

French Cities Exposed

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

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: France

11

Exposed Cyber Assets
in France

31

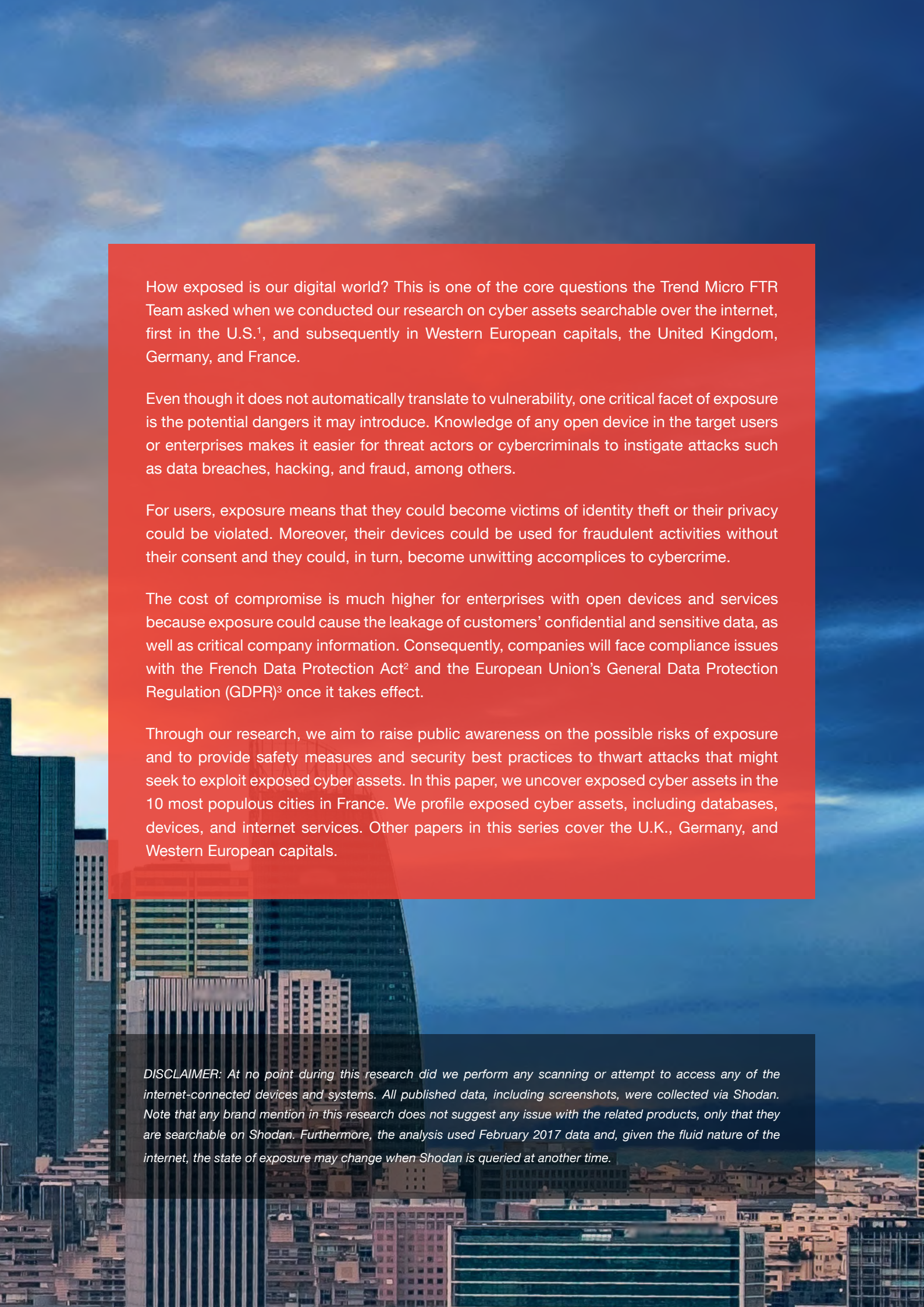
Safeguarding Against
Internet Exposure

36

Conclusion

37

Appendix



How exposed is our digital world? This is one of the core questions the Trend Micro FTR Team asked when we conducted our research on cyber assets searchable over the internet, first in the U.S.¹, and subsequently in Western European capitals, the United Kingdom, Germany, and France.

Even though it does not automatically translate to vulnerability, one critical facet of exposure is the potential dangers it may introduce. Knowledge of any open device in the target users or enterprises makes it easier for threat actors or cybercriminals to instigate attacks such as data breaches, hacking, and fraud, among others.

For users, exposure means that they could become victims of identity theft or their privacy could be violated. Moreover, their devices could be used for fraudulent activities without their consent and they could, in turn, become unwitting accomplices to cybercrime.

The cost of compromise is much higher for enterprises with open devices and services because exposure could cause the leakage of customers' confidential and sensitive data, as well as critical company information. Consequently, companies will face compliance issues with the French Data Protection Act² and the European Union's General Data Protection Regulation (GDPR)³ once it takes effect.

Through our research, we aim to raise public awareness on the possible risks of exposure and to provide safety measures and security best practices to thwart attacks that might seek to exploit exposed cyber assets. In this paper, we uncover exposed cyber assets in the 10 most populous cities in France. We profile exposed cyber assets, including databases, devices, and internet services. Other papers in this series cover the U.K., Germany, and Western European capitals.

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 admin 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: France

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

We examined the Shodan scan data for France for February 2017, excluding data belonging to known hosting providers since hosting infrastructure is complex and difficult to map or accurately port to back-end applications. The filtered data set contains a total of 7,029,627 records generated from scanning 2,177,319 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. The list of hosting providers whose IP addresses were excluded can be found in the Appendix.

This section provides a general overview of cyber asset exposure in the top 10 cities in France by population, as well as discusses numbers on exposed devices, systems, products, OSs, and other assets that are visible in the Shodan scan data.

Cyber Asset Exposure in France

Of the 10 cities with the highest populations in France, Paris had the most number of exposed cyber assets (around 400,000). Aside from being the capital and the most populous city in France, Paris has a growing technology industry, especially with the emergence of startups.⁴ It's also one of the business and economic hubs in the country. The majority of internet service providers (ISPs) and hosting providers operate out of Paris and Marseille.

Lyon and Toulouse had exposed cyber assets at around 26,000 and 17,000, respectively. Being industrial centers could have contributed to their being at the top of the list.

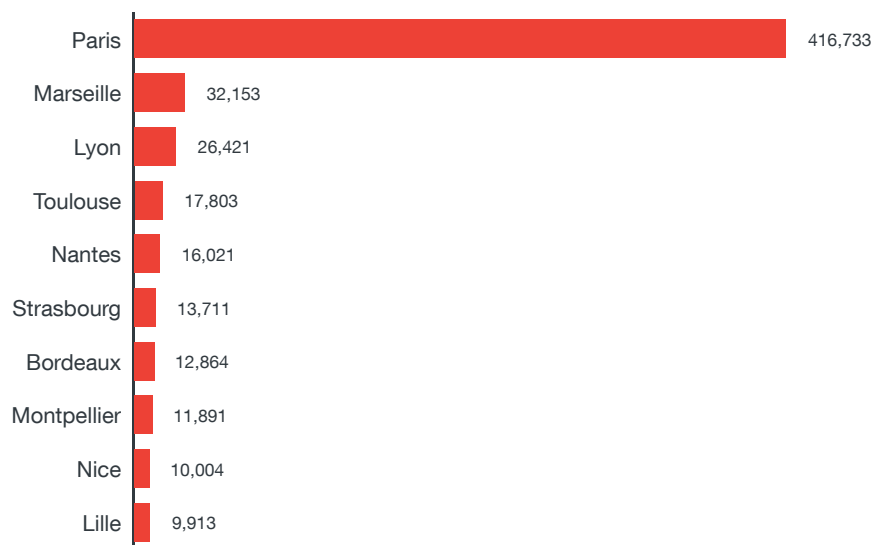


Figure 1. Number of exposed cyber assets in the top 10 French cities by population

City	Population
Paris	2,220,445
Marseille	852,516
Lyon	496,343
Toulouse	453,317
Nice	343,629
Nantes	291,604
Strasbourg	274,394
Montpellier	268,456
Bordeaux	241,287
Lille	228,652

Table 1. Top 10 French cities by population⁵

How Exposed Devices Access the Internet

A majority of open devices in France connect to the internet via Ethernet or modems. This is similar to our findings for Western European capitals and U.K. cities. Interestingly, exposed cyber assets also access the internet through Serial Line Internet Protocol (SLIP), an internet protocol used for modem connections.

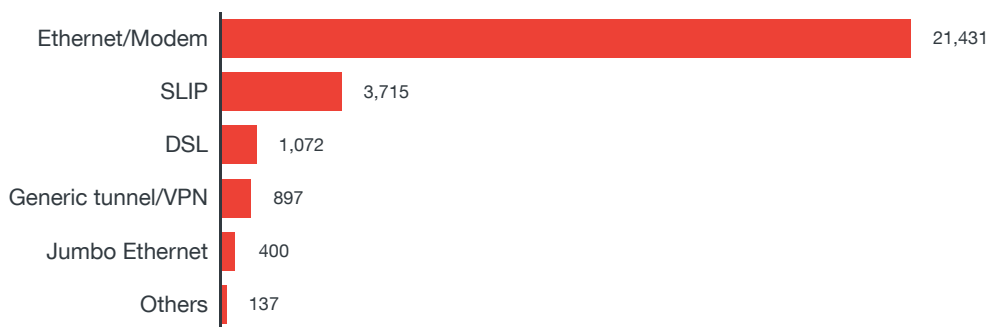


Figure 2. Means by which exposed devices access the internet

OSs Running on Exposed Internet-connected Devices

Linux® systems accounted for more than half of the OSs running on exposed devices. This can be attributed to Apache servers, NGINX, and Internet of Things (IoT) devices that are searchable in Shodan. Moreover, around 30 percent of exposed devices on Linux were open webcams, and storage devices accounted for around the same percentage. There were also exposed devices running Microsoft® Windows® and Apple® iOS. If an exposed device's information such as OS installed is exposed, it runs the risk of attackers using vulnerabilities and exploits specifically targeting that platform to gain entry to the system or network.

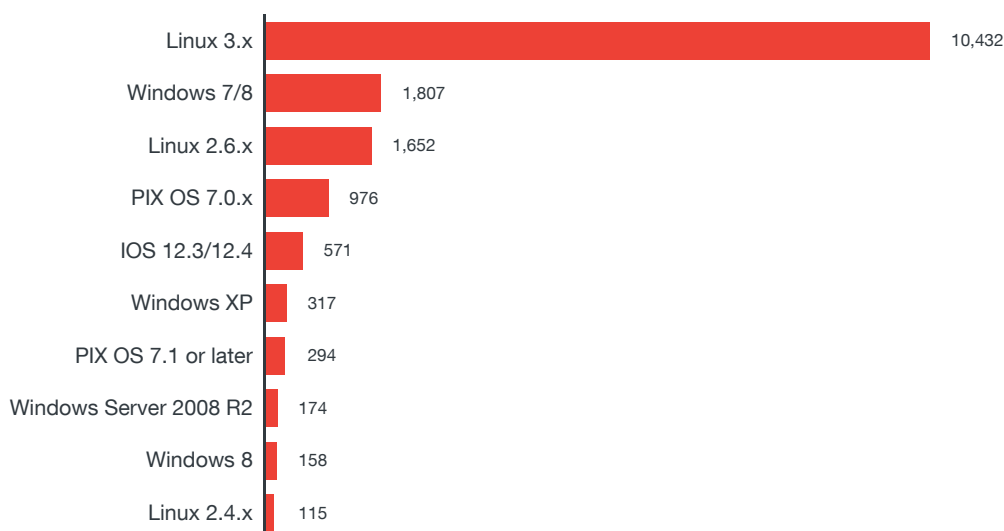


Figure 3. OSs that run on exposed devices (top 10)

Top Exposed and Vulnerable Products

Web and email servers, Secure Shell (SSH) devices, and FTP servers dominated the list of searchable products over the internet. From this result, we can surmise that Apache servers are widely used in France. It is interesting to note that M5T SIP stacks were included in the scan data, which means that there were Voice over Internet Protocol (VoIP) phones left exposed.

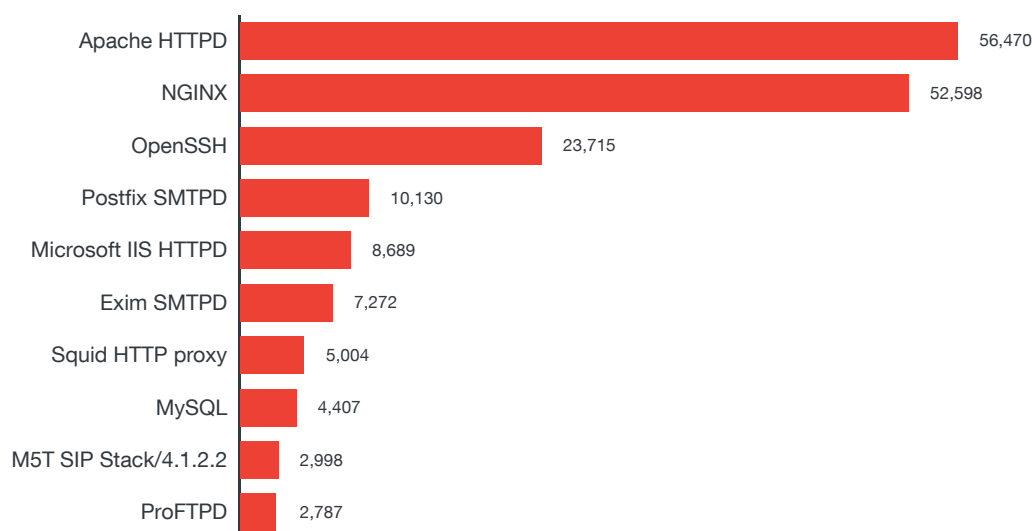


Figure 4. Number of exposed cyber assets by product/service name (top 10)

To determine if certain exposed products are vulnerable, the Shodan crawler tests vulnerabilities such as CVE-2014-0160 (also known as Heartbleed⁶), CVE-2015-0204⁷ (Freak, an OpenSSL vulnerability), CVE-2013-1899⁸ (an argument injection vulnerability in PostgreSQL), CVE-2016-9244⁹ (Ticketbleed, Transport Layer Security [TLS]/Secure Sockets Layer [SSL] stack in BIG-IP virtual servers), CVE-2013-1391¹⁰ (digital video recorder [DVR] configuration disclosure), and CVE-2015-2080¹¹ (also known as JetLeak).

Based on our scan data, we identified products with vulnerabilities which had the most number of exposed cyber assets. These were Apache, NGINX, and Microsoft Internet Information Service (IIS) Hypertext Transfer Protocol daemon (HTTPD) web servers, followed by Exim and Postfix email servers.

Web and email servers contain confidential and sensitive data such as intellectual property rights, customer information, personal identifiable information (PII), and trade secrets. Servers, especially those we identified as most exposed and vulnerable, should be secured as soon as possible to prevent attackers from exploiting vulnerabilities, gaining entry to the enterprise environment, and stealing critical data.

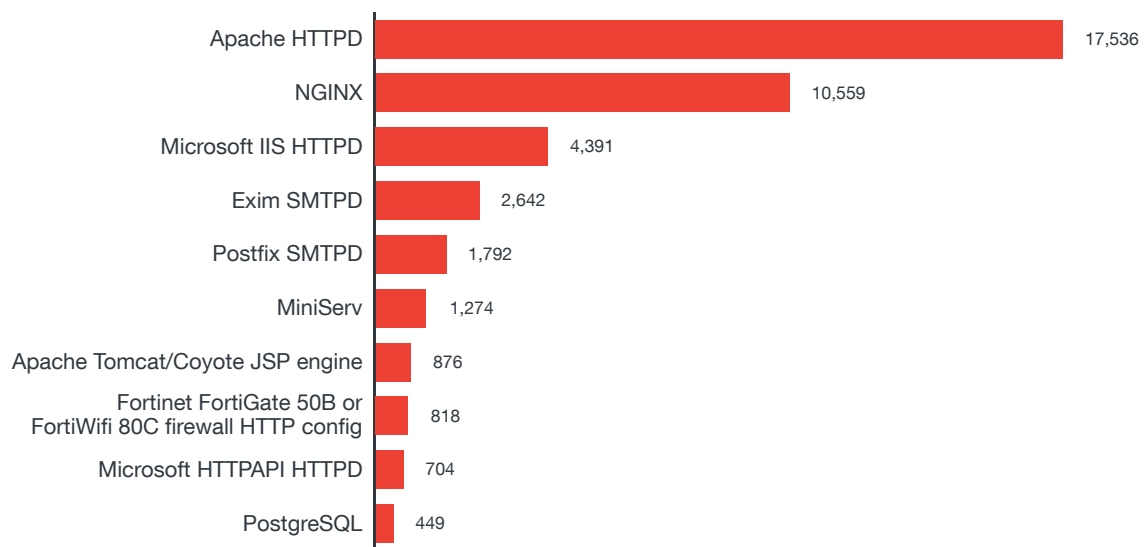


Figure 5. Number of exposed cyber assets by product/service name vulnerable to CVE-2013-1391, CVE-2013-1899, CVE-2014-0160, CVE-2015-0204, CVE-2015-2080, or CVE-2016-9244 (top 10)

Top Exposed and Vulnerable Device Types

Webcams ranked first as the most exposed device type. This could be attributed to the numerous network services enabled by default like Simple Mail Transfer Protocol (SMTP), FTP, and Universal Plug and Play (UPnP), which can be abused to launch attacks such as DDoS. With users normally retaining the default passwords and usernames, leaving webcams exposed can make it easier for cybercriminals to perform brute-force attacks. Open webcams can pose dangers to privacy and security as they can be compromised for spying and blackmail purposes.

Firewalls also ranked high in the list. However, this is to be expected since firewalls are internet-facing, with certain ports (e.g., port 80, 443, and 22) open to inbound traffic to protect web servers from threats.

Although there were only a few exposed VoIP phones, printers, and PBX systems, the fact that they are open can be worrisome. In particular, cybercriminals can leverage VoIP phones to instigate fraudulent activities like vishing (voice phishing) and telephony denial-of-service (TDoS).

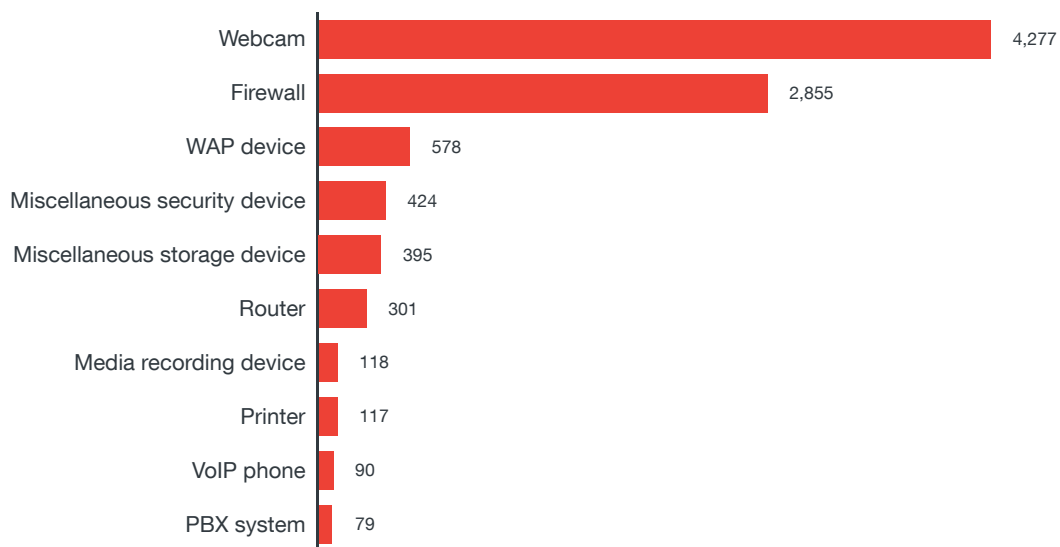


Figure 6. Number of exposed cyber assets by device type (top 10)

We tested the Shodan crawler for exposed device types with vulnerabilities, using the same vulnerabilities tested for exposed products (i.e., CVE-2014-0160, CVE-2015-0204, CVE-2013-1899, CVE-2016-9244, CVE-2013-1391, and CVE-2015-2080). We found that there were more open vulnerable firewalls than webcams. When the security of firewalls is compromised, attackers can lower the restrictions to further their attacks.

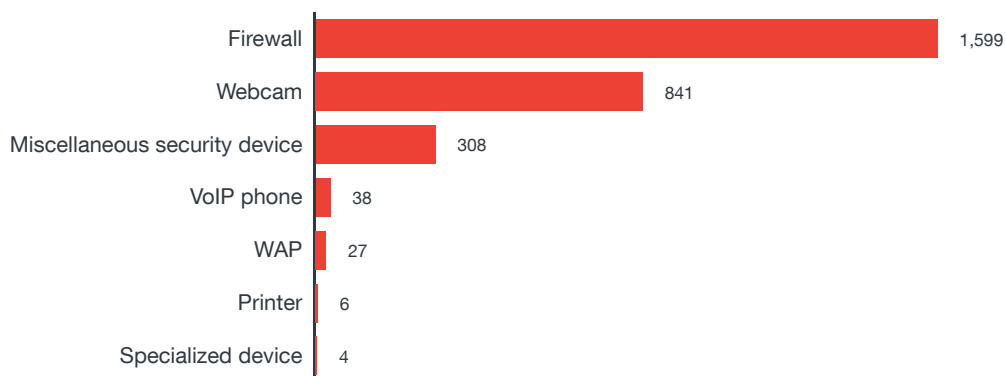


Figure 7. Number of exposed cyber assets by device type vulnerable to CVE-2013-1391, CVE-2013-1899, CVE-2014-0160, CVE-2015-0204, CVE-2015-2080, or CVE-2016-9244

Exposed Cyber Assets in France

Exposed Devices

We took a more in-depth look at the most exposed devices in the February 2017 Shodan scan data and present the results in this section for the top 10 French cities based on population. Our findings revealed that most of the cities in France covered by this study have visible webcams and storage devices. This could be due to the extensive use of these devices in offices, homes, and public spaces. The results are somehow different from U.K. cities, where routers and webcams topped the list.

Searchable devices over the internet could increase the risk of data theft, privacy breaches, and use by a botnet for DDoS attacks. Another real danger is when cybercriminals use exposed devices without the owners knowing it for fraudulent activities, thus making the owners unwitting accomplices to cybercrime. Companies whose systems and servers are used for cybercrime to target other enterprises might be held accountable for such incidents.

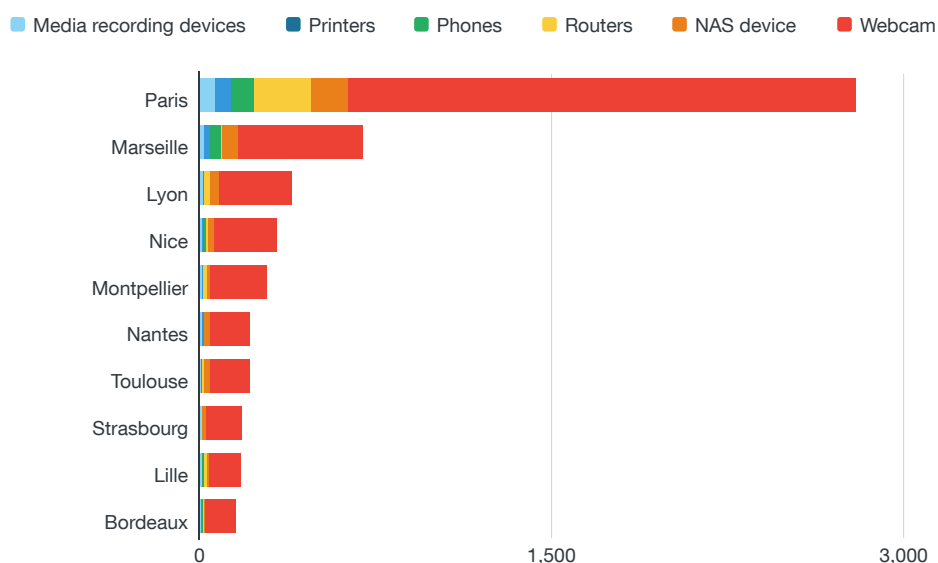


Figure 8. Overview of top exposed devices by city

Exposed Webcams

Paris had the most number of exposed webcams, followed by Marseille and Lyon. The numbers may be due to exposed HTTP service in webcam products, which is open to enable the remote viewing of photos. This convenient feature may, however, make owners of exposed cameras vulnerable to attacks.

What makes webcams a viable target? Aside from being used for surveillance and reconnaissance, the lack of an auto-update feature makes webcams easier for cybercriminals to exploit, especially since they are rarely patched. In addition to that, users might be using weak passwords or worse, continue to use default passwords. This makes webcams susceptible to brute-force attacks. Firmware vulnerabilities existing in webcams can also be abused to compromise security.

The privacy of users and companies suffer when cybercriminals compromise webcams. In one particular incident, footage from webcams, baby monitors, and closed-circuit television (CCTV) cameras were posted on a Russian website. Reports¹² cited that 2,000 webcams in France were affected.

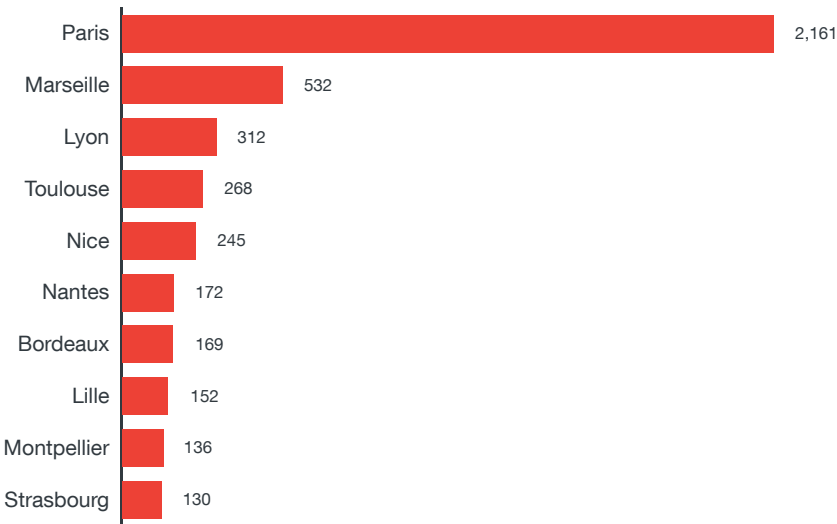


Figure 9. Number of exposed webcams by city

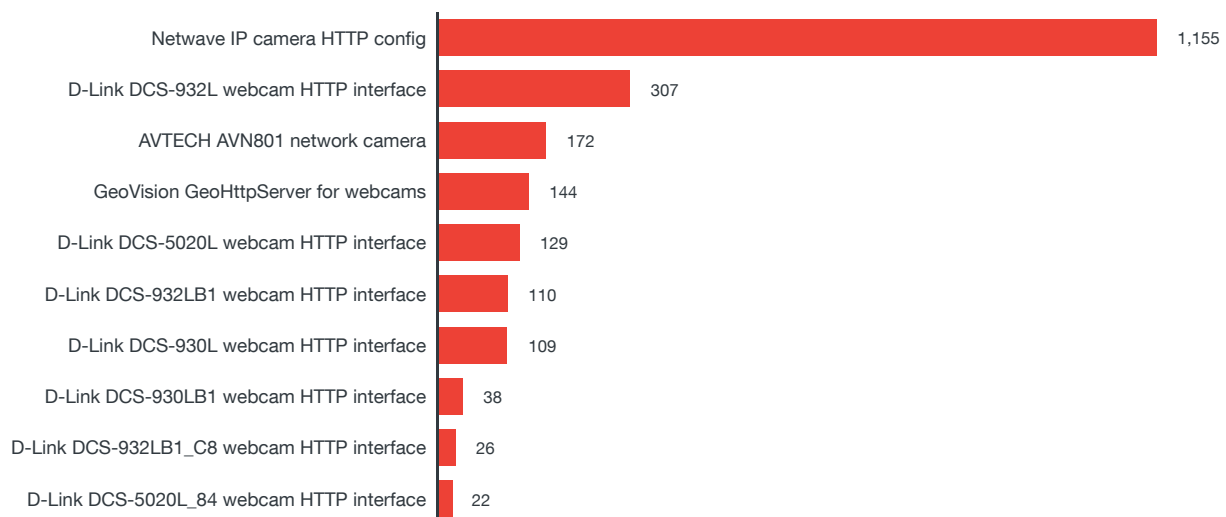


Figure 10. Number of exposed webcams by product/service name

Exposed NAS Devices

Network-attached storage (NAS) devices are one to two hard drives placed in a box with network cables attached and services on top. They store a wide array of sensitive and critical information and files that can be accessed by employees. It is the second most exposed device next to webcams. The bulk of open NAS devices were found in Paris, followed by Marseille and Lyon. The Seagate GoFlex NAS device solid state hybrid drive (SSHD) dominated the list of exposed products.

NAS devices are also attractive targets for cybercriminals because most of the time the passwords remain unchanged, which means that attackers could compromise a device and obtain confidential information.

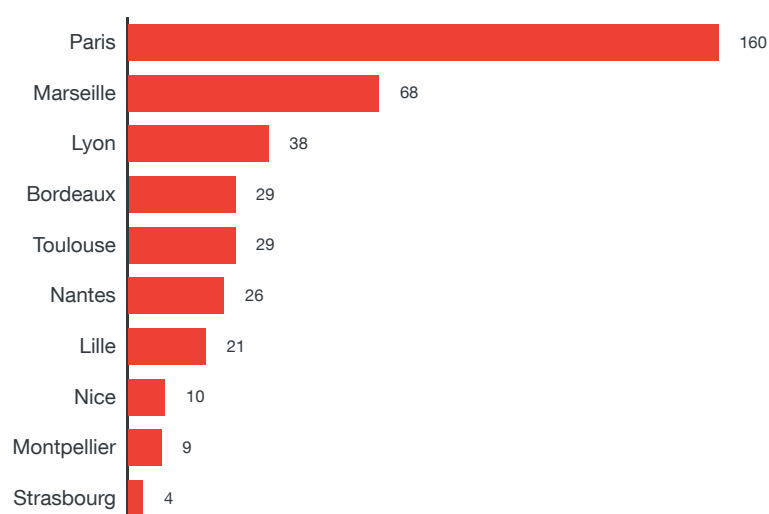


Figure 11. Number of exposed NAS devices by city

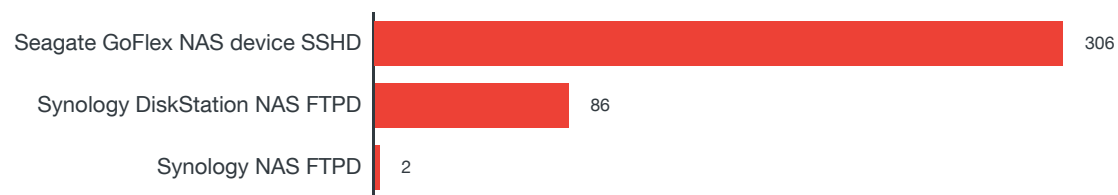


Figure 12. Number of exposed NAS devices by product/service name

Exposed Routers

Paris again led in the number of exposed routers, with a total of 241 – a long way from the next city, Lyon, which had 25.

Prior to the rise of IoT botnets like Mirai¹³, router security went unnoticed. However, attackers found a way to infiltrate a home or enterprise network by way of hacking a router. With all types of information from devices passing through some form of router, this device type is a lucrative target for cybercriminals. Stolen data can be peddled in underground markets; users accessing certain sites can also be redirected to malicious websites.

Predefined credentials and router configurations make routers prone to attacks and threats. Security flaws existing in the router's OS, firmware, and web applications also serve as entry points.

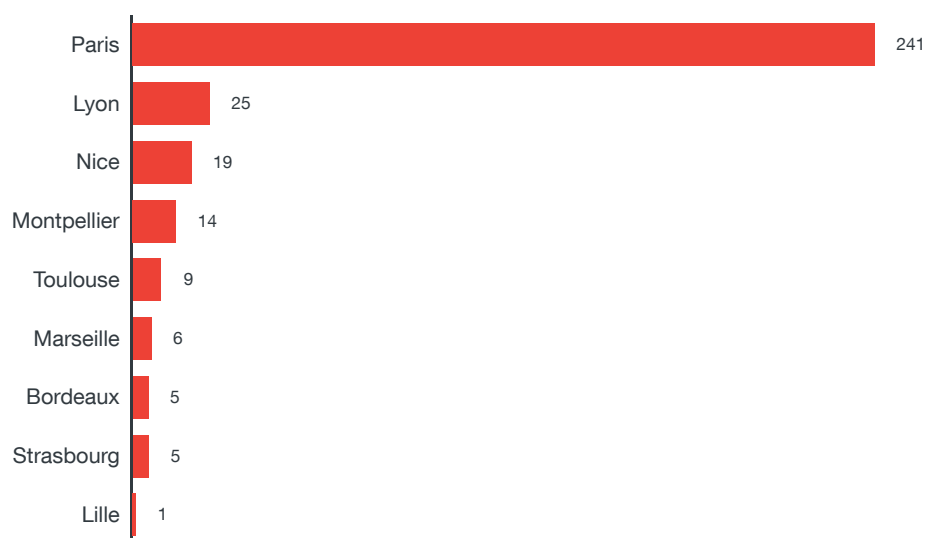


Figure 13. Number of exposed routers by city

Another risk that users and enterprises face is their own device being used for cybercriminal activity without their knowledge. Unsecured routers could be modified to become a part of a botnet to launch DDoS attacks like in the case of Mirai. The said botnet took down several notable sites, including Twitter and investigative reporter Brian Krebs' website.

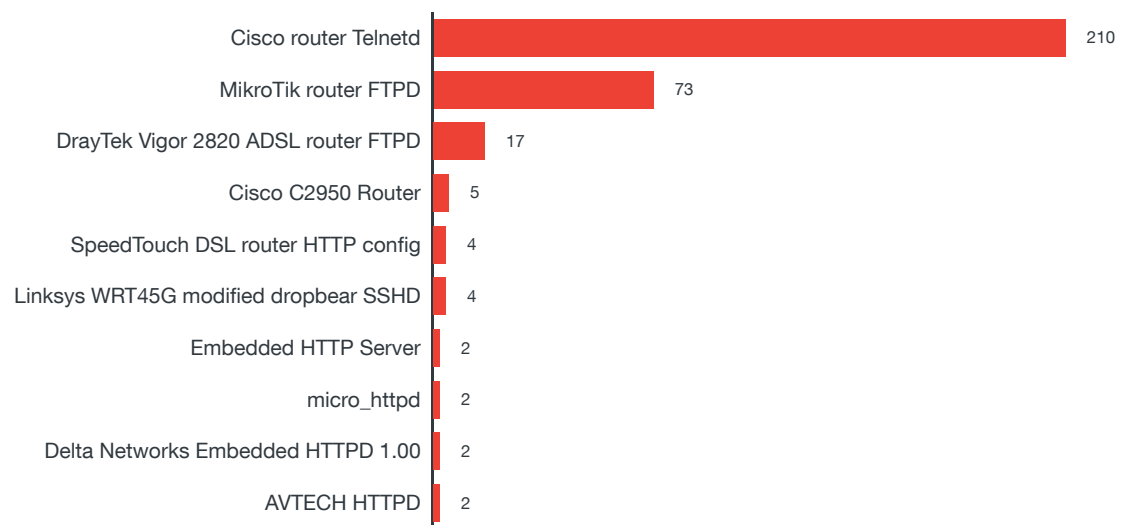


Figure 14. Number of exposed routers by product/service name

Most routers have a firewall feature which, when enabled, adds a layer of protection against threats. Modifying the device's credentials and applying patches are some security measures to keep the router and, consequently, the network protected.

Exposed Printers

Although there are fewer instances of exposed printers in Shodan compared to routers or firewalls, it is still alarming to see this device in the list of exposed cyber assets. How so? Printers contain a plethora of confidential information such as intellectual property, customer data, and PII. Users and employees print copies of documents containing sensitive data, such as tax and employment forms, bank statements, and emails, among others. Printers can store cached copies of these documents and exposure could leave sensitive data unprotected from cybercriminals.

Compromised printers could also be used for lateral movement within a network. Several services in printers may be employed in attacks like Simple Service Discovery Protocol (SSDP) (for reflective DDoS attacks), SMTP (for sending spam and phishing emails), and plain old telephone service (POTS) calls (for vishing and telephony denial-of-service [TDoS] attacks).

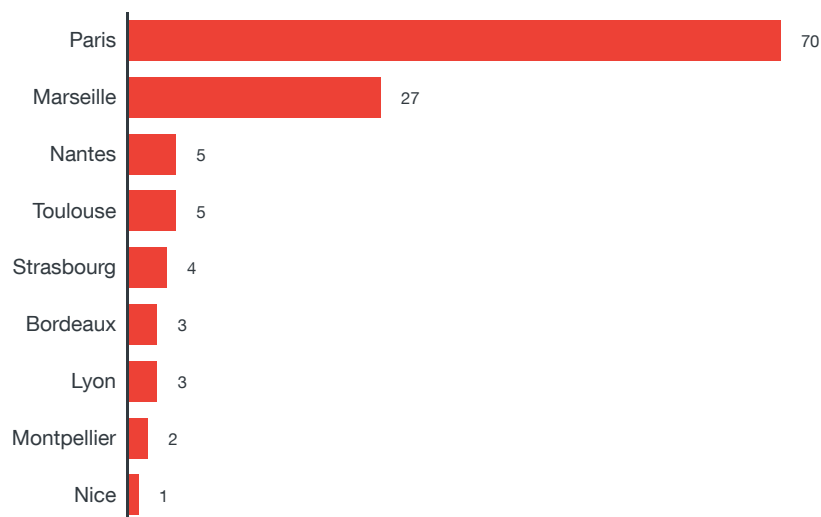


Figure 15. Number of exposed printers by city

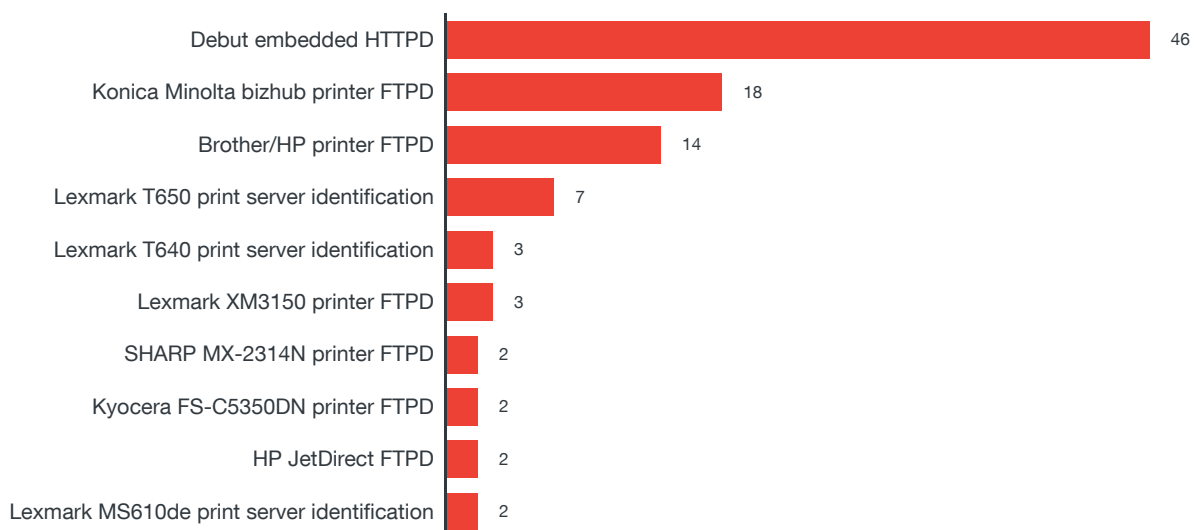


Figure 16. Number of exposed printers by product/service name

Exposed VoIP Phones

What makes VoIP phones an attractive target for threat actors? Customer information, business transactions, and other types of what can be considered as sensitive data are transmitted over VoIP lines and can then be recorded and used for attacks. Exposed VoIP phones pose risks of targeted attacks by cybercriminals.

Based on our Shodan scan results, we found that most of the exposed VoIP phones were Free Private Branch Exchange (FPBX) devices, or telephone systems in enterprises that allow employees to have a common external line. It was followed by Polycom SoundPoint VoIP phone http config.

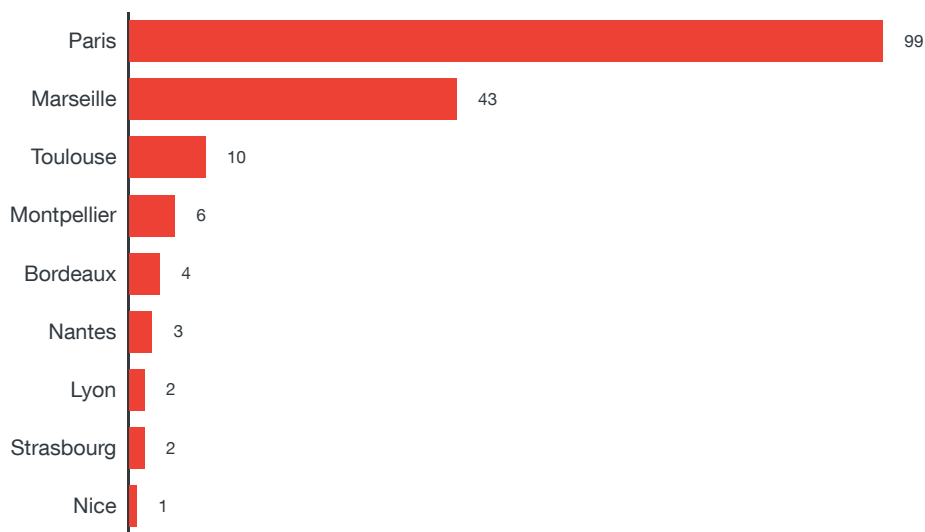


Figure 17. Number of exposed phones by city

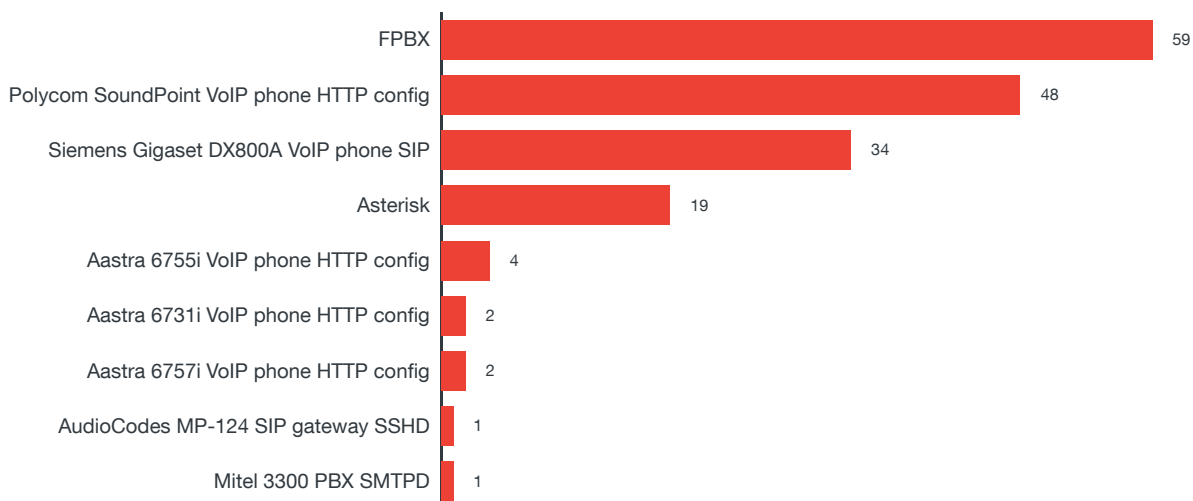


Figure 18. Number of exposed phones by product/service name

Exposed Media Recording Devices

Based on our Shodan scan results, most of the open media recording devices in France were found in Paris. This number is driven by the FTPD service in Freebox, a type of modem offering services such as Internet Protocol television (IPTV), video recording, and digital radio, among others.

While seemingly harmless, exposed media recording devices are plausible attack targets because they can be a source of intel for reconnaissance or for surveillance purposes, particularly in the case of CCTV video feeds. They can be employed as an attack vector into an enterprise environment.

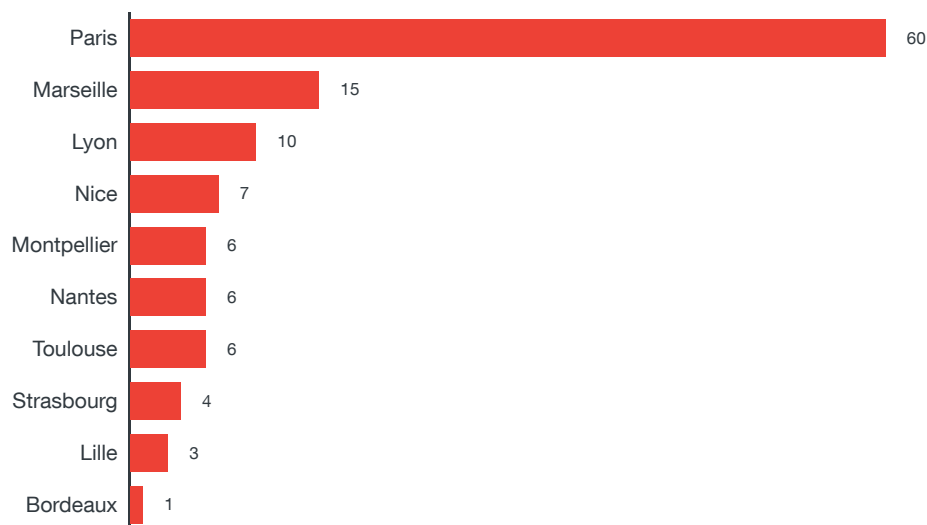


Figure 19. Number of exposed media recording devices by city

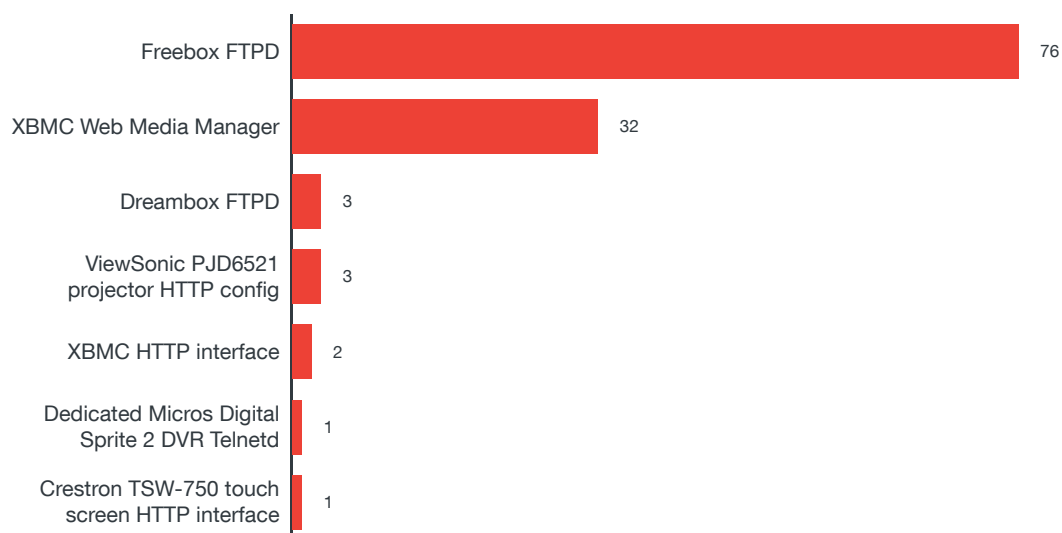


Figure 20. Number of exposed media recording devices by product/service name

Exposed Email/Web Services and Databases

Aside from looking into specific exposed device types, we also delved into exposed web and email services and databases. We discuss our findings in this section, including the risks that come with server and database exposure.

Exposed Web Services

Web services refer to system software that allows machine or device communication over a network or the web. They provide application programming interfaces (APIs), which permit apps to communicate with one another through the web or a network. They also pertain to web-based interfaces used by web servers.

In the France Shodan scan data, the bulk of exposed web services were from Paris, followed by Marseille and Lyon. The high number of web services exposed can be attributed to open web servers such as Apache, NGINX, and Microsoft IIS, which topped the list of exposed web services by product/service name. We can surmise that there is a high usage of the said web servers in the top cities in France.

What risks do exposed web services pose? Web servers also have known vulnerabilities that threat actors can exploit. Corporate networks may become susceptible to DDoS and Structured Query Language (SQL) injection attacks, data theft, unauthorized hosting of illegal data, and malware attacks.

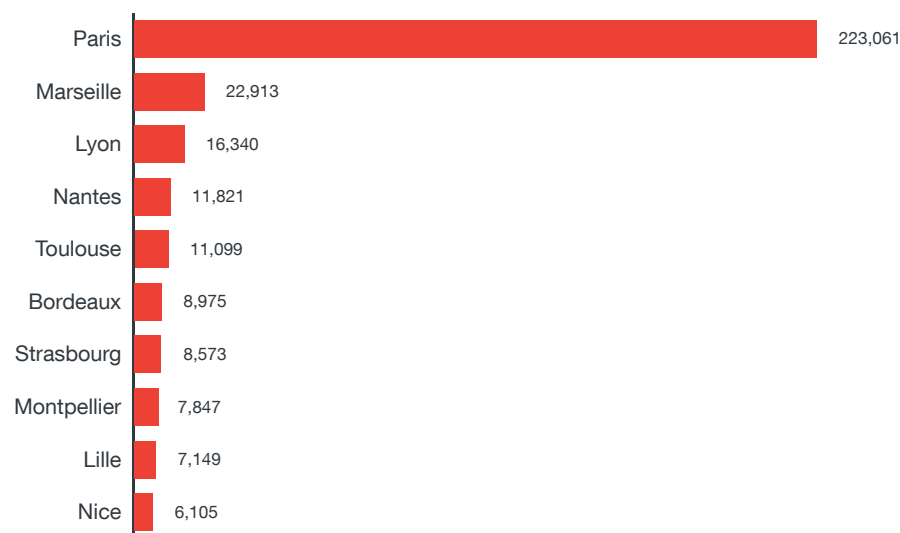


Figure 21. Number of exposed web services by city

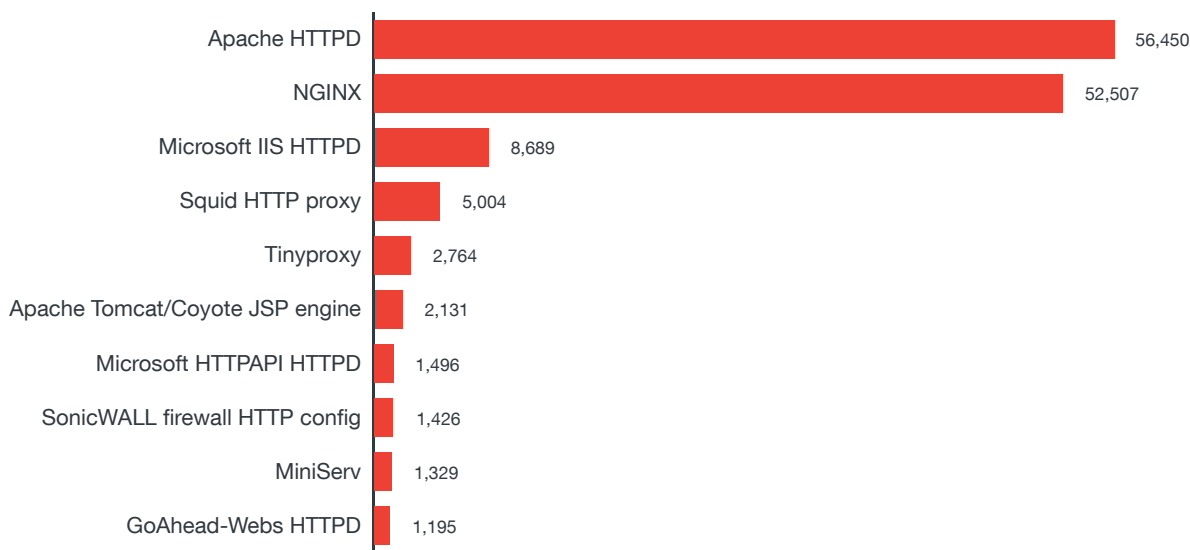


Figure 22. Number of exposed web services by product/service name

Exposed Email Services

Email remains the primary means of business communication and operations. Due to email’s critical function and the trove of information that email servers contain, threat actors find exposed email assets as viable attack targets. IT administrators should protect email servers by keeping them updated with the latest patches.

Similar to our findings for Western European capitals and the U.K. most of the exposed email services came from *nix-based servers such as Postfix and Exim.

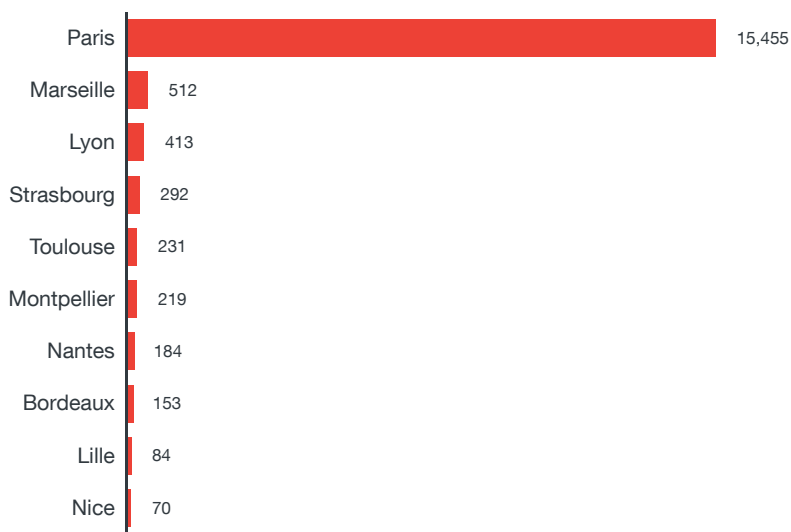


Figure 23. Number of exposed email services by city

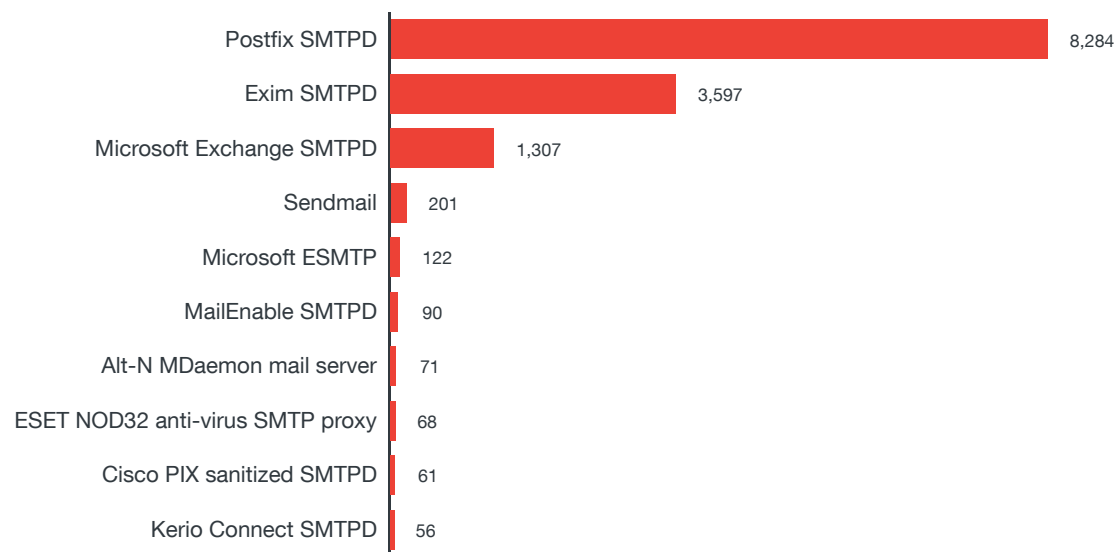


Figure 24. Number of exposed email services by product/service name

Exposed Databases

A database stores organized information classified as critical company data or “crown jewels,” such as customer PII, intellectual property, trade secrets, and the like. Targeting databases yields a higher payoff for threat actors because of the goldmine of information they can sell in the underground markets or use for other attacks.

For enterprises and large organizations, unauthorized access of their databases has serious consequences: data theft and loss, damage to brand and reputation, possible fines with the implementation of GDPR, as well as other operational costs. On the other hand, affected customers could become targets of identity theft.

An open database does not automatically mean compromise—but it could be a jumping-off point for that. This year, MongoDB databases were hit by a slew of ransom attacks¹⁴ wherein the threat actors searched for unsecured databases over the internet, deleted all files while saving their own copy in their servers, and demanded a ransom of 0.15 bitcoins (US\$560.70 as of September 17, 2017). There were nearly 76,000 victims, with hackers reportedly earning over 24 bitcoins¹⁵ (US\$89,712 as of September 17, 2017). Security researchers noted that the affected databases were still using default log-ins.

While there were only a few instances of MongoDB in Shodan scans in our study of exposed databases in France, the security incidents highlight the risks of leaving databases open and unprotected over the internet.

In addition, attackers can use knowledge of a database’s security flaws and vulnerabilities to gain access to searchable databases. For example, a big percentage of exposed databases in France were MySQL. A search in the Common Vulnerabilities and Exposures (CVE) database yielded 244 vulnerabilities affecting the said database alone. Administrators should therefore ensure that security best practices are applied for their enterprises’ critical databases.

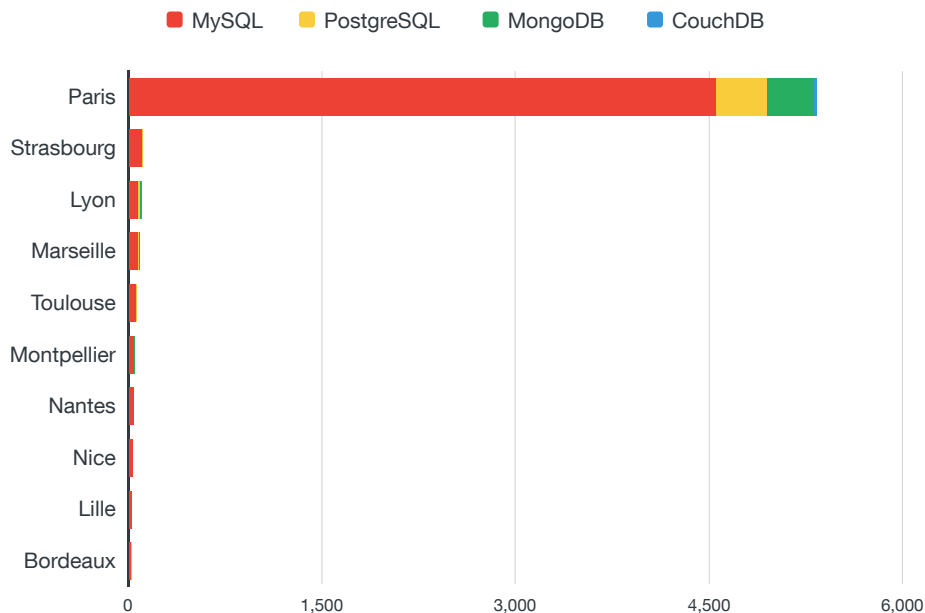


Figure 25. Overview of exposed databases by city

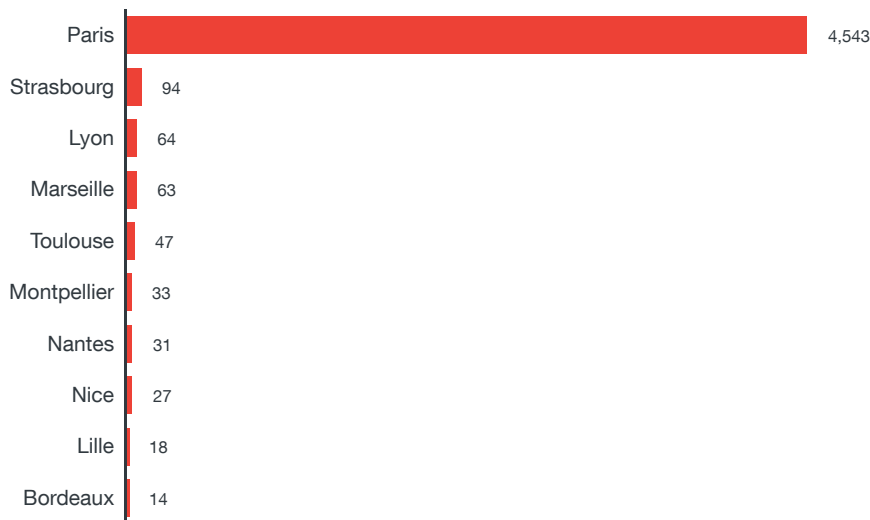


Figure 26. Number of exposed MySQL databases by city



Figure 27. Number of exposed PostgreSQL databases by city



Figure 28. Number of exposed MongoDB databases by city



Figure 29. Number of exposed CouchDB databases by city

Exposed Service Protocols

A variety of cyber assets run a variety of service protocols, each having its own exploitable vulnerability. We analyzed the exposed cyber assets in France based on service protocols such as Network Time Protocol (NTP), UPnP/SSDP, Simple Network Management Protocol (SNMP), SSH, Remote Desktop Protocol (RDP), Telnet, and FTP. It is important to explore exposure in terms of service protocols since security vulnerabilities found in these protocols can be exploited to breach the security of devices that run them.

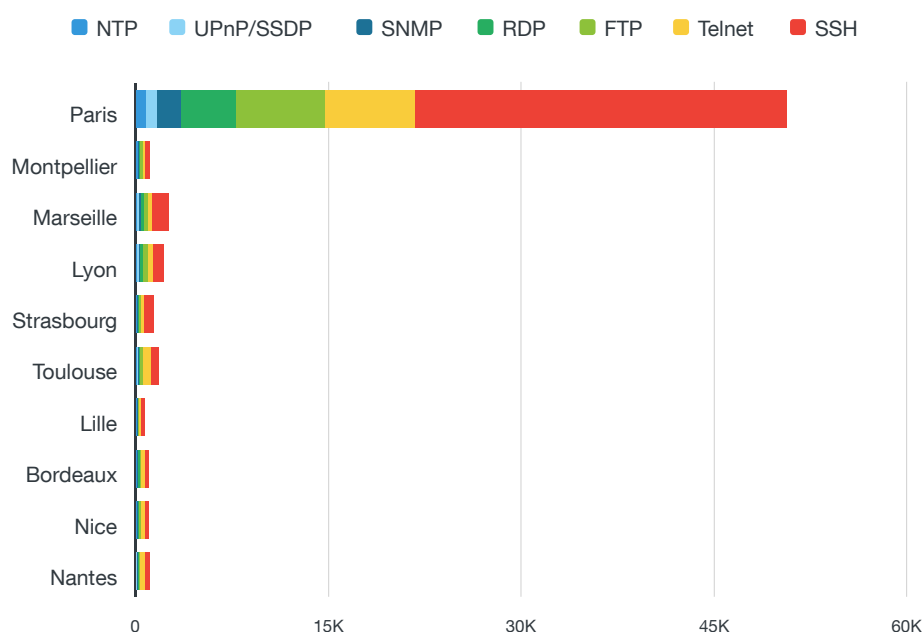


Figure 30. Overview of exposed service protocols by city

Exposed NTP-enabled Devices

NTP is one of the oldest internet protocols in use. It plays a critical function in time synchronization of system clocks connected to a network. Accurate timestamping is required for a number of system tasks such as running scheduled backups, intrusion analysis, or tracing back system logs and events to know how a network was breached. In some cases, compliance regulations like HIPAA¹⁶ need timestamps for data and other transactions.

In our analysis, Paris had the most number of open devices using NTP, followed by, but by a large margin, Montpellier and Marseille.

Exposed NTP-enabled devices pose the risk of attackers exploiting security bugs to launch a DDoS attack via the NTP reflection technique¹⁷ or a man-in-the-middle (MitM) attack.

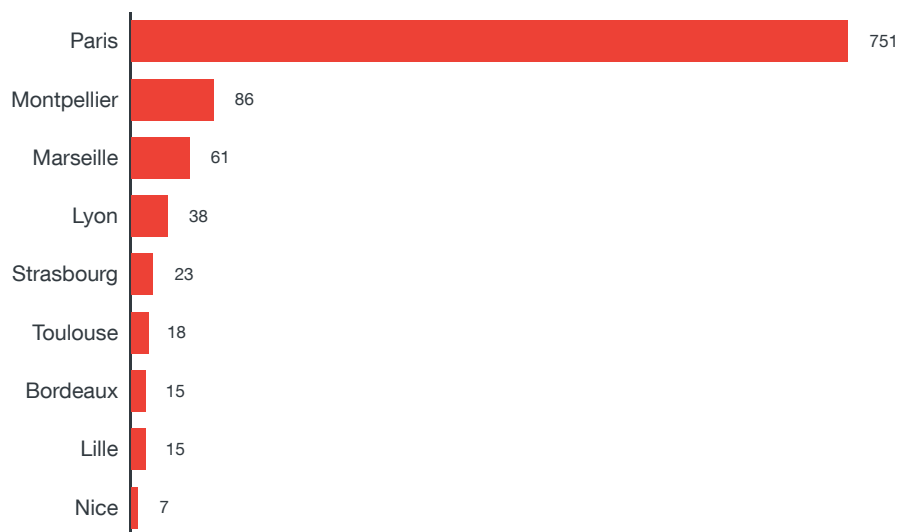


Figure 31. Number of exposed NTP-enabled devices by capital

Exposed UPnP-/SSDP-enabled Devices

Networked devices such as routers, printers, mobile devices, and computers can easily discover each other and perform functions like communication and data sharing through UPnP. Connections are made using the Dynamic Host Configuration Protocol (DHCP) networking protocol,¹⁸ which gives a unique IP address to each device. SSDP, on the other hand, is used to see other UPnP devices, typically in small office environments. There are only a few instances of exposed devices (particularly, Intel® Software for UPnP Technology) that use UPnP/SSDP.

Security bugs found in this protocol can be abused to infiltrate a network. A quick search of CVE yielded at least 58 entries¹⁹ that either directly or indirectly affected UPnP and 17 entries²⁰ for SSDP.

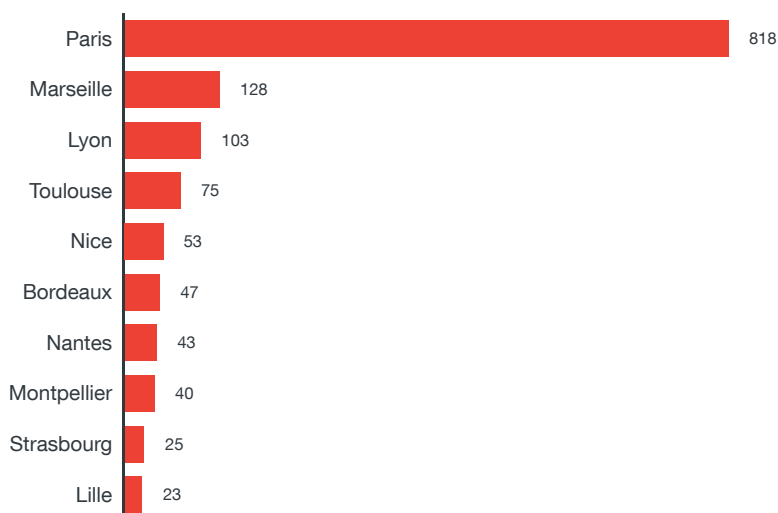


Figure 32. Number of exposed UPnP-/SSDP-enabled devices by city

Exposed SNMP-enabled Devices

IT administrators use SNMP to monitor and map all of the devices connected to a network. This gives them accurate details about the network topology and infrastructure. Attackers leverage this protocol in order to know their target enterprise’s environment during reconnaissance and lateral movement.

In the data for Western European capitals, 90 percent of exposed SNMP-enabled devices were linked to Cisco routers. For France, only six were visible as Cisco routers.

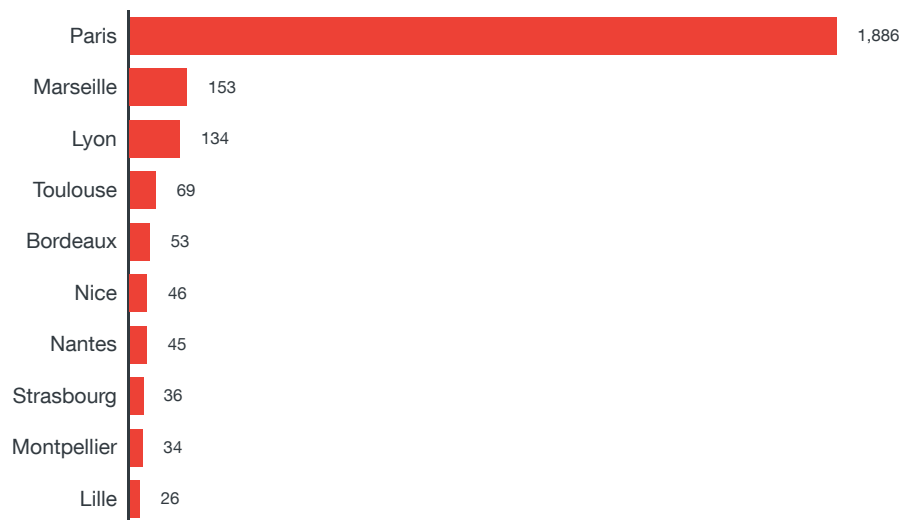


Figure 33. Number of exposed SNMP-enabled devices by city

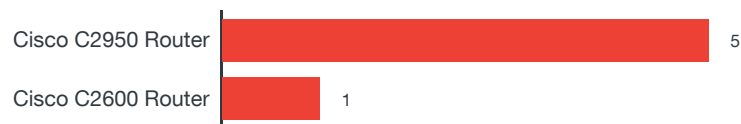


Figure 34. Number of exposed SNMP-enabled devices by product/service name

Exposed SSH-enabled Devices

SSH allows a wide variety of devices to be remotely accessed in a secure manner. It was supposedly developed as an alternative to less secure protocols like Telnet. Why do threat actors attack this port? For one thing, it gives them access to devices connected to their target device. For another, once the target device is compromised, attackers can simply open and close necessary ports to perform attacks against other devices. Connected devices are instrumental to threat actors looking to exploit open SSH ports because they rarely have strong security.

A high number of exposed devices using SSH were concentrated in Paris, and most were storage and security devices. This is somehow different from the U.K. data, where majority were routers, firewalls, and NAS devices.

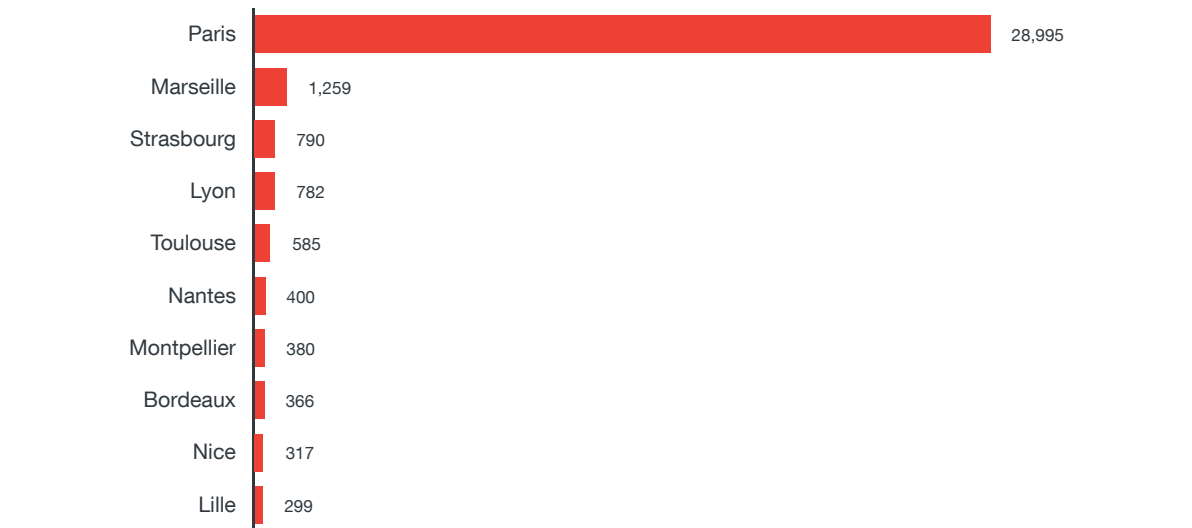


Figure 35. Number of exposed SSH-enabled devices by city

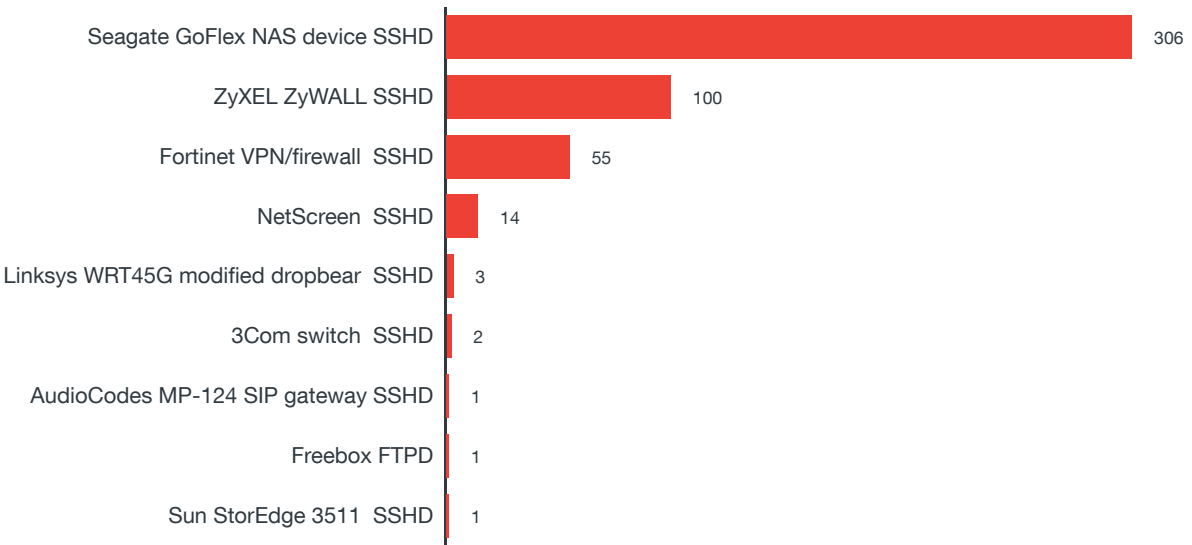


Figure 36. Number of exposed SSH-enabled devices by product/service name

Exposed RDP-enabled Devices

RDP is a protocol developed by Microsoft to connect to a system in a network. Exploiting RDP is not uncommon among cyberattacks as it can be used in data exfiltration (in targeted attacks) or sharing malicious files with systems over a network. An example of such an attack was used by the Crysis ransomware²¹, which performed a brute-force RDP attack to transfer the malware from a remote system to a victim’s computer. Another security incident involved the point-of-sale (PoS) malware Backoff²², which abused remote desktop applications such as RDP to infiltrate target companies.

Paris ranked first again in this area, having exposed devices running RDP in the thousands. Lyon and Marseille followed at second and third, respectively, although their numbers were only in the hundreds.

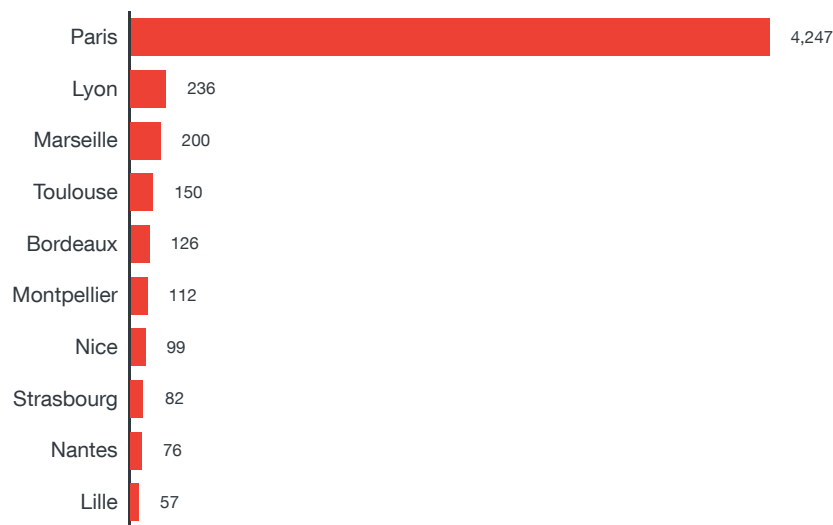


Figure 37. Number of exposed RDP-enabled devices by city

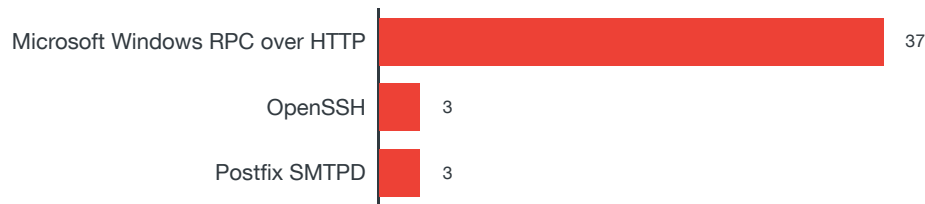


Figure 38. Number of exposed RDP-enabled devices by product/service name

Exposed Telnet-enabled Devices

Telnet is a network protocol whose main function is to connect remote systems over a TCP/IP network. Just like SSH, it is used for device-to-device communication, but it sends data in an unencrypted manner (plain text) and, thus, is susceptible to network packet sniffing attacks. Threat actors can attack Telnet to intercept user credentials and compromise devices.

Our findings revealed that most exposed Telnet devices, such as Cisco routers, were from Paris.

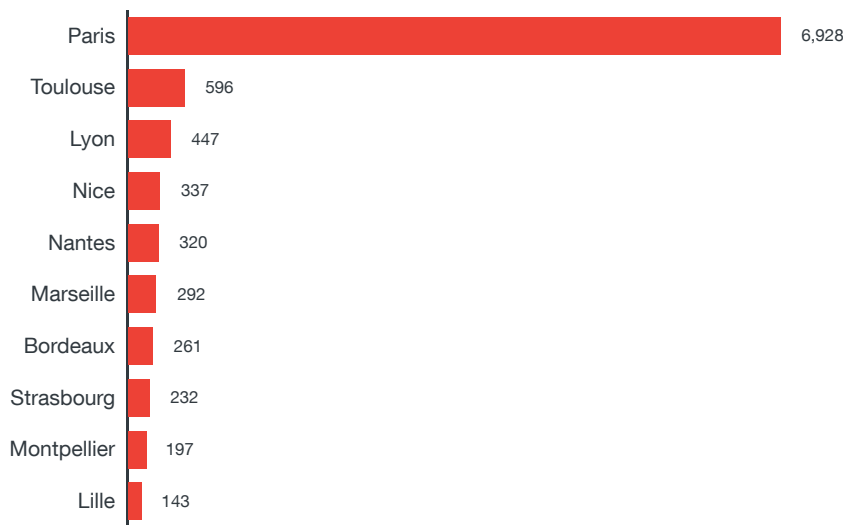


Figure 39. Number of exposed Telnet-enabled devices by city



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

Exposed FTP-enabled Devices

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

Based on Shodan scans, most exposed devices that use FTP were located in Paris, and mostly consisted of storage devices and routers.

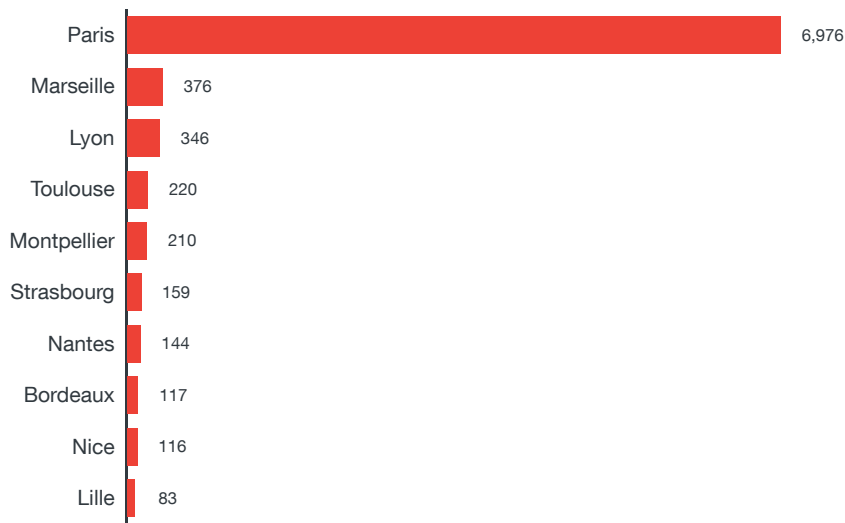


Figure 41. Number of exposed FTP-enabled devices by city

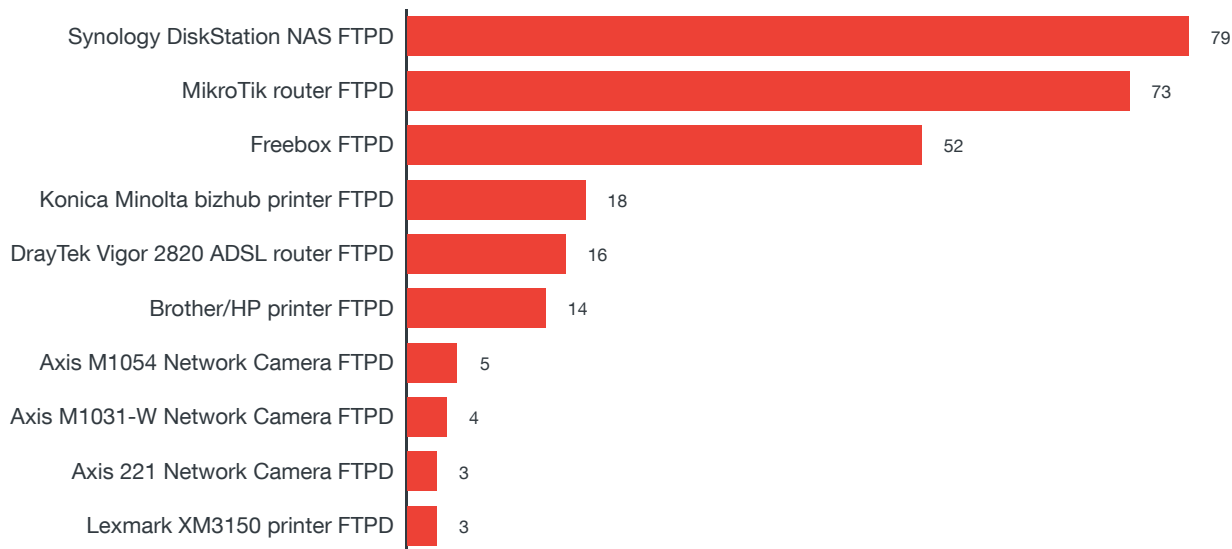


Figure 42. Number of exposed FTP-enabled devices by product/service name

Safeguarding Against Internet Exposure

For Enterprises

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

The French Digital Republic Bill²³ enacted in 2016 allows the French Data Protection Authority (CNIL) to impose fines of up to €3 million (US\$3,583,470 as of September 18, 2017) for violators of the French Data Protection Act until the GDPR takes effect. The said data protection law from 1978 highlighted confidentiality and security in the processing of personal data by government and private sectors. The Directive 95/46/EC, GDPR's predecessor which promotes the right to privacy of citizens regarding the processing of their information, was also influenced by this law.

The current data protection law in France is aligned with the GDPR, which will take effect on May 2018. GDPR requires compliance among businesses regardless of size and industry. GDPR puts a premium on protecting the data and privacy of private citizens. It will apply to enterprises and even small and medium-sized businesses²⁴ even if they are not physically based in Europe, as long as they process the data of citizens of the European Union (EU). Where does cyber asset exposure fit into this? Exposed devices and services can leak information without the user's knowledge, subsequently leading to compliance issues that can cause businesses to possibly pay penalties of as much as 4 percent of their annual turnover.

Moreover, the EU Directive 2016/1148²⁵ aims to enhance cybersecurity in Europe by creating strategies to secure network and information systems and building computer security incident response teams (CSIRTs) that will take action during cyber incidents. This directive (to be implemented in 2018), which applies to the operators of essential services and digital service providers, can impact businesses in

France. Similar to this, the Loi de programmation militaire²⁶ (LPM) 2014-2019, which is promoted by the ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Informations or French National Security Agency), also ensures the security of critical infrastructures or “essential service operators.”

While GDPR focuses on user data, EU Directive 2016/1148 calls for better systems and network security as threats could pose serious dangers and effects on the operations/activities²⁷ of critical sectors such as utilities (specifically water provision), energy, banking or financial services, and education. Any visible and searchable device over the internet can be the starting point of a far more destructive attack on certain enterprises and organizations.

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

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

A strong security checklist includes the following:

- Securing the network infrastructure by:
 - Segmenting a network according to function, department, geographic location, level of security, or any other logical separation (taking contractors, third-party vendors, and others into account).
 - Implementing log analysis for threat detection and remediation and building threat intelligence; the data can be fed into Security Information and Event Management (SIEM) software to help a response team understand ongoing attacks.
 - Properly configuring user access profiles, workstations, and servers, including internet-connected devices, using the least-privilege model.
- Protecting sensitive data via:
 - Data classification by determining the sensitivity of data sets and establishing different access and processing guidelines for each category.
 - Establishing endpoint-to-cloud protection through identity-based and cloud encryption.
 - Building a data protection infrastructure with multitiered access where sensitive tiers are in a disconnected network, others require multifactor authentication, and others can remain on regular file servers.

- Building an incident response team consisting of technical, human resources, legal, and public relations personnel, and executive management.
- Building internal and collecting external threat intelligence, acted upon by knowledgeable human analysts who can determine, through identifying patterns in attacker's tools, tactics, and procedures (TTPs), if an attack is ongoing inside the network.

Ultimately, no defense is impregnable against determined adversaries. Having effective alert, containment, and mitigation processes is critical. Companies should look further into fulfilling the Critical Security Controls (CSC)²⁸ best practice guidelines published by the Center for Internet Security. The CSC goes through periodic updates to address new risks posed by an evolving threat landscape.

For Homes

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



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

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

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

- Enable password protection on your devices. This is an easy option to enable on most connected devices that support passwords. It should be mandatory for smartphones, tablets, laptops, webcams, and so on.
- Replace default with strong passwords. Users routinely do not change the factory default passwords on their devices and these can be easily discovered using any internet search engine. The other usual suspect is weak passwords that can be defeated using brute-force or dictionary attacks.
- Change default settings. Many devices have all their supported services enabled by default, many of which are not essential for regular daily use (e.g., Telnet on webcams). If possible, disable nonessential services. The only caveat is that advanced technical knowledge may be required to decide which services to disable and how to correctly do that. We do not expect the average user to be knowledgeable about this so it is up to device manufacturers to make sure their devices are secure out of the box.
- Do not jailbreak devices. This can disable built-in security features, making it easier for hackers to compromise them. Jailbreaking is popular especially with smartphones, as this allows users with phones locked to a particular service provider to make them work for all service providers or in different countries.
- Do not install apps from unverified third-party marketplaces. Only use verified app marketplaces such as Apple's App Store®, Google Play™, Amazon Appstore, and others. This is especially a big security risk for jailbroken iOS and Android™ devices. Apps installed from unverified third-party marketplaces can have backdoors built into them that criminals can use to steal personal information or, worse, take control of them. Verified app marketplaces are not immune to hosting malicious apps but the probability of that happening is small.
- Update firmware. This will fix known security vulnerabilities. On the flip side, there are many caveats with firmware updates—some device firmware are not easy to update; the latest firmware may be unstable and introduces new bugs or issues; there are too many devices to update; it is difficult to track firmware updates; users may not see the need to update the firmware when the device is functioning properly; and updating the firmware may not even be possible.

- Enable 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.
- Some router-specific best practices include enabling the firewall, using faster but shorter-range 5GHz Wi-Fi signals to limit access-point-hacking attempts, disabling Wi-Fi Protected Setup (WPS) and enabling the Wi-Fi Protected Access-2 (WPA2) security protocol, and using a strong password for Wi-Fi access.
- Other router security suggestions that unfortunately may limit device usage and functionality include configuring the router to limit device network access to set hours during the day or night, disabling UPnP though this will limit the operation of connected devices such as Wi-Fi-enabled printers, and allowing only a hardcoded list of device media access control (MAC) addresses to access a network (the MAC address list will have to be constantly updated).
- In extreme cases, disconnect the device from the network if internet access is optional for it to function properly. But this practice goes against one of the core IoT principles—always online. For devices such as the Wi-Fi bathroom scale, internet access is not required to measure body weight but is a must for sending the information to an online portal that tracks daily changes and provides fitness suggestions.

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

Conclusion

In this research paper, we shed light on the exposed cyber assets found in the top 10 French cities by population to raise awareness for both home users and enterprises. The results are quite expected — Paris had the most number of searchable cyber assets in Shodan for February 2017 because it's the most populous city and one of the biggest business hubs in the country.

In comparison to the exposure numbers in U.K. cities however, French cities had fewer instances of exposed devices such as webcams, routers, and printers, among others. This could be due to either a fewer number of users of these devices or a high number of properly configured devices.

Webcams figured prominently among exposed device types, which is cause for concern since they can be used for surveillance, subsequently leading to breach of users' privacy.

Open databases could be dangerous, too, as exemplified by the ransom attacks that hit MongoDB database owners. Attackers can simply create a backup of any company's critical data then delete them from the company server and demand for a ransom. Or in some cases, PII can be stolen and then sold underground. Such a scenario may lead to compliance issues on policies such as data protection laws in France and the GDPR.

Enterprises or businesses can use our findings in this paper to enhance their database or device security. 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.

Appendix

Research Coverage

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

City	Population
Paris	2,220,445
Marseille	852,516
Lyon	496,343
Toulouse	453,317
Nice	343,629
Nantes	291,604
Strasbourg	274,394
Montpellier	268,456
Bordeaux	241,287
Lille	228,652

Table 2. List of French 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.²⁹ 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 France 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 French cities. The data set used contained a total of 7,029,627 records generated from scanning 2,177,319 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 France. 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 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 internet usage means the IPv4 address space is fast getting depleted. The IPv4 address space supports a maximum of 2^{32} addresses. IPv6, with its maximum of 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.³⁰ This translates to finding multiple devices and systems visible from the same IP address in the Shodan scan data, most likely sitting behind a router or a firewall.

Hosting Providers

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

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

References

1. Numaan Huq, Stephen Hilt, and Natasha Hellberg. (15 February 2017). *Trend Micro Security News*. "U.S. Cities Exposed." Last accessed on 18 September 2017, <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/us-cities-exposed-in-shodan>.
2. Library of Congress. "Online Privacy Law: France." Last accessed on 21 September 2017, <https://www.loc.gov/contact/>.
3. Trend Micro. "EU General Data Protection: Time to Act." Last accessed on 18 September 2017, <http://www.trendmicro.co.uk/enterprise/data-protection/eu-regulation/>.
4. Shona Ghosh. (1 June 2017). *Business Insider UK*. "Paris is Coming Closer to Toppling London as Europe's Tech Hub." Last accessed on 21 September 2017, <http://uk.businessinsider.com/benefits-of-paris-technology-startups-investment-station-f-london>.
5. 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>.
6. Pawan Kinger. (8 April 2014). *TrendLabs Security Intelligence Blog*. "Skipping a Heartbeat: The Analysis of the Heartbleed OpenSSL Vulnerability." Last accessed on 21 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 21 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2015-0204>.
8. The MITRE Corporation. (2013). *Common Vulnerabilities and Exposures*. "CVE-2013-1899." Last accessed on 21 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1899>.
9. The MITRE Corporation. (2016). *Common Vulnerabilities and Exposures*. "CVE-2016-9244." Last accessed on 21 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9244>.
10. The MITRE Corporation. (2013). *Common Vulnerabilities and Exposures*. "CVE-2013-1391." Last accessed on 21 September 2017, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1391>.
11. The MITRE Corporation. (2015). *Common Vulnerabilities and Exposures*. "CVE-2015-2080." Last accessed on 21 September 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2080>.
12. Terrence McCoy. (21 November 2014). *The Washington Post*. "How a Russian Web site Peers into Your Home, and Your Baby's Room, by Hacking Webcams." Last accessed on 21 September 2017, https://www.washingtonpost.com/news/morning-mix/wp/2014/11/21/how-a-russian-web-site-peers-into-your-home-even-your-babys-room-by-hacking-webcams/?utm_term=.354df63b18f8.
13. Trend Micro. (31 January 2017). *TrendLabs Security Intelligence Blog*. "Routers Under Attack: Current Security Flaws and How to Fix Them." Last accessed on 5 September 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/routers-under-attack-current-security-flaws-and-how-to-fix-them/>.
14. Phil Muncaster. (11 September 2017). *InfoSecurity Magazine*. "MongoDB Ransom Victims Had No Account Passwords." Last accessed on 21 September 2017, <https://www.infosecurity-magazine.com/news/mongodb-ransom-victims-no/>.
15. Phil Muncaster. (6 September 2017). *InfoSecurity Magazine*. "MongoDB Customers Held to Ransom Again." Last accessed on 21 September 2017, <https://www.infosecurity-magazine.com/news/mongodb-installations-held-to/>.
16. Paul Rubens. (15 December 2009). *Enterprise Networking Planet*. "It's About Time: Why Your Network Needs an NTP Server." Last accessed on 21 September 2017, <http://www.enterprisenetworkingplanet.com/netsp/article.php/3853601/Its-About-Time-Why-Your-Network-Needs-an-NTP-Server.htm>.

17. Lucian Constantin. (11 February 2014). *Computerworld*. "Attackers Use NTP Reflection in Huge DDoS Attack." Last accessed on 21 September 2017, <http://www.computerworld.com/article/2487573/network-security/attackers-use-ntp-reflection-in-huge-ddos-attack.html>.
18. TechTerms. (2017). "UPnP." Last accessed on 21 September 2017, <https://techterms.com/definition/upnp>.
19. The MITRE Corporation. (2017). *Common Vulnerabilities and Exposures*. Last accessed on 29 August 2017, <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=UPnP>.
20. The MITRE Corporation. (2017). *Common Vulnerabilities and Exposures*. Last accessed on 8 September 2017, <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SSDP>.
21. Jay Yaneza. (9 February 2017). *TrendLabs Security Intelligence Blog*. "Brute-Force RDP Attacks Plant CRYISIS Ransomware." Last accessed on 21 September 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-crysis-ransomware/>.
22. Rod Trent. (1 August 2014). *ITPro Windows*. "Remote Desktop Applications Being Exploited on POS Systems." Last accessed on 21 September 2017, <http://windowsitpro.com/security/remote-desktop-applications-being-exploited-pos-systems>.
23. Hunton & Williamas LLP. (31 October 2016). *Privacy & Information Security Law Blog*. "Entry into Force of the French Digital Republic Bill." Last accessed on 21 September 2017, <https://www.huntonprivacyblog.com/2016/10/31/entry-force-french-digital-republic-bill/>.
24. Trend Micro. (20 December 2016). *Trend Micro Security News*. "A Practical Introduction to the European General Data Protection Regulation for SMBs." Last accessed on 29 August 2017, <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/a-practical-introduction-to-the-european-general-data-protection-regulation-for-smb>s.
25. The European Parliament and the Council of the European Union. (6 July 2016). *Official Journal of the European Union*. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union." Last accessed on 31 August 2017, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN>.
26. Danilo D'Elia. (13 February 2014). *Chaire Castex de Cyberstratégie*. "Military Programming Laws and Protecting Essential Services Operators." Last accessed on 21 September 2017, <http://www.cyberstrategie.org/?q=en/military-programming-laws-and-protecting-essential-services-operators>.
27. The Mayer Brown Practices. (July 2016). "A New EU Framework on Cybersecurity: The Network and Information Security Directive." Last accessed on 31 August 2017, https://www.mayerbrown.com/files/Publication/5da28c2e-a8fd-4f19-bdc2-d62d6fc27f0b/Presentation/PublicationAttachment/2b75998a-2615-4e9d-828b-ee9b6e8e96e3/cybersecurity-update_jul2616.pdf.
28. CIS. (2016). *CIS*. "CIS Controls for Effective Cyberdefense." Last accessed on 29 August 2017, <https://www.cisecurity.org/critical-controls/>.
29. 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.
30. 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