Malware Landscape 2023

A Study of the Scope and Distribution of Malware

Lyman Chapin, David Piscitello, Dr. Colin Strutt
Interisle Consulting Group, LLC

14 March 2023

Interisle
Consulting Group

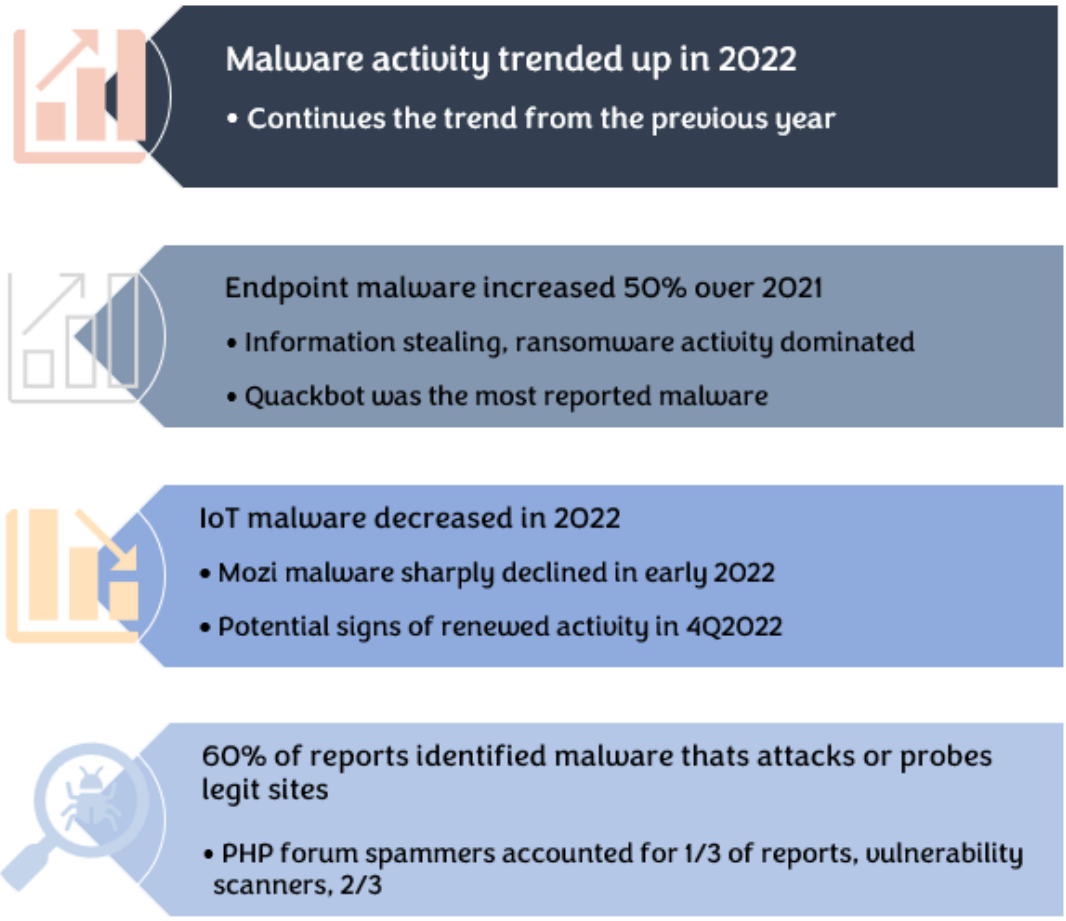
Executive Summary

Malware — **mal**icious soft**ware** — can infect and compromise any device connected to a network. Criminals use malware to steal information, perpetrate identity theft or financial fraud, and remotely control compromised devices. Malware is also used for surveillance or to inject malicious content into forums or social media. It is an organized criminal business that costs governments, corporations, and individuals hundreds of billions of dollars every year.

This report quantifies the ways in which malware criminals use the ordinary services of the global Internet—naming, addressing, and hosting – at a relentless pace and scale. We identify the resources that criminals misappropriate, and how and from whom they acquire them. Armed with reliable data, cybercrime investigators and public policy makers can make informed decisions about how to pursue and deter criminal abuse of the Internet.

For this study we captured over 7 million malware reports from four widely respected threat intelligence sources: Malware Patrol, MalwareURL, Spamhaus, and URLhaus. Analyzing these reports yielded important insights into what malware was most prevalent, where malware was served from or distributed, and what resources criminals used to pursue their attacks.

Principal Findings



Malware hosting activity most intense in China, India, and USA

- Malware hosting tends to be regionalized

Use of domain names for malware distribution grew sharply

- 121% increase in domain names in malware URLs in 4Q 2022
- Attackers misused file sharing services and code repositories

Future Opportunities

Mitigating malware requires cooperation and determined efforts by all parties that comprise the naming, addressing, and hosting ecosystem exploited by cyberattackers:

HOSTING & CLOUD SERVICE PROVIDERS

- Adopt Terms of Service that allow you to remove malicious content quickly and legally
- Scan your IP address spaces for malware and remove malware you detect
- Act quickly on malware reported by investigators

DOMAIN REGISTRARS & REGISTRIES

- Adopt Terms of Service that allow you to remove or suspend domains reported for serving malware quickly and legally
- Coordinate suspensions with hosting services

ALL OPERATORS

- Maintain complete and accurate domain registration or user account information.
- Routinely re-assess mitigation practices to ensure timely responses to documented and verified malware complaints.

TARGETS OF MALWARE

- Consider whether legislation or regulation may be necessary for effective mitigation of malware threats.