registries that ultimately coordinate with internet service providers (ISPs), which assign internet addresses to users and organisations.

The metadata associated with these internet address assignments, such as the organisation names, location information, points of contact, and potentially the parent internet service provider, is stored in a distributed set of databases called the WHOIS service. The WHOIS service is a public resource that allows a user to retrieve information about an IP number, including the organisation that owns the internet address and the organisation's point of contact. Each registry maintains its own WHOIS database.[29] Individuals can use WHOIS to make interactive queries to these systems, and bulk copies of WHOIS database information are made available to organisations that will use the data for technical research purposes.

When an organisation wishes to manage its own internet-connected resources, it makes a request to a local ISP or local registry and is assigned one or more contiguous sets of addresses to use. This attribution metadata is stored in the appropriate WHOIS service. To illustrate what this looks like, Table 8 shows the internet address block assignments for Rapid7:

**Table 8: Rapid7 WHOIS Record Summary**

| INTERNET ADDRESS ASSIGNMENT | WHOIS ATTRIBUTION |
|---|---|
| 71.6.233.0/24 | Rapid7 Labs. Traffic originating from this network is expected and part of Rapid7 Labs Project Sonar sonar.labs.rapid7.com (C07045996) |
| 208.118.237.0/24 | Rapid7 LLC (C02934565) |

Unlike the Fortune 500 ICER, using the IANA registry methodology to locate FTSE 250+ company-owned space proved to be far easier given the level of detail provided in the RIPE network allocation database.[30] Over 90% of organisations had identifiable entries in the RIPE IPv4 registry. That does not mean the other 10% do not have blocks assigned to them, but it does mean there is an increase in the error rates when attempting to attribute those blocks.

Care was taken to avoid the inclusion of IPv4 ranges of organisations that also act as end-user or business internet service providers or cloud service providers.

## Attributing DNS Records to an Organisation

A similar WHOIS registration and database service exists for DNS assignments, except this is a far more distributed service that places direct control of all the underlying records for a domain into the hands of an organisation. Once assigned a domain name (e.g., "rapid7.com"), an organisation sets up its own DNS server (or uses one from a DNS service provider or cloud provider), then publishes and maintains records that map DNS names to a wide array of record types and values. Organisations can add, change, or delete records at will.

DNS "A" (address) records map names to internet addresses (e.g., <www.rapid7.com> currently maps to 13.33.37.212), but it is also possible to associate other types of information with an internet name.

[29] RIPE WHOIS Database Index, https://www.ripe.net/about-us/ (Last accessed May 21, 2019)

[30] RIPE Database, https://apps.db.ripe.net/db-web-ui/#/fulltextsearch (Last accessed May 21, 2019)

DNS "TXT" (text) records facilitate storing arbitrary text strings with internet names. A number of formal standards exist that provide rules for crafting specially formatted text records to convey additional metadata about that internet name resource or the domain name's proper owner.

DMARC[31] and the SPF[32] are two key TXT records for inferring the "safety" of an organisation's email configuration. These standards enable an organisation to communicate which systems are authorised to send mail on its behalf and what should be done with forged emails sent by attackers or spammers. Missing, improperly configured, or overly permissive configurations of these records put organisations at risk for both increased spam and phishing attacks. Since phishing attacks have been the primary means of attackers gaining a foothold within an organisation for the past few years, lack of care and attention to appropriate DMARC and SPF configuration significantly increases the likelihood of successful attacks against that organisation. Anyone can query the DNS for these and other records. As part of our research efforts into ecosystem-wide cybersecurity, Rapid7 performs millions of DNS lookups every month and stores the time-stamped record results in a large, historical database, which makes it possible to perform large-scale queries and track changes over time.

The Q1 2019 FTSE 250+ list includes the primary, well-known domain names of the members of the list. For example, "`weir.co.uk`" is the well-known domain for Weir Group (an Engineering, Construction, and Industrials organisation), and while "`global.weir`" is also owned by Weir, this domain isn't expected to handle email, nor does it have a valid email configuration. These sites were systematically scanned by Project Sonar, and the associated DNS names for the attributed organisations were used to determine the presence of DMARC and SPF.

[31] The DMARC Standard, https://dmarc.org/ (Last accessed May 21, 2019)

[32] The SPF Standard, April 26, 2014 http://www.openspf.org/ (Last accessed May 21, 2019)

# About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 7,200 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organisations. For more information, visit our website, check out our blog, or follow us on Twitter.

## QUESTIONS?

Email us at research@rapid7.com

RAPID7