censys

How Secure Is Our Modern Internet?

Key Findings from the Censys 2023 State of the Internet Report

The internet, with all its complexities, has become an integral part of our lives and businesses.. It's a vast and dynamic infrastructure – and its rapid expansion continues to pose challenges to organizational security practices. That's why in our 2023 State of the Internet Report, we provide insights into the state of security on the modern internet, and do so by examining web entities and their exposures.

What are Web Entities on the Internet?

Web entities are services running on the internet that utilize the HTTP protocol. These entities include web servers, load balancers, web-based APIs, and more. In a recent snapshot of the internet, Censys observed over 1.3 billion HTTP services across 740 million hosts.

Cloud Provider Usage:
Approximately 18% of HTTP services are hosted on major cloud providers such as Amazon, Oracle, Google Cloud Platform (GCP), or Microsoft Azure.

Named vs. Unnamed Hosts:
Over 85% of HTTP services are running on named hosts, while 14% are running on unnamed hosts accessible only by their IP addresses.

Web Server Technologies:
The majority of HTTP services, both on named and unnamed hosts, utilize web server technologies. Apache HTTPD and Nginx are the most popular choices.

The presence of discontinued or scrutinized web server products on unnamed hosts suggests that these devices may have non-optimal security practices in place.

2023 State of the Internet Key Findings

Positive Adoption of TLS Encryption:
Censys observed that over 90% of web traffic is encrypted, with nearly 95% supporting the latest TLS versions (1.2 and 1.3). The growth in TLS 1.3 adoption is encouraging and indicates a shift away from less secure versions. Let's Encrypt, offering free TLS certificates, has played a significant role in widespread TLS adoption, responsible for 49% of browser-trusted certificates. It provides a convenient and cost-effective alternative to the previously cumbersome certificate acquisition process.

Misconfigurations Remain a Serious Problem:

Censys identified 8,336 servers hosting sensitive information, including database dumps, backup files, passwords, Excel worksheets, and SSL/SSH private keys.

- 1,000 hosts exposed more than 2,000 SQL database files without authentication requirements;
- 5,000 hosts exposed backup files and directories containing potentially confidential or credential-related information;
- 400 hosts exposed WordPress configuration files ("wp-config.php"), potentially providing access to underlying databases; and
- 147 hosts exposed 18,000 CSV files publicly.

Unauthenticated Monitoring Tools and API Documentation:

Threat actors can exploit unauthenticated monitoring tools (Prometheus) and API documentation (SwaggerUI) to gather detailed insights into target networks. Our data revealed over 40,000 instances of each, providing potential avenues for reconnaissance.

- **Prometheus**, a popular monitoring tool, may expose monitoring data and network information to the internet. Over 41,800 Prometheus servers are exposed, monitoring over 219,400 endpoints. Around 48% of monitored endpoints exist in private IP and DNS space, typically not visible to the global internet.
- **SwaggerUI**, an API documentation tool, when unintentionally exposed, can reveal sensitive information about private APIs. Censys observed over 42,800 hosts running SwaggerUI, with over 46% located in the United States. Over 35,000 hosts run SwaggerUI on standard HTTP ports, while over 8,000 hosts use non-standard ports.

Security Practices Lagging:

The popularity of web servers with vulnerabilities or end-of-life status suggests inadequate security practices among certain hosts. These vulnerabilities may expose organizations to risks.

Conclusion

While the adoption of secure practices is increasing, there are still vulnerabilities and risks present on the internet. Although misconfigurations, default security settings, and exposures may seem like minor oversights in the short-term, they can serve as a foothold for threat actors to gain unauthorized access to an organization's network, potentially resulting in more severe security incidents with long-term consequences.Organizations can reduce their exposure by adopting proactive security strategies, including asset management, vulnerability management, and patching. Strong foundational security practices are crucial for creating a safer internet, and Censys aims to raise awareness and encourage collaboration towards this goal.