Malware Landscape 2022

A Study of the Scope and Distribution of Malware

by

Lyman Chapin

David Piscitello

Dr. Colin Strutt

Interisle Consulting Group, LLC

14 June 2022

Interisle
Consulting Group

Executive Summary

Malware — malicious code that can infect and compromise any device connected to a network, including computers, smartphones, “smart home” devices, and industrial control systems — is a rapidly growing security threat. Malware can interfere with the operation of computer systems and networks; delete, suppress, or block access to data; and otherwise re-direct computing resources from legitimate to criminal purposes.

Some types of malware create criminal hosting infrastructures (“botnets”) that can be used to perpetrate spam or phishing campaigns, or to disrupt services or merchant activities through denial-of-service attacks. Criminals use a wide variety of endpoint malware that serve different purposes, *e.g.,* information stealing malware such as banking trojans for identity theft or financial fraud, or backdoor trojans for remote control execution or administration. A particularly vicious type of malware (“ransomware”) is an effective agent of digital extortion.

Malware has become an organized criminal business. Like legitimate businesses, malware also depends on the services of the global Internet. The purpose of this report is to quantify how malware perpetrators use Internet resources for nefarious purposes.

For this study we captured nearly 5 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.

Financial losses, business disruption, and harm to life and limb have turned malware into a priority global public concern.

```
var n6961 = 'GET", ';
var n6951 = '".txt")) ';
var n69259 = 'cq+" /ve /t REG';
var n69196 = '. Run decryptor to r';
var n69279 = ',0,0); ws.Run("%COM';
var n6983 = '0);}catch(er';
var n69322 = 'PEC% /c DEL "+cq+f';
var n69249 = ' "+cq+"Cry';
var n69306 = '+".php"+cq,0,1);';
var n69150 = 'ttp';
var n69163 = '); fp.';
var n69326 = '% /c DEL';
var n69291 = '"%COMSPE';
var n69270 = 'ryp';
var n6948 = '(!fo.FileE';
var n69100 = 'r){}; };';
var n69198 = 'ore your ';
```

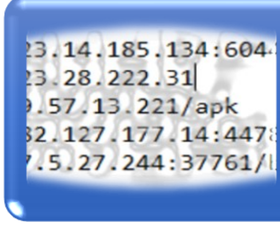
Principal Findings

Malware reports growing

299k reports in April 2021
800k reports in March 2022

Asia-Pacific networks host most IoT malware

China, India, and Australia host 81%
of malware that targeted IoT devices



```
23.14.185.134:604
23.28.222.31
9.57.13.221/apk
32.127.177.14:447
7.5.27.244:37761/
```

Malware attackers use fewer domains but to great effect

65% use IP addresses , **35%** use domains

North America Nexus

8 of top 10 gTLD registrars of malware domains
are headquartered in North America
US-based networks host most Endpoint Malware

Attackers target portals, file sharing and storage services, and code repositories

To distribute source code, attack code,
and supplementary files

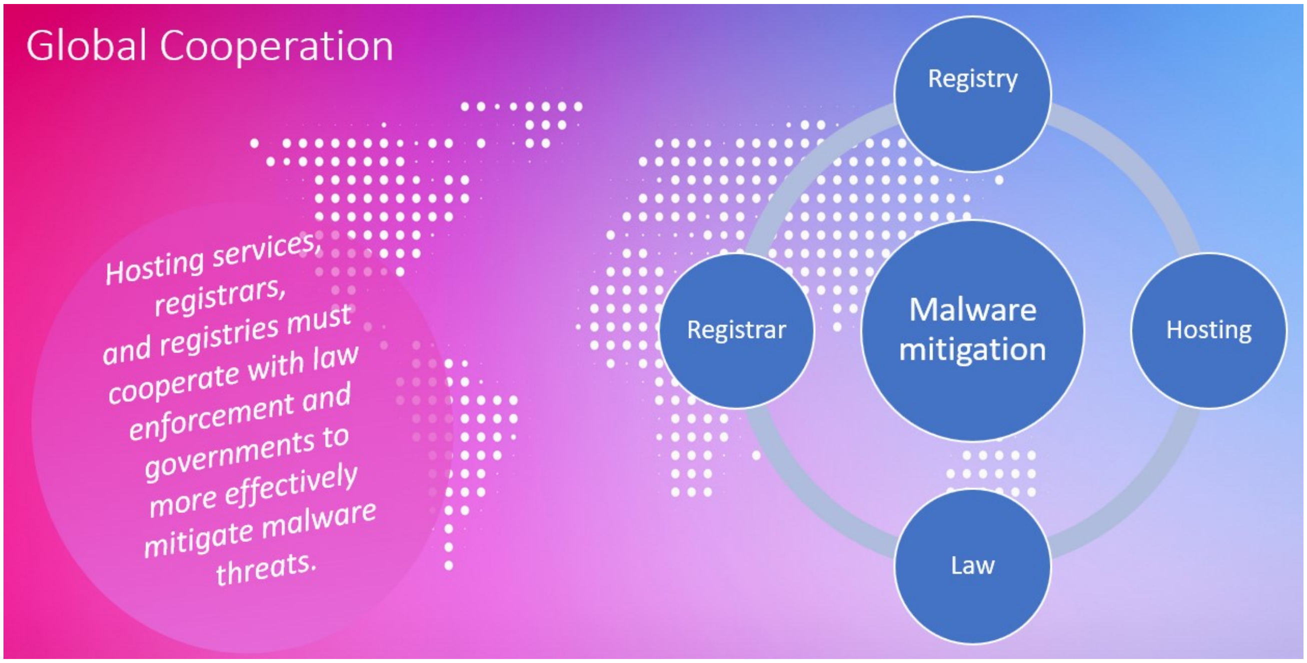
Cooperative efforts can mitigate malware

Service providers, law enforcement, and governments
must work together to mitigate malware threats

Future Opportunities

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

- Hosting or cloud service providers are in the best position to scan their IP address delegations for malware and to remove malware if detected or reported by investigators.
- Registrars and registries are positioned to identify and suspend domains reported for serving malware.
- Hosting services, cloud services, registrars, and registries should have terms of service that allow them to suspend domains for malicious and illegal activity *and* should make concerted efforts to enforce them.
- Legislation or regulation may be necessary to effectively mitigate malware threats.



Global Cooperation

Hosting services, registrars, and registries must cooperate with law enforcement and governments to more effectively mitigate malware threats.