Malware Landscape 2021

A Study of the Scope and Distribution of Malware

by

Greg Aaron

Lyman Chapin

David Piscitello

Dr. Colin Strutt

Interisle Consulting Group, LLC

17 November 2021

Executive Summary

Malware — "malicious software" — is defined by the Organization for Economic Cooperation and Development as "a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners". Malware can manipulate data; 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.

Malware has diverse purposes. Several formidable types of malware are distributed to create criminal hosting infrastructures that can be used to perpetrate spam or phishing campaigns, or to disrupt services or merchant activities through denial-of-service attacks. Other types of malware, *infostealers*, target personal, financial, or other sensitive information. A particularly vicious form of malware, *ransomware*, is an effective kind of digital extortion. Financial losses, business disruption, and harm to life and limb have turned ransomware into a priority global public concern. In a recent survey, the U.S. Treasury Department's Financial Crimes Enforcement Network identified Bitcoin wallet addresses used for payments related to the ten most common ransomware variants. Those wallets sent Bitcoin valued at $5.2 billion to known criminal entities.

To assemble a deep and reliable set of data, we captured and analyzed 1,686,033 malware reports during a six-month study period from four widely used and respected threat intelligence sources: Malware Patrol, Malware URL, Spamhaus, and URLhaus. From these source or *malware reports*, we created 1,255,598 records suitable for analysis to understand what malware was most prevalent, where malware was served from or distributed, and what resources criminals used to pursue their attacks.

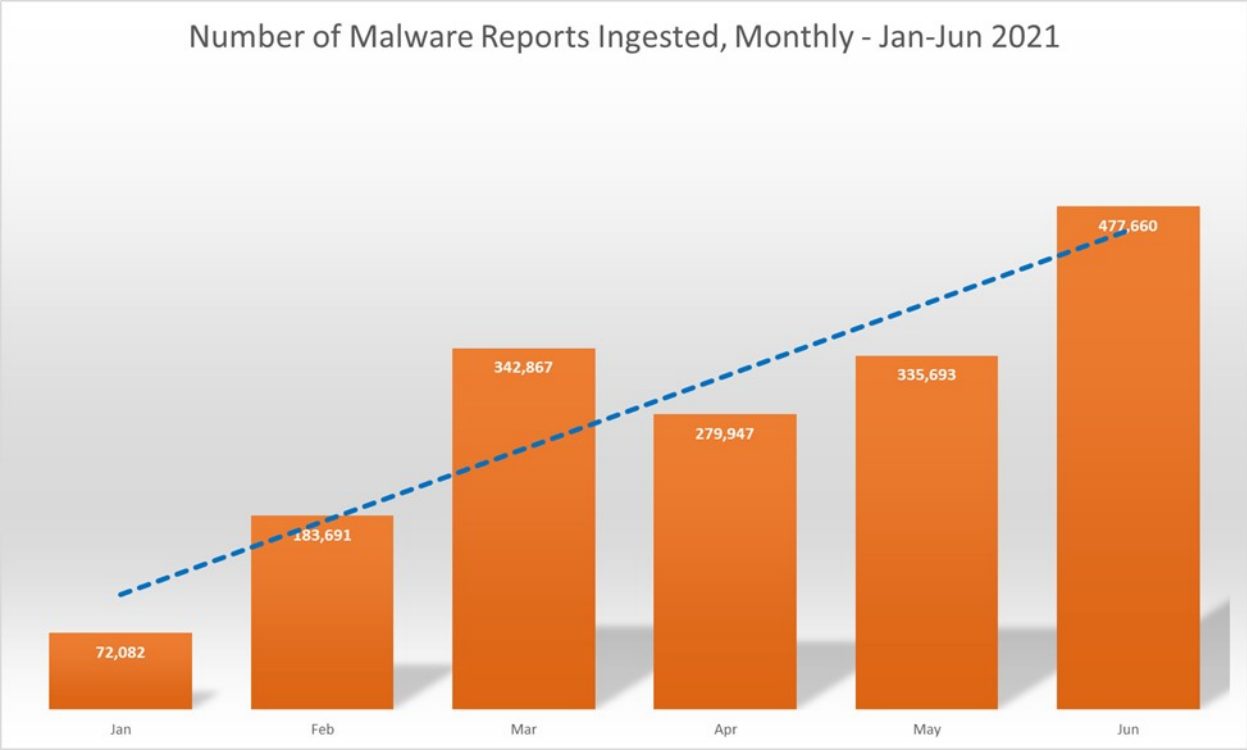

Figure 1 Monthly Malware Reports Ingested, January - June 2021

Domain names are essential resources for spam and phishing attacks, but the data we collected revealed that they are less commonly used for serving malware or for malware distribution; consequently, this malware study focused less on domain name registries and registrars than our annual phishing surveys, and more on the hosting services or cloud services that support the serving and distribution of malicious content.

Principal Findings

- **Malware is growing rapidly.**
  The number of malware reports that we collected from threat feeds trended upward from approximately 72,000 to nearly 480,000 over our 6-month study period.
- **Malware that exploits Internet of Things (IoT) devices is the fastest growing malware.**
  IoT Malware accounted for 56% of the malware reports we collected, and 86% of the malware reports that we were able to classify.
- **99% of the records that we associated with IoT Malware were identified as Mozi malware.**
  Mozi malware accounts for between 80-95% (370,956 of 376,194) of the IoT malware reported in five hosting networks.
- **The majority of malware reports identify or include IPv4 addresses rather than domain names.**
  However, we did not find any IPv6 addresses in our study data.
- **Information stealers and ransomware account for 40% of malware that exploits endpoint devices.**
  Ransomware and banking trojans are perpetrations of financial fraud or extortion. Other types of malware commonly provide the means to install or deliver malware that is used to collect or exact a monetary reward.
- **Malware attackers use fewer domains but to great effect.**
  While phishing attacks and spam campaigns use large numbers of domain names as “bait”, our data revealed that Internet addresses are more frequently identified as serving up malware than domain names.
- **Domains registered in the new TLDs are disproportionately attractive to malware attackers.**
  The new TLDs represent only 6% of the domain name registration market, but they contain 16% of reported malware domains. By contrast, ccTLDs represent 43% of the market, but contain only 28% of the malware domains.
- **Registrars with high malware domain counts tend also to have high phishing domain counts.**
  Comparing this study’s results with those reported in Interisle’s Phishing Landscape 2021, we found that many of the operators in the “top 10” are the same for malware and phishing.
- **Malware attackers extensively misuse file sharing services, code repositories, and storage services.**
  456,182 URLs from records in our malware data set are associated with the anonymous file service anonfiles.com. 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. Google Drive and Microsoft OneDrive are also misused but to a lesser extent, and by a particular malware, GuLoader.

Future Opportunities

Our data suggest that there may be opportunities for hosting services (*e.g.*, companies that operate data centers, dedicated servers or virtual private servers), registrars, registries, and cloud services, to assist with the timely mitigation of malware threats.

1. Hosting service and 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. They are also in a position to monitor hosts and networks for suspicious user activities, *e.g.*, to identify the origin addresses of users who upload malware to file sharing repositories, or who run malicious software on shell accounts, or whose user accounts generate or receive network traffic that is anomalous, suspicious or known to be a pattern associated with malware.

2. Registrars and registries are in an excellent position to identify and suspend domains reported for serving malware. These parties possess key information – contact data and billing data – that no one else does. This data is highly useful for identifying malicious customers at the time of registration. The DNS Abuse Institute (dnsabuseinstitute.org) has prepared a Framework to Address Abuse (dnsabuseframework.org) – a best practice that obliges registrars and registries to "promptly investigate allegations of DNS Abuse and Website Content Abuse", including malware. The 50 signatory registrars and registries have an opportunity to lead by example by working cooperatively with cybersecurity and law enforcement communities to mitigate malware.

3. Malware is arguably a crime in all the countries and regions where domain names are used or registered. Malware also falls within the scope of Articles 2 and 6 of the Council of Europe's Convention on Cybercrime, which has been signed or ratified by 67 nations worldwide. Hosting services, cloud services, registrars, and registries should not only have terms of service that allow them to suspend domains for malicious and illegal activity but should make concerted efforts to enforce them.