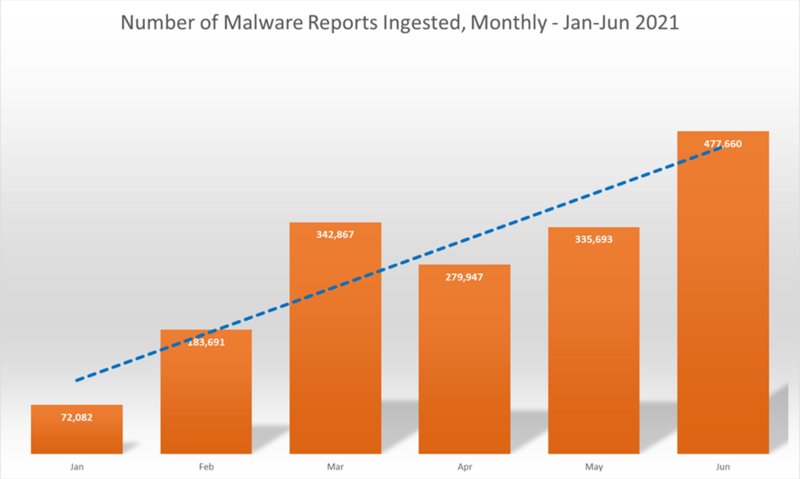
EINPRESSWIRE

Interisle study shows 663% increase in malware reports, alarming spike in IoT malware

HILTON HEAD ISLAND, SC, UNITED STATES, November 17, 2021 /EINPresswire.com/ -- Interisle Consulting Group today announced the publication of Malware Landscape 2021: A Study of the Scope and Distribution of Malware. The study, which analyzed nearly 1.7 million malware reports collected from January 1, 2021 to June 30, 2021, shows a 663% increase in malware reports in the first half of 2021.



Study shows a 663% increase in malware reports in the first half of 2021

Among the major findings in the study, Interisle reports that:

• Malware that exploits Internet of Things (IoT) devices is the fastest growing category of malware. IoT Malware accounted for 56% of the malware reports collected.

• Mozi malware dominated the IoT malware landscape.

• Information stealers and ransomware account for 40% of malware that exploited user devices such as tablets, mobile phones, laptops, and PCs.

• Malware attackers use fewer domains but to great effect. Phishing attacks and spam campaigns use large numbers of domain names as “bait”. Our data revealed Internet addresses are more frequently identified as serving up malware than domain names.

• Domains registered in the new Top-level Domains (TLDs) are disproportionately attractive to malware attackers. The new TLDs represent only 6% of the domain name registration market, but they contained 16% of reported malware domains. By contrast, the country code TLDs represent 43% of the market, but only 28% of the reported malware domains.

• Domain registrars with high malware domain counts tend also to have high phishing domain counts.

• Malware attackers extensively misused file sharing services, code repositories, and storage services. While most uses of anonymous file sharing and code repositories are well-intentioned, malware attackers have used these services to distribute source code, attack code, and files containing compromised credentials or cryptographic keys.

According to Lyman Chapin, Interisle partner and co-author, “Malware is diverse but always dangerous. Ransomware is particularly insidious malware. When this malware hijacks your device you lose control and the criminal takes over—they can alter or destroy your data, encrypt your files, and extort ransom payments. Other forms of malware steal credentials or personal data, which criminals then sell or use for financial gain. The personal, business, and financial losses resulting from such malware can be catastrophic.”

According to Dave Piscitello, Interisle partner and co-author, “IoT malware is mostly used to build massive botnets for distributed denial of service attacks. Like the Mirai IoT Malware of 2016, the Mozi malware we observed in our study exploited known vulnerabilities in the embedded software of DVRs, routers, cameras, wearables, and the like. The IoT industry needs to lock these devices down.”

The full text of Interisle’s report is available at https://interisle.net/MalwareLandscape2021.html.

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.

Interisle is engaged in a long-term effort to collect and analyze data on the way in which criminals abuse the Internet and its users, so that Internet policy development can be informed by reliable and reproducible intelligence based on data rather than anecdotes. As part of this effort, Interisle publishes quarterly phishing and malware activity reports at the Cybercrime Information Center.

For more about Interisle, please visit: https://www.interisle.net.

David Piscitello
Interisle Consulting Group LLC
email us here