



Western European Cities Exposed

A Shodan-based Security Study on Exposed Cyber
Assets in Western Europe

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.

for Raimund Genes (1963-2017)

Contents

4

Exposed Cyber Assets

7

Exposed Cities:
Western European
Capitals

13

Exposed Cyber Assets
in Western European
Capitals

38

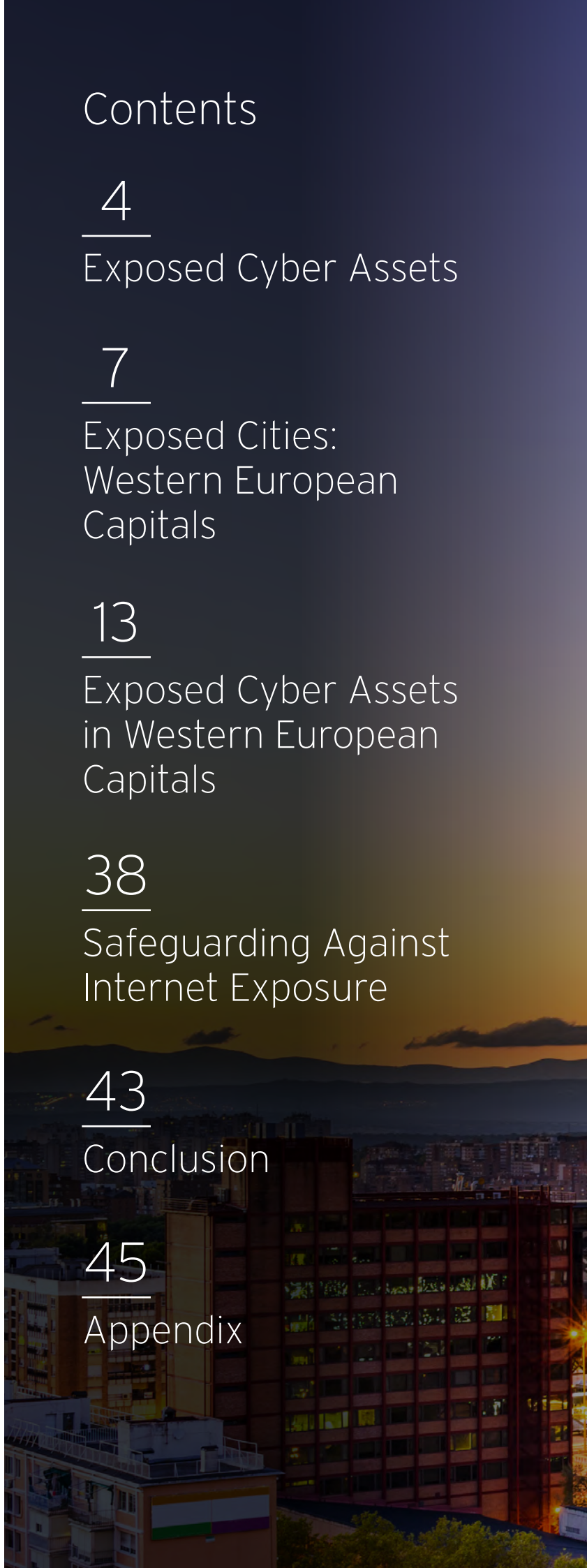
Safeguarding Against
Internet Exposure


43

Conclusion

45

Appendix

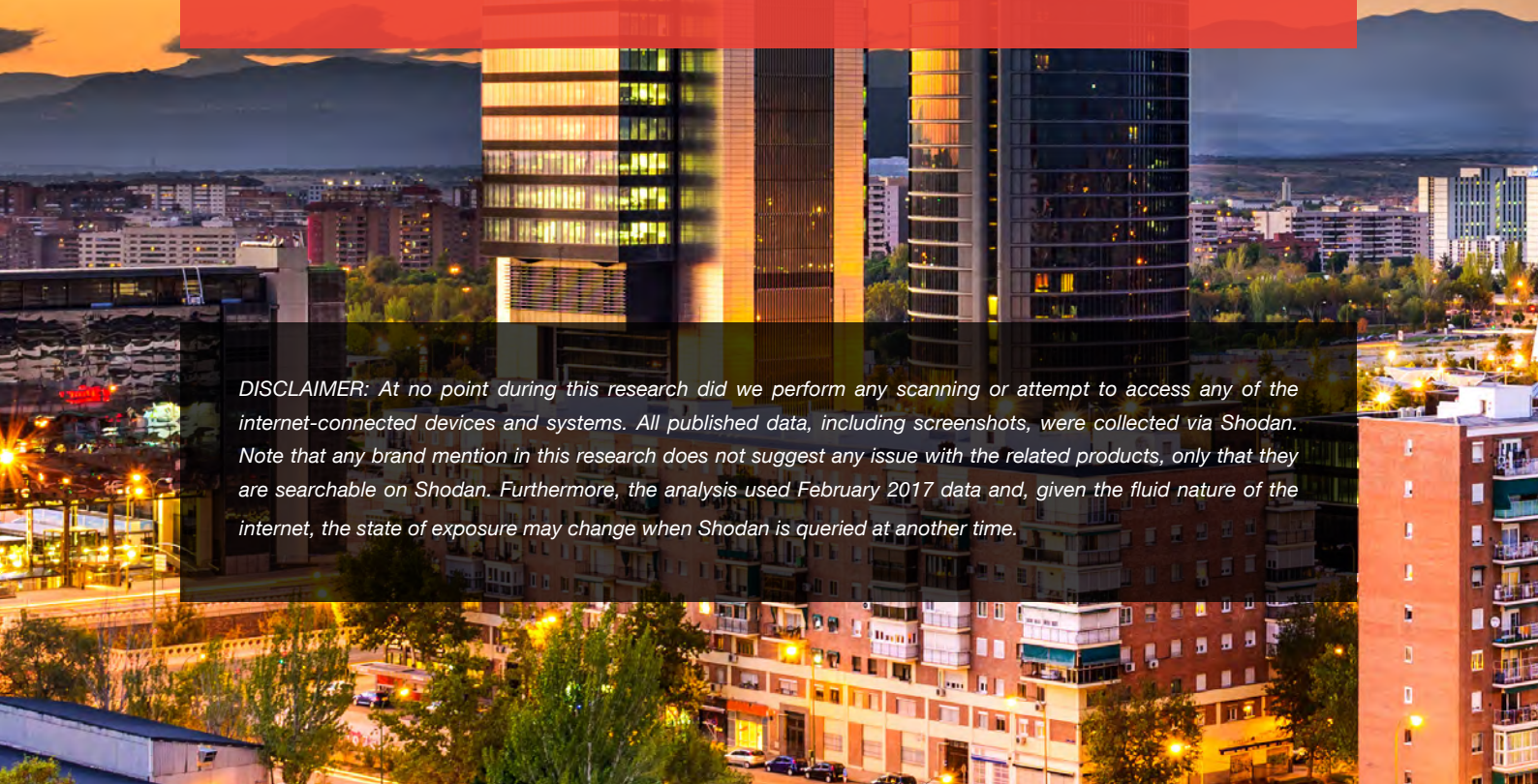




Much of the success of cyberattacks or any prevalent threat is due to security gaps, whether in devices or network topology, exploited by cybercriminals and threat actors. Leaving systems, servers, or devices exposed on the internet is one such gap. Exposed cyber assets are internet-connected devices and systems that are discoverable via network enumeration tools, Shodan, or similar search engines and are accessible via the public internet. Exposed cyber assets potentially introduce serious risks such as data theft, system compromise, and fraud, among others. Depending on the end goal, actors targeting cyber assets are not only limited to cybercriminal groups but also include nation-states, competitors, hacktivists, and script kiddies.

Our paper “U.S. Cities Exposed¹” sparked the right discussions around what network administrators and users in the U.S. can do to minimize the exposure of and secure internet-connected devices. We continue our exploration of exposed cities and ask the same kinds of questions, this time about Europe, which has a similar profile with the U.S. when it comes to internet penetration and device usage². What does Western Europe’s landscape of internet-connected devices look like?

The main goal of this research paper series is to build public awareness about exposed cyber assets in Western Europe and to highlight problems and risks associated with them. In this paper, we uncovered exposed cyber assets in 10 representative capitals of Western European countries. We identified what devices, products, and services were exposed, where, and to what extent. Other papers in this series drill deeper, focusing on three countries—the U.K., France, and Germany.



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 devices and systems that are internet facing and that respond to requests either via network management or enumeration tools such as a ping or are discoverable by internet scanners like Shodan or similar search engines. To say a certain device or system is exposed does not automatically imply that the cyber asset is vulnerable or compromised. It simply means that the device or system can potentially be remotely connected to the internet—and therefore attacked.

Since an exposed cyber asset is accessible and visible to the public, attackers can take advantage of the available information about the machine. Whether by searching on internet scanners or directly profiling the machine using a variety of network tools such as Nmap, attackers can collect information on the device (including its potential vulnerabilities) and use that to mount an attack. For instance, an attacker might check if the associated software of a device is vulnerable or the administration console password is easy to crack.

This is why scanning the internet is a valuable exercise. As with other intelligence-gathering activities, it is important to understand where points of potential weakness exist given the homogeneous and highly interconnected nature of the internet. But scanning the internet is difficult and time consuming to do and poses a set of unique challenges. For our research on exposed cyber assets, we partnered with Shodan, a publicly available search engine for internet-connected devices and systems, to obtain scan data.

Shodan finds and lists devices and systems such as webcams, baby monitors, medical equipment, industrial control systems (ICS), home appliances, and databases. It collates and renders searchable both device metadata and banner information (i.e., services running) that internet-connected devices and systems are freely sharing with anyone who queries them. A majority of these require public internet access to function properly and thus, by their very nature, are exposed (e.g., firewalls). Some, such as ICS and medical devices, should never be directly connected to the public internet. If not properly configured, by virtue of being exposed on the internet, some of these devices and systems may be vulnerable to compromise and exploitation. This is not only a security issue; there is also the elephant in the room—privacy. What sensitive information, if any, is being exposed online?

Important questions that come to mind are:

- What potential risks are associated with exposed cyber assets? If not sufficiently hardened and safeguarded, risks include:
 - Exposed cyber assets could get compromised by hackers who steal sensitive data (e.g., personally identifiable information [PII], intellectual property, financial and corporate data, etc.).
 - Exposed cyber assets could leak sensitive data online without the owners' knowledge (e.g., open directories on web servers, unauthenticated webcam feeds, exposed ICS human machine interfaces [HMIs], etc.).
 - Hackers may use lateral movement strategies to gain entry into a corporate or an ICS network by compromising exposed cyber assets then commit espionage, sabotage, or fraud.
 - Compromised cyber assets can be used to run illegal operations such as launch distributed denial-of-service (DDoS) attacks, make them part of botnets, host illegal data, use them for fraud, and so on.
 - Compromised cyber assets can be held hostage for ransom. This is especially damaging if they are critical to an organization or individual's operations.
 - Cyber assets that operate critical infrastructure can jeopardize public safety if compromised.
- Why are cyber assets exposed on the internet? Common reasons for device and system exposure online include:
 - Incorrectly configured network infrastructure that allow direct device or system access
 - Devices and systems need to be internet connected in order to function properly
 - Remote access is enabled on devices and systems for remote troubleshooting or operation
- Who is targeting exposed cyber assets? Threats come from a variety of sources, depending on the types of cyber assets targeted. Actors include:
 - Nation-states, both developed and developing, which gather intelligence using software espionage tools and customized malware
 - Criminal syndicates, which include both criminal gangs who target consumers using different schemes such as ransomware to profit and those contracted by national governments for various political cyberattacks, including cyberespionage and subterfuge
 - Cyberterrorists who launch disruptive or destructive cyberattacks to cause physical destruction of property or potential loss of life and spread fear

- Competitors who look for information in order to gain strategic advantages over others in the industry
- Hacktivists or internet activists who attack cyber assets to draw attention to their causes
- Script kiddies, which represent the vast majority of threat actors who scan the internet to discover exposed smart and connected devices either out of curiosity or cause mischief

Today's digital warfare is asymmetrical with falling costs for those bent on disruption and fixed or increasing costs for the disrupted society. The cost of finding and exploiting critical infrastructure will continue to fall. The marginal cost of copying vulnerable infrastructure lists or exploits will tend toward zero. The cost of causing disruptions for hackers will continue to fall while that of disruption remediation will increase or remain relatively constant. An understanding of the exposure landscape and one's network and its attendant weaknesses is thus crucial.

Exposed Cities: Western European Capitals

For this research, we examined Shodan's Western European scan data for February 2017. We excluded 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 8,667,083 records generated from scanning 2,751,346 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 compared to 40 or so fields in Shodan's web interface.

Technical assumptions and observations about our use of Shodan data can be found in the Appendix, where we also further discuss what Shodan is and how we analyzed the data it generated. The list of hosting providers whose IP addresses were excluded can also be found in the Appendix.

Cyber Asset Exposure in Western European Capitals

Based on our analysis of Shodan data, the following capital cities in Western Europe together had more than 10 million exposed systems. London and Berlin had more than 2.5 million exposed systems while Amsterdam and Madrid numbers were in the region of a million. These results were mostly expected as London, Berlin, and Amsterdam all had large hi-tech sectors and hosted a large number of internet service providers (ISPs) that support the region.

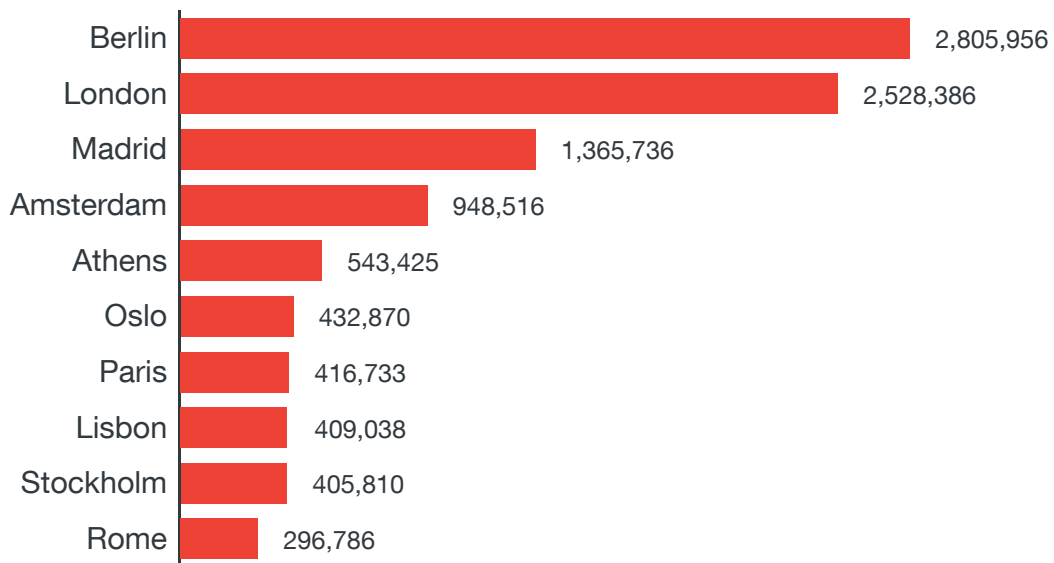


Figure 1. Number of exposed cyber assets in Western European capitals

When exposure is calculated based on per capita, places such as Amsterdam, Berlin, and Lisbon proportionally had significantly higher exposure levels than other cities. Conversely, some cities such as Paris, Athens, and Rome where we expected to see much higher per capita numbers did not have high exposure levels.



Figure 2. Exposed cyber assets per capita

(Number of exposed cyber assets for every 10 people in Western European capitals)

For the purposes of this research, we considered these 10 capital cities, chosen based on a combination of size, geographic diversity, and relative global presence, as representative of Western European cities as a whole and looked into different statistics for each.

How Exposed Devices Access the Internet

A vast majority of exposed devices in Western European capitals access the internet via Ethernet or modems. This observation likely reflects corporate and enterprise users running high-speed connected servers on the internet. Large ISPs such as Strato AG, Digital Ocean, Linode, and OVH operated the largest percentages of these servers (23, 27, 17, and 5 percent, respectively).

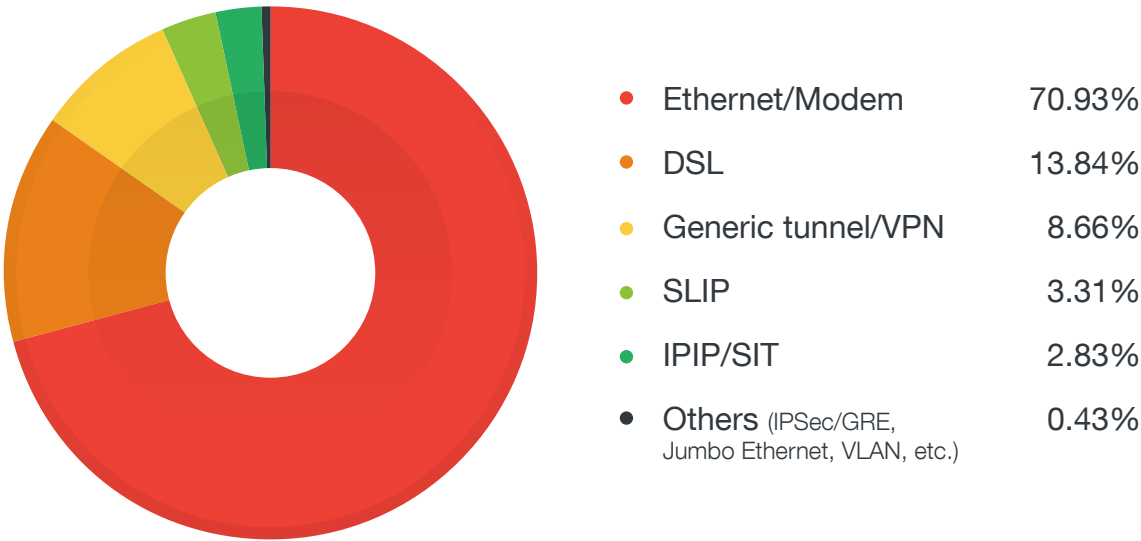


Figure 3. Distribution of means by which exposed devices access the internet

OSs Running on Exposed Internet-connected Devices

A majority (62 percent) of the exposed devices run on Linux-based OSs while Windows-based systems taken together accounted for roughly 20 percent. Upon closer analysis, this could be attributed to the large number of exposed web services related to Apache web servers, which predictably ran on Unix-based OSs.

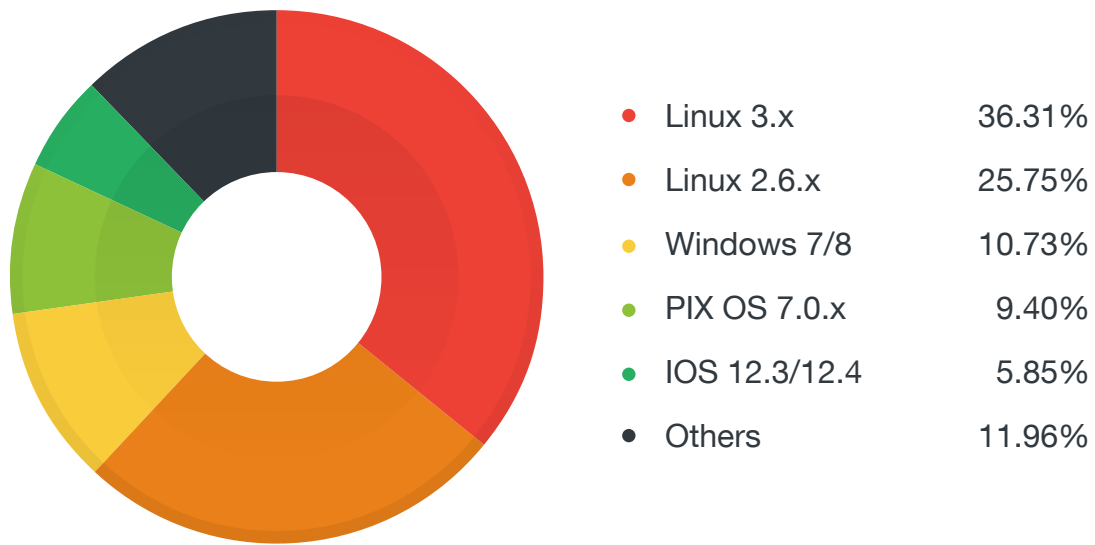


Figure 4. Distribution of OSs that run on exposed devices

Top Exposed and Vulnerable Products

The most exposed products in Western European capitals were software related to HyperText Transfer Protocol (HTTP) web servers such as Apache HyperText Transfer Protocol daemon (HTTPD), NGINX, OpenSSH, and Microsoft™ Internet Information Services (IIS) HTTPD. While this is an expected result, it also gave us an idea why internet-facing servers were such an attractive target for cybercriminals. Historically, cybercriminals targeted web servers with exploits using either zero-day or known and patched vulnerabilities. Administrators should be keenly aware of vulnerability issues, developments, and patches in order to keep their intrinsically open properties secure.

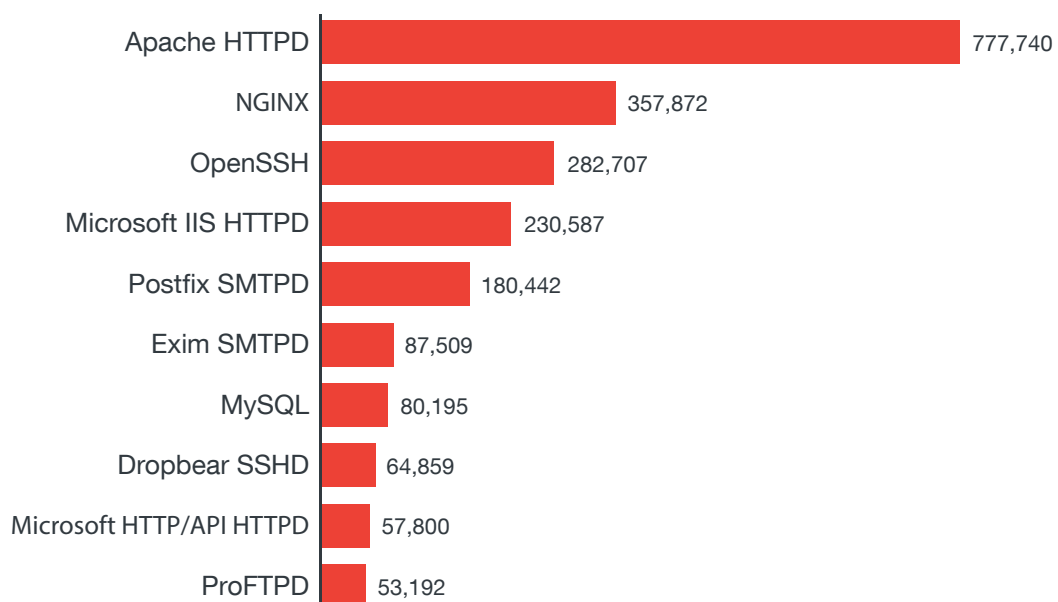


Figure 5. Number of exposed cyber assets by product/service name (top 10)

The Shodan crawler also tests for specific vulnerabilities including CVE-2013-1391³ (digital video recorder [DVR] configuration disclosure), CVE-2013-1899⁴ (argument injection in PostgreSQL), CVE-2014-0160⁵ (Heartbleed⁶, OpenSSL), CVE-2015-0204⁷ (Freak⁸, OpenSSL), CVE-2015-2080⁹ (Jetty remote unauthenticated credential disclosure), and CVE-2016-9244¹⁰ (Ticketbleed, Transport Layer Security [TLS]/Secure Sockets Layer [SSL] stack in BIG-IP virtual servers).

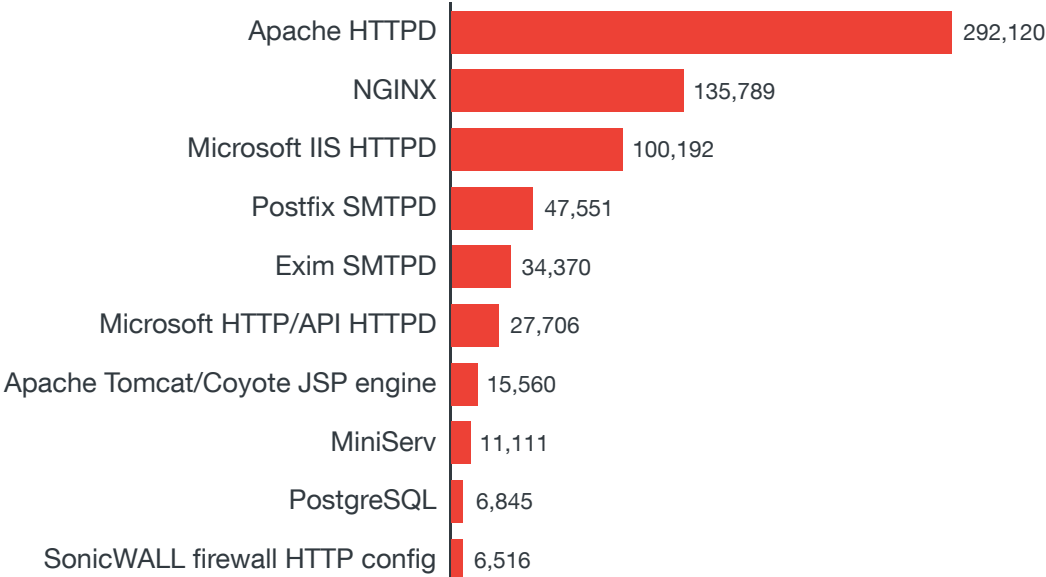


Figure 6. Number of exposed cyber assets by product/service name vulnerable to CVE-2013-1391, CVE-2013-1899, CVE-2014-0160, CVE-2015-0204, CVE-2015-2080, or CVE-2016-9244 (top 10)

Top 10 Exposed and Vulnerable Device Types

The bulk of exposed device types in Western European capitals included wireless access points (WAPs), which are generally networking hardware devices that allowed a Wi-Fi device to connect to a network. This is in no small part because of the heavy usage of Fritz!Boxes throughout Germany. Fritz!Boxes are fairly popular residential gateway devices that also provided VoIP services and have a large market share of the German DSL consumer base. The risk of exposed devices like these was already made clear in 2014 when criminals attacked port 443 on Fritz!Boxes to obtain user passwords, which they then used to avail of value-added telephone services charged to victims’ accounts^{11, 12, 13}.

We expected to find a number of firewalls in the scan data as they typically had internet-facing front ends. However, what was more interesting was the number of open webcams throughout Western European capitals. While homeowners or security teams installed webcams to monitor properties and prevent theft, exposed webcams defeated the intent by allowing outsiders to view private security feeds.

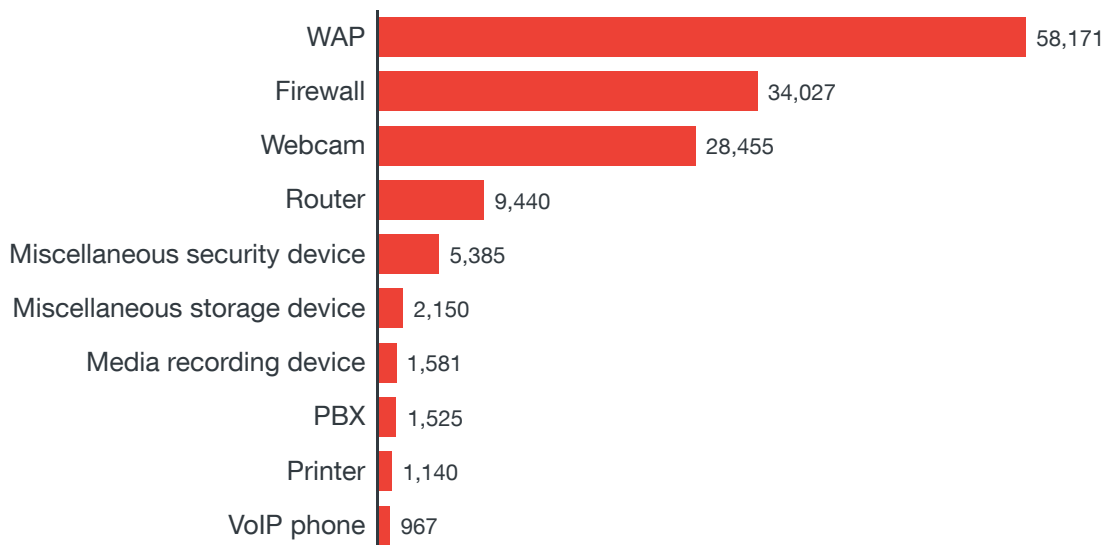


Figure 7. Number of exposed cyber assets by device type (top 10)

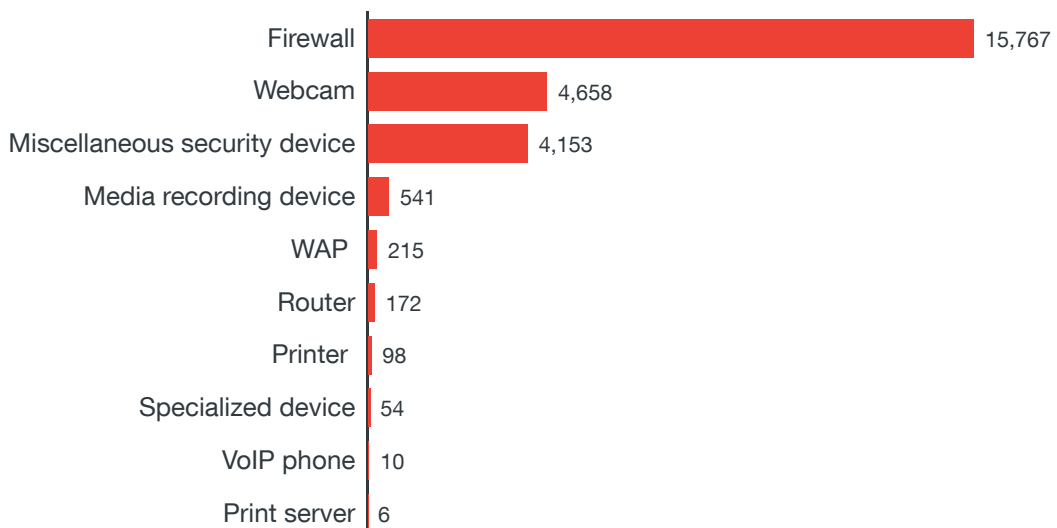


Figure 8. Number of exposed cyber assets by device type vulnerable to CVE-2013-1391, CVE-2013-1899, CVE-2014-0160, CVE-2015-0204, CVE-2015-2080, or CVE-2016-9244 (top 10)

Exposed Cyber Assets in Western European Capitals

Exposed Devices

This section digs deeper into the various exposed devices we found in Western European capitals using Shodan scan data for February 2017, including webcams; routers; printers; and NAS, VoIP, and media recording devices. These exposed devices are at risk of data theft, lateral movement, forced participation in DDoS attacks, and other threats.

Exposed Webcams

One of the reasons webcams are often the first exposed cyber asset that comes to mind is because of the rise in its visibility in homes, public spaces, retail stores, and the like. Add to that the number of highly publicized news reports of hacked webcams and how easy it is to find exposed webcams online; one would think more effort would be made to secure them.

We were able to find several open webcams that allowed outsiders to view inside houses, retail areas, warehouses, and other private spaces, especially in Athens and Stockholm. On the flip side, it was very good to see that certain cities had no open webcams—webcams for which no authentication was required to observe the images being captured—for instance, London and Brussels (not shown here).

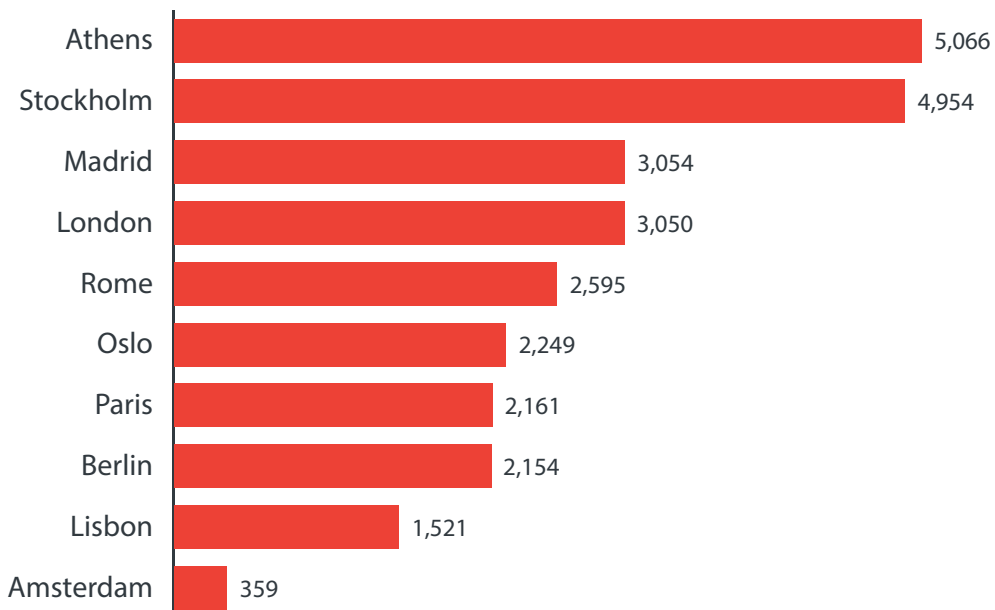


Figure 9. Number of exposed webcams by capital

We summarized the exposed webcams by brand or product name and found D-Link to be the most widely used. Webcams are rarely patched and most do not have auto-update functionality. This means they will remain vulnerable for months or even perpetually after purchase. Furthermore, it has long been known that the Achilles heel of webcams are users who do not change default passwords or use weak passwords that are vulnerable to brute-force or dictionary attacks.

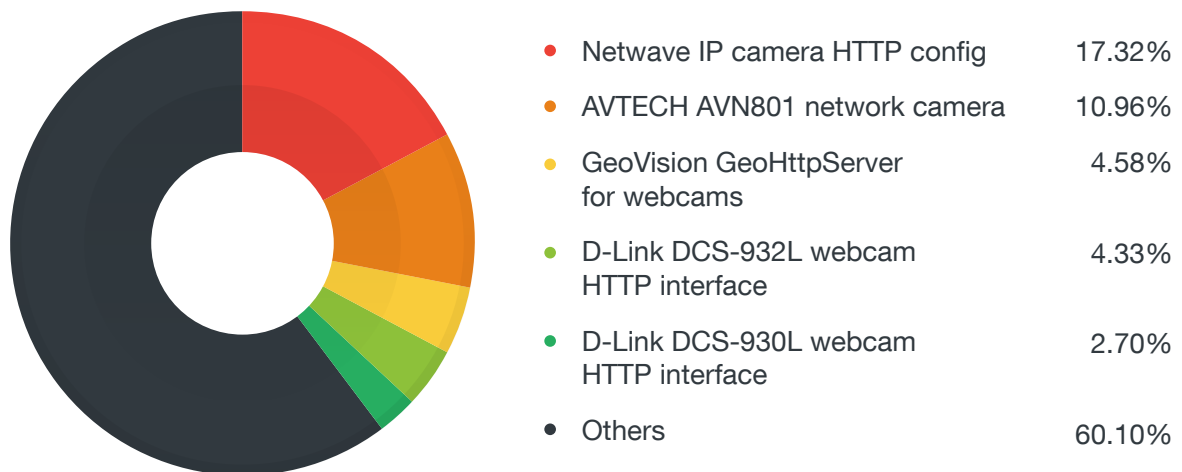


Figure 10. Distribution of exposed webcams by product/service name

The following images are some examples we found from open webcams.

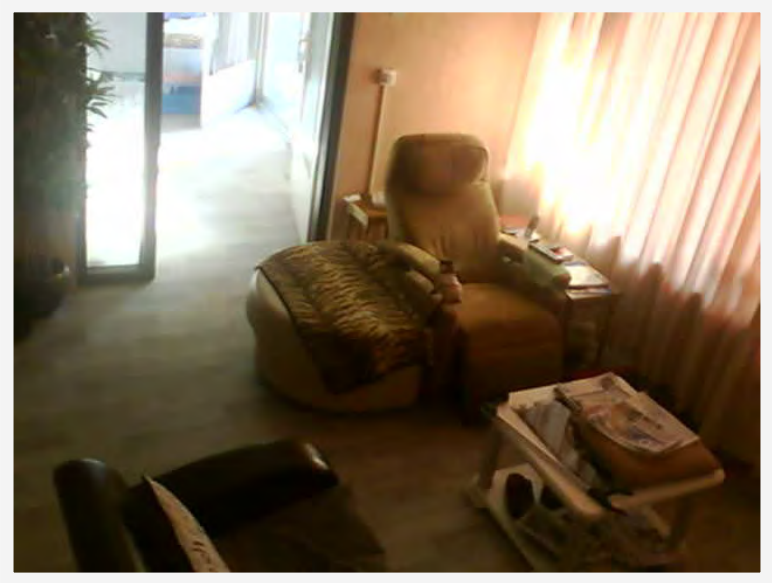


Figure 11. Webcam image from inside a home in Amsterdam



Figure 12. Webcam image of cell towers in Athens

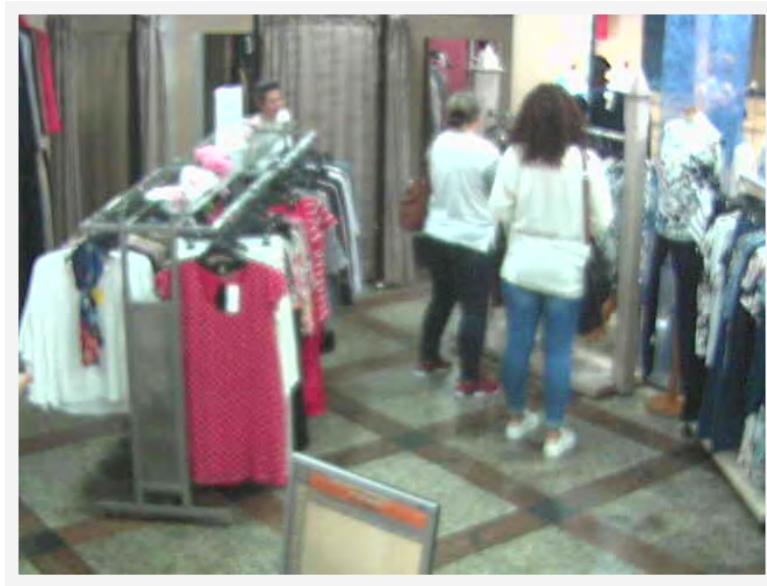


Figure 13. Webcam image in a retail store in Lisbon



Figure 14. Webcam image of a warehouse area in Stockholm

Exposed NAS Devices

Not a lot of NAS devices were exposed in Western European capitals but they are of interest because they are popular solutions for sharing files in collaborative work environments, system backups, and data storage. This means they can contain sensitive information that companies would want to keep private.

That said, we were still able to find a handful of exposed NAS devices. The most exposed product was Seagate GoFlex NAS, a consumer-grade device likely found in home networks and whose users were not aware of the need to secure them.

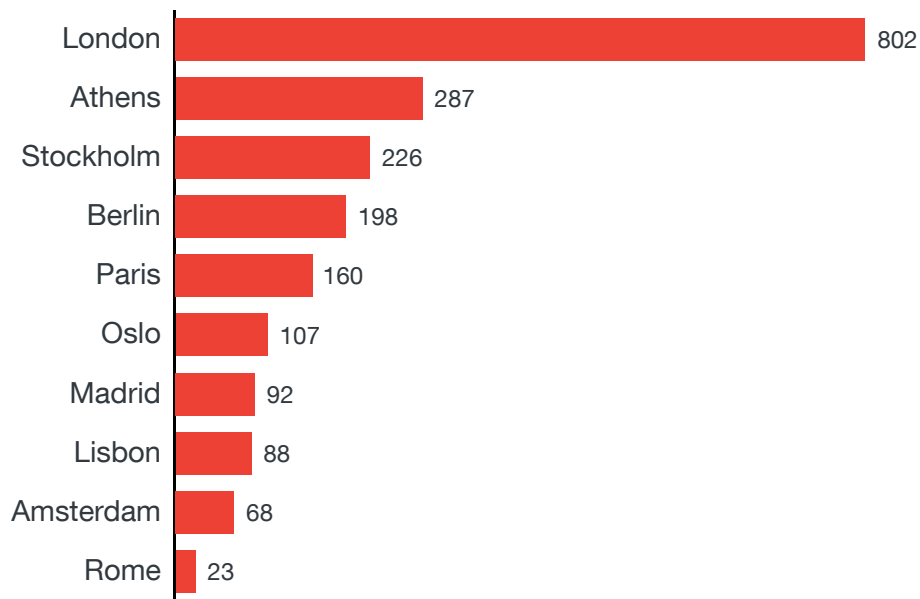


Figure 15. Number of exposed NAS devices by capital

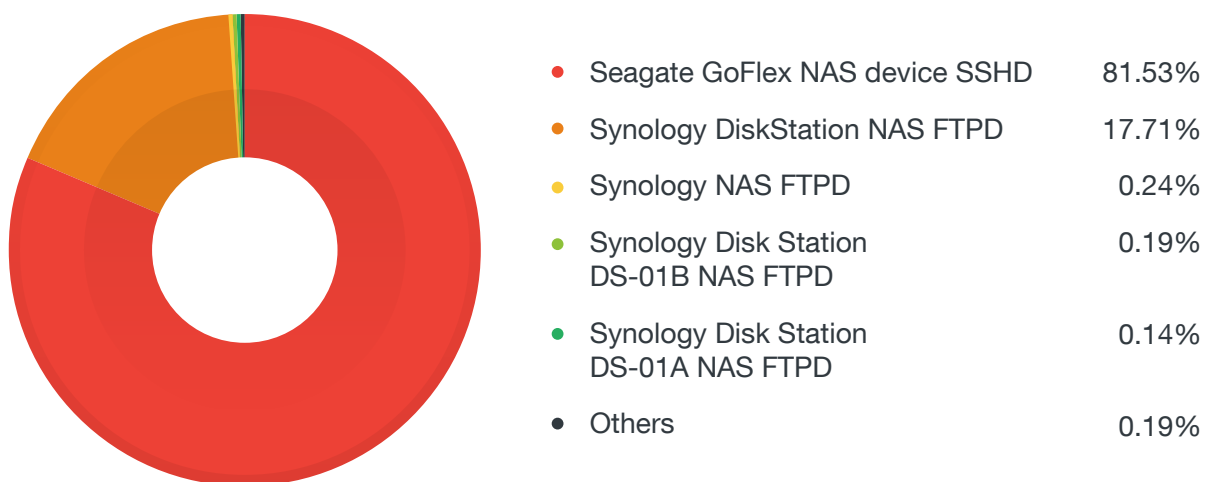


Figure 16. Distribution of exposed NAS devices by product/service name

Exposed Routers

Routers are another ubiquitous component of any networked environment. However, despite router security being regularly discussed in security conferences, security researchers continue to find new and exploitable firmware vulnerabilities in them. End users, meanwhile, often do not keep track of these developments and so do not patch their routers even if manufacturers have made fixes available.

Madrid, Athens, and London had the highest number of exposed routers while the rest of the identified Western European capitals had remarkably lower numbers.

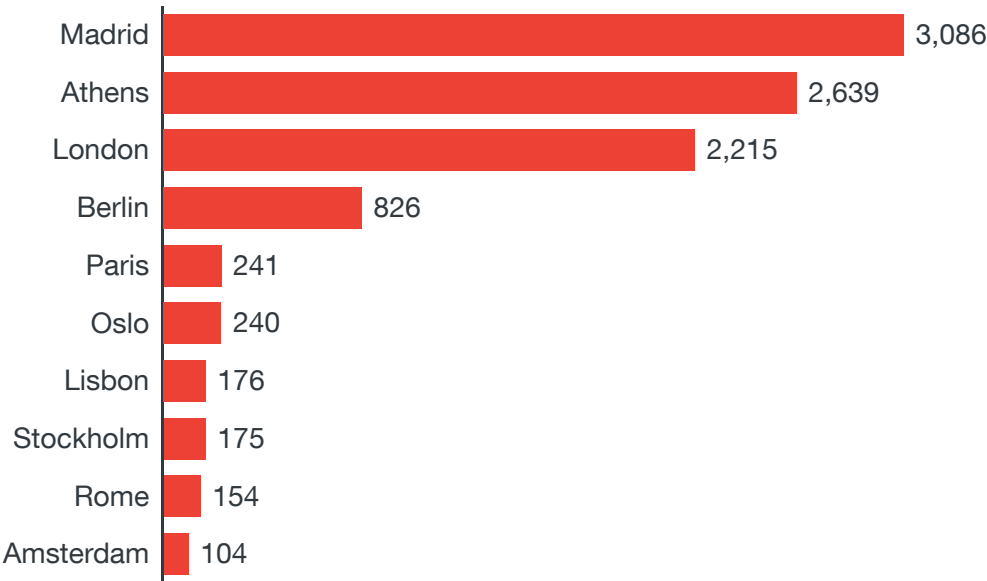


Figure 17. Number of exposed routers by capital

Unfortunately for users, compromised routers can be used to alter the functions of the internet itself. Routers are the traffic guides of the internet. If a router is exposed via FTP or Telnet, it could be compromised and altered to change how it handles internet traffic—redirecting traffic, users to malicious websites that steal credentials, or an organization’s sensitive data to a capture point; installing malware on a user’s computer; and so on.

Likewise, if Border Gateway Protocol (BGP)—the standard protocol designed to exchange routing information among autonomous systems on the internet—is exposed, how the routers talk to themselves could be altered and BGP hijacks could occur.

Cisco routers, which dominated the Shodan results, are typically installed by ISPs in customers’ homes. MikroTik and DrayTek routers are also other home router brands sold in Europe. In the context of Shodan, exposed routers refer to the exposure of the services operating on the devices; one would like to see no ports exposed on a router but Shodan can see when ports such as FTP, Telnet, Customer Premises Equipment Wide Area Network Management Protocol (CWMP), BGP, and the like are open.

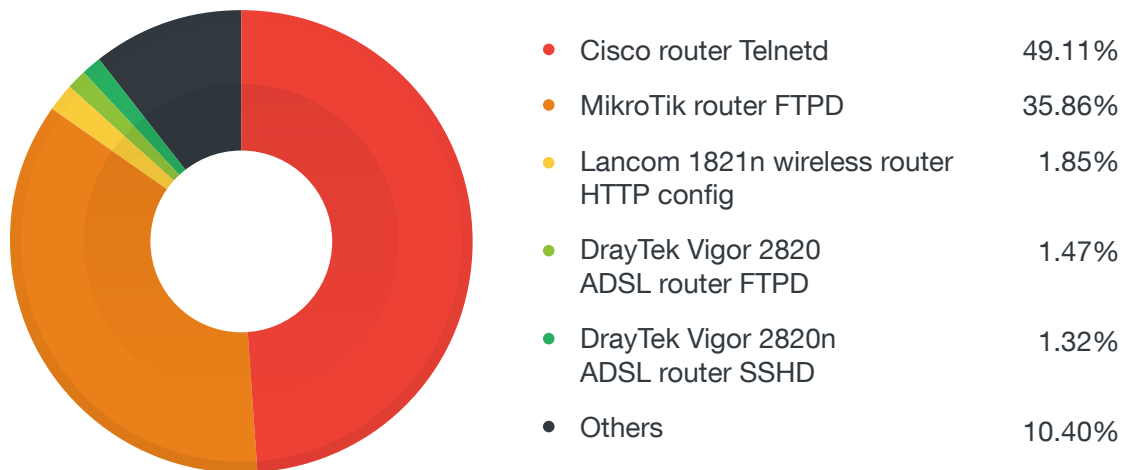


Figure 18. Distribution of exposed routers by product/service name

Exposed Printers

Printers can store cached copies of the documents they printed. For cybercriminals, access to exposed printers could also mean access to company secrets, intellectual property, PII, and various kinds of sensitive and personal data. Compromised printers can also be used for lateral movement within a target network to generate network traffic and participation in attacks against other organizations (e.g., DDoS and telephony denial-of-service [TDoS] attacks). Given their multifunctional nature, attacks utilizing network, voice, and cellular devices are all possible from poorly configured printers.

Most of the exposure observed in Shodan for printers appeared to come from a Debut embedded HTTPD service, a remote administration portal for Brother and HP printers. This service is known to be vulnerable and has been used in a variety of attacks in the past.

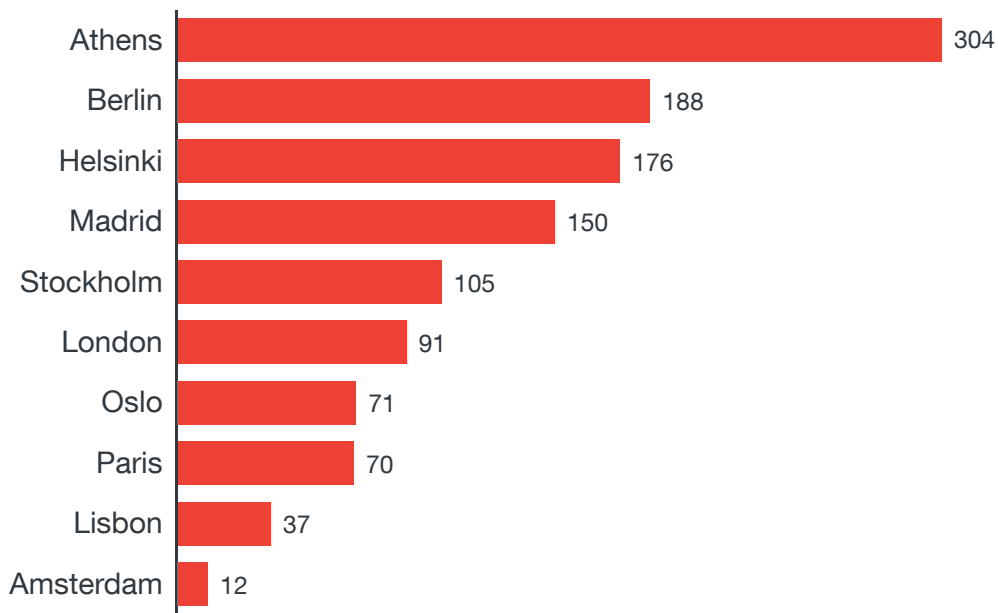


Figure 19. Number of exposed printers by capital

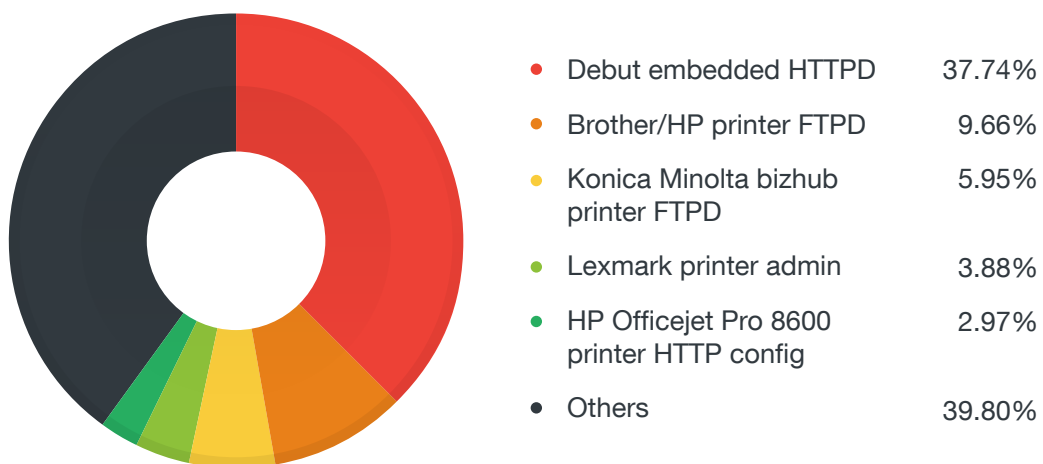


Figure 20. Distribution of exposed printers by product/service name

Exposed VoIP Devices

VoIP technology makes making phone calls (both local and overseas) a lot cheaper. Thus, many companies have switched to VoIP phones. We found over 3,000 exposed VoIP phones across Western European capitals, especially in London and Oslo, demonstrating relatively widespread adoption of the technology. The rest appeared to be sitting behind web application firewalls.

Compromising an organization’s telephone system allows hackers to monitor where calls are placed and by whom, eavesdrop on calls, access stored voice mail messages, and in extreme cases, disrupt voice communications, which may have adverse effects on daily business operations.

Worse yet, these VoIP phones can be used in a variety of telephone-based, cyber-facilitated attacks such as swatting. Sending voice spam and voice phishing or vishing and TDoS attacks are two other examples of how these exposed VoIP devices could be misused.

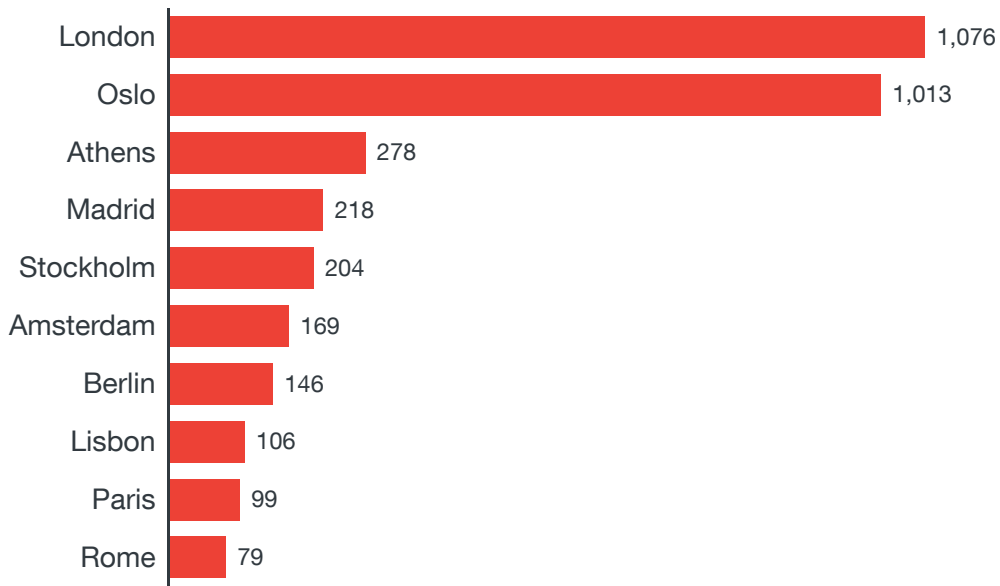


Figure 21. Number of exposed VoIP devices by capital

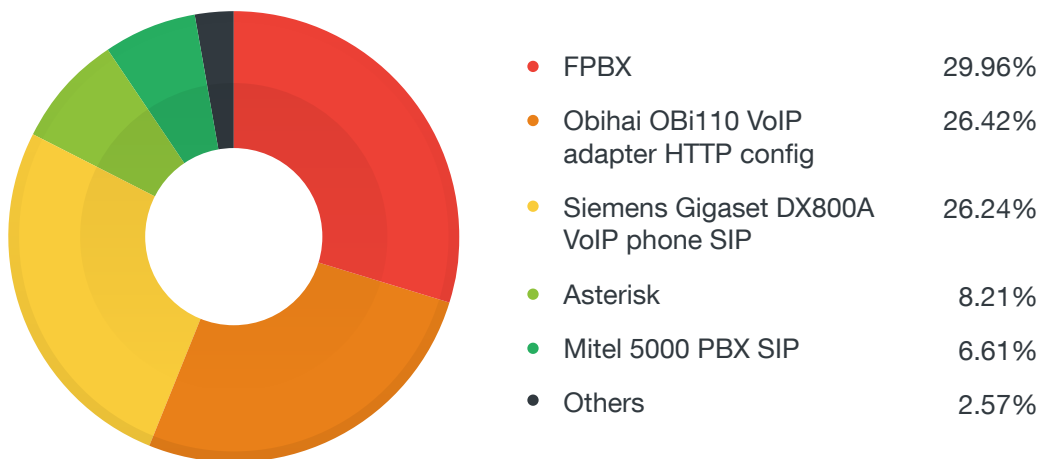


Figure 22. Distribution of exposed VoIP devices by product/service name

Exposed Media Recording Devices

Media recording devices such as digital video recorders (DVRs) are often tied to an online service or application that allows video sharing over the internet. We found over a thousand exposed DVRs across Western European capitals, a lot of which were located in Stockholm. TiVo, TalkTalk, and Dreambox were some of the players in the cable digital television industry as reflected by the distribution of brands of exposed media recording devices.

Exposed DVRs can easily become a security risk. For instance, closed-circuit television (CCTV) video feeds stored in DVRs could provide threat actors valuable surveillance information regarding targets. Compromised DVRs could also be used as points of entry into corporate networks. Finally, compromised DVRs could be used by hackers to generate network traffic as part of DDoS attacks.

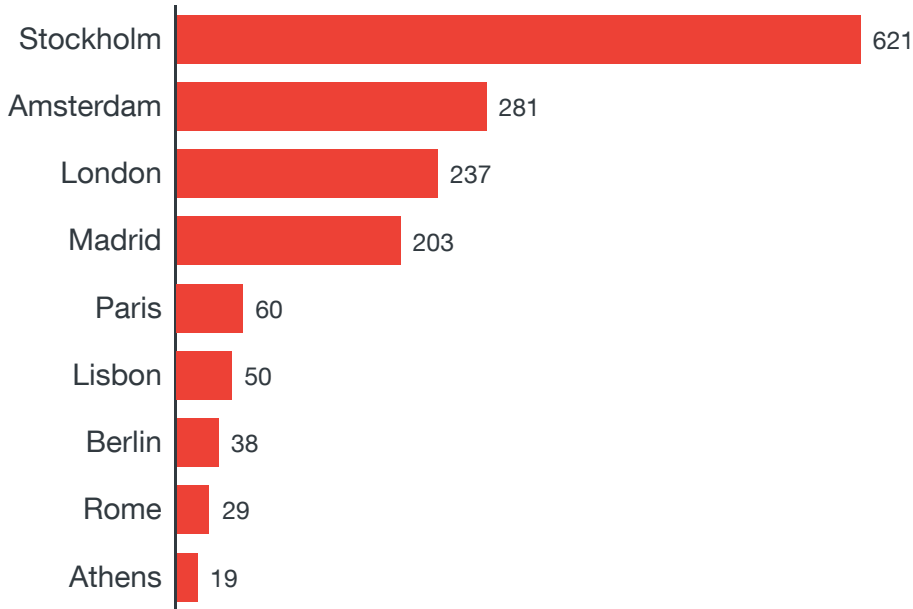


Figure 23. Number of exposed media recording devices by capital

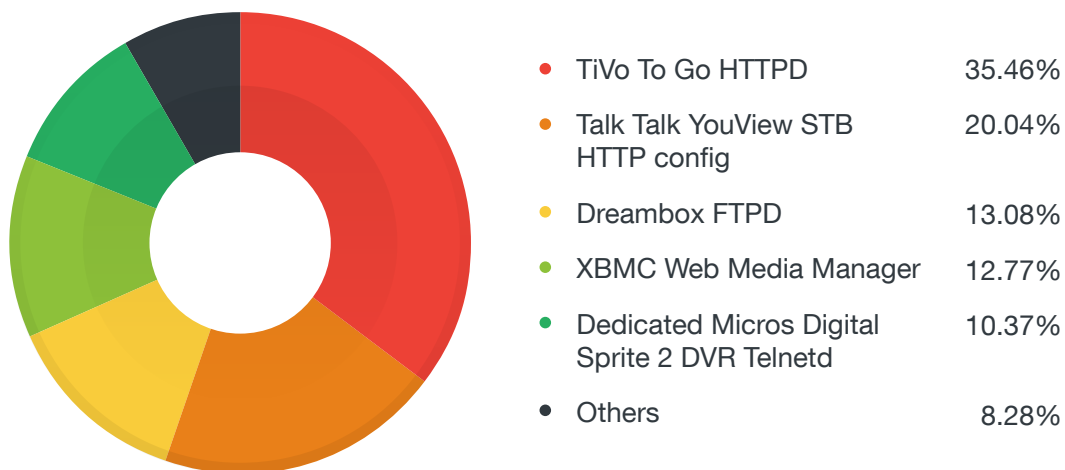


Figure 24. Distribution of exposed media recording devices by product/service name

Exposed Email/Web Services and Databases

This section digs deeper into exposed web services and databases such as web and email servers visible in the February 2017 Shodan scan data for the identified Western European capitals. These kinds of exposure put users at risk of data theft, lateral movement, fraud, and other threats.

Exposed Web Services

Traditional web services are internet facing by design. We expected services related to Apache servers to be the most prevalent type of exposed service in Western European capitals. These servers are widely used across the region because they are cheap and easy to deploy and manage and can often be fully implemented for free. NGINX, a free, open source, high-performance HyperText Transfer Protocol (HTTP) server, reverse proxy, and Internet Message Access Protocol (IMAP)/Post Office Protocol 3 (POP3) proxy server, was the second most prevalent web server software¹⁴ in the region.

A compromised web server can be used by attackers to redirect visitors to malicious sites, serve malware, host illegal data, and so on. A quick search in the National Vulnerability Database (NVD) showed 1,135 vulnerabilities that directly or indirectly affected Apache and 219 vulnerabilities for Microsoft IIS servers.

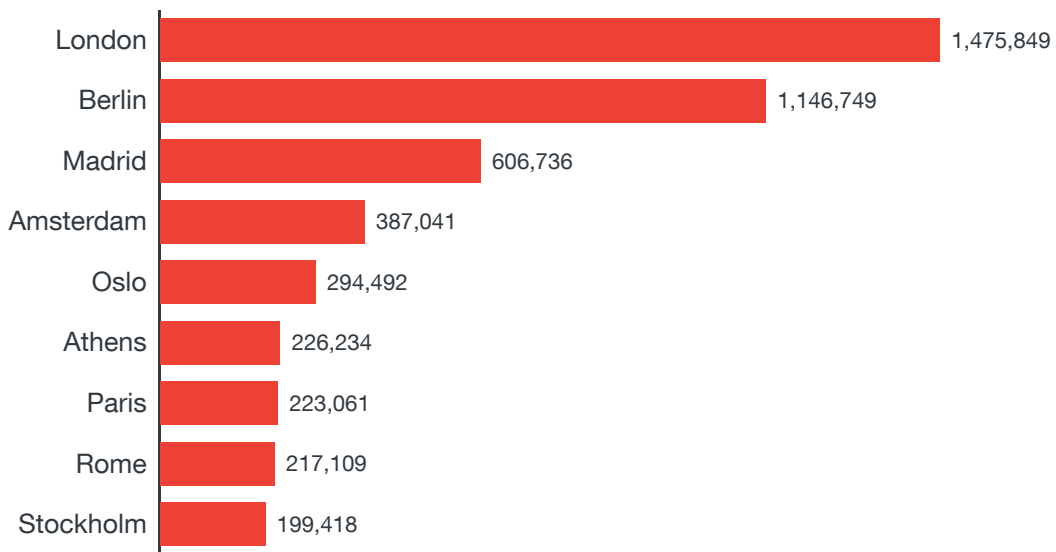


Figure 25. Number of exposed web services by capital

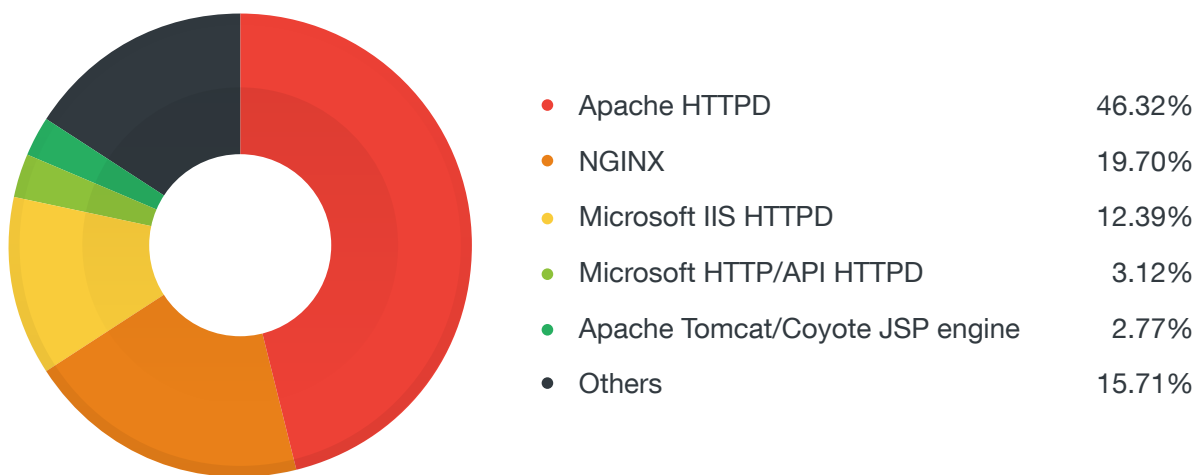


Figure 26. Distribution of exposed web services by product/service name

Exposed Email Services

Email servers are also internet facing by design, which is all the more reason for enterprises to secure them. Berlin had the highest number of exposed email services. Most of the exposed email services we saw in the Western European capitals data were related to Postfix SMTPD although a single organization accounted for more than two-thirds of this number.

Email is one of the main communication tools for modern businesses; a compromised email server means hackers have access to business-critical data (e.g., PII, internal documents, client communication, sales information, etc.). Also, any disruption to email services could severely affect daily business operations. Compromised personal email accounts can lead to the theft of PII, photos, financial information, credentials, and other sensitive information, inflicting damage to the affected individuals.

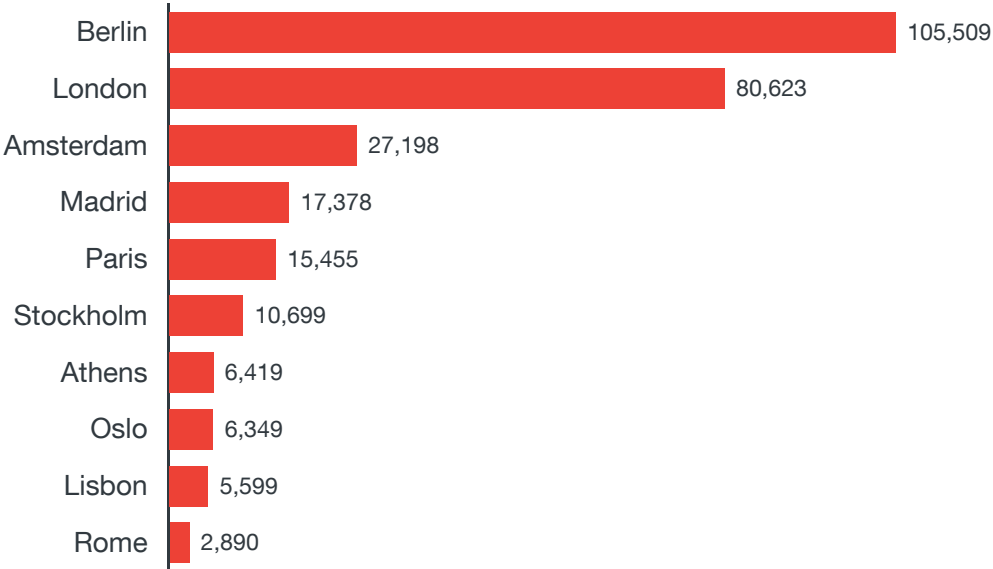


Figure 27. Number of exposed email services by capital

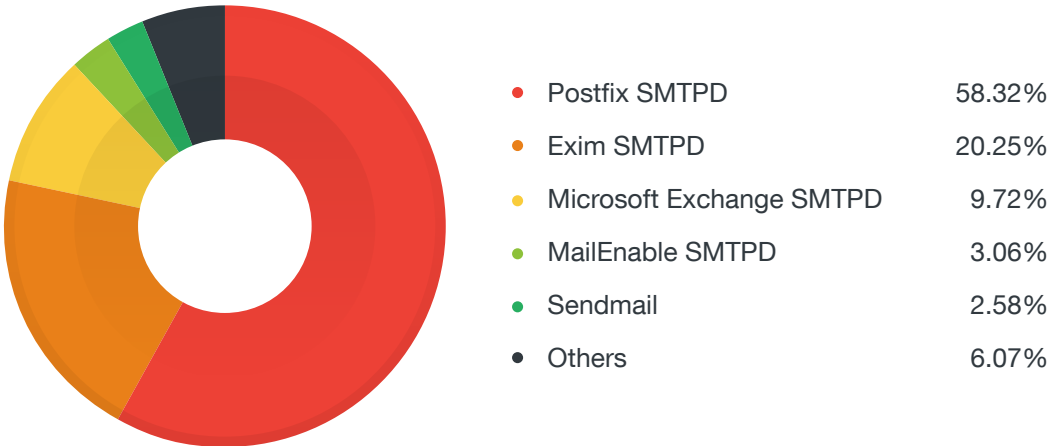


Figure 28. Distribution of exposed email services by product/service name

Exposed Databases

Databases are important to modern business operations. They store financial, customer, sales, and inventory data; PII; credentials; and other important information. This makes them lucrative targets for hackers as we have seen in reports of stolen database dumps making the rounds in cybercriminal fora.

We found several more exposed MySQL than PostgreSQL and MongoDB databases.

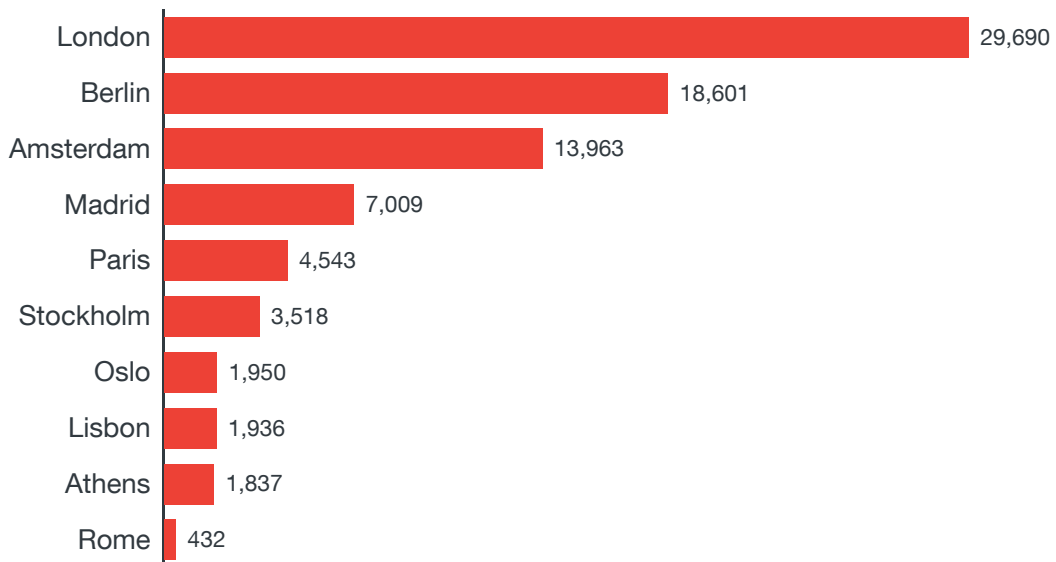


Figure 29. Number of exposed MySQL databases by capital

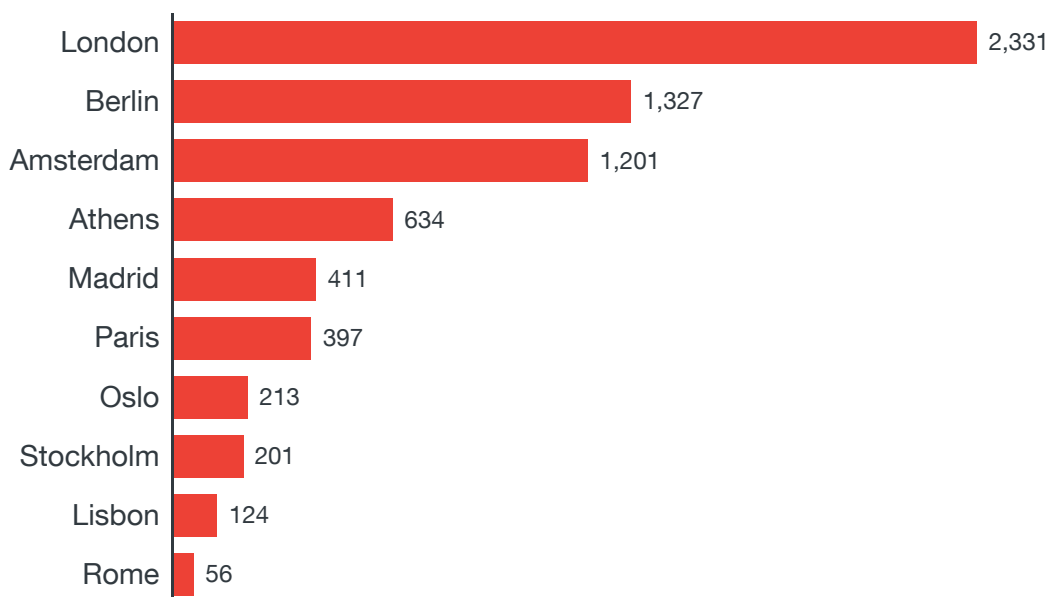


Figure 30. Number of exposed PostgreSQL databases by capital

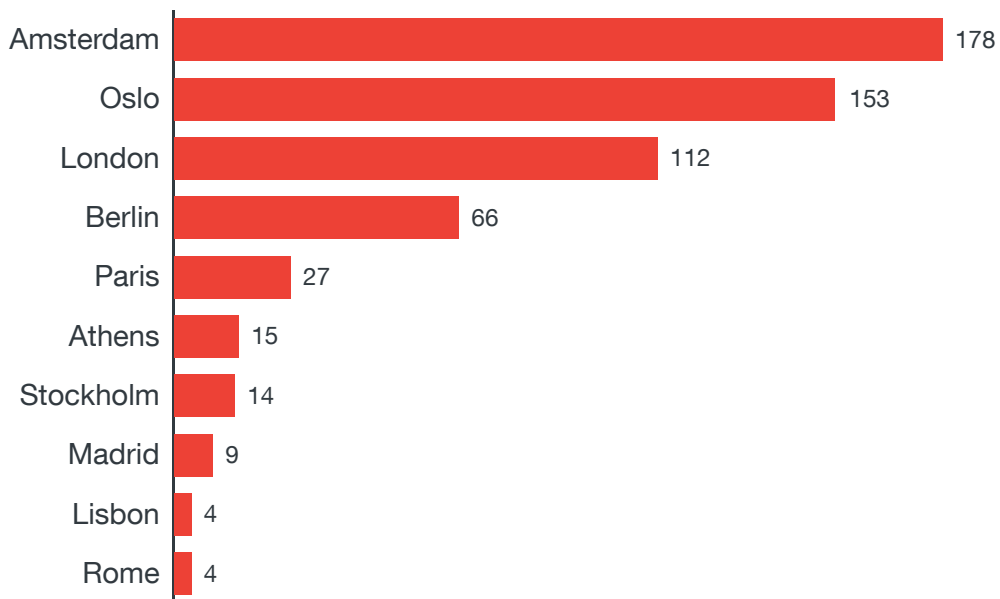


Figure 31. Number of exposed CouchDB databases by capital

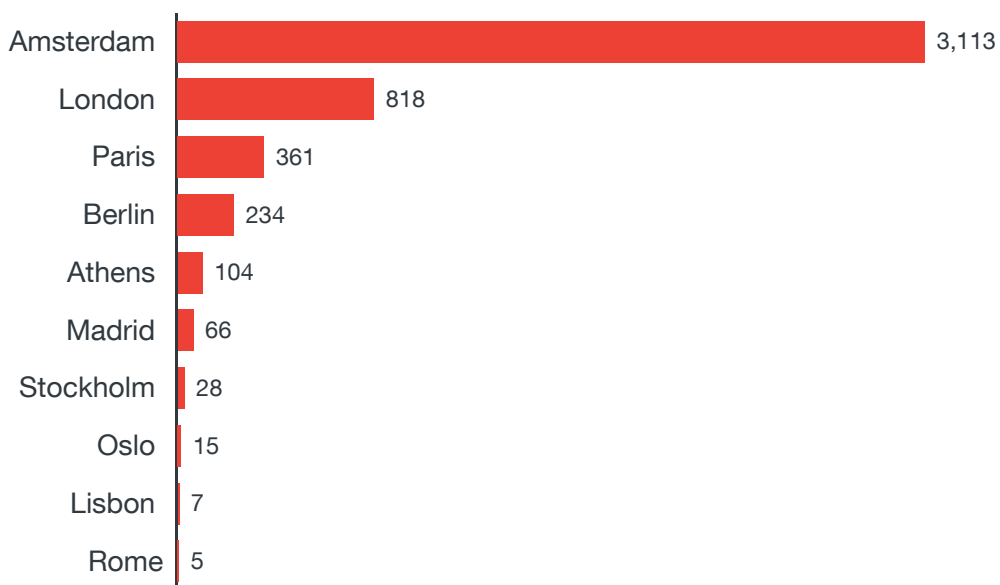


Figure 32. Number of exposed MongoDB databases by capital

Other database types did not leak size information unlike MongoDB databases. A closer look at the numbers showed that London exposed almost 17GB of data from MongoDB databases, followed by Oslo and Paris. Overall, we saw a lot more exposure than shown in Table 1. For instance, database exposure numbers in Dublin ran into hundreds of gigabytes of data.

Capital	Sum of Size in Bytes	Exposed Data Volume in MB
London	17,766,916,096	16,943.9
Oslo	4,547,014,656	4,336.4
Paris	3,576,238,080	3,410.6
Athens	1,946,370,048	1,856.0
Berlin	1,577,287,680	1,504.0
Madrid	553,680,896	528.0
Amsterdam	218,103,808	208.0
Stockholm	168,517,632	160.7
Lisbon	84,275,200	80.4
Rome	32,768	0.0

Table 1. Volume of exposed MongoDB data by capital

Exposed Service Protocols

This section digs deeper into exposed services such as Network Time Protocol (NTP), Universal Plug and Play (UPnP)/Simple Service Discovery Protocol (SSDP), Simple Network Management Protocol (SNMP), Secure Shell (SSH), RDP, Telnet, and FTP visible in the February 2017 Shodan scan data for Western European capitals. Vulnerabilities in the said protocols could be exploited to successfully compromise the devices or systems that run them.

Berlin		London		Madrid		Amsterdam		Athens	
Port	Number	Port	Number	Port	Number	Port	Number	Port	Number
5060	804,999	80	376,140	80	219,384	500	231,768	8080	55,406
8089	326,857	443	312,504	500	208,761	80	145,288	80	53,081
443	201,547	4567	298,980	443	98,315	443	101,495	443	33,499
80	182,392	22	163,808	22	76,593	22	86,267	500	25,010
22	98,711	7547	150,869	7547	63,306	53	20,654	4500	22,217
143	80,389	500	111,324	8081	59,088	110	18,944	7547	22,001
25	72,292	4500	104,643	23	43,612	995	17,039	1723	17,756
21	65,069	1723	92,945	5060	29,118	25	15,897	22	15,374
993	60,105	25	55,087	8080	27,503	8080	15,086	1900	12,142
110	56,134	53	53,798	4500	25,855	3306	13,963	23	10,970

Oslo		Paris		Lisbon		Stockholm		Rome	
Port	Number	Port	Number	Port	Number	Port	Number	Port	Number
7547	126,207	80	73,101	5060	226,661	80	73,502	443	102,066
80	56,089	443	47,161	80	25,985	443	60,188	7547	40,482
443	51,134	22	26,960	7547	22,005	500	23,444	80	21,733
500	18,298	7547	25,142	443	19,370	4500	20,771	8081	18,815
4500	17,595	8080	16,917	53	6,865	22	18,505	5060	6,927
22	12,024	53	15,845	22	6,611	8080	15,297	8089	6,733
23	8,856	500	13,296	1723	5,983	53	14,911	23	6,260
8080	7,859	4500	12,676	8080	4,979	5060	13,329	53	5,161
53	7,840	25	9,450	554	4,530	1723	10,662	8080	4,487
49152	7,785	1723	8,503	500	4,518	23	7,395	4567	4,188

Table 2. Number of exposed services by port used

Exposed NTP-enabled Devices

NTP is one of the internet’s oldest protocols. It is designed to synchronize time between computer systems that communicate over unreliable variable-latency network paths.

The biggest issue with exposed NTP servers is how they can be key to launching amplified DDoS attacks. Using specially crafted requests, attackers can get NTP servers to respond to a spoofed IP address and send a long reply to a short request. Targeted sites can thus suffer from DDoS attacks via NTP servers responding with large packets to spoofed requests.

A recently published paper by Boston University researchers¹⁵ also discussed methods of attacking NTP servers. Connections between computers and NTP servers are rarely encrypted, making it possible for hackers to perform man-in-the-middle (MitM) attacks that reset clocks to a time that is months or even years in the past. Hackers can wreak havoc on the internet with these NTP MitM attacks, causing malfunctions on a massive scale. These attacks can be used to snoop on encrypted traffic or bypass important security measures such as Domain Name System Security Extensions (DNSSEC) specifications, which are designed to prevent Domain Name System (DNS) record tampering. The most troubling scenario involves bypassing HyperText Transfer Protocol Secure (HTTPS) encryption by forcing a computer to accept an expired TLS certificate¹⁶.

London had the highest number of exposed devices that used NTP while Athens came in second. A single high-school network in Athens accounted for almost 60 percent of all the NTP servers in the city, the bulk of which were not run by major ISPs or network providers but rather by smaller organizations.

It is likely that these organizations would not be aware or understand the DDoS amplification issues that NTP servers could inflict on others.

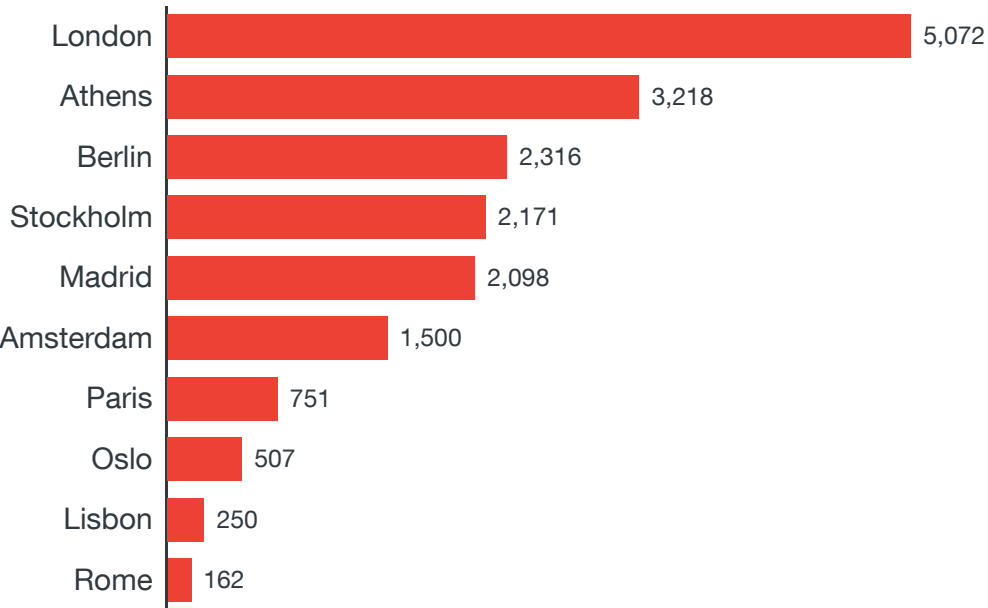


Figure 33. Number of exposed NTP-enabled devices by capital

Exposed UPnP-/SSDP-enabled Devices

UPnP¹⁷ is a set of networking protocols that permits networked devices such as computers, printers, internet gateways, WAPs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communication, and media playback. SSDP, meanwhile, is used to discover UPnP devices. It was first introduced in 1999 and is used by many routers and network devices. According to the NVD, 65 vulnerabilities directly or indirectly affected UPnP while 20 did so SSDP. The Metasploit framework includes many UPnP and SSDP modules that can be used to exploit and compromise UPnP- or SSDP-enabled devices.

A majority of the SSDP exposure came from Windows 7/8 devices, all of which used the Intel UPnP reference software development kit (SDK). Madrid and Athens, meanwhile, accounted for almost 70 percent of the exposed SSDP devices among the Western European capitals. In practice, there is no justifiable business application to have a computer's SSDP exposed on the internet. It is an internal network protocol just like NetBIOS.

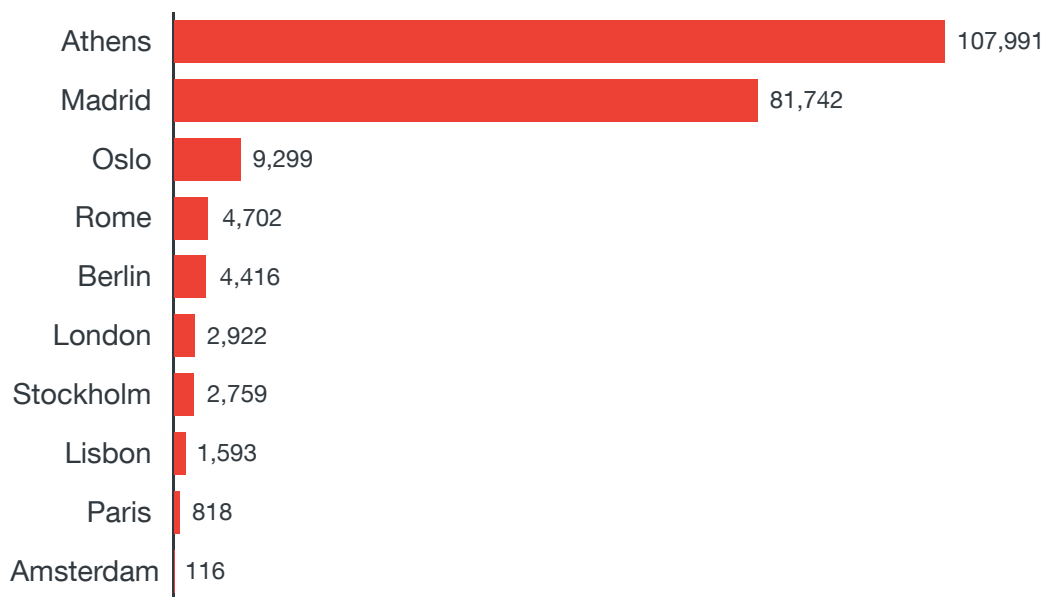


Figure 34. Number of exposed UPnP-/SSDP-enabled devices by capital

Exposed SNMP-enabled Devices

SNMP¹⁸ is a popular protocol for network management. It is used to collect information and configure network devices such as servers, printers, hubs, switches, and routers. It is also therefore a convenient way for hackers to figure out a target network's topology, which they can later use for lateral movement. It can also be used to manage devices (e.g., to shut down a network interface), making it a dangerous tool in the hands of threat actors¹⁹. Another big threat is hackers abusing devices configured to publicly respond to SNMP requests in order to amplify denial-of-service (DoS) attacks. Hackers use the IP address of an individual or organization they are targeting as the spoofed source of the SNMP request. They can then send bulk requests to devices configured to publicly respond to SNMP requests, which results in a flood of SNMP GetResponse data sent from the devices to victims²⁰.

We found more than 12,000 instances of SNMP exposure in Madrid and a little less than 8,000 each in London and Athens. Almost all SNMP exposure instances were related to Cisco routers, which were mostly operated by telecommunications companies.

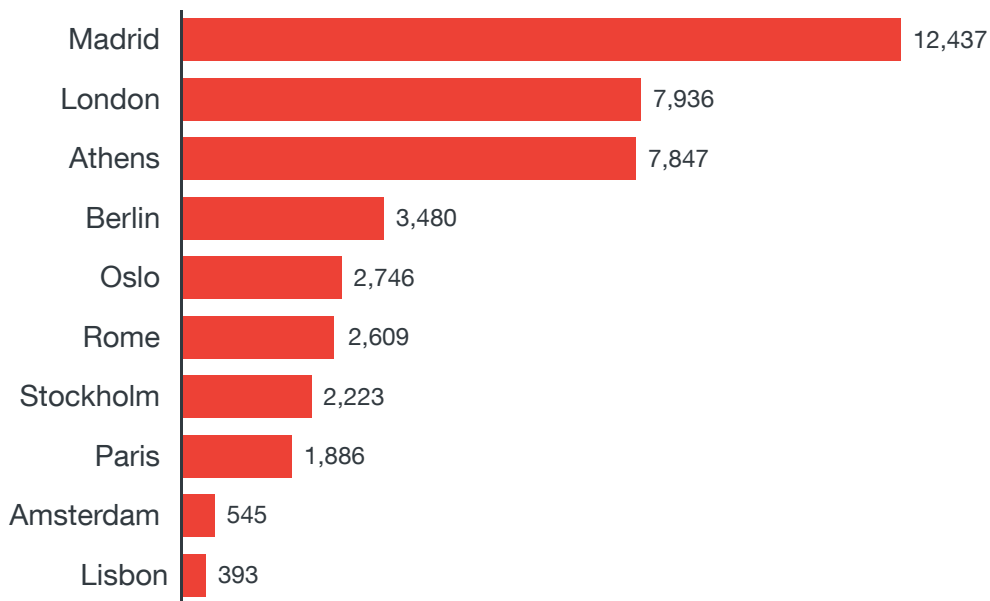


Figure 35. Number of exposed SNMP-enabled devices by capital

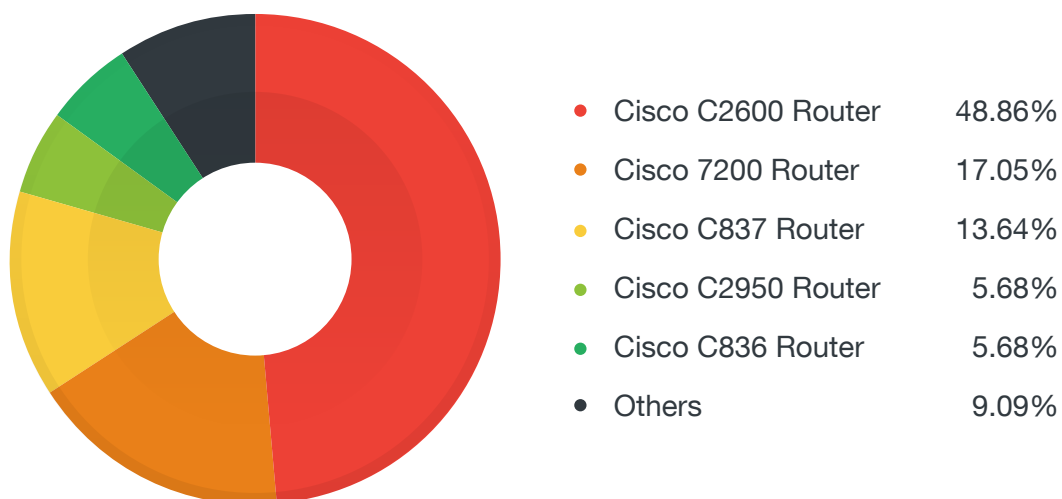


Figure 36. Distribution of exposed SNMP-enabled devices by product/service name

Exposed SSH-enabled Devices

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

Smart and connected devices are particularly valuable in these attacks. These devices rarely have strong security but have the processing capacity of most modern services. Once breached via this port, the

attacker is able to own the device then open and close necessary ports in order to perform attacks against other targets. London had over 170,000 instances of SSH exposure. A majority of the exposed devices, which employed SSH could be attributed to NAS devices.

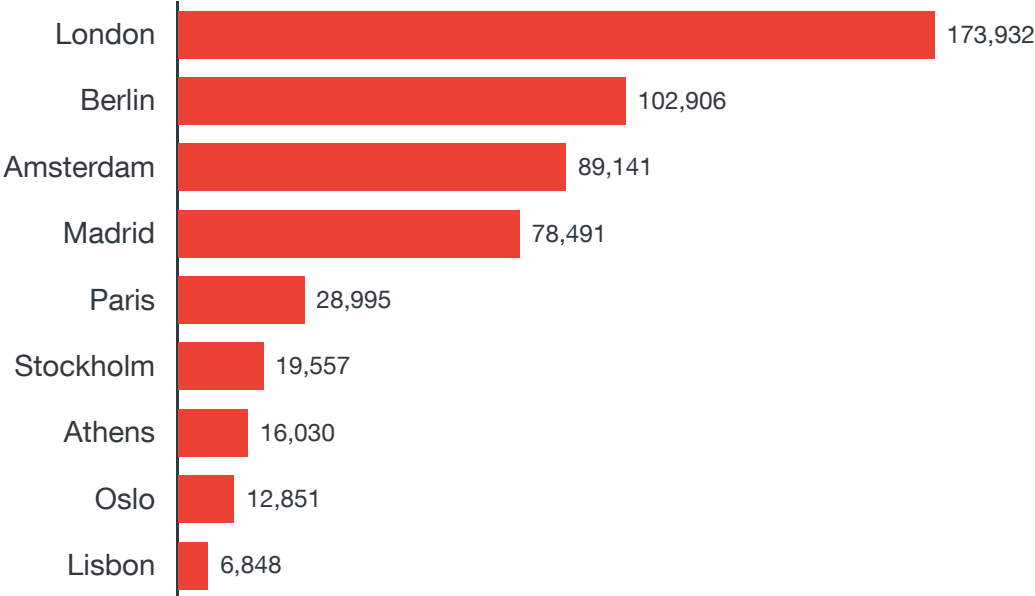


Figure 37. Number of exposed SSH-enabled devices by capital

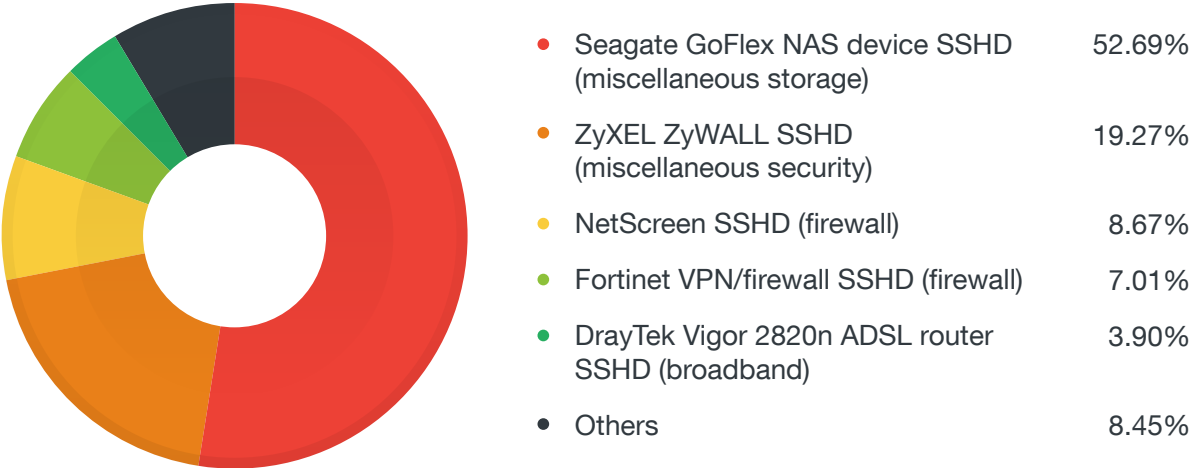


Figure 38. Distribution of exposed SSH-enabled devices by product/service name

Exposed RDP-enabled Devices

RDP²¹ is a proprietary protocol developed by Microsoft, which provides users with a graphical interface to connect to another computer over a network connection. Users employ RDP client software for this purpose while a target computer must run RDP server software, which comes standard in all Windows OSs. One of the popularly exploited RDP vulnerabilities is CVE-2012-0002 because the proof-of-concept (PoC) code for it was leaked online. RDP has traditionally been abused to remotely access computers and servers to then either leverage that system to:

- Commit attacks on other systems
- Exfiltrate data stored on that system as part of a targeted attack
- Steal information that can be sold in Deep Web marketplaces
- Integrate hijacked systems into botnets

Crysis ransomware were found able to brute-force RDP as an infection vector²².

A significant number of RDP exposure was seen among Windows XP boxes. In at least four cities, this accounted for 25 percent or more of all OSs that had RDP exposed. Given the end of support for Windows XP despite its continued use, affected organizations face a significant risk.

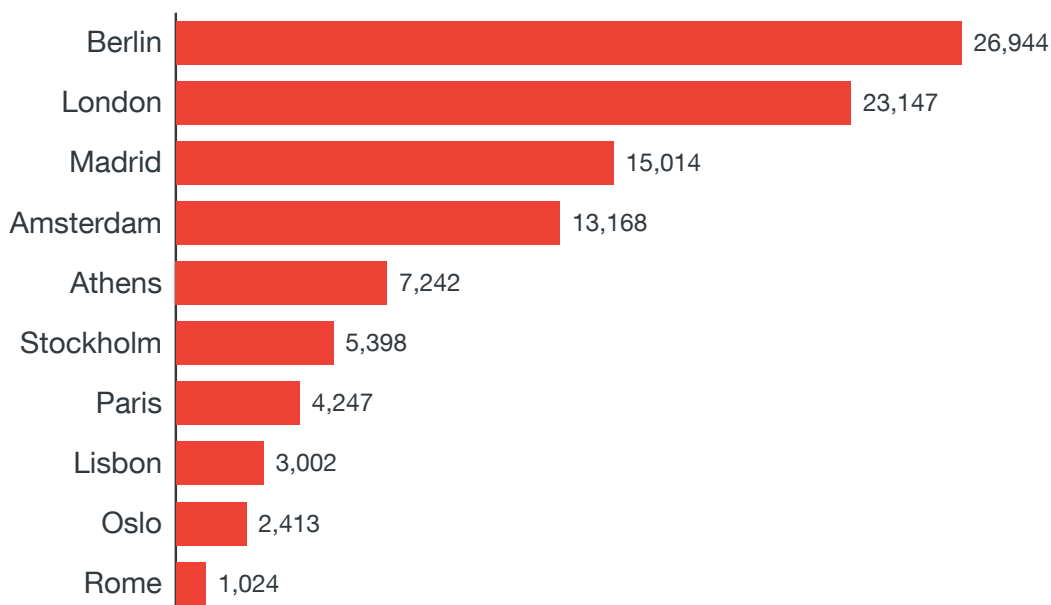


Figure 39. Number of exposed RDP-enabled devices by capital

Exposed Telnet-enabled Devices

Telnet²³ is an application layer protocol used on the internet or a LAN to provide bidirectional interactive text-oriented communication using a virtual terminal connection. In a Telnet session, all data is sent and received in clear text; there is no end-to-end content encryption. This makes Telnet highly vulnerable to packet-sniffing attacks. Telnet was first introduced in the early 1970s and over time, has been replaced by SSH.

We continued to see a lot of routers with Telnet open. Madrid led the count, most likely in order to allow for remote router administration. It is critical in such a case to ensure strong authentication in order to harden the service.

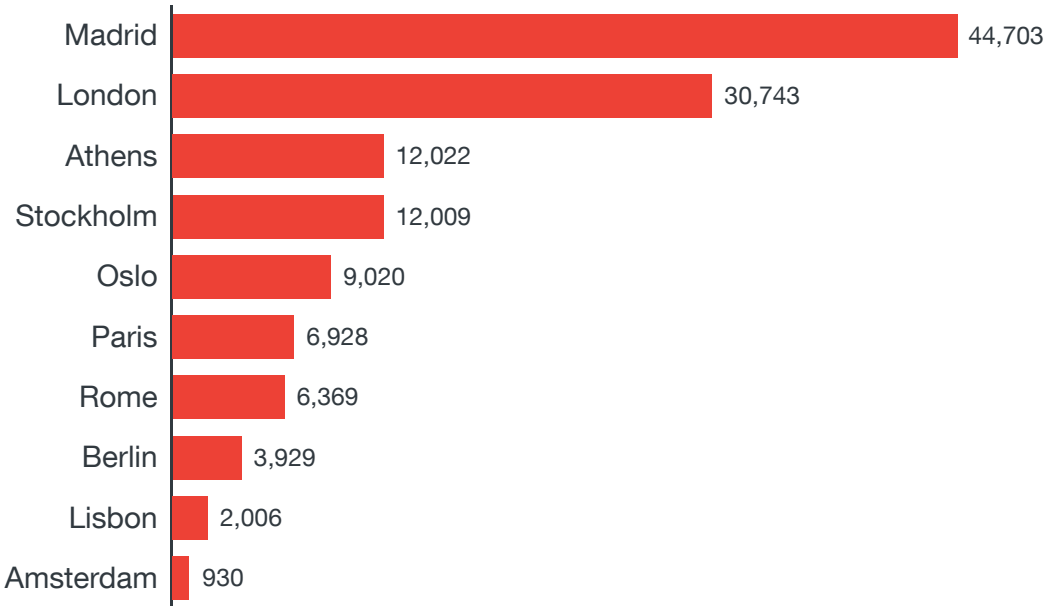


Figure 40. Number of exposed Telnet-enabled devices by capital

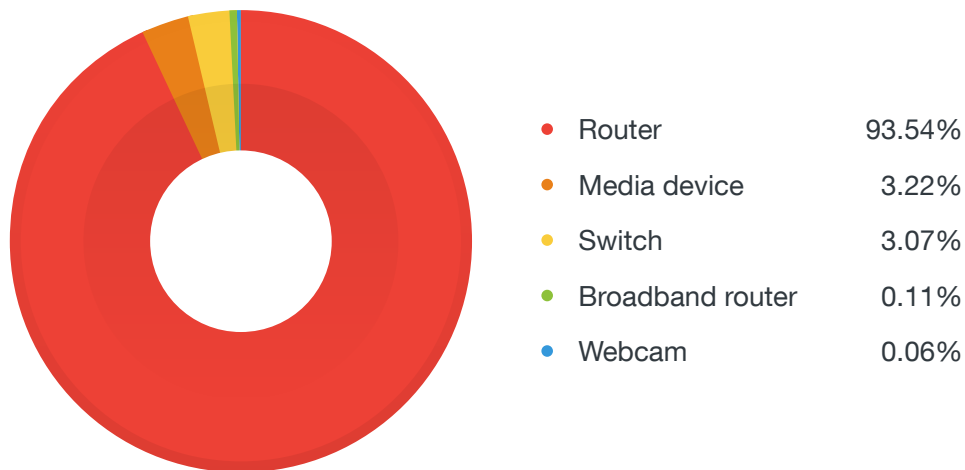


Figure 41. Distribution of exposed Telnet-enabled devices by asset type

Exposed FTP-enabled Devices

FTP²⁴ is a standard network protocol used to transfer files between a client and a server over a computer network. It is enabled by default on most web servers, which makes it a lucrative target for exploitation by hackers. Once FTP is exploited and the server compromised, hackers can access all hosted files and upload new malicious files. Looking at the Shodan data, we found routers, WAPs, NAS devices, printers, print servers, and webcams in the list of exposed FTP-enabled devices.

Berlin had the highest FTP exposure number, overshadowing the rest of the other capitals by a wide margin. One probable reason is the high number of users of ProFTPD, a free and open source FTP server type in the said city.

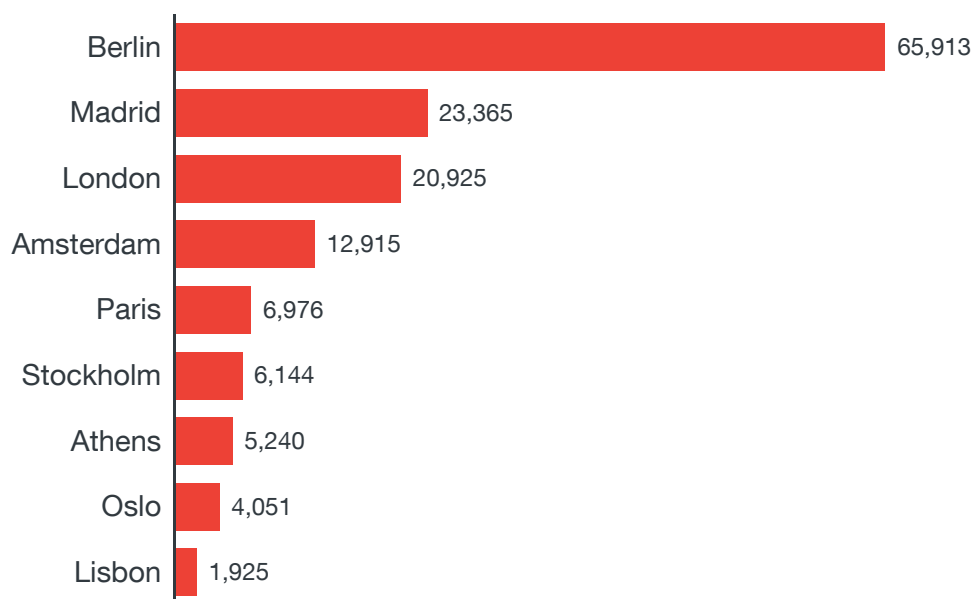


Figure 42. Number of exposed FTP-enabled devices by capital

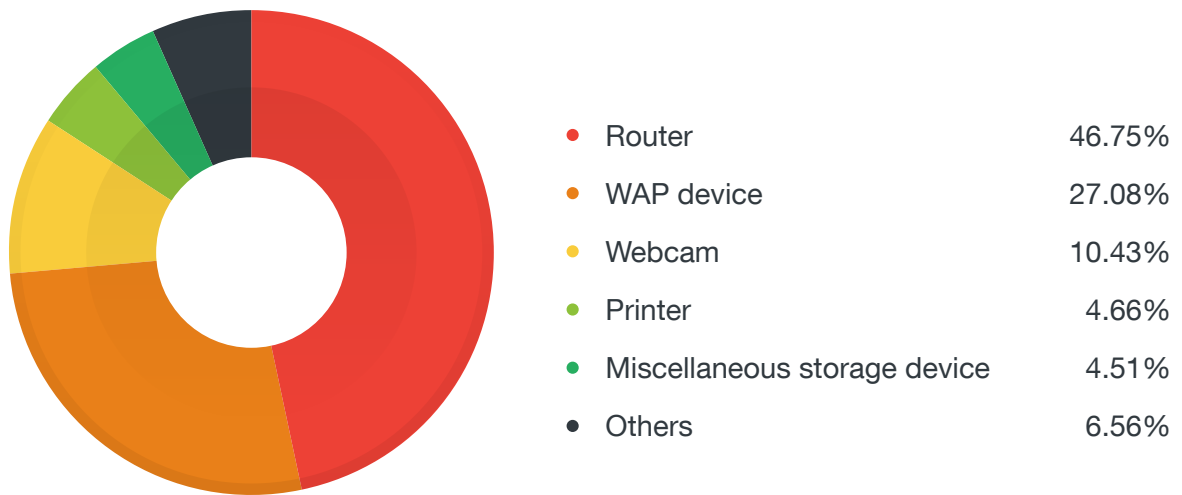


Figure 43. Distribution of exposed FTP-enabled devices by asset type

Safeguarding Against Internet Exposure

For Enterprises

Exposed cyber assets do not translate to compromise; rather, this 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 cybercriminals and threat actors to look for security flaws that may be used to infiltrate a company's network. And with the General Data Protection Regulation (GDPR)²⁵ taking effect on May 2018, businesses, regardless of size and industry, must ensure compliance or pay penalties—as much as 4 percent of annual turnover. GDPR puts a premium on consumer data protection and privacy and could affect enterprises and small and medium-sized businesses (SMBs) whether they are physically based in Europe or not, as long as they process the data of EU citizens. 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)²⁶ 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.

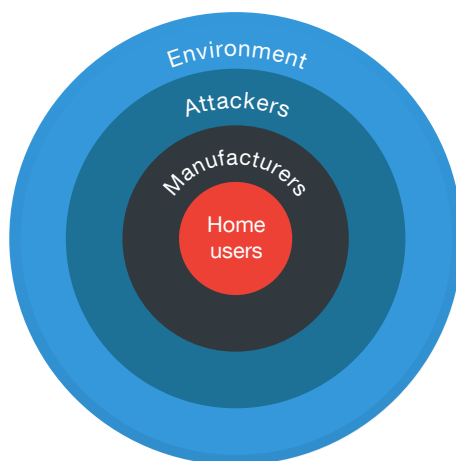


Figure 44. Risk factors increase with each additional layer to the Internet of Things (IoT) ecosystem

(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 information technology (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 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 operations 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

As the internet-connected world becomes more layered and complex, our collective sense of accountability for understanding the levels of exposure systems have to being hijacked and used for nefarious reasons must likewise develop. Our analysis of Shodan data for Western Europe revealed some startling numbers suggesting that even countries in the region have work to do when it comes to limiting the exposure of their internet-connected devices.

- London and Berlin had the highest number of exposed cyber assets at more than 2 million instances. Amsterdam and Madrid were both close behind.
- That webcams were the second most exposed devices in Western European capitals is staggering when their privacy risks are well-known. With just a few quick searches via Shodan, a number of webcam streams were found publicly viewable via remote unauthenticated access. These included webcams that belonged to a retail store, a telco, a warehouse, and many homeowners. These have fairly significant privacy and security consequences for those affected, particularly for those at home who may not realize the personal safety risks that invasive viewing using these cameras pose, especially if they have children. The high number of exposed WAPs and VoIP devices could be attributed to the heavy use of Fritz!Boxes in Germany. The vulnerabilities in Fritz!Boxes are well-known, having been the subject of well-publicized attacks in 2014 and the many publications on the vulnerabilities within these.
- A surprising number of both printers and private branch exchange (PBX) devices were exposed throughout the region, which can be leveraged not only to commit or reflect traditional cyber-based attacks but also telephony-based attacks (i.e., TDoS, telefraud, vishing, etc.).
- The most exposed software products in Western European capitals were related to HTTP web servers such as Apache HTTPD, NGINX, OpenSSH, and Microsoft IIS HTTPD.
- The use of proxies across Europe was surprisingly high. It was also interesting to note that port 8080 and similar HTTP proxy ports were actually observed almost as often as its traditional port 80 equivalent.
- It was also interesting to note some outlier protocol usage throughout Western Europe and their exposure to being utilized as part of DDoS attacks against others:

- Exposed NTP with monlist enabled from a school system in Athens could be leveraged to reflect significantly strong DDoS attacks to render many networks inoperable.
- Similarly, the high numbers of UPnP/SSDP exposure in Madrid and Athens due to exposed printers could also be used in reflective, amplified DDoS attacks against others.

The risks of maintaining exposed cyber assets vary. Exposed cyber assets could leak sensitive data unbeknownst to their owners (e.g., open directories, unauthenticated webcam feeds, etc.), allow hackers to steal sensitive data (e.g., PII, intellectual property, financial and corporate data, etc.), help attackers perform reconnaissance or lateral movement in targeted attack campaigns, be used by disruptors for DDoS attacks, or be held hostage for ransom by cyber extortionists.

Furthermore, as the May 2018 deadline to comply with the GDPR approaches, companies must hold themselves to a higher standard when it comes to protecting the data of EU citizens. There will be greater pressure to look at all points of weakness and exposed cyber assets are definitely one such opening.

Consumers are likewise demanding more from companies. A recent legal case involved a consumer organization that filed a lawsuit against an electronic store for selling an Android phone with 15 open security issues.

In order to protect their networks, defenders must employ a mindset that assumes compromise to formulate better strategies in protecting their systems. This will inevitably include an audit of all open and searchable cyber assets and measures to contain them. Homeowners must follow our list of recommendations to ensure that their internet-connected devices are not exposed as well.

We also made follow-through research on searchable devices in Shodan for cities in the U.K., France, and Germany.

Appendix

Research Coverage

We covered the following 10 capitals in Western Europe in terms of population.

City	Population
London	9,787,426 ²⁷
Berlin	3,520,031 ²⁸
Amsterdam	848,861 ²⁹
Madrid	3,165,235 ³⁰
Athens	3,168,846 ³¹
Oslo	925,228 ³²
Paris	2,220,445 ³³
Lisbon	545,245 ³⁴
Stockholm	1,515,017 ³⁵
Rome	2,872,021 ³⁶

Table 3. List of Western European capitals 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 more³⁷. 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 banners. 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 Western European 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 10 Western European capitals. The data set used contained a total of 8,667,083 records generated from scanning 2,751,346 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 devices³⁸. 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 in Shodan." Last accessed on 20 September 2017, <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/us-cities-exposed-in-shodan>.
2. Jacob Poushter. (22 February 2016). *Pew Research Center*. "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies." Last accessed on 26 September 2017, <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>.
3. The MITRE Corporation. (2013). *Common Vulnerabilities and Exposures*. "CVE-2013-1391." Last accessed on 20 September 2017, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1391>.
4. The MITRE Corporation. (2013). *Common Vulnerabilities and Exposures*. "CVE-2013-1899." Last accessed on 20 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1899>.
5. The MITRE Corporation. (2014). *Common Vulnerabilities and Exposures*. "CVE-2014-0160." Last accessed on 20 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160>.
6. Pawan Kinger. (8 April 2014). *TrendLabs Security Intelligence Blog*. "Skipping a Heartbeat: The Analysis of the Heartbleed OpenSSL Vulnerability." Last accessed on 20 September 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/skipping-a-heartbeat-the-analysis-of-the-heartbleed-openssl-vulnerability/>.
7. The MITRE Corporation. (2015). *Common Vulnerabilities and Exposures*. "CVE-2015-0204." Last accessed on 20 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2015-0204>.
8. Trend Micro. (5 March 2015). *Trend Micro Security News*. "FREAK Attack on TLS/SSL Flaw Affects Popular Domains and Browsers." Last accessed on 20 September 2017, <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/freak-attack-on-tls-ssl-flaw-affects-popular-domains-and-browsers>.
9. The MITRE Corporation. (2015). *Common Vulnerabilities and Exposures*. "CVE-2015-2080." Last accessed on 20 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2080>.
10. The MITRE Corporation. (2016). *Common Vulnerabilities and Exposures*. "CVE-2016-9244." Last accessed on 20 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9244>.
11. AVM. (10 February 2014). *AVM*. "Attacks on FRITZ!Box Clarified—Security Advice Still in Effect—Updates Will Be Released Shortly." Last accessed on 20 September 2017, <http://web.archive.org/web/20160918112503/https://en.avm.de/press/pressreleases/2014/02/attacks-on-fritzbox-clarified-security-advice-still-in-effect-updates-will-be-released-shortly/>.
12. AVM. (10 February 2014). *AVM*. "AVM with a Security Update for the FRITZ!Box." Last accessed on 20 September 2017, <http://web.archive.org/web/20160918112508/https://en.avm.de/press/press-releases/2014/02/avm-with-a-security-update-for-the-fritzbox/>.
13. AVM. (6 February 2014). *AVM*. "Important Security Information for FRITZ!Box Users with Remote Access Enabled." Last accessed on 20 September 2017, <http://web.archive.org/web/20160918112516/https://en.avm.de/press/press-releases/2014/02/important-security-information-for-fritzbox-users-with-remote-access-enabled/>.
14. NGINX Inc. (2017). *NGINX*. "Welcome to NGINX Wiki!" Last accessed on 20 September 2017, <https://www.nginx.com/resources/wiki/>.
15. Aanchal Malhotra, Isaac E. Cohen, Erik Brakke, and Sharon Goldberg. (20 August 2015). "Attacking the Network Time Protocol." Last accessed on 20 September 2017, <http://www.cs.bu.edu/~goldbe/papers/NTPattack.pdf>.

16. Dan Goodin. (22 October 2015). *ArsTechnica*. "New Attacks on Network Time Protocol Can Defeat HTTPS and Create Chaos." Last accessed on 20 September 2017, <https://arstechnica.com/information-technology/2015/10/new-attacks-on-network-time-protocol-can-defeat-https-and-create-chaos/>.
17. TechTarget. (March 2011). *TechTarget*. "Universal Plug and Play (UPnP)." Last accessed on 20 September 2017, <http://whatis.techtarget.com/definition/Universal-Plug-and-Play-UPnP>.
18. Microsoft. (28 March 2003). *Microsoft TechNet*. "What Is SNMP?" Last accessed on 20 September 2017, <https://technet.microsoft.com/en-us/library/cc776379%28v=ws.10%29.aspx>.
19. John McCormick. (11 April 2001). *TechRepublic*. "Lock IT Down: Don't Allow SNMP to Compromise Network Security." Last accessed on 20 September 2017, <http://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-network-security/>.
20. Kelly Jackson Higgins. (22 May 2014). *Dark Reading*. "SNMP DDoS Attacks Spike." Last accessed on 20 September 2017, <https://www.darkreading.com/attacks-breaches/snmp-ddos-attacks-spike/d/d-id/1269149>.
21. Techopedia Inc. (2017). *Techopedia*. "Remote Desktop Protocol (RDP)." Last accessed on 20 September 2017, <https://www.techopedia.com/definition/3422/remote-desktop-protocol-rdp>.
22. Jon Oliver. (19 September 2016). *TrendLabs Security Intelligence Blog*. "A Show of (Brute) Force: Crysis Ransomware Found Targeting Australian and New Zealand Businesses." Last accessed on 20 September 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/>.
23. TechTarget. (2017). *TechTarget*. "Telnet." Last accessed on 20 September 2017, <http://searchnetworking.techtarget.com/definition/Telnet>.
24. TechTarget. (2017). *TechTarget*. "File Transfer Protocol (FTP)." Last accessed on 20 September 2017, <http://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol>.
25. Trend Micro. (2017). *EU General Data Protection: Time to Act*. "New Legal Considerations for Security Professionals." Last accessed on 26 September 2017, <http://www.trendmicro.co.uk/enterprise/data-protection/eu-regulation/>.
26. CIS. (2016). *CIS*. "CIS Controls for Effective Cyberdefense." Last accessed on 29 August 2017, <https://www.cisecurity.org/critical-controls/>.
27. 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>.
28. Wiesbaden: Federal Statistical Office of Germany. (31 December 2015). "Städte in Deutschland nach Fläche und Bevölkerung auf Grundlage des ZENSUS 2011 und Bevölkerungsdichte: Gebietsstand 31.12.2015." Last accessed on 20 September 2017, <https://www.destatis.de/DE/ZahlenFakten/LaenderRegionen/Regionales/Gemeindeverzeichnis/Administrativ/Aktuell/05Staedte.xls>.
29. Provincie NoordHolland. Province of Noord-Holland. Last accessed on 20 September 2017, https://www.noord-holland.nl/English/Province_of_Noord_Holland.
30. Instituto Nacional de Estadística. (30 June 2015). "Urban Indicators (Urban Audit) Year 2015." Last accessed on 20 September 2017, http://www.ine.es/en/prensa/np920_en.pdf.
31. Quandl. "Population of Athinai [Athens], ATT, Greece." Last accessed on 29 August 2017, https://www.quandl.com/data/CITYPOP/CITY_ATHINAIATHENSATTGREECE.
32. Innovation Norway. (17 October 2017). *VisitNorway.com*. "About Norway." Last accessed on 17 October 2017, <https://www.visitnorway.com/media/facts/about/>.

33. Quandl Inc (2017). *Quandl*. "National Institute of Statistics and Economic Studies [France]." Last accessed on 26 September 2017, <https://www.quandl.com/data/INSEE-National-Institute-of-Statistics-and-Economic-Studies-France>.
34. WorldAtlas. *WorldAtlas.com*. "Portugal Facts." Last accessed on 17 October 2017, <http://www.worldatlas.com/webimage/countrys/europe/portugal/ptfacts.htm>.
35. WorldAtlas. *WorldAtlas.com*. "Biggest Cities In Sweden." Last accessed on 17 October 2017, <http://www.worldatlas.com/articles/the-biggest-cities-in-sweden.html>.
36. Italian National Institute of Statistics. *ISTAT*. "ISTAT Official Population Estimates (19 December 2014)." Last accessed on 17 October 2017, <http://www.demo.istat.it/bilmens2014gen/query.php?lingua=ita&Rip=S3&Reg=R12&Pro=P058&Com=91&submit=Tavola>.
37. Paul Didier, Fernando Macias, James Harstad, Rick Antholine, Scott A. Johnston, Sabina Piyevesky, 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.
38. 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