# 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*

Interisle
Consulting Group

# Table of Contents

## Table of Figures



## Table of Tables

## 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.

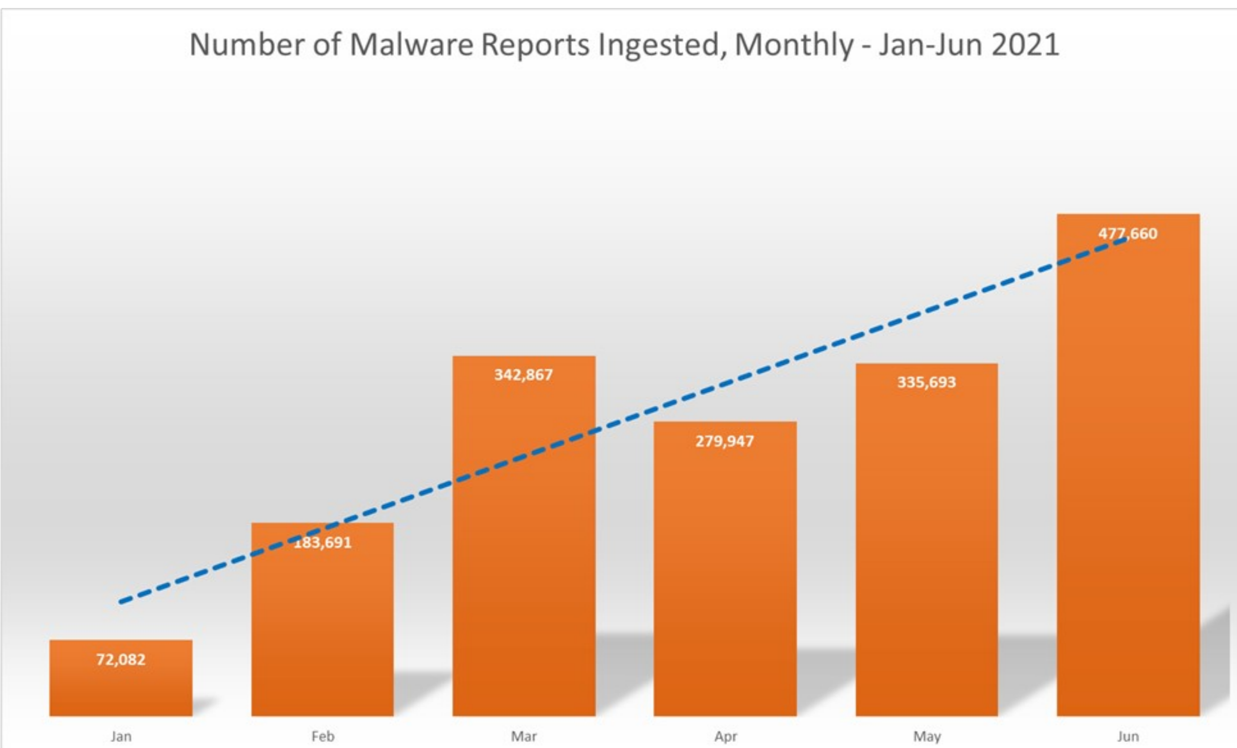


*Figure 1 Monthly Malware Reports Ingested, January - June 2021*

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.

## Introduction

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".[1] 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.

The independent research institute, AV-TEST GmbH[2] is registering 450,000 new malware and potentially unwanted applications daily. Figure 2 illustrates the increase in total malware since 2012.

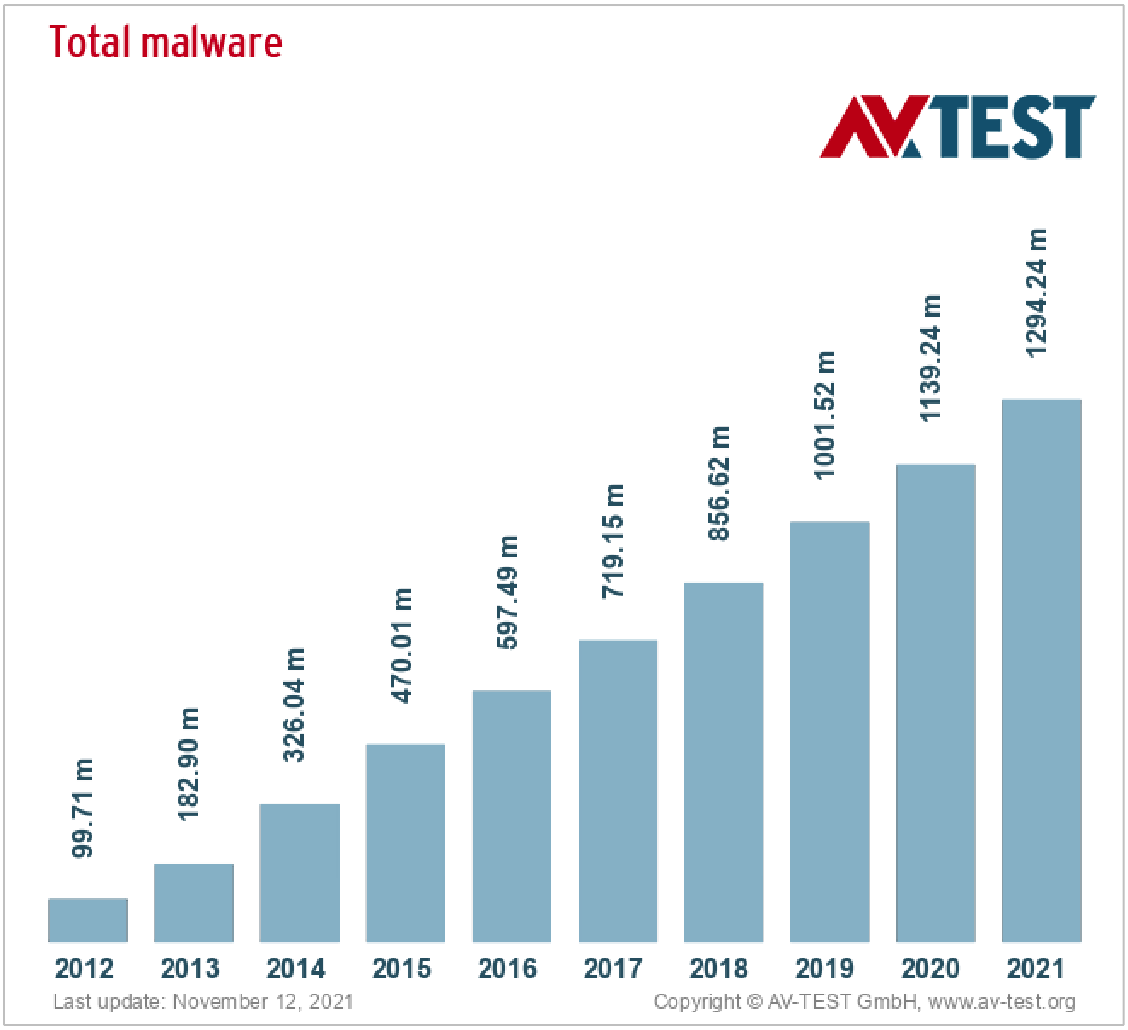


*Figure 2 Total Malware Since 2012 – (Source: AV-TEST.org)*

### The Malware Landscape

Malware has diverse purposes. Several formidable types of malware are distributed to create criminal hosting infrastructures such as botnets 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 target personal, financial, or other sensitive information.

*Ransomware* is a particularly vicious form of extortion malware, and it is growing rapidly: in its April 2021 report "Combating Ransomware" [3] the Ransomware Task Force of the Institute for Security and Technology documents a 150% increase in the number of attacks and 300% increase in the amount of ransom paid from 2019 to 2020.

Financial losses, business disruption, and harm to life and limb have turned ransomware into a priority global public concern.[4] In addition to the indirect costs of business and service disruption, ransomware inflicts a substantial direct financial cost in the form of ransom payments. In a recent survey, the U.S. Treasury Department's Financial Crimes Enforcement Network identified 177 unique Bitcoin wallet addresses used for ransomware payments.[5] Those wallets sent Bitcoin valued at $5.2 billion to known criminal entities.

These financial rewards accrue to state-supported or -sanctioned criminal enterprises as well as to ordinary criminals, which makes malware both a law-enforcement and a geopolitical issue.[6] The government of North Korea, for example, engages in overtly criminal activity ranging from bank heists to the deployment of ransomware and the theft of cryptocurrency from online exchanges. In 2019, a United Nations panel of experts on sanctions against North Korea issued a report estimating that the country had raised two billion dollars through cybercrime.[7] The nexus of state involvement and criminal enterprise is a grave concern. The Director of the U.S. Federal Bureau of Investigation, Christopher A. Wray, told The Wall Street Journal in an interview published on June 4, 2021 that the ransomware threat was comparable to the challenge of global terrorism in the days after the September 11, 2001 World Trade Center attack.[8]

With the stakes this high, understanding — and reliably measuring — the malware landscape is among the highest priorities for members of the cybersecurity community.

## The Malware Study

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 analyses to understand what malware was most prevalent, where malware was served from or distributed, and what resources criminals used to pursue their attacks.

There are hundreds of different types of malware — some of which are polymorphic, evolving in response to countermeasures or to accommodate new criminal intentions. In conducting our research, we noticed significant differences between malware attacks on user-attended devices (such as computers and mobile phones) and malware attacks on Internet of Things (IoT) devices (such as "smart" thermostats, sensors, wearables, and embedded technologies). User-attended device ("endpoint") malware is commonly used for financial fraud or theft; IoT device malware is commonly used for denial-of-service attacks or to create criminal infrastructures ("botnets" [9]). Consequently, we study these separately.

## Domain Names and Malware

Domain names are essential resources for spam and phishing attacks; however, the data we collected reveal 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 malware. We thus concentrate on Hosting Networks or Autonomous Systems.

## Hosting Resources and Malware

The majority of malware reports that we collected during our study period contain Internet Protocol (IPv4) addresses. In this study, we identify and discuss the hosting services or cloud services that criminals misuse to serve or distribute malware by Autonomous System Number (ASN).

An Autonomous System (AS) is a collection of the IP addresses (routing prefixes) controlled by a common network administrator—a web hosting provider, a business, a university, an Internet Service Provider (ISP), or a network operator providing service to several of those types of entities. Each AS is identified by a unique number (ASN). It is common for larger hosting services and cloud services to have several AS numbers. Business and operational practices may cause an AS (and its number) to be transferred from one service provider to another (*e.g.,* following an acquisition or divestiture). An AS and its number may be re-allocated because of other events (*e.g.,* bankruptcy or business closure). Considering this churn, we report on individual hosting networks (ASNs).

## Classifying Malware

For this study, we set out to identify and measure the resources that attackers used to deliver or "serve" malware to client or endpoint devices.

Malware can be written to perform different functions. There are hundreds of malware executables, many of which are polymorphic. Some malware evolves by adding or borrowing code from other malware, open source, or commercial software. A malware may begin as an executable with a single purpose, *e.g.*, to download other malware, but the creator or others may add new components or functionality to a malware that sees success in the wild, for example to serve up ransomware. Researchers, blocklist service providers, and commercial security companies further complicate classification by adopting their own naming conventions.

Classification, including ours, is thus subjective. Our classification may be consistent with that of some but not all malware research or commercial anti-malware companies.

We began by "normalizing" metadata provided by Malware URL and URLhaus, where our subscriptions provided sufficient metadata to study the types of malware that were being served from hosting resources. We use a classification of malware proposed by the Computer Antivirus Research Organization (CARO [10]) as a baseline to create a taxonomic ranking, where:

Class = *Threat*

Order = *Cybercrime*

Family = *Crime Type*

Sub-family = *Targeted Devices*

Genus = *Malware Type*

Species = *Malware (name)*

The Order, *Cybercrime*, adopts the cyberthreats identified as cybercrimes in the Council of Europe's Convention on Cybercrime.[11, 12] We are measuring *Crime Types* that The Convention describes as illegal access or misuse (malware, generally), and data or system interference with data or systems (*e.g.*, ransomware). We identify two sub-families in Crime Type = Malware based on the kinds of devices that malware targets. We attempt to group or classify malware according to the primary or original purpose the malware serves. Within Genus, we identify malware by one of the names commonly associated with the malware.

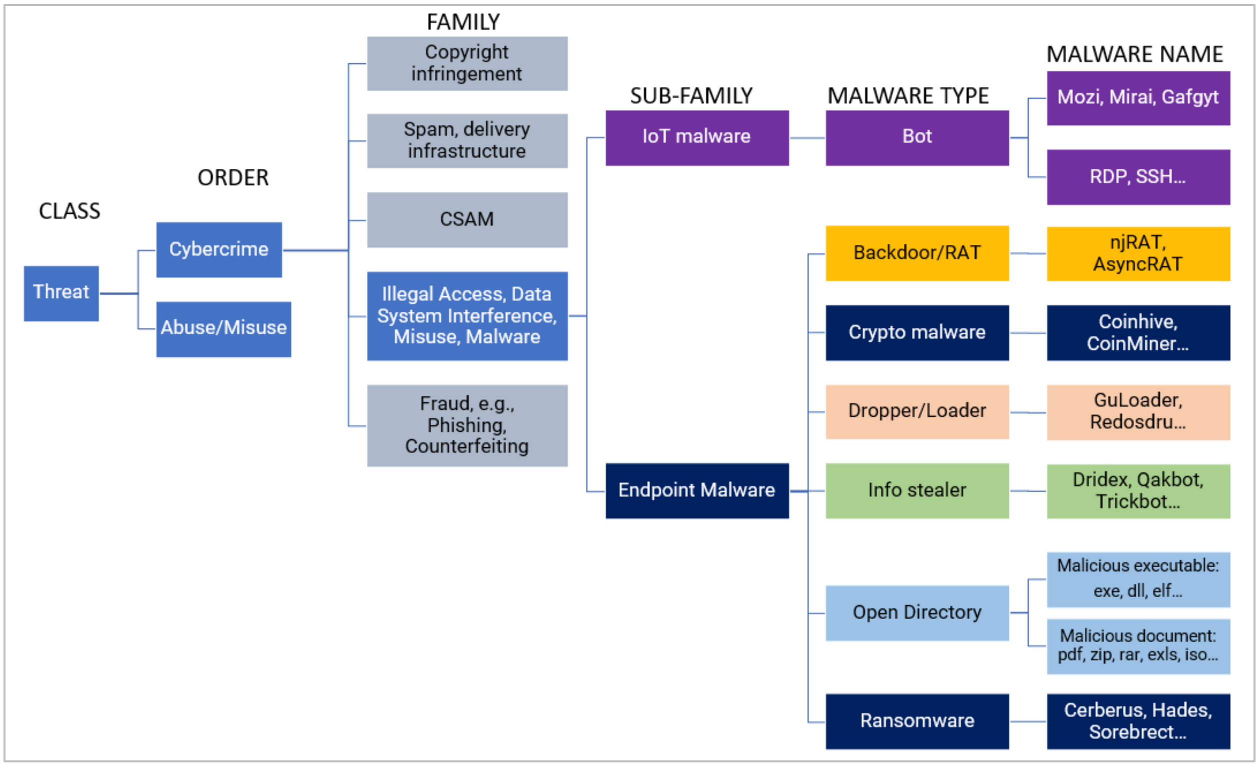


*Figure 3 Illustration of a Taxonomic Ranking of Malware*

The Genus, *Malware Type,* in this study includes these malware types:

**Backdoor/RAT.** A backdoor is malware that installs a software tool that provides remote access or administration of the infected endpoint, *i.e.*, a means for an attacker to enter the computer unobserved or "through a back door". RAT is an acronym for remote administration tool or trojan.[13]

**Bot.** A bot (Internet robot, also called zombie, spider, or crawler) is a form of malware that installs on an infected device and then contacts a command-and-control host (C2) to be "enrolled" into a criminal hosting infrastructure. Once enrolled, the bot communicates with the C2 for instructions or to download malware for second stage attacks, *e.g.*, denial-of-service, relay spam, keylogging, or backdoor installation.[14]

**Cryptocurrency malware**. Malware that targets cryptocurrency. Some cryptocurrency malware targets digital wallets (much like a banking trojan [15]) but others exploit or "hijack" the infected devices' resources to mine cryptocurrencies and are called *cryptojackers*.[16]

**Dropper/loader**. A dropper/loader is a malware that installs other malware. The terms "dropper" and "loader" are often used interchangeably, but some use the term "dropper" for malware that is installed from something physically present on an infected device, *e.g.*, a removable media or a malicious email attachment, and reserve the term "loader" for malware that is downloaded over a network connection from a host that an attacker uses to serve malware to infected computers.[17, 18]

**Infostealer**. A type of malware that steals usernames, passwords, or banking or credit card credentials, or any personal or sensitive information that can be used or sold for profit.[19]

**Malicious document**. An Office document that contains a malicious macro, or a PDF, compressed file, image, or archive (ISO) file that contains harmful code or a component for a malicious executable, is considered a malicious document.[20]

**Ransomware**. Malware that is used for extortion. Originally, criminals used ransomware to extract payments from individuals for the recovery of personal information. Today, attackers extort payments from corporations, government agencies, healthcare services, and critical infrastructures (power grids, water supply systems, etc.) for the recovery of sensitive information or service restoration.[21]

In most cases, we adopted a simplified Malware Type that is based on the CARO naming scheme.[22] When confronted with multiple names for a given malware, (*e.g.*, Quakbot, Qbot, Qakbot), we chose arbitrarily from these. In some cases, our feeds used generic tags, *e.g.*, open directory (opendir); here, we treated file types associated with such tags as species.

## Key Statistics

To assemble a deep and reliable set of data, we collected malware reports for a six-month period, from 1 January 2021 through 30 June 2021, from four widely used and respected threat data providers: MalwareURL, Malware Patrol, Spamhaus Domain Block List, and URLhaus (see Appendix A: Data Sources and Methodology).

In Table 1 we highlight key statistics for this period of malware activity.

| Measurement | Endpoint Malware | IoT Malware | Uncategorized | Total |
|---|---|---|---|---|
| Total number of malware reports from threat feeds | 307,007 (18%) | 392,107 (23%) | 986,919 (59%) | 1,686,033 |
| Unique domain names reported that were identified in malware reports | 16,983 | 14 | 20,869 | 35,294 |
| Top-level domains where we observed malware domains | 336 | 10 | 299 | 296 |
| Registrars that had domains under management reported for malware | 328 | 6 | 409 | 512 |
| Number of Internet Addresses (IPv4) where malware was hosted | 198,963 | 250,493 | 47,634 | 272,017 |
| Hosting Networks (ASNs) where malware web sites were reported | 2,906 | 3,826 | 1,941 | 5,576 |

*Table 1 Key Statistics for the Period of Malware Activity, January – June 2021*

In the table, we provide a total count of malware for each Key Statistic and counts for entries that we assigned to the sub-families we employ in our taxonomic ranking.

In many cases the identification of a malware is definitive, but the malware report lacks the information necessary to confidently classify the malware as "Endpoint Malware" or "IoT Malware". For the purposes of analysis and reporting, these cases are represented as "uncategorized" and counted separately from the sub-families.

In making this differentiation we have been careful to assign a malware report to a sub-family only when the available information (metadata) unambiguously supports the assignment.

## Malware Trends

We began with 1,686,033 reports collected from four threat feeds. We used the methodology described in Appendix A: Data Sources and Methodology to produce 1,255,598 malware records suitable for analysis. Figure 4 shows the number of malware records, by month.

**Malware generally increased during our study period. IoT Malware showed a greater increase month over month than Endpoint Malware.**

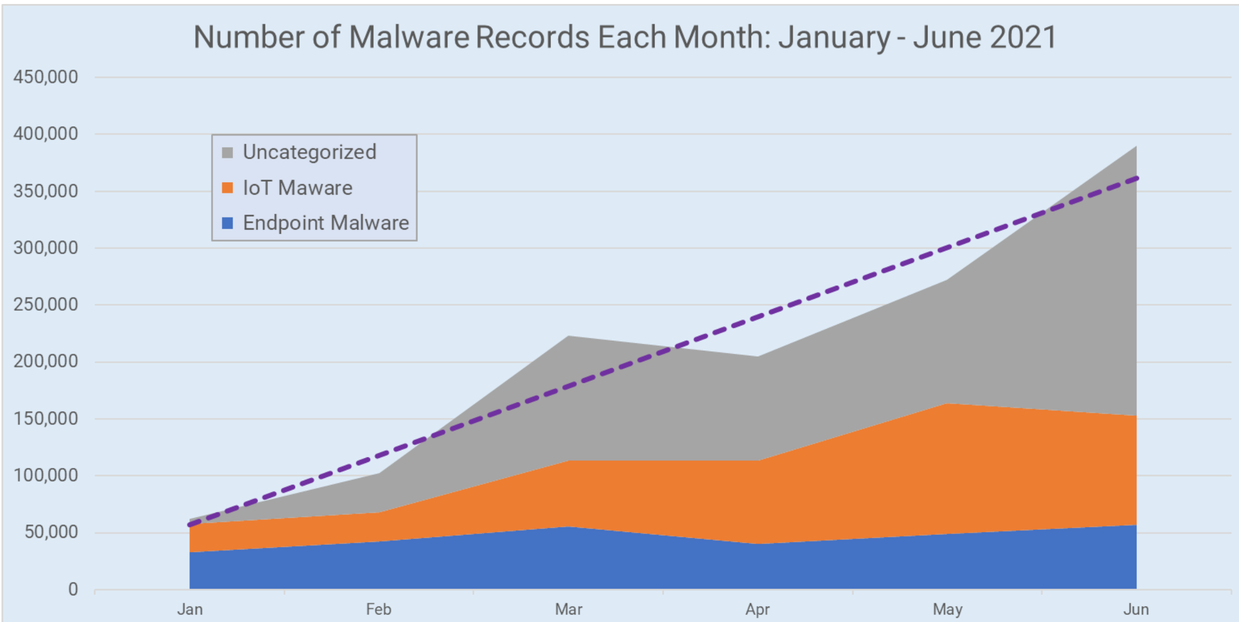


*Figure 4 Monthly Malware Records, January - June 2021*

Figure 5 shows the number of malware records we processed by day of week.

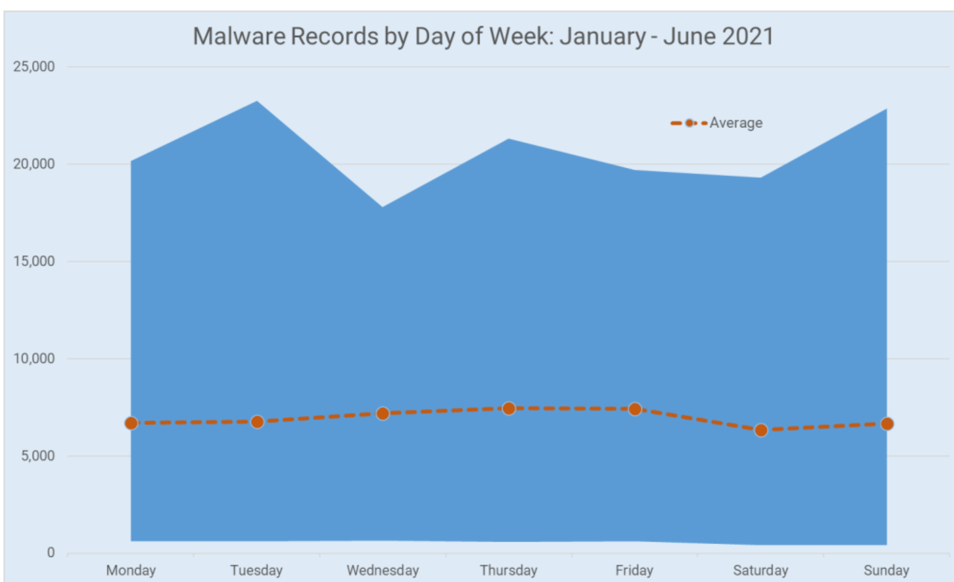


*Figure 5 Malware Records by Day of Week, January - June 2021*

In Figure 5, we see that malware reports have no discernable peaks. This is distinctly different from phishing — historically, phishing activity is highest in the Monday through Wednesday period, when potential victims are working and are checking their emails. The high numbers of malware reported as IoT Malware compared to the numbers of malware that target user-attended devices might suggest a plausible answer: IoT devices run 24x7. They don't take weekends off or have other behavior patterns such as holidays or catastrophic events that phishers would exploit through forms of social engineering. However, when we parsed Endpoint Malware records separately from IoT Malware, we saw little difference in the daily patterns, and this held true for Uncategorized records as well.

We note that there is a delay between when malware is hosted and consequently served and when the host that is serving or distributing malware is blocklisted, meaning that the malware downloads or peer distribution occurred earlier.

## Distribution of Malware by Sub-Family

Two of our threat intelligences feeds identify malware URLs, IP addresses, or domain names, but do not identify malware by name and do not provide the metadata that we require to place malware in a Family or Type. We include counts of **uncategorized as well as malware** in our TLD, Registrar and Hosting Networks rankings.

Figure 6 illustrates the distribution of malware reports collected during this study period.

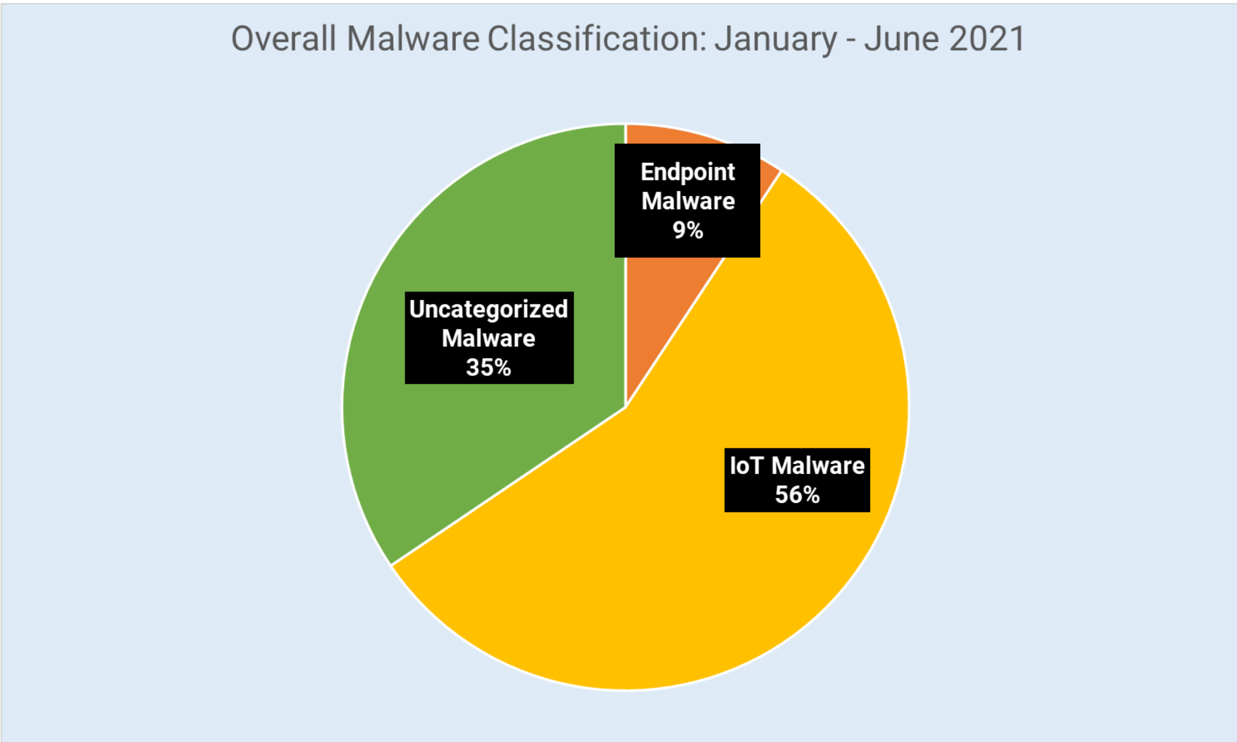


*Figure 6 Distribution of Malware Reports Collected, January – June 2021*

*Uncategorized* does not mean that the malware report is "unconfirmed" or that the reports are not validated with the same degree of confidence as other reports we collect; rather, it is our means of distinguishing malware reports that identify a resource used such as a domain name, but do not identify the specific malware or malicious activity.

We observed that 456,176 (78%) of the *uncategorized* malware records were associated with the domain anonfiles.com [23], an anonymous file sharing service. We discuss this service in the section Case Study: Anonfiles.com.

Figure 7 shows that IoT malware dominated the malware reports that we collected for which we had sufficient metadata to classify malware.

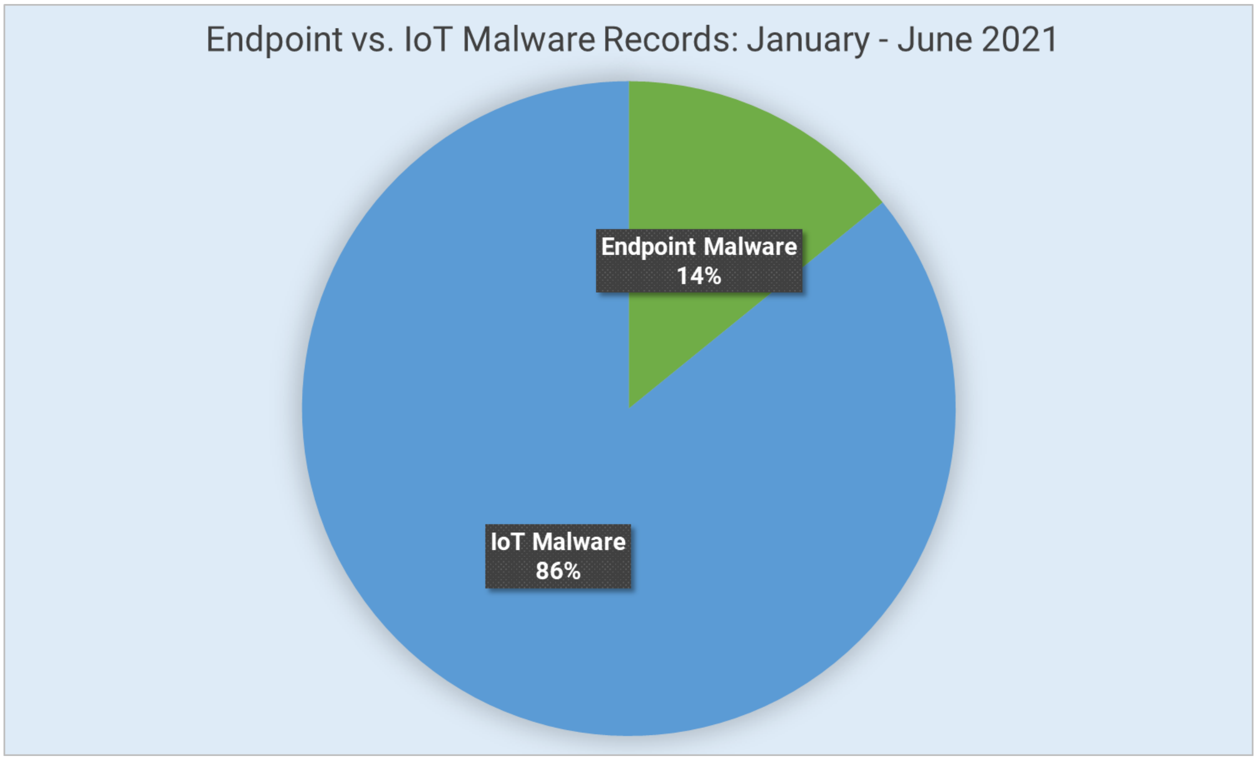


*Figure 7 IoT Malware Dominates the Landscape*

**86% of malware that we were able to classify was IoT Malware.** This finding is consistent with findings in other reports. SonicWall Capture Labs reported a 66% increase in malware attacks from 2019 to 2020.[24] While the measurements are different (SonicWall is measuring attacks and we are measuring reported malware), the enormity of IoT Malware activity is effectively demonstrated using both measures.

## IoT Malware.

**IoT Malware accounted for 56% of the malware reports we collected**.

IOT Malware targets Internet of Things (IoT) devices – routers, sensors, DVR or IP cameras, wearables, and embedded technologies. These devices commonly use or "embed" a Linux operating system or derivative, but the manufacturers did not adequately secure or "harden" the operating system against attacks and so left them vulnerable to attackers that exploit unsecured services such as Telnet or weak default passwords. Outdated software is a known issue: exploits for which patches have been released leave devices vulnerable to exploits that have been known in some cases for decades.

IoT malware is often multi-staged, where the first stage or "compromise" attack gains administrative control over the device and subsequent stages loads denial of service attack or other malware.

Raw numbers of reported IoT Malware reflect how infected devices are used. Large numbers, often thousands of infected IoT devices are often used to conduct *volumetric* denial of service attacks; in such attacks, these devices send traffic at a target, intending to overwhelm ("flood") the targeted server or network and in so doing, disrupt services that the target offers. In some cases, the attackers may try to extort the target, but in other cases, the attacks are acts of political or social protest, or a response to a perceived wrong.[25] Raw numbers may also offer an insight into an increasingly worrisome business model: Malware as a Service (MaaS), offered in the public and dark web, creates opportunities for unsophisticated criminals to perpetrate malware or ransomware attacks.

Nearly all the records that we associated with IoT Malware were identified as Mozi malware (370,956 of 376,194, or 99%). Gafgyt (Bashlite [26]) accounted for approximately 1% (4,480) and bots that exploit Secure Shell (SSH [27, 28]) to gain remote administrative control, 1% (381).

### Peer-to-Peer IoT Malware Case Study: Mozi

Mozi is one of a family of malware – including Mirai, Gafgyt, and IoT Reaper – that exploit Linux-based IoT devices such as DVR cameras and consumer grade routers. Mozi malware uses a password-based Telnet attack to gain control over unpatched or weakly-passworded devices. Compromised IoT devices use a distributed hash table (DHT) to store contact information for other clients or "peers". This method of communication allows the botnet to operate without a central command-and-control, and the DHT traffic may appear typical for services like BitTorrent that employ DHT for distributed file or database synchronization.[29]

Mozi has been linked to DDoS attacks, spam campaigns, and data exfiltration attacks. ThreatPost estimates Mozi to represent 90% of IoT botnet traffic.[30] Our findings are quite similar: we associated 367,227 of 391,853 IoT Malware URLs with Mozi Malware (94%); of these, 320,878 were URLs of the form http://a.b.c.d:ppppp/Mozi.*, where a.b.c.d is an IP address and ppppp is a number assigned from the ephemeral TCP/UDP port range.[31] The only other IoT botnet with meaningful count was Mirai, with 2,791 URLs reported.

Figure 8 shows the Hosting Networks (ASNs) with the largest numbers of devices hosting Mozi malware.

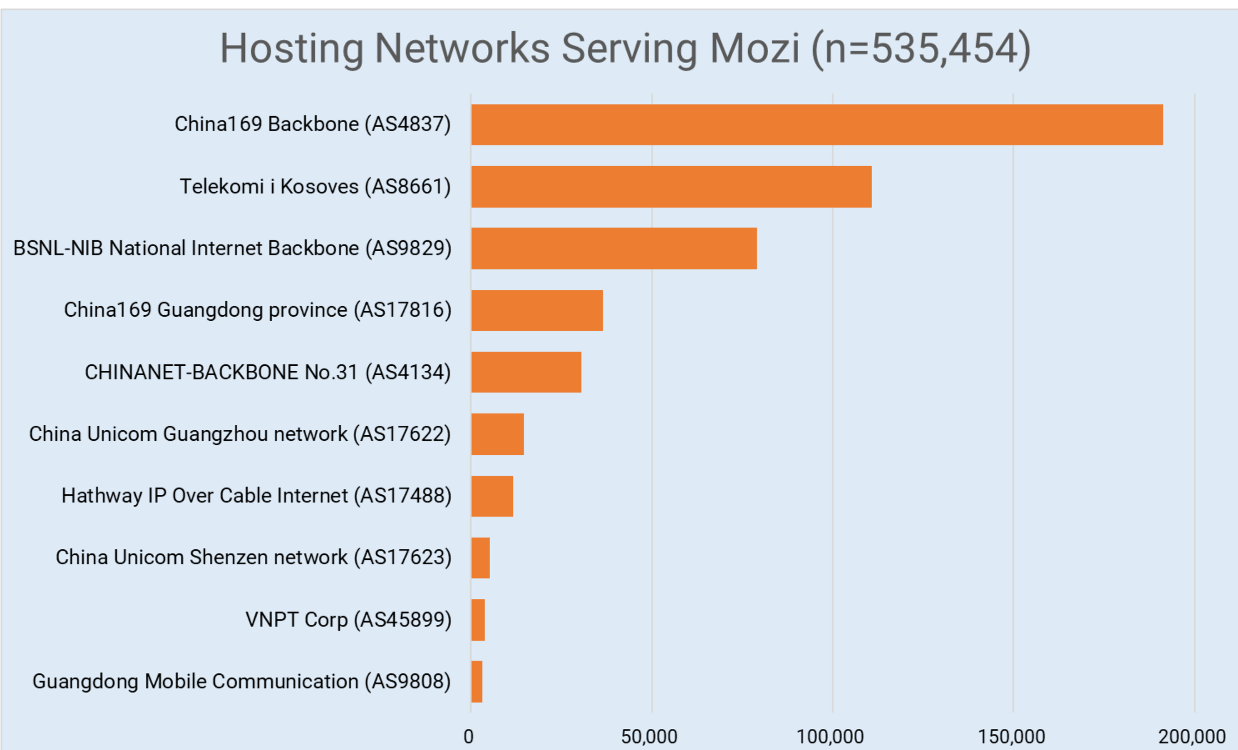


*Figure 8 Autonomous Systems with Large Numbers of Mozi P2P Bots, January – June 2021*

ASNs in China have the largest numbers of Mozi malware IoT bots. A10 Networks' October 2021 DDoS threat intelligence report includes China Unicom and China Telecom in its lists of top ASNs hosting DDoS Weapons. ASNs in Brazil, India, South Korea, and Venezuela are also included as top hosts of reflected amplification attacks.[32]

Figure 9 shows that China, India, Brazil, and Russia have the largest numbers of Mozi IoT Malware. This geographic distribution is consistent with an April 2020 study by Lumen Black Lotus Labs, who reported that "throughout the life of the Mozi botnet, the bulk of the nodes have been located in Asia".[33]

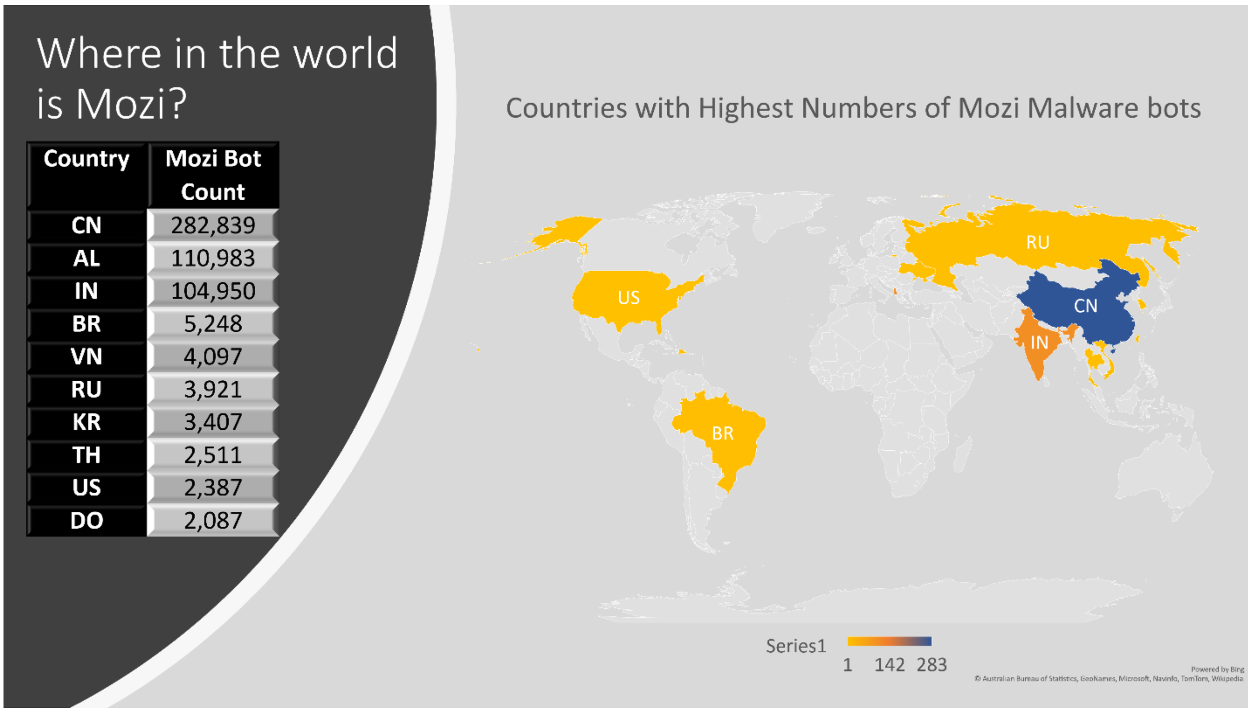


*Figure 9 Geographic Distribution of Mozi IoT Malware, January – June 2021*

## Endpoint Malware

An endpoint is a device – a laptop, phone, tablet, or server – that is connected to a network and used or administered by a user. Endpoint malware compromises these mostly human-attended devices through a user action such as the opening of an email attachment or the visiting of a malicious URL through a browser.

**Classifying Endpoint Malware is a highly subjective exercise**. There are few widely adopted norms for naming or typing malware and this creates challenges for anyone who is trying to measure malware. It also creates opportunities to focus attention on a particular type of malware such as ransomware.

For example, Interisle classifies the banking trojans Trickbot and Qakbot as information stealers. Others who report on ransomware, *e.g.*, Cybriant, classify these families as ransomware.[34] Changing the classifications of these two families affects the percentage of Malware Types reported: ransomware increases to 18% of the Types reported and infostealer decreases to 34%.

We could also affect the percentages by moving SMB from our classification as a loader to ransomware. This would be consistent with a US-CERT CISA Alert (TA17-132A), Indicators Associated with WannaCry

Ransomware,[35] which notes that "a hacker or hacking group behind the WannaCry campaign is gaining access to enterprise servers through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010 vulnerability on March 14, 2017". Changing the classification of SMB to ransomware further influences the percentages of Malware Types reported: ransomware now increases to 46% and loader decreases to 13%.

Figure 10 compares the effects that these changes to classification can have.

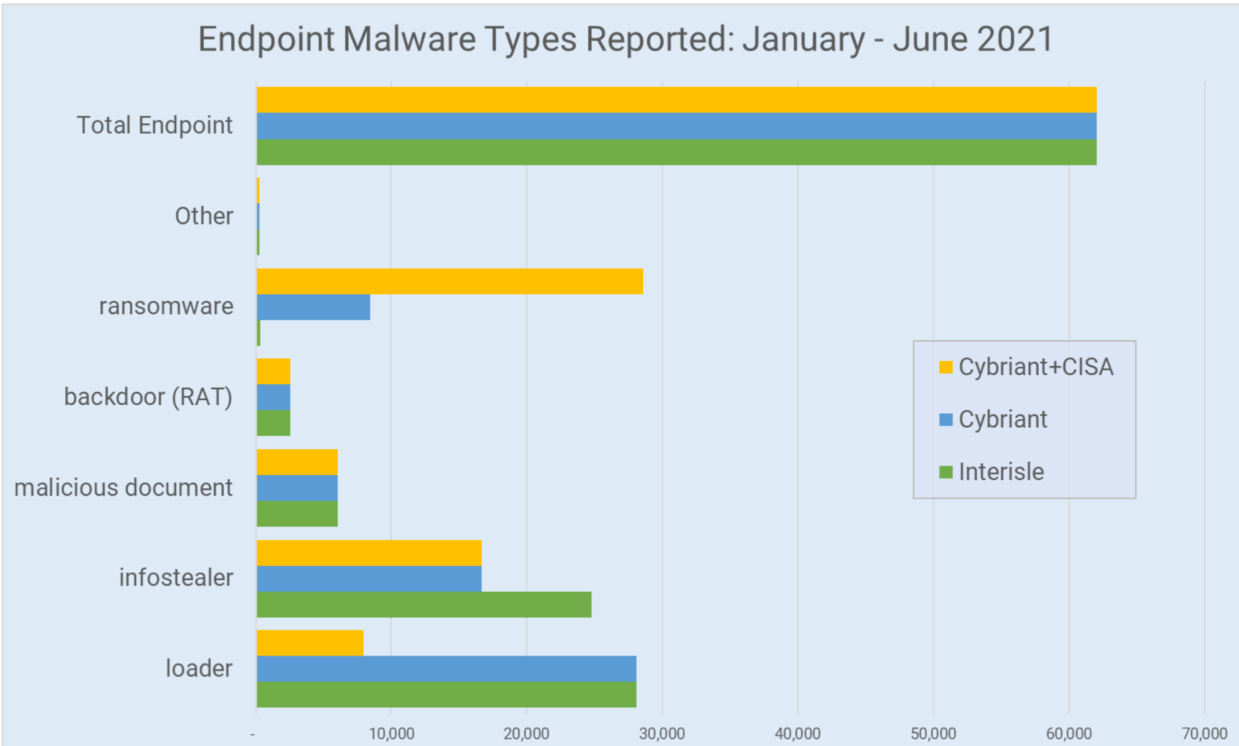


*Figure 10 Types of Endpoint Malware Reported, January – June 2021*

Malware classification is an imperfect science, and it can serve as an imperfect tool for calling attention to the prevalent malware problem of the moment. What we are able to learn from this exercise – is it an infostealer or ransomware? – is that how one classifies certain malware is relative and mostly unimportant. What is important is that the intent of the attacker is the same: whether by fraud or extortion, attackers seek financial rewards.

## Prevalent Endpoint Malware

The most frequently reported Endpoint Malware in our study data are described below:

**SMB**

SMB malware uses maliciously crafted traffic to exploit a vulnerability in the Server Message Block protocol.[36] Successful exploits allow remote code execution, access to sensitive data, and file sharing. Attackers have used SMB attacks to distribute Wannacry and other ransomware across entire networks.[37]

**Silent Builder**

A loader that embeds a Dynamic Link Library (DLL) [38] in an email attachment (Excel file) that is signed with a digital certificate. When the Excel file is opened, a macro spawns a loader which then attempts to download other malware, including Qakbot.[39]

**Dridex**

A banking trojan that is primarily used to steal customer login information, typically delivered as an email attachment in phishing campaigns. Dridex can compromise browsers, determine online banking applications and websites, and inject malware such as keyloggers.[40]

**Qakbot**

A banking trojan that has persisted in the wild since 2007, largely due to stealth and self-propagating characteristics. It behaves as a man-in-the-middle browser – it alters what victims see when they visit a bank web site and captures bank credentials and online session information.[41]

**Ryuk**

Ryuk ransomware encrypts and locks files and then extorts victims for a ransom in exchange for decryption keys. Malwarebytes notes that Ryuk can “identify and encrypt network drives and resources, as well as delete shadow copies on the endpoint”, which makes recovery harder or impossible for victims.[42]

**Formbook**

An infostealer that is offered as a malware as a service (Maas) platform. ANY.RUN’s characterization of FormBook as “attractive to attackers, with low technical literacy, sold as a control panel, available on highly accessible online forums, for 30 dollars” [43] illustrates how far ransomware (and malware) have matured as profitable enterprises.

**GuLoader**

GuLoader is a downloader family that is distributed through spam campaigns as an encrypted executable in an archive attachment. When the archive is opened, the loader installs and then typically downloads other malware from Google Drive or Microsoft OneDrive.[44]

**Hancitor**

Embeds a DLL in an email attachment (Word document). When the document is opened a macro spawns a loader which then attempts to download other malware including CobaltStrike or Ficker.[45] Recent campaigns impersonate DocuSign.[46]

**Flubot**

An Android banking trojan that steals banking app or cryptocurrency account credentials. Flubot lures victims by impersonating shipping and delivery companies in SMS text messages.[47] The trojan also steals contact data that the attacker will use in subsequent SMS text messages.

Figure 11 shows the counts of the most frequently reported Endpoint Malware in our study data.

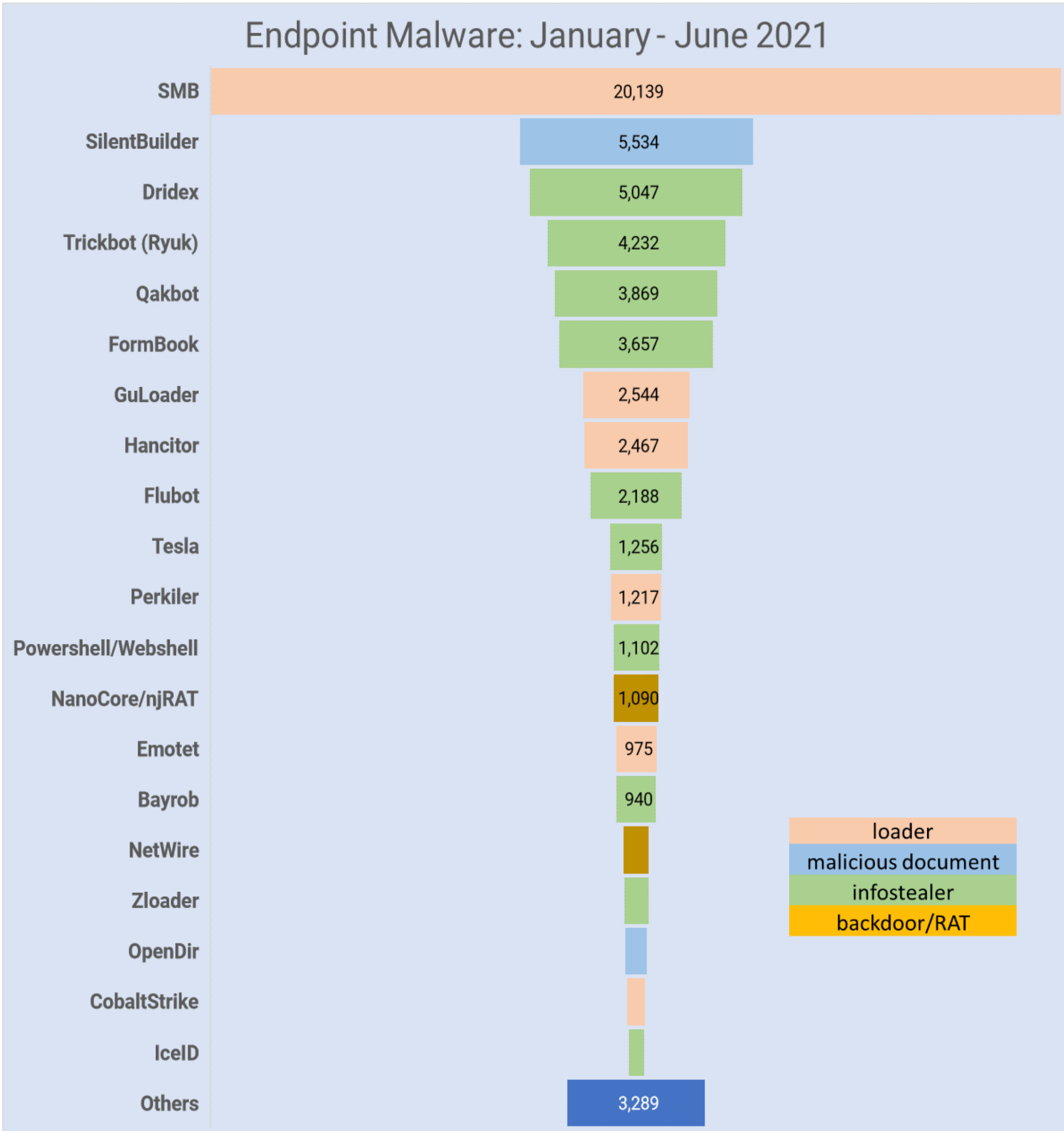


*Figure 11 Most Prevalent (named) Malware*

Table 2 shows the ASNs where the most reported Endpoint Malware were hosted.

| Malware Reported | AS name | AS # | Occurrences | Percent |
|---|---|---|---|---|
| SMB | VNPT-AS-VN VNPT Corp | 45899 | 1,187 | 6% |
| | TELKOMNET-AS-AP PT | 7713 | 958 | 5% |
| Silent Builder | UNIFIEDLAYER-AS-1 | 46606 | 1,579 | 29% |
| | PUBLIC-DOMAIN-REGISTRY | 394695 | 618 | 11% |
| Dridex | UNIFIEDLAYER-AS-1 | 46606 | 1,137 | 23% |
| | PUBLIC-DOMAIN-REGISTRY | 394695 | 260 | 5% |
| Qakbot | UNIFIEDLAYER-AS-1 | 46606 | 1,454 | 38% |
| | CLOUDFLARENET | 13335 | 673 | 18% |
| Ryuk | ITLDC-NL - ITL LLC | 21100 | 2,254 | 56% |
| | UNIFIEDLAYER-AS-1 | 46606 | 1,310 | 32% |
| FormBook | GOOGLE | 15169 | 682 | 19% |
| | AMAZON-02 | 16509 | 304 | 8% |
| GuLoader | GOOGLE | 15169 | 1,055 | 42% |
| | MICROSOFT-CORP-MSN | 8068 | 607 | 24% |
| Hancitor | GOOGLE | 15169 | 1,090 | 42% |
| | DIMENOC | 33182 | 287 | 11% |
| Flubot | CLOUDFLARENET | 13335 | 538 | 25% |
| | DIGITALOCEAN-ASN | 14061 | 162 | 8% |

*Table 2 Where Were the Top Endpoint Malware Hosted?*

Four ASNs — CLOUDFLARENET, GOOGLE, MICROSOFT-CORP-MSN-AS-BLOCK, and UNIFIEDLAYER-AS-1 – hosted significant percentages of two or more of the endpoint malware listed in Table 2. We found that:

- A ThreatMark analysis[48] revealed that the Flubot banking trojan used DNS over HTTPS (DOH) to resolve algorithmically generated domains of its command-control (C2) servers and "first evolutions" of the malware used CloudFlare's service exclusively (AS 13335, CLOUDFLARENET). This is an example of how encryption intended to provide protection for privacy-sensitive users is misused to hide communications between info-stealing clients and an attacker's C2.
- A Crowdstrike analysis of the GuLoader malware revealed that this loader stored encrypted payloads on Google Drive and Microsoft OneDrive to evade detection.[49] Crowdstrike further explains that GuLoader was used to distribute AgentTesla, FormBook, and NanoCore. The percentages of these malware hosted at AS 15169, GOOGLE and AS 8068, MICROSOFT-CORP-MSN-AS-BLOCK are consistent with this analysis.
- Seclytics Threat Intelligence has identified malicious activity hosted on IP addresses throughout address delegations assigned to AS 46606, UNIFIEDLAYER-AS-1 since 2014. The screenshot in Figure 12 shows that malicious activities continue to be pervasive in this ASN.

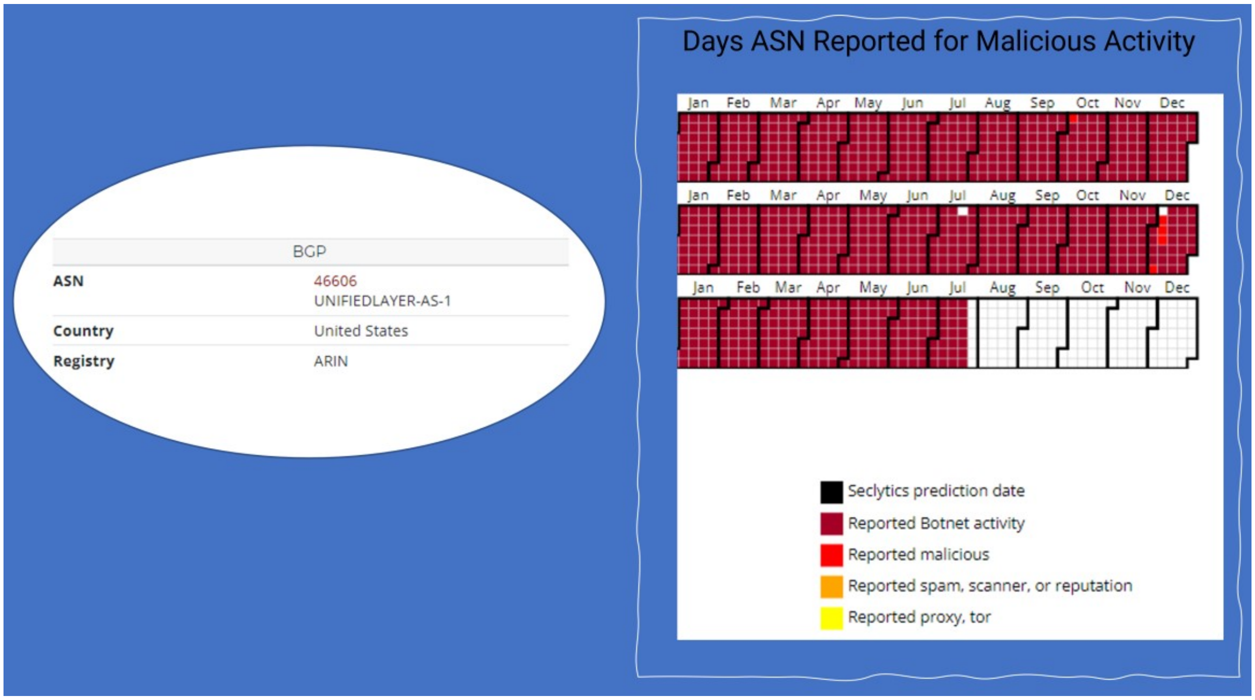


*Figure 12 Snapshot of Seclytics Threat Report, AS46606*

## Malware Reported by Hosting Networks (Autonomous Systems)

An Autonomous System (AS) is a collection of the IP addresses (routing prefixes) controlled by a common network administrator. That administrator may be a hosting provider, a business, a university, an Internet Service Provider, or a network operator providing service to several of those types of entities. Each Autonomous System is assigned a unique AS number (ASN) for routing and identification purposes. It is common for larger hosting services and cloud services to have several AS numbers. Business and operational practices may cause an Autonomous System (and number) to be transferred from one service provider to another (*e.g.*, following an acquisition or divestiture). An AS and its number may be re-allocated because of other events (*e.g.,* bankruptcy or business closure). Considering this churn, we report on individual hosting networks (ASNs).

We studied sites where malware was served from or distributed. We collected the IP addresses (A records) that reported malware were resolving to. We then looked up what autonomous system (AS) each IP address was in. This provides insight into the operators that hosted the reported malware.

We did not see malware on IPv6 addresses; the following sections are about IPv4 addresses only.

### Ranking of Hosting Networks (ASNs) by All Malware Reported

Table 3 shows where we identified hosting networks where large numbers of addresses were identified as serving or distributing malware.

| Rank | AS Name | AS Number | # Routed IPv4 Addresses | Total Malware Records ▼ |
|---|---|---|---|---|
| 1 | CHINA169-BACKBONE CHINA UNICOM | 4837 | 58,760,448 | 226,689 |
| 2 | PTK - Telekomi i Kosoves SH.A. | 8661 | 84,224 | 130,422 |
| 3 | BSNL-NIB National Internet Backbone | 9829 | 10,840,832 | 92,540 |
| 4 | CHINA169-GZ China Unicom Guangdong | 17816 | 3,948,288 | 38,928 |
| 5 | CHINANET-BACKBONE No.31 | 4134 | 115,596,032 | 36,983 |
| 6 | CNCGROUP-GZ China Unicom Guangzhou | 17622 | 1,352,960 | 15,101 |
| 7 | HATHWAY-NET-AP Hathway IP Over Cable | 17488 | 999,680 | 12,522 |
| 8 | UNIFIEDLAYER-AS-1 | 46606 | 1,393,664 | 10,474 |
| 9 | CLOUDFLARENET | 13335 | 2,353,664 | 9,987 |
| 10 | CNCGROUP-SZ China Unicom Shenzen | 17623 | 953,856 | 6,251 |
| 11 | VNPT-AS-VN VNPT Corp | 45899 | 19,107,328 | 5,780 |
| 12 | AS-COLOCROSSING | 36352 | 783,616 | 5,451 |
| 13 | GOOGLE | 15169 | 23,095,552 | 4,657 |
| 14 | CMNET-GD Guangdong Mobile | 9808 | 62,860,800 | 4,539 |
| 15 | DIGITALOCEAN-ASN | 14061 | 2,553,088 | 4,284 |
| 16 | KIXS-AS-KR Korea Telecom | 4766 | 69,337,344 | 3,619 |

| Rank | AS Name | AS Number | # Routed IPv4 Addresses | Total Malware Records ▼ |
|---|---|---|---|---|
| **17** | TOT-NET TOT Public Company | 23969 | 5,654,272 | 3,561 |
| **18** | MTNL-AP Mahanagar Telephone Nigam | 17813 | 2,744,320 | 3,426 |
| **19** | WIND Telecom S.A. | 27887 | 63,744 | 3,317 |
| **20** | ASIANET Cable ISP in India | 17465 | 116,736 | 2,955 |

*Table 3 Ranking of Malware Hosting Networks (ASNs), January – June 2021*

Seclytics Threat Intelligence has identified significant botnet activity hosted on IP addresses throughout address delegations assigned to the top-ranked AS4837, CHINA169-BACKBONE CHINA UNICOM since 2015. The screenshot in Figure 13 shows that malicious activities continue to be pervasive in this ASN.

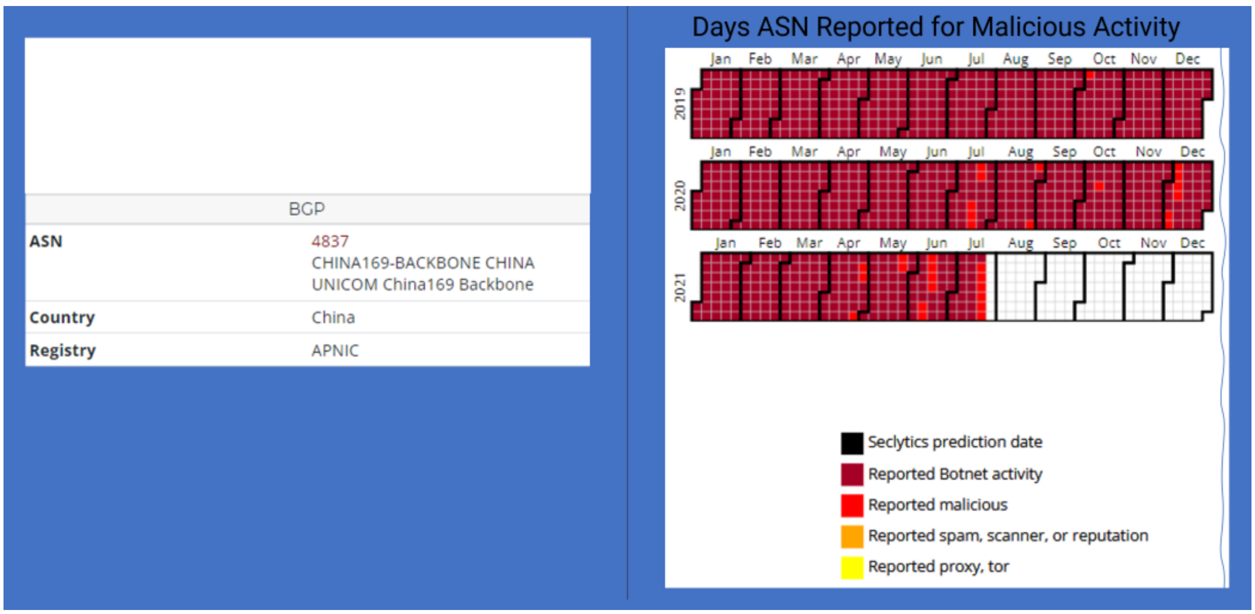


*Figure 13 Botnet Activity in AS4837 2019-2021, as Reported by Seclytics*

Some ASNs do not appear in the ranking but have very high counts of reported malware relative to their address delegations. Most notable among these are:

- PTK - Telekomi i Kosoves SH.A. (AS8661, with 84,224 addresses but 130,422 malware records)
- WIND Telecom S.A. (AS27887, with 63,744 addresses and 3,317 malware records)
- ASIANET Cable ISP in India (AS17465, with 116,736 addresses and 2,955 malware records)
- PONYNET (AS53667, with 69,672 addresses and 1,053 malware records)
- BEAMTELE-AS-AP ACTFIBERNET (AS131269, with 180,480 addresses and 2,300 malware records)

## Where do we Find Endpoint Malware in the Hosting World?

We determined that the following ASNs had the highest number of records identifying IP addresses that were serving these Endpoint Malware Types:

### Infostealers

**AS46606 UNIFIEDLAYER-AS-1: 4,178 records**
- 1,137 Dridex
- 1,454 Qakbot
- 1,310 Ryuk

**AS21100 ITLDC-NL – ITL: 2,280 records**
- 2,254 Ryuk

**AS13335 CLOUDFLARE-NET 2,023 records**
- 673 Qakbot
- 538 flubot

**AS 15169, GOOGLE: 1,652 records**
- 682 Formbook
- 559 Zloader

### Loaders

**AS15169 GOOGLE:  2,198 records**
- 1,055 GuLoader
- 1,088 Hancitor

**AS45899 VNPT-AS-VN: 1,191 records**
- 187 SMB

**AS7713 TELKOMNET-AS-AP: 965 records**
- 958 SMB

### Backdoor/RAT

**AS19679 DROPBOX: 1,099 records**
- 501 NanoCore/njRAT
- 591 NetWire

**AS8068 MICROSOFT-CORP-MSN: 440 records**
- 357 NanoCore/njRAT

### Malicious document

**AS46606 UNIFIEDLAYER-AS-1: 1,585 records**
- 1,579 SilentBuilder

**AS394695 PublicDomainRegistry: 619 records**
- 618 SilentBuilder

**AS26496 GODADDY.COM: 434 records**
- 432 SilentBuilder

## Where do we Find IoT Malware in the Hosting World?

We also determined that the following ASNs had the highest number of records identifying IP addresses that were serving IoT Malware.

### Mozi Malware

Mozi IoT malware was distributed across many hosting networks. Figure 14 shows the five ASNs with the most IP addresses reported for serving Mozi malware, representing 84% of all Mozi records. Three of these hosting networks are based in China, one in India, and one in Albania. Mozi malware accounted for 80-95% of IoT malware reported in these five ASNs.

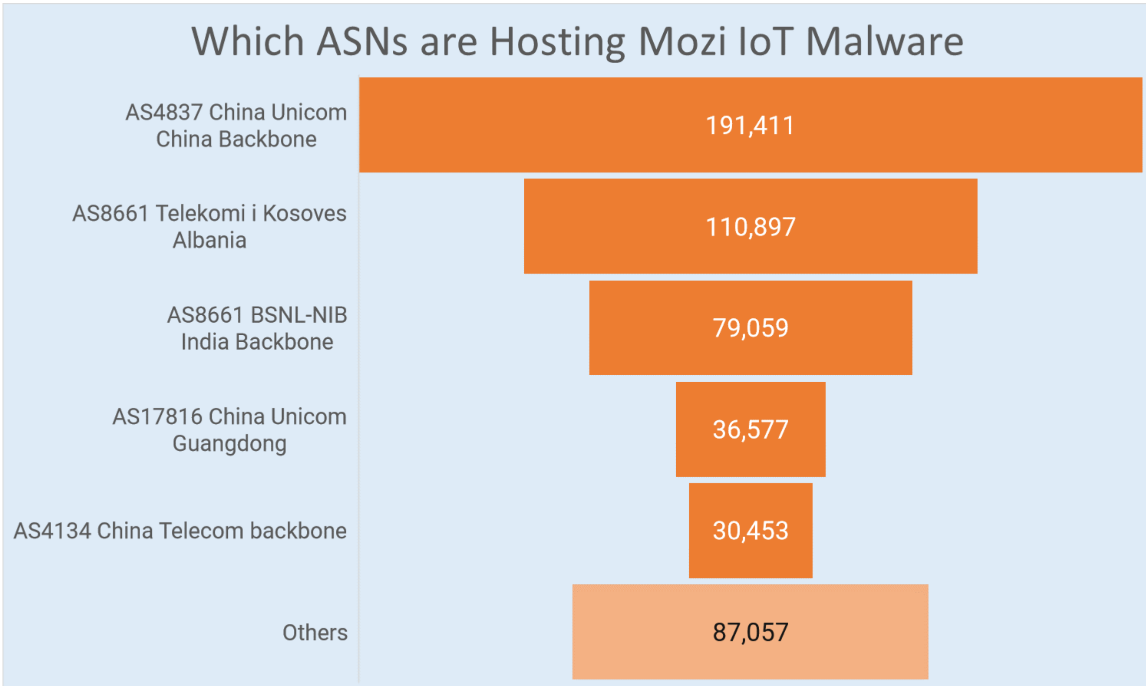


*Figure 14 Top 5 ASNs Hosting Mozi IoT Malware*

Of the 535,454 records identifying IP addresses that were serving Mozi,

- 191,411 records (36%) were in AS4837 (84% of all that ASN's records were identified as Mozi),
- 110,897 records (21%) were in AS8661 (85% of that ASN's records were identified as Mozi),
- 79,059 records (15%) were in AS9829 (81% of that ASN's records were identified as Mozi),
- 36,577 records (7%) were in AS17816 (94% of that ASN's records were identified as Mozi), and
- 30,453 records (6%) were in AS4134 (82% of that ASN's records were identified as Mozi).

We examine Mozi in some detail in the section Peer-to-Peer IoT Malware Case Study: Mozi.

We observed two other types of IoT Malware with numbers much smaller than Mozi but sufficient to merit analysis – Gafgyt and Mirai.

## Gafgyt Malware

Gafgyt IoT malware was distributed across many hosting networks. Of the 4,480 records identifying IP addresses that were serving Gafgyt,

- 977 records (22%) were in AS36352 COLOCROSSING and
- 844 records (19%) were in AS14061 DIGITALOCEAN-ASN.

## Mirai Malware

Like Gafgyt, Mirai malware was also widely distributed. Of the 3,794 records identifying IP addresses that were serving Mirai,

- 624 records (16%) were in AS36352, COLOCROSSING and
- 465 records (12%) were in AS21305 AS-SERVERION - Des Capital B.V.

## Where do we Find Uncategorized Malware in the Hosting World?

CLOUDFLARE-NET had 461,884 records that we were unable to classify, by far the largest number. Of these 456,176 (99%) identified the IP address 172.67.192.114. We discuss this outlying case in the section Malware in File Sharing and Code Repositories.

## Malware Domains Reported by Top-Level Domain (TLD)

The Q2 2021 Verisign Domain Name Industry Brief[50] reported that there were 367.3 million domain names in the world's registries. The overall domain name space can be divided into four types and is illustrated in the left half of Figure 15.

- .COM and .NET registries, operated by Verisign, represented 47% of the domains in the world.
- Country-code domains (ccTLDs) represented 43% of the world's domains.
- Legacy generic TLDs (those other than .COM and .NET and introduced before 2014, *e.g.,* .ORG, .BIZ, .INFO, .MOBI, etc.) represented 4% of the domains.
- New gTLDs (nTLDs) introduced from 2014 to the present represented the remaining 6%.

We analyzed the 35,181 unique domains that appeared in malware records to see how they were distributed across the top-level domains. Figure 15 compares the market share of the four TLD types to the percentage of domain names reported for serving malware against each type.

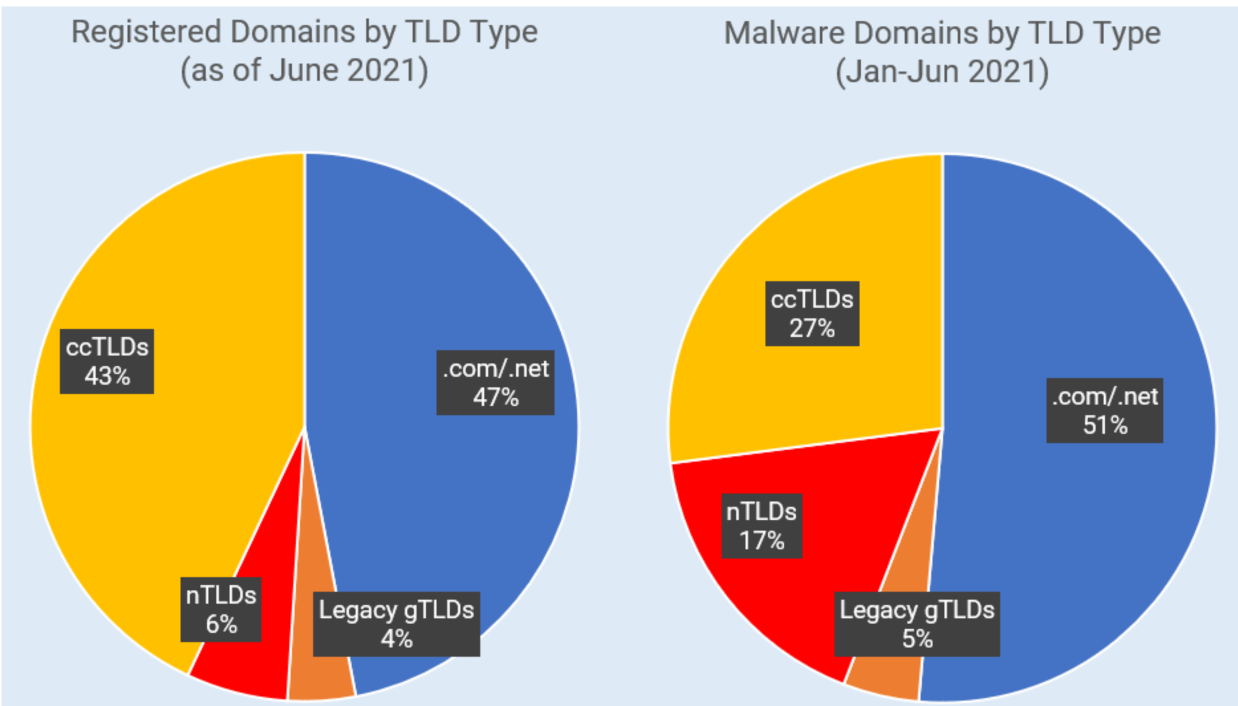


*Figure 15 TLD Market Share vs. Malware Reported, by TLD Type, January – June 2021*

The most noteworthy observations from the Figure are:

1. **The new gTLDs are only 6% of the market, but they contained 16% of the domain names reported for serving malware.**

2. The ccTLDs have attracted less attention from malware attackers. **While the ccTLDs represent 43% of the market, they contained only 28% of the domain names reported for serving malware.**

## Ranking of All TLDs by Malware Domains Reported

Table 4 ranks all TLDs (legacy, ccTLD, and new) by the total number of unique domain names that were reported for serving or hosting malware during our study period.

| Rank | TLD | Total Malware Domains ▼ |
|---|---|---|
| 1 | com | 15,906 |
| 2 | net | 2,225 |
| 3 | ru | 1,917 |
| 4 | xyz | 1,226 |
| 5 | br | 859 |
| 6 | org | 781 |
| 7 | buzz | 754 |
| 8 | top | 691 |
| 9 | in | 602 |
| 10 | cn | 466 |
| 11 | рф | 461 |
| 12 | info | 441 |
| 13 | uk | 304 |
| 14 | co | 264 |
| 15 | online | 253 |
| 16 | de | 249 |
| 17 | us | 244 |
| 18 | vip | 203 |
| 19 | za | 187 |
| 20 | biz | 186 |

Table 4 Ranking of Malware TLDs, by Unique Malware Domains, January – June 2021

In the discussion below, we note that the numbers indicate that malware existed in certain TLDs at rates higher than would be expected given their sizes, and conversely, in some TLDs, we observed lower rates than would be expected.

| | | |
|---|---|---|
| #1 | .COM | .COM is by far the largest and best-known TLD (157.5 million delegated domains). Due to its size and age, .COM should be expected to contain many of the domains that are compromised by criminals and used to harbor malware. |
| #2 | .NET | .NET is .COM's large sibling TLD, (13.3 million delegated domains). As for .COM, we expect .NET to contain many domains that are compromised by criminals to harbor malware. |
| #3 | . RU | . RU, the ccTLD of the Russian Federation, is the ninth largest TLD in the world, (4.9 million domains). Of the .RU domains with categorized malware appearing on them, the majority were flagged for harboring Cobalt Strike. Cobalt Strike is a paid penetration testing product that has been co-opted by criminals and allows an attacker to deploy an agent named "Beacon" on the victim machine. Beacon includes a wealth of functionality to the attacker, including command execution, keylogging, file transfer, SOCKS proxying, privilege escalation, and lateral movement.[51] The domain names were composed of three words (such as priceexperttry.ru and easypriceday.ru) and were likely registered by criminals, who used them to run the malware. |
| #4 | .XYZ | .XYZ, is one of the new gTLDs introduced in 2014 (3.4 million domains). The malware related to .XYZ domains was in a variety of families, including the banking trojans Trickbot and Dridex, SilentBuilder, and FormBook. FormBook is a keylogger that is sometimes delivered by phishing emails.[52] Many of the .XYZ domains involved appear to be maliciously registered –composed of random characters (*e.g.*, c2t6yg19yj3ern2g.xyz) or misspelled words appended with numbers (*e.g.*, fullvehdvideopleyer637.xyz). |
| #5 | .BR | .BR is the ccTLD of Brazil, ( 4.7 million domains). Of the .BR domains with categorized malware appearing on them, 70% were associated with Dridex and SilentBuilder. |
| #13 | .UK | .UK is the ccTLD of the United Kingdom, (11 million domains). .UK domains were compromised or registered by malware-operating criminals at a lower rate than many other TLDs. |
| #16 | .DE | .DE is the ccTLD of Germany, is the fourth largest TLD in the world (17 million domains). While it is a very large TLD (and therefore has active domains in it theoretically vulnerable to compromise), .DE domains are compromised or registered by malware-operating criminals at a lower rate than many other TLDs. |

The absence of domains used to disseminate IoT malware is notable: only two domains were used to disseminate IoT malware – one in .COM and one in .XYZ.

Of the top 20 TLDs ranked by malware domains reported, five are new gTLDs introduced after 2013 (.XYZ, .BUZZ, .TOP, .ONLINE, .VIP). Three are from the legacy TLDs — .COM, .NET, .ORG – and two are gTLDs introduced in 2001: .INFO and .BIZ. One is an Internationalized Domain Name, .рф (or .RU in Cyrillic). The remaining nine are ccTLDs: .RU, .BR, .IN, .CN, .UK, .CO, .DE, .US, and .ZA).

Among the top-ranking gTLDs, .BUZZ is notable because it had the seventh-most malware domains, but is a small TLD with only about 271,000 domains in it. Most of the .BUZZ domains appear to have been registered purposely for serving malware: they are conspicuously composed of either two random words (*e.g.*, bellyweek.buzz, hormonesol.buzz) or deliberate misspellings (bloodfloows.buzz, growssmooht.buzz).

## Malware Domains Reported, by gTLD Registrar

Malware attackers acquire domain names by registering names purposely for malware. They also break into the domain name management accounts or the hosting accounts of domain name owners in order to compromise (seize control of) their domains.

### Ranking of gTLD Registrars by Malware Domains Reported

Table 5 ranks gTLD registrars by the number of domain names reported for serving malware in their domains under management.

| Rank | IANA_ID | Registrar | Total Malware Domains ▼ |
|---|---|---|---|
| 1 | 146 | GoDaddy.com, LLC | 6,315 |
| 2 | 1068 | NameCheap, Inc. | 3,381 |
| 3 | 303 | PDR Ltd. d/b/a PublicDomainRegistry.com | 2,291 |
| 4 | 1479 | NameSilo, LLC | 2,254 |
| 5 | 69 | Tucows Domains Inc. | 1,392 |
| 6 | 48 | eNom, LLC | 1,085 |
| 7 | 420 | Alibaba Cloud Computing (Beijing) Co., Ltd. | 933 |
| 8 | 1606 | Registrar of Domain Names REG.RU LLC | 793 |
| 9 | 49 | GMO Internet, Inc. d/b/a Onamae.com | 768 |
| 10 | 472 | Dynadot, LLC | 740 |
| 11 | 955 | Launchpad.com Inc. | 448 |
| 12 | 2 | Network Solutions, LLC | 391 |
| 13 | 1647 | Hosting Concepts B.V. d/b/a Registrar.eu | 379 |
| 14 | 625 | Name.com, Inc. | 376 |
| 15 | 1331 | eName Technology Co., Ltd. | 335 |
| 16 | 440 | Wild West Domains, LLC | 322 |
| 17 | 269 | Key-Systems GmbH | 315 |
| 18 | 1154 | FastDomain Inc. | 312 |
| 19 | 1469 | Jiangsu Bangning Science & technology Co. Ltd. | 309 |
| 20 | 120 | Xin Net Technology Corporation | 246 |

*Table 5 Ranking of Registrars, by Unique Domains, January – June 2021*

#1 GoDaddy and #2 NameCheap are the two largest gTLD registrars. GoDaddy had almost twice as many malware domains as NameCheap, but GoDaddy sponsors more than five times the number of gTLD domains (65.7 million) as NameCheap (12.7 million).

There is an Endpoint Malware nexus among the malware domains registered using NameCheap and GoDaddy:

- We identified 26 species of malware on GoDaddy's domains. Banking trojans Formbook and Dridex, and the SilentBuilder loader (which typically downloads the banking trojan, Qakbot) were associated with approximately half of the GoDaddy domains that were reported for serving malware.
- The malware on NameCheap's domains was more diverse, where we identified 39 malware species. The malware species here was also more diffuse. The most numerous – Ryuk (a type of ransomware), and two banking trojans, Dridex and Formbook – accounted for 19%+ of the malware domains at NameCheap.

NameSilo is the eleventh largest gTLD registrar (with 3.7 million domains under management) but had the third-most malware domains.

Notably (and perhaps commendably) absent from the top 20 is Google Domains (IANA ID 895), which is the sixth largest gTLD registrar, with more than 6 million domains under management. Also absent was 1&1 Ionos (IANA ID 83), the tenth largest gTLD registrar, with more than 4.8 million gTLD domains under management.

## Malware in File Sharing and Code Repositories

456,182 URLs from records in our malware data set contained the domain name anonfiles.com. We treat them separately here for several reasons.

Including these in our measurements would skew rankings throughout our report; in particular, they would bias ASN rankings and domain registrar rankings, affecting Cloudflare and Tucows, respectively, and not in a sound way.

Further, we were unable to include these records in our taxonomic ranking: we had insufficient metadata to (i) classify the malware, or (ii) definitively explain how the files hosted at this anonymous file sharing service were used. For example, sharing these files with the intent to make them available for download (infection) is only one of several purposes.

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 — in some cases, under the guise of making penetration testing software available. For example:

- Malwarebytes blocks subdomains of anonfiles.com that were found to host malware.[53]
- Sophos and Avast have identified malware (malicious scanner) at Github.[54, 55]
- Fortinet Labs Threat Research Report revealed how malware writers "store part of the malicious content from their malware, and then fetch it later from inside the malicious executable using the share link".[56]

Given the large number of URLs containing anonfiles.com in our data set, we include a case study here.

### Case Study: Anonfiles.com

Anonfiles requires registration but does not collect personal identifying information or an email address to satisfy anonymity needs or wants. The service also obfuscates IP addresses of users to prevent tracking. A registered user can upload a file, and anonfiles provides a "unique URL that the user can share with [any] others who can then download the file instantly".[57]

To understand the URL composition, we created an account and uploaded the text file "benign.txt". Anonfiles returned the URL https://anonfiles.com/t8qbhaP7ub/benign_txt when the upload was completed. Using the anonfiles.com API,[58] we confirmed that that the URL Path element /t8qbhaP7ub following the domain name is a file identifier. We shared the shortened URL https://anonfiles.com/t8qbhaP7ub/ to confirm that any party could download the file.


*Figure 16 Anonfiles Download Page*

We queried the anonfiles API and obtained the file names of 129,670 of the 456,182 occurrences in the malware URLs. We then used resources at Any.run,[59] Hybrid Analysis,[60] Virus Total,[61] and Process Library [62] to identify the malware activity that cause the URL to be blocklisted. We found

- 64,110 URLs that served up the Nethell keylogger,[63]
- 55,184 URLs that served the banking trojan clipbanker,[64] and
- 4,348 URLs that served up an executable that makes connections to malicious IP addresses.[65]

We received “file not found” errors for the others. The anonfiles FAQ says that files remain online “For as long as possible unless the file violates our Terms of Use”.[66] The anonfiles Terms of Service [67] forbids the “spread” of viruses, trojans, and corrupt and/or illegal material, and the site provides a form to report abuse.[68] Anonfiles does appear to remove content that it forbids. Further study is needed to determine the timeliness of abuse mitigation. It is evident that this anonymous file sharing service is used for malware activity, and ongoing analysis may tell us whether the activity is persistently present.

## Malware and Phishing

We compared how operators rank with respect to serving malware versus how they ranked in our Phishing Landscape 2021 study.[69]

Table 6 presents a side-by-side view of the Top 10 hosting networks for phishing attacks against the Top 10 hosting networks for serving or distributing malware.

| Hosting Networks (ASNs) | | |
|---|---|---|
| Rank | Phishing | Malware |
| **1** | NAMECHEAP-NET | CHINA169-BACKBONE CHINA UNICOM Backbone |
| **2** | CLOUDFLARENET | PTK - Telekomi i Kosoves SH.A. |
| **3** | UNIFIEDLAYER-AS-1 | BSNL-NIB National Internet Backbone |
| **4** | GOOGLE | CHINA169-GZ China Unicom Guangdong |
| **5** | DIGITALOCEAN-ASN | CHINANET-BACKBONE No.31 |
| **6** | AWEX - Hostinger | CNCGROUP-GZ China Unicom Guangzhou |
| **7** | OVH - OVH SAS | HATHWAY-NET-AP Hathway IP Over Cable |
| **8** | WEEBLY | UNIFIEDLAYER-AS-1 |
| **9** | CONTABO - Contabo GmbH | CLOUDFLARENET |
| **10** | AMAZON-02 | CNCGROUP-SZ China Unicom Shenzen |

*Table 6 Comparison of Phishing Attacks vs. Malware Hosting, by Hosting Network*

CLOUDFLARENET and UNIFIEDLAYER-AS-1 rank among the top 10 for both cybercrimes.

Table 7 (left) presents a side-by-side view but of Top 10 TLDs. We see that .COM,.CN, .NET, and .TOP rank in the Top 10 TLDs for both phishing attacks and serving or distributing malware. Lastly, Table 7 (right) presents a side-by-side view but of the Top 10 gTLD registrars. Here, we observe that the Top 5 are the same for both phishing attacks and serving malware.

| Top-level Domains (TLDs) | | |
|---|---|---|
| Rank | Phishing | Malware |
| **1** | com | com |
| **2** | tk | net |
| **3** | xyz | ru |
| **4** | ml | xyz |
| **5** | ga | br |
| **6** | cf | org |
| **7** | gq | buzz |
| **8** | cn | top |
| **9** | top | in |
| **10** | net | cn |

| Domain Registrars | | |
|---|---|---|
| Rank | Phishing | Malware |
| **1** | NameCheap | GoDaddy |
| **2** | NameSilo | NameCheap |
| **3** | GoDaddy | PDR |
| **4** | PDR | NameSilo |
| **5** | Tucows | Tucows |
| **6** | Wild West Domains | eNom |
| **7** | Google | Alibaba Cloud |
| **8** | GMO Internet | REG.RU |
| **9** | Name.com | GMO Internet |
| **10** | WebNic.cc | Dynadot |

*Table 7 Comparison of Phishing Attacks vs. Malware Hosting, by TLD and by Domain Registrars*

# Appendix A: Data Sources and Methodology

The use of DNS blocklists to track and measure Internet abuse has a long history, and collating data reported by multiple sources is a standard procedure in academic and professional cybercrime studies.[70, 71, 72, 73, 74] To find malware attacks, blocklist operators use several techniques, including capturing spam email lures, reports from user, and heuristics that examine a variety of data and signals.

The following sources of malware-specific data were chosen because they are used by a wide variety of organizations to protect users, have low false-positive rates, and have meta-data that is useful for studies such as ours.[75, 76, 77]

> **Malware Patrol.**[78] We use Malware Patrol's Business Protect feed for ransomware and malware infection threat data. The feed is aggregated from diverse sources, including web crawlers, botnet monitors, spam traps, honeypots, research teams, partners, and historical data about malicious campaigns.
>
> **MalwareURL.**[79] The MalwareURL database uses proprietary software and analytic techniques to locate, assess and monitor suspected sources of web criminality, malware, Trojans and a multitude of other web-related threats. The feed offers metadata that assists us in identifying malware types and families.
>
> **URLhaus.**[80] Operated by abuse.ch, the URLhaus Malware URL Exchange collects, tracks and shares malware URL submissions with security solution providers, antivirus vendors and blacklist providers, including Google Safe Browsing (GSB), Spamhaus DBL and SURBL. The feed offers metadata that assists us in identifying malware types and families.
>
> **Spamhaus Domain Block List (DBL).**[81] The Spamhaus Domain Block List (DBL) provides an rsync feed of registered domain names that have been associated with a malicious or criminal activity. For this study, we used only DBL-listed domains that were associated with two return codes: malware domain (127.0.1.5) and abused legit malware domain (127.0.1.105). We used as the discovery date the timestamp of each rsync access.

We collected data covering the period 1 January to 30 June 2021. We collected and analyzed only newly found malware incidents reported during that time. We downloaded updated data from Malware Patrol and Spamhaus three times a day, and from MalwareURL and URLhaus once a day. The, MalwareURL and URLhaus feeds include historical listings and contain timestamps of when each listing was created. Thus we did not miss any listings that appeared between the daily downloads and did not have to worry about a delay of hours between the time the blocklist provider add an entry to its list and when we downloaded those blocklist updates. The Malware Patrol and Spamhaus DBL are stateful and do not offer "time-of-listing" time stamps; it is possible that we missed some short-lived listings there.

## Data Feed Import and DNS Data

We collected reports from each feed at least once per day to find new entries. This collected data set then required curation to allow data from different sources to be stored together and compared. Each time a URL (or plain domain) was reported, we stored that as a separate feed entry. Some URLs were reported by more than one feed source.

UTC time is the time convention used by the four data sources, and in all gTLD registry and registrar systems including WHOIS. We used UTC.

Two of the feeds merely provided domain names or URLs with no other malware classification information. MalwareURL provides a single "Type" field that provides additional categorization for malware reports (such as "Trojan", "Trojan njRat", "Malicious Domain (ryuk)", or "Dridex botnet IP"). URLhaus provides a set of "Tags" that categorize the malware in various ways (for example, "bashlite,elf,gafgyt" or "exe,GuLoader"). More details on how we normalized the 'type' and 'tag' fields in the section Data Normalization below.

Some sources provided IP (A record) data and AS data. For every domain reported, we also queried DNS and separately stored the A record we found and determined the AS by using Team Cymru's IP to ASN mapping service.[82] We relied upon RIPE-NCC's WHOIS [83] to find ASN name, organization, and IP prefix. When we list the number of IPv4 addresses in an AS, that is a count of routed addresses.

To identify TLDs we used the IANA root zone list.[84] We used the Public Suffix List [85] to identify registered domain names (zones in which registries offer third level registration, such as example.co.uk).

The "legacy generic TLDs" introduced before 2013 (other than .COM and .NET) are: .AERO, .ASIA, .BIZ, .CAT, .COOP, .INFO, .JOBS, .MOBI, .MUSEUM, .NAME, .ORG, .POST, .PRO, .TEL, .TRAVEL, and .XXX.

For gTLD domain names we obtained registry WHOIS to identify the sponsoring registrar, along with the registrar's IANA ID [86] for normalization. Some gTLD registries severely rate-limited [87] our queries and made it impossible to obtain basic data about their domain names, including the domain registration date and the identity of the domain's sponsoring registrar. For this reason, some gTLD domain names were not attributable to registrars and do not appear in the malware-by-registrar tables and could not be included in the analysis of registration-to-malware times. We did not obtain WHOIS for ccTLD domains due to limited access and non-uniformity of WHOIS output. Also, ccTLD registrars are not identified via a uniform identifier across ccTLD registries, making the compilation of by-registrar statistics difficult.

## Data Normalization

We developed a set of mappings for each MalwareURL "Type" and each item in URLhaus "Tags" to identify a canonical Malware Type and Malware Name (see Figure 3). We were able to identify some MalwareURL types that were referring to cybercrimes outside the area of concern – for example, ones that relate to Botnet C&C. Some URLhaus malware reports include "Tags" that yield malware of multiple types; for example, "encrypted,GuLoader,NetWire" was determined to be both a "Loader" (GuLoader) and a "Backdoor/RAT" (NetWire). In these cases, we created two distinct malware records from the single feed entry, one for each Malware Type.

As we combined malware reports from multiple sources, we maintained any original feed categorization as well as the normalized Malware Type and Malware Name.

## Data Deduplication

Noting that multiple feeds can report the same malware URL, and also that a malware URL might be based on a domain name or a domain address, we processed the resulting malware records to remove duplicates (though retaining both MalwareURL Type and URLhaus Tag fields as appropriate).

# About the Authors

**Greg Aaron** is an internationally recognized authority on the use of domain names for cybercrime, and is an expert on domain name registry operations, DNS policy, and related intellectual property issues. Mr. Aaron is Senior Research Fellow for the Anti-Phishing Working Group. As a member of ICANN's Security and Stability Advisory Committee (SSAC), he advises the international community regarding the domain name and numbering system that makes the Internet function. He works with industry, researchers, and law enforcement to investigate and mitigate cybercrime, and is also a licensed private detective. He was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG) and has been a member of ICANN's EPDP Working Group, which has been creating registration data access policies. He was the senior industry expert on a team that evaluated the policy and technical qualifications of more than one thousand new TLD applications to ICANN in 2012-2013. He has created products and services used by organizations to discover and track Internet-based threats, and has managed large top-level domains around the world, including .INFO, .ME, and .IN. He is President of Illumintel, Inc., a consulting company. Mr. Aaron is a *magna cum laude* graduate of the University of Pennsylvania.

**Lyman Chapin** has contributed to the development of technologies, standards, and policy for the Internet since 1977, and is widely recognized and respected as a leader in the networking industry and the Internet community. Mr. Chapin is a Life Fellow of the IEEE, and has chaired the Internet Architecture Board (IAB), the ACM Special Interest Group on Data Communication (SIGCOMM), and the ANSI and ISO standards groups responsible for Network and Transport layer standards. Mr. Chapin was a founding trustee of the Internet Society and a Director of the Internet Corporation for Assigned Names and Numbers (ICANN). He currently chairs ICANN's Registry Services Technical Evaluation Panel (RSTEP), which is responsible for assessing the impact of new Domain Name System (DNS) registry services on the security and stability of the Internet, and the DNS Stability Panel, which evaluates proposals for new Internationalized Domain Names (IDNs) as country code top-level domains (ccTLDs). He is also a member of ICANN's Security and Stability Advisory Committee (SSAC). He has written many other papers and articles over the past 40 years, including the original specification of the Internet standards process operated by the IETF. Mr. Chapin holds a B.A. in Mathematics from Cornell University.

**David Piscitello** has been involved in Internet technology and security for more than 40 years. Until July 2018, Mr. Piscitello was Vice President for Security and ICT Coordination at ICANN, where he participated in global collaborative efforts by security, operations, and law enforcement communities to mitigate Domain Name System abuse. He also coordinated ICANN's security capacity-building programs and was an invited participant in the Organisation for Economic Co-operation and Development (OECD) Security Expert Group. Dave is an Associate Fellow of the Geneva Centre for Security Policy. He served on the Boards of Directors at the Anti-Malware Working Group (APWG) and Consumers Against Unsolicited Commercial Email (CAUCE). He is the recipient of M3AAWG's 2019 Mary Litynski Award, which recognizes the lifetime achievements of individuals who have significantly contributed to making the Internet safer.

**Dr. Colin Strutt** has published and spoken extensively on networking technology, name collisions, enterprise management, eBusiness, and scenario planning, and has represented the interests of Digital Equipment, Compaq, and the Financial Services Technology Consortium in national and international industry standards bodies. He holds six patents on enterprise management technology and brings more than forty years of direct experience with information technology, as a developer, architect, and consultant, with recent work including design and operation of a regional public safety network, providing technical expertise relating to patents, and analysis of world-wide Internet use. Dr. Strutt holds a B.A. (with First Class Honours) and Ph.D. in Computer Science from Essex University (UK).

## About Interisle Consulting Group, LLC

Interisle's principal consultants 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: [www.interisle.net](http://www.interisle.net)

## Acknowledgments

The authors extend thanks to:

- Spamhaus, Malware Patrol, URLhaus, and MalwareURL, for their contribution of data and data interpretation for this study.
- Domain Tools, for access to historical and bulk parsed WHOIS.
- Saeed Abu-Nimeh for access to the Seclytics Predictive Threat Intelligence platform.
- Malware subject matter experts at Malware Patrol, URLhaus, Malware URL, and at Netenrich and Bambenek Labs for their assistance with our effort to create a taxonomic ranking of malware.
- All the security personnel who fight malware.

# End Notes

[1] Malicious Software (Malware): A Security Threat to the Internet Economy
http://www.oecd.org/internet/ieconomy/40724457.pdf

[2] AV-TEST Institute
https://www.av-test.org/

[3] Combatting Ransomware, Institute for Security andTechnology
https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf

[4] Of the attacks reported so far in 2021, the breach of Colonial Pipeline (https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html) in late April had the most news coverage. Other high-impact attacks in 2021 targeted JBS Foods (https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html), Acer (https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/), and the Washington DC Metropolitan Police Department (https://apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9).

[5] Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021
https://www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf

[6] Nation States, Cyberconflict and the Web of Profit
https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf

[7] North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report
https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

[8] FBI Director Compares Ransomware Challenge to 9/11
https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003

[9] A botnet (from “robot network”) is a network of communicating devices infected by malware that allows them to be controlled by an attacker who can command every device in the botnet to simultaneously carry out a coordinated criminal action, such as a distributed denial of service attack.

[10] CARO - Computer Antivirus Research Organization
http://www.caro.org/index.html

[11] Convention on Cybercrime
https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/

[12] Refer to the Cybercrime Information Center, Measurements, for a mapping of the Convention's Articles and Guidelines onto cyber threats, including malware.
https://www.cybercrimeinfocenter.org/measurements

[13] What is RAT (remote access Trojan)? - Definition from WhatIs.com
https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan

[14] What Are Bots?
https://us.norton.com/internetsecurity-malware-what-are-bots.html

[15] CoinDesk: Bitcoin, Ethereum, Crypto News and Price Data
https://www.coindesk.com/tech/2021/01/06/this-elusive-malware-has-been-targeting-crypto-wallets-for-a-year/

[16] Cryptojacking – What is it, and how does it work?
https://www.malwarebytes.com/cryptojacking

[17] Malware spotlight: Droppers - Infosec Resources
https://resources.infosecinstitute.com/topic/malware-spotlight-droppers/

[18] Malware Loaders Continue to Evolve, Proliferate - Flashpoint
https://www.flashpoint-intel.com/blog/malware-loaders-continue-to-evolve-proliferate/

[19] What Are Infostealers?
https://blog.f-secure.com/what-are-infostealers/

[20] The Rise of Document based Malware - Data Threat Detection and Prevention
https://www.sophos.com/en-us/security-news-trends/security-trends/the-rise-of-document-based-malware.aspx

[21] What Is Ransomware?
https://www.icann.org/fr/blogs/details/what-is-ransomware-13-3-2017-en

[22] Malware names
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/malware-naming

[23] Anonfiles
https://anonfiles.com

[24] 2021 SonicWall Cyber Threat Report
https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf

[25] Motives Behind DDoS Attacks, Scott Traer, Peter Bednar, Digital Transformation and Human Behavior
https://link.springer.com/chapter/10.1007/978-3-030-47539-0_10

[26] Gafgyt Botnet Lifts DDoS Tricks from Mirai
https://threatpost.com/gafgyt-botnet-ddos-mirai/165424/

[27] Secure Shell (SSH)
https://searchsecurity.techtarget.com/definition/Secure-Shell

[28] What Is SSH and How Do Hackers Attack It
https://www.cyclonis.com/what-is-ssh-how-hackers-attack/

[29] New Mozi Malware Family Quietly Amasses IoT Bots
https://blog.lumen.com/new-mozi-malware-family-quietly-amasses-iot-bots/

[30] Mozi Botnet Accounts for Majority of IoT Traffic
https://threatpost.com/mozi-botnet-majority-iot-traffic/159337/

[31] IETF Recommendations for Transport-Protocol Port Randomization, RFC6065
https://datatracker.ietf.org/doc/html/rfc6056

[32] DDoS Attack Mitigation: A Threat Intelligence Report, A10 Networks
https://www.a10networks.com/wp-content/uploads/A10-EB-ddos-attack-mitigation-a-threat-intelligence-report.pdf

[33] New Mozi Malware Family Quietly Amasses IoT Bots, Lumen Black Lotus Labs
https://blog.lumen.com/new-mozi-malware-family-quietly-amasses-iot-bots

[34] Top Ransomware Threats of 2020
https://cybriant.com/top-ransomware-threats-of-2020/

[35] US Cybersecurity and Infrastructure Security Agency (CISA) Alert (TA17-132A) Indicators Associated With WannaCry Ransomware
https://us-cert.cisa.gov/ncas/alerts/TA17-132A

[36] MS17-010: Security update for Windows SMB Server: March 14, 2017,
https://technet.microsoft.com/library/security/ms17-010

[37] What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?
https://www.avast.com/c-eternalblue#gref

[38] What is a DLL?
https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/dynamic-link-library

[39] Silentbuilder.xls malware report
https://tria.ge/201127-4a3yahbyfn

[40] Alert (AA19-339A) Dridex Malware
https://us-cert.cisa.gov/ncas/alerts/aa19-339a

[41] Qbot threat analysis
https://any.run/malware-trends/qbot

[42] Ryuk threat analysis
https://any.run/malware-trends/ryuk

[43] Formbook threat analysis
https://any.run/malware-trends/formbook\

[44] GuLoader: Peering Into a Shellcode-based Downloader, Crowdstrike
https://www.crowdstrike.com/blog/guloader-malware-analysis/

[45] Analysis Of Hancitor – When Boring Begets Beacon
https://binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon/

[46] Threat Thursday: Hancitor Malware
https://blogs.blackberry.com/en/2021/07/threat-thursday-hancitor-malware

[47] Android banking trojan FluBot impersonates international logistics companies
https://www.eset.com/blog/consumer/android-banking-trojan-flubot-impersonates-international-logistics-companies/

[48] FluBot Malware – All You Need to Know & to Act Now
https://www.threatmark.com/flubot-banking-malware/

[49] GuLoader: Peering Into a Shellcode-based Downloader
https://www.crowdstrike.com/blog/guloader-malware-analysis/

[50] Verisign Domain Name Industry Brief, Q2 2021. Volume 18, issue 3, September 2021.
https://www.verisign.com/assets/domain-name-report-Q22021.pdf

[51] Cobalt Strike
https://attack.mitre.org/software/S0154/

[52] Deep Analysis: New FormBook Variant Delivered in Phishing Campaign
https://www.fortinet.com/blog/threat-research/deep-analysis-new-formbook-variant-delivered-phishing-campaign-part-I

[53] Malwarebytes Labs, anonfiles.com
https://blog.malwarebytes.com/detections/anonfiles-com/

[54] Github uncovers malicious 'Octopus Scanner' targeting developers
https://nakedsecurity.sophos.com/2020/06/01/github-uncovers-malicious-scanner-targeting-developers/

[55] Greedy cybercriminals host malware on Github
https://blog.avast.com/greedy-cybercriminals-host-malware-on-github

[56] The Malicious Use of Pastebin
https://www.fortinet.com/blog/threat-research/malicious-use-of-pastebin

[57] FAQ - AnonFiles
https://anonfiles.com/faq

[58] API - Docs - AnonFiles
https://anonfiles.com/docs/api

[59] ANY.RUN Interactive Malware Hunting Service
https://any.run/

[60] Hybrid Analysis
https://www.hybrid-analysis.com/

[61] Virus Total
https://www.virustotal.com/

[62] Process Library
https://www.processlibrary.com/en/

[63] Process Library, Trojan.W32.Nethell
https://www.processlibrary.com/en/directory/files/file/25702/

[64] Malpedia: ClipBanker
https://malpedia.caad.fkie.fraunhofer.de/details/win.clipbanker

[65] Hybrid-Analysis of Astro.exe
https://www.hybrid-analysis.com/sample/7b12a81681be0f6115fb30d8805c8d2a46350085392e04f519d124a5b9c06167/5fe179688ca5c745a734c1bd

[66] Anonfiles FAQ
https://anonfiles.com/faq

[67] Anonfiles Terms of Use
https://anonfiles.com/terms

[68] Anonfiles Report Abuse
https://anonfiles.com/abuse

[69] G. Aaron, L. Chapin, D. Piscitello, C. Strutt. "Phishing Landscape 2021: An Annual Study of the Scope and Distribution of Phishing". https://www.interisle.net/PhishingLandscape2021.html

[70] A. Oest, Y. Safaei, A. Doupé, G. Ahn, B. Wardman, and K. Tyers. "PhishFarm: A Scalable Framework for Measuring the Effectiveness of Evasion Techniques Against Browser Malware Blacklists". In: 2019 IEEE Symposium on Security and Privacy (SP), 19-23 May 2019.
https://ieeexplore.ieee.org/document/8835369

[71] D. Piscitello, G. Aaron. "Domain Abuse Activity Reporting (DAAR) System Methodology". Internet Corporation for Assigned Names and Numbers (ICANN). November 2017.
https://www.icann.org/en/system/files/files/daar-methodology-paper-30nov17-en.pdf

[72] Dietrich C.J., Rossow C. (2009) Empirical research of IP blacklists. In: Pohlmann N., Reimer H., Schneider W. (eds) ISSE 2008 Securing Electronic Business Processes. Vieweg+Teubner.
https://doi.org/10.1007/978-3-8348-9283-6_17

[73] S. Maroofi, M. Korczynski, C. Hesselman, B. Ampeau, A. Dud, "COMAR: Classification of Compromised versus Maliciously Registered Domains". 2020 IEEE European Symposium on Security and Privacy (EuroS&P). http://mkorczynski.com/COMAR_2020_IEEEEuroSP.pdf and
https://comar-project.univ-grenoble-alpes.fr/

[74] Pitsillidis, C. Kanich, G.M. Voelker, K. Levchenko, S. Savage. "Taster's Choice: A Comparative Analysis of Spam Feeds". Proceedings of the 2012 Internet Measurement Conference, 427-440
https://cseweb.ucsd.edu/~apitsill/papers/imc12.pdf

[75] D. Piscitello. "Reputation Block Lists: Protecting Users Everywhere". 1 November 2017. Internet Corporation for Names and Numbers (ICANN)
https://www.icann.org/news/blog/reputation-block-lists-protecting-users-everywhere

[76] B. Greene. "What Makes a Good 'DNS Blacklist"?"
https://blogs.akamai.com/2017/08/what-makes-a-good-dns-blacklist.html and
https://www.akamai.com/us/en/products/security/enterprise-threat-protector.jsp

[77] G. Aaron, D. Piscitello. "Domain Abuse Activity Reporting (DAAR) System Methodology". Internet Corporation for Assigned Names and Numbers (ICANN). November 2017
https://www.icann.org/en/system/files/files/daar-methodology-paper-30nov17-en.pdf

[78] Malware Patrol
https://www.malwarepatrol.net/

[79] MalwareURL
https://www.malwareurl.com/

[80] URLhaus Malware URL Exchange
https://urlhaus.abuse.ch/

[81] The Spamhaus Project.
https://www.spamhaus.org/

[82] Team Cymru. IP to ASN Mapping Service
https://team-cymru.com/community-services/ip-asn-mapping/

[83] RIPE-NCC
https://stat.ripe.net/ and
https://www.ripe.net/manage-ips-and-asns/db/tools

[84] IANA root zone list
https://www.iana.org/domains/root/db

[85] Public Suffix List
https://publicsuffix.org/

[86] IANA Registrar IDs
https://www.iana.org/assignments/registrar-ids/registrar-ids.xhtml

[87] ICANN Security and Stability Advisory Committee (SSAC): SAC101v2: SSAC Advisory Regarding Access to Domain Name Registration Data. 12 December 2018
https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf