Leading search engines for internet-connected devices and services

DUBAI, DUBAI, UNITED ARAB EMIRATES, May 23, 2023 /EINPresswire.com/ -- Camilo Gutiérrez Amaya, Head of Awareness & Research at ESET gives a roundup of some of the handiest tools that security professionals can use to search for and monitor devices that are accessible from the internet

Internet security is a constant concern for technology and cybersecurity professionals. With the ever-increasing number of online devices and services, it is important to have a clear and accurate view of the online presence of these devices and services in order to protect them and data against online threats. Some search engines for internet-connected devices, such as Shodan, Censys, Zoomeye, Fofa and BinaryEdge, play a crucial role in this task.

They allow cybersecurity and other technology professionals to have a complete and accurate view of the online presence of their devices and services. Each offers detailed information about each device and service, including their IP address, operating system, software and open ports. In addition, they offer unique features that set them apart from other Internet search engines.

By monitoring these devices and services, cybersecurity professionals can take steps to protect them against online threats, including automated port scanning, the spreading of malware, and vulnerability scanning. In addition, these search engines can also be useful for other technology professionals who want to monitor their brands' online presence and protect their online reputation.

In this blogpost, we will look at five such tools, namely Shodan, Censys, Zoomeye, Fofa and BinaryEdge, and discuss their unique features, their applications and their importance for digital security.

Shodan

Shodan allows anyone to find internet-connected devices, including web servers, IP cameras, routers and more. Shodan is unique in that it focuses on searching for these devices and provides detailed information on each device, including IP address, operating system, software and open ports. It is a valuable tool for cybersecurity professionals who want to identify devices and services that may be exposed to potential security vulnerabilities.

Censys
Censys is another search engine that focuses on searching for devices connected to the internet. Like Shodan, Censys provides detailed information about each device, including IP address, operating system, software and open ports. However, unlike Shodan, Censys also focuses on device security and provides information about known vulnerabilities and SSL certificates. This information is valuable for monitoring and securing devices and online services.

Zoomeye
Zoomeye is another popular search platform for internet-connected devices and services. It allows anyone to search for and monitor online devices and services and receive real-time alerts about changes in their search results. Zoomeye focuses on identifying online devices and services and provides detailed information about each device.

Fofa
Fofa provides detailed information about each device and service, while also highlighting information regarding the brand. One interesting feature is the possibility to use a search syntax with different filters, which makes it possible to use one's own scripts and run more specific searches.

BinaryEdge
Finally, BinaryEdge is a security search engine that allows users to receive real-time alerts about changes in their search results. Similarly to Shodan or Censys, the information collected by BinaryEdge includes open ports and services with associated potential vulnerabilities, as well as data on accessible remote desktops, invalid SSL certificates and network shares with configurations that could lead to security breaches. It is also possible to verify if any email account is involved in a data leak.

Bonus: GreyNoise
GreyNoise is a cybersecurity tool that allows users to monitor and analyze unwanted internet traffic. GreyNoise uses machine learning algorithms to identify and classify network activity that is considered noise or could be considered malicious. The GreyNoise platform is constantly updated to reflect the latest threats and trends in cybersecurity.

Unlike the other search engines mentioned above, GreyNoise focuses on identifying and classifying network activities that are considered noise, such as automated port scanning, malware spreading and vulnerability scanning. GreyNoise also offers an API that allows cybersecurity professionals to integrate the information supplied by GreyNoise into their existing

tools and systems.

Conclusion
These search engines offer unique and valuable features for cybersecurity and other technology professionals who want to monitor and protect their online devices and services; especially for those companies that need to increase their threat intelligence efforts. When considering which of these scanners is right for one's needs, it is important to consider the specific features and capabilities of each and how they can be used to meet one's specific needs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
