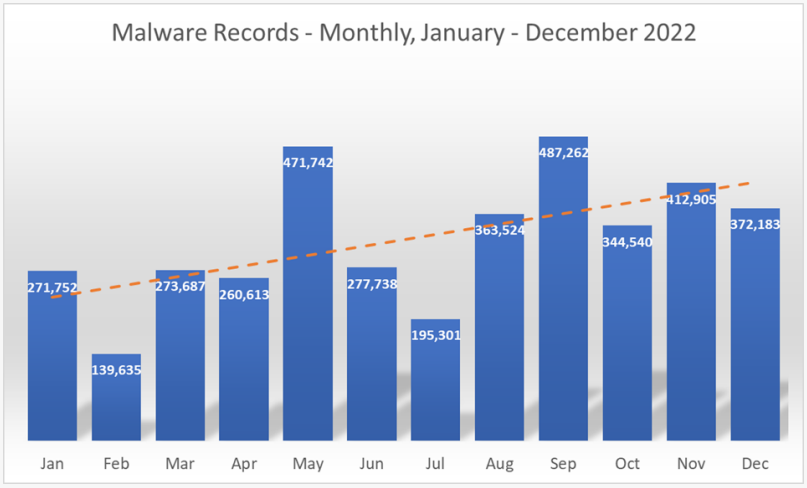
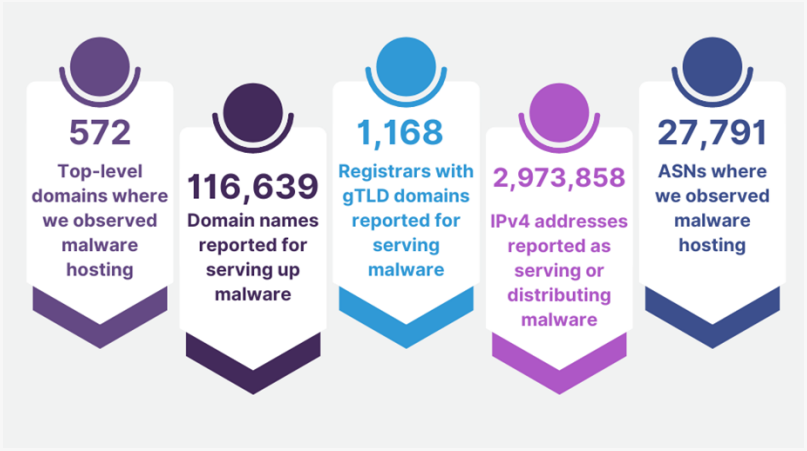
Interisle reports that malware hosting activity in 2022 was most intense in China, India and United States

Information stealing and ransomware continue to rise, as does misuse of cloud and file sharing services for malware distribution.



Malware Activity Trended Up in 2022



Findings from 2022 Malware Landscape Study

HOPKINTON, MA, USA, March 14, 2023 /EINPresswire.com/ -- Interisle Consulting Group today announced the publication of their annual Malware Landscape report, which shows that Malware activity continued to increase in 2022 and that Malware hosting was concentrated in China, India, and the United States.

Interisle reviewed over 7 million reports of distinct malware events from January 2022 to December 2022 collected by the Cybercrime Information Center, examining malware that attacks both IoT and user-attended devices ("endpoints"). This year Interisle also studied reports of malicious traffic sources: malware that is used to scan web sites for exploitable vulnerabilities, to inject malicious content into web forms, or to conduct denial of service attacks.

The major findings of the study are:

- Malware activity increased in 2022, continuing the trend from the previous year. Information stealing and ransomware were the dominant malware threats in 2022.

• Endpoint malware activity increased 50% over 2021. The Quackbot banking trojan was the most reported endpoint malware.

• IoT malware activity decreased in 2022. Mozi IoT malware reporting sharply declined in early 2022 but showed signs of renewed activity in 4Q 2022.

• 60% of reports identified malware that attacks or probes legitimate web sites. Nearly two-thirds of the reported probes were vulnerability scanners. PHP forum spammers accounted for one-third of attackware reported.

• Malware hosting activity was most intense in China, India, and the United States.

• The use of domain names in malware URLs grew sharply. Interisle found a 121% increase in the use of domain names in 4Q 2022.

• Attackers continued to exploit file sharing services and code repositories to distribute malware.

Interisle partner Lyman Chapin explains that “malicious traffic source reports show that target identification malware is prevalent and persistent. Second stage attacks to acquire resources for DDOS attacks or exploitation often follow.”

The findings strongly suggest that mitigating malware requires cooperation and determined efforts by all parties that comprise the naming, addressing, and hosting ecosystem exploited by cyberattackers. The Interisle study discusses several means by which coordinated efforts among these parties, law enforcement, and private sector “first responders” could result in more effective malware mitigation.

Dave Piscitello, director of the Cybercrime Information Center and Interisle partner, warns that, "Global patience is wearing thin. Our past studies have been cited by the European Union Internet Governance expert group on DNS Abuse and in lawsuits alleging cybersquatting violations and trademark infringement. Our 2023 report discusses several means by which coordinated efforts among these parties, law enforcement, and private sector first responders could result in more effective malware mitigation. But if cooperation doesn’t mature quickly, we expect to see more regulatory and litigatory activity that seeks to effect change.”

The full text of Interisle’s report is available at https://interisle.net/MalwareLandscape2023.html.

About the Cybercrime Information Center

The Cybercrime Information Center is a repository for studies, measurements, data sets, statistics, and analyses of global security threats involving the Internet’s the Domain Name

System (DNS) and numbering systems (Internet protocol addresses and Autonomous System numbers). The project operates through support or data contributed by the Anti-Phishing Working Group (APWG), the Coalition Against Unsolicited Commercial Email (CAUCE), Domain Tools, InvaluementURI, Malware Patrol, MalwareURL, OpenPhish, PhishTank, The Spamhaus Project, and The URLhaus Malware URL Exchange. The Cybercrime Information Center reports quarterly malware activity at https://cybercrimeinfocenter.org/malware-activity.

About Interisle Consulting Group:

Interisle's principal consultants and associates are experienced practitioners with extensive track records in industry and academia and world-class expertise in business and technology strategy, Internet technologies and governance, financial industry applications, and software design.
For more about Interisle, please visit: https://www.interisle.net.

David Piscitello
Interisle Consulting Group
+1 843-295-9329
email us here
Visit us on social media:
Facebook
Twitter
YouTube
