RAPID7

National Exposure Index

Inferring Internet Security Posture by Country through Port Scanning

Rapid7, Inc. | June 7, 2016

Tod Beardsley, Security Research Manager
Bob Rudis, Chief Data Scientist
Jon Hart, Senior Security Researcher

TABLE OF CONTENTS

Executive Summary

Given the increased reliance we all have on the internet for everything from ecommerce, to monitoring the power grid, to adjusting our thermostats, we wanted to see if it might be possible to use the reach of Project Sonar to understand overall internet threat exposure at both a general level and at a country/region level. The term "exposure" can mean many things. In the context of this report, we define "exposure" as offering services that either expose potentially sensitive data over cleartext channels or are widely recognized to be unwise to make available on the internet, such as database systems. We looked for the presence of 30 of the most prevalent TCP services across the internet, tallied up the results and performed cross-country comparisons to produce a National Exposure Index, a ranked aggregation of the results of Rapid7's internet-wide scans of 16 usually cleartext or highly targeted common services, based on the in-country prevalence of those services

Key findings include:

- Millions of systems on the internet offer services that should not be exposed to the public network. Our survey uncovered 15 million nodes appearing to offer telnet, 11.2 million appearing to offer direct access to relational databases, and 4.5 million apparent printer services.[1]
- 4.7 million systems expose one of the most commonly attacked ports used by Microsoft systems, 445/TCP.
- SSH (secure shell) adoption over telnet (cleartext shell) is gaining ground over telnet, with over 50% of regions offering more ssh servers than telnet servers.
- Non-web-based access to email (via cleartext POP or IMAP protocols) is still the norm versus the exception in virtually every country.
- There is a correlation between the GDP of a nation, overall internet "presence" in terms of services offered, and the exposure of insecure, cleartext services.
- The most exposed nations on the internet today include countries with the largest GDPs, such as the United States, China, France, and Russia.

1 We counted 7.8 million MySQL databases and 3.4 million Microsoft SQL Server systems. This study did not include ports for other popular database systems, notably, PostgreSQL and OracleDB.

Introduction

Sir William Thomson (better known as Lord Kelvin), noted for his research into thermodynamics and his accomplishment of laying down, literally, the communication foundations of the internet in the form of the first transatlantic telegraph cable has a famous saying: "To measure is to know." This drive "to know" is at the core of everything we do here at Rapid7, whether it's developing solutions to help organizations identify, understand, and manage their vulnerabilities and exposure, or providing solutions to help them detect and deter attackers. It is also what motivates us to develop research initiatives such as Project Sonar, our active scanning infrastructure, and Heisenberg, our distributed collection of passive honeypots. These projects make it possible to ask questions at internet scale and mine the results for answers.

To that end, this paper takes the initial steps towards validating some key assumptions about the nature of the internet that IT and information security professionals take for granted, using the exploratory research tools we have built out here at Rapid7.

The first part of the study establishes—through empirical methodology—that there is, in fact, a relationship between a country's economic strength and the quantity of discoverable services hosted on the internet.

The second part of the study measures e the prevalence of cleartext, unencrypted services on the Internet and their encrypted counterparts, by country, and use this ratio to generate an overall National Exposure Index score. In addition, we break out different protocol families, such as world wide web services, remote administration, e-mail, and others, and rank countries on their adoption of fully encrypted and cleartext implementations of these services.

Throughout this exploration, we discuss why fully encrypted communication is important for overall internet safety, usability, and sustainability. Today's internet touches virtually everyone's lives and is a critical component of economic security. Counterintuitively, the adoption of fully encrypted protocols for core internet services has not scaled with our personal, national, and global dependence on the internet.

This is a foundational paper, intended to educate readers about the core principles on which internet-based services operate. Future papers from Rapid7 will build upon this work, exploring related areas of security and exposure.

01

MEASURING INTERNET ADOPTION

We began this paper to test a fairly simple hypothesis: do countries with larger, more robust economies have a correspondingly larger internet presence, and how does this presence relate to overall exposure to internet-based threats? To answer this, we first needed to measure each country's count of unique internet services offered, which itself is a somewhat tricky proposition. In order to participate on the internet, a computer must be reachable by an Internet Protocol (IP) address. An IP address is (generally) a globally-unique identifier used to signify how to reach that computer. Each IP address "lives" in a network and that network "lives" in something called an autonomous system (AS). Internet providers manage how routing occurs between each AS, so one way to identify the owner of an IP address is by the network provider. Another way is to try to find the organization that might have purchased the IP addresses and geographically identify it with them and their locale, which is generally referred to as geolocation of IP addresses. There are many services that provide tools and data for performing geolocation, but you will often be bitterly disappointed[1] if you try to identify a specific street address with an IP address. However, geolocation becomes far more accurate the more you "zoom out". We used a commercial feed by MaxMind[2] along with the `iptools`[3] and `rgeolocate`[4] R packages (written by Rapid7 researchers Oliver Keyes and Bob Rudis) to associate IP addresses with their country/region of origin. In this section, we take a look at the rate of internet participation per country, and can make some assertions about a nation's GDP as it relates to internet adoption.

1 http://theweek.com/articles/624040/how-internet-mapping-glitch-turned-kansas-farm-into-digital-hell

2 https://www.maxmind.com/en/home

3 https://cran.rstudio.com/web/pa ckages/iptools/index.html

4 https://cran.rstudio.com/web/packages/rgeolocate/index.html

A Crash Course on IP Addressing

Any given IP address has two parts, the network address and the host address; for example, many home networks have a computer at "192.168.1.100," where the network part of the address is "192.168.1.0" and the host address is the last digit, "100."

In the early days of the internet, every computer that connected to the internet had its own address, and maintained a local host file that provided the addresses of every other computer on the internet. This became impractical as the internet grew, and services such as the Dynamic Host Configuration Protocol (DHCP) and the Domain Name Service (DNS) became common and standardized. DHCP allows computers to acquire and reserve an IP address and other pertinent configuration information, and DNS allows computers to match human readable names to IP addresses and catalog all sorts of other useful address record information.

This brief explanation of IP addressing leaves out important details such as subnet addressing, broadcast and multicast addressing, and how routing between networks works, but is enough to sketch out how Internet Protocol addressing in general works. However, it is specific to IP version 4 -- the "dotted quad" notation that is the traditional internet addressing scheme. This brings us to Network Address Translation (NAT) and IP version 6 (IPv6), both of which sought to solve the problem of a rapidly vanishing pool of unused and available IPv4 addresses.

Solving Address Exhaustion

In the mid-1990s, after the emergence of the World Wide Web, it became obvious that the world was going to run out of internet-routable IP addresses in the face of the sudden high demand for IPv4 addresses. In order to address this explosive growth, two solutions emerged. The first was NAT, a system that allowed computers with private IP

addresses to transparently offer services and be reachable "behind" a single public IP address. NAT is the technology that allows homes to have several "internet-connected" endpoints, such as computers, tablets, smartphones, and other devices, all on one shared, public-facing address. NAT was intended as a short term, stop-gap measure to conserve IP addresses and make it possible for Internet Service Providers (ISPs) to meet the immediate residential and commercial demands for connectivity[1].

IPv6 came slightly later as a more general solution to the address exhaustion problem. IPv6 addressing is similar to IPv4 addressing, in that there is a network part and a host part to an address, but the possible address space is much larger than IPv4. In fact, the address space is stupendously larger. While IPv4 offers a theoretical maximum of 4.2 billion addresses (discounting practicalities such as reserved address ranges), the total theoretical IPv6 address space is about 340 billion billion billion billion (or 340 undecillion). Since the mass of planet Earth, in grams, is about 6 billion billion billion (or 6 octillion), you could assign every gram of matter its own IPv6 address, and you would have enough room for another billion Earths before starting to get worried about address exhaustion.

One of the barriers to adopting IPv6 is that it is not directly compatible with IPv4 addressing, so computers and applications that rely on and expect IPv4 addresses need to deal with an intermediary translation layer to communicate. Complicating this is the fact that NAT is already an effective translation layer. To paraphrase Milton Friedman, there is nothing quite so permanent as a temporary solution.

NAT, it turns out, was a pretty great "temporary" solution, since it also brought a major security side benefit: it offers effective segmentation, by accident, between "private" address space and "public" address space. While it might be convenient to have enough address space to connect literally every thing to the internet, the wisdom of such an approach to universal connectivity is suspect, at least until every device is capable of handling its own address resolution, firewalling, and authentication challenges.

1 http://www.internetsociety.org/articles/retrospective-view-nat

Internet Adoption by Country

Since the internet is such a useful engine for economic growth, we hypothesized that countries with higher GDP might have higher utilization of IP address space. We took a look at this from two different vantage points. First, we correlated GDP and the number of nodes counted by our study (Figure 1) and then we used data we received from CAIDA (see 'The Challenges With "Counting the Internet"' sidebar) on statistically measured IPv4 space utilization.

Both analyses show a linear relationship between GDP and internet services, with the "outliers" of the United States, China and India adding some uncertainty (the expanding, gray region in Figure 1). Given the need for certain levels of education, infrastructure, and commerce to warrant internet network expansion, this relationship was expected, and matches most people's intuition. Neither of these correlations are meant to prove causation; it's not as if a country can increase its GDP simply by adding more internet nodes, nor does an increased GDP independently cause more nodes to spring up.

We've only just begun to tap into what constitutes "exposure" and need to research additional factors as we expand our study on IP utilization in future reports. Over time, we'll be working to identify more discrete components underlying GDP that are likely influencing this relationship.

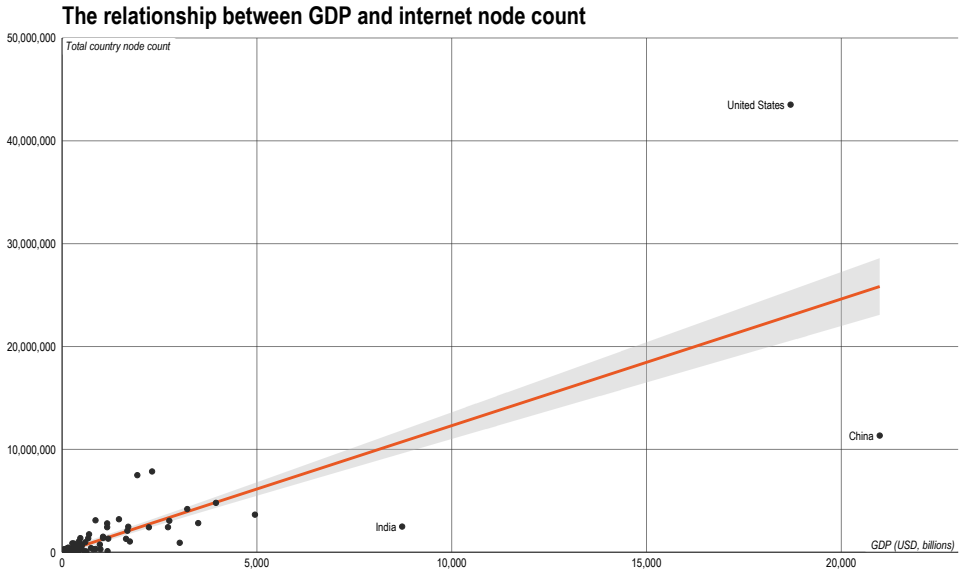


Figure 1

Mapping the Internet

We painted a picture of the reach of our study in Figure 2. The technical term for this chart is a "heatmap of /24 network block in a 12th-order Hilbert space." We like to think of it as a proper map of the internet[1]. Every pixel represents a "/24" network (i.e. 254 usable nodes per network). Rather than order it from left to right (and wrapping when you hit the right edge), a mathematical transformation is used to place similar /24 networks close to each other.

Since we contacted individual IPv4 addresses, we need to color each pixel by how many we received responses from within a given network. The black areas mean we received no signal at all, the darker blue areas mean we picked up a few nodes and the yellow areas means we picked up many or most nodes.

1 though this representation will always be much cooler: https://xkcd.com/195/

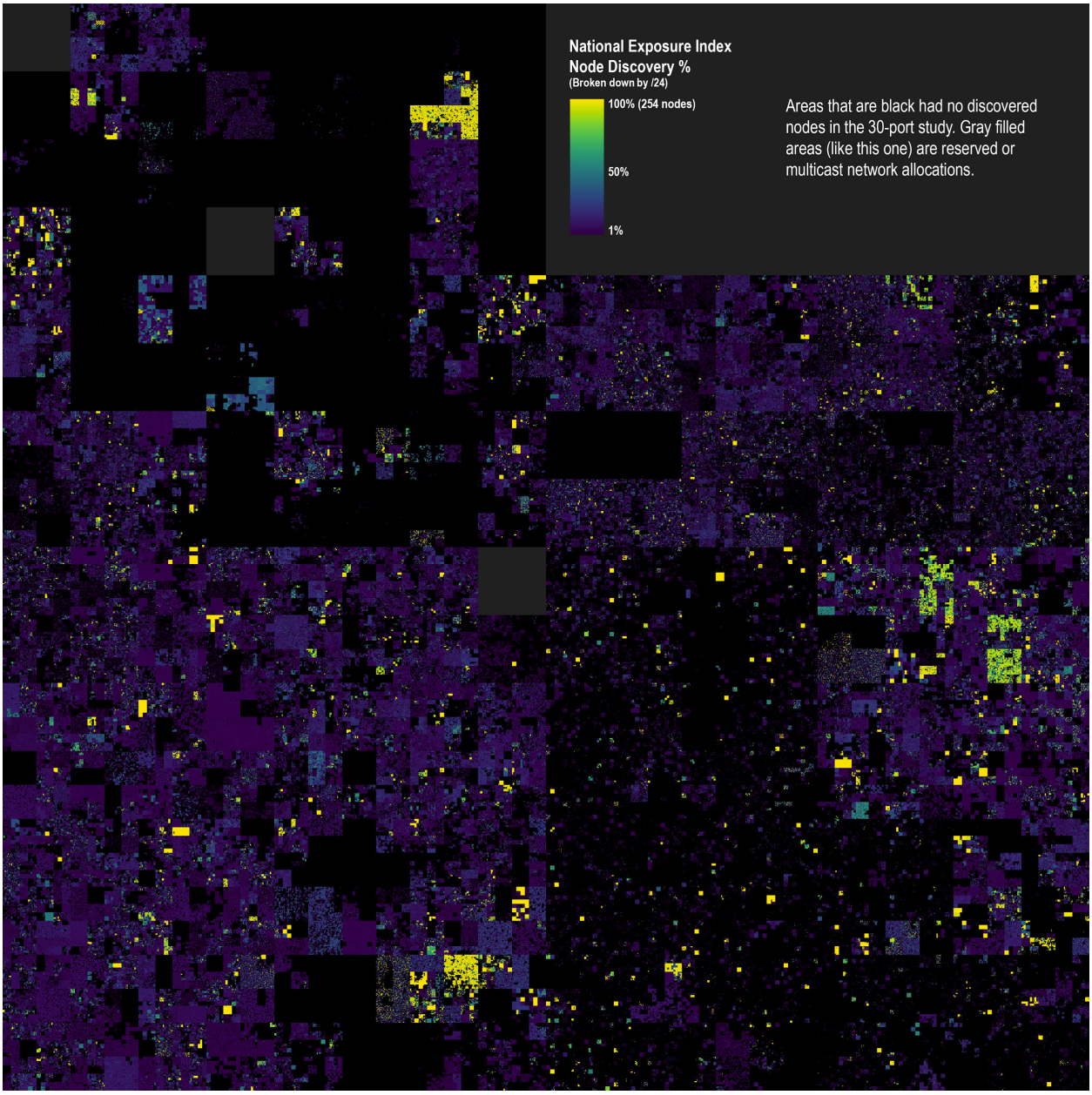


Figure 2: Heatmap of the Internet as seen by our study.

Since we geolocated these IPv4 addresses, that means countries can be plotted with their borders on this map, just like a regular map. The following alternate map view shows all the IPv4 address space "owned" (but not necessarily utilized) by the twelve most prevalent countries. The gray areas have no IPv4 nodes at all, as they are "reserved" addresses. Unlike traditional country outlines, these network-level borders are very fragmented and co-mingled. If you visually compare the two maps, it's clear there are vast, unexplored regions in our study. But, it's also clear that there is much life left in IPv4, despite the calls to move to IPv6.

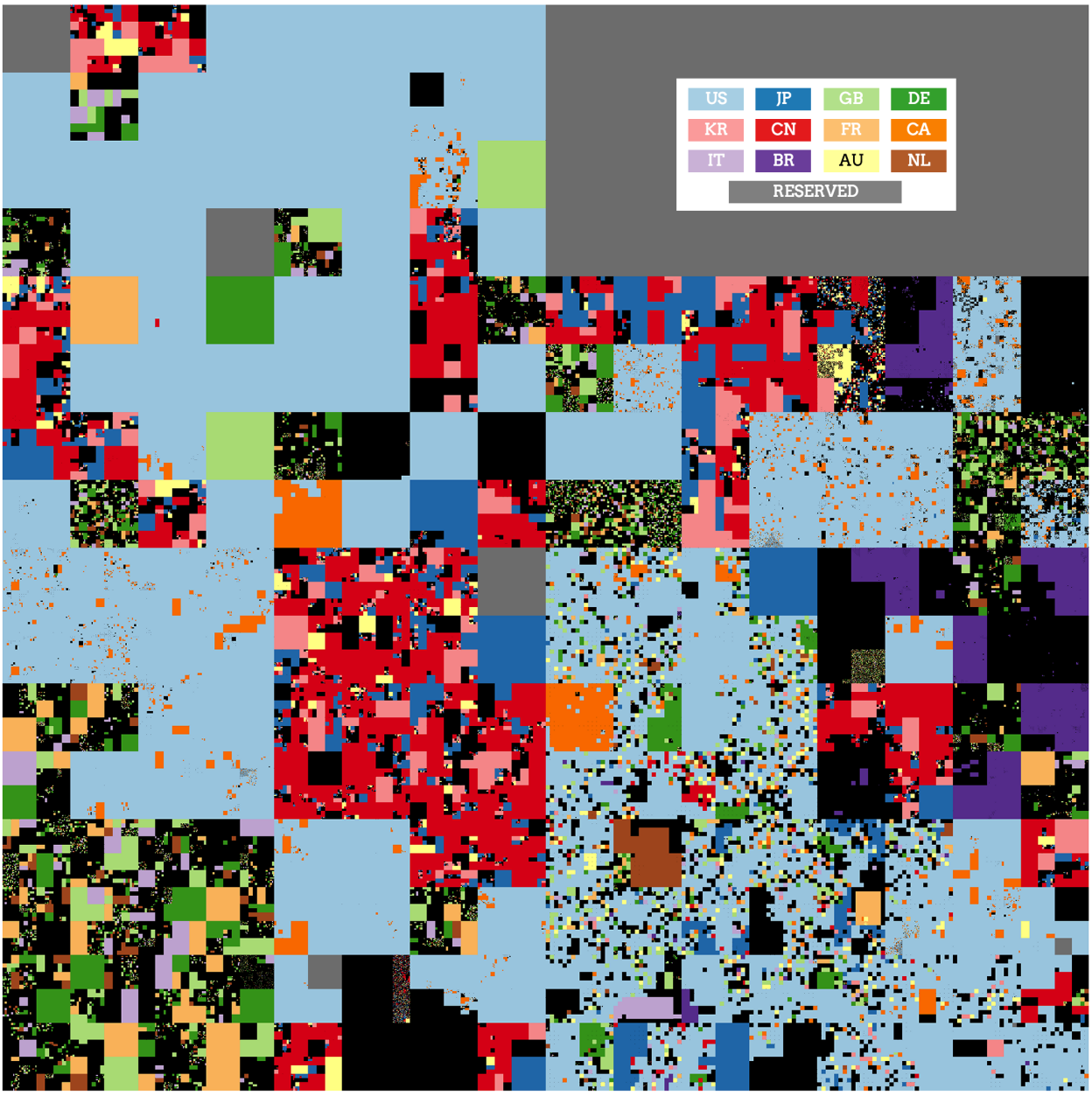


Figure 3: Heatmap of the Internet, politically color-coded

There are two sides to internet adoption: hosting/exposing services and expansion of internet clients (i.e. users). This country-level, service-centric view—the one provided by Project Sonar—enables researchers, over time, to observe patterns such as the migration of cloud service providers into different regions and identify new and potentially innovative corporate, government and educational/research initiatives. As we continue to study adoption it will also be important to include a view into the use and expansion of IPv6 in each region to see how that changes the mix the type and amount of services offered.

02

MEASURING EXPOSURE

Now that we can measure the general adoption of the internet, by country, we can move on to assessing the security of each of those countries' adoption. However, because it is impossible to simply look at any given endpoint and give an assessment of "secure or insecure," we will be using a much simpler metric to infer the security posture of geographically-located services in the aggregate. We will ask: are the services offered likely using some form of encryption, or are they being offered as unencrypted, unauthenticatable services?

A Crash Course in TCP/IP Services

Say you wanted to "visit a website," a task nearly all the readers of this paper will perform several times per day. In TCP/IP networking parlance, this involves using a client application (a web browser) to connect to a service (the web server) on the internet. In order to find this service, your client application needs to learn at least three things: The IP address of the remote computer you intend to connect to (as described above), the protocol (TCP or UDP), and the port number that the remote service is listening on.

For example, if you wanted to visit the web service signified by "http://www.rapid7.com," your computer would look up the IP address matching that name (which, according to DNS, is the IP address, "54.192.6.49"). Then, your web browser would, by default, assume you wanted to connect to port 80, since port 80 is the common and well-known port number for the web service.

This leaves out a lot of detail, for example, we're setting aside the important steps involved in contacting DNS in the first place, how routing from your computer across the several networks to where www.rapid7.com occurs, or how network address translation (NAT) and content distribution networks (CDNs) conspire in the illusion that it's a straight line between your PC and the remote computer.

This process is effectively how transport control protocol (TCP) client/server operations work on the internet. In order to read a webpage, your computer (or tablet, or smartphone) establishes a connection to an IP address and a web service port. The address and port combination of "54.192.6.49:80" is effectively what "http://www.rapid7.com" translates to, as far as your computer's routing table is concerned.

Different Ports for Different Services

Port 80 is, by far, the most popular listening service on the internet, thanks to the wild success of HTTP as a protocol to distribute documents, photos, and all sorts of other media. Coming in at a distant second is port 443, which is also a web service port, but it's intended for "secure" web services, HTTPS, which is HTTP wrapped in an additional protocol that provides encryption. Therefore, "`https://www.rapid7.com`" (note the 's' in "https") translates to your computer's operating system as "54.192.6.49:443." While it would seem that these two protocols serve the same function, the fact that one is encrypted and one is in cleartext means that these two protocols have different "handshakes," and need to distinguish themselves on different ports in order for your browser to make sense of the data.

There are many other ports, though, and the survey of these ports is why this paper exists. As in the case of HTTP versus HTTPS, there are protocols that are (usually) cleartext, protocols that are encrypted, and some protocols that can go either way (but are usually cleartext, and always start off that way). And while there are 65,535 possible listening ports for every IP-addressable endpoint on the internet, we are concerned primarily with a sampling of the "most popular" TCP ports on the internet.

Port Scanning Targets

Rapid7 conducted a series of port scans, intended to cover the entire addressable IPv4 internet space, over the end of April and beginning of May, 2016. The goal was simple: discover and confirm the ranking of which of the most popular ports, aside from the usual HTTP service ports, were open and listening on the internet, and of those, how much of the active service space is reasonably "secure."

Candidate Ports to Scan

Of the TCP protocols, 30 were chosen to assess the state of the most common protocols found on the internet and other TCP/IP networks. The source of this initial popularity was guided by both the nmap services list and the Rapid7 Labs team's collective wisdom on what one should expect to find. The top 15 protocols are one-for-one matches with the most frequent protocols identified by a series of private nmap scans of the internet conducted in 2008[1], while the remaining 15 are protocols which we hypothesized should come up fairly routinely[2].

Encryption as Stand-In for Security

As mentioned above, "security" is tricky to measure directly, since doing so would involve some fairly complicated and often invasive procedures, unique for each of the protocols selected for scanning, and many techniques are often illegal to conduct without the prior consent of the owners[3] of those endpoints[4]. However, quantifying whether a service is encrypted should be an effective proxy for a difficult-to-measure quality like "security," as explained below.

The Virtues of Encrypted Services

When the internet began, notions of security were fairly limited; after all, it was merely a network of machines whose operators were well-known to each other, and few people outside of the U.S. military and academic circles were even aware of its existence, much less how it worked. Once the World Wide Web was introduced, gained traction, and resulted in explosive commercial interest in the internet, the ability to authenticate people offering services and people connecting to those services became much more important. Thus, encryption technologies were lain atop the original permissive and largely personally-anonymous design of the internet.

At the risk of being extremely reductive, encryption offers two essential features to internet protocols that were not available in plain, cleartext protocols.

First, encryption offers the ability to **certify** that a server is operated by an entity which actually is the entity it claims to be, through the use of **signed certificates** that are difficult to forge. It is important for a retail store, bank, or government office to be able to appear legitimate to its customers, or else those customers would not feel comfortable sharing personal details or financial information with that service. We do this in the offline world easily enough by inspecting signage, surroundings, badges, and other obvious markings, but on the internet, we have no such visual cues that the person we're dealing with is actually representing the service we're trying to use.

Second, encryption ensures that only the parties involved in a transaction can see the details of that transaction by enforcing **confidentiality**. A common transaction involves the user of a service offering a secret password, which is then validated by the service to confirm that the person on the other end is actually who they say they are. Without this confidentiality, anyone could eavesdrop on the transactions and replay them or alter them. Recall that the internet is a collection of different networks, and the experience of directly connecting to a service is, in fact, an illusion -- connections traverse several networks when they are established, all of which have an opportunity to eavesdrop on traffic.

Without these twin guarantees that endpoints are who they say they are, and that secrets can be passed with confidence, it would be difficult to conduct any transaction on the internet that involves any reasonable level of security. Unfortunately, these features came later to the internet, and many services still running today do **not** offer the level of confidentiality or integrity that is demanded by modern best practices. Therefore, for the purposes of this study, while a given encrypted service isn't necessarily secure, we are presuming that **any service that is not encrypted is necessarily insecure**.

Ports Chosen

Table 1 on page 11 lists each port scanned by number, the usual protocol identified for that port, its score on the nmap services frequency table, and if the protocol is typically or usually offered as an encrypted service. It is sorted by the frequency with which they were observed across the entire IPv4 address space in the scans conducted for this research.

1 https://nmap.org/book/nmap-services.html

2 We surveyed Rapid7's body of researchers and data scientists and aggregated their expert opinions to build the complete list.

3 for more on these legal issues, see The Attacker's Dictionary, pp 24-25, "Chilling Effects and Legislative Bug-Fixing"

4 https://information.rapid7.com/attackers-dictionary.html

Port	Protocol/ Service	Encrypted?	Observed Count	(Percent)	Description
80	HTTP	FALSE	76,266,507	19.89%	HyperText Transport Protocol, used to serve web pages and web application.
443	HTTPS	TRUE	50,507,072	13.17%	HyperText Transport Protocol (Secure), used to serve web pages and web applications.
22	SSH	TRUE	21,692,582	5.66%	Secure Shell, an encrypted-by-default alternative to Telnet, used to administer remote servers and tunnel other protocols.
21	FTP	FALSE	20,375,533	5.31%	File Transfer Protocol, a means to transfer files for a variety of purposes.
25	SMTP	FALSE	19,888,484	5.19%	Simple Mail Transport Protocol, used to send mail.
8080	http-alt0	FALSE	17,477,357	4.56%	An alternative port for 80/TCP, usually used for HTTP and HTTP proxy services.
23	telnet	FALSE	14,871,682	3.88%	Telnet, a remote command shell service used to administer remote servers.
53	DNS	FALSE	12,602,272	3.29%	Domain Name Service, used to resolve names to IP addresses. While DNS is usually served over UDP, large responses that would otherwise be fragmented are instead passed over TCP.
143	IMAP	FALSE	11,467,158	2.99%	Interim Mail Access Protocol, used to download email by end users.
110	POP3	FALSE	11,073,439	2.89%	Post Office Protocol version 3, used to download email by end users.
8081	http-alt1	FALSE	9,256,437	2.41%	An alternative port for 80/TCP, usually used for HTTP and HTTP proxy services
995	POP3S	TRUE	8,966,597	2.34%	POP3 (Secure)
3389	RDP	FALSE	8,875,022	2.31%	Microsoft Remote Desktop Protocol, a graphical remote administration service.
465	SMTPS	TRUE	8,429,878	2.20%	SMTP (Secure)
587	SMTP submission	FALSE	8,219,606	2.14%	SMTP submission service, used usually for endpoint clients to send email.
993	IMAPS	TRUE	8,066,032	2.10%	IMAP (Secure)
3306	MySQL	FALSE	7,889,329	2.06%	MySQL service, used by the popular and usually open source database server maintained by Oracle.
111	rpcbind	FALSE	7,788,299	2.03%	Remote Procedure Call / Portmapper
1723	PPTP	TRUE	7,020,817	1.83%	Point-to-Point Tunneling Protocol, a Virtual Private Network endpoint
8443	https-alt	TRUE	6,477,445	1.69%	An alternative port for 443/TCP, usually used for HTTPS
8888	http-alt8	FALSE	5,787,295	1.51%	An alternative port for 80/TCP, usually used for HTTP and temporary sites
135	MS-RPC	FALSE	5,392,061	1.41%	Microsoft Remote Procedure Call, an older standard developed by Microsoft for distributed computing.
5900	RFB	FALSE	5,269,641	1.37%	Virtual Network Computer (VNC), a graphical remote administration service
445	SMB/CIFS	FALSE	4,698,909	1.23%	Server Message Block / Common Internet File System, used in Microsoft networks for a variety of tasks such as file sharing and administration.
389	LDAP	FALSE	4,688,371	1.22%	Lightweight Directory Access Protocol, usually used for authentication and user and asset lookup services.
5000	uPNP	FALSE	4,532,209	1.18%	Universal Plug and Play, a protocol used for machine-to-machine discovery and configuration.
9100	jetdirect	FALSE	4,519,611	1.18%	HP JetDirect, a printer control service used to schedule print jobs.
990	FTPS	TRUE	4,031,195	1.05%	FTP (Secure)
139	NBSS	FALSE	3,889,131	1.01%	NetBIOS Session Service, used in NetBios over TCP/IP in (usually older) Microsoft networks to transfer files and conduct printing operations.
1433	MSSQL	FALSE	3,395,533	0.89%	Microsoft SQL Server service, a popular database

Table 1 Ports Scanned

Note that while it is possible for some of these protocols to enable encryption, they are generally unencrypted in deployment. For example, recent versions of SMB/CIFS (typically on port 445) allow for encrypted usage, but the majority of SMB exposed to the internet is of the cleartext, older variety.

In addition, some protocols, such as SMTP and MSSQL, allow for opportunistic encryption in some non-default configurations. Protocols like these are fraught with chicken and egg issues; in order to request a reasonable level of security, one must first establish an insecure connection. The act of negotiating an encrypted standard, such as SMTP's STARTTLS option, could be undermined by an active attacker who can simply impersonate either end of the connection to avoid asking for, or accepting, the negotiated encryption. So, while these in-band signaling solutions to open an encrypted channel can defend against against passive monitoring, they are not sufficient against active attacks.

Most services on the internet are unencrypted, which is worrisome for any standards or enforcement body charged with keeping up a reasonable security profile for an organization. Indeed, the Internet Architecture Board advised specifically for strong, trustable, internationally available encryption standards in 1996 in the (rather portentously numbered) RFC 1984: "As more and more companies connect to the Internet, and as more and more commerce takes place there, security is becoming more and more critical. Cryptography is the most powerful single tool that users can use to secure the Internet[1]." The Internet Engineering Task Force (IETF) reiterated this position in 2014 in a privacy context as part of RFC 7258, where it identified pervasive monitoring as a "widespread attack" that protocol designers should mitigate against with cryptographic solutions[2].

1 https://tools.ietf.org/html/rfc1984
2 https://tools.ietf.org/html/rfc7258

Characterizing Protocols

A laundry list of TCP ports is not particularly informative on its own, and many ports form relationships. As we see later in the "Ports Per Address" section, many machines offer more than one service, so these port families are discussed below.

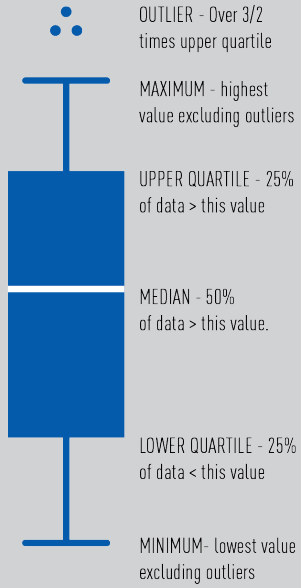
World Wide Web Protocols

The most popular services on the internet today, unsurprisingly, are connected to the World Wide Web. The standard HTTP and HTTPS ports, 80 and 443, account for just under a third of all observed service ports on the internet, and when considering the typical "alternative" ports of 8080, 8081, and 8888, that figure rises to over 40%. Counting web services by port counting, however, does miss some important considerations. For example, modern CDNs, virtual hosting, and other techniques are used to aggregate web services to one TCP/IP address and port, so while we count 76 million listening port 80 services, the actual number of individual websites is much larger. Netcraft, for example, puts the count of total websites at over one billion, while the number of "web-facing computers" at about 5.8 million. The authors of this paper do not believe that we have discovered an extra 70 million web-facing computers, however; port scanning is not the same as delineating unique services, or even unique computers; recall that many computers can appear to share a single IP address, and a single computer can have multiple IP addresses. Netcraft also focuses primarily on hosting providers, while our Project Sonar studies encompass the entire internet.

It's interesting, and encouraging, to note that the delta between listening port 80 and listening port 443 services is somewhat narrow; the count of cleartext HTTP services appear to be only about 25% more than their encrypted counterparts. This is likely due to the fact that most websites which desire authentication will offer encrypted services for at least the authentication form, and until recently,

Unwrapping Boxplots

We've used boxplots to help compare the similarities and differences in the distribution of the counts of ports on servers. A boxplot is a more compact way of describing a distribution than, say, a histogram, though it leaves some details out. There aren't many boxplots in cybersecurity reports and the last time most practitioners have seen one was back in school, so here's a quick refresher/introduction to boxplots that you can refer back to when looking at the comparison charts.



If you look at just the boxplot for port 80 in Figure 4, you can make out that the median is near 17,000 (log scales are common in cybersecurity data but are notoriously hard to read at a glance) and the range of the "box" is between approximately 1,800 and 180,000. This is where most of the server counts are per-country. If all the server+port distributions were the same, each box would be at the same spot on the y-axis. By comparing the differences in box size, box positions and the positions of the medians, we can see that there are, in general, more servers running port 80 in each country than there are running port 443 and other web-oriented services.

Rank and File

We've made liberal use of ordered, stacked segment charts to help see the ratio of encrypted to unencrypted services. For most of these charts we've sorted the list of countries by "worst" (i.e. more unencrypted services) to "best" (i.e. fewest unencrypted services). Because this changes the order of the countries in every chart, we've annotated each of them with the list of countries on the opposite ends of each scale and also provided an accompanying table of top- and bottom-ranked regions. Finally, to help see where the "midpoint" happens we've placed a marker at the first country with a 50/50 mix of servers running encrypted and unencrypted services. Ideally this line would always be way over to the left to show that all countries mostly have encrypted servers running. As you'll see in all of the charts, this is clearly not the case.

encrypting only the authentication form was a fairly common practice in web hosting. Today, many of the most popular websites on the internet offer their services entirely over encrypted channels, and web servers are much easier to configure for encryption today than ever before.

While the alternative ports for HTTP are often used for testing and temporary websites, a popular use of alternative HTTP ports is for proxying web traffic; these services do not offer websites of their own, but instead, proxy user requests on to the ultimate destination.

Finally, many of these HTTP services are not websites in a traditional sense; the rise of the web meant that, in many locations, it became standard fare to block traffic sent to any port **not** associated with the web; as a result, client/server applications that are normally designed to operate across network boundaries are increasingly being developed to work over port 80 and port 443. Nearly every mobile app used on a smartphone, for example, communicates with a web-based service on port 80 or port 443 in order to minimize the risk of firewall blocks, but these services are not traditional web servers, in the sense that they do not provide HTML files to be rendered by a client browser.

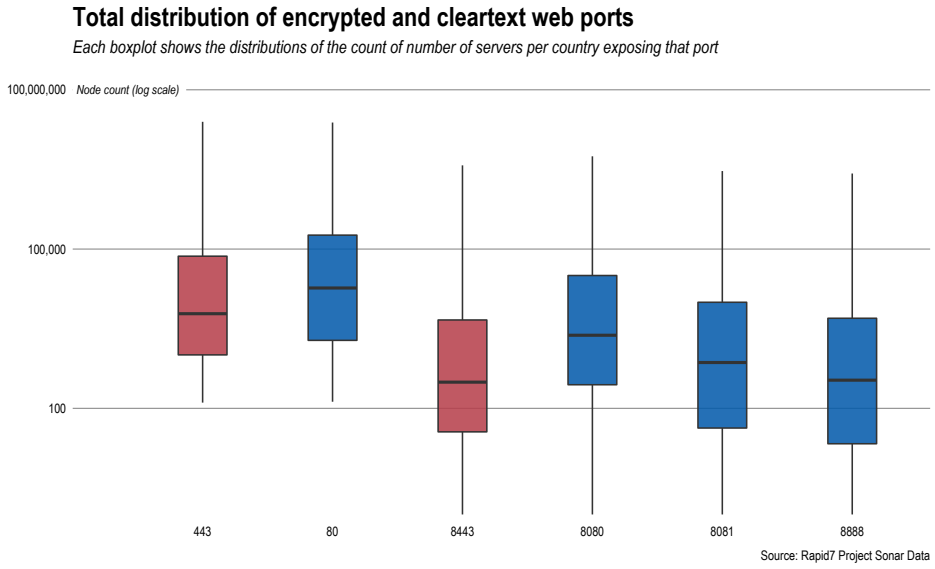


Figure 4

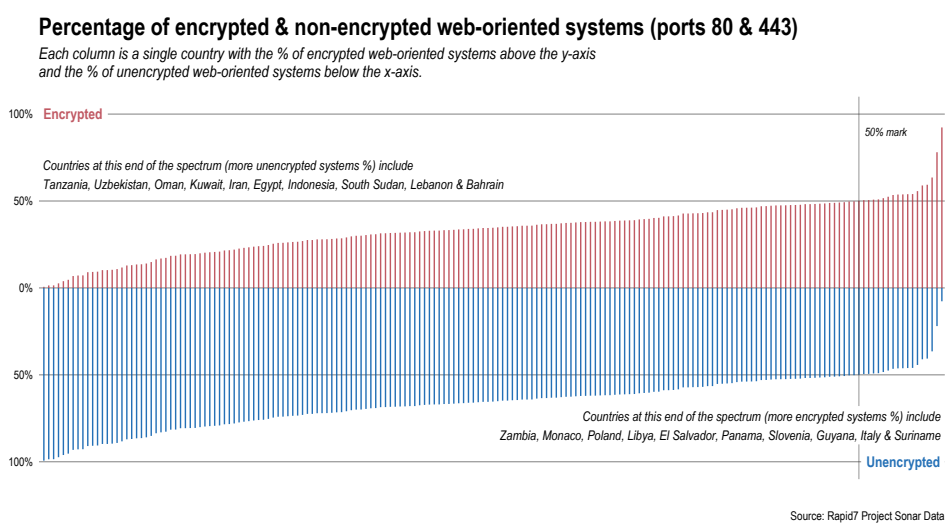


Figure 5

Most Exposed (in order)
Tanzania, United Republic of
Uzbekistan
Oman
Kuwait
Iran, Islamic Republic of

Least Exposed (in order)
Suriname
Italy
Guyana
Slovenia
Panama

Table 2: Countries at the extreme ends of the unencrypted to encrypted web service ratio

Telnet and SSH

The seventh most common service on the internet is telnet, a remote interface (or "shell") to a computer's command prompt, usually used for system management. Described in 1969 in RFC 15, it predates the TCP/IP standards that are foundational for the internet by several years, so it is not surprising that security concerns were never addressed with telnet in any sort of widespread way. Every networked operating system has a telnet client available, and until recently, most shipped with one out of the box.

However, modern administrators tend to use SSH, a cryptographically secure alternative to telnet that offers strong client and server authentication and a robust set of encryption protocols. In fact, it is the third most common service observed on the internet, after HTTP and HTTPS, which bodes well for the modernization of the internet.

However, SSH does not merely offer the same remote shell capabilities that telnet provides. SSH, thanks to its early adoption of passwordless, scriptable authentication, its native compression and session resumption capabilities, and the configurability on both the client and server side, has become an easy choice for most administrators.

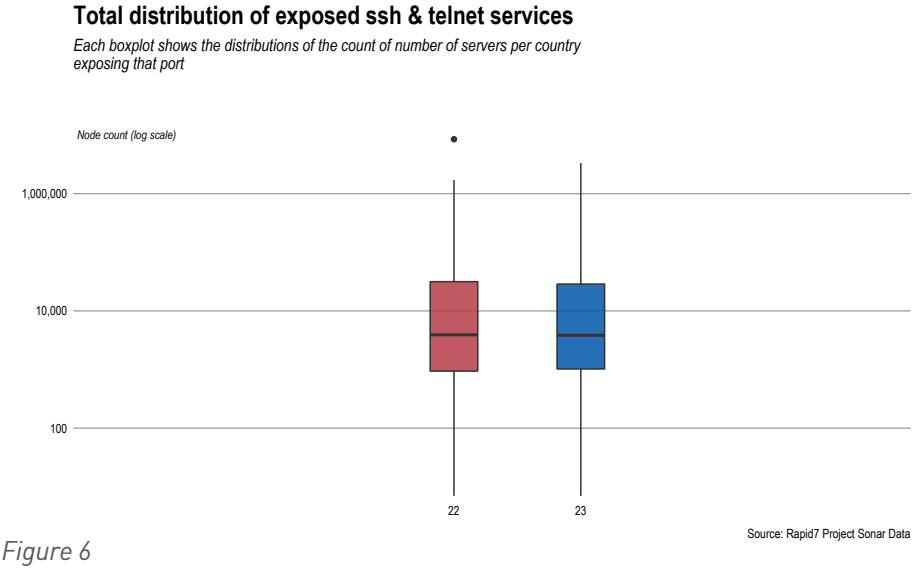


Figure 6

Because of these and other considerations, SSH is not only a more secure solution, it's a more pleasant solution; the fact that it makes people's jobs easier, rather than "merely" offering superior security, makes the "ssh or telnet" choice an easy one for system administrators.

That said, the fact that we cannot seem to stomp out telnet in production completely is both frustrating and worrying. According to our scans, there are over 14 million devices that appear to be offering telnet services on the internet today.

Most Exposed (in order)
Sudan
Jordan
Guatemala
Viet Nam
Korea, Republic of

Least Exposed (in order)
Germany
United Arab Emirates
Netherlands
Estonia
Ireland

Table 3: Countries at the extreme ends of the unencrypted to encrypted remote shell service ratio.

Email Protocols

SMTP (port 25), POP3 (port 110), and IMAP (port 143) are the foundational services for traditional email over the internet. The two client protocols, POP3 and IMAP, are what email clients use to receive mail from a mail server, while SMTP is used to deliver mail, either from an email client or between email domains.

Historically, all three of these protocols are cleartext. Most major email providers have switched to SSL-wrapped services for IMAP and POP3 (on ports 995 and 993), since transmitting passwords in the clear is roundly considered bad practice for the reasons outlined above, and SSL-wrapped services are the typical means to encrypt otherwise cleartext protocols, as we do with HTTPS and HTTP.

SMTP is a different matter, though. Many "secure" SMTP services use STARTTLS, an opportunistic method to upgrade a cleartext connection to an encrypted connection, as described above. Because of this, it's difficult to predict if an SMTP session over ports 25 or 587 is, in fact, secure or not, due to the problem of an active attacker denying the upgrade to STARTTLS, and many mail clients fail back to a cleartext connection if STARTTLS negotiation is unsuccessful. In the case of an SMTP-to-SMTP delivery of mail, it's similarly impossible for the end users to determine if STARTTLS was actually in use, since there is no practical way to signal to the user if a failure occurred. In the end, only a properly SSL-wrapped SMTP service on port 465 could be considered reliably encrypted.

Total distribution of exposed mail-oriented services

Each boxplot shows the distributions of the count of number of servers per country exposing that port

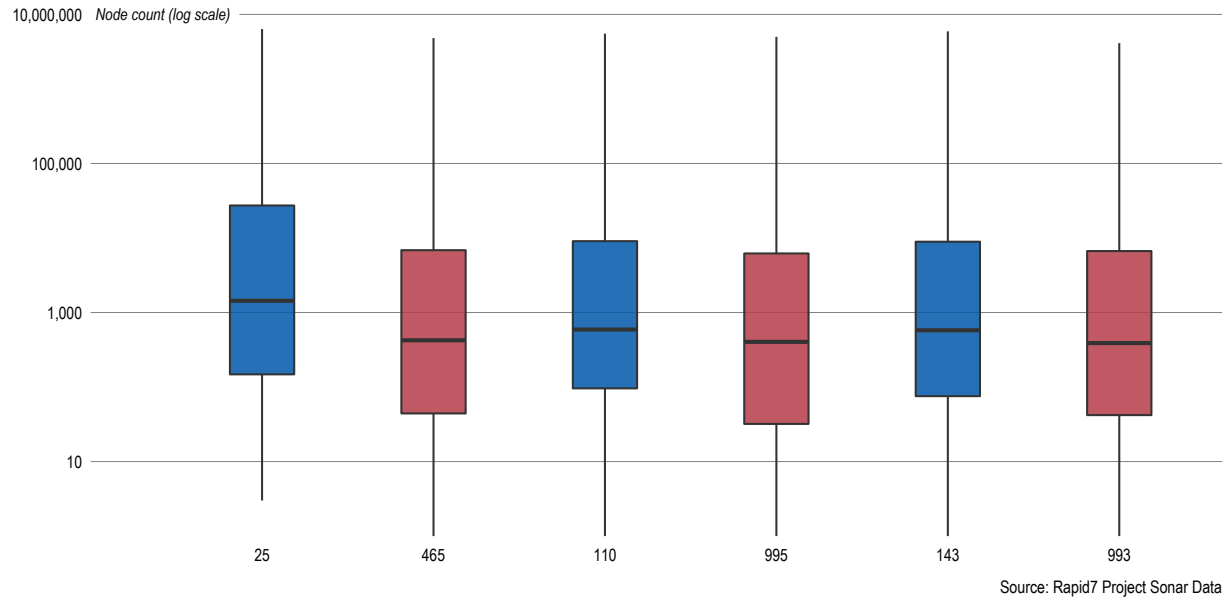


Figure 7

Percentage of encrypted (port 465) and unencrypted (port 25) mail systems

Each column is a single country with the % of encrypted systems above the y-axis and the % of unencrypted systems below the x-axis.

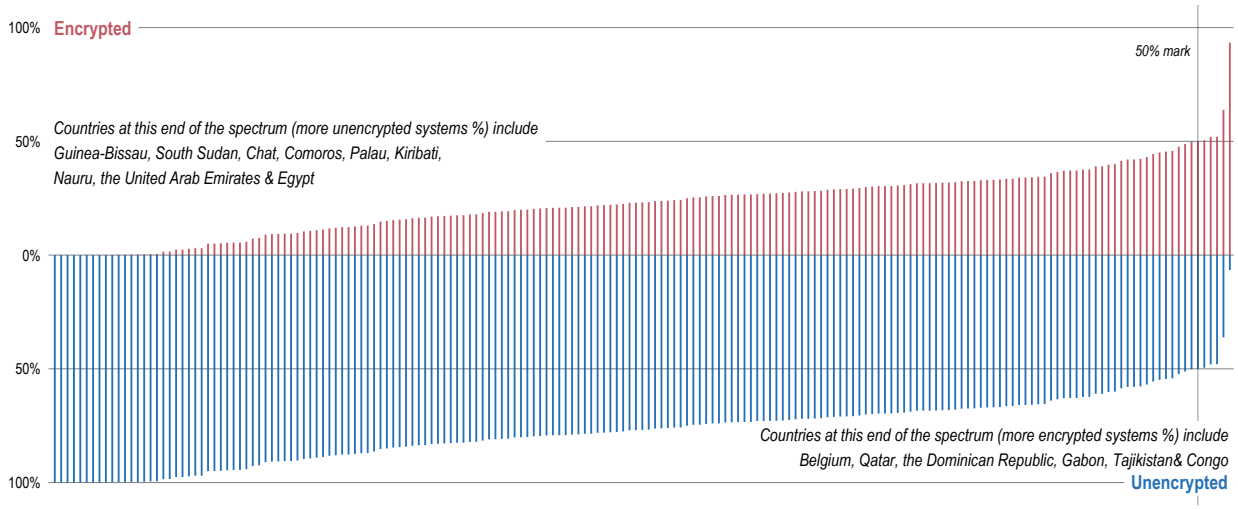


Figure 8

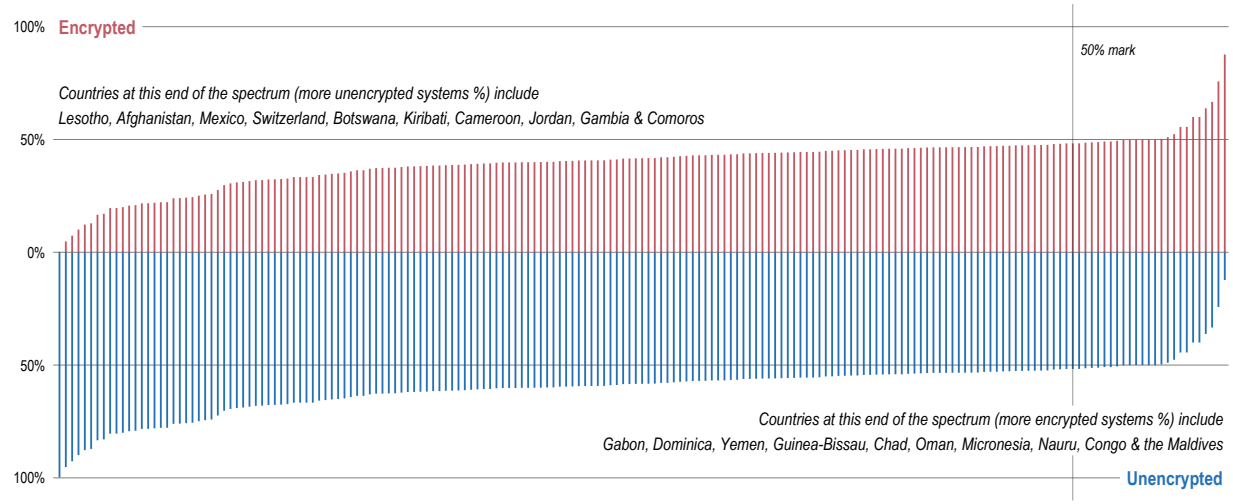
Source: Rapid7 Project Sonar Data

Most Exposed (in order)	**Least Exposed** (in order)
Guinea-Bissau	Congo
South Sudan	Maldives
Chad	Mozambique
Sao Tome and Principe	Zimbabwe
Comoros	Tajikistan

Table 4: Countries at the extreme ends of the unencrypted to encrypted SMTP service ratio.

Percentage of encrypted (port 995) and unencrypted (port 110) mail access (POP) systems

Each column is a single country with the % of encrypted systems above the y-axis and the % of unencrypted systems below the x-axis.



Source: Rapid7 Project Sonar Data

Figure 9

Most Exposed (in order)
Lesotho
Afghanistan
Mexico
Swaziland
Botswana

Least Exposed (in order)
Maldives
Congo
Micronesia, Federated States of
Oman
Chad

Table 5: Countries at the extreme ends of the unencrypted to encrypted POP3 service ratio

Percentage of encrypted (port 993) and unencrypted (port 143) mail access (IMAP) systems

Each column is a single country with the % of encrypted systems above the y-axis and the % of unencrypted systems below the x-axis.

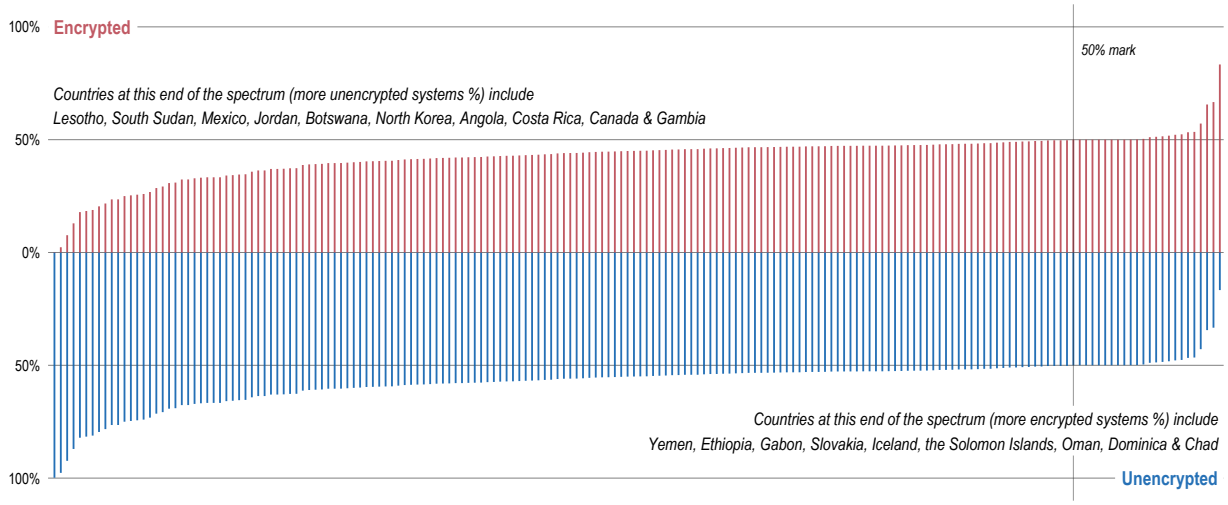


Figure 10

Source: Rapid7 Project Sonar Data

Most Exposed (in order)
Lesotho
South Sudan
Mexico
Jordan
Botswana

Least Exposed (in order)
Chad
Dominica
Oman
Solomon Islands
Iceland

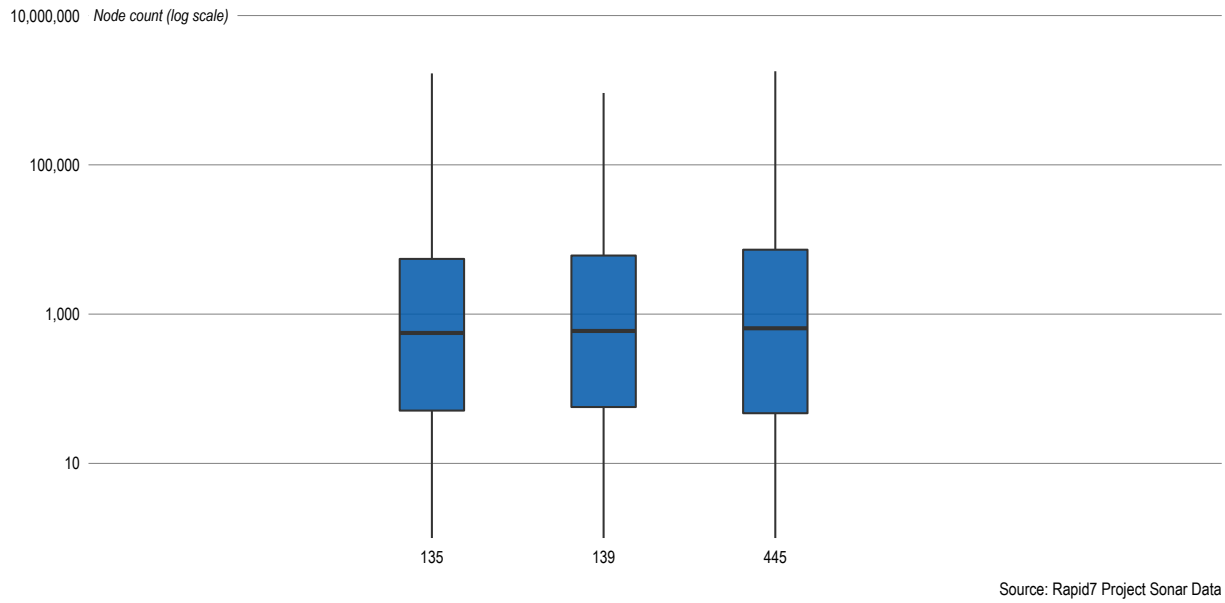
Table 6: Countries at the extreme ends of the unencrypted to encrypted IMAP service ratio

Microsoft Protocols

The set of protocols that make up NetBios and SMB/CIFS (ports 135/TCP, 139/TCP, and 445/TCP, among others) are usually associated with Microsoft Windows operating systems running on servers, desktop PCs, and laptops (While other operating systems may also expose these ports, it is would seem unlikely those servers would be directly addressable over the internet. Apple MacOS servers are a vanishingly small population in comparison to Microsoft Windows, and the Linux servers that are configured for Samba tend to not find themselves accidentally exposed. However, more protocol-level survey work is warranted to discern exactly how much SMB/CIFS is actually Microsoft Windows) . While recent versions of these protocols do support encryption, they tend to operate like STARTTLS where they must be negotiated as part of the protocol, and are subject to the same man-in-the-middle attacks.

Total distribution of exposed Microsoft services

Each boxplot shows the distributions of the count of number of servers per country exposing that port

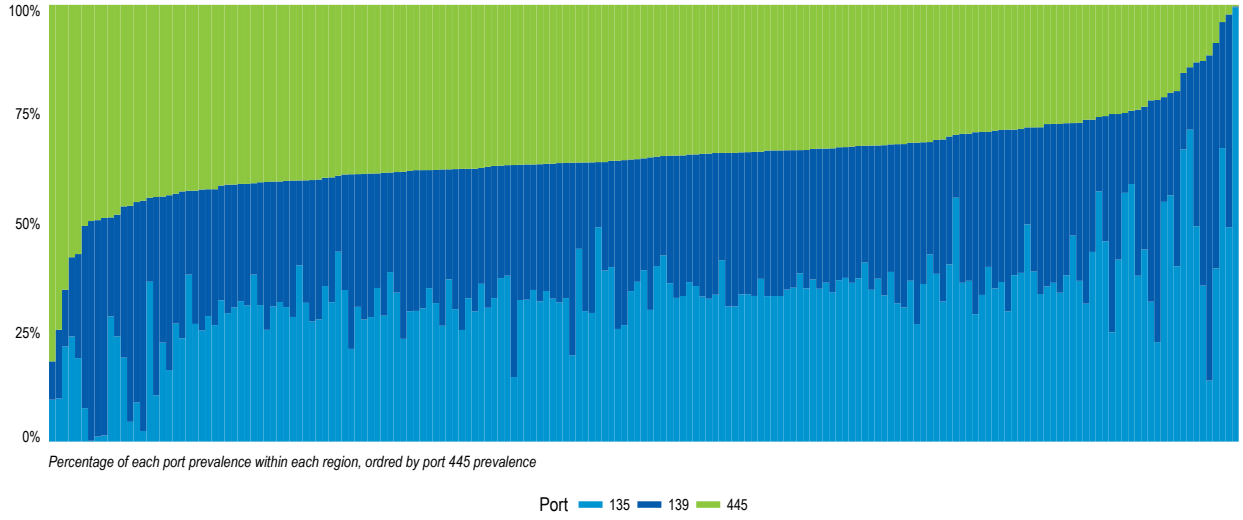


Source: Rapid7 Project Sonar Data

Figure 11

The Three (Microsoft) Amigos (Act I)

In theory, we should see ports 135 & 139 working in tandem more often than not as they (together) service 'NBT over IP' while 445 is generally self-sufficient. We can see from this chart that these port-configurations are far from uniform across all the regions.



Source: Rapid7 Project Sonar Data

Figure 12

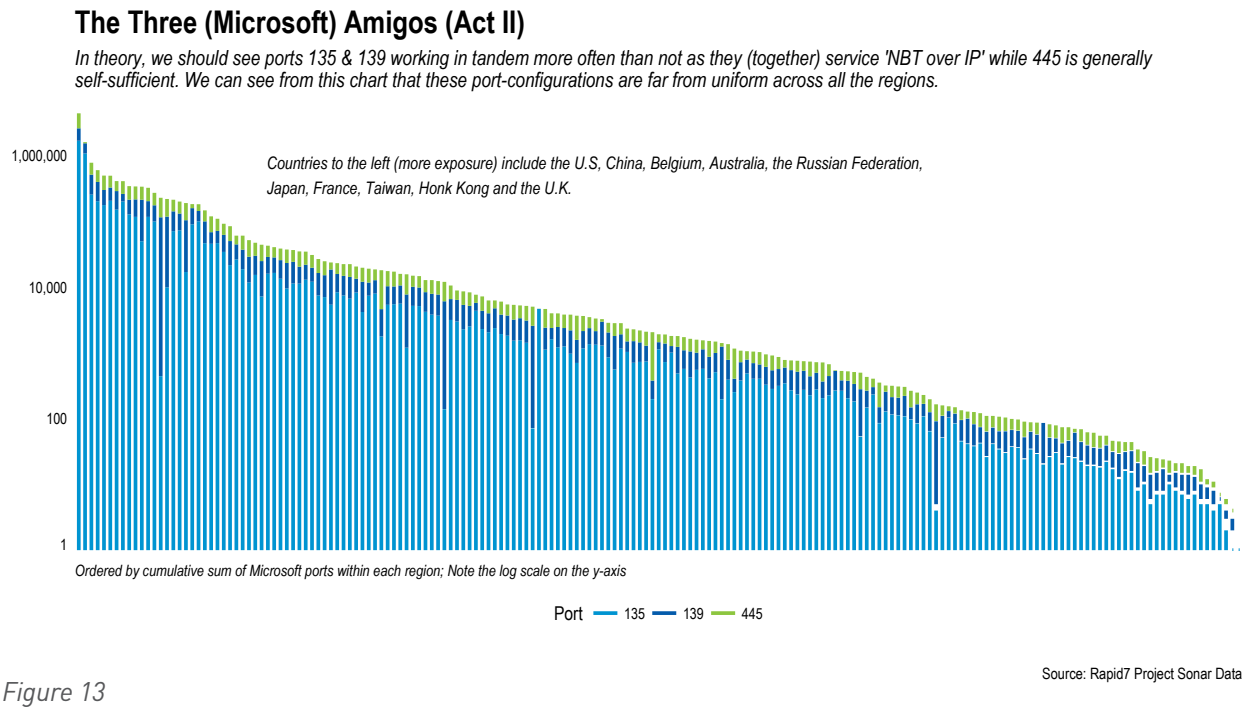


Figure 13

Most Exposed (in order)
United States
China
Belgium
Australia
Russia

Least Exposed (in order)
Timor-Leste
Bhutan
Tuvalu
Tonga
Kiribati

Table 7: Countries at the extreme ends of offering Microsoft SMB/NetBIOS services.

Database Protocols

The MySQL and Microsoft SQL Server ports of 3306 and 1433, respectively, represent a curious case. These protocols, like others mentioned above, may (but usually don't) offer encryption which must be negotiated between client and server. More importantly, though, are the risks associated with exposing direct access to database applications to the internet. Fundamentally, databases hold all the data that makes web applications interesting, notably, proprietary data. Using databases efficiently in an application's context is an entire information technology discipline unto itself, so exposing a database directly to the internet intentionally is ill-advised; there are essentially infinite ways that uninformed or malicious users can cause denial of service conditions for database servers. They also tend to contain secrets such as passwords and proprietary data. While various encryption techniques exist to protect data, ranging from individual cell encryption to entire database level encryption, encrypting database data is usually intended to protect sensitive personal information from accidental or malicious disclosure by internal users, not the internet at large.

In the days when the internet was a shared resource among a very few academic and military institutions, exposing databases and connecting directly to them across the internet made some sense. However, even in a case where encryption and strong authentication is possible, exposing a database directly to the 3.5 billion human internet population is no longer a sensible act.

We counted 7.8 million MySQL databases and 3.4 million Microsoft SQL Server systems. Six countries, the United States, China, Hong Kong, Belgium, Australia and Poland expose 75% of discovered Microsoft SQL nodes. Those same countries expose 67% of MySQL nodes.

Databases exposed on the internet represent a distinct configuration exposure that is interesting and worrying in and of itself, and we expect to cover this topic in depth in a future paper.

Ports Per Address

The more services offered by a server or device, the greater the attack surface/exposure of that server or device. Sure, you can harden a system and introduce other, compensating controls, but the base premise holds as a general rule along with the assertion that the attack surface also increases by the number of servers or devices in operation. By combining these two posits, we can paint two different pictures of exposure by region.

We counted up the number of IPv4 addresses in each region that expose between one port and thirty ports (the left axis on the heatmaps, below). It turns out that most servers run between 1 and 3 active ports—at least from the 30 we looked for (Figure 14). We then sorted the list of regions by how many of these port combinations they had. Where there were ties, we further sorted by total number of servers/devices. We used this information to create two exposure heatmaps.

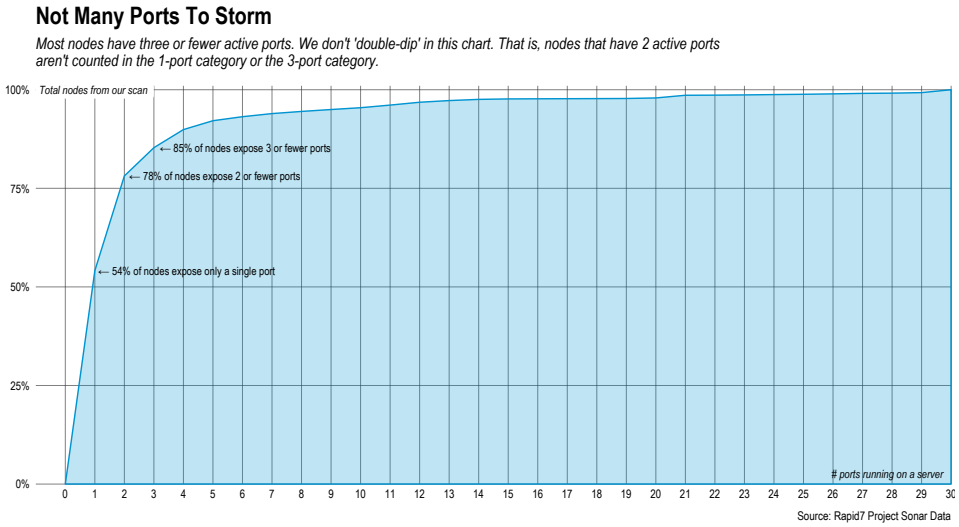


Figure 14

The heatmap in Figure 15is colored by percent of servers/devices in a country exposing the number of ports on the y-axis. For example, all the way on the left is Kiribati (population 102,000) with 198 total nodes exposed, 55.6% of which expose three ports but with five nodes exposing seven, eight, ten, twelve and 24 ports, respectively.

Conversely, the United States (all the way on the right) has a total of 43 million servers/devices exposing every port combination in the Sonar study.

The reason for providing the "percentage in country" view is to show how exposed a particular region may be relative to its overall size. If you only have 20 nodes on your internet segment and all 20 are configured with an egregious number of open ports/services, you are arguably (from one point of view) more exposed than your neighbor that has 1,000 nodes on their internet segment but only has 50 nodes exposing similar ports/services.

Looking at the heatmap, we see that most regions have the bulk of their nodes exposing between one and five ports. The large, gray void (no nodes running that number of port combinations) was encouraging since that indicates more controlled configurations in those regions.

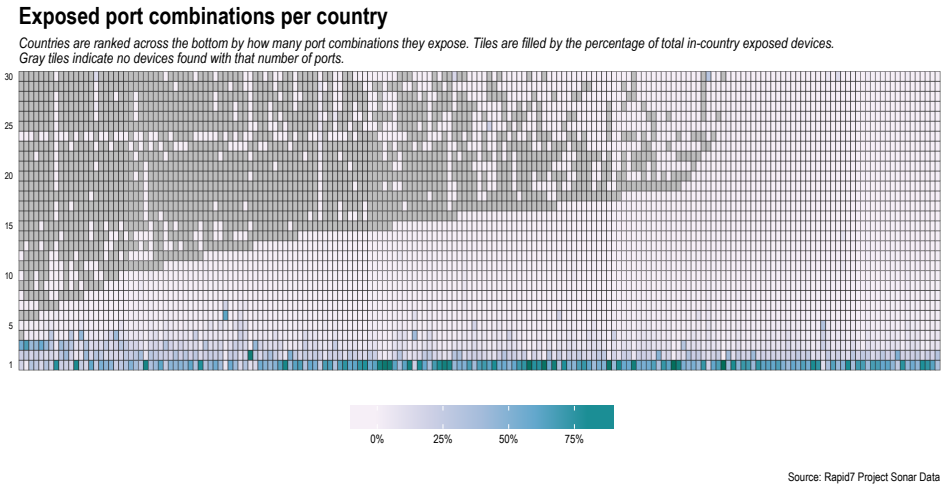


Figure 15

As we analyzed this view, some outliers and unusual patterns came to our attention[1]:

- French Polynesia has 28.3% of their systems/devices (1,700) exposing 30 ports
- Belgium has 31% of their systems/devices (216,553) exposing 30 ports
- Australia has 12% of their systems/devices (153,808) exposing 30 ports
- Qatar has 21% of their systems/devices (8,619) exposing 25 ports
- Gibraltar has 31% of their systems/devices (1,724) exposing 23 ports
- The Falkland Islands has 83% of their systems/devices (1,814) exposing 14 ports
- Lesotho has 63% of their systems/devices (3,515) exposing 6 ports
- Plus, there's a noticeable "line" across the chart at port count 24, which looks like we may have caught some Dionaea honeypots and/or port-forwarding firewalls/routers[2].

Until we add the "Clairvoyance" module to Project Sonar to determine intent, we can only show what the makeup of a region is, versus understanding why the configurations are so non-uniform.

Raw Exposure

While it's important to look at the relative exposure within a region, raw exposed counts also matter. Opportunistic attackers in need of a drop site or just in search of new targets can and will prey upon vulnerable nodes. We grabbed daily samples from the SANS Internet Storm Center[3], and averaged the number of targets on any given day (Table 8). While not comprehensive, this shows there is at least active probing occurring on all of the ports used in our Sonar study.

To see the total node volume view, we've taken the same heatmap layout in Figure 15 and used the node count for the fill color (Figure 14). We used a base 10 log scale for the fill due to the skewed nature of the port combination node count distribution (Figure 16).

Port	Mean Target Count
23	15,190
1433	9,745
445	4,406
80	3,856
3389	3,670
22	3,208
53	2,300
3306	2,032
21	1,780
8080	1,665
5900	1,438
25	1,364
443	1,246
1723	1,182
111	1,071
135	979
110	873
8888	865
8081	840
139	726
995	681
465	604
993	485
143	476
8443	473
587	393
5000	274
9100	240
990	212
389	134

Table 8: DShield-reported probes

1 Many of these smaller regions are *not* represented in most of the data in this paper, as they tend to be smaller dependencies that do not have their GDP calculated by the International Monetary Fund

2 Hat-tip to Jason Trost from Anomali for virtually instantaneously recognizing the most prevalent port configuration

3 https://www.dshield.org/

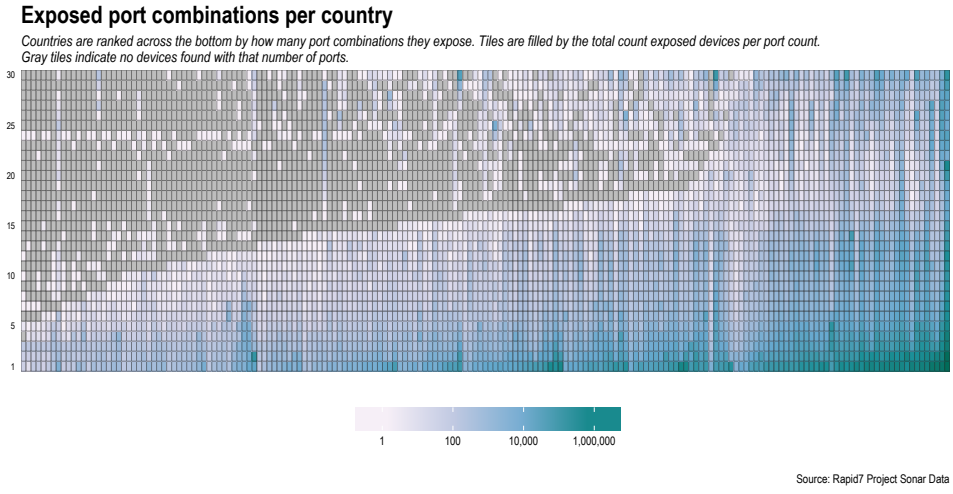


Figure 16

Region	Total Devices
United States	43,518,110
China	11,342,574
Mexico	7,853,286
Korea, Republic of	7,491,677
Germany	4,800,606
Brazil	4,198,027
Japan	3,654,163
Iran, Islamic Republic of	3,207,055
Netherlands	3,104,238
United Kingdom	3,058,560
Russian Federation	2,832,044
Taiwan, Province of China	2,803,975
India	2,494,952
Spain	2,480,065
France	2,434,588
Thailand	2,431,997
Italy	2,425,545
Canada	2,088,264
Colombia	1,744,118
Poland	1,509,083
Australia	1,319,312
Turkey	1,304,294
Hong Kong	1,051,711
Saudi Arabia	1,045,001

Region (CONT)	Total Devices
Viet Nam	968,617
Indonesia	918,427
Romania	752,802
Argentina	746,712
Sweden	740,103
Ukraine	720,259
Europe	567,305
Czech Republic	501,959
South Africa	404,439
Denmark	403,654
Austria	388,551
Hungary	335,408
Malaysia	318,846
Chile	260,802
Greece	209,586
Peru	168,699
Nigeria	102,647
Macao	39,267
Kenya	28,927
Mauritius	24,547
Satellite Provider (not a country)	9,608
Gabon	9,151

Table 9 lists the regions that have devices listening on all 30 ports. We didn't "double dip" here. If an IPv4 address only had 1 port exposed, it's only in the "1" port category (y-axis of Figure 14 above). If it had 2 ports exposed it's only in the "2" port category, and not the "1" category as well. So, for a node to be in the "30 ports exposed" category, it had to have all 30 scanned ports exposed and will not be in any other port-count category.

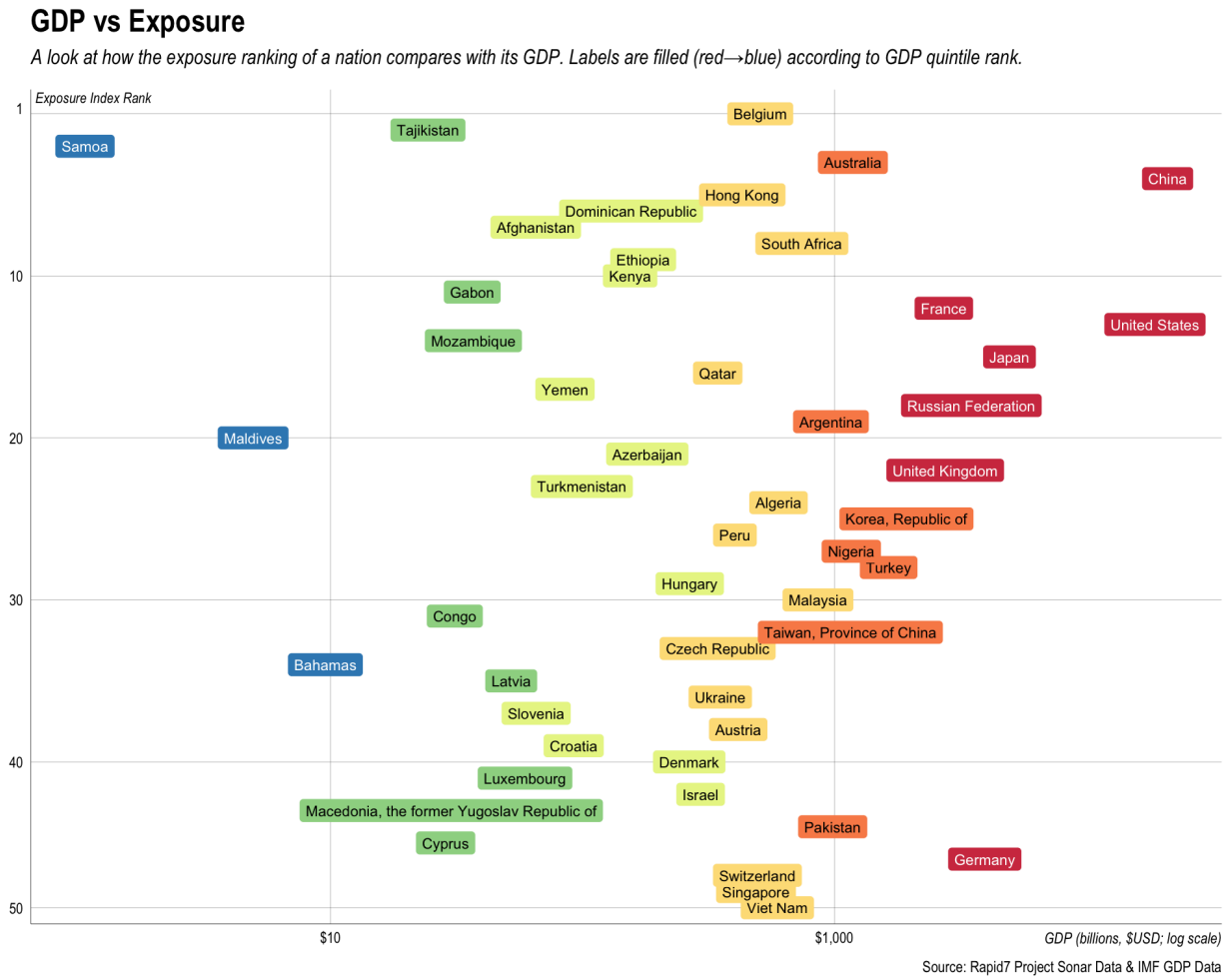
03

NATIONAL EXPOSURE INDEX

Now that we have geolocated port scan data, and have looked at the prevalence of cleartext implementations of protocols and protocol families, and looked at the exposure of several unrelated services offered by individual IP addresses, we can measure the overall exposure of individual nations when it comes to offering insecure services. The below is the National Exposure Index, which identifies the top 50 countries, from more exposed to less exposed overall:

Exposure Rank	Country
1	Belgium
2	Tajikistan
3	Samoa
4	Australia
5	China
6	Hong Kong
7	Dominican Republic
8	Afghanistan
9	South Africa
10	Ethiopia
11	Kenya
12	Gabon
13	France
14	United States
15	Mozambique
16	Japan
17	Qatar
18	Yemen
19	Russian Federation
20	Argentina
21	Maldives
22	Azerbaijan
23	United Kingdom
24	Turkmenistan
25	Algeria
26	Korea, Republic of
27	Peru
28	Nigeria
29	Turkey
30	Hungary
31	Malaysia
32	Congo
33	Taiwan, Province of China
34	Czech Republic
35	Bahamas
36	Latvia
37	Ukraine
38	Slovenia
39	Austria
40	Croatia
41	Denmark
42	Luxembourg
43	Israel
44	Macedonia
45	Pakistan
46	Cyprus
47	Germany
48	Switzerland
49	Singapore
50	Viet Nam

The chart below represents each of these nations as they rank relative to each other in terms of GDP. The order is the same as the table above on the Y-axis, while the X-axis placement of each country name is based on their GDP. Additionally, each country label is colored by their GDP rank quintile. The top 20% countries by GDP are labelled in red, the second highest quintile are orange, and so on through the bottom 20% colored blue.



The scatterplot shows there is no dominant relationship between GDP and the Exposure Index ranking of a country. This may change, however, as we refine the study methodology, look more at actual vulnerabilities and known negative outcomes and identify components of the underlying factors relating to internet growth within regions.

Appendix A expands upon this list and provides full node and port information per-region. You can find more detailed information on the overall methodology for building this report in Appendix C.

CONCLUSIONS

By surveying available services on the internet, and grouping by geolocated IP address, we can see that, in general, there is some correlation between internet connectivity and a region's overall economic strength as expressed by GDP. This relationship may or may not be causal — we cannot determine that from this single point-in-time study. Future investigations may help illustrate if changes in GDP contribute to corresponding changes in internet services offered, or vice-versa.

We can also see that in certain functional areas of the internet, there are operational preferences for encrypted services over unencrypted counterparts. For example, the prevalence of SSH instead of telnet seems to indicate that SSH is winning out in production, as system administrators clearly prefer SSH over telnet. But, there is still ample attack surface for passive monitoring of remote administration tasks that continue to rely on telnet.

Unfortunately, the imbalance between encrypted versus unencrypted services in other areas — especially in email transmission — continues to be troubling. While STARTTLS-style, opportunistic encryption is a useful defense against passive monitoring, its deployment is difficult to rely on due to the possibility of a man-in-the-middle active attack subverting the process and the inability of users to act in the face of a failure, either by default in end user mail clients or when STARTTLS failures occur between mail exchangers after the message is sent.

These results all speak to a fundamental failure in modern internet engineering. Despite calls from the Internet Architecture Board, the Internet Engineering Task Force, and virtually every security company and security advocacy organization on Earth, compulsory encryption is not a default, standard feature in internet protocol design. Cleartext protocols "just work," and security concerns are doggedly secondary.

This state of affairs cannot last for much longer without dire consequences for the world's largest economies. It is difficult to imagine a future where healthy, robust economies make *less* use of the internet, rather than more. Recall that since the internet was effectively standardized on TCP/IP in 1982, 40% of the world's population now uses the internet directly on a regular basis[1], and virtually everyone is indirectly dependent on the internet's functionality.

The internet is far too important an engine of economic growth and stability to leave to legacy, security-optional services. With the race towards an IoT-dominated future well underway, we must rethink how we design, deploy, and manage our existing infrastructure.

1 http://www.internetlivestats.com/internet-users/

APPENDIX A: THE TOP 50 EXPOSURE INDEX

Rank	Country	Total Nodes	DNS	FTP	FTPS	HTTP	http-alt0	http-alt1	http-alt8	HTTPS	https-alt
1	Belgium (BE)	8,464,783	264,024 (3.12%)	315,280 (3.72%)	262,367 (3.10%)	357,882 (4.23%)	295,665 (3.49%)	325,706 (3.85%)	266,122 (3.14%)	371,551 (4.39%)	269,582 (3.18%)
2	Tajikistan (TJ)	74,201	2,707 (3.65%)	2,908 (3.92%)	1,849 (2.49%)	3,494 (4.71%)	2,517 (3.39%)	2,566 (3.46%)	2,684 (3.62%)	3,400 (4.58%)	2,677 (3.61%)
3	China (CN)	26,354,436	884,978 (3.4%)	1,864,809 (7.1%)	324,626 (1.2%)	4,785,032 (18.2%)	799,567 (3.0%)	605,006 (2.3%)	567,611 (2.2%)	1,490,444 (5.7%)	405,195 (1.5%)
4	Australia (AU)	8,009,320	263,698 (3.29%)	322,965 (4.03%)	187,539 (2.34%)	715,007 (8.93%)	275,099 (3.43%)	206,479 (2.58%)	196,903 (2.46%)	604,832 (7.55%)	214,811 (2.68%)
5	South Africa (ZA)	1,465,326	69,678 (4.8%)	97,100 (6.6%)	22,525 (1.5%)	192,620 (13.1%)	43,094 (2.9%)	50,385 (3.4%)	21,610 (1.5%)	122,522 (8.4%)	28,226 (1.9%)
6	Samoa (WS)	10,630	728 (6.85%)	430 (4.05%)	284 (2.67%)	973 (9.15%)	322 (3.03%)	287 (2.70%)	284 (2.67%)	593 (5.58%)	288 (2.71%)
7	Dominican Republic (DO)	2,685,610	84,626 (3.15%)	132,129 (4.92%)	70,528 (2.63%)	316,688 (11.79%)	86,132 (3.21%)	71,594 (2.67%)	70,662 (2.63%)	111,052 (4.14%)	70,674 (2.63%)
8	Hong Kong (HK)	4,735,019	160,335 (3.39%)	223,392 (4.72%)	84,857 (1.79%)	531,374 (11.22%)	160,671 (3.39%)	110,940 (2.34%)	95,500 (2.02%)	261,568 (5.52%)	96,659 (2.04%)
9	Afghanistan (AF)	16,729	232 (1.4%)	632 (3.8%)	437 (2.6%)	6,300 (37.7%)	298 (1.8%)	232 (1.4%)	212 (1.3%)	983 (5.9%)	217 (1.3%)
10	Ethiopia (ET)	3,105	65 (2.1%)	39 (1.3%)	16 (0.5%)	806 (26.0%)	78 (2.5%)	33 (1.1%)	21 (0.7%)	420 (13.5%)	29 (0.9%)
11	Gabon (GA)	32,167	829 (2.6%)	994 (3.1%)	613 (1.9%)	7,325 (22.8%)	843 (2.6%)	720 (2.2%)	262 (0.8%)	4,762 (14.8%)	719 (2.2%)
12	France (FR)	8,953,383	328,064 (3.7%)	466,751 (5.2%)	92,630 (1.0%)	1,438,053 (16.1%)	333,789 (3.7%)	162,701 (1.8%)	102,700 (1.1%)	968,841 (10.8%)	144,522 (1.6%)
13	Kenya (KE)	79,860	2,768 (3.5%)	2,721 (3.4%)	759 (1.0%)	12,851 (16.1%)	5,131 (6.4%)	925 (1.2%)	848 (1.1%)	6,054 (7.6%)	1,099 (1.4%)
14	United States (US)	154,026,408	3,472,032 (2.3%)	7,823,502 (5.1%)	2,236,330 (1.5%)	24,188,773 (15.7%)	5,590,508 (3.6%)	2,948,794 (1.9%)	2,650,086 (1.7%)	24,968,357 (16.2%)	3,774,950 (2.5%)
15	Mozambique (MZ)	30,205	1,199 (4.0%)	2,316 (7.7%)	533 (1.8%)	3,777 (12.5%)	810 (2.7%)	582 (1.9%)	557 (1.8%)	2,319 (7.7%)	668 (2.2%)
16	Russian Federation (RU)	5,649,172	345,062 (6.1%)	366,626 (6.5%)	8,964 (0.2%)	1,128,121 (20.0%)	256,054 (4.5%)	46,975 (0.8%)	44,856 (0.8%)	612,333 (10.8%)	32,668 (0.6%)
17	Qatar (QA)	269,819	9,392 (3.5%)	9,716 (3.6%)	8,966 (3.3%)	16,632 (6.2%)	10,039 (3.7%)	27,160 (10.1%)	9,109 (3.4%)	16,067 (6.0%)	9,236 (3.4%)
18	Korea, Republic of (KR)	12,534,801	326,388 (2.6%)	835,644 (6.7%)	118,131 (0.9%)	2,628,764 (21.0%)	844,998 (6.7%)	149,149 (1.2%)	223,827 (1.8%)	1,206,368 (9.6%)	138,143 (1.1%)
19	Maldives (MV)	31,699	1,447 (4.6%)	1,353 (4.3%)	450 (1.4%)	4,168 (13.1%)	1,338 (4.2%)	464 (1.5%)	124 (0.4%)	1,615 (5.1%)	286 (0.9%)
20	Yemen (YE)	13,994	133 (1.0%)	3,212 (23.0%)	166 (1.2%)	983 (7.0%)	281 (2.0%)	36 (0.3%)	139 (1.0%)	929 (6.6%)	144 (1.0%)
21	Japan (JP)	13,381,433	470,945 (3.5%)	1,005,118 (7.5%)	119,078 (0.9%)	2,183,449 (16.3%)	386,939 (2.9%)	136,423 (1.0%)	129,535 (1.0%)	1,201,750 (9.0%)	161,529 (1.2%)
22	Argentina (AR)	1,366,185	92,399 (6.8%)	68,539 (5.0%)	7,620 (0.6%)	249,600 (18.3%)	121,060 (8.9%)	16,339 (1.2%)	21,425 (1.6%)	139,085 (10.2%)	10,410 (0.8%)
23	United Kingdom (GB)	8,972,665	285,618 (3.2%)	398,330 (4.4%)	74,204 (0.8%)	1,447,985 (16.1%)	284,089 (3.2%)	589,425 (6.6%)	82,040 (0.9%)	1,311,762 (14.6%)	161,023 (1.8%)
24	Azerbaijan (AZ)	76,004	4,731 (6.2%)	8,851 (11.6%)	629 (0.8%)	16,156 (21.3%)	3,379 (4.4%)	876 (1.2%)	702 (0.9%)	5,737 (7.5%)	710 (0.9%)
25	Ukraine (UA)	1,429,390	87,718 (6.1%)	84,566 (5.9%)	666 (0.0%)	320,781 (22.4%)	50,009 (3.5%)	7,490 (0.5%)	6,591 (0.5%)	173,972 (12.2%)	3,312 (0.2%)
26	Algeria (DZ)	87,575	1,860 (2.1%)	3,706 (4.2%)	1,381 (1.6%)	9,447 (10.8%)	1,774 (2.0%)	30,615 (35.0%)	1,468 (1.7%)	2,985 (3.4%)	1,486 (1.7%)
27	Malaysia (MY)	660,150	25,458 (3.9%)	42,919 (6.5%)	3,495 (0.5%)	194,567 (29.5%)	36,974 (5.6%)	5,664 (0.9%)	5,937 (0.9%)	86,934 (13.2%)	7,323 (1.1%)
28	Turkey (TR)	2,911,299	292,214 (10.0%)	148,897 (5.1%)	5,393 (0.2%)	463,755 (15.9%)	61,476 (2.1%)	537,217 (18.5%)	12,566 (0.4%)	184,305 (6.3%)	31,008 (1.1%)
29	Congo (CG)	140,014	839 (0.6%)	2,973 (2.1%)	612 (0.4%)	29,275 (20.9%)	1,700 (1.2%)	9,869 (7.0%)	2,554 (1.8%)	3,558 (2.5%)	13,098 (9.4%)
30	Latvia (LV)	251,612	12,330 (4.9%)	13,586 (5.4%)	429 (0.2%)	52,414 (20.8%)	19,233 (7.6%)	2,911 (1.2%)	1,082 (0.4%)	31,379 (12.5%)	1,232 (0.5%)
31	Mauritius (MU)	38,808	1,016 (2.6%)	1,364 (3.5%)	235 (0.6%)	13,051 (33.6%)	1,057 (2.7%)	346 (0.9%)	334 (0.9%)	6,708 (17.3%)	481 (1.2%)
32	Nigeria (NG)	168,486	3,233 (1.9%)	4,548 (2.7%)	922 (0.5%)	51,217 (30.4%)	2,365 (1.4%)	22,315 (13.2%)	980 (0.6%)	12,251 (7.3%)	1,450 (0.9%)
33	Hungary (HU)	697,893	36,914 (5.3%)	45,038 (6.5%)	2,195 (0.3%)	129,891 (18.6%)	31,742 (4.5%)	7,653 (1.1%)	5,264 (0.8%)	75,000 (10.7%)	4,850 (0.7%)
34	Bahamas (BS)	21,848	802 (3.7%)	1,165 (5.3%)	106 (0.5%)	6,759 (30.9%)	1,677 (7.7%)	327 (1.5%)	151 (0.7%)	2,623 (12.0%)	287 (1.3%)
35	Czech Republic (CZ)	1,406,756	93,886 (6.7%)	98,071 (7.0%)	4,891 (0.3%)	265,791 (18.9%)	73,267 (5.2%)	12,689 (0.9%)	13,791 (1.0%)	151,780 (10.8%)	9,811 (0.7%)
36	Macedonia (MK)	63,741	3,393 (5.3%)	3,418 (5.4%)	281 (0.4%)	18,473 (29.0%)	4,325 (6.8%)	743 (1.2%)	539 (0.8%)	7,935 (12.4%)	430 (0.7%)
37	Austria (AT)	790,526	18,914 (2.4%)	51,172 (6.5%)	2,686 (0.3%)	183,003 (23.1%)	38,894 (4.9%)	7,864 (1.0%)	4,307 (0.5%)	157,085 (19.9%)	10,412 (1.3%)
38	Slovenia (SI)	196,981	6,303 (3.2%)	10,071 (5.1%)	776 (0.4%)	35,533 (18.0%)	8,698 (4.4%)	1,796 (0.9%)	1,224 (0.6%)	51,894 (26.3%)	2,050 (1.0%)
39	Croatia (HR)	141,852	6,490 (4.6%)	9,295 (6.6%)	124 (0.1%)	22,486 (15.9%)	8,629 (6.1%)	2,973 (2.1%)	1,245 (0.9%)	17,337 (12.2%)	732 (0.5%)
40	Denmark (DK)	798,429	15,787 (2.0%)	44,352 (5.6%)	4,546 (0.6%)	260,010 (32.6%)	31,789 (4.0%)	38,671 (4.8%)	5,126 (0.6%)	115,575 (14.5%)	7,840 (1.0%)
41	Israel (IL)	643,226	14,838 (2.3%)	60,048 (9.3%)	1,390 (0.2%)	168,951 (26.3%)	19,945 (3.1%)	3,395 (0.5%)	3,441 (0.5%)	81,337 (12.6%)	8,401 (1.3%)
42	Uganda (UG)	15,657	529 (3.4%)	624 (4.0%)	62 (0.4%)	4,254 (27.2%)	475 (3.0%)	64 (0.4%)	83 (0.5%)	1,618 (10.3%)	185 (1.2%)
43	Djibouti (DJ)	1,245	31 (2.5%)	14 (1.1%)	2 (0.2%)	289 (23.2%)	19 (1.5%)	2 (0.2%)	1 (0.1%)	270 (21.7%)	4 (0.3%)
44	Portugal (PT)	487,611	18,252 (3.7%)	22,080 (4.5%)	345 (0.1%)	91,501 (18.8%)	16,826 (3.5%)	51,306 (10.5%)	2,696 (0.6%)	64,407 (13.2%)	9,517 (2.0%)
45	Cyprus (CY)	78,151	2,511 (3.2%)	4,655 (6.0%)	110 (0.1%)	16,618 (21.3%)	3,292 (4.2%)	410 (0.5%)	320 (0.4%)	10,417 (13.3%)	1,718 (2.2%)
46	Mauritania (MR)	1,807	63 (3.5%)	106 (5.9%)	1 (0.1%)	476 (26.3%)	24 (1.3%)	9 (0.5%)	4 (0.2%)	252 (13.9%)	8 (0.4%)
47	Viet Nam (VN)	1,552,545	341,976 (22.0%)	77,659 (5.0%)	654 (0.0%)	325,482 (21.0%)	75,583 (4.9%)	6,419 (0.4%)	25,844 (1.7%)	142,229 (9.2%)	4,765 (0.3%)
48	Bulgaria (BG)	863,198	56,676 (6.6%)	43,187 (5.0%)	523 (0.1%)	201,503 (23.3%)	86,259 (10.0%)	6,890 (0.8%)	3,290 (0.4%)	82,558 (9.6%)	3,847 (0.4%)
49	Singapore (SG)	1,404,889	31,457 (2.2%)	56,667 (4.0%)	2,622 (0.2%)	345,408 (24.6%)	40,385 (2.9%)	14,854 (1.1%)	6,565 (0.5%)	261,514 (18.6%)	15,251 (1.1%)
50	South Sudan (SS)	2,842	5 (0.2%)	45 (1.6%)	16 (0.6%)	1,780 (62.6%)	56 (2.0%)	22 (0.8%)	11 (0.4%)	137 (4.8%)	13 (0.5%)

Rank	Country	IMAP	IMAPS	jetdirect	LDAP	MS-RPC	MSSQL	MySQL	NBSS	POP3	POP3S
1	Belgium (BE)	265,348 (3.13%)	277,284 (3.28%)	266,716 (3.15%)	253,438 (2.99%)	254,699 (3.01%)	274,015 (3.24%)	265,743 (3.14%)	258,597 (3.05%)	263,586 (3.11%)	263,351 (3.11%)
2	Tajikistan (TJ)	2,159 (2.91%)	1,713 (2.31%)	2,663 (3.59%)	2,156 (2.91%)	2,302 (3.10%)	2,040 (2.75%)	1,832 (2.47%)	2,063 (2.78%)	2,707 (3.65%)	2,059 (2.77%)
3	China (CN)	361,059 (1.4%)	339,123 (1.3%)	328,782 (1.2%)	320,894 (1.2%)	1,075,745 (4.1%)	622,378 (2.4%)	1,079,022 (4.1%)	461,879 (1.8%)	454,806 (1.7%)	337,560 (1.3%)
4	Australia (AU)	250,389 (3.13%)	240,891 (3.01%)	192,029 (2.40%)	190,439 (2.38%)	202,306 (2.53%)	188,649 (2.36%)	216,080 (2.70%)	195,249 (2.44%)	252,320 (3.15%)	235,675 (2.94%)
5	South Africa (ZA)	37,667 (2.6%)	38,202 (2.6%)	22,862 (1.6%)	19,402 (1.3%)	34,286 (2.3%)	21,904 (1.5%)	34,126 (2.3%)	28,019 (1.9%)	41,666 (2.8%)	37,558 (2.6%)
6	Samoa (WS)	304 (2.86%)	304 (2.86%)	284 (2.67%)	285 (2.68%)	226 (2.13%)	283 (2.66%)	290 (2.73%)	218 (2.05%)	314 (2.95%)	303 (2.85%)
7	Dominican Republic (DO)	70,576 (2.63%)	70,678 (2.63%)	70,572 (2.63%)	70,583 (2.63%)	70,971 (2.64%)	70,891 (2.64%)	70,681 (2.63%)	70,990 (2.64%)	70,686 (2.63%)	70,640 (2.63%)
8	Hong Kong (HK)	171,874 (3.63%)	101,070 (2.13%)	88,108 (1.86%)	86,543 (1.83%)	127,443 (2.69%)	333,230 (7.04%)	197,045 (4.16%)	86,396 (1.82%)	113,620 (2.40%)	102,482 (2.16%)
9	Afghanistan (AF)	14 (0.1%)	12 (0.1%)	303 (1.8%)	234 (1.4%)	485 (2.9%)	249 (1.5%)	261 (1.6%)	748 (4.5%)	178 (1.1%)	9 (0.1%)
10	Ethiopia (ET)	33 (1.1%)	36 (1.2%)	24 (0.8%)	34 (1.1%)	112 (3.6%)	50 (1.6%)	50 (1.6%)	96 (3.1%)	40 (1.3%)	32 (1.0%)
11	Gabon (GA)	692 (2.2%)	761 (2.4%)	404 (1.3%)	724 (2.3%)	551 (1.7%)	465 (1.4%)	702 (2.2%)	456 (1.4%)	708 (2.2%)	778 (2.4%)
12	France (FR)	284,990 (3.2%)	257,229 (2.9%)	86,725 (1.0%)	93,682 (1.0%)	150,695 (1.7%)	90,478 (1.0%)	232,024 (2.6%)	137,803 (1.5%)	286,935 (3.2%)	250,656 (2.8%)
13	Kenya (KE)	2,207 (2.8%)	1,965 (2.5%)	666 (0.8%)	1,039 (1.3%)	2,380 (3.0%)	1,015 (1.3%)	1,395 (1.7%)	2,382 (3.0%)	2,443 (3.1%)	1,875 (2.3%)
14	United States (US)	5,932,850 (3.9%)	4,119,321 (2.7%)	2,697,880 (1.8%)	2,990,761 (1.9%)	1,679,225 (1.1%)	991,957 (0.6%)	3,162,867 (2.1%)	918,154 (0.6%)	5,531,186 (3.6%)	5,001,682 (3.2%)
15	Mozambique (MZ)	771 (2.6%)	633 (2.1%)	540 (1.8%)	603 (2.0%)	277 (0.9%)	555 (1.8%)	603 (2.0%)	221 (0.7%)	842 (2.8%)	629 (2.1%)
16	Russian Federation (RU)	112,447 (2.0%)	95,043 (1.7%)	19,043 (0.3%)	13,553 (0.2%)	176,725 (3.1%)	13,037 (0.2%)	154,359 (2.7%)	122,975 (2.2%)	119,521 (2.1%)	91,877 (1.6%)
17	Qatar (QA)	9,287 (3.4%)	9,072 (3.4%)	8,985 (3.3%)	9,000 (3.3%)	267 (0.1%)	387 (0.1%)	9,267 (3.4%)	265 (0.1%)	9,070 (3.4%)	9,035 (3.3%)
18	Korea, Republic of (KR)	539,211 (4.3%)	121,473 (1.0%)	124,636 (1.0%)	118,885 (0.9%)	90,100 (0.7%)	85,723 (0.7%)	194,808 (1.6%)	68,615 (0.5%)	170,873 (1.4%)	124,361 (1.0%)
19	Maldives (MV)	2,108 (6.7%)	1,890 (6.0%)	255 (0.8%)	210 (0.7%)	1,293 (4.1%)	2,065 (6.5%)	221 (0.7%)	1,682 (5.3%)	284 (0.9%)	2,023 (6.4%)
20	Yemen (YE)	149 (1.1%)	160 (1.1%)	143 (1.0%)	149 (1.1%)	403 (2.9%)	174 (1.2%)	157 (1.1%)	263 (1.9%)	127 (0.9%)	159 (1.1%)
21	Japan (JP)	614,651 (4.6%)	419,049 (3.1%)	116,774 (0.9%)	117,855 (0.9%)	205,266 (1.5%)	81,143 (0.6%)	257,290 (1.9%)	121,387 (0.9%)	897,709 (6.7%)	535,018 (4.0%)
22	Argentina (AR)	16,301 (1.2%)	13,492 (1.0%)	8,804 (0.6%)	7,875 (0.6%)	9,924 (0.7%)	12,562 (0.9%)	14,942 (1.1%)	108,197 (7.9%)	16,987 (1.2%)	13,518 (1.0%)
23	United Kingdom (GB)	260,128 (2.9%)	219,825 (2.4%)	75,198 (0.8%)	76,583 (0.9%)	116,932 (1.3%)	75,142 (0.8%)	247,920 (2.8%)	98,814 (1.1%)	250,579 (2.8%)	206,696 (2.3%)
24	Azerbaijan (AZ)	1,333 (1.8%)	1,293 (1.7%)	622 (0.8%)	742 (1.0%)	1,823 (2.4%)	808 (1.1%)	913 (1.2%)	1,874 (2.5%)	1,411 (1.9%)	1,225 (1.6%)
25	Ukraine (UA)	24,120 (1.7%)	22,208 (1.6%)	2,605 (0.2%)	1,642 (0.1%)	45,545 (3.2%)	1,650 (0.1%)	40,901 (2.9%)	22,855 (1.6%)	26,270 (1.8%)	21,723 (1.5%)
26	Algeria (DZ)	1,534 (1.8%)	1,514 (1.7%)	1,363 (1.6%)	1,425 (1.6%)	198 (0.2%)	1,412 (1.6%)	1,486 (1.7%)	181 (0.2%)	1,554 (1.8%)	1,500 (1.7%)
27	Malaysia (MY)	14,250 (2.2%)	11,019 (1.7%)	2,756 (0.4%)	2,605 (0.4%)	8,264 (1.3%)	4,087 (0.6%)	12,106 (1.8%)	5,152 (0.8%)	15,398 (2.3%)	10,957 (1.7%)
28	Turkey (TR)	87,498 (3.0%)	63,141 (2.2%)	7,580 (0.3%)	9,837 (0.3%)	46,631 (1.6%)	28,218 (1.0%)	66,025 (2.3%)	24,928 (0.9%)	92,602 (3.2%)	63,732 (2.2%)
29	Congo (CG)	2,695 (1.9%)	2,186 (1.6%)	720 (0.5%)	2,580 (1.8%)	1,783 (1.3%)	2,095 (1.5%)	1,374 (1.0%)	2,840 (2.0%)	912 (0.7%)	2,849 (2.0%)
30	Latvia (LV)	6,287 (2.5%)	5,518 (2.2%)	526 (0.2%)	671 (0.3%)	3,813 (1.5%)	887 (0.4%)	3,948 (1.6%)	4,104 (1.6%)	5,865 (2.3%)	5,333 (2.1%)
31	Mauritius (MU)	404 (1.0%)	368 (0.9%)	236 (0.6%)	311 (0.8%)	508 (1.3%)	280 (0.7%)	359 (0.9%)	489 (1.3%)	441 (1.1%)	372 (1.0%)
32	Nigeria (NG)	737 (0.4%)	389 (0.2%)	895 (0.5%)	1,984 (1.2%)	3,002 (1.8%)	1,830 (1.1%)	1,840 (1.1%)	3,393 (2.0%)	1,080 (0.6%)	498 (0.3%)
33	Hungary (HU)	13,434 (1.9%)	12,814 (1.8%)	2,636 (0.4%)	3,096 (0.4%)	11,288 (1.6%)	2,482 (0.4%)	9,202 (1.3%)	9,166 (1.3%)	13,527 (1.9%)	11,054 (1.6%)
34	Bahamas (BS)	327 (1.5%)	240 (1.1%)	120 (0.5%)	156 (0.7%)	30 (0.1%)	142 (0.6%)	245 (1.1%)	34 (0.2%)	335 (1.5%)	224 (1.0%)
35	Czech Republic (CZ)	31,661 (2.3%)	31,325 (2.2%)	4,452 (0.3%)	5,658 (0.4%)	15,324 (1.1%)	5,457 (0.4%)	25,107 (1.8%)	14,628 (1.0%)	30,976 (2.2%)	27,013 (1.9%)
36	Macedonia (MK)	577 (0.9%)	513 (0.8%)	301 (0.5%)	355 (0.6%)	1,160 (1.8%)	851 (1.3%)	648 (1.0%)	757 (1.2%)	591 (0.9%)	496 (0.8%)
37	Austria (AT)	15,357 (1.9%)	11,538 (1.5%)	2,865 (0.4%)	3,324 (0.4%)	6,676 (0.8%)	2,659 (0.3%)	8,769 (1.1%)	7,606 (1.0%)	16,214 (2.1%)	9,059 (1.1%)
38	Slovenia (SI)	4,339 (2.2%)	4,079 (2.1%)	902 (0.5%)	834 (0.4%)	571 (0.3%)	1,231 (0.6%)	2,922 (1.5%)	561 (0.3%)	4,365 (2.2%)	3,707 (1.9%)
39	Croatia (HR)	2,940 (2.1%)	2,364 (1.7%)	380 (0.3%)	522 (0.4%)	1,932 (1.4%)	995 (0.7%)	2,285 (1.6%)	1,889 (1.3%)	2,744 (1.9%)	2,208 (1.6%)
40	Denmark (DK)	10,621 (1.3%)	9,522 (1.2%)	5,320 (0.7%)	4,593 (0.6%)	7,045 (0.9%)	5,008 (0.6%)	9,709 (1.2%)	8,119 (1.0%)	10,445 (1.3%)	8,362 (1.0%)
41	Israel (IL)	14,614 (2.3%)	9,593 (1.5%)	2,723 (0.4%)	1,996 (0.3%)	9,529 (1.5%)	4,674 (0.7%)	3,956 (0.6%)	13,748 (2.1%)	17,002 (2.6%)	11,389 (1.8%)
42	Uganda (UG)	204 (1.3%)	180 (1.1%)	50 (0.3%)	115 (0.7%)	269 (1.7%)	89 (0.6%)	149 (1.0%)	277 (1.8%)	268 (1.7%)	184 (1.2%)
43	Djibouti (DJ)	11 (0.9%)	8 (0.6%)	1 (0.1%)	10 (0.8%)	18 (1.4%)	7 (0.6%)	15 (1.2%)	17 (1.4%)	11 (0.9%)	9 (0.7%)
44	Portugal (PT)	11,874 (2.4%)	10,114 (2.1%)	545 (0.1%)	1,135 (0.2%)	5,379 (1.1%)	2,189 (0.4%)	8,196 (1.7%)	4,931 (1.0%)	11,949 (2.5%)	9,919 (2.0%)
45	Cyprus (CY)	2,088 (2.7%)	835 (1.1%)	1,771 (2.3%)	157 (0.2%)	854 (1.1%)	322 (0.4%)	1,031 (1.3%)	1,191 (1.5%)	2,211 (2.8%)	741 (0.9%)
46	Mauritania (MR)	18 (1.0%)	12 (0.7%)	3 (0.2%)	15 (0.8%)	24 (1.3%)	3 (0.2%)	10 (0.6%)	28 (1.5%)	25 (1.4%)	11 (0.6%)
47	Viet Nam (VN)	18,487 (1.2%)	15,415 (1.0%)	664 (0.0%)	2,117 (0.1%)	15,981 (1.0%)	8,437 (0.5%)	16,878 (1.1%)	12,761 (0.8%)	20,915 (1.3%)	15,780 (1.0%)
48	Bulgaria (BG)	26,233 (3.0%)	25,386 (2.9%)	733 (0.1%)	954 (0.1%)	7,958 (0.9%)	4,521 (0.5%)	18,342 (2.1%)	4,782 (0.6%)	26,136 (3.0%)	23,700 (2.7%)
49	Singapore (SG)	26,874 (1.9%)	24,041 (1.7%)	4,121 (0.3%)	4,125 (0.3%)	12,961 (0.9%)	7,139 (0.5%)	46,291 (3.3%)	8,913 (0.6%)	27,875 (2.0%)	23,642 (1.7%)
50	South Sudan (SS)	42 (1.5%)	1 (0.0%)	9 (0.3%)	24 (0.8%)	34 (1.2%)	17 (0.6%)	29 (1.0%)	29 (1.0%)	36 (1.3%)	32 (1.1%)

Rank	Country	PPTP	RDP	RFB	rpcbind	SMB-CIFS	SMTP	SMTP-sub	SMTPS	SSH	telnet	uPNP
1	Belgium (BE)	306,058 (3.62%)	277,836 (3.28%)	265,684 (3.14%)	258,180 (3.05%)	265,242 (3.13%)	294,878 (3.48%)	273,362 (3.23%)	268,675 (3.17%)	312,991 (3.70%)	290,426 (3.43%)	280,495 (3.31%)
2	Tajikistan (TJ)	2,930 (3.95%)	2,498 (3.37%)	1,891 (2.55%)	1,948 (2.63%)	2,851 (3.84%)	2,497 (3.37%)	1,539 (2.07%)	2,547 (3.43%)	3,526 (4.75%)	2,807 (3.78%)	2,671 (3.60%)
3	China (CN)	680,491 (2.6%)	1,019,021 (3.9%)	339,392 (1.3%)	476,319 (1.8%)	63,168 (0.2%)	466,881 (1.8%)	331,761 (1.3%)	338,515 (1.3%)	1,717,366 (6.5%)	3,340,828 (12.7%)	472,178 (1.8%)
4	Australia (AU)	284,054 (3.55%)	274,427 (3.43%)	199,419 (2.49%)	194,176 (2.42%)	202,730 (2.53%)	329,947 (4.12%)	237,546 (2.97%)	241,840 (3.02%)	372,971 (4.66%)	256,774 (3.21%)	264,076 (3.30%)
5	South Africa (ZA)	50,014 (3.4%)	53,595 (3.7%)	25,900 (1.8%)	26,757 (1.8%)	29,594 (2.0%)	57,485 (3.9%)	38,693 (2.6%)	33,157 (2.3%)	96,731 (6.6%)	66,892 (4.6%)	23,056 (1.6%)
6	Samoa (WS)	431 (4.05%)	307 (2.89%)	299 (2.81%)	295 (2.78%)	228 (2.14%)	344 (3.24%)	293 (2.76%)	291 (2.74%)	471 (4.43%)	387 (3.64%)	284 (2.67%)
7	Dominican Republic (DO)	71,919 (2.68%)	72,620 (2.70%)	70,647 (2.63%)	70,706 (2.63%)	71,094 (2.65%)	71,069 (2.65%)	70,611 (2.63%)	70,614 (2.63%)	83,242 (3.10%)	240,795 (8.97%)	70,940 (2.64%)
8	Hong Kong (HK)	266,519 (5.63%)	157,650 (3.33%)	91,182 (1.93%)	107,413 (2.27%)	129,228 (2.73%)	138,944 (2.93%)	98,632 (2.08%)	98,206 (2.07%)	212,543 (4.49%)	197,059 (4.16%)	104,536 (2.21%)
9	Afghanistan (AF)	507 (3.0%)	323 (1.9%)	386 (2.3%)	439 (2.6%)	569 (3.4%)	66 (0.4%)	86 (0.5%)	9 (0.1%)	848 (5.1%)	1,277 (7.6%)	183 (1.1%)
10	Ethiopia (ET)	156 (5.0%)	122 (3.9%)	26 (0.8%)	37 (1.2%)	100 (3.2%)	97 (3.1%)	29 (0.9%)	24 (0.8%)	189 (6.1%)	291 (9.4%)	20 (0.6%)
11	Gabon (GA)	841 (2.6%)	860 (2.7%)	547 (1.7%)	679 (2.1%)	580 (1.8%)	749 (2.3%)	539 (1.7%)	748 (2.3%)	1,529 (4.8%)	1,087 (3.4%)	700 (2.2%)
12	France (FR)	207,088 (2.3%)	218,782 (2.4%)	107,396 (1.2%)	192,912 (2.2%)	120,766 (1.3%)	440,685 (4.9%)	232,416 (2.6%)	217,586 (2.4%)	812,564 (9.1%)	348,545 (3.9%)	145,375 (1.6%)
13	Kenya (KE)	2,010 (2.5%)	2,710 (3.4%)	998 (1.2%)	1,337 (1.7%)	1,505 (1.9%)	2,933 (3.7%)	1,241 (1.6%)	934 (1.2%)	6,302 (7.9%)	8,551 (10.7%)	816 (1.0%)
14	United States (US)	1,703,083 (1.1%)	4,044,271 (2.6%)	3,242,457 (2.1%)	4,338,529 (2.8%)	1,793,759 (1.2%)	6,362,237 (4.1%)	4,174,042 (2.7%)	4,817,189 (3.1%)	8,508,072 (5.5%)	3,175,010 (2.1%)	1,188,544 (0.8%)
15	Mozambique (MZ)	1,001 (3.3%)	1,114 (3.7%)	582 (1.9%)	602 (2.0%)	223 (0.7%)	568 (1.9%)	654 (2.2%)	616 (2.0%)	3,870 (12.8%)	1,922 (6.4%)	618 (2.0%)
16	Russian Federation (RU)	165,624 (2.9%)	116,723 (2.1%)	21,203 (0.4%)	151,001 (2.7%)	196,472 (3.5%)	245,103 (4.3%)	83,549 (1.5%)	83,573 (1.5%)	504,945 (8.9%)	294,205 (5.2%)	26,535 (0.5%)
17	Qatar (QA)	9,639 (3.6%)	10,038 (3.7%)	9,029 (3.3%)	378 (0.1%)	12 (0.0%)	9,537 (3.5%)	9,147 (3.4%)	9,098 (3.4%)	10,857 (4.0%)	11,793 (4.4%)	9,339 (3.5%)
18	Korea, Republic of (KR)	516,676 (4.1%)	229,717 (1.8%)	166,364 (1.3%)	639,591 (5.1%)	24,079 (0.2%)	484,970 (3.9%)	128,035 (1.0%)	126,371 (1.0%)	238,208 (1.9%)	1,024,663 (8.2%)	846,030 (6.7%)
19	Maldives (MV)	2,183 (6.9%)	330 (1.0%)	407 (1.3%)	373 (1.2%)	285 (0.9%)	263 (0.8%)	271 (0.9%)	464 (1.5%)	2,160 (6.8%)	1,540 (4.9%)	147 (0.5%)
20	Yemen (YE)	1,312 (9.4%)	417 (3.0%)	166 (1.2%)	187 (1.3%)	361 (2.6%)	164 (1.2%)	170 (1.2%)	119 (0.9%)	832 (5.9%)	2,213 (15.8%)	146 (1.0%)
21	Japan (JP)	297,109 (2.2%)	175,699 (1.3%)	143,369 (1.1%)	224,630 (1.7%)	167,617 (1.3%)	1,162,553 (8.7%)	652,485 (4.9%)	299,588 (2.2%)	622,006 (4.6%)	336,242 (2.5%)	139,227 (1.0%)
22	Argentina (AR)	31,177 (2.3%)	27,419 (2.0%)	12,405 (0.9%)	11,543 (0.8%)	100,644 (7.4%)	23,650 (1.7%)	15,513 (1.1%)	12,425 (0.9%)	88,984 (6.5%)	75,187 (5.5%)	18,159 (1.3%)
23	United Kingdom (GB)	433,529 (4.8%)	228,824 (2.6%)	82,492 (0.9%)	113,975 (1.3%)	123,463 (1.4%)	465,833 (5.2%)	209,033 (2.3%)	217,597 (2.4%)	533,194 (5.9%)	211,440 (2.4%)	90,992 (1.0%)
24	Azerbaijan (AZ)	1,971 (2.6%)	2,236 (2.9%)	717 (0.9%)	1,169 (1.5%)	1,751 (2.3%)	1,838 (2.4%)	1,232 (1.6%)	1,176 (1.5%)	4,283 (5.6%)	4,907 (6.5%)	909 (1.2%)
25	Ukraine (UA)	36,174 (2.5%)	21,883 (1.5%)	3,207 (0.2%)	21,192 (1.5%)	50,691 (3.5%)	84,892 (5.9%)	18,014 (1.3%)	19,195 (1.3%)	139,388 (9.8%)	84,033 (5.9%)	6,097 (0.4%)
26	Algeria (DZ)	1,836 (2.1%)	1,629 (1.9%)	1,406 (1.6%)	1,533 (1.8%)	1,684 (1.9%)	1,824 (2.1%)	1,500 (1.7%)	1,500 (1.7%)	2,791 (3.2%)	3,439 (3.9%)	1,544 (1.8%)
27	Malaysia (MY)	10,214 (1.5%)	21,148 (3.2%)	6,716 (1.0%)	6,073 (0.9%)	7,148 (1.1%)	19,503 (3.0%)	11,268 (1.7%)	10,976 (1.7%)	27,455 (4.2%)	29,298 (4.4%)	14,486 (2.2%)
28	Turkey (TR)	31,483 (1.1%)	67,791 (2.3%)	11,347 (0.4%)	34,191 (1.2%)	37,883 (1.3%)	130,360 (4.5%)	77,491 (2.7%)	60,303 (2.1%)	82,113 (2.8%)	128,320 (4.4%)	22,994 (0.8%)
29	Congo (CG)	11,687 (8.3%)	3,426 (2.4%)	3,735 (2.7%)	570 (0.4%)	13,426 (9.6%)	897 (0.6%)	1,089 (0.8%)	12,733 (9.1%)	5,436 (3.9%)	1,693 (1.2%)	810 (0.6%)
30	Latvia (LV)	8,059 (3.2%)	6,379 (2.5%)	1,622 (0.6%)	7,181 (2.9%)	4,858 (1.9%)	10,132 (4.0%)	4,403 (1.7%)	4,362 (1.7%)	22,807 (9.1%)	9,199 (3.7%)	1,062 (0.4%)
31	Mauritius (MU)	704 (1.8%)	1,077 (2.8%)	318 (0.8%)	344 (0.9%)	488 (1.3%)	795 (2.0%)	394 (1.0%)	346 (0.9%)	2,349 (6.1%)	3,241 (8.4%)	392 (1.0%)
32	Nigeria (NG)	2,177 (1.3%)	3,451 (2.0%)	1,400 (0.8%)	1,124 (0.7%)	2,491 (1.5%)	13,637 (8.1%)	12,518 (7.4%)	339 (0.2%)	7,636 (4.5%)	7,737 (4.6%)	1,047 (0.6%)
33	Hungary (HU)	23,267 (3.3%)	17,099 (2.5%)	4,839 (0.7%)	10,928 (1.6%)	14,434 (2.1%)	94,324 (13.5%)	9,816 (1.4%)	9,849 (1.4%)	47,413 (6.8%)	28,736 (4.1%)	9,942 (1.4%)
34	Bahamas (BS)	590 (2.7%)	772 (3.5%)	184 (0.8%)	236 (1.1%)	40 (0.2%)	643 (2.9%)	221 (1.0%)	263 (1.2%)	1,111 (5.1%)	1,726 (7.9%)	312 (1.4%)
35	Czech Republic (CZ)	45,816 (3.3%)	40,766 (2.9%)	10,264 (0.7%)	22,045 (1.6%)	17,301 (1.2%)	67,977 (4.8%)	18,816 (1.3%)	27,871 (2.0%)	161,066 (11.4%)	66,318 (4.7%)	12,938 (0.9%)
36	Macedonia (MK)	1,728 (2.7%)	2,007 (3.1%)	389 (0.6%)	537 (0.8%)	913 (1.4%)	954 (1.5%)	471 (0.7%)	424 (0.7%)	3,868 (6.1%)	5,869 (9.2%)	795 (1.2%)
37	Austria (AT)	34,892 (4.4%)	20,536 (2.6%)	5,818 (0.7%)	8,874 (1.1%)	8,066 (1.0%)	42,081 (5.3%)	11,909 (1.5%)	11,842 (1.5%)	56,012 (7.1%)	23,137 (2.9%)	8,955 (1.1%)
38	Slovenia (SI)	9,705 (4.9%)	8,049 (4.1%)	1,545 (0.8%)	1,772 (0.9%)	419 (0.2%)	8,356 (4.2%)	3,662 (1.9%)	3,783 (1.9%)	11,396 (5.8%)	4,444 (2.3%)	1,994 (1.0%)
39	Croatia (HR)	9,011 (6.4%)	7,121 (5.0%)	1,055 (0.7%)	1,048 (0.7%)	2,196 (1.5%)	4,509 (3.2%)	2,106 (1.5%)	2,332 (1.6%)	10,524 (7.4%)	13,435 (9.5%)	945 (0.7%)
40	Denmark (DK)	24,461 (3.1%)	19,478 (2.4%)	5,824 (0.7%)	9,337 (1.2%)	9,548 (1.2%)	27,307 (3.4%)	10,741 (1.3%)	8,741 (1.1%)	47,910 (6.0%)	20,069 (2.5%)	12,573 (1.6%)
41	Israel (IL)	10,233 (1.6%)	14,528 (2.3%)	3,311 (0.5%)	5,527 (0.9%)	14,003 (2.2%)	29,865 (4.6%)	7,751 (1.2%)	7,103 (1.1%)	29,490 (4.6%)	65,402 (10.2%)	5,043 (0.8%)
42	Uganda (UG)	302 (1.9%)	430 (2.7%)	80 (0.5%)	151 (1.0%)	221 (1.4%)	435 (2.8%)	157 (1.0%)	136 (0.9%)	1,968 (12.6%)	2,006 (12.8%)	92 (0.6%)
43	Djibouti (DJ)	124 (10.0%)	29 (2.3%)	4 (0.3%)	21 (1.7%)	20 (1.6%)	27 (2.2%)	10 (0.8%)	4 (0.3%)	93 (7.5%)	171 (13.7%)	3 (0.2%)
44	Portugal (PT)	26,393 (5.4%)	21,394 (4.4%)	2,416 (0.5%)	2,233 (0.5%)	7,209 (1.5%)	18,782 (3.9%)	9,086 (1.9%)	9,899 (2.0%)	27,801 (5.7%)	15,026 (3.1%)	4,211 (0.9%)
45	Cyprus (CY)	2,925 (3.7%)	1,975 (2.5%)	302 (0.4%)	906 (1.2%)	818 (1.0%)	4,922 (6.3%)	2,240 (2.9%)	969 (1.2%)	6,813 (8.7%)	4,085 (5.2%)	944 (1.2%)
46	Mauritania (MR)	136 (7.5%)	26 (1.4%)	3 (0.2%)	14 (0.8%)	38 (2.1%)	50 (2.8%)	9 (0.5%)	7 (0.4%)	172 (9.5%)	255 (14.1%)	5 (0.3%)
47	Viet Nam (VN)	45,079 (2.9%)	37,426 (2.4%)	3,221 (0.2%)	6,715 (0.4%)	13,887 (0.9%)	25,511 (1.6%)	15,653 (1.0%)	15,043 (1.0%)	43,183 (2.8%)	195,951 (12.6%)	22,830 (1.5%)
48	Bulgaria (BG)	11,915 (1.4%)	10,864 (1.3%)	2,754 (0.3%)	14,637 (1.7%)	5,836 (0.7%)	45,555 (5.3%)	18,434 (2.1%)	17,752 (2.1%)	84,626 (9.8%)	23,696 (2.7%)	3,651 (0.4%)
49	Singapore (SG)	16,648 (1.2%)	42,264 (3.0%)	4,791 (0.3%)	11,719 (0.8%)	12,751 (0.9%)	45,505 (3.2%)	23,311 (1.7%)	23,039 (1.6%)	211,213 (15.0%)	43,591 (3.1%)	9,352 (0.7%)
50	South Sudan (SS)	42 (1.5%)	30 (1.1%)	18 (0.6%)	22 (0.8%)	25 (0.9%)	45 (1.6%)	40 (1.4%)	0 (0%)	180 (6.3%)	90 (3.2%)	12 (0.4%)

APPENDIX B: RANKING NATIONAL ECONOMIES

When comparing relative national economies, we chose to use the Gross Domestic Product (GDP) based on purchasing power parity (PPP) figures published by the International Monetary Fund (IMF) as of the World Economic Outlook report of October, 2015[1]. This is a commonly referenced statistic is used to measure the relative economic strengths of 189 member nations, though as in any statistical analysis, some sampling and estimation errors are to be expected.

The complete ranking is listed below, for reference.

1 https://www.imf.org/external/pubs/ft/weo/2015/02/weodata/index.aspx

Country	GDP (in Billions)
China	20,985.63
United States	18,697.92
India	8,727.96
Japan	4,949.22
Germany	3,948.83
Russia	3,493.04
Brazil	3,212.11
Indonesia	3,018.89
United Kingdom	2,751.48
France	2,717.52
Mexico	2,309.50
Italy	2,227.64
Korea	1,930.48
Saudi Arabia	1,738.76
Spain	1,697.82
Canada	1,675.15
Turkey	1,641.00
Islamic Republic of Iran	1,459.05
Australia	1,183.26
Nigeria	1,166.41
Taiwan Province of China	1,156.44
Thailand	1,156.08
Poland	1,050.95
Egypt	1,050.74
Pakistan	984.21
Argentina	968.48
Malaysia	860.23
Netherlands	856.99
Philippines	798.39
South Africa	742.46
Colombia	691.54
United Arab Emirates	669.86
Bangladesh	623.30
Algeria	599.83
Vietnam	593.51
Iraq	575.62
Belgium	507.76
Switzerland	494.81
Singapore	488.35
Sweden	486.96
Venezuela	467.58
Kazakhstan	445.87
Chile	440.09
Romania	432.02
Hong Kong SAR	430.68
Austria	415.05
Peru	402.82
Norway	361.48
Ukraine	352.34
Qatar	344.25
Czech Republic	343.93
Kuwait	299.56
Portugal	296.49
Israel	294.42
Myanmar	293.67
Morocco	287.96
Greece	281.22
Hungary	266.58
Denmark	265.30
Ireland	262.95
Sri Lanka	252.94
Finland	229.35
Uzbekistan	201.19
Angola	194.06
Ecuador	184.07
Azerbaijan	180.86
Oman	178.74
Sudan	176.23
Ethiopia	174.16
New Zealand	172.03
Slovak Republic	167.35
Belarus	166.54
Dominican Republic	156.04
Kenya	154.60
Tanzania	149.79
Bulgaria	136.71
Tunisia	132.59
Guatemala	131.78
Ghana	121.22
Serbia	99.90
Turkmenistan	99.47
Libya	95.83
Croatia	92.31
Panama	88.40
Jordan	87.13
Lebanon	86.98
Côte d'Ivoire	85.31
Lithuania	85.30
Yemen	85.28
Uganda	85.10
Costa Rica	77.97
Bolivia	77.37
Cameroon	76.90

Table 10: Countries ranked by GDP (continued on page 28).

Country (CONTINUED)	GDP (in Billions)
Uruguay	76.72
Nepal	74.02
Democratic Republic of the Congo	68.69
Zambia	68.00
Bahrain	67.78
Slovenia	65.52
Afghanistan	65.30
Paraguay	63.93
Luxembourg	59.18
Cambodia	58.75
El Salvador	54.85
Latvia	52.16
Trinidad and Tobago	45.47
Honduras	42.98
Bosnia and Herzegovina	41.13
Lao P.D.R.	40.96
Estonia	39.43
Senegal	38.91
Botswana	38.82
Mongolia	38.19
Madagascar	37.64
Mozambique	36.93
Georgia	36.85
Gabon	36.54
Brunei Darussalam	34.35
Albania	34.28
Chad	33.75
Burkina Faso	33.44
Nicaragua	32.89
Republic of Congo	31.16
Mali	30.99
FYR Macedonia	30.17
Zimbabwe	28.92
Cyprus	28.64
Namibia	26.40
Armenia	26.07
Equatorial Guinea	26.05
Mauritius	25.74
Jamaica	25.41
Tajikistan	24.38
South Sudan	22.88
Benin	22.54
Rwanda	22.00
Papua New Guinea	21.98
Malawi	21.84
Kyrgyz Republic	20.77
Niger	20.23
Haiti	19.87
Moldova	18.26
Mauritania	17.68
Guinea	16.21
Iceland	15.93
Malta	15.45
Togo	11.56
Swaziland	11.08
Montenegro	10.44
Sierra Leone	9.88
The Bahamas	9.55
Suriname	9.37
Burundi	8.39
Eritrea	8.21
Fiji	8.18
Timor-Leste	7.36
Bhutan	7.00
Guyana	6.13
Lesotho	6.02
Maldives	4.94
Barbados	4.77
Liberia	4.04
Cabo Verde	3.65
The Gambia	3.49
Djibouti	3.35
Central African Republic	3.27
Belize	3.21
Guinea-Bissau	2.84
Seychelles	2.66
Antigua and Barbuda	2.17
St. Lucia	2.09
San Marino	2.00
Grenada	1.44
St. Kitts and Nevis	1.42
St. Vincent and the Grenadines	1.26
Comoros	1.26
Solomon Islands	1.19
Samoa	1.06
Dominica	0.86
Vanuatu	0.72
São Tomé and Príncipe	0.71
Tonga	0.54
Micronesia	0.32
Palau	0.27
Kiribati	0.20
Marshall Islands	0.19
Tuvalu	0.04

APPENDIX C: STUDY METHODOLOGY

How We Picked the Countries

Unless otherwise noted, we limited our survey of ports to those countries that are members of the International Monetary Fund (described in Appendix B). Some visualizations were limited to only the top 50 countries, by GDP. Together, these "Top 50" nations account for 92% of the world economy.

How We Picked The Ports

Starting with the nmap ranked TCP services list[1] we surveyed Rapid7 researchers for their combined expert opinion on which ports to include in the study. Project Sonar uses zmap for port scans and we configured it to send a SYN ("*is anybody home*?") request for each TCP port. We performed multiple, full-sweeps of the internet for each port, honoring our "Do Not Scan" block list, which does impact the reach of Project Sonar.

How We Surveyed The Internet

We compared our scan target results to the most recent ICMP survey by the University of Michigan (our scans.io partner) and noted that we reached roughly 50% of the over 300 million pingable nodes. Data from CAIDA suggests there may be closer to 700 million to 1 billion client/server/device nodes on the internet, but not all of them respond to direct network probes. As noted in "*The Challenges With "Counting the Internet"* (pg 7), we fully acknowledge the limitations of the Sonar scans used in this study but believe they provide a representative sample to extract knowledge from. Once we have more definitive, accurate data on internet utilization by country, future studies of this nature will identify the statistical uncertainty levels associated with Sonar sampling.

How We Identified IP Addresses To Countries

The commercial version of MaxMind's geolocation databases was used to match each IPv4 address to a country. MaxMind claims[2] 99.8% accuracy on the country level. We then narrowed the populaton to those present on the International Monetary Fund list[3] to focus on regions wtih globally recognized, established economies and to facilitate comparisons by Gross Domestic Product (GDP).

How We Made The Exposure Index

The Exposure Index was created by aggregating the results of 16 individual rankings for exposed, usually cleartext ports — web, mssql, mysql, smtp, pop, imap, ldap, rdp, rfb, upnp, jetd, pptp, rpcbind, nbss, msrpc, cifs — based on in-country prevalence, and combined, ranked total port exposure per-country. We chose these services from the thirty ports covered in the full study scans as there is either a greater likelihood of exposure of sensitive information over cleartext channels with them or they expose services, such as Microsoft file sharing protocols, that have been identified with extensive vulnerabilities over time.

The final list was generated by using a weighted, seeded Cross Entropy Monte Carlo (CEMC) algorithm[4]. Aggregating sixteen exposure rankings plus overall service counts per country fits into the category of a combinatorial optimization problem[5] and the CEMC approach provides a stochastic computational means to iterate over each ranked list, perform importance sampling and derive a final outcome. It is our belief that the nature of these ranked lists makes this a prefered methodology over others.

Our intent is to expand and enhance the list of individual ranked elements with more per-node and per-service data—including studies of IPv6, DNS configurations and in-country autonomous systems rankings—and welcome participation from research partners who also look at things at internet scale.

R[6] and RStudio[7] were used for all data processing, analysis and visualizations. Full data sets, code and further details on the analyses will be released with links provided on http://community.rapid7.com/.

---

1 https://svn.nmap.org/nmap/nmap-services
2 https://support.maxmind.com/geoip-faq/geoip2-and-geoip-legacy-databases/how-accurate-are-your-geoip2-and-geoip-legacy-databases/
3 http://www.imf.org/external/country/index.htm
4 The Cross-Entropy Method for Continuous Multi-Extremal Optimization; Kroese, Porotsky, Rubinstein; DOI 10.1007/s11009-006-9753-0
5 https://en.wikipedia.org/wiki/Combinatorial_optimization
6 http://r-project.org/
7 http://rstudio.com

The Challenges With "Counting the Internet"

Project Sonar honors each and every Project Sonar "Do Not Scan" request that we have received. Our survey for this study did not attempt to probe approximately 42 million non-reserved, non-private IP addresses per our blocklist, and 592 million reserved or private addresses that are not routable over the internet. We performed all telemetry actions from our well-publicized scanning nodes and used lightweight TCP SYN scans for each port in the study. These restrictions create some challenges when trying to "count all the things." Note that a number of these challenges were noted in "Balkanization from Above."[1]

Even with us honoring our blocklist requests, there are many organizations and internet service providers that completely block our scanning nodes, and we do not attempt to subvert or evade those blocking controls. This reduces the active target collections substantially. To gauge our scan effectiveness, we asked the Center for Applied Internet Data Analysis (CAIDA)[2] for their best estimates of IPv4 utilization. While we picked up roughly 146 million unique IPv4 addresses in our port queries, their telemetry-based statistical estimates suggest we only caught between 20% and 40% of utilized IPv4 space.

Some readers may remember the 2012 Internet Census[3], which also had greater effective visibility into the devices connected to the internet. The researchers involved in that study generated quite a bit of discourse due to the fact that they exploited a vulnerability in a common, household router to perform their scans. Their "hackcensus" methodology gave them unprecedented visibility into vast portions of the internet, but they did not honor blocklist requests (mostly due to the fact that they didn't tell anyone what they were doing), they did not ask for permission for any actions they took, and they probed a wider range of ports.

We also only looked for 30 ports. ICMP (i.e. "ping" or "are you there?") probes performed alongside our study—in conjunction with the University of Michigan scans.io project (Project Sonar is a founding member of that research initiative)—indicate there are over 300 million IPv4 nodes that respond to ICMP requests from their less-restrictive scanner.

Our modern internet is quite ephemeral. Cloud services enable rapid provisioning and deprovisioning of systems, and Amazon itself has over 30 million IPv4 addresses at its disposal[4]. Satellite networks, 3G & 4G/LTE wireless carriers, along with cable, DSL and FiOS internet providers all employ their own access and blocking rules as well.

Then there are all the researchers like us here at Rapid7 who deploy honeypots (i.e. "listening posts") to try to detect malicious behavior on the internet. Many of these honeypots are "any port in a storm"-type systems that gladly acknowledge the "hey there" from any scanner. This, in a way, pollutes the overall results—i.e. many of the systems with 10+ ports listening, especially in "strange" combinations, could very well be honeypot sensors.

Finally, there are a number of firewalls, routers and/or other networking devices that listen on a single IPv4 address for a multitude of ports to which they then forward the requests. These are likely suspects also polluting the "10 ports or more" category.

We fully acknowledge these challenges and the potential deficiencies in the scanning studies associated with this report. Even with Project Sonar's less-than-perfect visibility, we believe there is enough signal to warrant both your attention and our future explorations in this space.

About Rapid7

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cyber security. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks. Rapid7 is trusted by more than 5,300 organizations across over 100 countries, including 36% of the Fortune 1000. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

1 Geer/Moore 2015, https://www.usenix.org/system/files/login/articles/login_aug15_14_geer.pdf
2 https://www.caida.org/home/
3 http://internetcensus2012.bitbucket.org/
4 Amazon cloud CIDR blocks: https://ip-ranges.amazonaws.com/ip-ranges.json