

UK Cities Exposed

A Shodan-based Security Study on Exposed Cyber Assets in the UK

Natasha Hellberg and Rainer Vosseler
Trend Micro Forward-Looking Threat Research (FTR) Team

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

Exposed Cyber Assets

5

Exposed Cities: UK

10

Exposed Cyber Assets
in the UK

29

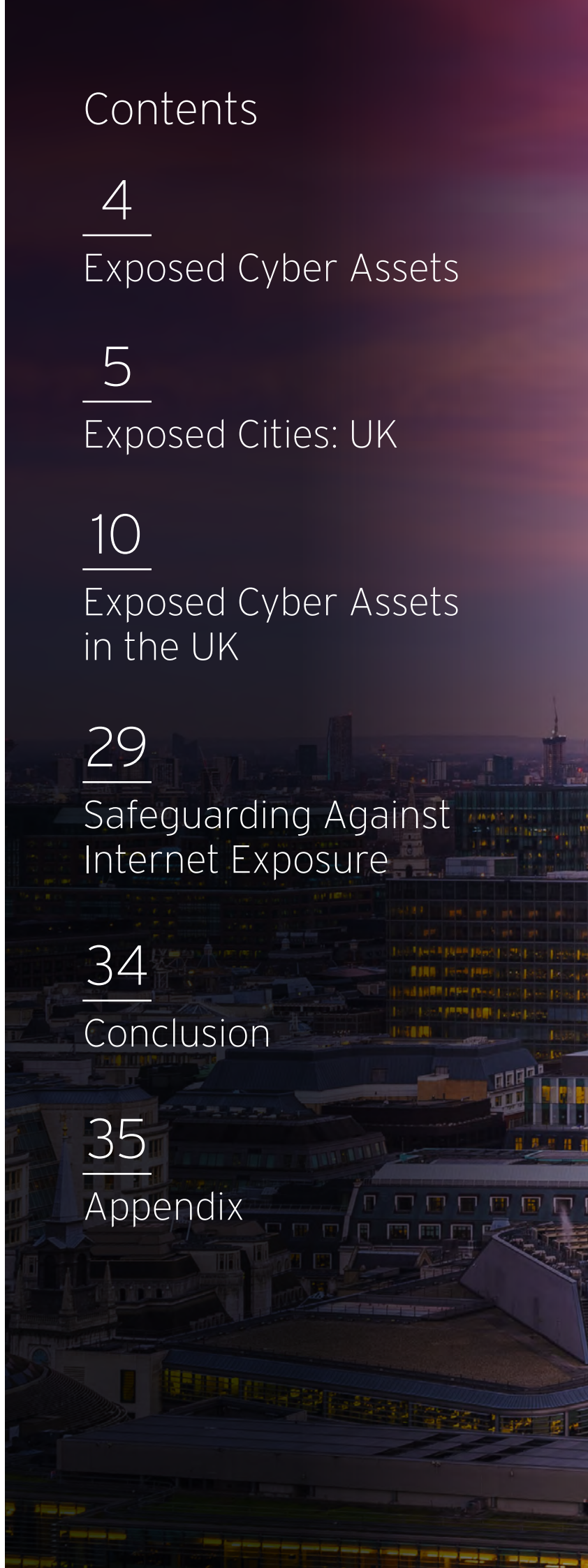
Safeguarding Against
Internet Exposure


34

Conclusion

35

Appendix



A cityscape at dusk with a large orange semi-transparent box containing text. The background shows a mix of modern glass skyscrapers and older stone buildings, with lights from the buildings glowing against the twilight sky.

Continuing our exploration of the exposed world, we ask: Why is it critical to tackle exposed cyber assets such as devices, services, servers, and databases? Much of the success of cyberattacks or any prevalent threat is due to security gaps—whether in the devices or network topology leveraged by cybercriminals and threat actors. Hackers can take advantage by simply knowing about open cyber assets or users in target enterprises to further their attacks. Leaving systems, servers, or devices exposed on the internet potentially introduces serious risks such as data theft, system compromise, and fraud, among others.

As our “U.S. Cities Exposed¹” paper revealed, incorrect configurations in network infrastructure that allow direct device or system access is a factor in exposing a cyber asset on the internet. Depending on the end goal, actors targeting cyber assets are not only limited to cybercriminal groups but also nation-states, competitors, hacktivists, and script kiddies.

We profiled all of the exposed cyber assets in the top 10 cities in the U.K. by population to raise public awareness on the risks that they bring. Despite the U.K.’s decision to separate from the European Union (EU), companies in the country regardless of size and industry still need to comply with the statutes of the General Data Protection Regulation (GDPR), which will take full effect on May 2018, as long as they process the data of EU citizens.

Apart from highlighting the potential dangers of visible and searchable cyber assets on the internet, we provided best practices to help readers harden their device security, along with some tips on mitigating possible risks associated with cyber asset exposure. We also conducted similar research on Western European capitals and major cities in Germany and France.

DISCLAIMER: At no point during this research did we perform any scanning or attempt to access any of the internet-connected devices and systems. All published data, including screenshots, were collected via Shodan. Note that any brand mention in this research does not suggest any issue with the related products, only that they are searchable on Shodan. Furthermore, the analysis used February 2017 data and, given the fluid nature of the internet, the state of exposure may change when Shodan is queried at another time.

Exposed Cyber Assets

Exposed cyber assets are internet-connected devices and systems that are discoverable via network enumeration tools, Shodan, or similar search engines and are accessible via the public internet. To say a certain device or system is exposed does not automatically imply that the cyber asset is vulnerable or compromised. However, since an exposed device is searchable and visible to the public, attackers can take advantage of the available information online to mount an attack. For instance, an attacker may check if the associated software of a device is vulnerable, the administration console's password is easy to crack, or data is sitting open on the internet either in a database or on a network share.

What potential risks are associated with exposed cyber assets? Hackers who steal confidential data such as corporate information, intellectual property, and personally identifiable information (PII) can compromise exposed cyber assets. These cyber assets can also leak data online or be held hostage for ransom. Owners of exposed cyber assets may unknowingly become accomplices to cybercriminal operations when their open devices, systems, or servers are abused for fraud, phishing email distribution, or distributed denial-of-service (DDoS) attacks.

Given the potential threats to exposed cyber assets, an understanding of the exposure landscape and one's network and its attendant weaknesses is therefore crucial.

Exposed Cities: UK

We partnered with Shodan, a publicly available database of scan data, for our research on exposed cyber assets. Technical assumptions and observations about our use of Shodan data for this project can be found in the Appendix, where we also discuss what Shodan is and how we analyzed the data we obtained through it. Note that the scan data used was merely a point-in-time snapshot.

We examined the Shodan U.K. scan data for February 2017, excluding data belonging to known hosting providers since hosting infrastructure is complex and difficult to map or accurately port to back-end applications. The filtered data set contains a total of 29,384,559 records generated from scanning 8,660,791 unique Internet Protocol (IP) addresses. The raw scan data was indexed using Elasticsearch and queried using Kibana, which allowed us to search more than 550 fields versus more than 40 fields using Shodan’s web interface. The list of hosting providers whose IP addresses were excluded can be found in the Appendix.

This section provides a general overview of cyber asset exposure numbers and all types of exposed devices, systems, products, OSs, and other assets that are visible in the February 2017 Shodan U.K. scan data for the top 10 cities by population.

Cyber Asset Exposure in the UK

Based on the Shodan scan data, London had the highest number of exposed cyber assets in the U.K. — a little over 2.5 million. Manchester followed with around 320,000 and Glasgow with around 160,000.

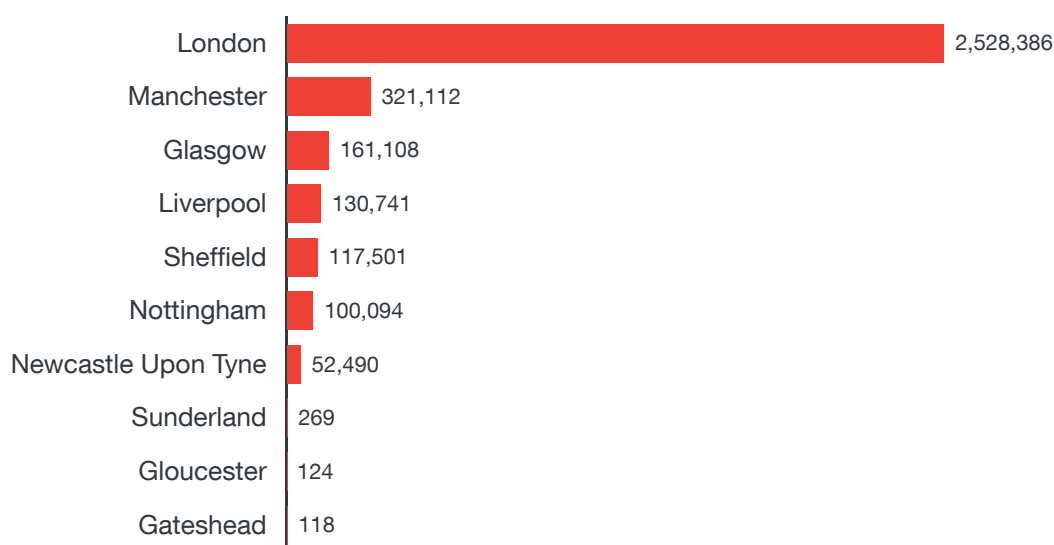


Figure 1. Cities with the highest number of exposed cyber assets

**Note that three of the cities (Sunderland, Gloucester, and Gateshead) in the figure above are not part of the list of top 10 U.K. cities by population.*

| City-Region | Region | Population (2011 Census) |
|--------------------------------|--------------------|--------------------------|
| London | Greater London | 9,787,426 |
| Manchester | Greater Manchester | 2,553,379 |
| Birmingham–Wolverhampton | West Midlands | 2,440,986 |
| Leeds–Bradford | West Yorkshire | 1,777,934 |
| Glasgow | Greater Glasgow | 1,209,143 |
| Liverpool | Liverpool | 864,122 |
| Southampton–Portsmouth | South Hampshire | 855,569 |
| Newcastle Upon Tyne–Sunderland | Tyneside | 774,891 |
| Nottingham | Nottingham | 729,977 |
| Sheffield | Sheffield | 685,368 |

Table 1. Top 10 U.K. cities by population²

How Exposed Devices Access the Internet

Nearly 80 percent of the exposed devices accessed the internet via Ethernet or modems. This is reflective of our findings in Western European capitals and French cities. Most of the capital cities use Ethernet because businesses required high-speed internet access. In the U.K., connecting via landline was most common (fiber and copper-based DSL in cities), followed by 4/5G cellular directly on phones or via 4G hot spots. In rural areas, providers used cellular towers for their networks.

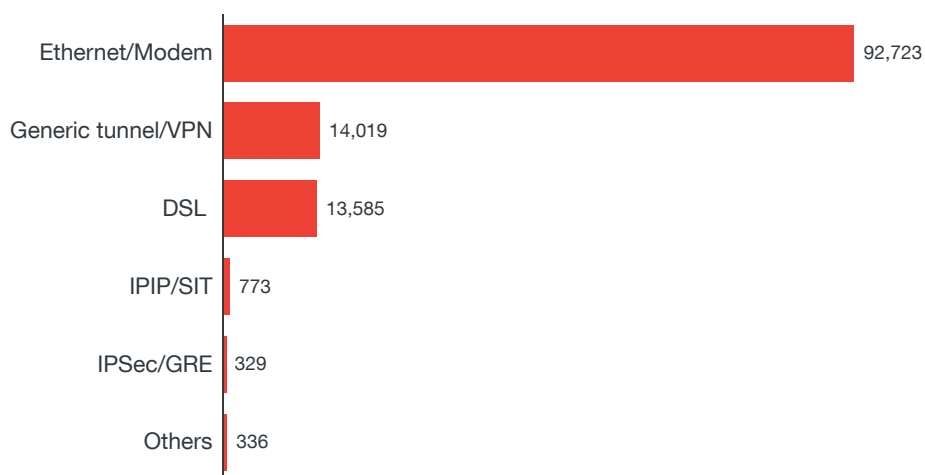


Figure 2. Means by which exposed devices access the internet

OSs Running on Exposed Internet-connected Devices

A majority of the exposed internet-connected devices run on Linux-based platforms. These included Apache servers, NGINX, and Internet of Things (IoT) devices that run on Linux or Unix. A small number of legacy systems such as those that run on Windows® XP were still in the mix, which can pose grave risks, given that Microsoft no longer supports³ the platform.

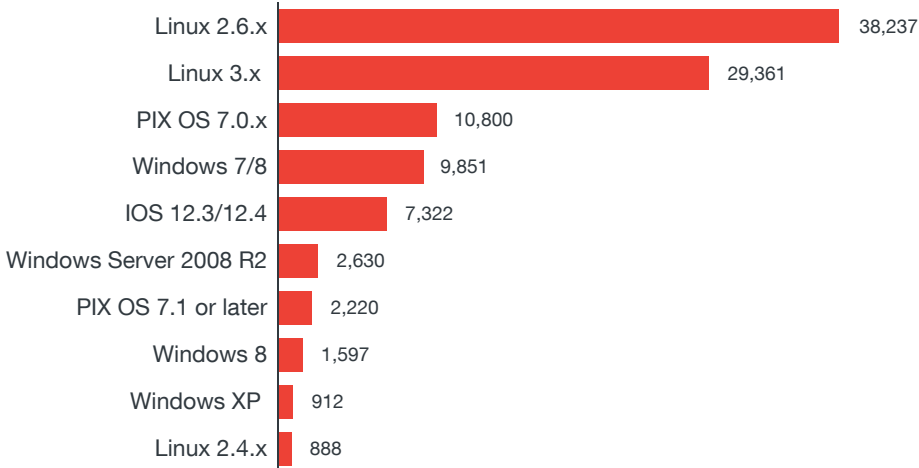


Figure 3. OSs that run on exposed devices (top 10)

Top Exposed and Vulnerable Products

Apache, NGINX, and Microsoft web servers; Secure Shell (SSH) devices; email servers; and firewalls dominated the list of exposed products in the top 10 U.K. cities by population. Both web and email servers are lucrative targets because attackers could exploit existing security bugs in them to infiltrate an enterprise network and obtain confidential data.

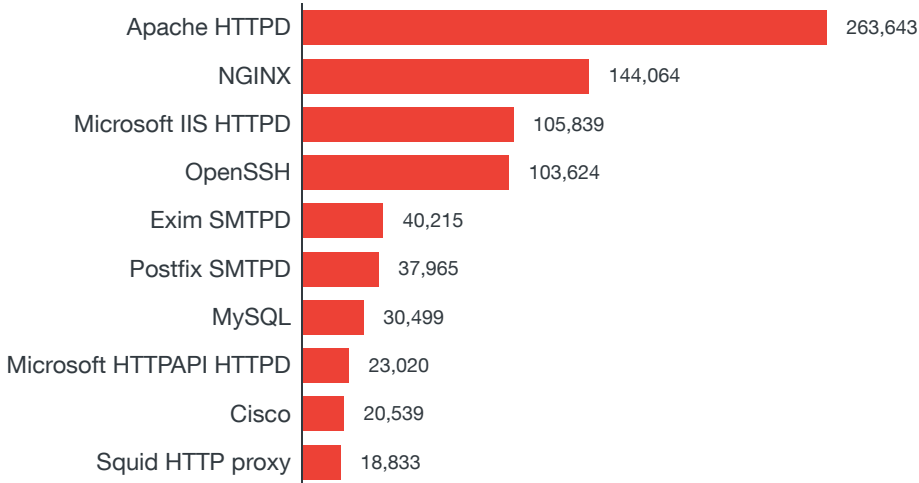


Figure 4. Number of exposed cyber assets by product/service name (top 10)

The Shodan crawler tests for certain vulnerabilities such as CVE-2014-0160 (also known as Heartbleed⁴), CVE-2015-0204⁵ (an OpenSSL vulnerability), CVE-2013-1899⁶ (an argument injection vulnerability in PostgreSQL), CVE-2016-9244⁷, CVE-2013-1391⁸, and CVE-2015-2080⁹ (also known as JetLeak) to determine if certain exposed products are vulnerable.

The results for the most exposed vulnerable products were quite expected. Apache, Microsoft™ Internet Information Service (IIS) Hypertext Transfer Protocol daemon (HTTPD), and NGINX web servers led the pack, closely followed by email servers, firewalls, and databases. OpenSSL, which is vulnerable to Heartbleed, is widely used in Apache and NGINX web and email servers.

Flaws in firewalls can be exploited to lower access restrictions, allowing threats to bypass an enterprise's first line of defense. Knowledge on security flaws in databases and email and web servers, meanwhile, can aid threat actors in launching attacks.

Web administration interfaces of firewalls were also exposed, particularly for SonicWall, because remote administration was enabled. Do note that firewalls commonly have this feature enabled to secure the web servers behind them. Shodan scans tag them as “exposed” but it does not necessarily follow that they could pose risks to a network.

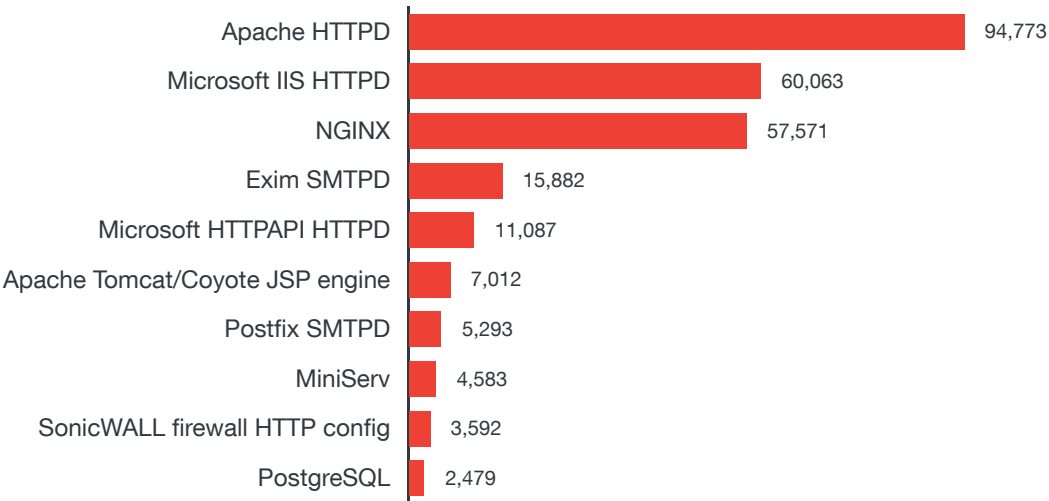


Figure 5. Number of exposed vulnerable products (top 10)

Top Exposed and Vulnerable Device Types

As the internet-facing layer of protection against network-based attacks, it is no wonder that a majority of exposed device types in the U.K. were firewalls. Firewalls by design have a number of open ports to allow traffic from the internet to the devices behind them that they are designed to protect. Because these ports are open, the firewall appears to be exposed on the internet when in fact this is by design and there are safeguards on the device to protect against remote exploitation.

It is also ironic to see that webcams figured in the chart toppers because they are supposed to protect against invasion of user privacy. This could be due to the fact that webcams have a number of network services enabled by default such as Simple Mail Transfer Protocol (SMTP), FTP, and Universal Plug and Play (UPnP), which are abused to launch reflective DDoS attacks¹⁰. Routers are exposed because they allow traffic to pass through. By definition, they have to be internet facing.

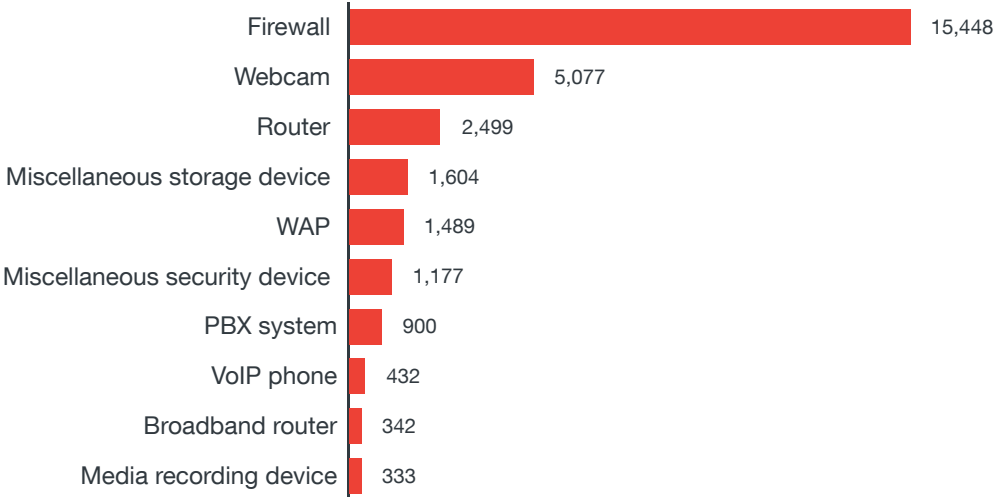


Figure 6. Number of exposed cyber assets by device type (top 10)

Contrary to the results for most exposed device types, the bulk of searchable exposed vulnerable devices comprised firewalls and security devices, followed by webcams and wireless access points (WAPs). The Shodan crawler tests for vulnerabilities including CVE-2014-0160 or Heartbleed, CVE-2015-0204, CVE-2013-1899, CVE-2016-9244, CVE-2013-1391, and CVE-2015-2080 or JetLeak.

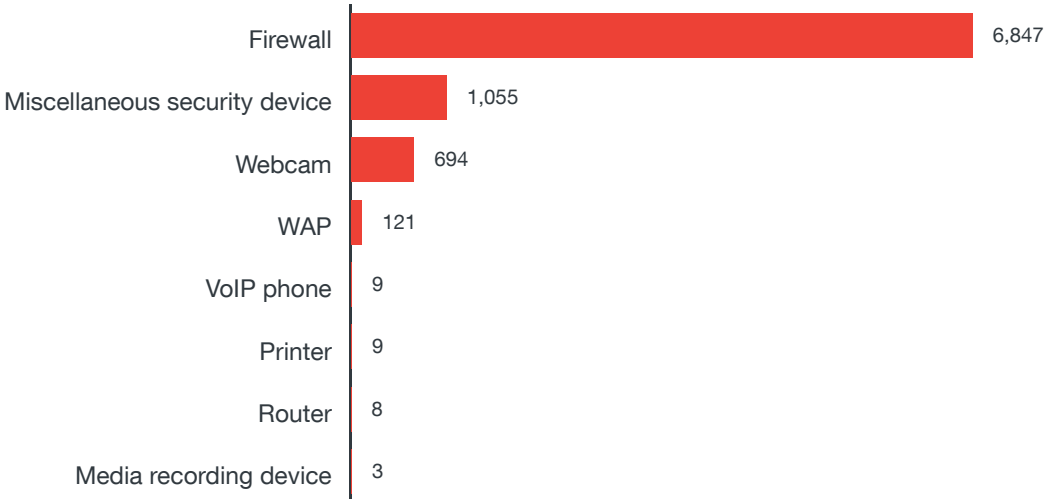


Figure 7. Top exposed device types vulnerable to CVE-2013-1391, CVE-2013-1899, CVE-2014-0160, CVE-2015-0204, CVE-2015-2080, or CVE-2016-9244

Exposed Cyber Assets in the UK

Exposed Devices

This section delves into the most commonly exposed devices such as webcams, routers, printers, phones, and media recording devices in the February 2017 Shodan scan data for the top 10 U.K. cities by population. Our findings revealed that a majority of U.K. cities had exposed webcams and routers, probably due to their extensive use in offices, homes, and public places.

Visible devices on the internet introduce risks such as data theft. It is also possible to compromise these devices to make them part of botnets for use in DDoS attacks, consequently making device owners unknowing accomplices to cybercrime.

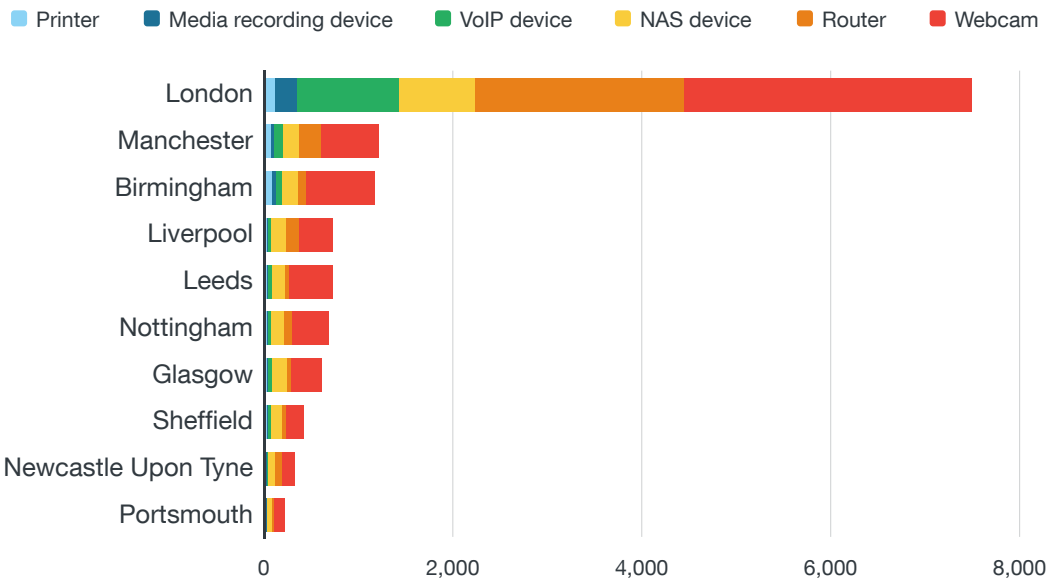


Figure 8. Overview of the top exposed devices by city

Exposed Webcams

Webcams are ubiquitous devices whose security often takes a backseat. Default passwords often remain unchanged or users employ weak passwords, making them vulnerable to brute-force attacks.

Exposed webcams also pose risks to user privacy as they arm attackers with knowledge on potential targets. Footage stolen from webcams can potentially be used for blackmailing purposes. In 2014, live feeds¹¹ from webcams, baby monitors, and closed-circuit television (CCTV) cameras were posted on a Russian website, exposing home users and businesses in the U.K. to potential attacks.

Our findings revealed that London had a much-higher number of exposed webcams compared with any other city in the U.K. This number comprised exposed AVTECH AVN801 network cameras and Netwave IP camera HyperText Transfer Protocol (HTTP) configuration services, among others.

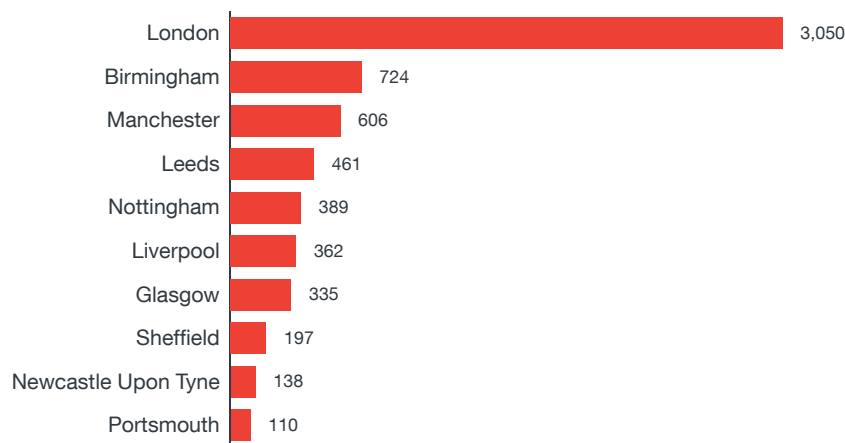


Figure 9. Number of exposed webcams by city

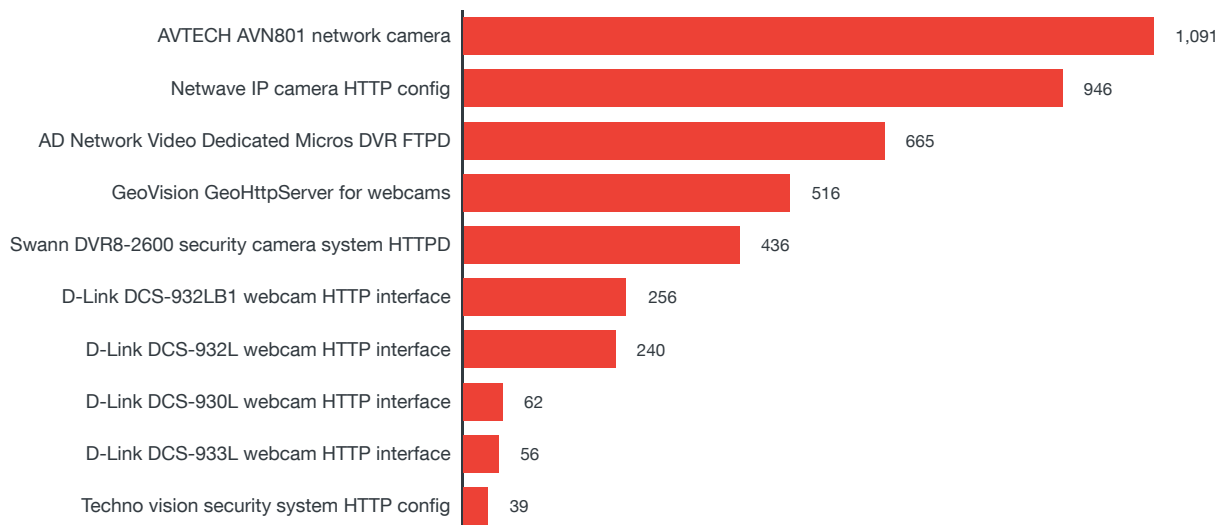


Figure 10. Number of exposed webcams by product/service name

Exposed NAS Devices

Network-attached storage (NAS) devices store and contain various kinds of data and files that can be accessed by corporate employees. In some cases, they serve as system backups. Home users with IoT devices also employ NAS devices for centralized data storage. Compared with routers or webcams, we saw fewer exposed NAS devices, a majority of which were found in London. Seagate GoFlex dominated the list of exposed NAS devices, most likely due to the fact that popular vendors left these settings open by default to allow for usability.

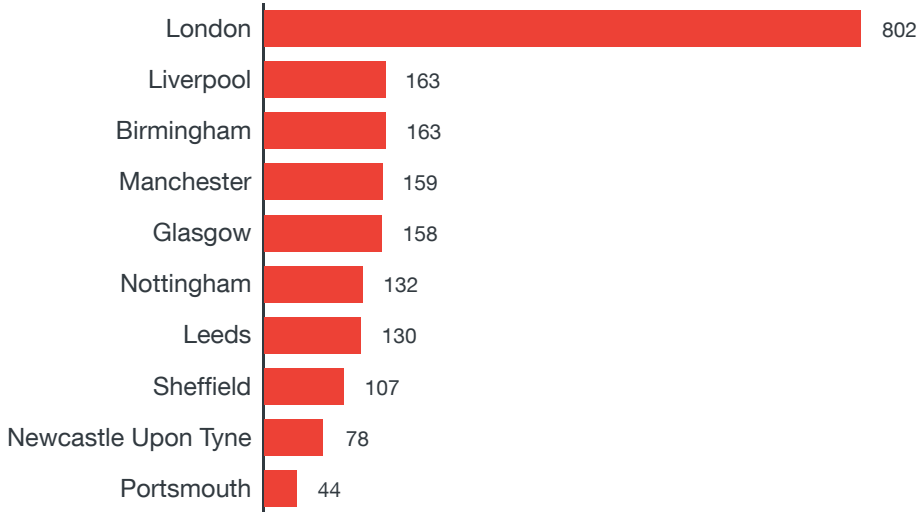


Figure 11. Number of exposed NAS devices by city

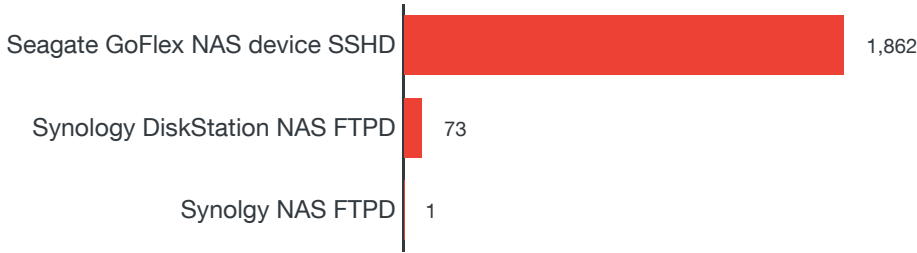


Figure 12. Number of exposed NAS devices by product/service name

Exposed Routers

All types of information coming from connected devices in homes or workplaces must pass through some form of router in order to access the internet (customer-premises equipment [CPE] routers at home all the way up to BX routers between major telecommunications companies). This makes them a viable target for cybercriminals who can profit from gaining unauthorized access and peddling stolen data in underground markets. Compromised routers can be made part of botnets and used for DDoS attacks as well. This type of attack was evidenced by Mirai¹², which affected even high-profile targets such as Twitter.

Poorly set router configurations also make the devices vulnerable to attacks. Predefined credentials that are easily searchable over the web could make it easier for threat actors to perform brute-force attacks to gain entry into networks. Security bugs in the routers' OS, hardware, and web applications can be possible entry points as well. From 1999 to January 2017, nearly 600 router vulnerabilities with designated Common Vulnerabilities and Exposures (CVE) numbers have been found and reported by researchers. Hijacked routers can also be used to redirect corporate traffic to alternate destinations.

London had the highest number of exposed routers in the U.K., specifically Cisco and MikroTik routers according to our Shodan scan for February 2017. Most of these routers' Telnet port (port 23) was visible.

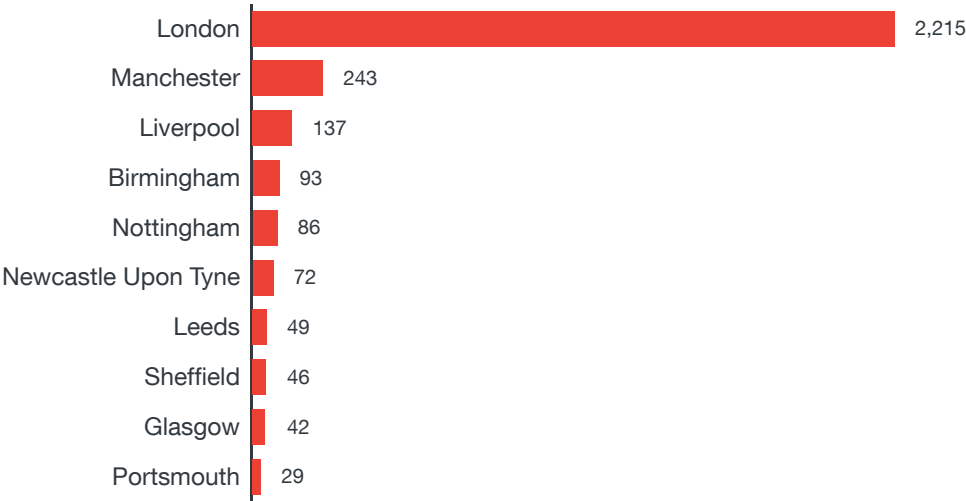


Figure 13. Number of exposed routers by city

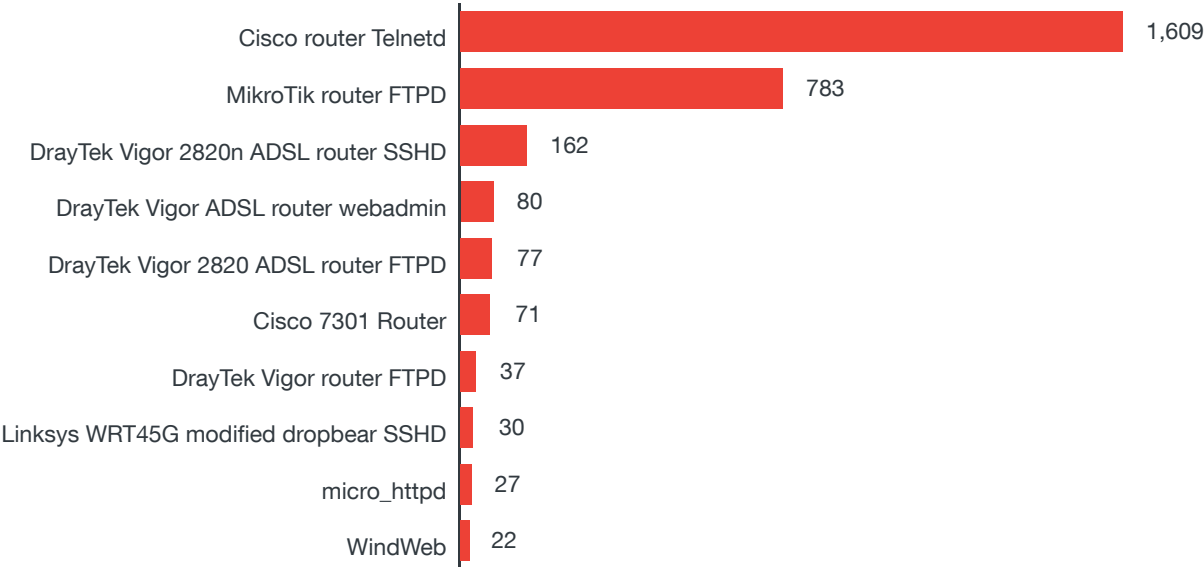


Figure 14. Number of exposed routers by product/service name

Although exposure does not necessarily translate to infection or vulnerability, knowing which routers are open and if they have security gaps could aid actors in attacks. To thwart threats from compromising router security, regularly apply patches and enable firewall settings to add another layer of protection.

Exposed Printers

Printers store confidential information such as intellectual property, customer data, and PII. Users print copies of what can be considered sensitive documents such as bank statements, W-2 forms, emails, and flight itineraries. This makes exposed printers an attractive target for attackers. Compromised printers could also be used for lateral movement within a network. Printers have additional services most people do not consider particularly sensitive but may also be utilized in attacks such as Simple Service Discovery Protocol (SSDP) (for reflective DDoS attacks), SMTP (for sending spam and phishing emails), and plain old telephone service (POTS) calls (for voice phishing or vishing and telephony denial-of-service [TDoS] attacks). Very few printers, however, were found exposed in the U.K.

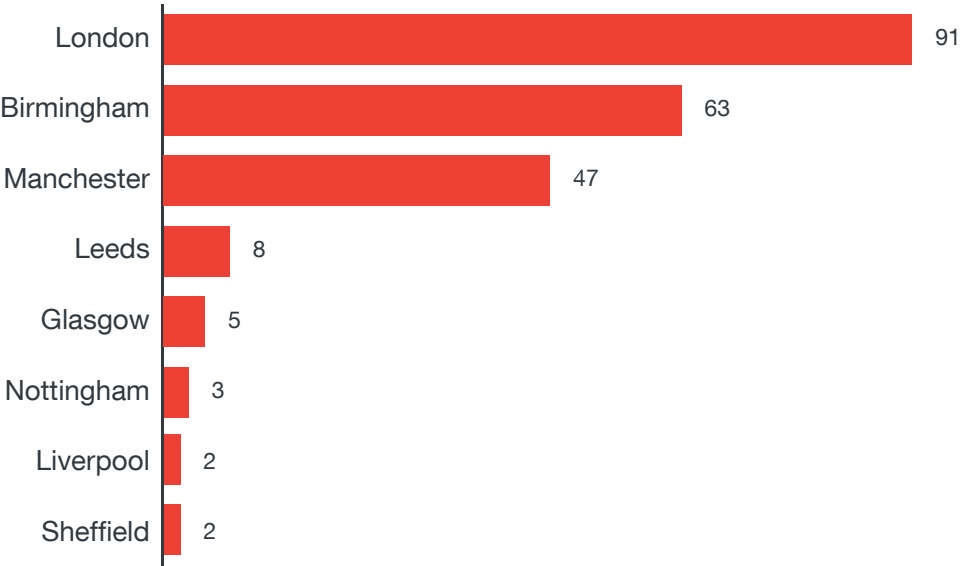


Figure 15. Number of exposed printers by city

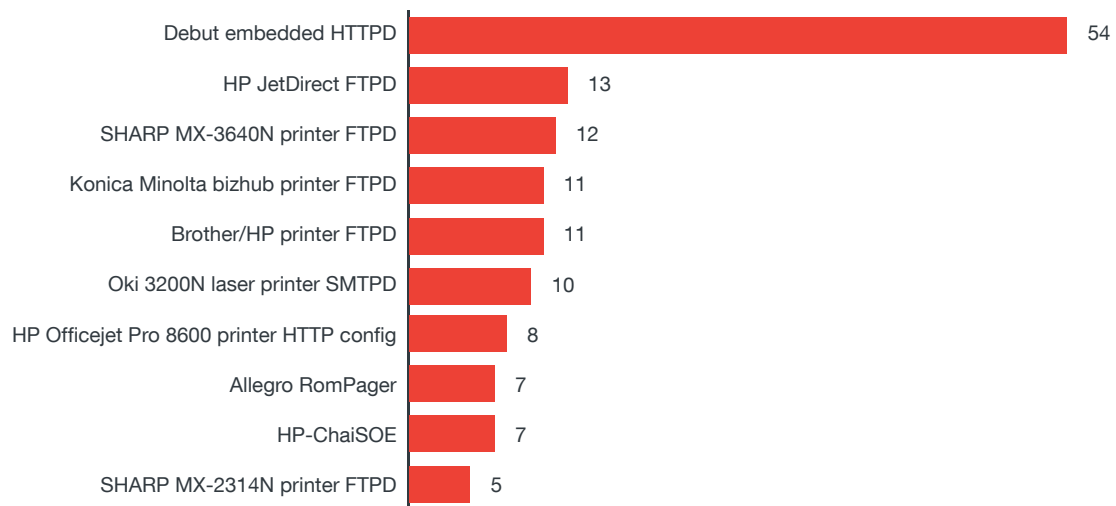


Figure 16. Number of exposed printers by product/service name

Exposed VoIP Devices

The emergence of Voice over Internet Protocol (VoIP) technology enables cost-efficient local and overseas communication. It is no surprise then to see businesses jumping onto the VoIP phone bandwagon for global competitiveness without costing an arm and a leg. In our Shodan scan results for February 2017, Free Private Branch Exchange (FPBX) devices or telephone systems in enterprises that permit employees to have a common external line topped the list. This was followed by another VoIP phone product, Siemens Gigaset DX800A VoIP phone Session Initiation Protocol (SIP), which offers a multiline function for home offices and small businesses.

VoIP devices make a viable target for threat actors in that business transactions, customer information, and other sensitive data transmitted over their lines can be recorded and used for attacks.

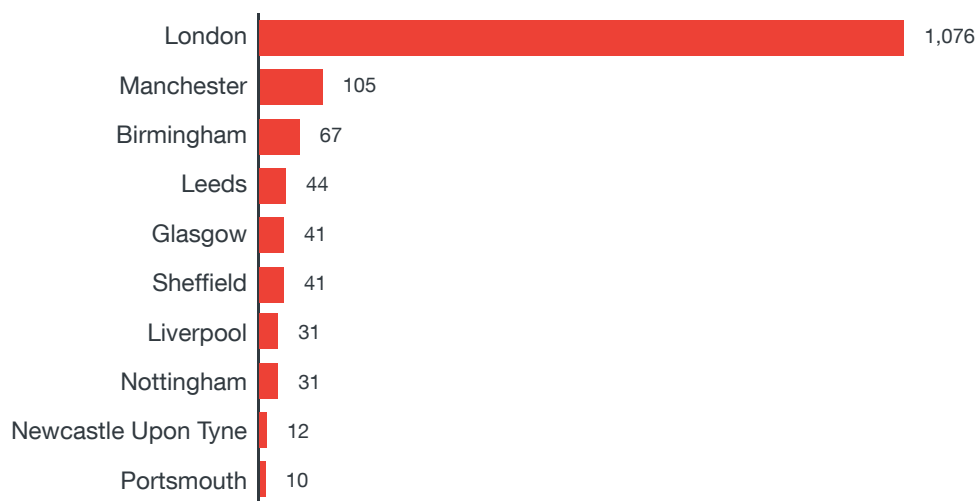


Figure 17. Number of exposed VoIP devices by city

Even worse, VoIP devices can be used to commit a variety of fraudulent activities such as TDoS and vishing attacks. Mobile phones, meanwhile, can be used to instigate Short Message Service (SMS) attacks and telefraud.

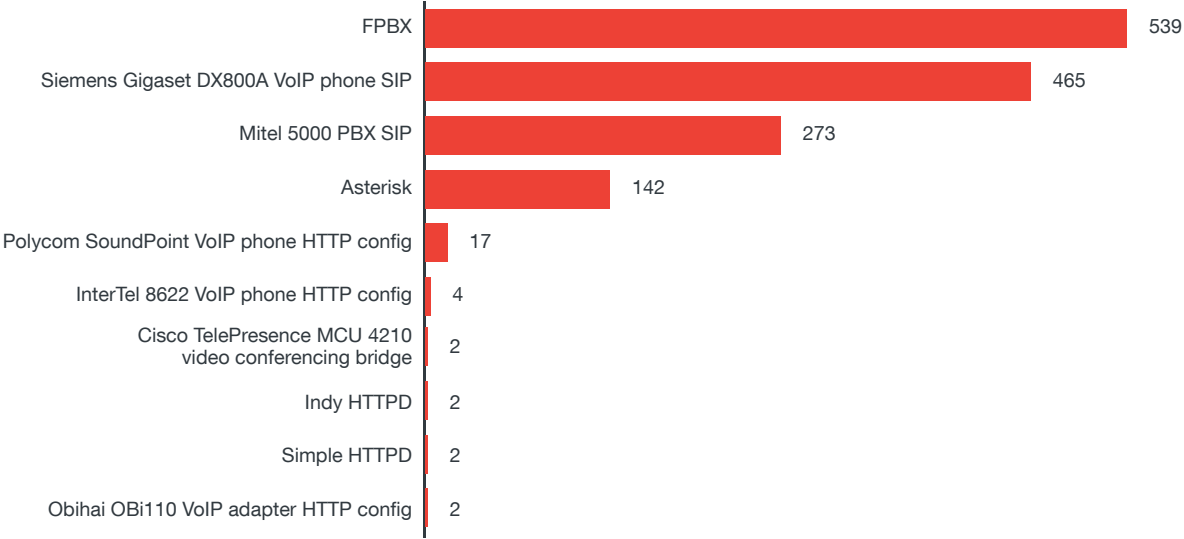


Figure 18. Number of exposed VoIP devices by product/service name

Exposed Media Recording Devices

What risks do exposed media recording devices such as digital video recorders (DVRs) pose? What makes them plausible attack targets? Most of the video feeds coming from CCTV cameras that are widely used in public spaces and businesses are stored in DVRs and can be a source of intel for reconnaissance or surveillance purposes. They can also be used as entry points into corporate networks for use in attacks such as Mirai¹³.

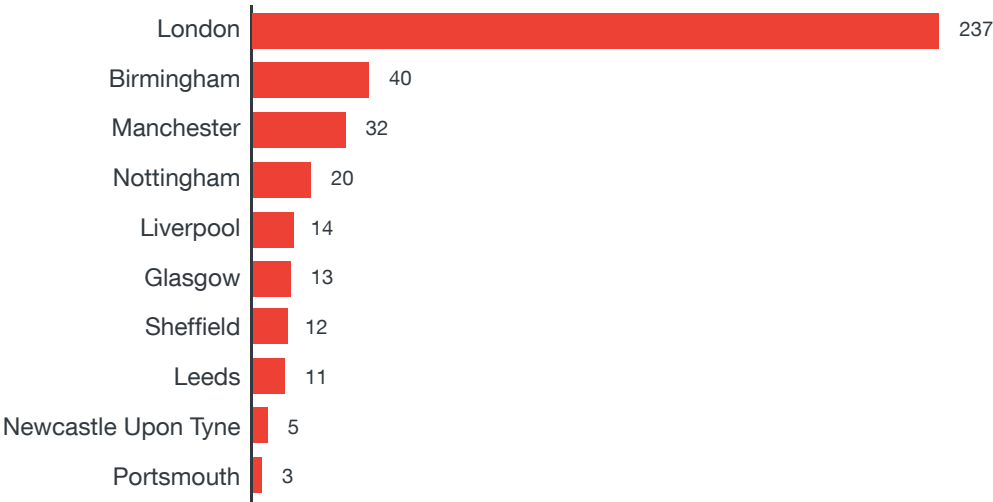


Figure 19. Number of exposed media recording devices by city

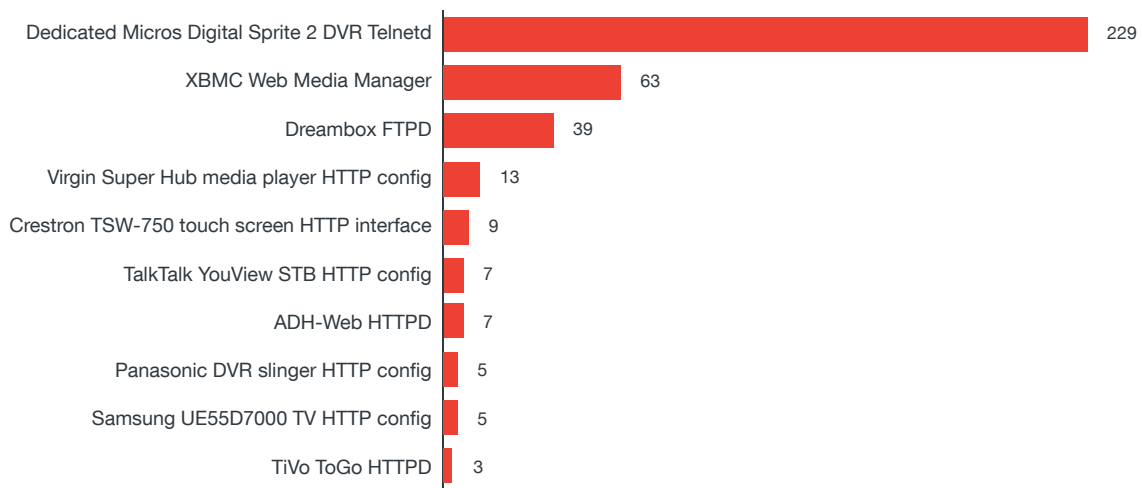


Figure 20. Number of exposed media recording devices by product/service name

Exposed Email/Web Services and Databases

This section digs deeper into exposed web and email services including open databases based on the February 2017 Shodan U.K. scan data for the top 10 cities by population. We also discuss the risks that come with server and database exposure such as data theft.

Exposed Web Services

“Web services,” by definition, pertain to system software that allows machine or device communication over a network or the web. They provide application programming interfaces (APIs), which permit apps to communicate with one another through the web or a network. They also refer to web-based interfaces used by web servers. Exposure of web services can introduce network risks via DDoS and Structured Query Language (SQL) injection attacks and data theft.

The most exposed web services based on our Shodan scan results were related to Apache HTTPD, NGINX, Microsoft IIS HTTPD, and Microsoft HTTPAPI HTTPD. This makes sense since most of the websites¹⁴ (with known web servers) as of August 2017 used Apache (49 percent), NGINX (34 percent), and Microsoft IIS (11 percent).

The results for London were unsurprising given that the city is a technology hub and so the highest density of technology could be found in it.

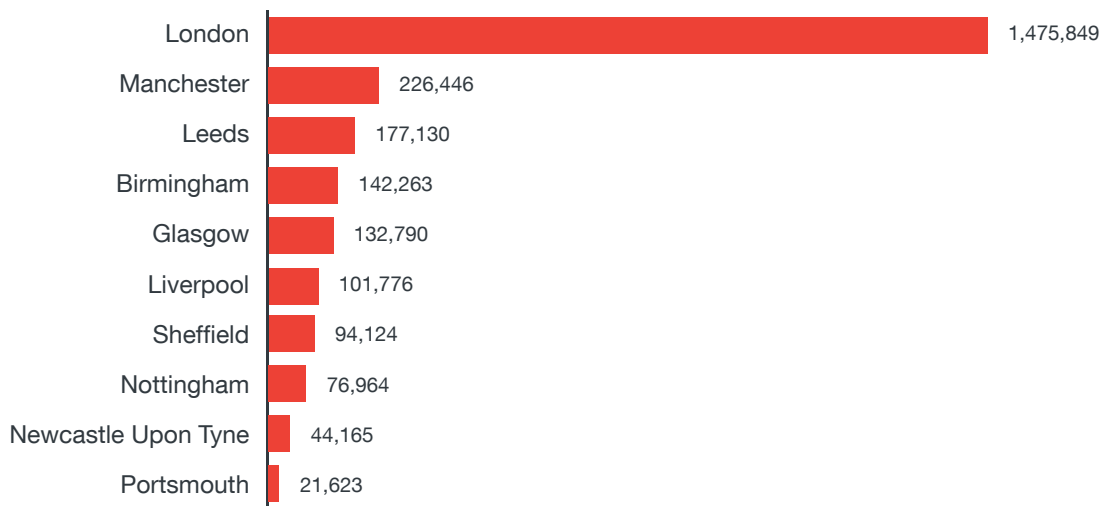


Figure 21. Number of exposed web services by city

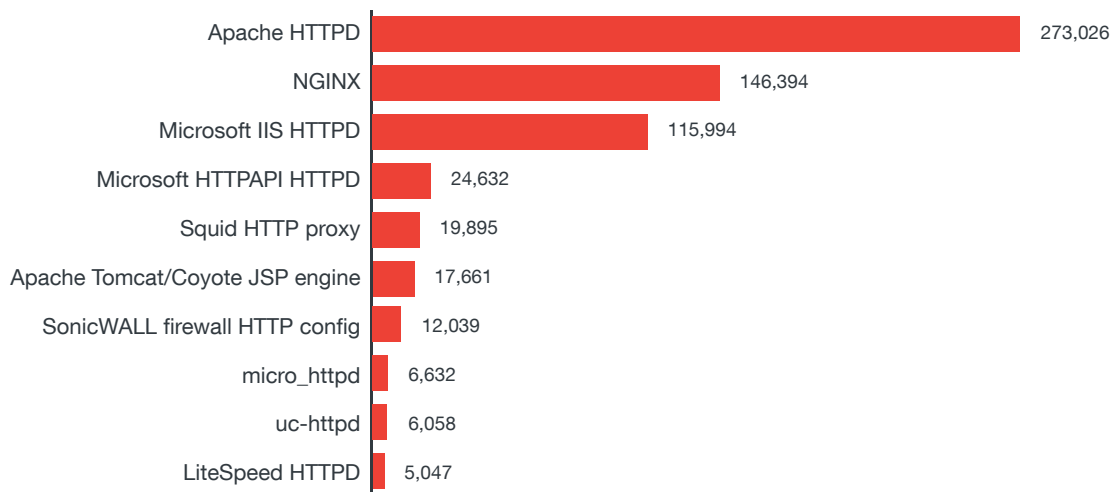


Figure 22. Number of exposed web services by product/service name

Exposed Email Services

Email is crucial for business communications and operations. Because of the troves of information (company data, credentials, etc.) that email servers contain, information technology (IT) administrators should secure them by keeping them updated with the latest patches.

We observed that the bulk of exposed email servers were in London, Manchester, and Birmingham. It is interesting to note that similar to our findings in the U.S., *NIX-based servers such as Postfix and Exim reigned supreme in our Shodan scan results.

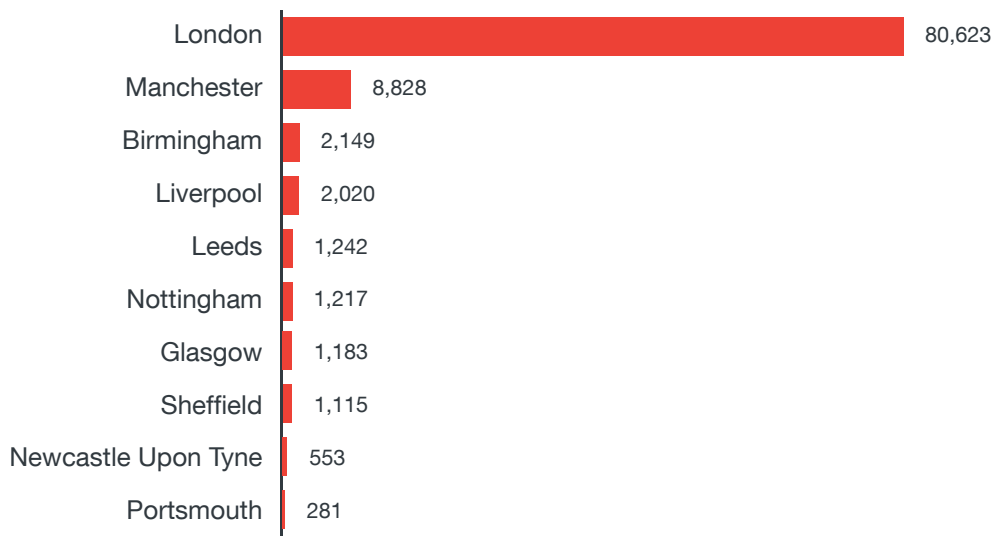


Figure 23. Number of exposed email services by city

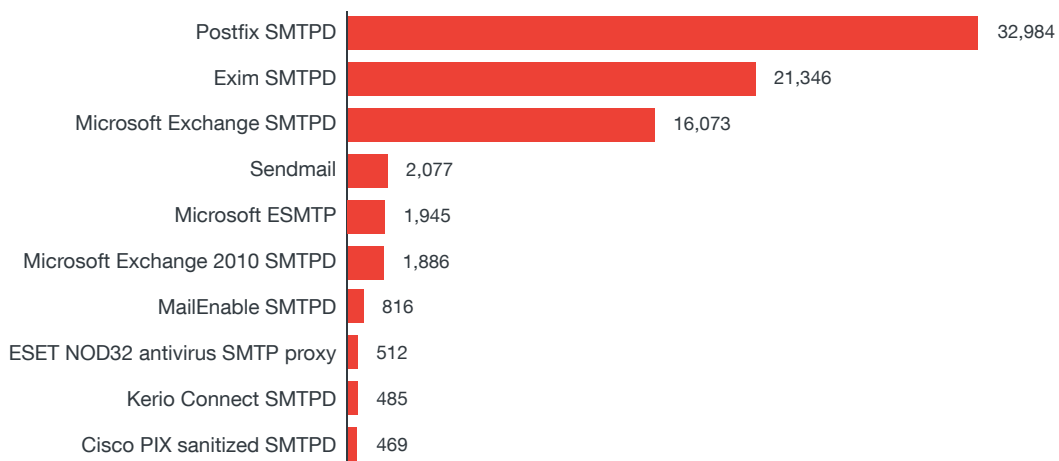


Figure 24. Number of exposed email services by product/service name

Exposed Databases

Critical company data or so-called “company crown jewels” such as the customer PII, intellectual property, trade secrets, and the like are stored in databases. Unauthorized access to them can thus lead to serious repercussions such as data theft and loss, which can consequently damage a company’s brand and reputation. Our study of databases in the U.K. unfortunately revealed a disturbing number of exposed databases with no authentication enabled at all.

Most companies in the U.K. use MySQL databases due to their ease of use, affordability, and scalability. At the time of publishing, around 244 vulnerabilities with CVE details were found to affect MySQL databases. Although it does not necessarily follow that exposed databases are also vulnerable, attackers can use their knowledge of database flaws to easily spot potential targets.

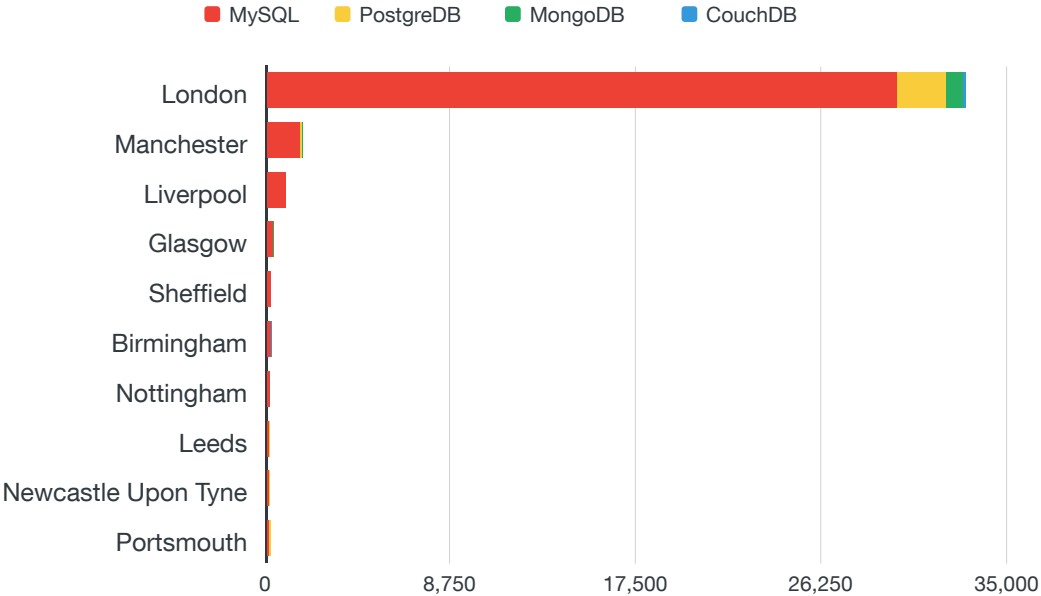


Figure 25. Overview of exposed databases by city

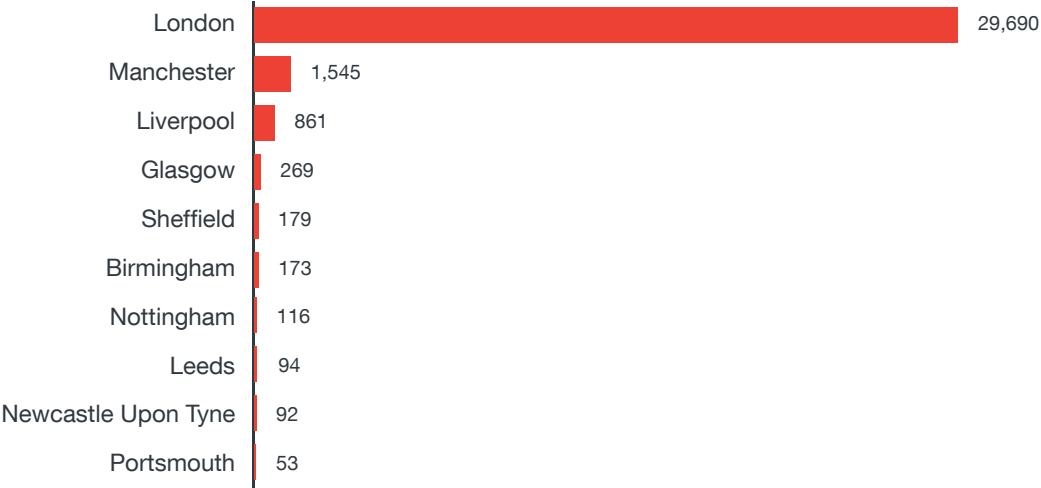


Figure 26. Number of exposed MySQL databases by city

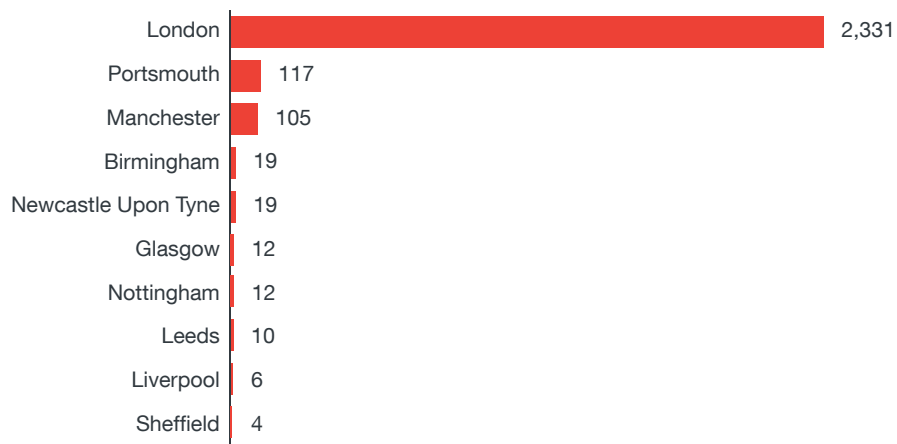


Figure 27. Number of exposed PostgreSQL databases by city



Figure 28. Number of exposed MongoDB databases by city

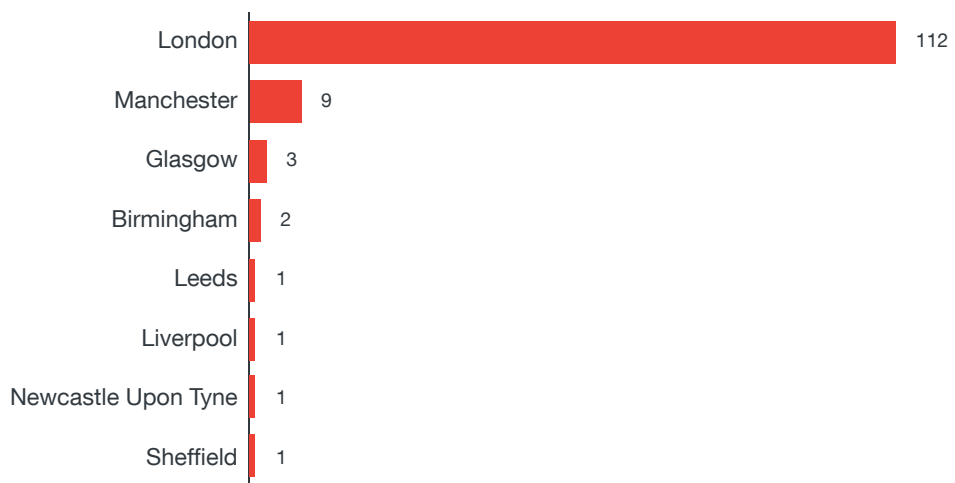


Figure 29. Number of exposed CouchDB databases by city

Exposed Service Protocols

This section explores exposed service protocols such as Remote Desktop Protocol (RDP), Network Time Protocol (NTP), Telnet, FTP, UPnP/SSDP, Simple Network Management Protocol (SNMP), and SSH that were exposed based on the February 2017 Shodan U.K. scan data for the top 10 cities by population. Security flaws found in these protocols could be exploited to breach the security of devices that run them.

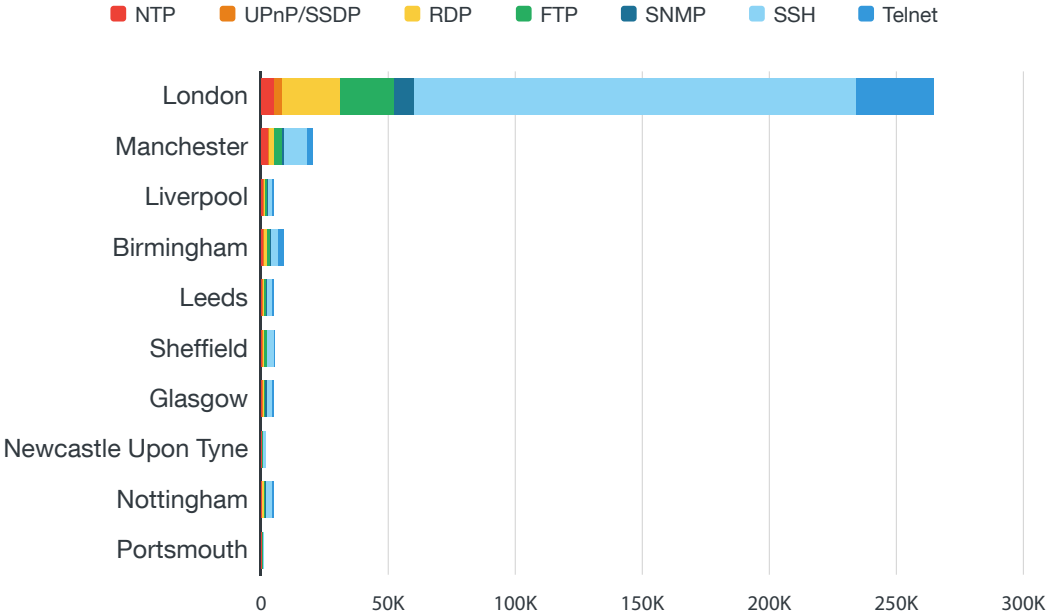


Figure 30. Overview of exposed service protocols by city

Exposed NTP-enabled Devices

Developed by Professor David L. Mills, NTP is a protocol used for the time synchronization of system clocks connected to a network. It is critical¹⁵ for a business in that in case of a breach, the IT administrator can accurately trace back system logs and events to know how the network or system was compromised and possibly track the stolen data. In addition, synchronizing time is critical for running scheduled backups.

Attackers can exploit an NTP bug to launch a DDoS attack via the NTP reflection technique¹⁶ or a man-in-the-middle (MitM) attack.

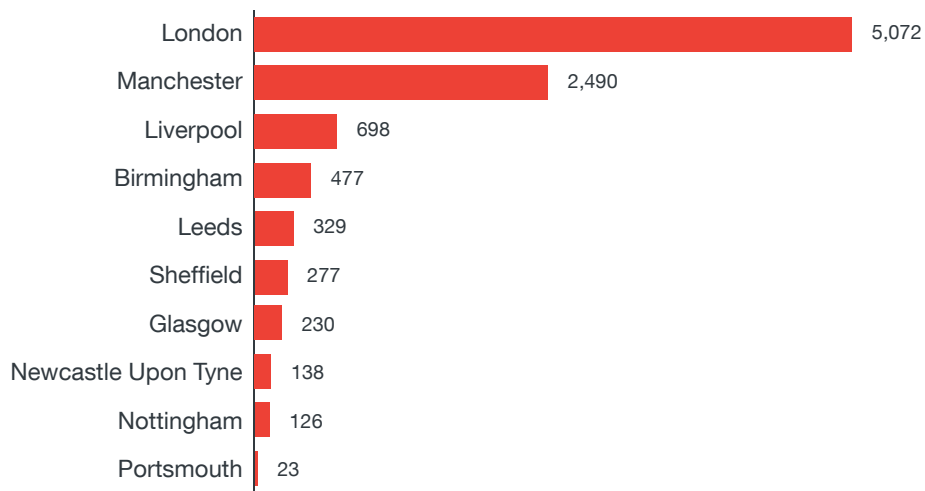


Figure 31. Number of exposed NTP-enabled devices by city

Exposed UPnP-/SSDP-enabled Devices

UPnP enables networked devices such as routers, printers, mobile devices, and computers to see one another in a network and easily conduct functions such as communication and data sharing. SSDP, meanwhile, is used to spot UPnP devices, typically in small office environments. Security bugs found in this protocol could be exploited to infiltrate a network. A quick search of CVE yielded at least 58 entries¹⁷ that either directly or indirectly affected UPnP and 17 entries¹⁸ for SSDP.

A significant number of devices that use Intel® Software for UPnP Technology in London were exposed. Attackers could take advantage of this to amplify network traffic requests in a reflective DDoS attack¹⁹.

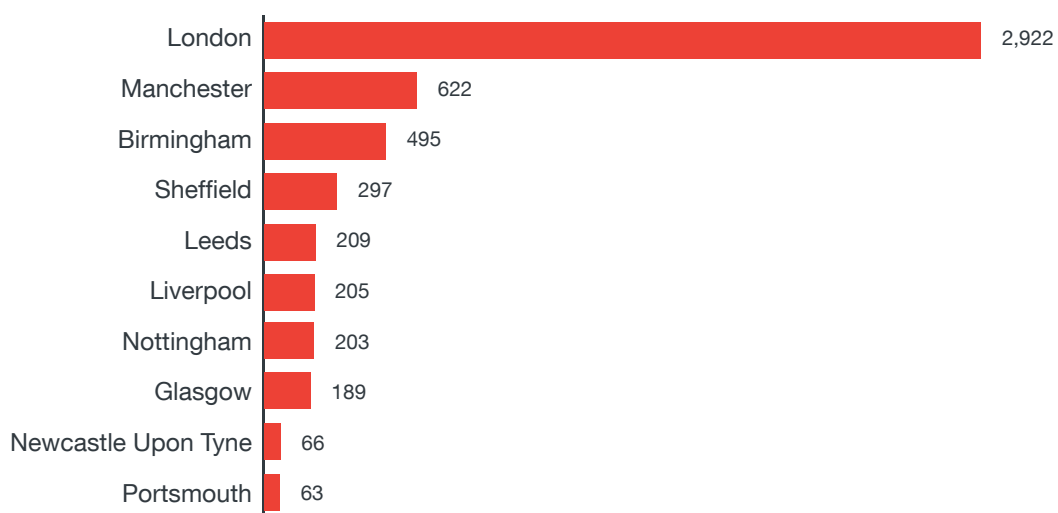


Figure 32. Number of exposed UPnP-/SSDP-enabled devices by city

Exposed SNMP-enabled Devices

Monitoring a network and mapping all of the devices connected to it becomes easier for IT administrators with the aid of SNMP. Attackers can exploit this protocol though to know the network topology of any target company during reconnaissance and lateral movement. Exposed SNMP services in routers, switches, and printers, among others, can put corporate and home networks at risk of several threats including denial of service (DoS) and vulnerability exploitation.

Most of the exposed devices that used SNMP were from London, many of which were tied to certain Cisco router models.

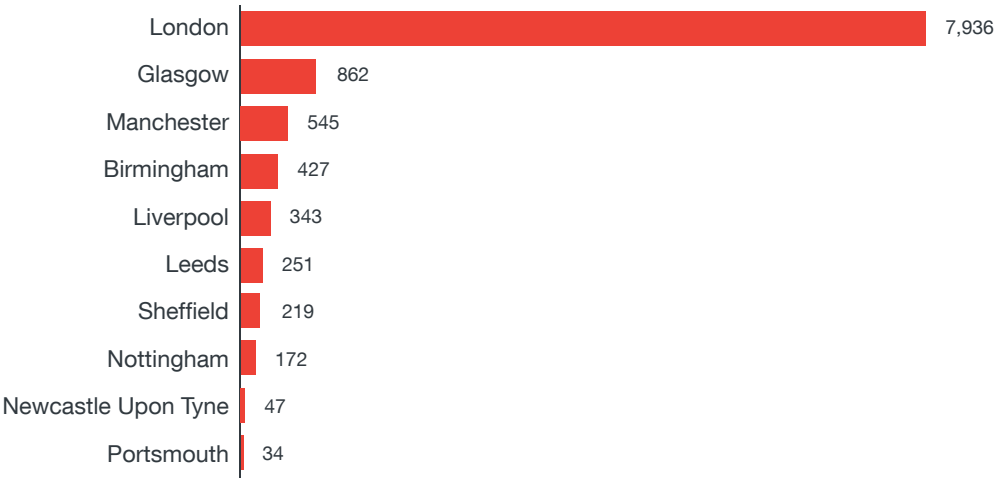


Figure 33. Number of exposed SNMP-enabled devices by city

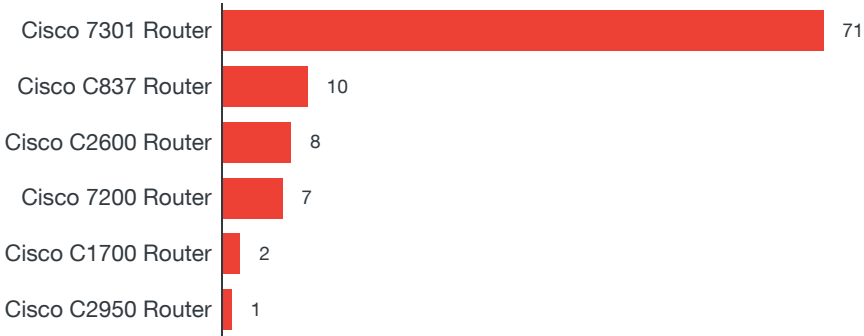


Figure 34. Number of exposed SNMP-enabled devices by product/service name

Exposed SSH-enabled Devices

SSH is one of the most critical protocols on the internet, allowing a wide variety of devices to be remotely accessed in a secure manner. Compromising this port gives threat actors access to a target device as well as network access to the devices connected to the target device through a back channel.

IoT devices are particularly valuable in attacks that exploit open SSH ports because they rarely have strong security despite a processing capacity equal to most modern services. Once a device is breached via this port, it is “owned”; attackers can open and close necessary ports to perform attacks against other targets.

Based on our February 2017 Shodan U.K. scan results for the top 10 cities by population, London had the highest number of exposed devices that used SSH such as NAS devices, routers, and firewalls.

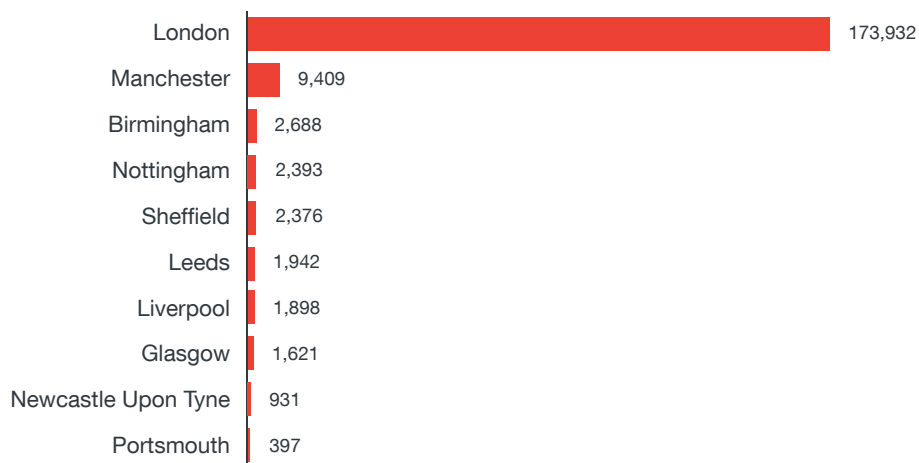


Figure 35. Number of exposed SSH-enabled devices by city

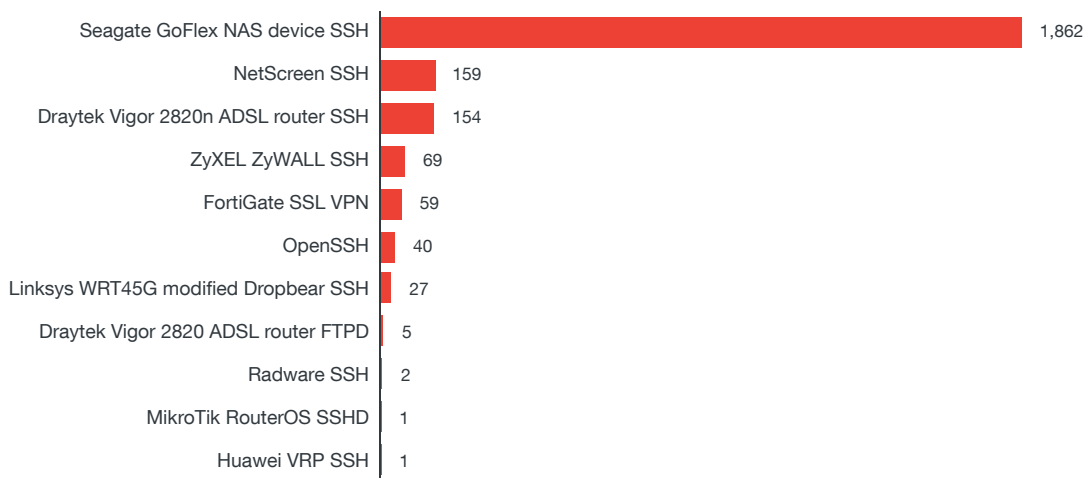


Figure 36. Number of exposed SSH-enabled devices by product/service name

Exposed RDP-enabled Devices

Our findings revealed that the exposure of most devices that used RDP could be attributed to the utilization of Microsoft Windows Remote Procedure Calls (RPC) over HTTP. Abusing RDP is not uncommon as it can aid in data exfiltration (in targeted attacks) or sharing malicious files with systems over a network. A notable example of such an attack was used by Crysis ransomware²⁰, which performed a brute-force RDP attack to transfer the malware from a remote system to a victim’s computer.

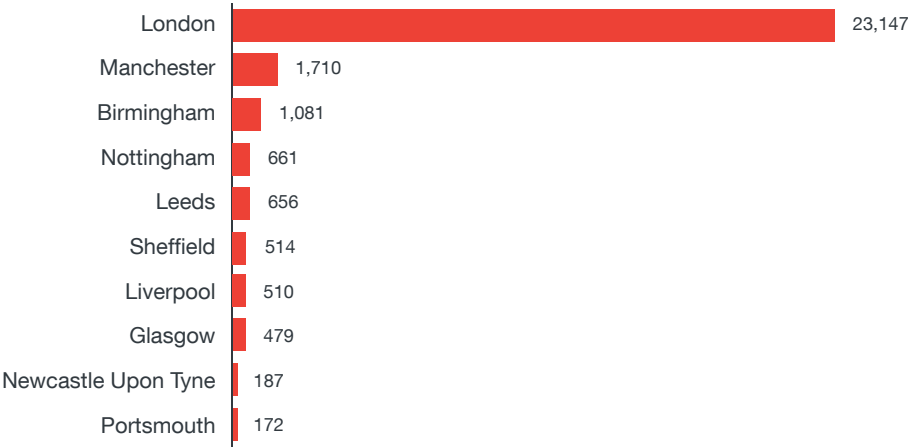


Figure 37. Number of exposed RDP-enabled devices by city

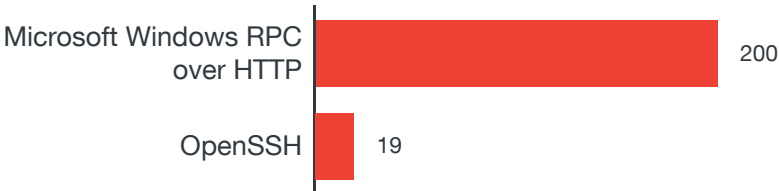


Figure 38. Number of exposed RDP-enabled devices by product/service name

Exposed Telnet-enabled Devices

Telnet, like SSH, is used for device-to-device communication. Telnet sends data in an unencrypted manner (plain text), making it unsecure²¹ and prone to network-packet-sniffing attacks. Threat actors can attack Telnet to intercept credentials and compromise devices.

A significant number of exposed devices that used Telnet were seen in the U.K., most of which were routers and media recording devices.

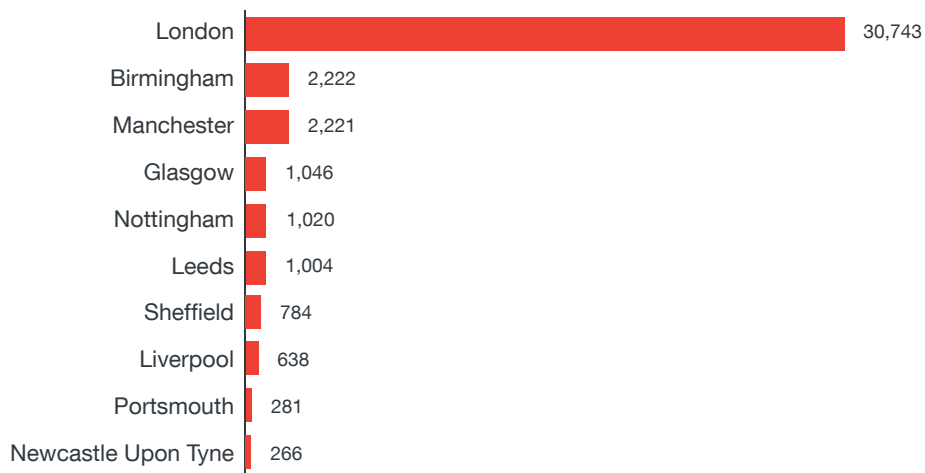


Figure 39. Number of exposed Telnet-enabled devices by city

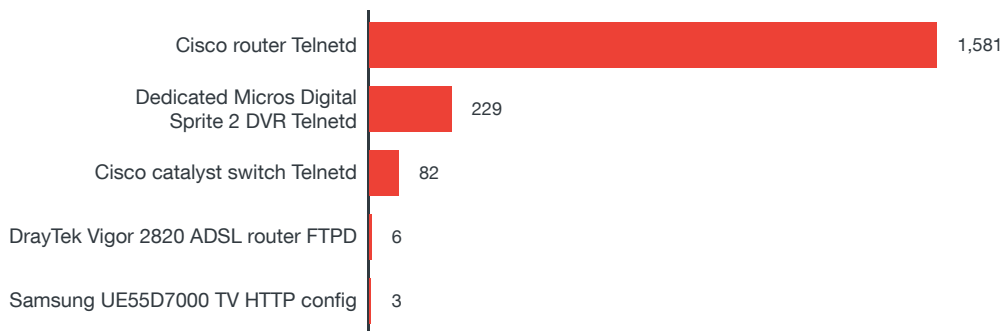


Figure 40. Number of exposed Telnet-enabled devices by product/service name

Exposed FTP-enabled Devices

FTP enables effective file transfers between two systems in the same network. Employees can share data or files in a location on the network that other employees can also access. It is highly dangerous if attackers gain access to a company's FTP because this could allow them to compromise systems and web servers, which contain troves of confidential information.

Findings revealed that a majority of exposed devices that used FTP were from London. This could primarily be due to the fact that London is the U.K.'s technology hub. FTP usage is also a means by which remote server and device operation can be conducted. Based on Shodan data, routers, printers, and NAS and media recording devices were the most exposed FTP-enabled assets.

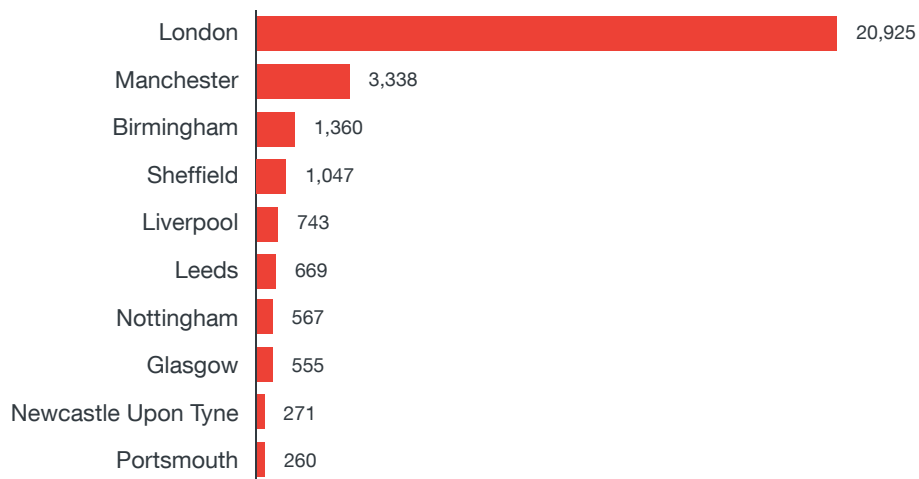


Figure 41. Number of exposed FTP-enabled devices by city

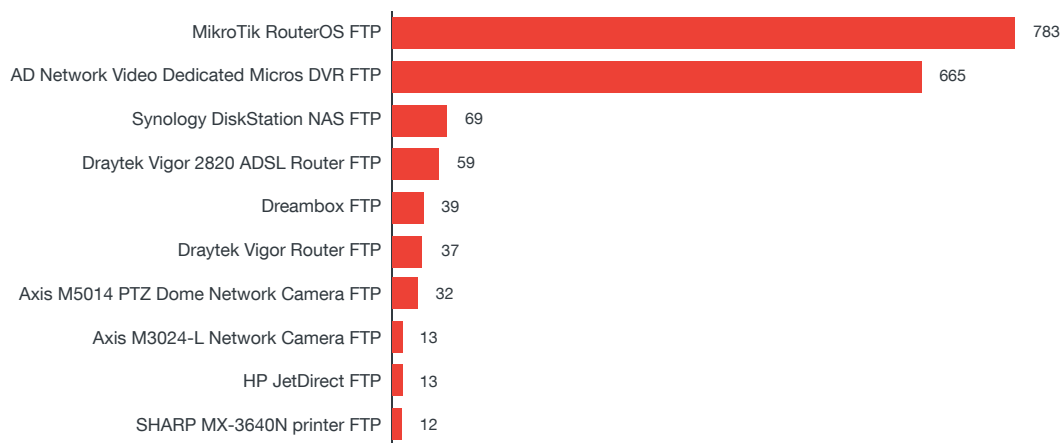


Figure 42. Number of exposed FTP-enabled devices by product/service name

Safeguarding Against Internet Exposure

For Enterprises

Exposure of cyber assets does not directly translate to compromise; rather, exposure means some device, system, or network is poorly configured. On the flip side, by virtue of being exposed on the internet, this device or system is vulnerable to compromise. Knowledge of any open protocol, device, or server would make it easier for threat actors to look for security flaws that may be used to infiltrate a company's network.

GDPR²², which will take effect on May 2018, requires compliance among businesses regardless of size and industry. The regulation puts a premium on protecting the data and privacy of consumers, which could affect enterprises and even small and medium-sized businesses (SMBs)²³ even if they are not physically based in Europe as long as they process the data of EU citizens. Where does cyber asset exposure fit into this? Exposed devices and services can leak information without the users' knowledge, subsequently leading to compliance issues that can cause businesses to possibly pay penalties of as much as 4 percent of their annual turnover. Although the U.K. has decided to separate from the EU in a historical decision (also known as BREXIT), the GDPR will likely affect U.K. companies that handle the data of EU citizens.

EU Directive 2016/1148²⁴ aims to enhance cybersecurity in Europe by creating strategies to secure network and information systems and building computer security incident response teams (CSIRTs) that will take action during cyber incidents. This directive (to be implemented in 2018), which applies to the operators of essential services and digital service providers, can impact U.K. businesses that fall under these categories until BREXIT takes full effect²⁵, supposedly in 2019.

While GDPR focuses on user data, EU Directive 2016/1148 calls for better systems and network security as threats could pose serious dangers and effects on the operations or activities²⁶ of critical sectors such as utilities (specifically water provision), energy, banking or financial services, and education. Any visible

and searchable device over the internet can be the starting point of a far more destructive attack on certain enterprises and organizations.

Given these factors, cyberattack and data breach prevention strategies should be considered an integral part of daily business operations. The key principle of defense is to assume compromise and take countermeasures such as the following:

- Quickly identify and respond to ongoing security breaches.
- Contain the security breach and stop the loss of sensitive data.
- Preemptively prevent attacks by securing all exploitable avenues.
- Apply lessons learned to further strengthen defenses and prevent repeat incidents.

A strong security checklist includes the following:

- Securing the network infrastructure by:
 - Segmenting a network according to function, department, geographic location, level of security, or any other logical separation (taking contractors, third-party vendors, and others into account).
 - Implementing log analysis for threat detection and remediation and building threat intelligence; the data can be fed into Security Information and Event Management (SIEM) software to help a response team understand ongoing attacks.
 - Properly configuring user access profiles, workstations, and servers, including internet-connected devices, using the least-privilege model.
- Protecting sensitive data via:
 - Data classification by determining the sensitivity of data sets and establishing different access and processing guidelines for each category.
 - Establishing endpoint-to-cloud protection through identity-based and cloud encryption.
 - Building a data protection infrastructure with multitiered access where sensitive tiers are in a disconnected network, others require multifactor authentication, and others can remain on regular file servers.
- Building an incident response team consisting of technical, human resources, legal, and public relations personnel, and executive management.
- Building internal and collecting external threat intelligence, acted upon by knowledgeable human analysts who can determine through identifying patterns in attacker's tools, tactics, and procedures (TTPs), if an attack is ongoing inside the network.

Ultimately, no defense is impregnable against determined adversaries. Having effective alert, containment, and mitigation processes is critical. Companies should look further into fulfilling the Critical Security Controls (CSC)²⁷ best practice guidelines published by the Center for Internet Security. The CSC goes through periodic updates to address new risks posed by an evolving threat landscape.

For Homes

Today’s society is adopting connected technologies at a faster rate than we are able to secure them. Every home is unique and hosts a wide variety of connected devices that serve different functions. Unfortunately, there is no one-size-fits-all cybersecurity solution for connected devices. Compared to a business environment, a connected home is unstructured, dynamic, and tends to be function oriented. A vast majority of people are either unaware or unconcerned about the potential security risks that their exposed connected devices pose. The IoT ecosystem is multilayered and risk factors tied to successful compromises increase with each additional layer.

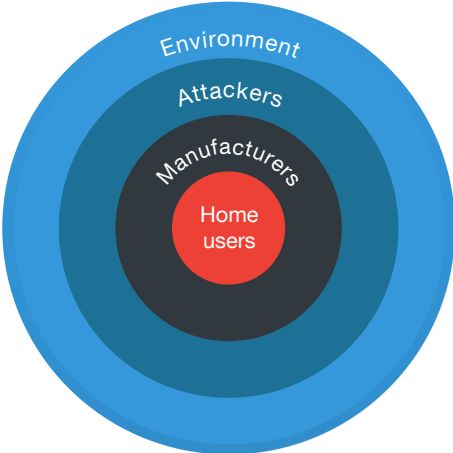


Figure 43. Risk factors increase with each additional layer to the IoT ecosystem

(Source: <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-smart-homes>)

It is not unusual for the average home to have several connected devices. We came up with a set of general guidelines and best practices that home users should follow to protect their connected devices. Many of the recommendations are basic security practices and cybersecurity experts will repeatedly recommend them. When discussing how to secure connected devices at home, we also need to be mindful of three core IoT principles—always online, always available, and easy to use. We also need to remember that the average household does not have a resident IT guru who can secure everything connected so enabling security features should be made as simple as possible. Our recommendations are as follows:

- Enable password protection on your devices. This is an easy option to enable on most connected devices that support passwords. It should be mandatory for smartphones, tablets, laptops, webcams, and so on.
- Replace default with strong passwords. Users routinely do not change the factory default passwords on their devices and these can be easily discovered using any internet search engine. The other usual suspect is weak passwords that can be defeated using brute-force or dictionary attacks.
- Change default settings. Many devices have all their supported services enabled by default, many of which are not essential for regular daily use (e.g., Telnet on webcams). If possible, disable nonessential services. The only caveat is that advanced technical knowledge may be required to decide which services to disable and how to correctly do that. We do not expect the average user to be knowledgeable about this so it is up to device manufacturers to make sure their devices are secure out of the box.
- Do not jailbreak devices. This can disable built-in security features, making it easier for hackers to compromise them. Jailbreaking is popular especially with smartphones as this allows users with phones locked to a particular service provider to make them work for all service providers or in different countries.
- Do not install apps from unverified third-party marketplaces. Only use verified app marketplaces such as Apple's App Store®, Google Play™, Amazon Appstore, and others. This is especially a big security risk for jailbroken iOS and Android™ devices. Apps installed from unverified third-party marketplaces can have backdoors built into them that criminals can use to steal personal information or worse, take control of them. Verified app marketplaces are not immune to hosting malicious apps but the probability of that happening is small.
- Update firmware. This will fix known security vulnerabilities. On the flip side, there are many caveats with firmware updates—some device firmware are not easy to update; the latest firmware may be unstable and introduces new bugs or issues; there are too many devices to update; it is difficult to track firmware updates; users may not see the need to update the firmware when the device is functioning properly; and updating the firmware may not even be possible.
- Enable both disk and communication encryption. Enable disk encryption for smartphones, tablets, laptops, and other devices to secure the data on them even if they are stolen. Encryption is not a bulletproof solution but will secure the data on the disk against theft from the most skilled and resourceful hackers. Enabling HyperText Transfer Protocol Secure (HTTPS) instead of HTTP for communication secures devices against MitM and packet-sniffing attacks.
- Some router-specific best practices include enabling the firewall, using faster but shorter-range 5GHz Wi-Fi signals to limit access-point-hacking attempts, disabling Wi-Fi Protected Setup (WPS) and enabling the Wi-Fi Protected Access-2 (WPA2) security protocol, and using a strong password for Wi-Fi access.

- Other router security suggestions that unfortunately may limit device usage and functionality include configuring the router to limit device network access to set hours during the day or night, disabling UPnP though this will limit the operation of connected devices such as Wi-Fi-enabled printers, and allowing only a hardcoded list of device media access control (MAC) addresses to access a network (the MAC address list will have to be constantly updated).
- In extreme cases, disconnect the device from the network if internet access is optional for it to function properly. But this practice goes against one of the core IoT principles—always online. For devices such as the Wi-Fi bathroom scale, internet access is not required to measure body weight but is a must for sending the information to an online portal that tracks daily changes and provides fitness suggestions.

Connected devices are an integral part of our daily lives. Device security should ideally not affect availability and be transparent to a user. As previously stated, there is no one-size-fits-all cybersecurity solution for connected devices. In addition to the listed best practices and general guidelines, users must be able to rely on device manufacturers to enable strong security out of the box. Ultimately, we may need to rely on security by obscurity—hiding our devices among billions of other connected devices online to avoid getting compromised.

Conclusion

Our analysis of Shodan data for the top 10 U.K. cities by population revealed that London, being the country's capital and thus the most populous, had the highest number of exposed cyber assets. For the rest of the cities on the list, however, the results for exposed devices, databases, and services varied. For instance, although Manchester was the second most populous city in the U.K., it only fell third on the list of cities with the highest number of exposed printers and media recording devices. Glasgow, meanwhile, ranked next to Manchester in terms of overall number of exposed cyber assets even though it was the fifth most populous city.

Firewalls made up the bulk of exposed vulnerable device types, which could spell disaster for businesses and home users that depended on them as their first line of defense. One probable primary cause of this is that the remote administration feature is enabled. The U.K. also had a high number of exposed webcams, which attackers could use for surveillance or stealing and publishing live video feeds from compromised devices.

While exposure does not necessarily translate to vulnerability or infection, this paper aims to shed light on what certain devices, databases, or services are searchable on the internet in the top 10 U.K. cities by population that could pose serious risks if miscreants use them for attacks. Enterprises can use our findings to enhance their database or device security. The cost of compromise can be high, especially with the emergence of policies such as GDPR that require strict compliance.

Appendix

Research Coverage

We covered the following top 10 cities in the U.K. in terms of population.

| City-Region | Region | Population (2011 Census) |
|--------------------------------|--------------------|--------------------------|
| London | Greater London | 9,787,426 |
| Manchester | Greater Manchester | 2,553,379 |
| Birmingham–Wolverhampton | West Midlands | 2,440,986 |
| Leeds–Bradford | West Yorkshire | 1,777,934 |
| Glasgow | Greater Glasgow | 1,209,143 |
| Liverpool | Liverpool | 864,122 |
| Southampton–Portsmouth | South Hampshire | 855,569 |
| Newcastle Upon Tyne–Sunderland | Tyneside | 774,891 |
| Nottingham | Nottingham | 729,977 |
| Sheffield | Sheffield | 685,368 |

Table 2. List of U.K. cities covered in this paper

What Is Shodan?

Scanning the internet is important because security flaws can be quickly discovered and fixed before they are exploited. But it is difficult and time consuming to do because of the massive IP address space that needs to be scanned—IPv4 supports a maximum of 2^{32} unique addresses and IPv6 supports a maximum of 2^{128} unique addresses. In addition to this massive address space, carrier and traditional Network Address Translation (NAT) hides millions of connected nodes. IPv6 gateways also support NAT64, which connects IPv6 to IPv4. Other challenges when scanning the internet include administrators seeing network scans as attacks, some IP ranges being blocked by different countries, legal complaints, dynamic IP addresses, ICS operations affected by active network scanning, powerful hardware required for processing and storage, exclusion lists, agreements with ISPs so they do not block internet access, and so on. For this research, we bypassed all of these issues and hurdles and simply used a public data source—Shodan.

Shodan is a search engine for internet-connected devices. The basic unit of data that Shodan gathers is the banner, which contains textual information that describes a service on a device. For web servers, this would be the headers that are returned; for Telnet, it would be the log-in screen. The banner content greatly varies depending on service type. In addition to banners, Shodan also grabs metadata about a

device such as geographic location, hostname, OS, and more²⁸. Shodan uses a GeoIP database to map the scanned IP addresses to physical locations.

A Shodan crawler works as follows. First, it generates a random IPv4 address. Next, it generates a random port to test from a list of ports that it understands. Finally, it scans the generated IPv4 address on the generated port and grabs any returned banner. This means the Shodan crawlers do not scan incremental network ranges. Completely random crawling is performed to ensure uniform coverage of the internet and prevent bias in the data at any given time. Scan data is collected from around the world to prevent geographic bias. Shodan crawlers are distributed around the world to ensure that any sort of countrywide blocking will not affect the data gathering.

Shodan provides an easy one-stop solution to conduct open source intelligence (OSINT) gathering for different geographic locations, organizations, devices, services, and others. Software and firmware information collected by Shodan can potentially help identify unpatched vulnerabilities in exposed cyber assets. Shodan was the first search engine to bring awareness to the large variety and massive volume of everyday exposed cyber assets all around us.

Shodan Data Analysis

For this research, we partnered with Shodan, who provided us with access to raw scan data in JavaScript Object Notation (JSON) format. We examined the Shodan U.K. scan data for February 2017. Since the Shodan crawler roughly takes three weeks to cycle through the entire IPv4 address space, a month's worth of Shodan scan data provides a fairly accurate picture of the different online devices and systems in the top 10 U.K. cities by population. The data set used contained a total of 29,384,559 records generated from scanning 8,660,791 unique IP addresses. The raw scan data was indexed using Elasticsearch and queried using Kibana, which allowed us to search more than 550 fields instead of only 40 or so fields in Shodan's web interface. Observations and assumptions include the following:

- We did not study month-to-month changes in the Shodan scan data because these tend to be gradual. To observe marked differences, we would need to study changes in the scan data over many months, if not several years, which is outside the scope of this research paper. Realistically, only significant regional or national events will dramatically affect the number of internet-exposed devices and systems; hence, we assumed that a month's worth of scan data would give us an accurate snapshot of what devices and systems are exposed online in Western Europe. Profiling exposed cyber assets in different countries as well as tracking long-term trends in Shodan data will make for interesting future research.

- IP addresses appear and disappear from month to month from the Shodan scan data. In some cases, the devices and systems are offline and the IP address and port scan returns no results. A device or system absent in Shodan does not mean it is not exposed online. On the flip side, Shodan may rescan the same IP address multiple times in the same month (e.g., we found an IP address with 58,143 scan records).
- Explosion in the usage of the internet means the IPv4 address space is fast getting depleted. The IPv4 address space supports a maximum of 2^{32} addresses. IPv6, with its maximum 2^{128} addresses, will more than solve the address space shortage problem but this will still take several years to be fully implemented or adopted. And even then, IPv4 will continue to be used. NAT is an essential tool in conserving global IPv4 address space allocations. NAT allows a single device such as a router to act as an agent between the internet and a local (or “private”) network. This means that only a single unique IP address is required to represent an entire group of computers and devices²⁹. This translates to finding multiple devices and systems visible from the same IP address in the Shodan scan data, most likely sitting behind a router or a firewall.

Hosting Providers

In this research, we excluded IP addresses that belonged to known hosting providers since hosting infrastructure is complex and difficult to map or accurately port to back-end applications. Including hosting providers would also unnecessarily skew the data and impact our overall analysis. The following hosting providers were excluded from our scan data.

- AkamaiGHost
- Amazon.com
- CloudFlare
- Digital Ocean
- Hetzner
- Host1Plus
- Linode
- Microsoft Azure
- Microsoft Hosting
- NTT
- OVH
- Rackspace

References

1. Numaan Huq, Stephen Hilt, and Natasha Hellberg. (15 February 2017). *Trend Micro Security News*. “U.S. Cities Exposed.” Last accessed on 29 August 2017, <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/us-cities-exposed-in-shodan>.
2. U.K. Office for National Statistics. (2011). “Census 2011 Quick Statistic Population density.” Last accessed on 20 September 2017, <http://www.nomisweb.co.uk/census/2011/qs102ew>.
3. David Sancho. (7 April 2014). *TrendLabs Security Intelligence Blog*. “Windows XP Support Ending—Now What?” Last accessed on 29 August 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/windows-xp-support-ending-now-what/>.
4. Pawan Kinger. (8 April 2014). *TrendLabs Security Intelligence Blog*. “Skipping a Heartbeat: The Analysis of the Heartbleed OpenSSL Vulnerability.” Last accessed on 31 August 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/skipping-a-heartbeat-the-analysis-of-the-heartbleed-openssl-vulnerability/>.
5. The MITRE Corporation. (2015). *Common Vulnerabilities and Exposures*. “CVE-2015-0204.” Last accessed on 31 August 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2015-0204>.
6. The MITRE Corporation. (2013). *Common Vulnerabilities and Exposures*. “CVE-2013-1899.” Last accessed on 31 August 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1899>.
7. The MITRE Corporation. (2016). *Common Vulnerabilities and Exposures*. “CVE-2016-9244.” Last accessed on 31 August 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9244>.
8. The MITRE Corporation. (2013). *Common Vulnerabilities and Exposures*. “CVE-2013-1391.” Last accessed on 31 August 2017, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1391>.
9. The MITRE Corporation. (2015). *Common Vulnerabilities and Exposures*. “CVE-2015-2080.” Last accessed on 31 August 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2080>.
10. Brian Prince. (16 October 2014). *Security Week*. “Attackers Abuse UPnP Devices in DDoS Attacks, Akamai Warns.” Last accessed on 26 September 2017, <http://www.securityweek.com/attackers-abuse-upnp-devices-ddos-attacks-akamai-warns>.
11. Loulla-Mae Eleftheriou-Smith. (20 November 2014). *The Independent*. “Baby Monitors, CCTV Cameras, and Webcams from U.K. Homes and Businesses Hacked and Uploaded onto Russian Website.” Last accessed on 29 August 2017, <http://www.independent.co.uk/life-style/gadgets-and-tech/baby-monitors-cctv-cameras-and-webcams-from-uk-homes-and-businesses-hacked-and-uploaded-onto-russian-9871830.html>.
12. Trend Micro. (31 January 2017). *TrendLabs Security Intelligence Blog*. “Routers Under Attack: Current Security Flaws and How to Fix Them.” Last accessed on 5 September 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/routers-under-attack-current-security-flaws-and-how-to-fix-them/>.
13. Brian Krebs. (21 October 2016). *Krebs on Security*. “Hacked Cameras, DVRs Powered Today’s Massive Internet Outage.” Last accessed on 6 September 2017, <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>.
14. Q-Success. *W3Techs*. “Usage of Web Servers for Websites.” Last accessed on 5 September 2017, https://w3techs.com/technologies/overview/web_server/all.
15. Paul Rubens. (15 December 2009). *Enterprise Networking Planet*. “It’s About Time: Why Your Network Needs an NTP Server.” Last accessed on 29 August 2017, <http://www.enterprisenetworkingplanet.com/netsp/article.php/3853601/Its-About-Time-Why-Your-Network-Needs-an-NTP-Server.htm>.

16. Lucian Constantin. (11 February 2014). *Computerworld*. "Attackers Use NTP Reflection in Huge DDoS Attack." Last accessed on 29 August 2017, <http://www.computerworld.com/article/2487573/network-security/attackers-use-ntp-reflection-in-huge-ddos-attack.html>.
17. The MITRE Corporation. (2017). *Common Vulnerabilities and Exposures*. Last accessed on 29 August 2017, <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=UPnP>.
18. The MITRE Corporation. (2017). *Common Vulnerabilities and Exposures*. Last accessed on 8 September 2017, <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SSDP>.
19. Bill Brenner. (15 October 2014). *Akamai.com*. "UPnP Devices Used in DDoS Attacks." Last accessed on 26 September 2017, <https://blogs.akamai.com/2014/10/upnp-devices-used-in-ddos-attacks.html>.
20. Jay Yaneza. (9 February 2017). *TrendLabs Security Intelligence Blog*. "Brute-Force RDP Attacks Plant CRYISIS Ransomware." Last accessed on 29 August 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-cryisis-ransomware/>.
21. Erez Zukerman. (15 December 2011). *MakeUseOf.com*. "What Is Telnet & What Are Its Uses?" Last accessed on 29 August 2017, <http://www.makeuseof.com/tag/telnet-makeuseof-explains/>.
22. Trend Micro. "EU General Data Protection: Time to Act." Last accessed on 29 August 2017, <http://www.trendmicro.co.uk/enterprise/data-protection/eu-regulation/>.
23. Trend Micro. (20 December 2016). *Trend Micro Security News*. "A Practical Introduction to the European General Data Protection Regulation for SMBs." Last accessed on 29 August 2017, <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/a-practical-introduction-to-the-european-general-data-protection-regulation-for-smb>.
24. The European Parliament and the Council of the European Union. (6 July 2016). *Official Journal of the European Union*. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union." Last accessed on 31 August 2017, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN>.
25. Alice Foster. (23 June 2017). *Express*. "EU Referendum 2016 Aftermath: All the Key Dates: When Will Britain Leave the EU?" Last accessed on 31 August 2017, <http://www.express.co.uk/news/politics/644178/EU-referendum-dates-European-Union-Brexit-David-Cameron-Brussels>.
26. The Mayer Brown Practices. (July 2016). "A New EU Framework on Cybersecurity: The Network and Information Security Directive." Last accessed on 31 August 2017, https://www.mayerbrown.com/files/Publication/5da28c2e-a8fd-4f19-bdc2-d62d6fc27f0b/Presentation/PublicationAttachment/2b75998a-2615-4e9d-828b-ee9b6e8e96e3/cybersecurity-update_jul2616.pdf.
27. CIS. (2016). *CIS*. "CIS Controls for Effective Cyberdefense." Last accessed on 29 August 2017, <https://www.cisecurity.org/critical-controls/>.
28. Paul Didier, Fernando Macias, James Harstad, Rick Antholine, Scott A. Johnston, Sabina Piyevsky, Mark Schillace, Gregory Wilcox, Dan Zaniewski, and Steve Zuponcic. (9 September 2011). *Cisco and Rockwell Automation*. "Converged Plantwide Ethernet (CPwE) Design and Implementation Guide." Last accessed on 29 August 2017 https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter2.html.
29. Jeff Tyson. (2 February 2001). *HowStuffWorks.com*. "How Network Address Translation Works." Last accessed on 29 August 2017, <http://computer.howstuffworks.com/nat.htm>.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud

www.trendmicro.com