Most cyber attacks focused on these 3 TCP ports only

Small and medium-sized businesses can fully protect themselves from most cyber attacks by increasing defenses against ports that are most often targeted by malicious actors.

Small and medium-sized businesses can fully protect themselves from most cyber attacks by increasing defenses against ports that are most often targeted by malicious actors. Three of these network gateways are often the favorite target of attackers with 130,000 times becoming targets related to network incidents.

The latest report released by intelligence and defense security firm Alert Logic lists some of the top weaknesses commonly observed in cyber attacks targeting more than 4,000 of their customers. . Specifically how we will find out now.

1. Awareness and experience - the most important factor in all network security processes

Enterprise network security

TCP ports are most often hacked

As reported by Alert Logic, the ports most commonly used to carry out an attack are 22, 80 and 443, respectively with SSH (Secure Shell), HTTP (Hypertext Transfer Protocol) and HTTPS. (Secure hypertext transfer protocol).

Alert Logic experts say these three ports appear in about 65% of all reported cyber security incidents. This is reasonable because these are the most commonly used ports, and for communication, they will all need to be opened, be it in the form of confidential or plain text.

In fourth place is the port for Microsoft's Remote Desktop Protocol (RDP), which is responsible for creating remote communications connections between computer systems. RDP is the name that has garnered a lot of attention this year through patches for several major vulnerabilities, which could lead to remote code execution attacks (CVE-2019-1181, CVE- 2019-1182 and CVE-2019-0708) exert serious impact on users.

1. What is malware analysis? What are the steps?

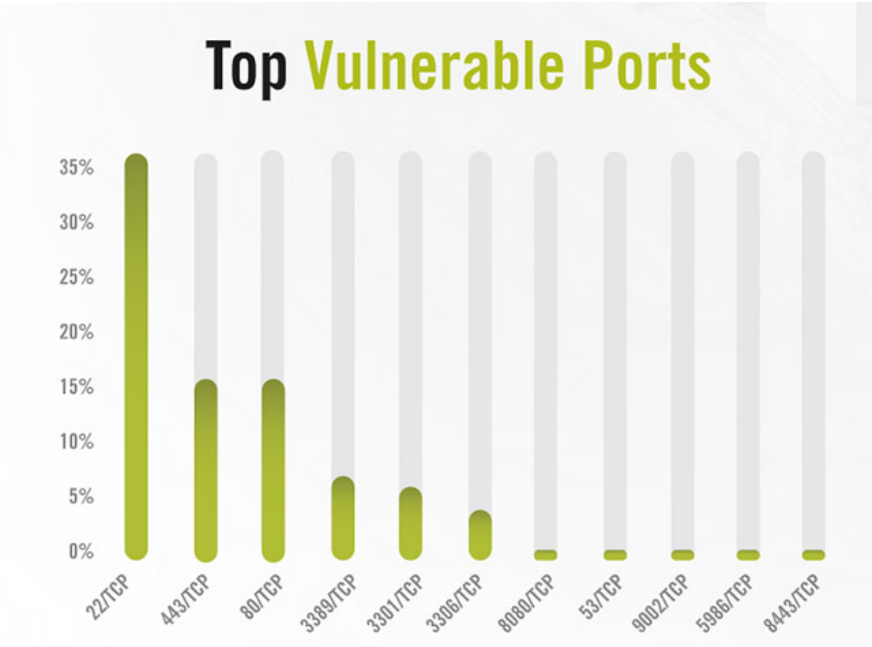
HTTPS is one of the most commonly used protocols today

"According to the basic guidelines, the security status on all network gateways must include defense mechanisms in depth. Unused ports should be closed and organizations, businesses and even individuals should set up firewalls on every server, as well as constantly deploying port traffic monitoring and filtering operations as well as good practices to help ensure that no vulnerabilities are missed and that Out of control "- Alert Logic.

In addition, the File Transfer Protocol (FTP - 20, 21) port is also considered a serious risk for any organization if it is not fully protected. Active servers have been found on printers, cameras and uninterruptible power supplies.

Alert Logic's recommendation to minimize potential risks from these ports is to ensure that devices, software or services are always updated to the latest version, along with reinforcing security capabilities. for devices and software based on these ports, thereby minimizing the opportunity for attack by crooks.

1. Detecting many serious vulnerabilities that allow an attacker complete control of 4G router

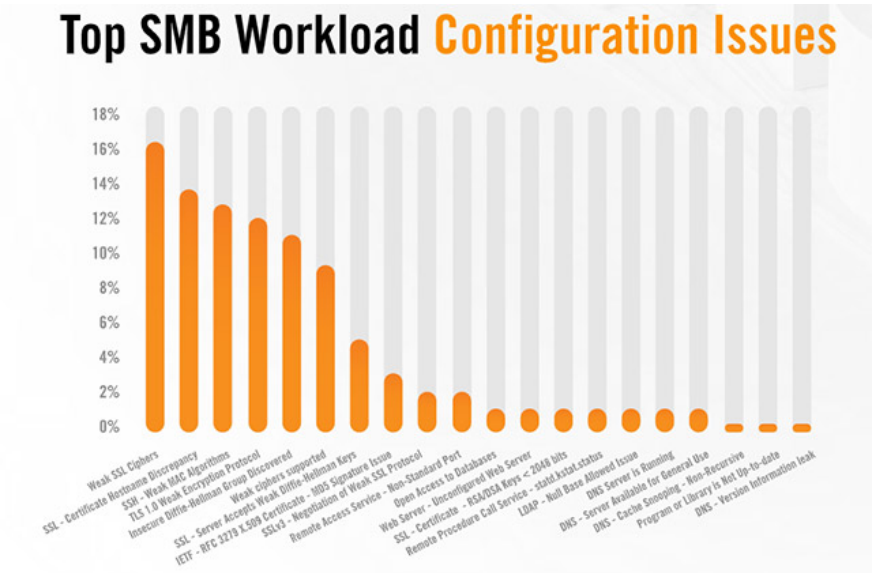


List of the most vulnerable TCP ports as per Alert Logic's survey

Using outdated software

Additional vulnerabilities that weaken the overall security state of an organization or enterprise related to outdated encryption software account for 66% and 75% of all problems Alert Logic notices, respectively. with their customers.

1. Discover many new ways to hack WiFi passwords protected with WPA3

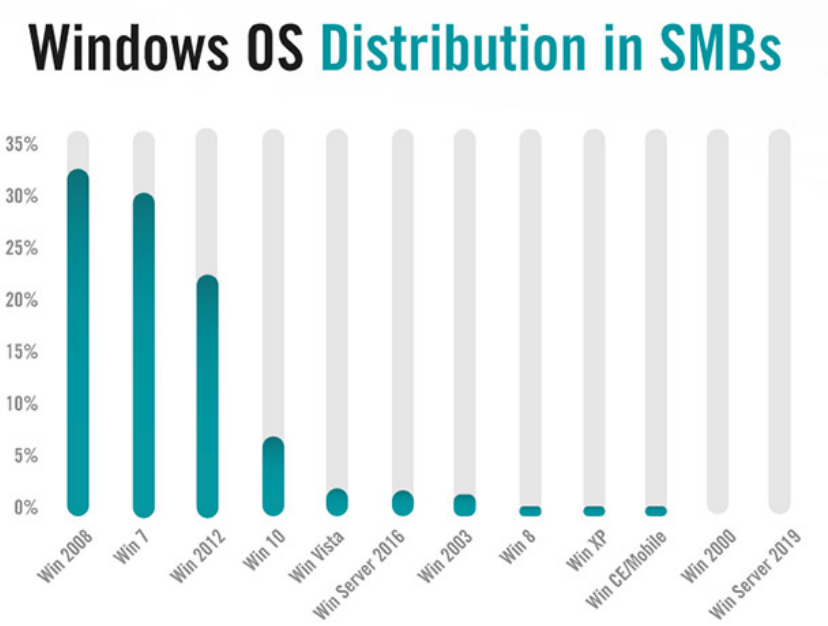


The vulnerabilities weaken the overall security status of an organization or enterprise

To make matters worse, the security firm found that more than 66% of the servers it scanned were still running on Windows 7, an operating system that's nearly 10 years old and will no longer be supported by Microsoft. support since January 14, 2020. On the opposite side, Windows Server 2019 is hardly found on the infrastructure of small and medium enterprises - a sad situation for not only Microsoft but also the security specialist.

Worse, it's unclear for what reason that Windows XP, an operating system launched in 2011, the last release in 2008, and end of support in 2014, continues to be available for a while. "the number is not small" the systems surveyed. Alert Logic said it even found Windows NT devices (released in 1993) on the network of a few customers. This is obviously the bait could not be better for hackers, who just wait for your system to have loopholes and exploits.

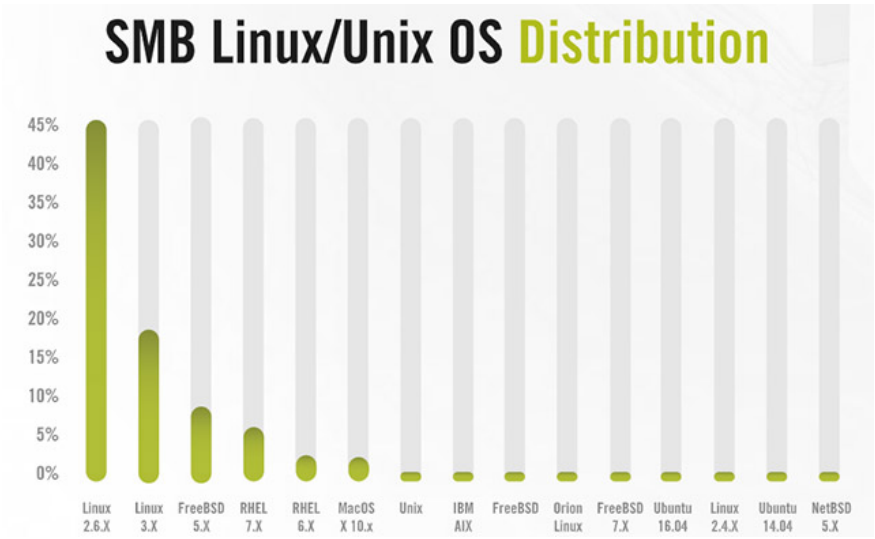
1. Despite Microsoft's efforts, Windows 7 is still used in nearly 50% of businesses surveyed



The list of most commonly used Windows versions for small and medium businesses according to the Alert Logic survey

The same situation appears for Linux. Nearly half of all Linux systems tested by Alert Logic still run outdated kernels. Many organizations still use version 2.6, which has been deprecated for the past 3 years and contains up to 65 vulnerabilities, large and small.

1. Secure desktop apps - weaknesses are often overlooked

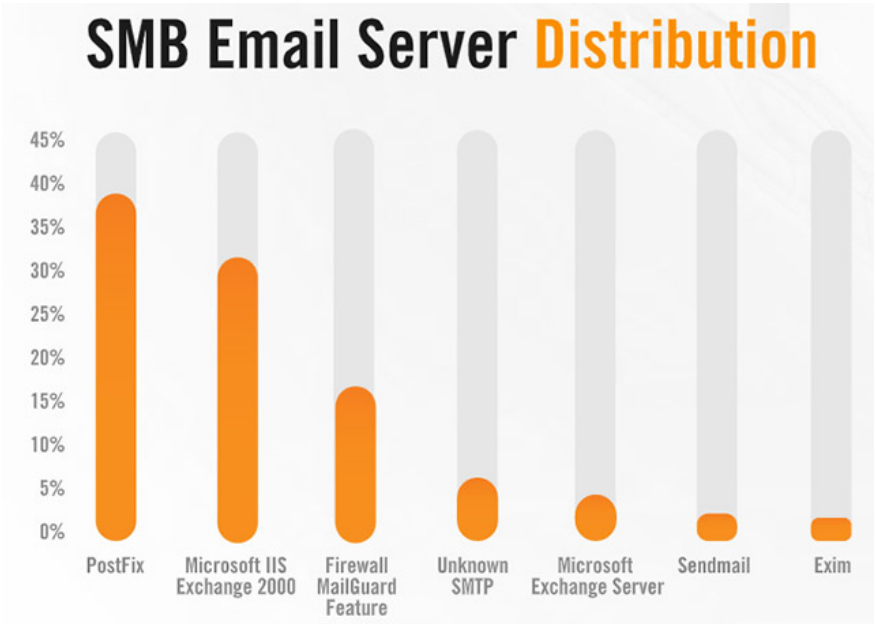


List of the most popular Linux distributions for small and medium businesses

Another example of the use of outdated software in organizations and businesses is the Exchange 2000 email server, which accounts for nearly a third of all email servers discovered by Alert Logic. The problem is that Exchange 2000 stopped supporting support in July 2010, more than 9 years ago.

The most common email server for small and medium businesses tracked by Alert Logic is PostFix, while Exim - a very popular email server, is in the last place.

1. Overview of building an enterprise security detection and feedback system



List of the most popular email servers for small and medium businesses

Alert Logic says these data are aggregated from about 5,000 recorded attacks, targeting their customers' infrastructure over a period of 6 months, from November 2018 to April 2019. .

In fact, businesses are the ones who are the 'laziest' to upgrade the operating system because they often uphold the stability of the system, so if the old operating system can still meet the needs while New executives do not bring too many obvious benefits or are simply not stable, they of course are not foolish to upgrade.

However, an old operating system and no longer receive security patches will be a serious cyber security risk - a lucrative bait for hackers. Therefore, businesses and users should update to the latest version of Windows, regardless of the reason!