

German Cities Exposed

A Shodan-based Security Study on Exposed Cyber
Assets in Germany

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: Germany

12

Exposed Cyber Assets in Germany

33

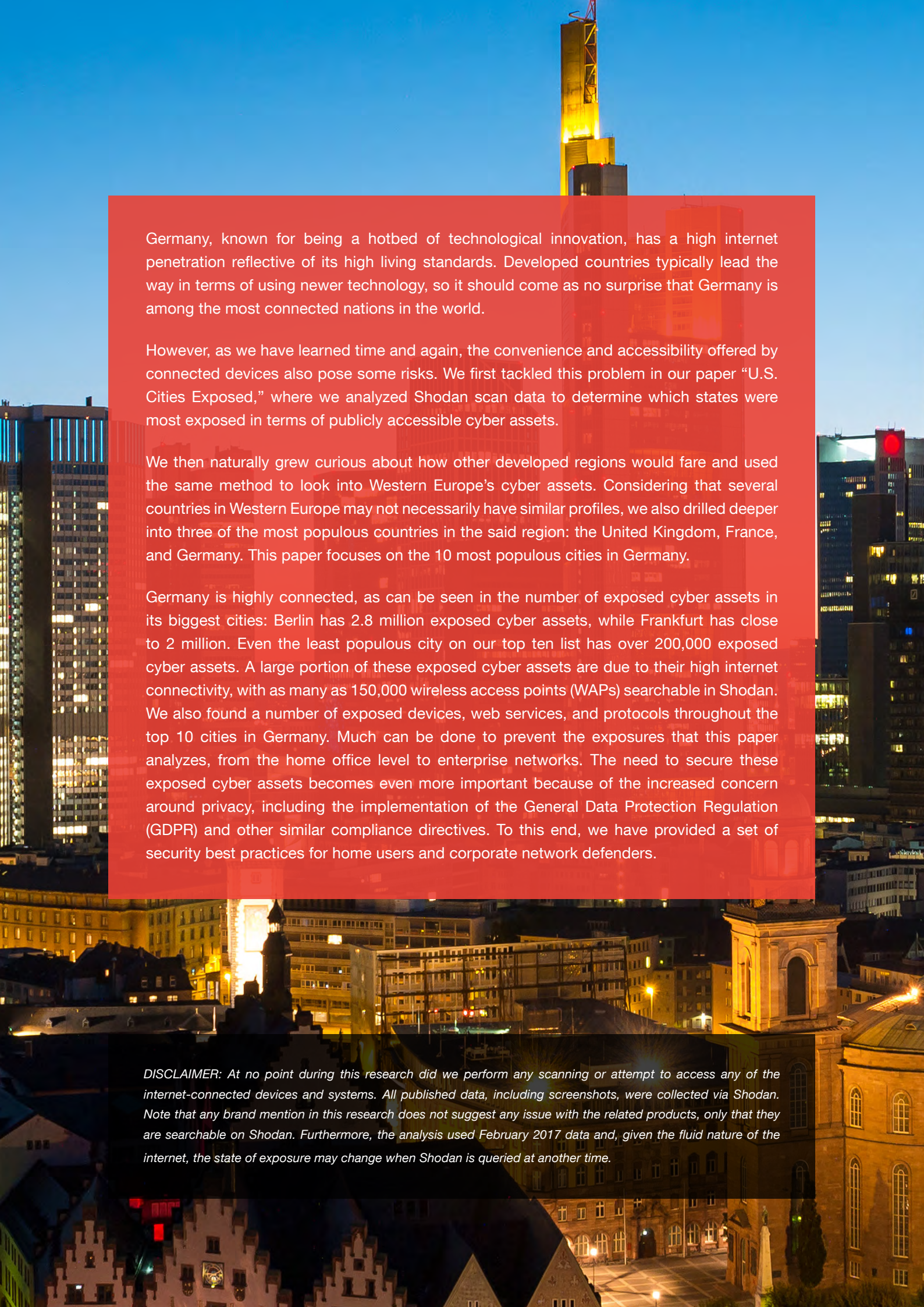
Safeguarding Against Internet Exposure

38

Conclusion

39

Appendix



Germany, known for being a hotbed of technological innovation, has a high internet penetration reflective of its high living standards. Developed countries typically lead the way in terms of using newer technology, so it should come as no surprise that Germany is among the most connected nations in the world.

However, as we have learned time and again, the convenience and accessibility offered by connected devices also pose some risks. We first tackled this problem in our paper “U.S. Cities Exposed,” where we analyzed Shodan scan data to determine which states were most exposed in terms of publicly accessible cyber assets.

We then naturally grew curious about how other developed regions would fare and used the same method to look into Western Europe’s cyber assets. Considering that several countries in Western Europe may not necessarily have similar profiles, we also drilled deeper into three of the most populous countries in the said region: the United Kingdom, France, and Germany. This paper focuses on the 10 most populous cities in Germany.

Germany is highly connected, as can be seen in the number of exposed cyber assets in its biggest cities: Berlin has 2.8 million exposed cyber assets, while Frankfurt has close to 2 million. Even the least populous city on our top ten list has over 200,000 exposed cyber assets. A large portion of these exposed cyber assets are due to their high internet connectivity, with as many as 150,000 wireless access points (WAPs) searchable in Shodan. We also found a number of exposed devices, web services, and protocols throughout the top 10 cities in Germany. Much can be done to prevent the exposures that this paper analyzes, from the home office level to enterprise networks. The need to secure these exposed cyber assets becomes even more important because of the increased concern around privacy, including the implementation of the General Data Protection Regulation (GDPR) and other similar compliance directives. To this end, we have provided a set of security best practices for home users and corporate network defenders.

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: Germany

Scanning the internet is a valuable exercise because, 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, time-consuming, and poses a set of unique challenges. For our research on exposed cyber assets, we partnered with Shodan, a publicly available database of scan data. Technical assumptions and observations about our use of Shodan data in this project can be found in the Appendix. It also discusses what Shodan is and how we analyzed the Shodan data.

Shodan's scan data is a point-in-time snapshot. We examined the Shodan Germany scan data for February 2017. We filtered out those belonging to hosting providers that provide services throughout all or most of Europe since hosting infrastructure is complex and difficult to map or accurately port to back-end applications. However, we did not exclude those that are less global in nature (like Strato AG). The filtered data set contains a total of 51,576,513 entries generated from 16,553,265 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.

Cyber Asset Exposure in Germany

We identified representative cities in Germany by looking at the top 10 most populous cities in the country, some of which are not necessarily state capitals. The ranking of the top 10 cities based on volume of exposed cyber assets does not exactly match the city's ranking based on population, but it is, relatively, not too far off either. Frankfurt has the highest exposure per capita, landing itself in second place for the most number of exposed cyber assets even if it is only the fifth most populous city in Germany. Meanwhile, Leipzig has the lowest exposure per capita.

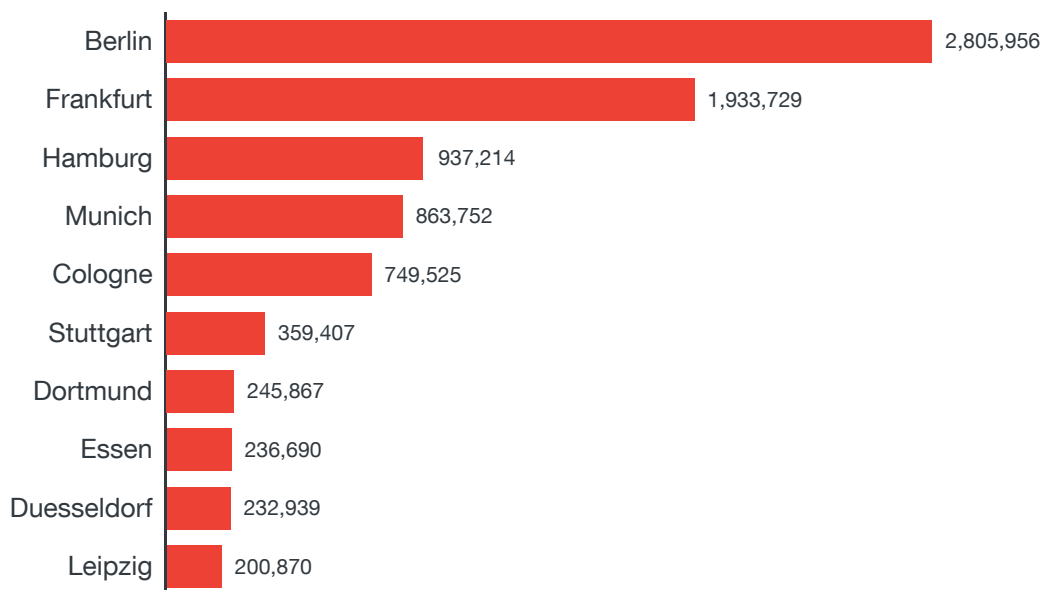


Figure 1. Number of exposed cyber assets in the top 10 German cities by population

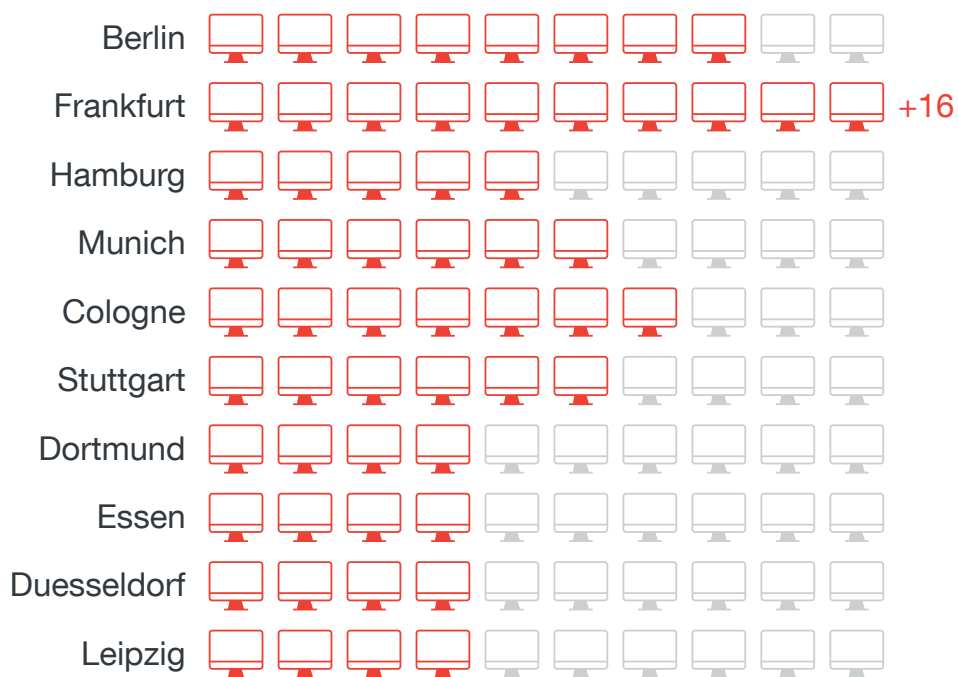


Figure 2. Exposed cyber assets per capita

(Number of exposed cyber assets for every 10 people in German cities)

City	Population
Berlin	3,520,031
Hamburg	1,787,408
Munich ^a	1,450,381
Cologne ^b	1,060,582
Frankfurt ^c	732,688
Stuttgart	623,738
Duesseldorf ^d	612,178
Dortmund	586,181
Essen	582,624
Leipzig	560,472

Table 1. Top 10 cities in Germany by population¹

How Exposed Devices Access the Internet

A great majority of devices in Germany are connected to the internet via Ethernet or modems. This observation likely reflects corporate and enterprise users running high-speed connected servers on the internet. It is therefore expected that majority of the exposed cyber assets will show this as well.

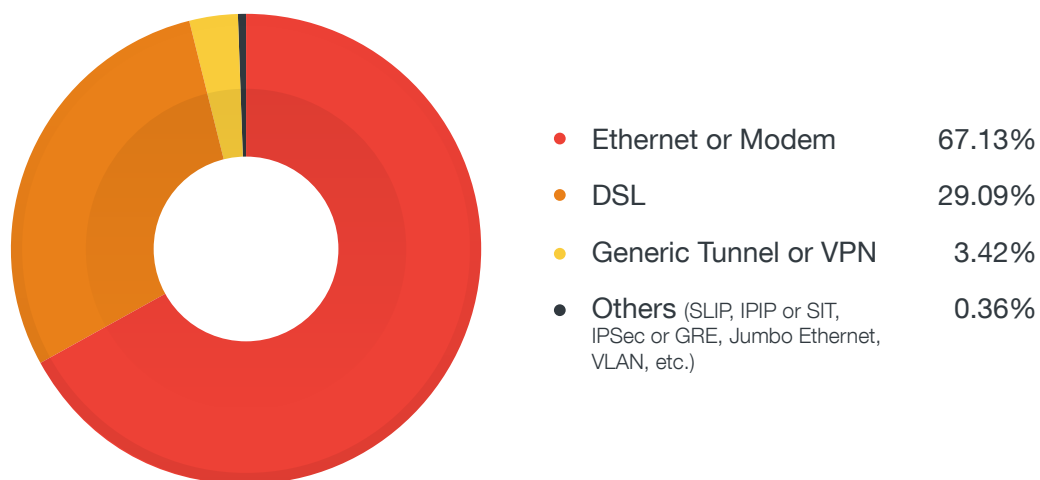


Figure 3. Distribution of means by which exposed devices access the internet

^a German: München.

^b German: Köln.

^c Also includes Frankfurt am Main.

^d German: Düsseldorf.

OSs Running on Exposed Internet-connected Devices

More than 75 percent of exposed devices were found running Linux-based operating systems while Windows-based systems taken together were at roughly 15 percent. Upon closer analysis, this can be attributed to the large number of exposed web services related to Apache web servers, which would predictably be running Unix-based OSs.

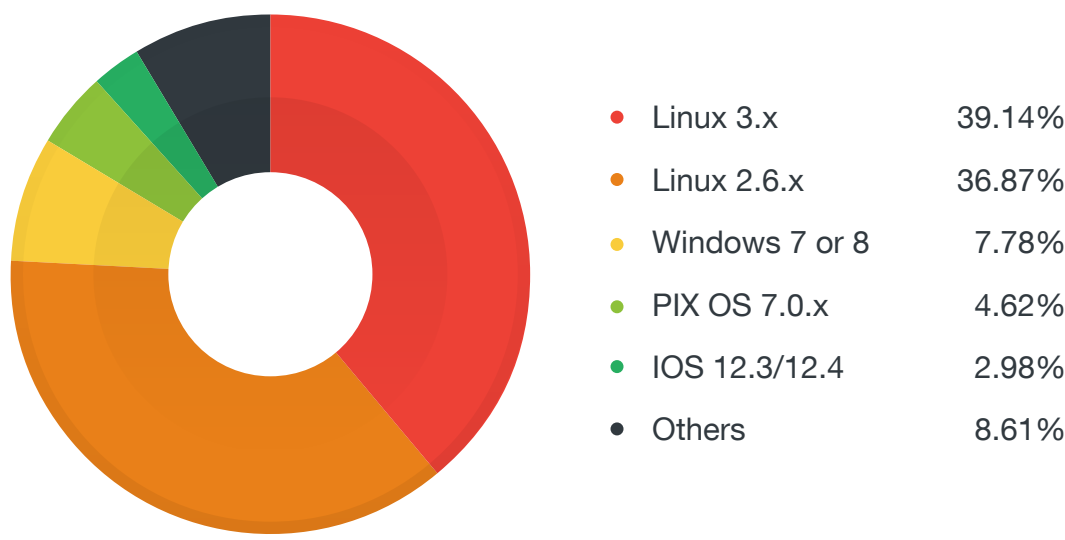


Figure 4. Distribution of exposed device OSs

Top Exposed and Vulnerable Products

The most exposed products in the top 10 cities in Germany were software related to HTTP web servers or services used to operate them, like Apache Hypertext Transfer Protocol daemon (HTTPD), NGINX, OpenSSH, and Microsoft® Internet Information Services (IIS) HTTPD. While this is as expected, it also gives us an idea why internet-facing servers are such an attractive target for cybercriminals. Historically, cybercriminals have 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.

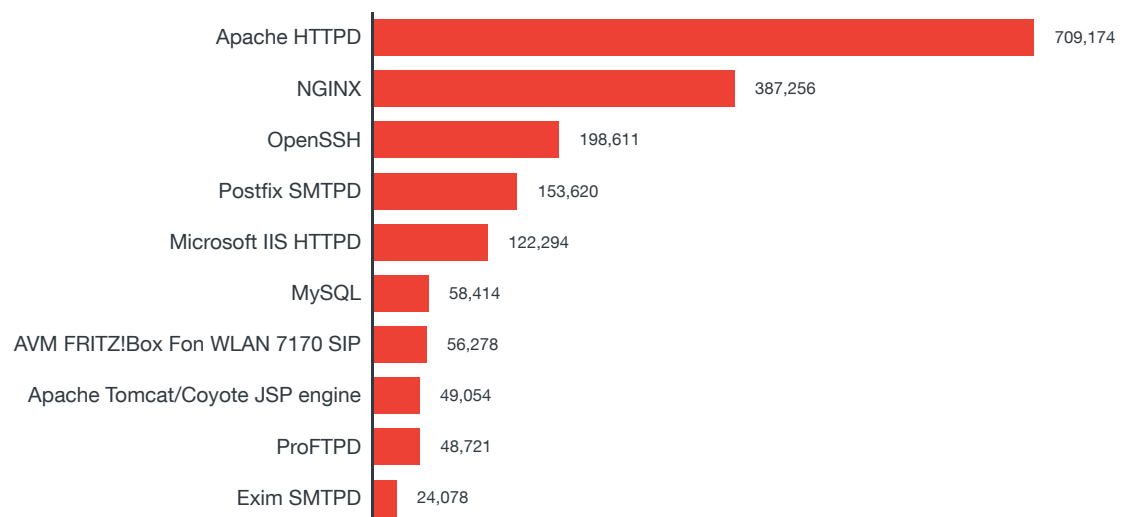


Figure 5. Number of exposed cyber assets by product/service name (top 10)

The Shodan crawler also tests for specific vulnerabilities: CVE-2013-1391 (digital video recorder [DVR] configuration disclosure), CVE-2013-1899 (argument injection in PostgreSQL), CVE-2014-0160 (Heartbleed, OpenSSL), CVE-2015-0204 (Freak, OpenSSL), CVE-2015-2080 (Jetty remote unauthenticated credential disclosure), and CVE-2016-9244 (Ticketbleed, TLS/SSL stack in BIG-IP virtual servers). Here we find that a significant subset of the exposed cyber assets are also vulnerable to known software issues.

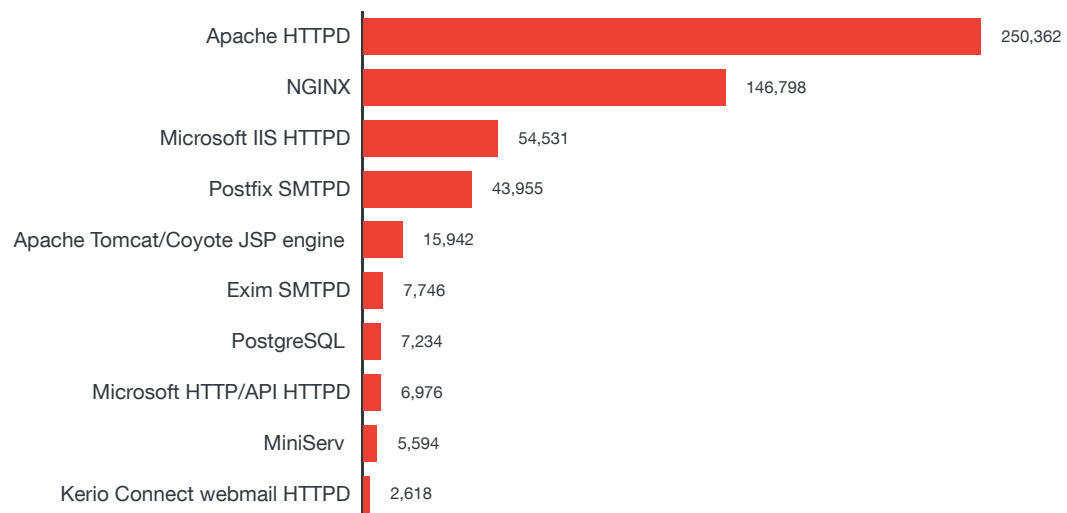


Figure 6. Number of exposed cyber assets by product/service name vulnerable to CVE-2013-1391, CVE-2013-1899, CVE-2014-0160, CVE-2015-0204, CVE-2015-2080, or CVE-2016-9244 (top 10)

Top Exposed and Vulnerable Device Types

An overwhelming bulk of exposed device types in the top German cities were wireless access points, which are generally networking hardware devices that allow 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 provide Voice over Internet Protocol VoIP services that 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. Because of this, the device manufacturer needed to develop firmware updates for over 30 affected models.^{2, 3, 4}

We expected to find a number of firewalls in the scan data, as they typically have an internet-facing front-end. However, what is more interesting is the number of open webcams throughout Germany. While homeowners or security teams install webcams for monitoring properties and preventing theft, exposed webcams defeat this purpose by allowing outsiders to view private security feeds.

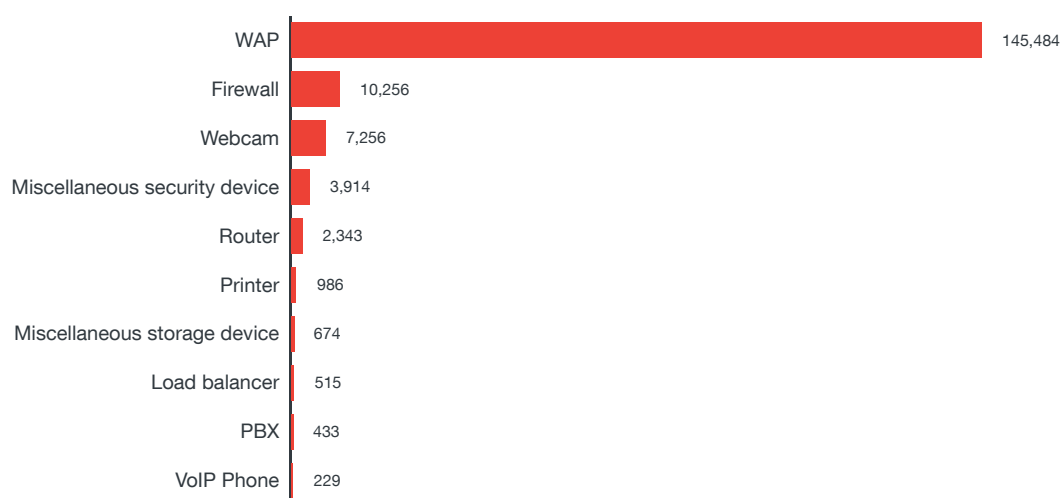


Figure 7. Exposed cyber assets by device type (top 10)

There are a handful of identifiable device types in the Shodan scan data that are vulnerable to the above-mentioned vulnerabilities, majority of which are firewalls.

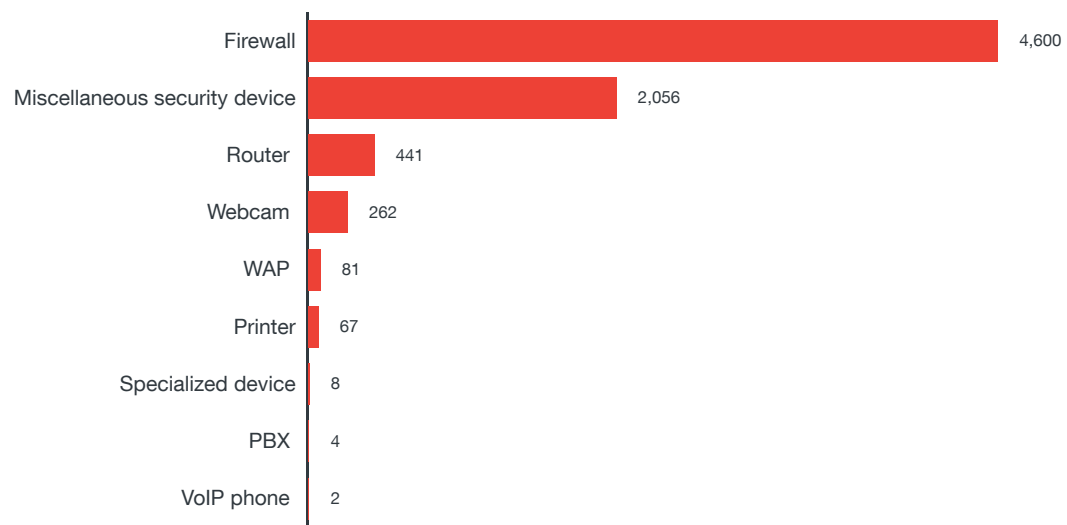


Figure 7. Number of exposed cyber assets by device type vulnerable to CVE-2013-1391, CVE-2013-1899, CVE-2014-0160, CVE-2015-0204, CVE-2015-2080, or CVE-2016-9244

Exposed Cyber Assets in Germany

Exposed Devices

This section digs deeper into the various exposed devices we found in the top 10 most populous German cities using Shodan scan data for February 2017. Firewalls and WAPs are the most prevalent exposed devices, but one can argue that this is to be expected. However, apart from these two, we found several other device types that should not be inadvertently left exposed on the public internet. These exposed devices are at risk of data theft, lateral movement, forced participation in DDoS attacks, and other threats.

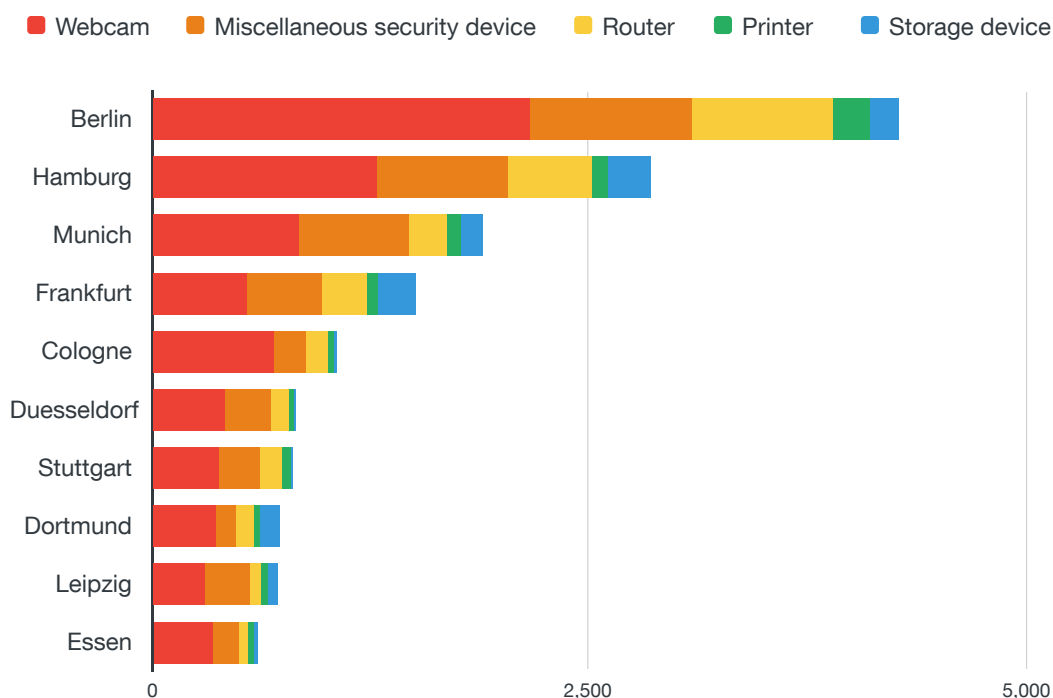


Figure 9. Overview of the top exposed devices (excluding firewalls and WAP) by city

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.

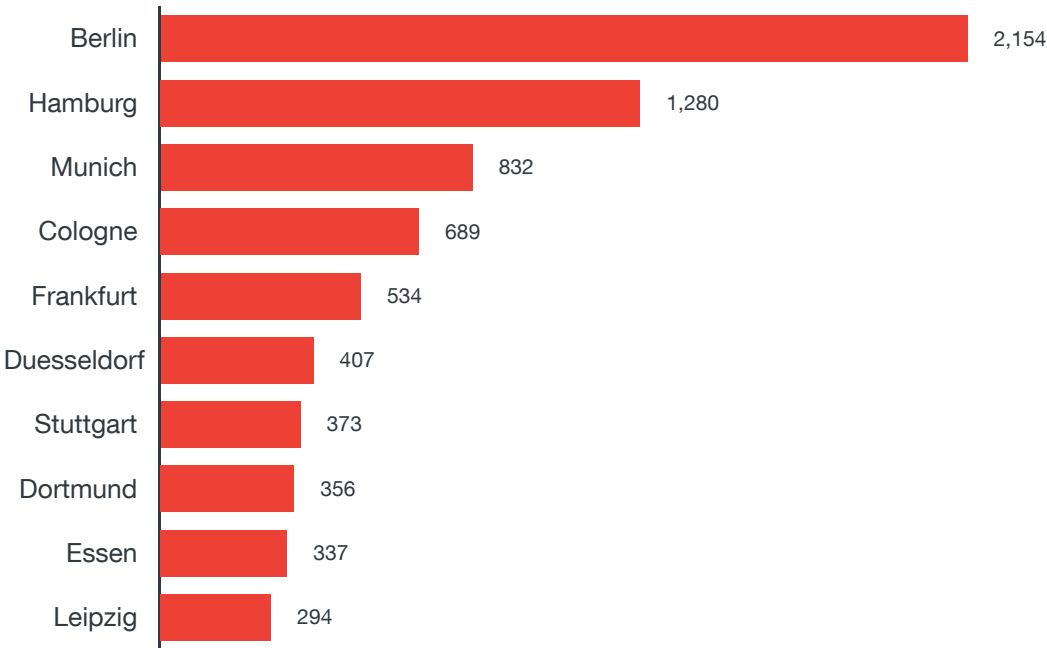


Figure 10. Number of exposed webcams by city

We summarized the exposed webcams by model and found the Netwave IP camera to be the most widely used among them. D-Link came second on a per-brand basis, and Avtech came in third.

Webcams are rarely patched and most do not have auto-update functionality. This means webcams could remain vulnerable for months or even perpetually after purchase if the user doesn't specifically update and patch them, which users rarely think to do. Furthermore, the Achilles heel of webcams are unchanged default passwords or weak passwords that are vulnerable to brute-force or dictionary attacks.

Botnet malware like Mirai⁵ and Persirai⁶ have been known to target vulnerable IP cameras, access their passwords, if any, and deploy command injections. Mirai is used to conduct DDoS attacks using a compromised network of smart and connected devices.

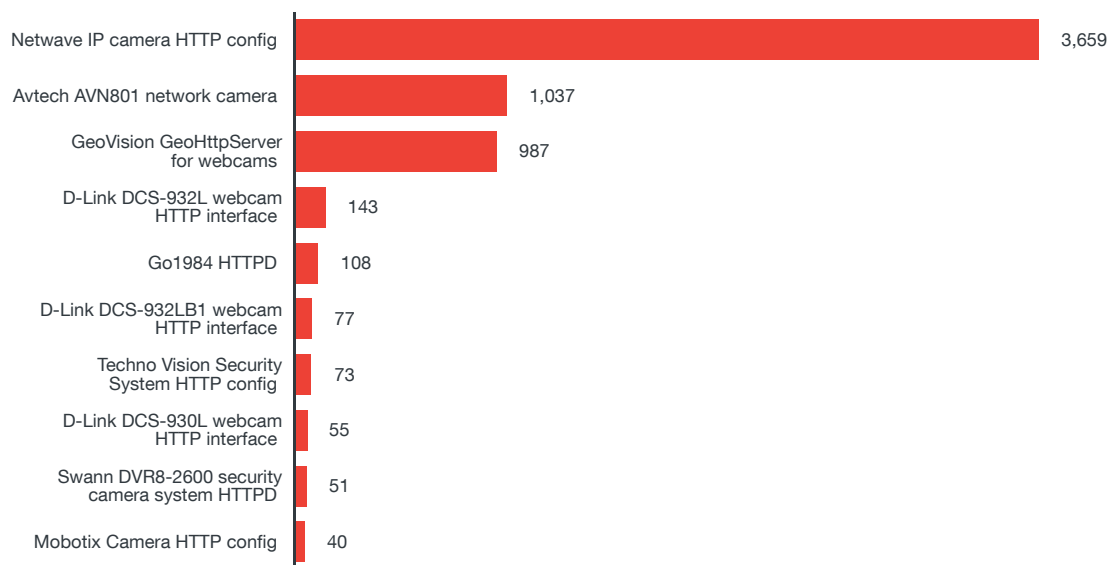


Figure 11. Number of exposed webcams by product/service name (top 10)

Exposed NAS Devices

There were not a lot of exposed network-attached storage (NAS) devices in Germany, 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 will want to keep private.

That said, we were still able to find a handful of exposed NAS devices.

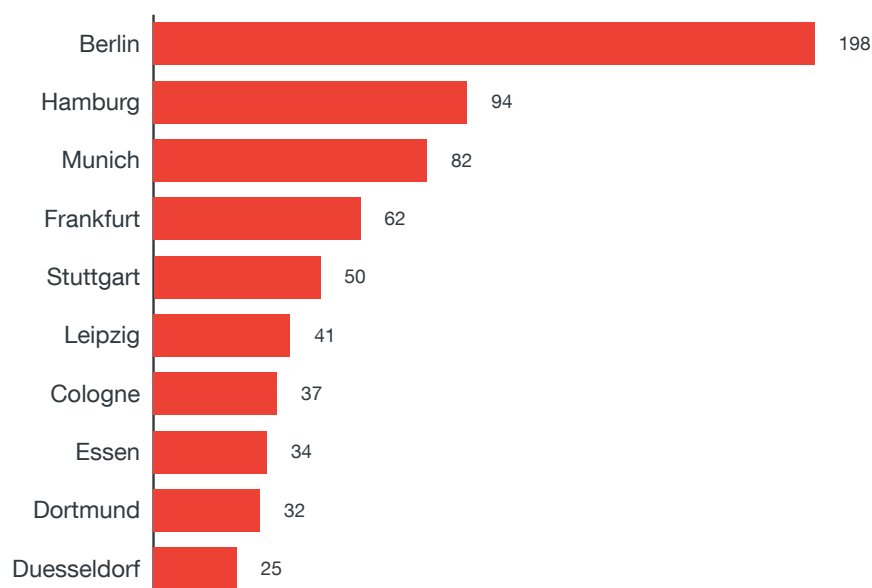


Figure 12. Number of exposed NAS devices by city

The exposed NAS devices observed were either Seagate GoFlex NAS or different models of Synology Disk Station NAS, both of which are consumer-grade NAS likely to be found in home networks, where users are not aware of the need to secure their devices.



Figure 13. Number 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. 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.

There are over 50,000 exposed routers in Berlin, followed by Munich with around 20,000. Compared to the other countries in Western Europe we analyzed, Germany—Berlin, in particular—has the most number of exposed routers.

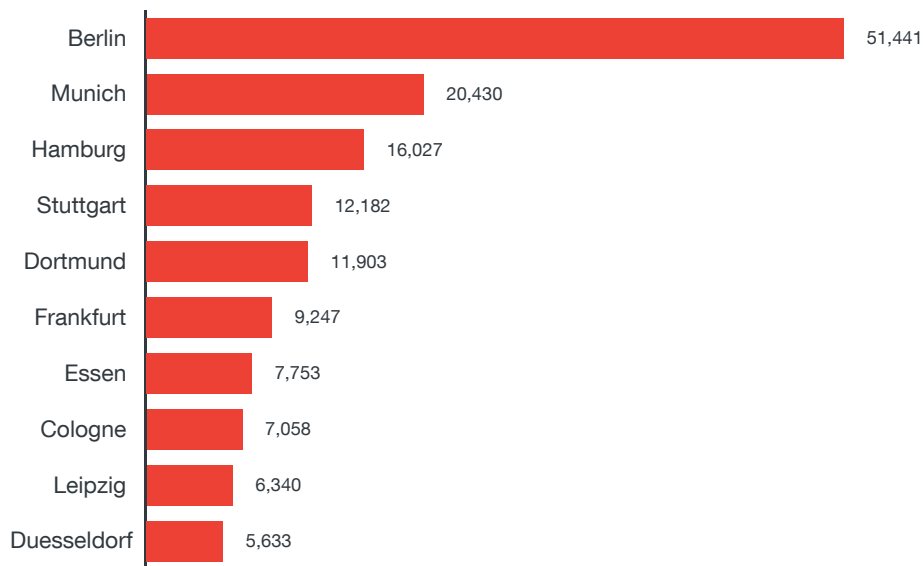


Figure 14. Number of exposed routers by city

As mentioned in an earlier section, the volume of exposed routers is driven primarily by Fritz!Boxes. The 7170 model which we saw most prevalently (as shown below), in particular, is a wireless model, albeit a relatively old one. While we cannot assume the actual usage for the exposed AVM Fritz!Box Fon WLAN 7170 routers, it is likely that a number of these are used in home networks. The most recent model in our data is the 7390, while the current models offered in the market are the newer 74xx and 75xx series.

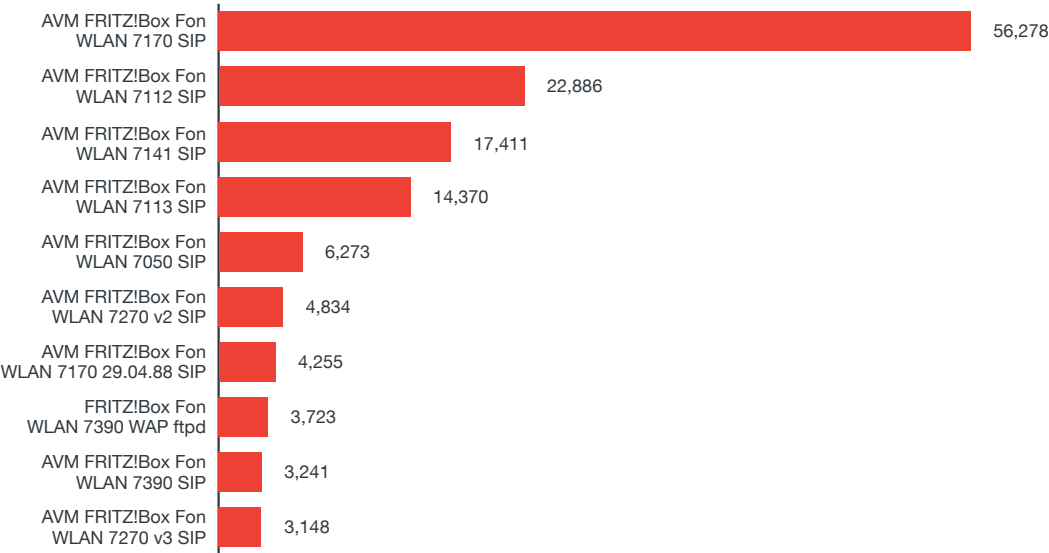


Figure 15. Number of exposed routers by product/service name

Exposed Printers

A printer can store cached copies of documents it printed. For cybercriminals, access to exposed printers can also mean access to company secrets, intellectual property, PII, and various kinds of sensitive and personal information. Compromised printers can also be used for lateral movement within a target network, to generate network traffic, and to participate in attacks against other organizations such as DDoS and telephony denial-of-service (TDoS). Given the multifunctional nature of printers, attacks utilizing network, voice, and cellular are all possible from poorly configured printer devices.

There are only a handful of exposed printers in the top German cities. A quarter of them are in Hamburg.

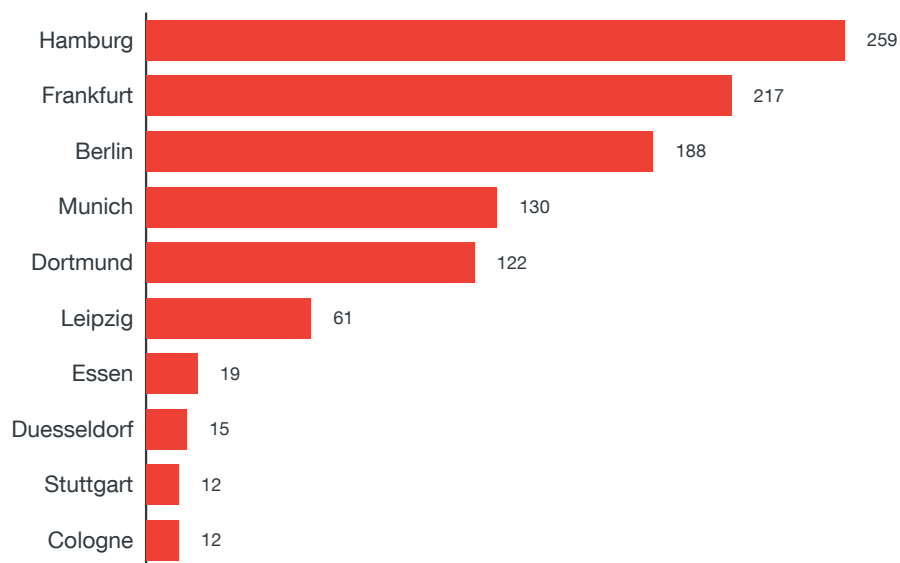


Figure 16. Number of exposed printers by city

Most of the exposures observed in Shodan for printers appear 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.

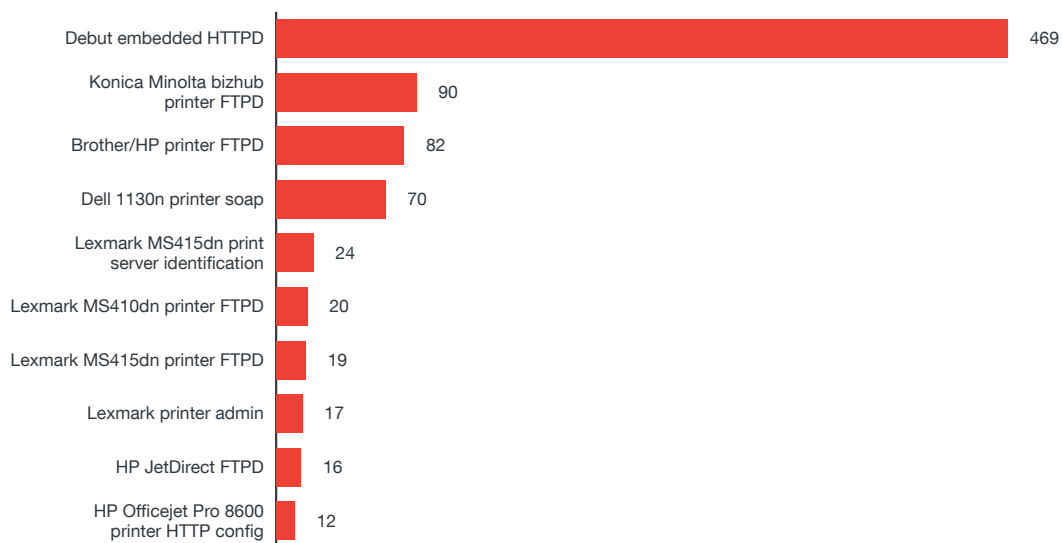


Figure 17. Number of exposed printers by product/service name

Exposed VoIP Devices

VoIP technology makes making phone calls (both local and overseas) cheaper. Thus, many companies are switching to VoIP phones. We found less than a thousand exposed VoIP phones across the top 10 cities in Germany. The rest appeared to be sitting behind web application firewalls or were classified by Shodan as exposed routers.

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 operations.

Worse yet, these VoIP phones can be used in a variety of telephone-based, cyber-facilitated attacks like swatting. Sending voice spam (vphish) and TDoS are two other examples of how these exposed VoIP devices can be misused.

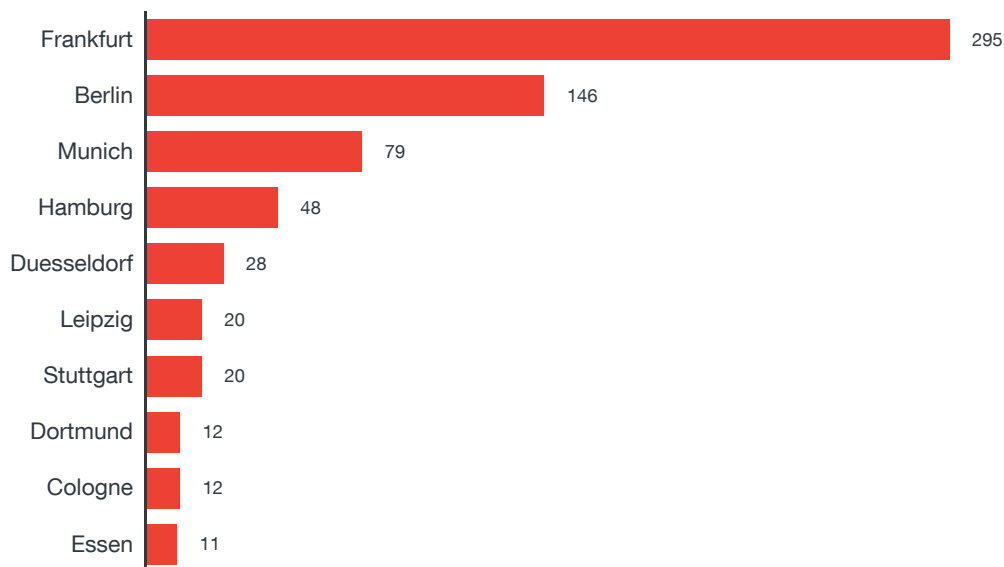


Figure 18. Number of exposed phones by city

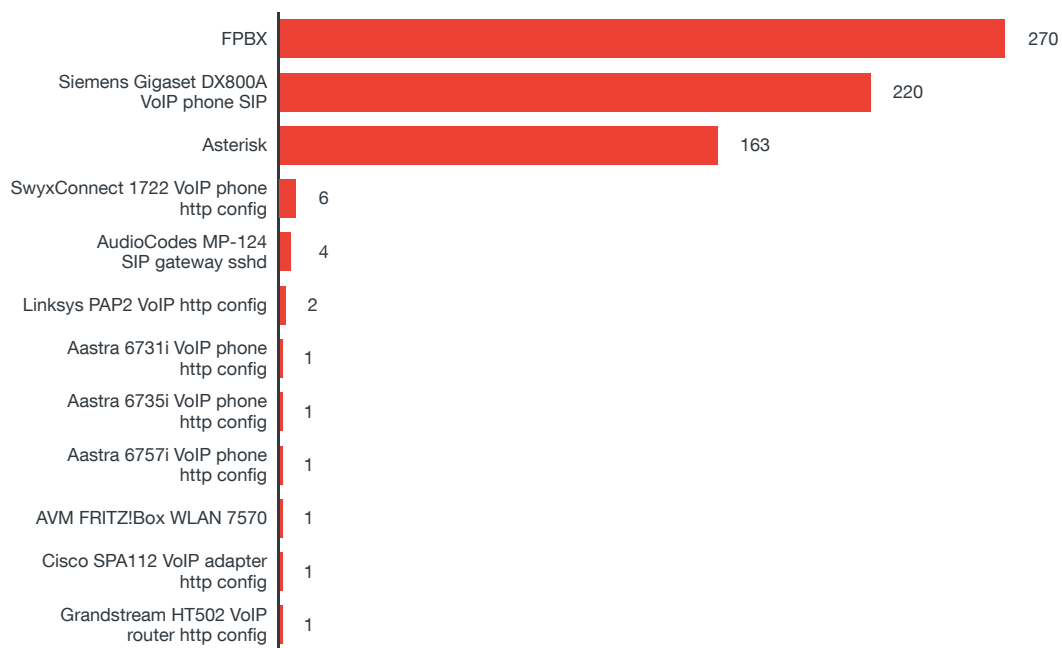


Figure 19. Number of exposed phones by product/service name

Exposed Media Recording Devices

Media recording devices like 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 German cities, a number of which were in Munich. Dreambox, Kodi (XBMC), and Hauppauge Digital are some of the players in the digital television industry, as reflected in the volume of brands of exposed media devices.

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

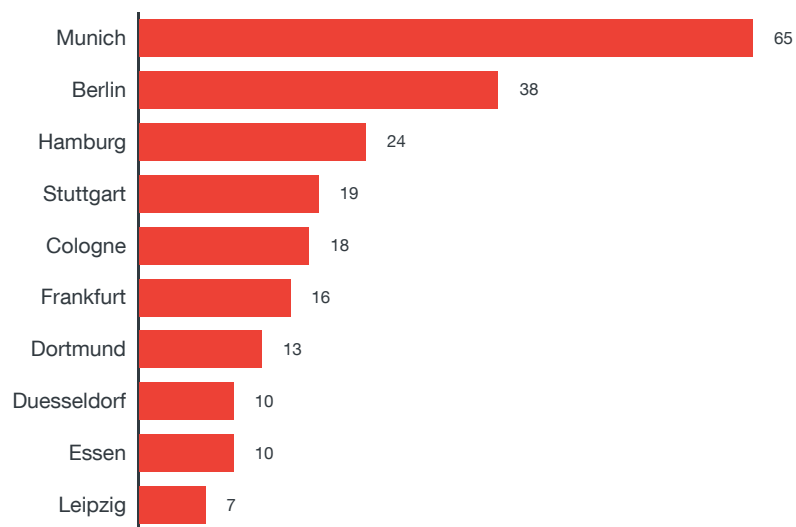


Figure 20. Number of exposed media recording devices by city

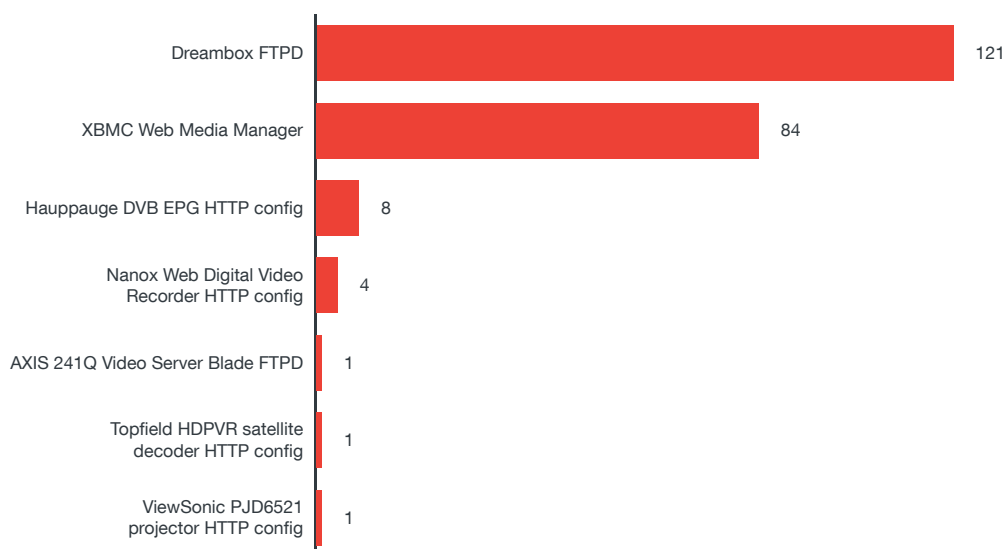


Figure 21. Number of exposed media recording devices by product/service name

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 top 10 cities in Germany. 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 to see that the most prevalent type of web service in Germany are related to Apache servers. These types of servers are widely used because they are cheap and easy to deploy and manage, and often can be fully implemented for free. NGINX, a free, open-source, high-performance HTTP server, reverse proxy, and Internet Message Access Protocol (IMAP)/Post Office Protocol 3 (POP3) proxy server, is the second most prevalent web server software.⁷

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 affect Apache and 219 vulnerabilities that directly or indirectly affect Microsoft IIS servers.

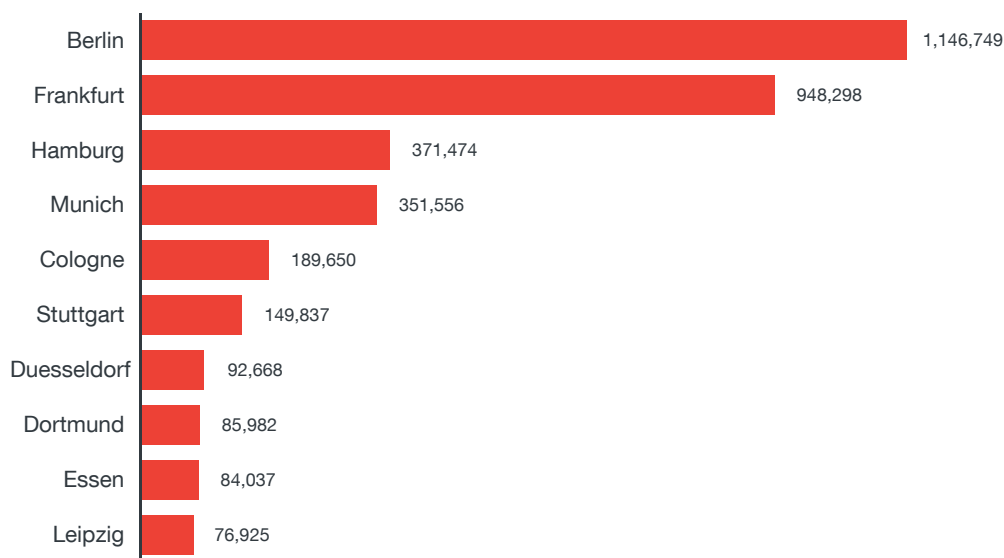


Figure 22. Number of exposed web services by city

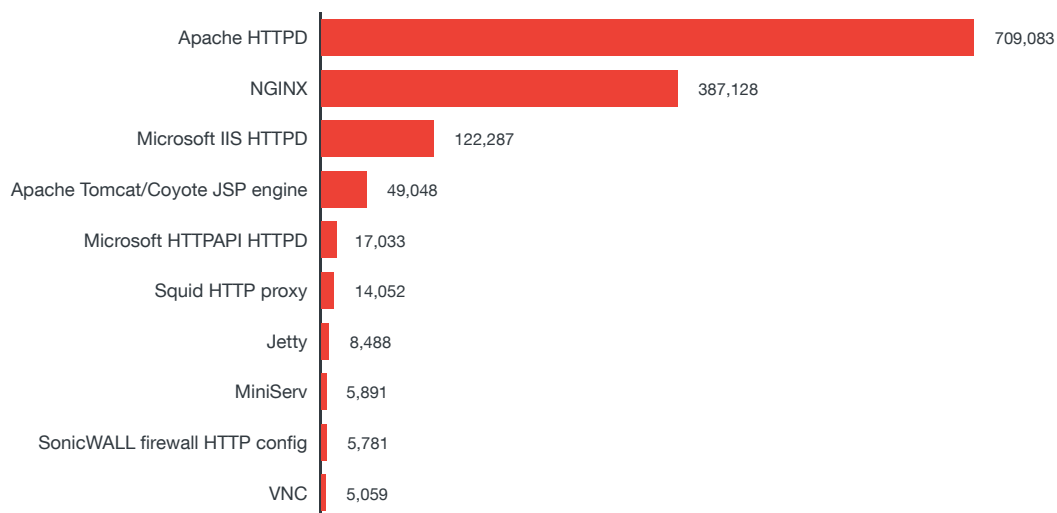


Figure 23. Number of exposed web services by software (top 10)

Exposed Email Services

Email servers are also internet-facing by design, which is all the more reason for enterprises to secure them. Berlin has the most number of exposed email services. Most of the exposed email services we saw in the German Shodan data are Postfix SMTPD.

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 will severely affect daily business operations. Compromised personal email accounts can lead to the theft of PII, photos, financial information, credentials, and other sensitive information, and can possibly inflict damage to the affected individuals.

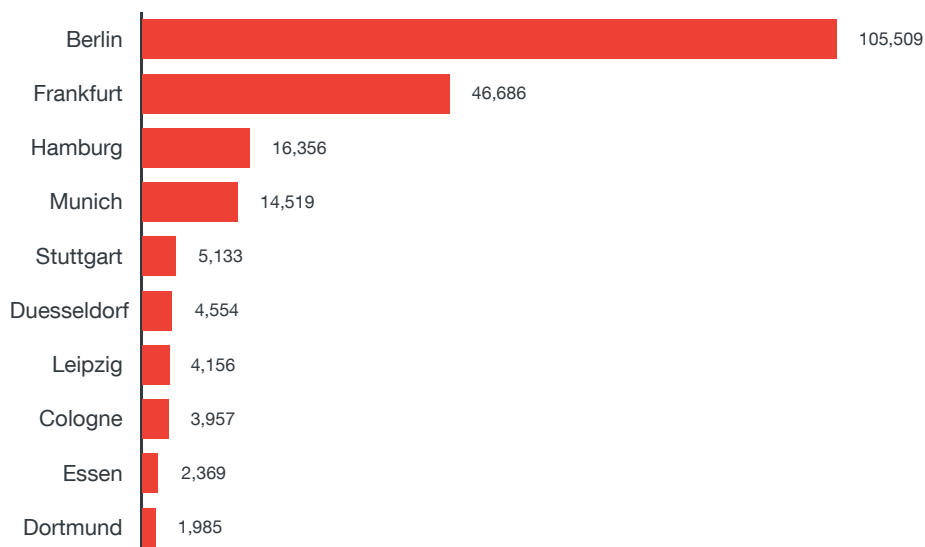


Figure 24. Number of exposed email servers by city

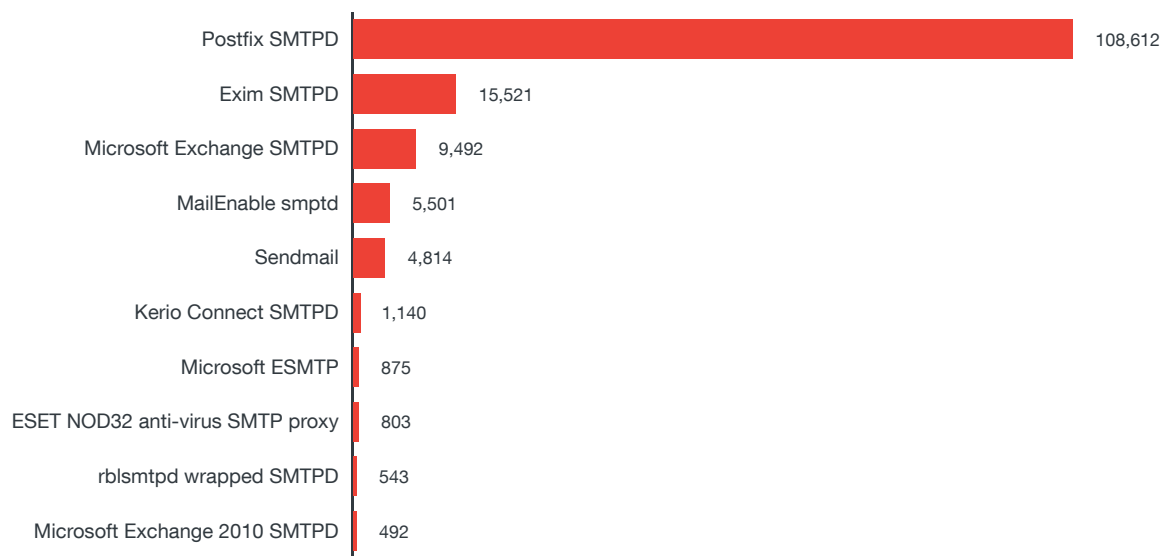


Figure 25. Number of exposed email servers by product/service name (top 10)

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 the cybercriminal fora.

Frankfurt overtook Berlin in having the most number of exposed databases for all types.

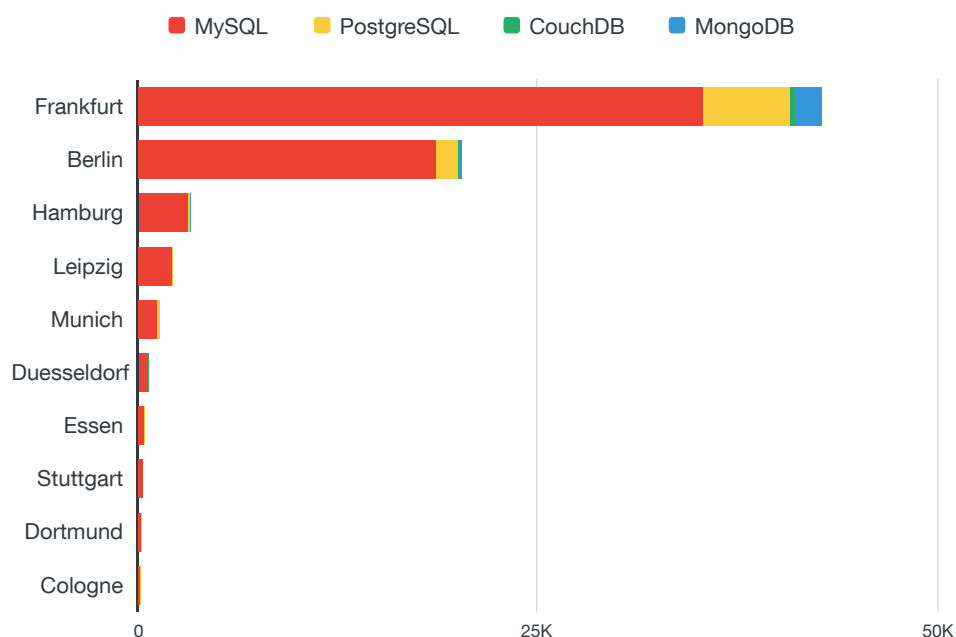


Figure 26. Overview of exposed databases by city

We found that there were many more exposed MySQL databases than PostgreSQL, CouchDB, and MongoDB. At the time of publishing, around 244 vulnerabilities with CVE details were found to affect MySQL. 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.

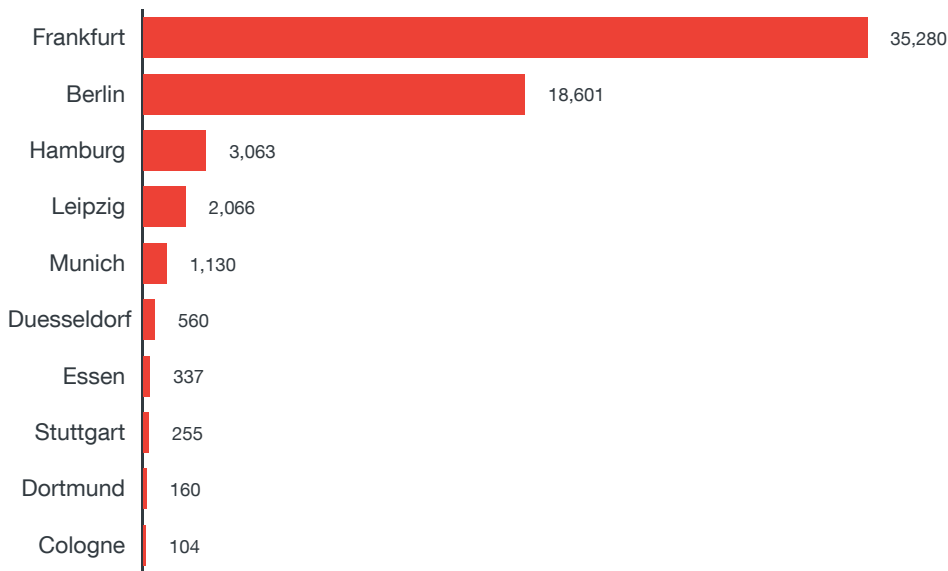


Figure 27. Number of exposed MySQL databases by city

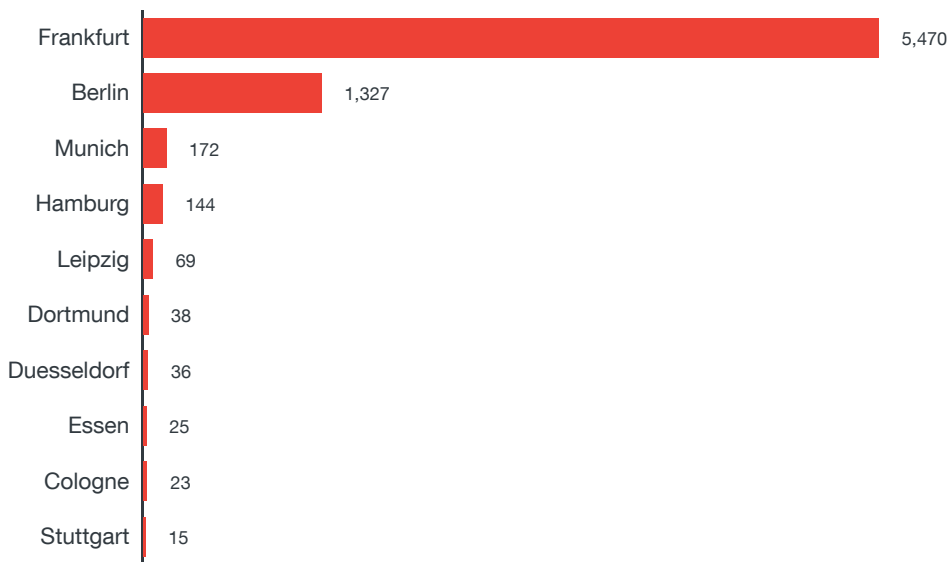


Figure 28. Number of exposed PostgreSQL databases by city

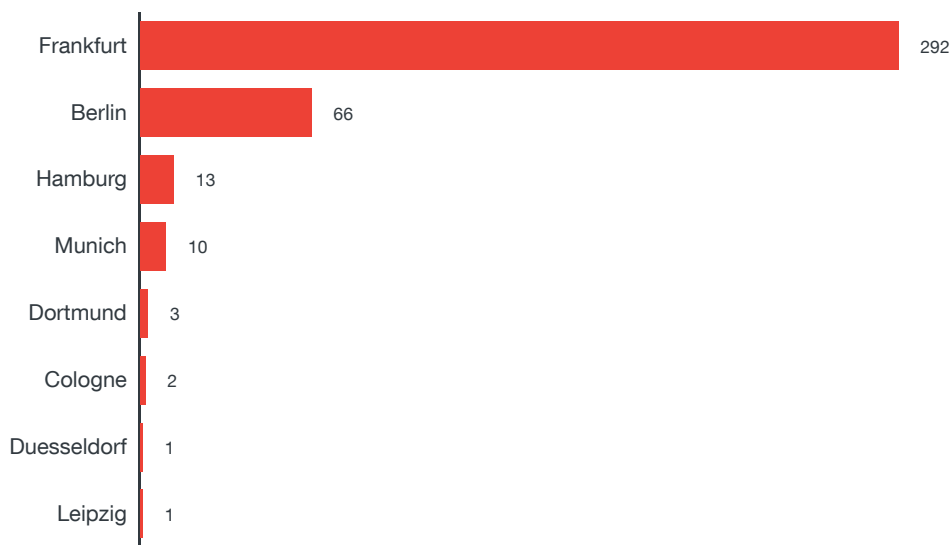


Figure 29. Number of exposed CouchDB databases by city

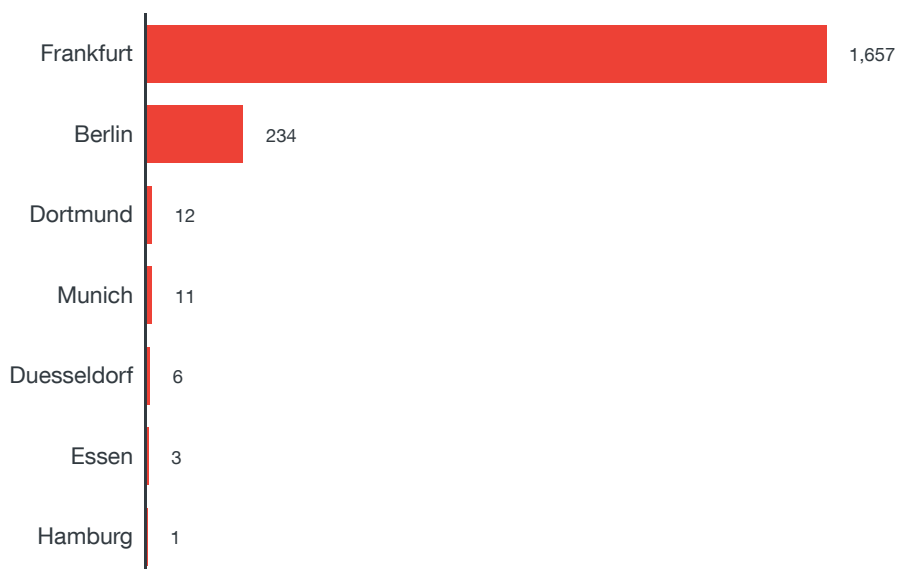


Figure 29. Number of exposed MongoDB databases by city

Exposed Service Protocols in Germany

This section digs deeper into exposed services such as Network Time Protocol (NTP), Universal Plug and Play (UPnP) or 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 Germany. Vulnerabilities in the said protocols can be exploited to successfully compromise the devices or systems running them.

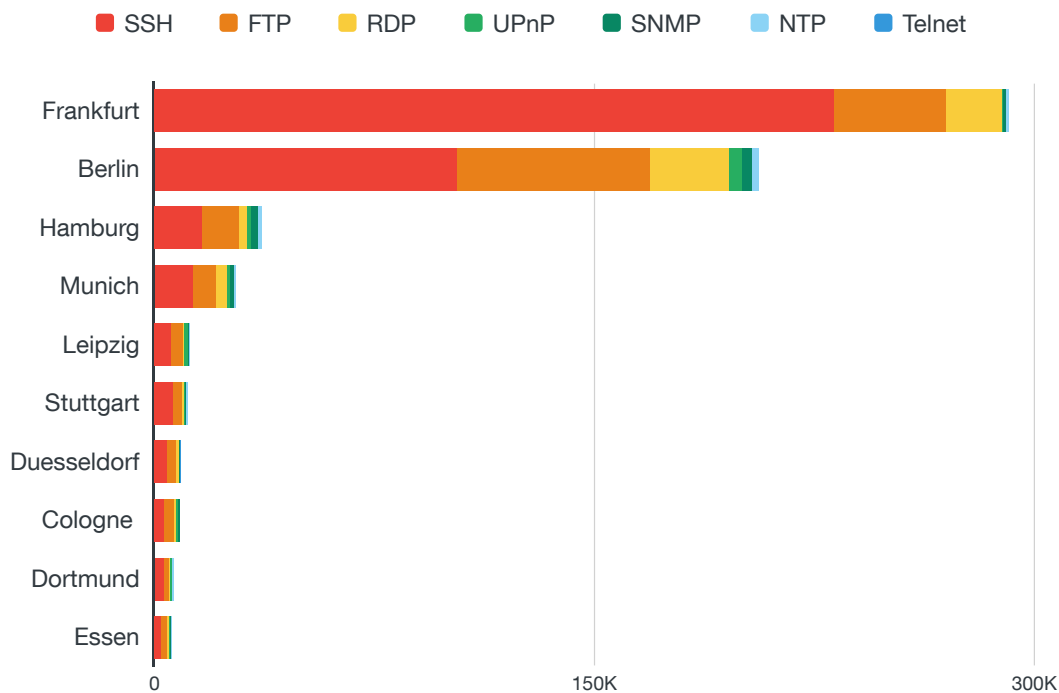


Figure 31. Overview of exposed service protocols by city

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.

In addition, a paper by Boston University researchers⁸ 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 times that are 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 DNS record tampering. The most troubling scenario involves bypassing HyperText Transfer Protocol Secure (HTTPS) encryption by forcing a computer to accept an expired transport layer security (TLS) certificate.⁹

Berlin has the most number of exposed NTP at a little over 2,000, while Hamburg comes in second.

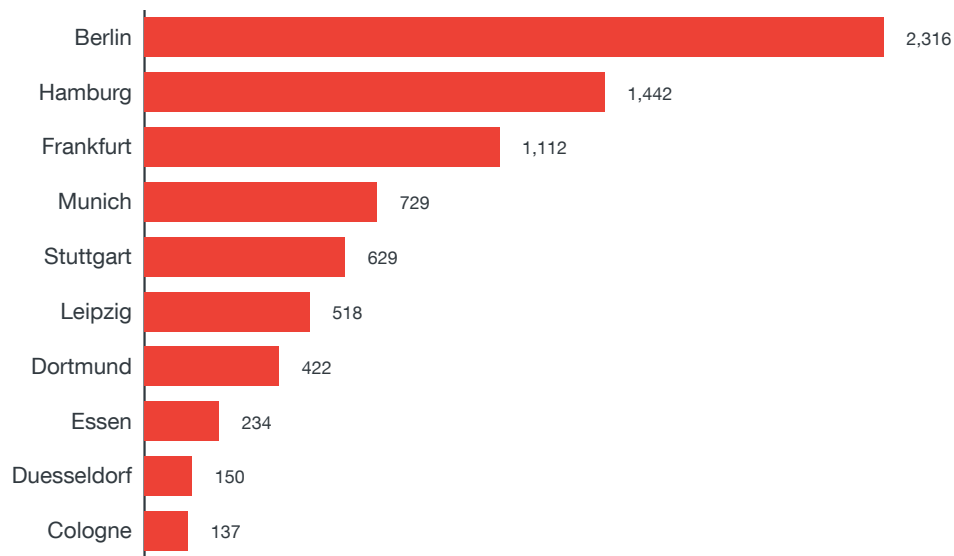


Figure 32. Number of exposed NTP-enabled devices by city

Exposed UPnP/SSDP-enabled Devices

UPnP¹⁰ 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, there are 65 vulnerabilities that directly or indirectly affect UPnP while 20 vulnerabilities directly or indirectly affect SSDP. The Metasploit framework includes many UPnP and SSDP modules that can be used to exploit and compromise UPnP- or SSDP-enabled devices.

Berlin had the most number of exposed UPnP/SSDP-enabled devices among the top 10 German cities, with a total exposed device count almost three times that of Hamburg, which came second. 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.

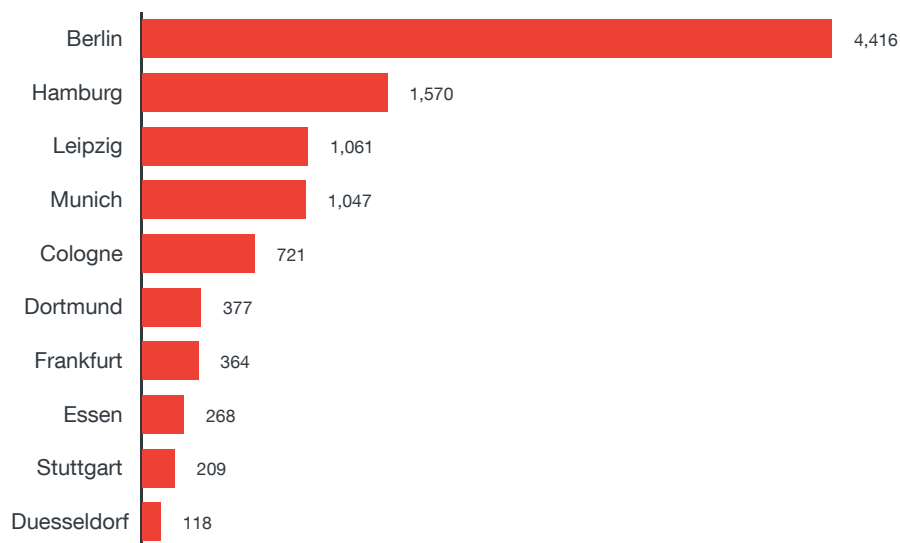


Figure 33. Number of exposed UPNP-/SSDP-enabled devices by city

Exposed SNMP-enabled Devices

SNMP¹¹ 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 therefore a convenient way for hackers to figure out network topology, which they can later use for lateral movement within the target network. It can also be used to manage devices, for instance, to shut down a network interface, making it a dangerous tool in the hands of threat actors.¹² 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 an 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 being sent from the devices to the victims.¹³

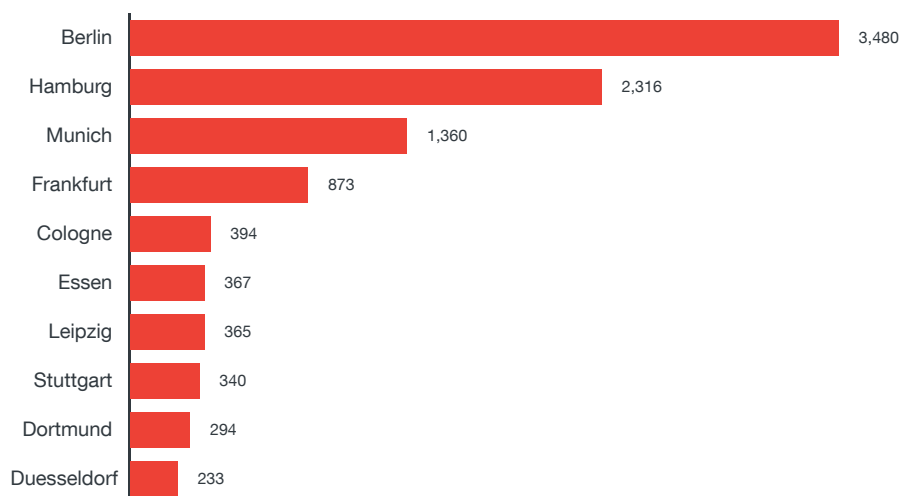


Figure 34. Number of exposed SNMP-enabled devices by city

Exposed SSH-enabled Devices

SSH is a cryptographic network protocol used to securely operate network services over an unsecured network.¹⁴ It is one of the protocols frequently targeted by hackers, usually via brute-force attacks. In an SSH brute-force attack, an automated program tests combinations of usernames and passwords on a server to gain entry. This is effective against weak username/password combinations.

Frankfurt has over 200,000 exposed SSH-enabled devices, more than twice as many as Berlin. Hamburg and the rest together total a little less than 55,000.

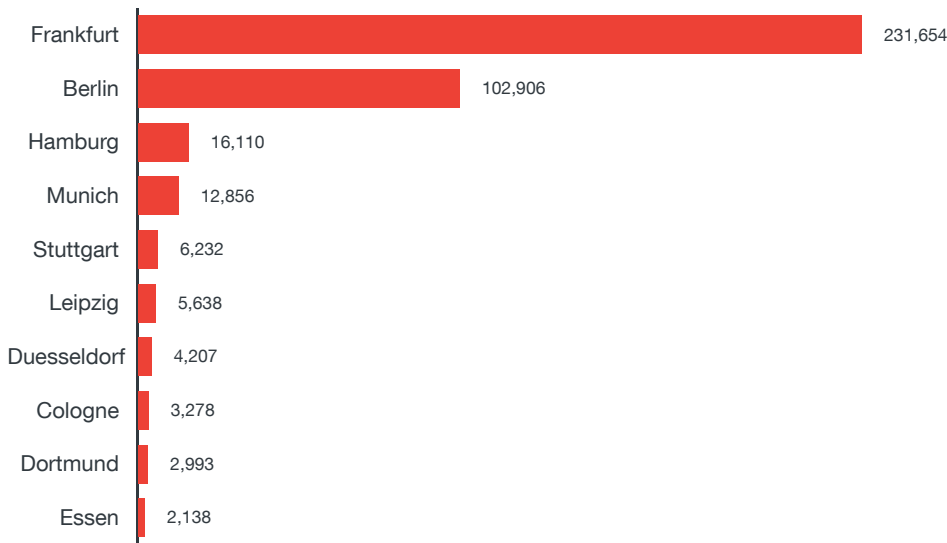


Figure 35. Number of exposed SSH-enabled devices by city

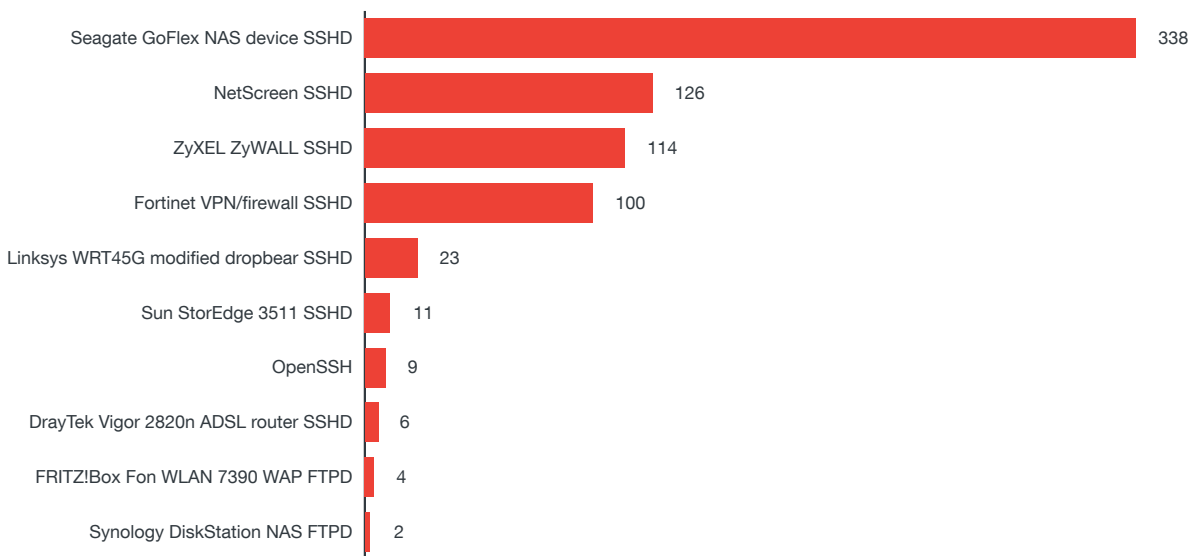


Figure 35. Number of exposed SSH-enabled devices by product/service name

Exposed RDP-enabled Devices

RDP¹⁵ 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. One of the popularly exploited RDP vulnerabilities is CVE-2012-0002. The proof-of-concept (PoC) code for CVE-2012-0002 was leaked online, leading to widespread exploitation. RDP has traditionally been abused to exfiltrate data as part of a targeted attack, steal information that can be sold in Deep web marketplaces, and integrate hijacked systems into botnets. Recently, Crysis ransomware was found to be able to brute-force RDP as an infection vector.¹⁶ Given the end of support for Windows XP despite its continued use, affected organizations face a significant risk.

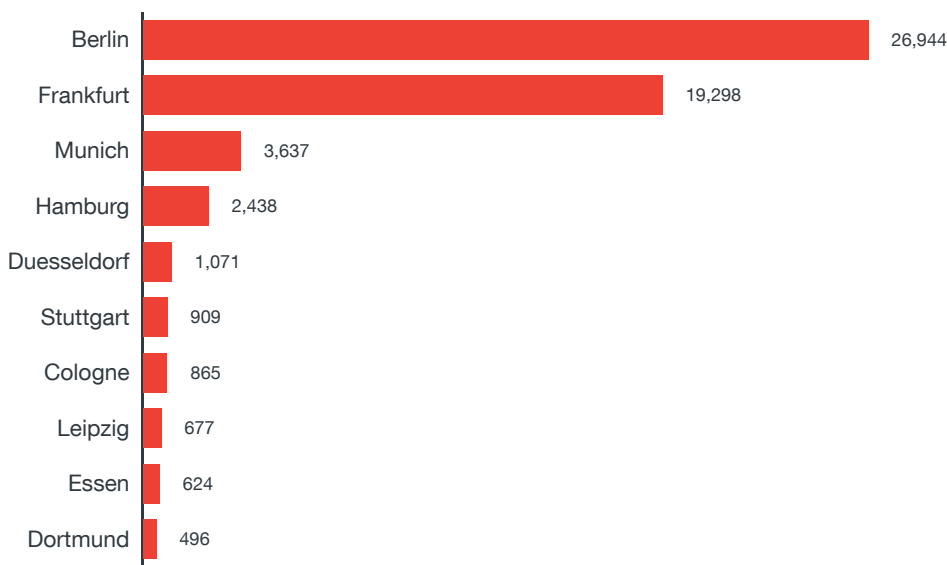


Figure 37. Number of exposed RDP-enabled devices by city

Exposed Telnet-enabled Devices

Telnet¹⁷ 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.

However, we continued to see that a lot of routers have Telnet open, most likely to allow for remote administration of the router. It is critical in these cases to ensure strong authentication in order to harden the service.

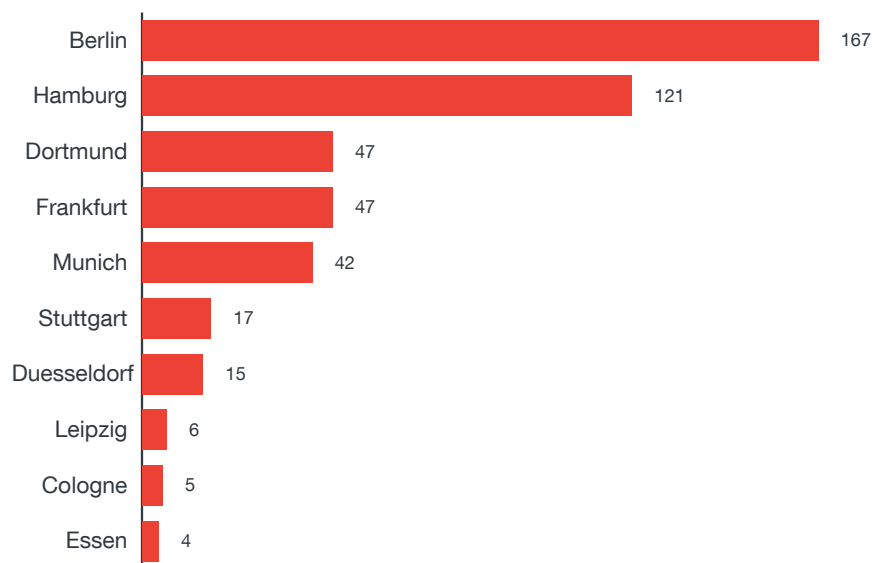


Figure 38. Number of exposed Telnet-enabled devices by city

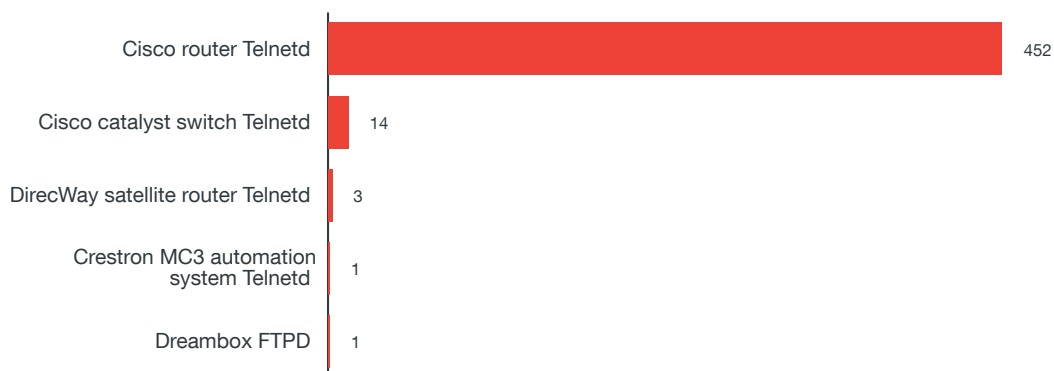


Figure 39. Number of exposed Telnet-enabled devices by product/service name

Exposed FTP-enabled Devices

FTP¹⁸ 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, WAP and NAS devices, printers, print servers, and webcams in the list of exposed FTP-enabled devices.

Berlin has the most instances of exposed FTP, followed by Frankfurt. One probable reason is the high number of users of ProFTPD, a free and open-source FTP server type in the said cities.

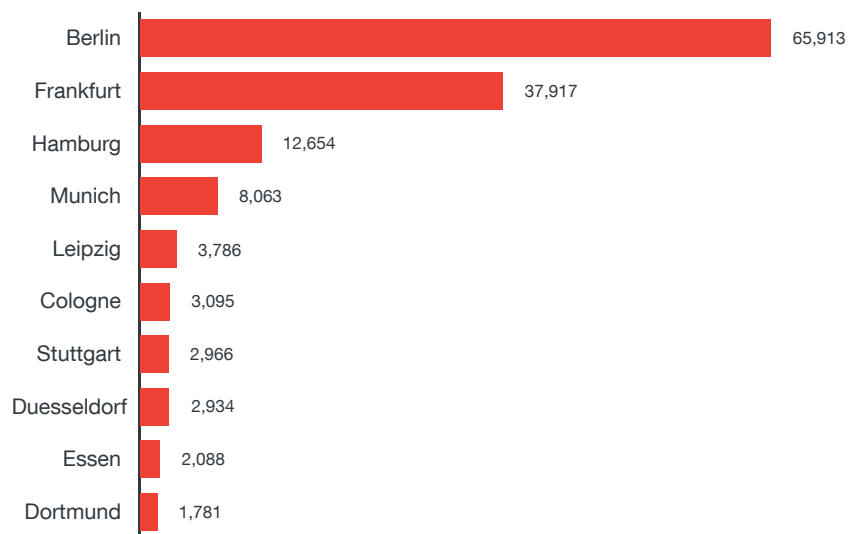


Figure 40. Number of exposed FTP-enabled devices by city

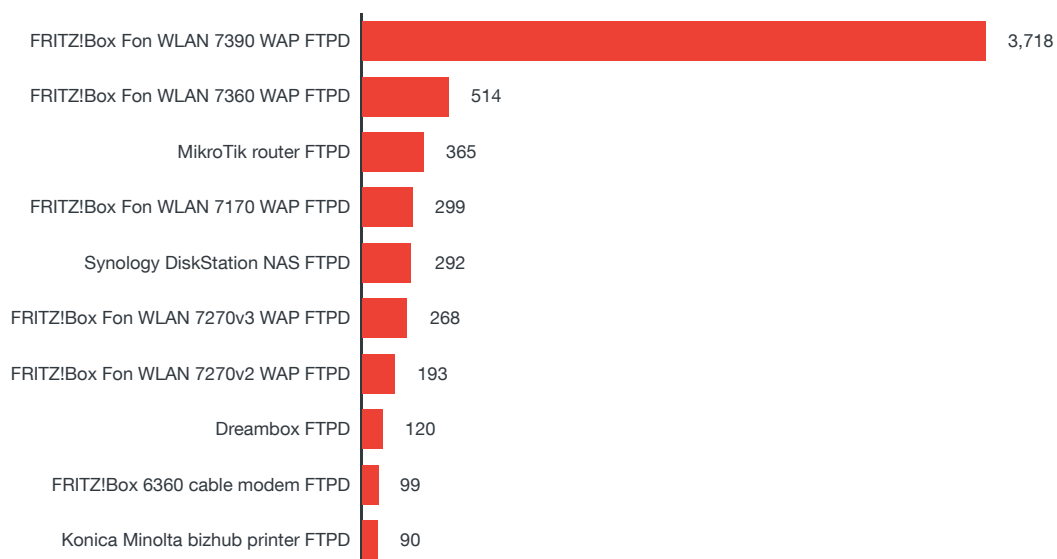


Figure 41. Number of exposed FTP-enabled devices by product/service name

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)¹⁹ taking effect on May 2018, businesses regardless of size and industry must ensure compliance or pay penalties—up to 4 percent of annual turnover. GDPR puts a premium on data protection and privacy of consumers and could affect enterprises and small and medium-sized businesses²⁰ whether they are physically based in Europe or not, as long as they process 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 and help the response team understand ongoing attacks.
- Properly configured 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 further look into fulfilling the Critical Security Controls (CSC)²¹ 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 with 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.

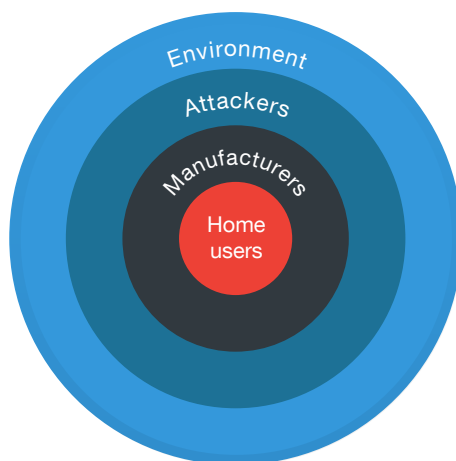


Figure 44. Risk factors increase with the addition of each layer in the IoT ecosystem

(Source: “Securing Your Smart Homes”²²)

It is not unusual for the average home to have several connected devices. As such, 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 common sense 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 passwords with strong ones. 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 the use of 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 daily operations (e.g., Telnet on webcams). If possible, users should 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 encryption for both disk and communication. 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.
- Secure your routers. 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 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 required for the bathroom scale to send the measured weight to an online portal that tracks daily changes in weight and provides fitness suggestions.

Connected devices are an integral part of our daily lives. Ideally, device security should not affect availability and should be transparent to the 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—our connected devices hide among billions of other connected devices online and avoid getting compromised by hackers.

Conclusion

Exposed cyber assets can be easily secured. However, we continue to find different devices, servers, databases, and protocols that are operating openly, fully accessible to different types of threat actors who can make rudimentary conclusions based on information as simple as those that can be found in Shodan records' banner and metadata. Compared with our observation of developed countries like the United States, the United Kingdom, and France, Germany, more than any other country we have looked at, is highly networked. That is, we could see a far higher level of technology use per capita than any other country we have analyzed.

Some of our findings include:

- The use of Fritz!Boxes, residential gateway devices that also provide VoIP (Voice over IP) services, is widespread, and close to 150,000 devices acting as wireless access points were searchable in Shodan. This is concerning given a prior resolved issue in 2014 wherein cybercriminals attacked port 443 on these routers in order to obtain user passwords.
- Unlike many other countries, even smaller towns in Germany are highly connected, as observed in the data. Even many cities in the bottom half of the top 10 most populous cities in Germany are more interconnected than some capital cities of other European countries.
- Of the 700,000 exposed Apache web servers in Germany, around 250,000 were also found to be vulnerable to some or all of the security issues scanned for by Shodan.
- Frankfurt had the most number of systems with exposed protocols, at a little over 200,000, specifically via SSH-enabled devices. SSH is usually targeted by hackers using brute-force attacks.

Fortunately, there are several known ways to secure exposed devices, whether in the context of the home office or the corporate network. For home network owners, securing connected devices is mostly a matter of educating oneself about the connected devices that one buys, and to perform routine maintenance including the regular changing of strong passwords. For enterprises, the most effective security strategy goes above and beyond a security checklist and works under the assumption that a network is already compromised. It should also consider how to detect threats in that scenario as well as prevent future threats.

Appendix

Research Coverage

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

City	Population
Berlin	3,520,031
Hamburg	1,787,408
Munich	1,450,381
Cologne	1,060,582
Frankfurt	732,688
Stuttgart	623,738
Duesseldorf	612,178
Dortmund	586,181
Essen	582,624
Leipzig	560,472

Table 2. List of German 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 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 more.²³ 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 German 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 cities in Germany. The data set used contained a total of 51,576,513 records generated from scanning 16,553,265 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 using 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 impact the number of internet-exposed devices and systems; hence, we assume a month's worth of scan data will give us an accurate snapshot of what devices and systems are exposed online in Germany. 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 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 being absent from Shodan scans does not mean it is not exposed online. On the other hand, Shodan may rescan the same IP address multiple times in the same month.
- 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 devices.²⁴ 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. 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>.
2. AVM. (10 February 2014). *AVM Press Release*. "Attacks on FRITZ!Box clarified - Security advice still in effect - Updates will be released shortly." Last accessed on 11 October 2017, <http://web.archive.org/web/20160918112503/https://en.avm.de/press/press-releases/2014/02/attacks-on-fritzbox-clarified-security-advice-still-in-effect-updates-will-be-released-shortly/>.
3. AVM. (10 February 2014). *AVM Press Release*. "AVM with a Security Update for the FRITZ!Box." Last accessed on 11 October 2017, <http://web.archive.org/web/20160918112508/https://en.avm.de/press/press-releases/2014/02/avm-with-a-security-update-for-the-fritzbox/>.
4. AVM. (6 February 2014). *AVM Press Release*. "Important security information for FRITZ!Box users with remote access enabled." Last accessed on 11 October 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/>.
5. Giannina Escueta. (13 February 2017). *TrendLabs Security Intelligence Blog*. "Mirai Widens Distribution with New Trojan that Scans More Ports." Last accessed on 11 October 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/mirai-widens-distribution-new-trojan-scans-ports/>.
6. Kenneth Lu Tim Yeh and Dove Chiu. (8 June 2017). *TrendLabs Security Intelligence Blog*. "The Reigning King of IP Camera Botnets and its Challengers." Last accessed on 11 October 2017, <https://blog.trendmicro.com/trendlabs-security-intelligence/reigning-king-ip-camera-botnets-challengers/>.
7. NGINX Inc. (2017). *NGINX*. "Welcome to NGINX Wiki!" Last accessed on 11 October 2017, <https://www.nginx.com/resources/wiki/>.
8. Aanchal Malhotra, Isaac E. Cohen, Erik Brakke, and Sharon Goldberg. (October 2015). *Boston University*. "Attacking the NTP." Last accessed on 2 October 2017, <http://www.cs.bu.edu/~goldbe/papers/NTPattack.pdf>.
9. Dan Goodin. (21 October 2015). *ArsTechnica*. "New Attacks on NTP Can Defeat HTTPS and Create Chaos." Last accessed on 2 October 2017, <http://arstechnica.com/security/2015/10/new-attacks-on-network-time-protocol-can-defeat-https-andcreate-chaos/>.
10. Wikimedia Foundation Inc. (31 August 2016). *Wikipedia*. "UPnP." Last accessed on 2 October 2017, https://en.wikipedia.org/wiki/Universal_Plug_and_Play.
11. Microsoft. (28 March 2003). *Microsoft TechNet*. "What Is SNMP?" Last accessed on 2 October 2017, <https://technet.microsoft.com/en-us/library/cc776379%28v=ws.10%29.aspx>.
12. John McCormick. (11 April 2001). *TechRepublic*. "Lock IT Down: Don't Allow SNMP to Compromise Network Security." Last accessed on 2 October 2017, <http://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-networksecurity/>.
13. Kelly Jackson Higgins. (22 May 2014). *Dark Reading*. "SNMP DDoS Attacks Spike." Last accessed on 2 October 2017, <http://www.darkreading.com/attacks-breaches/snmp-ddos-attacks-spike/d/d-id/1269149>.
14. Wikimedia Foundation Inc. (29 September 2016). *Wikipedia*. "SSH." Last accessed on 2 October 2017, https://en.wikipedia.org/wiki/Secure_Shell.
15. Wikimedia Foundation Inc. (8 September 2016). *Wikipedia*. "RDP." Last accessed on 2 October 2017, https://en.wikipedia.org/wiki/Remote_Desktop_Protocol.

16. 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 2 October 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/>.
17. Wikimedia Foundation Inc. (19 September 2016). *Wikipedia*. "Telnet." Last accessed on 2 October 2017, <https://en.wikipedia.org/wiki/Telnet>.
18. Wikimedia Foundation Inc. (19 September 2016). *Wikipedia*. "FTP." Last accessed on 2 October 2017, https://en.wikipedia.org/wiki/File_Transfer_Protocol.
19. Trend Micro Inc. "EU General Data Protection: Time to Act." Last accessed on 11 October 2017, <http://www.trendmicro.co.uk/enterprise/data-protection/eu-regulation/>.
20. Trend Micro Inc. *Trend Micro Security News*. "A Practical Introduction to the European General Data Protection Regulation for SMBs" Last accessed on 11 October 2017, <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/a-practical-introduction-to-the-european-general-data-protection-regulation-for-smb>s.
21. CIS. (2016). *CIS*. "CIS Controls for Effective Cyberdefense." Last accessed on 7 January 2017, <https://www.cisecurity.org/critical-controls/>.
22. TrendLabs. (3 November 2016). *Trend Micro Security News*. "Securing Smart Homes." Last accessed on 5 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-smart-homes>.
23. 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 11 October 2017, http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter2.html.
24. Jeff Tyson. (2 February 2001). *HowStuffWorks.com*. "How Network Address Translation Works." Last accessed on 11 October 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