# 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*

# Contents

## 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 ';
```

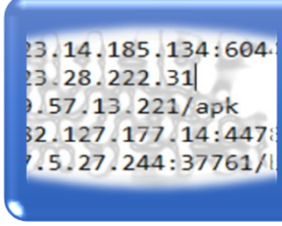
## Principal Findings

### 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



```
3.14.185.134:604
3.28.222.31
.57.13.221/apk
2.127.177.14:447
.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

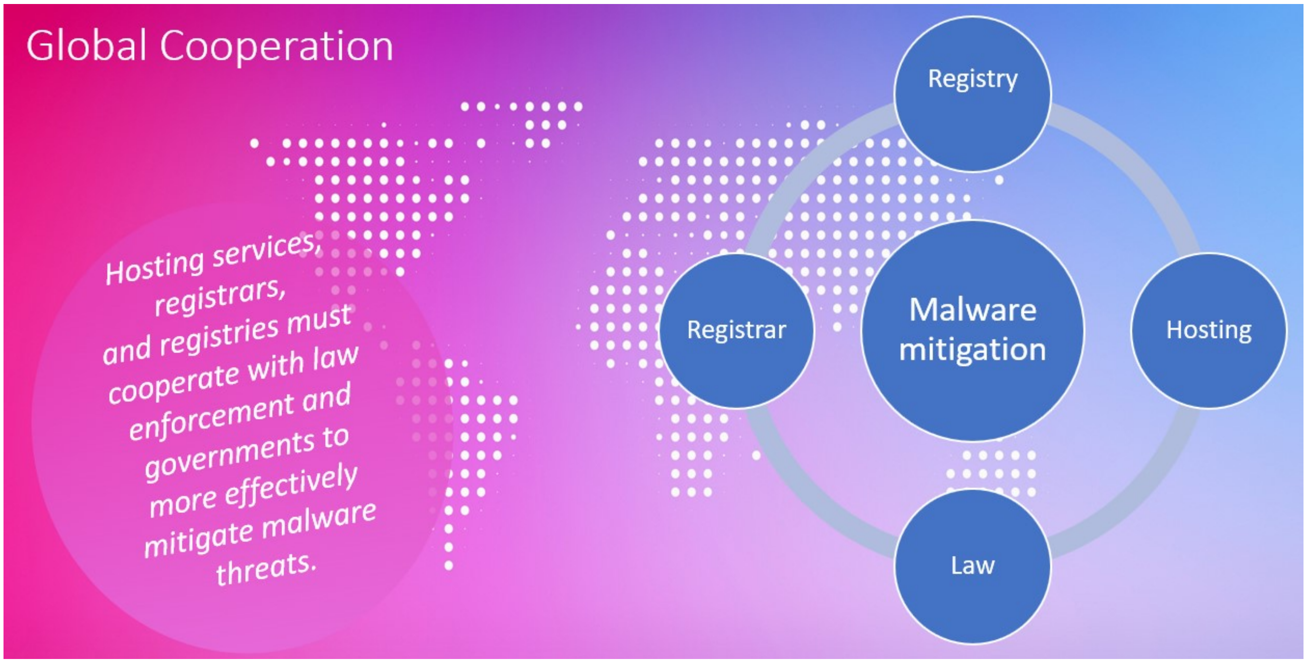
### Cooperative efforts can mitigate malware

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.

## 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". Malware can manipulate data; interfere with the operation of computer systems and networks; delete, suppress, or block access to data; and re-direct computing resources from legitimate to criminal purposes.

The independent research institute AV-TEST GmbH registers new malware and potentially unwanted applications daily. Figure 1 illustrates the steady increase in total malware since 2013.

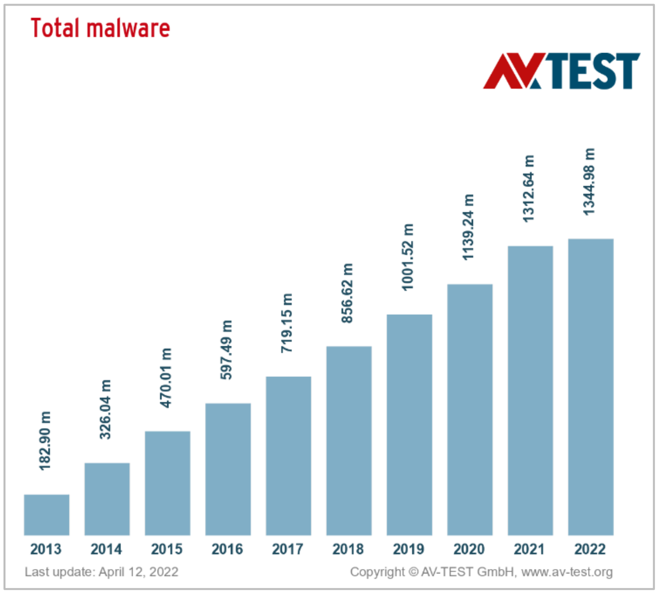


*Figure 1 Total Malware Since 2013 – (Source: AV-TEST.org)*

The objective of this study and resulting report is to quantify how malware *lives off the land* – the Internet and associated services – to exploit or victimize individuals, organizations, and state agencies of all types.

To assemble a deep and reliable set of data, we captured and analyzed nearly 5 million malware reports during a 12-month study period (April 2021 to March 2022) from four widely used and respected threat intelligence sources: Malware Patrol, MalwareURL, Spamhaus, and URLhaus (see Appendix C – Data Sources and Methodology). We removed duplicates from this set of malware reports, creating 2,493,014 records of distinct malware events. These records enabled us to determine 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" [1]). We studied each separately.

## 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.

Malware is being fueled by several factors:

- The technical sophistication and efficacy of malware have been improving substantially over recent years. Many malware variants exploit multiple vulnerabilities and bring powerful tools to leverage each compromise to extend reach beyond the initial exploit. The Solar Winds [2] and Kaseya [3] incidents are examples of how this pivoting reaches well beyond initial intrusions.
- Malware has been openly commercialized by legitimate businesses, and the use of malware by nation states, as evidenced during events preceding and during Russia's incursion into Ukraine, has fundamentally changed the threat landscape.[4, 5]
- Malware actors have exploited the same high-performance technology (*e.g.,* cloud computing) that serves global enterprises and have even adopted the "as a service" model for commercializing malware and ransomware attacks.[6]

*Ransomware* is a particularly vicious form of extortion malware, and it is growing rapidly: a 2022 Ransomware Threat Report [7] documents that "the average ransom demand on cases worked by Palo Alto's Unit 42 consultants last year climbed 144% to $2.2 million, while the average payment rose 78% to $541,010."

Financial losses, business disruption, and harm to life and limb have turned ransomware into a priority global public concern.[8] A ComplyAdvantage State of Financial Crime Report indicates that cybercrime has overtaken fraud as the top predicate offense of concern for corporate compliance teams.[9] 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.[10] 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.[11] 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.[12] 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.[13]

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

| | |
|---|---|
| 2,493,017 | Malware records studied |
| 110,833 | Unique domain names |
| 505 | Top-level domains hosting malware |
| 1,199 | Registrars of malware domains |
| 582,475 | Internet Addresses (IPv4) hosting malware |
| 7,871 | ASNs hosting malware |

### Malware Trends

Malware reporting generally increased during our study period.

**Malware reports growing**

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

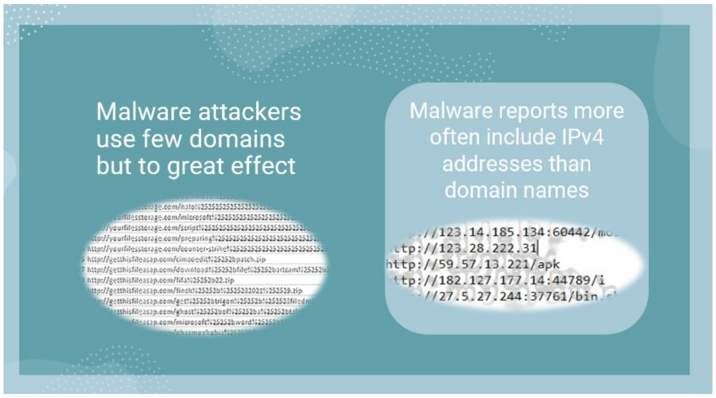
We began with over 5 million malware reports collected from four threat intelligence feeds. However, we found significant duplication of reports within and between feeds. Removing duplications showed a decrease in IoT malware reports over the 12-month period, but an increase in Endpoint malware reports during the same period.

We continue to observe that malware reporting has no discernable peaks by day of week. This is distinctly different from phishing, where historically activity is highest in the Monday to Wednesday period, when many potential victims return to work and check their emails.

### Domain Names and Malware

Domain names are essential resources for spam and phishing attacks; the data we collected reveal that they are less commonly used for serving malware or for malware distribution.

Of the 2,493,017 malware records that we examined for this study, 1,611,028 (65%) were IP address-based, and 881,989 (35%) were domain-based. 110,835 unique domain names were reported for serving up malware, which means that individual domain names were used for multiple malware attacks. This malware study therefore focused less on domain name registries and registrars than our annual phishing landscape study.[14]


Malware attackers use few domains but to great effect
Malware reports more often include IPv4 addresses than domain names
://123.14.185.134:60442/mo
tp://123.28.222.31
http://59.57.13.221/apk
tp://182.127.177.14:44789/i
//27.5.27.244:37761/bin

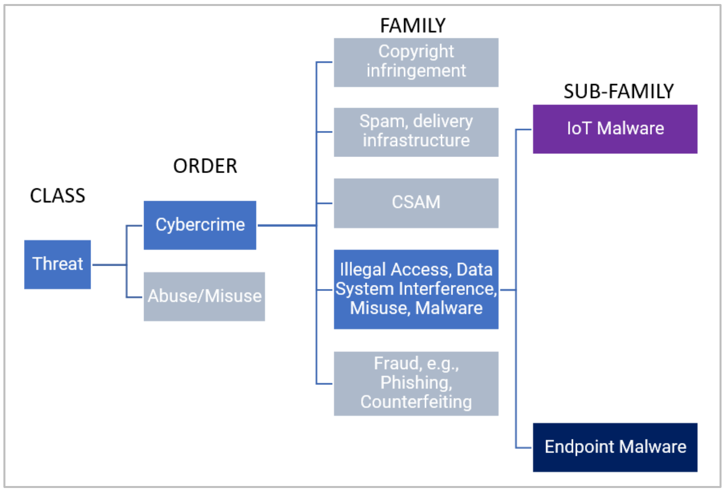
## Hosting Resources and Malware

Most malware reports that we collected contain Internet Protocol v4 (IPv4) addresses in URLs rather than domain names. No IPv6 addresses appeared in the malware reports. We concentrate on Hosting Networks or Autonomous Systems (ASs) in this study; we identify the hosting services or cloud services that criminals misuse to serve or distribute malware by **Autonomous System Number (ASN).**[15]

We extracted the IP addresses of hosting sites from address-based URLs that were reported for serving or distributing malware and used DNS name resolution to find the IP addresses of domain names extracted from name-based URLs. We then associated the IP addresses with the Autonomous System that advertised them and filtered the resulting data set so that we could identify the ASNs with the highest occurrences of IPv4 addresses reported for serving malware.

## Classification of Malware

For our malware studies, we set out to identify and measure the resources that attackers use to distribute or serve malware. To meaningfully measure hundreds of different types of malware, we adapted a malware taxonomy based on a classification system proposed by the Computer Antivirus Research Organization. Our taxonomy attempts to align cyberthreats generally to cybercrimes in the Council of Europe's Convention on Cybercrime.[16, 17] In Appendix A – Classifying Malware, we describe this taxonomy in detail.


FAMILY
Copyright infringement
Spam, delivery infrastructure
CSAM
Illegal Access, Data System Interference, Misuse, Malware
Fraud, e.g., Phishing, Counterfeiting
SUB-FAMILY
IoT Malware
Endpoint Malware
CLASS
Threat
ORDER
Cybercrime
Abuse/Misuse

In our taxonomy, we identify two malware sub-families based on the kinds of devices that a malware targets. IoT Malware targets Internet of Things (IoT) devices (such as surveillance cameras, sensors, or embedded technologies). Endpoint Malware targets user-attended devices (such as computers or mobile phones).

Two of our threat intelligence 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 assign malware to a Malware Sub-family.

We further attempted to apply our classification to reports that did not provide metadata by submitting URLs to one or more of three malware analysis services: Virus Total [18], Hybrid Analysis [19], and ANY.RUN. [20] Where available, we augmented our metadata with information from these reports.

Sometimes the malware reports from our threat intelligence feeds lack the information necessary to classify the malware as *IoT Malware* or *Endpoint Malware*. For this study, we have been careful to assign a malware report to a sub-family only when supported by the available information (metadata) unambiguously.

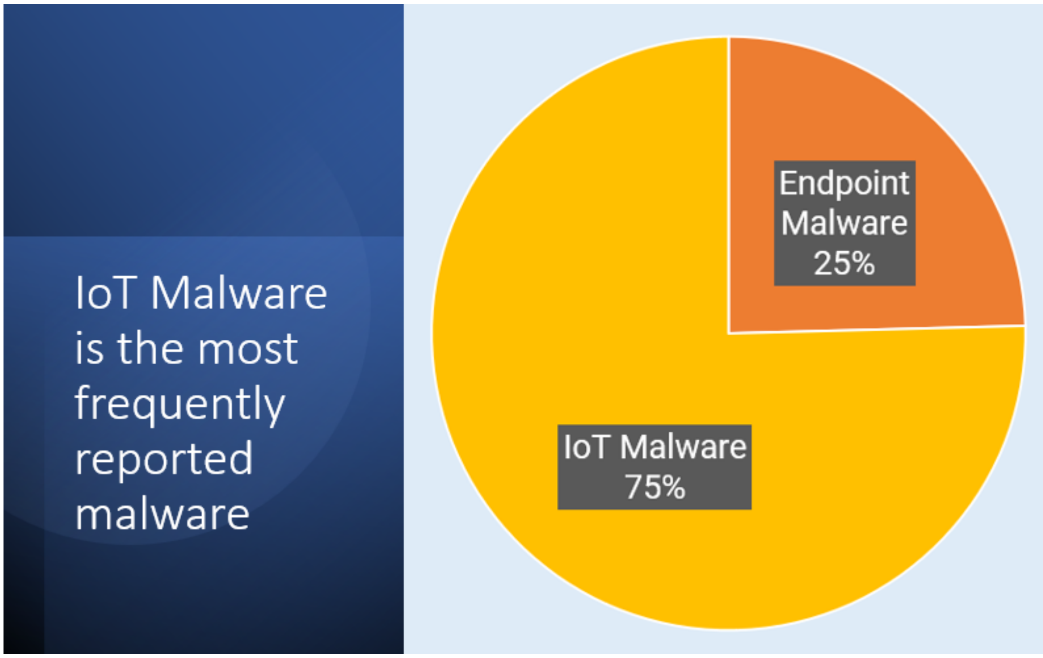
Where insufficient information existed to determine if a report was *IoT Malware* or *Endpoint Malware* we considered that report to be *Uncategorized*. Uncategorized malware are important in understanding overall malware activity. We include all malware reports – IoT, Endpoint, and Uncategorized – in the quarterly malware activity reporting at the Cybercrime Information Center.

We excluded the remaining *uncategorized* malware reports from this study, so the tables, charts, and analyses in this study focus on the IoT and Endpoint sub-families. [21]

### Distribution of Malware by Sub-Family

In Appendix B – Key Statistics, we provide a total count of malware for each Key Statistic and counts for entries that we assigned to the Endpoint Malware or IoT Malware sub-families.

For the study period, we classified a supermajority (75%) of the 1.75 million malware reports where we could identify the sub-family as malware targeting IoT devices. We classified the remaining and still significantly large set of reports as malware that targeted Endpoint Devices.



The high numbers of malware that target IoT devices compared to those that target user-attended (Endpoint) devices suggests 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.

Our analyses of these sub-families follow.

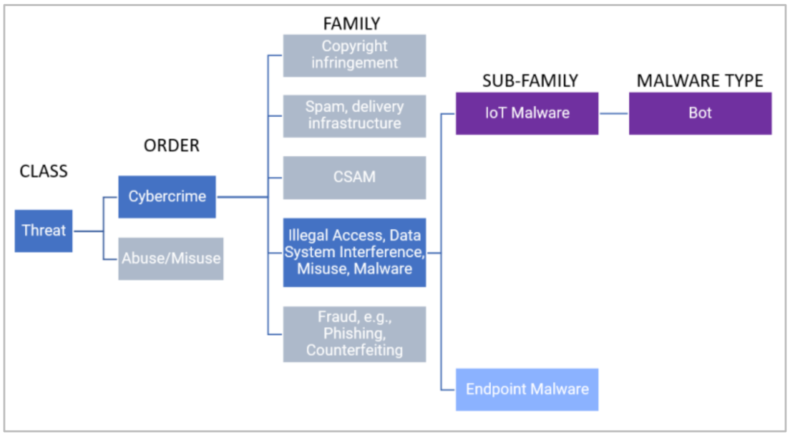
## IoT Malware

**Internet of Things (IoT) Malware accounted for 53% of the 2,493,017 malware records.** Appendix A – Classifying Malware describes how we produced malware records suitable for analysis for this study.

**Asia-Pacific networks host most IoT malware**

China, India, and Australia host 81% of IoT malware

IoT Malware targets 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 system services (*e.g.,* Telnet) or device management access.  Connecting devices in these unsecured states to the Internet leaves them vulnerable to unauthorized remote access and misuse.


FAMILY
Copyright infringement
Spam, delivery infrastructure
CSAM
Illegal Access, Data System Interference, Misuse, Malware
Fraud, e.g., Phishing, Counterfeiting
SUB-FAMILY
IoT Malware
Endpoint Malware
MALWARE TYPE
Bot
ORDER
Cybercrime
Abuse/Misuse
CLASS
Threat

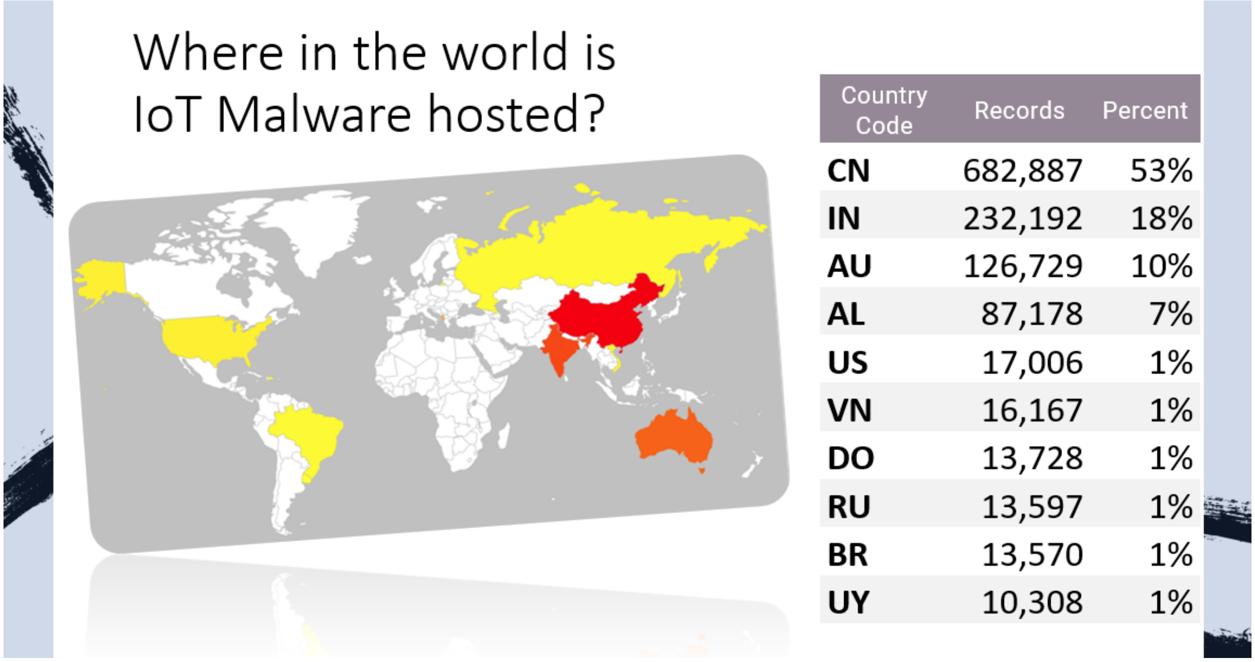
Outdated software is a known contributor to the persistent malware growth. In some cases, poor patch management practices are to blame. In other cases, the devices cannot be patched, or software supply-chain issues leave devices vulnerable to decades-old exploits.

IoT malware is often multi-staged, where the first stage or *compromise* attack gains administrative control over the device and subsequent stages load denial of service attacks or other malware. The use of IoT devices in this manner, to *pivot* into target networks to plant other malware or establish an APT presence, is an emerging and growing problem.

Raw numbers of reported IoT Malware reveal the intended misuse of infected devices. Large numbers (often thousands) of infected IoT devices are 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 disrupt its services. 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.  Raw numbers may also offer an insight into an increasingly worrisome business model: Malware as a Service, offered in the public and dark web, creates opportunities for unsophisticated criminals to perpetrate malware or ransomware attacks.

### Where in the world is IoT Malware Hosted?

We determined the top 10 countries reported for serving or distributing IoT malware, by number of malware records and by percent of the 1,279,007 records for which we could determine a country used.



Where in the world is IoT Malware hosted?

| Country Code | Records | Percent |
|---|---|---|
| CN | 682,887 | 53% |
| IN | 232,192 | 18% |
| AU | 126,729 | 10% |
| AL | 87,178 | 7% |
| US | 17,006 | 1% |
| VN | 16,167 | 1% |
| DO | 13,728 | 1% |
| RU | 13,597 | 1% |
| BR | 13,570 | 1% |
| UY | 10,308 | 1% |

Table 1 shows where we identified hosting networks reported for serving or distributing IoT malware, by total IoT malware records.

| Rank | AS Name | AS number | # Routed IPv4 Addresses | Total IoT Malware Records ▼ |
|---|---|---|---|---|
| 1 | China169 Backbone | 4837 | 59,099,904 | **497,402** |
| 2 | National Internet Backbone | 9829 | 10,849,792 | **170,616** |
| 3 | CHINANET-BACKBONE No.31 | 4134 | 113,161,984 | **118,364** |
| 4 | China169 Guangdong province | 17816 | 3,948,288 | **93,723** |
| 5 | Telekomi i Kosoves | 8661 | 84,224 | **86,999** |
| 6 | China Unicom Guangzhou network | 17622 | 1,371,648 | **60,806** |
| 7 | Hathway IP Over Cable Internet | 17488 | 1,006,592 | **28,316** |
| 8 | China Unicom Shenzen network | 17623 | 942,336 | **14,465** |
| 9 | VNPT-AS-VN VNPT Corp | 45899 | 19,409,408 | **13,665** |
| 10 | WIND Telecom S.A. | 27887 | 63,744 | **13,634** |

*Table 1 Ranking of Hosting Networks Serving IoT Malware, by Total IoT Malware Records*

## Prevalent "Named" IoT Malware

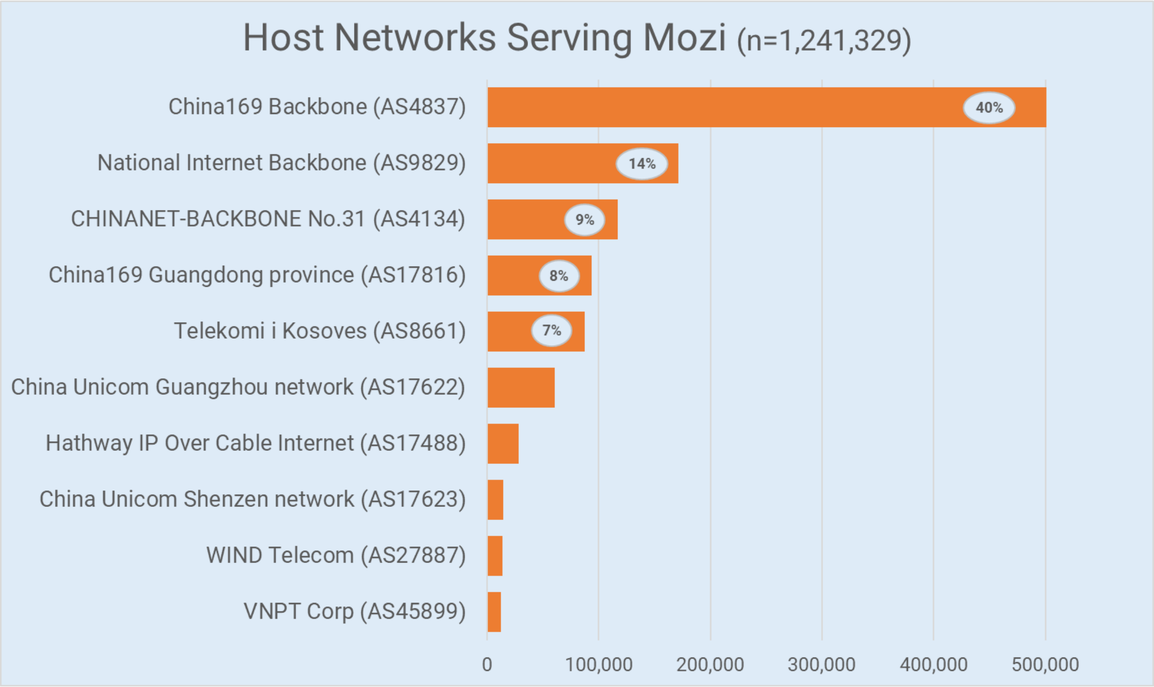
To identify IoT malware by name, we used tags provided by our feeds. We also examined URLs from feeds that do not provide tags, and observed common characteristics; for example, tens of thousands of URLs contained the same scheme and file or resource location, differing only by host address and port. We submitted samples of these URLs to the community malware analysis services (Virus Total, Hybrid Analysis, and ANY.RUN) to confirm our suspicion that these could be classified by name.

Using the results of these malware checks, we associated 1,279,563 of the IoT malware records with Mozi malware and 111,878 records with Mirai malware. We examine these IoT Malware more carefully in sections which follow. We did observe conflicting reporting across our source feeds while processing IoT malware. In some cases, a URL was reported in one feed as serving Mozi but in a second feed as serving Mirai.

## Mozi Malware

Mozi is one of a family of malware – including Mirai, Gafgyt, and IoT Reaper – that exploits Linux-based IoT devices such as DVR cameras and consumer grade routers. Mozi has been linked to DDoS attacks, spam campaigns, and data exfiltration attacks. 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.

Of the 1,739 ASNs hosting Mozi, **the top 10 ASNs account for 89% of the reported addresses and the top 30 ASNs account for 94%**.



Five of the ten ASNs are in China, along with two ASNs in India, and one each in Albania, Dominican Republic, and Vietnam.

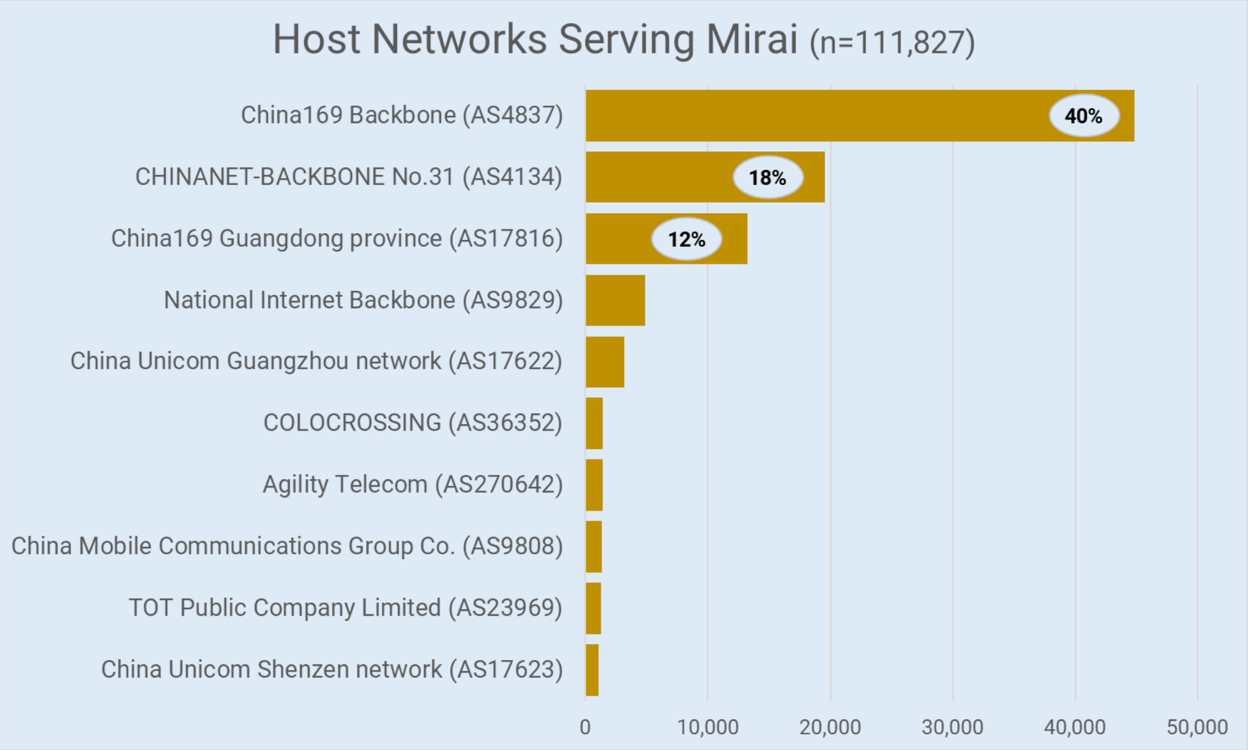
Of the five ASNs in China, four are operated by CHINA UNICOM Industrial Internet Backbone: AS 4837, AS 17622, AS 17623, and AS 17816. F5 Labs identified AS 4837 as one of the top source traffic ASNs for Cyberattacks Targeting Latin America, January through March 2021.[22] The remaining ASN in China, AS 4134, CHINANET-BACKBONE No.31, is operated by China Telecom.

China UNICOM, CHINANET-BACKBONE, along with India's Hathway IP (AS 17488) and BSNL (Bharat Sanchar Nigam Ltd, AS 9829), are listed in the top malware hosting networks by ASN *and* by hosting active malware content by URLhaus, a research project at the Institute for Cybersecurity and Engineering hosted at the Bern University of Applied Sciences (BFH) in Switzerland [23] (and one of our primary sources).

## Mirai Malware

Mirai gained notoriety in 2016 as a malware used to enlist surveillance or monitoring cameras (such as closed-circuit television – CCTV), DVRs, and routers into botnets subsequently used in DDoS attacks.[24] Mirai variants appeared throughout our study period and were among the IoT malware that was associated with botnet-based DDoS attacks against Ukraine.[25]

We used tags provided by our feeds and common URL characteristics to associate 111,827 IoT malware records with Mirai malware.



Six of the top 10 ASNs with the largest number of Mirai distribution hosts are ASNs in China. ASNs operated by China Telecom and CHINA UNICOM have large numbers of IPv4 addresses reported for serving Mirai *and* Mozi malware.

India’s Hathway IP (AS 17488) and BSNL (Bharat Sanchar Nigam Ltd, AS 9829) were also among the Top 10 ASNs reported for serving Mirai *and* Mozi malware. Brazil’s Agility Telecom (ASN 270642) and ColoCrossing (AS 36352) in the United States round out the top 10.

In Figure 2 we compare monthly reporting of Mozi malware with Mirai malware.

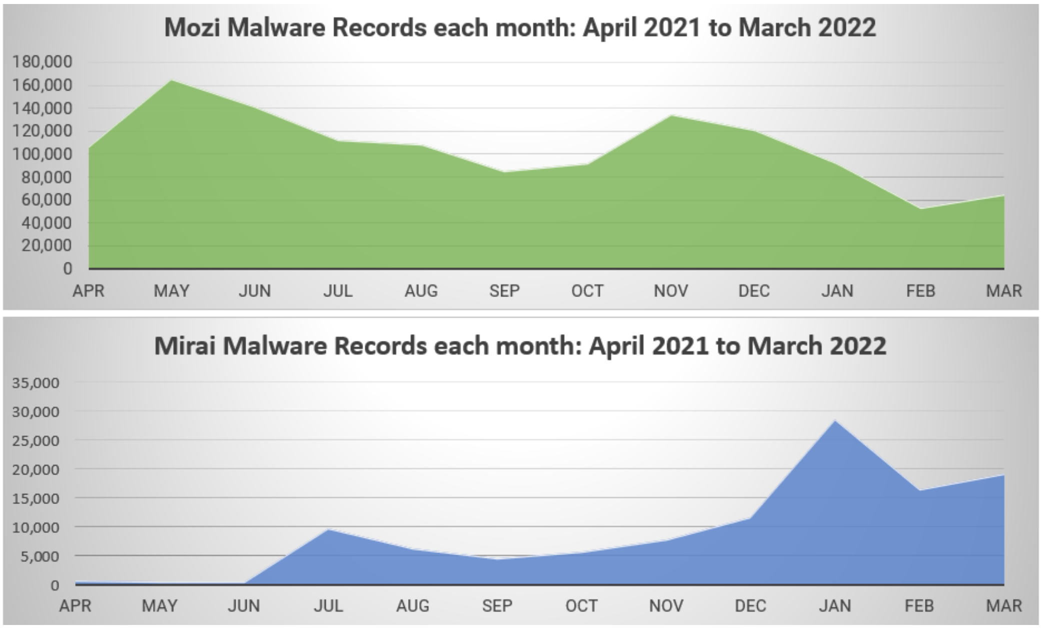
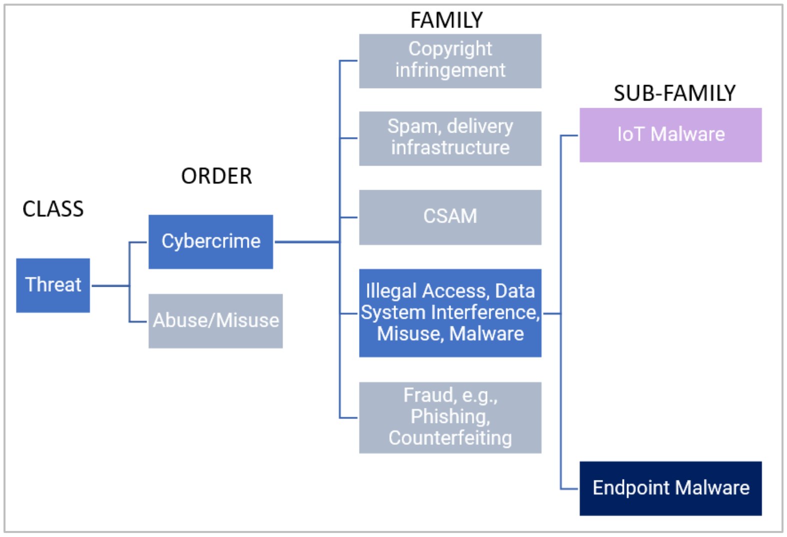


*Figure 2 Comparison of Mozi and Mira Malware Distribution*

Mozi distribution appears to have declined as Mirai distribution rose; however, Mozi malware continued to be reported in much higher numbers through March 2022. Mirai distribution has yet to increase to the same scale as Mozi.

## 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. Criminals use a wide variety of endpoint malware that serve different purposes, *e.g.,* they will use ransomware for extortion, information stealing malware such as banking trojans for identity theft or financial fraud, or backdoor trojans for remote control execution or administration.


CLASS
Threat
ORDER
Cybercrime
Abuse/Misuse
FAMILY
Copyright infringement
Spam, delivery infrastructure
CSAM
Illegal Access, Data System Interference, Misuse, Malware
Fraud, e.g., Phishing, Counterfeiting
SUB-FAMILY
IoT Malware
Endpoint Malware

While hundreds of organizations and individual malware investigators work to identify, reverse engineer, or mitigate malware, there are few widely adopted norms for naming or typing malware and this creates challenges for anyone who is trying to measure malware and so classifying Endpoint Malware proves to be a highly subjective exercise.

For example, we classify 422 malware reports that identified the Log4j vulnerability[26] exploit as a remote control execution (RCE) because the vulnerability allows an attacker to execute code remotely and assume remote control over infected devices. Others tag Log4j as a backdoor/RAT. Interisle classifies the banking trojans Trickbot and Qakbot as information stealers: we consider stealing as different from cyber extortion or ransomware attacks. Others who report on ransomware classify these malware as ransomware.

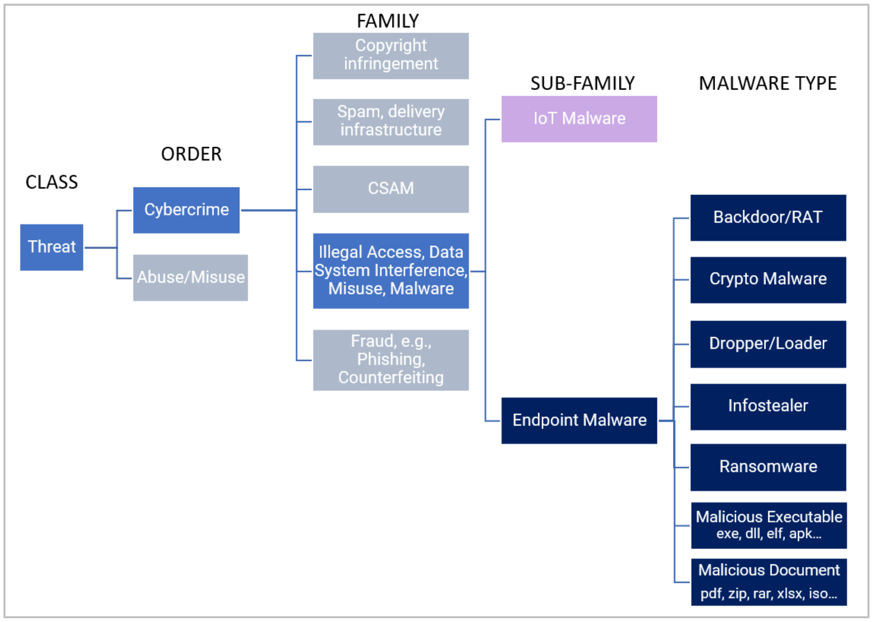
Whether by fraud or extortion, attackers seek financial rewards

Malware classification is an imperfect science. Consequently, classification may, or may not, be helpful in characterizing new malware strains, or attack methodologies that leverage multiple forms of attack. In the constantly evolving malware landscape, even the goals of attackers might be merging or morphing into combinations that attempt to maximize benefit or value to the attacker. For example, traditional ransomware has morphed into attacks that first steal information, then encrypt the victims' data.

Our interpretation of what malware is ransomware, combined with the fact that our malware feeds report very few domains or URLs for hosting ransomware, results in very low ransomware measurements. This doesn’t diminish the ransomware threat; rather, it shows that a different or more accurate ransomware measurement would require threat feeds that focus more on indicators of cyber extortion.

It is increasingly common for ransomware perpetrators to leverage information theft as a means to include disclosure of sensitive information as a further incentive for the victim to pay the ransom; however, information theft is motivated by very different objectives, and it is likely that information theft is significantly under-reported, because it is a covert operation that often succeeds when the victim never discovers that information was lost.

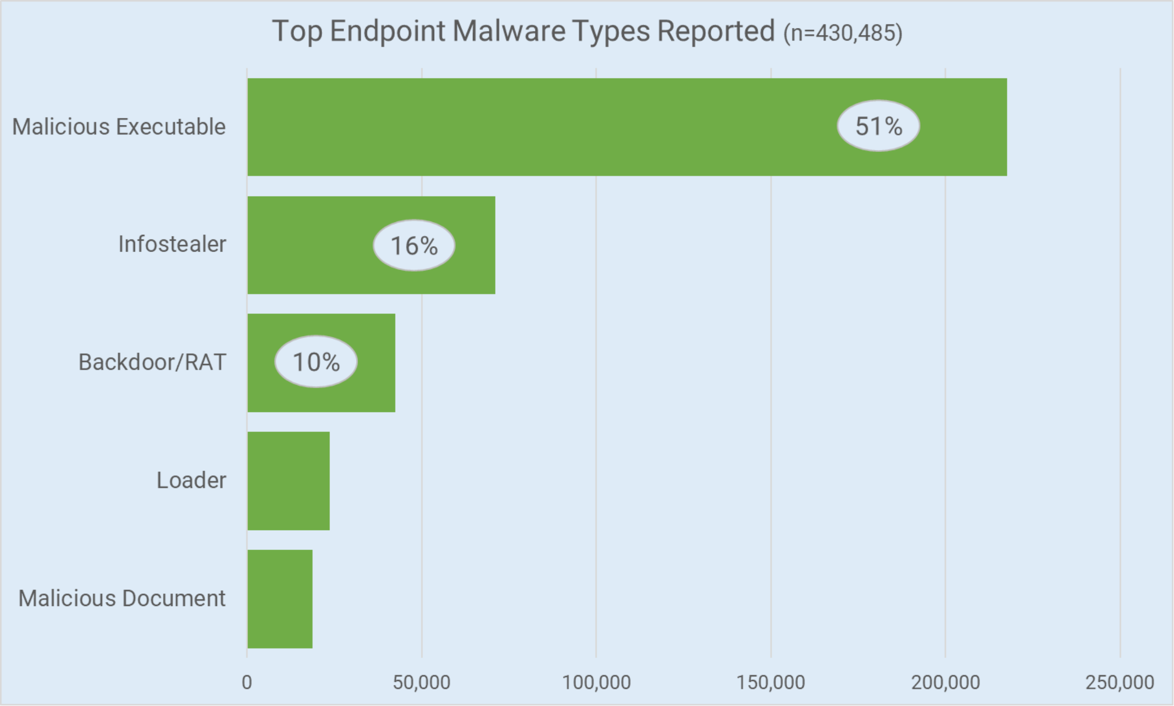
## Classifying Endpoint Malware by Malware Type


FAMILY
SUB-FAMILY
MALWARE TYPE
ORDER
CLASS
Threat
Cybercrime
Abuse/Misuse
Copyright infringement
Spam, delivery infrastructure
CSAM
Illegal Access, Data System Interference, Misuse, Malware
Fraud, e.g., Phishing, Counterfeiting
IoT Malware
Endpoint Malware
Backdoor/RAT
Crypto Malware
Dropper/Loader
Infostealer
Ransomware
Malicious Executable exe, dll, elf, apk…
Malicious Document pdf, zip, rar, xlsx, iso…

Malicious Executable was the most reported endpoint malware type. This malware type includes executable code (often self-extracting), identified by file extension or MIME type, for which we were unable to identify a more specific malware type such as loader or RAT.

Infostealers and Backdoors/RATs accounted for 16% and 10% of the Endpoint Malware that we were able to type, respectively. The remaining 23% is distributed across a long tail of other malware types.

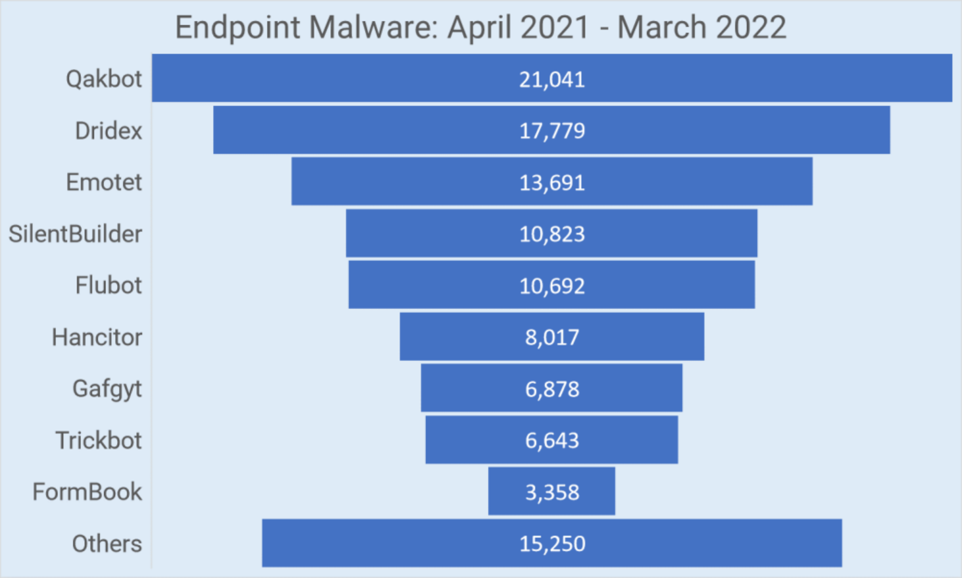
Our classification at the Malware Type level is influenced by individual behavior, *i.e.,* the malware reporters themselves and the level of detail that they provide. Some reporters provide ample and unambiguous reports and attempt to follow the loosely defined conventions that are typical of the malware blocklist where they submit their findings. Others submit minimal information or tags of their own convention or invention. The Malicious Document and Malicious Executable types thus represent our best efforts to identify a malware as “computer code” versus “harmful file”.



Specific or "named" malware of the types – infostealers, trojans, RATs, and loaders (downloaders or droppers – are examined in detail in next the section.

## Prevalent Endpoint Malware ("Named" Malware)

Malware reporters and security vendors use various conventions to assign names to malware. The result is that a given malware may have dozens of names. Naming malware is further complicated when malware developers develop variants or embed components of other named malware. For our taxonomy, we normalized to what we determined to be the most recognizable names. In some cases, we also called attention to popular aliases. We did not attempt to track or count by variant.



**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.[27]

**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.[28]

**Emotet**

Emotet is a polymorphic banking Trojan that primarily functions as a loader of other banking Trojans. It uses Dynamic Link Libraries (DLLs) to continuously evolve and update capabilities.[29]

**SilentBuilder**

A loader that embeds a Dynamic Link Library (DLL) [30] 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.[31]

**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.[32] The trojan also steals contact data that the attacker will use in subsequent SMS text messages.

**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.[33] Recent campaigns impersonate DocuSign.[34]

**Gafgyt**

A Linux malware that targets IoT devices, enrolling these into botnets that are used in large scale DDoS attacks. Under constant evolution since 2014, Gafgyt has used Shellshock for its initial compromise, and like Mirai, it propagates by brute-forcing weak Telnet passwords.[35]

**Trickbot**

Trickbot ransomware (also called) Ryuk 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.[36]

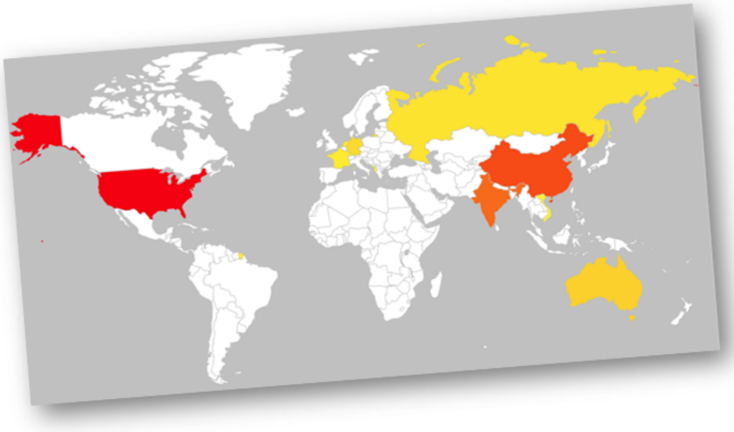
**Formbook**

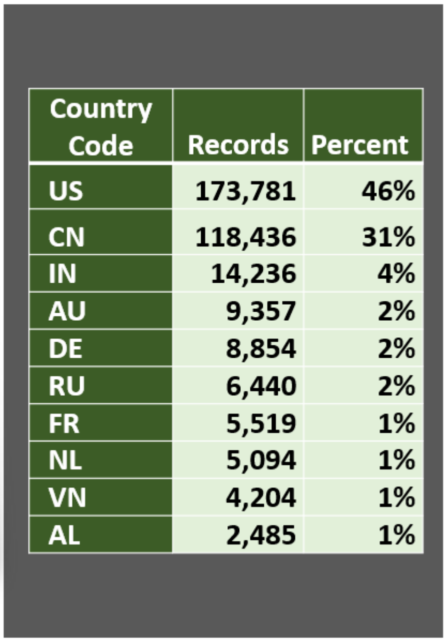
An infostealer that is offered as a Malware as a Service platform. ANY.RUN’s characterization of FormBook as “attractive to attackers, with low technical literacy, sold as a control panel, available on highly accessible online forums, for 30 dollars” [37] illustrates how far ransomware (and malware) have matured as profitable enterprises.

## Countries Where Endpoint Malware was Hosted

We determined the top 10 countries reported for hosting malware, by number of malware records and by percentage of the 380,763 records for which we could determine a country.

Where in the world is endpoint malware hosted?





| Country Code | Records | Percent |
|---|---|---|
| US | 173,781 | 46% |
| CN | 118,436 | 31% |
| IN | 14,236 | 4% |
| AU | 9,357 | 2% |
| DE | 8,854 | 2% |
| RU | 6,440 | 2% |
| FR | 5,519 | 1% |
| NL | 5,094 | 1% |
| VN | 4,204 | 1% |
| AL | 2,485 | 1% |

The United States and China accounted for more than ¾ of the Endpoint Malware for which we could determine ASN and country.

Table 2 shows where we identified hosting networks reported for serving or distributing endpoint malware, by total endpoint malware records.

| Rank | AS Name | AS number | # Routed IPv4 Addresses | Total Endpoint Malware Records ▼ |
|---|---|---|---|---|
| 1 | China169 Backbone | 4837 | 59,099,904 | **99,170** |
| 2 | CLOUDFLARENET | 13335 | 2,400,768 | **62,181** |
| 3 | UNIFIEDLAYER-AS-1 | 46606 | 1,133,568 | **12,839** |
| 4 | National Internet Backbone | 9829 | 10,849,792 | **10,320** |
| 5 | China Unicom IP network | 133119 | 219,904 | **7,959** |
| 6 | DIGITALOCEAN-ASN | 14061 | 2,696,960 | **7,838** |
| 7 | CNSERVERS | 40065 | 580,352 | **7,319** |
| 8 | AS-COLOCROSSING | 36352 | 771,328 | **7,238** |
| 9 | GOOGLE | 15169 | 23,098,624 | **6,881** |
| 10 | QUANTILNETWORKS | 54994 | 116,992 | **6,585** |

*Table 2 Ranking of Hosting Networks Serving Endpoint Malware, by Total Endpoint Malware Records*

Some ASNs exhibited very high ratios of Endpoint Malware records to IPv4 addresses reported for serving Endpoint Malware; for example,

- MICROSOFT-CORP-MSN-AS-BLOCK (AS 8068) has 14,155 Endpoint Malware records across 8 IPv4 addresses
- UNICOM-CN China Unicom IP network (AS 133119) has 7,959 Endpoint Malware records across 3 IPv4 addresses
- QUANTILNETWORKS (AS 54994) has 6,585 Endpoint Malware records across 10 IPv4 addresses
- CNSERVERS (AS 40065) has 7,319 Endpoint Malware records across 21 IPv4 addresses

It is unclear how concentrated malware activity of this kind could persist over time without detection or mitigation.

## Top-level Domains where Malware Was Reported

We used Domain Tools [38] as our source for determining TLD domains under management (DUM). According to Domain Tools, at the end of March 2022 there were 358,179,079 registered domains as shown in Figure 3. L*egacy TLDs* refers to Top-level Domains other than .COM and .NET and introduced before 2012 (*e.g.,* .ORG, .BIZ, .INFO, .MOBI) and *new gTLDs* refers to Top-level domains delegated since 2012 (*e.g.,* .CLUB, .TOP, .XYZ).

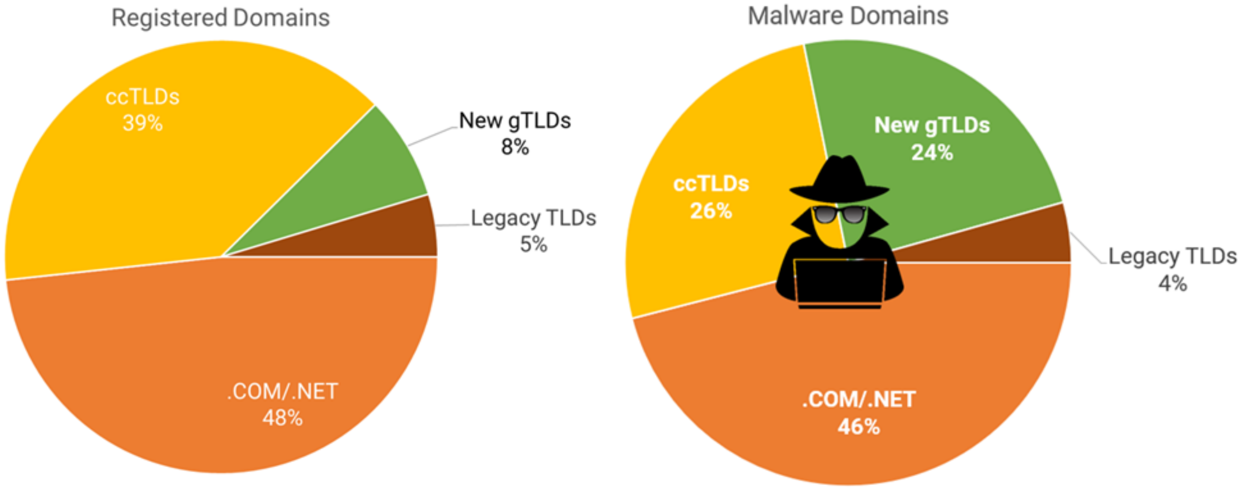


*Figure 3 Registered Domains and Malware Domains by TLD Type*

Figure 3 also shows the percentage of malware domains reported in .COM/.NET, ccTLDs, legacy TLDs, and new gTLDs. By comparing the two charts in Figure 3, we see that

- The percentage of Endpoint Malware domains reported in .COM and .NET are nearly the same as the market share of these combined TLDs. The .COM and .NET registries, operated by Verisign, represented 48% of the domains in the world but 46% of the endpoint malware domains reported for serving malware.
- The percentage of Endpoint Malware domains reported in the legacy TLDs (other than .COM and .NET) is slightly smaller than the market share.

- The ccTLDs have attracted less attention from malware attackers. While the ccTLDs represent 39% of the market, they contained only 26% of the domain names reported for serving endpoint malware.
- The new TLDs have attracted more attention from malware attackers than their market share would suggest. In our Malware Landscape Study 2021 [40], the new gTLDs represented 6% of the market but accounted for 16% of the domain names reported for serving malware. From our 2022 data, we found that the new TLDs market share increased to 8%, but its share of domain names reported for serving endpoint malware grew to 24%.

Table 3 ranks TLDs by Endpoint Malware Domains Reported.

| Rank | TLD | TLD Type | Total Endpoint Malware Domains ▼ | Total URLs |
|---|---|---|---|---|
| 1 | com | Legacy | 19,269 | 147,181 |
| 2 | xyz | New | 9,486 | 11,165 |
| 3 | br | Country | 1,481 | 3,751 |
| 4 | in | Country | 1,287 | 4,205 |
| 5 | net | Legacy | 1,259 | 3,411 |
| 6 | org | Legacy | 1,153 | 5,422 |
| 7 | club | New | 589 | 802 |
| 8 | ru | Country | 550 | 1,578 |
| 9 | top | New | 511 | 1,087 |
| 10 | biz | Legacy | 479 | 661 |

*Table 3 Ranking of TLDs by Endpoint Malware Domains Reported*

We observe that while .COM is ranked #1, .NET #5, and .ORG #6, these TLDs have far more domain names under management than #2 TLD .XYZ (and collectively the rest of the Top 10). Relative to domain names used for phishing [14] or spam, the numbers are very small for all Top-level domains.

## gTLD Registrars where Malware Was Reported

Table 4 ranks gTLD registrars by Endpoint Malware Domains Reported.

**North America Nexus**

8 of top 10 gTLD registrars of malware domains headquartered in North America

| Rank | IANA ID | Registrar | Country of Operation | Domains Under Management | Total Endpoint Malware Domains ▼ |
|---|---|---|---|---|---|
| **1** | 146 | GoDaddy.com | USA | 66,021,659 | **14,686** |
| **2** | 1068 | NameCheap | USA | 13,485,978 | **4,033** |
| **3** | 303 | PublicDomainRegistry.com | USA | 4,981,799 | **2,449** |
| **4** | 472 | Dynadot | USA | 2,968,360 | **1,039** |
| **5** | 69 | Tucows Domains | CA | 10,193,648 | **787** |
| **6** | 48 | eNom | USA | 4,695,593 | **737** |
| **7** | 1479 | NameSilo | USA | 4,510,037 | **677** |
| **8** | 955 | Launchpad.com | USA | 794,424 | **432** |
| **9** | 1418 | Danesco Trading | Cyprus | 82,430 | **345** |
| **10** | 420 | Alibaba Cloud Computing (Beijing) | China | 4,993,709 | **330** |

*Table 4 Ranking of gTLD Registrars by Endpoint Malware Domains Reported*

Few gTLD registrars had high numbers of domain names reported for hosting Endpoint Malware relative to their respective total number of domains under management. However, we observed that 8 of the top 10 gTLD registrars were headquartered in North America.

The counts of domains reported includes domains registered by a criminal to carry out a malicious or criminal act as well as domain names that were registered for legitimate purposes but co-opted by criminals through some form of compromise.

## Where in the Hosting World Do We Find "Named" Endpoint Malware?

We determined that the following ASNs had the highest number of malware records identifying IP addresses that were serving the most named Endpoint Malware:

### Infostealers

**AS13335 CLOUDFLARENET 13,568 records**

| | |
|---|---|
| Dridex | 9,115 |
| Flubot | 1,763 |
| Qakbot | 1,510 |

**AS8068 MICROSOFT-CORP-MSN 9,873 records**

| | |
|---|---|
| Ryuk | 5,755 |
| Dridex | 2,198 |
| Qakbot | 1,738 |

**AS46606 UNIFIEDLAYER 5,442 records**

| | |
|---|---|
| Qakbot | 3,961 |
| Dridex | 1,051 |

### Loaders

**AS15169 GOOGLE 4,240 records**

| | |
|---|---|
| Hancitor | 3,670 |
| GuLoader | 480 |

**AS13335 CLOUDFLARENET 1,741 records**

| | |
|---|---|
| Emotet | 1,296 |
| Hancitor | 236 |

**AS26496 GO-DADDY-COM 1,116 records**

| | |
|---|---|
| Hancitor | 631 |
| Emotet | 460 |

### Backdoor/RAT

**AS36352 AS-COLOCROSSING 1,582 records**

| | |
|---|---|
| Gafgyt | 1,391 |
| Remcos RAT | 103 |

**AS14061 DIGITALOCEAN-ASN 884 records**

| | |
|---|---|
| Gafgyt | 881 |

**AS8068 MICROSOFT-CORP-MSN 726 records**

| | |
|---|---|
| NanoCore | 599 |
| Remcos RAT | 86 |

### Malicious document

**AS46606 UNIFIEDLAYER 3,362 records**

| | |
|---|---|
| SilentBuilder | 3,362 |

**AS394695 PUBLIC-DOMAIN-REGISTRY 1,309 records**

| | |
|---|---|
| SilentBuilder | 1,309 |

**AS8068 MICROSOFT-CORP-MSN 918 records**

| | |
|---|---|
| SilentBuilder | 918 |

Table 5 shows the ASNs where the most reported named Endpoint Malware were hosted, showing the percentage of each named malware that was hosted by each ASN.

| Named Malware Reported | AS name | AS # | Malware Records | Percent of Named Malware |
|---|---|---|---|---|
| Quakbot | UNIFIEDLAYER | 46606 | 3,961 | 21% |
| | MICROSOFT-CORP-MSN | 8068 | 1,738 | 9% |
| Dridex | CLOUDFLARENET | 13335 | 9,115 | 52% |
| | MICROSOFT-CORP-MSN | 8068 | 2,198 | 13% |
| Emotet | CLOUDFLARENET | 13335 | 1,296 | 10% |
| | OVH SAS | 16276 | 719 | 5% |
| SilentBuilder | UNIFIEDLAYER | 46606 | 3,362 | 32% |
| | PUBLIC-DOMAIN-REGISTRY | 394695 | 1,309 | 13% |
| Flubot | CLOUDFLARENET | 13335 | 1,763 | 17% |
| | DIGITALOCEAN | 14061 | 538 | 5% |

*Table 5 Where Were the Top Endpoint Malware Hosted?*

A recent analysis of Quakbot (a.k.a. Qbot) by ANY.RUN[20] reports that “[m]ost of the targets that Qbot goes after are US-based organizations. Only about twenty percent of the new attack businesses are located outside of the United States.” We observed that the ASNs with the highest occurrences of IPv4 addresses reported for serving Quakbot are US-based Unified Layer (AS 46606) and Microsoft Corporation (AS 8068). We did not find further evidence to draw any conclusions regarding this possible nexus.

Over one-half of the occurrences of IPv4 addresses reported for serving Dridex were in Cloudflare AS 1335. Cloudflare provides a DNS redirection service that protects its customers from denial-of-service attacks. Malware attackers appear to take advantage of Cloudflare because its service prohibits observers from seeing the real hosting locations behind its defense network. This is consistent with our phishing web site hosting findings. AS 13335 was also reported for the highest occurrences of Emotet and Flubot malware.

A May 5, 2021 ThreatMark analysis[39] explains that the Flubot Android 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.

## Most Abused Portals, File Sharing and Storage Services, and Code Repository Sites

In our Malware Landscape 2021[40] report, we used the file upload site `anonfiles.com` as a case study to illustrate how malware attackers misused file sharing services.

We also observed that code repositories such as github[41] and pastebin[42] were used to distribute source code, attack code, and files containing compromised credentials or cryptographic keys, and that widely used file and cloud services offered by Google, Microsoft, and Amazon were similarly abused.

Attackers target file sharing, storage services, code repositories

To distribute source code, attack code, and supplementary files

Our 2022 data shows that web sites that offer mobile app downloads, or serve as Internet archives, and even IT professional portals were misused to serve malware.

### Most abused web sites, file shares, and code repositories

anonfiles.com

zol.com.cn

usinenovelle.com

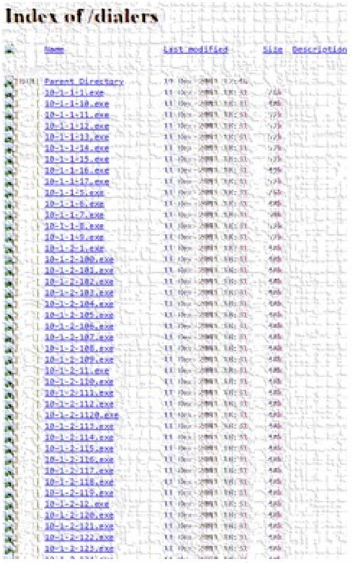
amazonaws.com

1drv.com

live.com

google.com

archive.org



# Index of /dialers

```
Name                 Last modified   Size   Description
Parent Directory     [illegible]
10-1-1-1.exe         [illegible]     [illegible]
10-1-1-10.exe        [illegible]     [illegible]
10-1-1-11.exe        [illegible]     [illegible]
10-1-1-12.exe        [illegible]     [illegible]
10-1-1-13.exe        [illegible]     [illegible]
10-1-1-14.exe        [illegible]     [illegible]
10-1-1-15.exe        [illegible]     [illegible]
10-1-1-16.exe        [illegible]     [illegible]
10-1-1-17.exe        [illegible]     [illegible]
10-1-1-5.exe         [illegible]     [illegible]
10-1-1-6.exe         [illegible]     [illegible]
10-1-1-7.exe         [illegible]     [illegible]
10-1-1-8.exe         [illegible]     [illegible]
10-1-1-9.exe         [illegible]     [illegible]
10-1-2-1.exe         [illegible]     [illegible]
10-1-2-100.exe       [illegible]     [illegible]
10-1-2-101.exe       [illegible]     [illegible]
10-1-2-102.exe       [illegible]     [illegible]
10-1-2-103.exe       [illegible]     [illegible]
10-1-2-104.exe       [illegible]     [illegible]
10-1-2-105.exe       [illegible]     [illegible]
10-1-2-106.exe       [illegible]     [illegible]
10-1-2-107.exe       [illegible]     [illegible]
10-1-2-108.exe       [illegible]     [illegible]
10-1-2-109.exe       [illegible]     [illegible]
10-1-2-11.exe        [illegible]     [illegible]
10-1-2-110.exe       [illegible]     [illegible]
10-1-2-111.exe       [illegible]     [illegible]
10-1-2-112.exe       [illegible]     [illegible]
10-1-2-1120.exe      [illegible]     [illegible]
10-1-2-113.exe       [illegible]     [illegible]
10-1-2-114.exe       [illegible]     [illegible]
10-1-2-115.exe       [illegible]     [illegible]
10-1-2-116.exe       [illegible]     [illegible]
10-1-2-117.exe       [illegible]     [illegible]
10-1-2-118.exe       [illegible]     [illegible]
10-1-2-119.exe       [illegible]     [illegible]
10-1-2-12.exe        [illegible]     [illegible]
10-1-2-120.exe       [illegible]     [illegible]
10-1-2-121.exe       [illegible]     [illegible]
10-1-2-122.exe       [illegible]     [illegible]
10-1-2-123.exe       [illegible]     [illegible]
```

**Anonfiles** 378,397 of the 380,758 malware URLs that included the domain name `anonfiles.com` occurred during Q2 2021, with a peak of 218,958 in June 2021. Anonfiles's Terms of Service[43] forbids the "spread" of viruses, trojans, and corrupt and/or illegal material, and the site provides a form to report abuse. Anonfiles does appear to remove content that it forbids, and notably smaller number of URLs reported since July 2021 suggest that malware attackers have moved elsewhere, perhaps because of changes in anonfiles's malware mitigation measures.

**Zol.com.cn** is a Chinese technology and science portal for professionals, acquired by CNET Networks in 2004. We observed the most malware activity at `zol.com.cn` during Q1 2022, when we identified 55,522 unique malware URLs, with a spike in March 2022. We were able to classify nearly all these URLs as malicious executables. VirusTotal tags these as application/x-msdownload. Multiple commercial security scanners identify the executable as Qjwmonkey adware.

Usinenovelle.com is a French business magazine. As was the case with zol.com.cn, we observed the most malware activity at usinenovelle.com during Q1 2022, with a spike of 48,209 in March 2022. Here, the majority of URLs reported as malware appear to be malicious java scripts.

Amazonaws.com is a domain used by Amazon.com for the cloud infrastructure service Amazon Web Services. We observed little malware activity here in 2021, but in Q1 2022 we identified 38,821 malware URLs; of these, 36,730 were reported in January 2022. These URLs were ingested from a threat feed that did not provide sufficient data to classify the malware (and are thus not included in malware type and family measurements) but we observed that most of the URLs reported were of the form http://****.**.amazonaws.com/installers/nnnnn and identified as suspicious xml files.

1drv.com is a domain used by Microsoft Corporation for its OneDrive online file and photo storage service. Nearly all the 14,048 malware URLs that we associated with 1drv.com were reported in Q4 2021, with the most activity in October (6589) and November (7125). For Q4, we associated 5,803 URLs with infostealer malware (primarily Ryuk/trickbot, but also identified 1,284 malicious documents (653 of these identified as SilentBuilder).

Live.com is used by Microsoft for Outlook.com and OneDrive products. Most of the 4,843 malware URLs reported in this file sharing domain occurred in Q4 2021 (2,354 malware URLs) and Q1 2022 (1842). The infostealers dridex and Ryuk/trickbot were the top malware reported in Q4 2021. A March 2022 flurry of Qakbot activity accounted for nearly all the malware URLs in Q1 2022.

Google.com subdomains – feedproxy.google.com, docs.google.com, and drive.google.com – had 4,345 URLs reported for serving malware in Q2-Q4 2021, but only 41 in Q1 2022. Loader malware was the most reported Malware Type across the three subdomains. Hancitor was the most reported Loader malware, accounting for 3292 of the 3381 malware URLs containing feedproxy.google.com. GuLoader was the most reported Loader among URLs containing drive.google.com.

Archive.org – also known as the Wayback Machine of the Internet Archive – provides a history of over 682 billion web pages on the Internet. Of the 1,381 malware URLs containing the domain name archive.org, 1,282 URLs resolved to archived web pages containing automatic phone dialers. These pages were flagged by commercial antivirus software as malicious and quarantined.

## Malware Mitigation Opportunities

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

**Cooperative efforts can mitigate malware**

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

**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**. They are well positioned to identify the origin addresses of users uploading malware to file sharing repositories, or running 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.

**Registrars and registries are positioned 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 could be used to identify malicious customers at the time of registration. All registrars and registries should be encouraged, contractually obliged, or compelled by law to investigate DNS or web site content abuse, including 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**. Malware is arguably a crime in all the countries and regions where domain names are used or registered. Malware 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.

**Legislation or regulation may be necessary to effectively mitigate malware threats**. Regulations that mandate accurate contact information from Internet as a Service operators [44], or that oblige operators to "lock and suspend" [45] a hosting or registration service while an investigation of a malware threat is conducted may provide protections against malware that currently do not exist across an ecosystem that has no single policy or administrative authority.

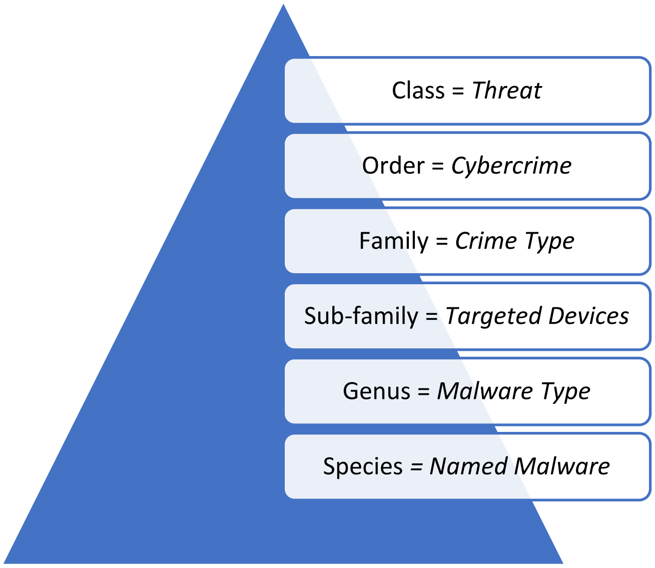
## Appendix A – Classifying Malware

For our malware studies, 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 security companies.

We began by "normalizing" metadata provided by MalwareURL 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[46]) as a baseline to create a taxonomic ranking, where:



The Order, *Cybercrime*, adopts the cyberthreats identified as cybercrimes in the Council of Europe's Convention on Cybercrime. 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.

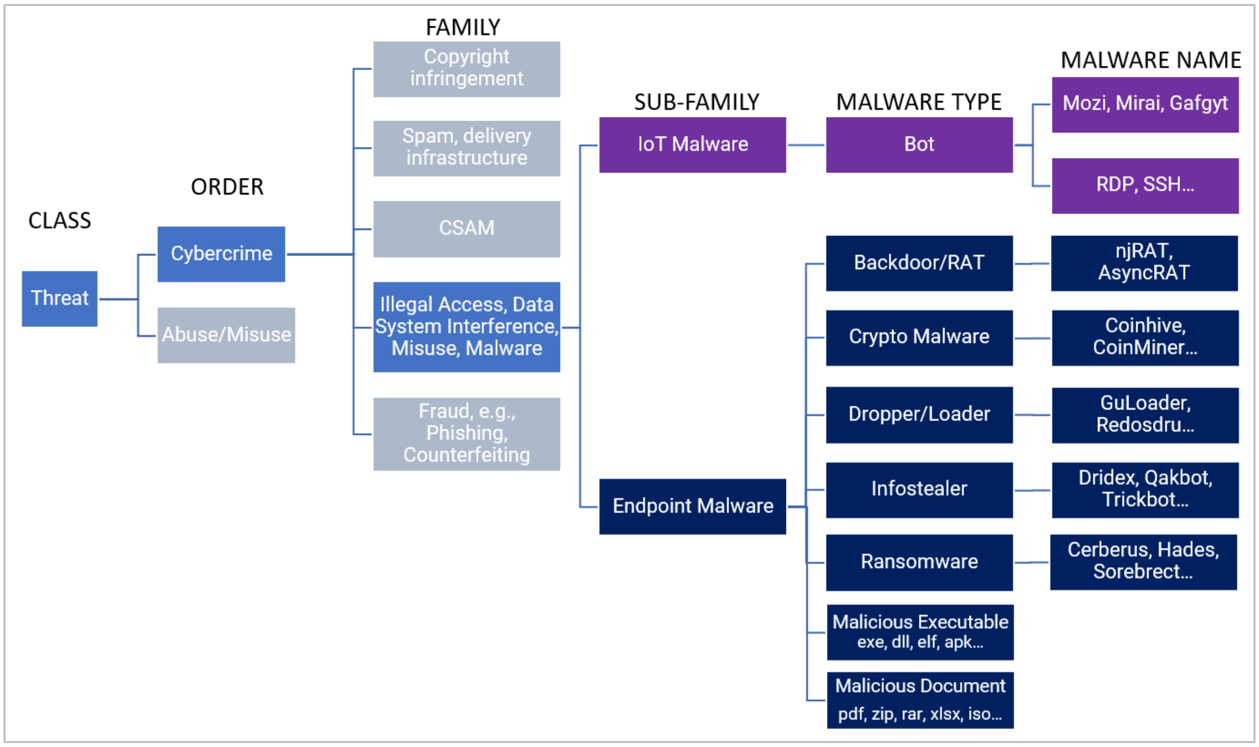


*Figure 4 Illustration of a Taxonomic Ranking of Malware*

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.[47]

**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.[48]

**Cryptocurrency malware**. Malware that targets cryptocurrency. Some cryptocurrency malware targets digital wallets (much like a banking trojan [49]) but others exploit or "hijack" the infected devices' resources to mine cryptocurrencies and are called *cryptojackers*.[50]

**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.[51, 52]

**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.[53]

**Malicious document**. Documents that contain harmful code, for example, an Office document that contains a malicious macro, or a PDF, compressed file, image, or archive (ISO) file that contains harmful code. Some malicious documents contain components or instructions for a malicious executable.[54] Also known as a "maldoc".

**Malicious executable**. A harmful, self-executing computer program, for example, a Windows, Linux, or Android application or app, a scripting language, or (Java) applet. Also known as malicious code or "malex",

**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.[55]

**Remote code execution.** Remote code execution (RCE) malware exploits vulnerabilities that can grant a malicious actor unauthorized access to a in computer program or operating system. Following a successsful exploitation, the attacker can execute any arbitrary code on the compromised remote host from a LAN the Internet.[56]

In most cases, we adopted a simplified Malware Type that is based on the CARO naming scheme.[57] When confronted with multiple names for a given malware, (*e.g.*, Quakbot, Qbot, Qakbot), we chose arbitrarily from these. To impose our classification on malware reports that do not provide sufficient information to identify a Malware Type and Malware Name, we submitted malware URLs to Virus Total, Hybrid Analysis, or ANY.RUN and augmented our metadata with information from these reports. While we still were unable to obtain a Malware Name in all attempts, we were able to associate a Malware Type to significantly more malware URLs.

# Appendix B – Key Statistics

## Key Malware Statistics from All Study Data

Table 6 summarizes the key malware statistics for the April 2021 – March 2022 period.

| Measurement | Endpoint Malware | IoT Malware | Uncategorized | Total |
|---|---|---|---|---|
| Unique domain names reported that were identified in malware reports | 49,872 | 76 | 67,307 | 110,833 |
| Top-level domains where we observed malware domains | 419 | 20 | 421 | 505 |
| Registrars that had domains under management reported for malware | 424 | 16 | 1,136 | 1,199 |
| Number of Internet Addresses (IPv4) where malware was hosted | 88,407 | 566,690 | 142,116 | 582,475 |
| Hosting Networks (ASNs) where malware web sites were reported | 3,779 | 5,085 | 3,212 | 7,871 |

*Table 6 Malware Statistics for April 2021 — March 2022*

## Key Malware Statistics from Endpoint Malware Data

Table 7 summarizes the endpoint malware statistics for the April 2021 – March 2022 period.

| Endpoint Malware | | | | |
|---|---|---|---|---|
| **Measurement** | **Apr-Jun 2021** | **Jul-Sep 2021** | **Oct-Dec 2021** | **Jan-Mar 2022** |
| Unique domain names reported that were identified in malware reports | 8,059 | 17,478 | 10,408 | 14,129 |
| Top-level domains where we observed malware domains | 255 | 235 | 256 | 287 |
| Registrars that had domains under management reported for malware | 234 | 198 | 207 | 333 |
| Number of Internet Addresses (IPv4) where malware was hosted | 145,090 | 106,178 | 107,236 | 23,675 |
| Hosting Networks (ASNs) where malware web sites were reported | 2,014 | 1,789 | 1,913 | 2,366 |

*Table 7 Endpoint Malware Statistics for April 2021 — March 2022*

## Key Malware Statistics from IoT Malware Data

Table 8 summarizes the IoT malware statistics for the April 2021 – March 2022 period.

| IoT Malware | | | | |
|---|---|---|---|---|
| **Measurement** | **Apr-Jun 2021** | **Jul-Sep 2021** | **Oct-Dec 2021** | **Jan-Mar 2022** |
| Unique domain names reported that were identified in malware reports | 21 | 31 | 10 | 14 |
| Top-level domains where we observed malware domains | 9 | 10 | 5 | 8 |
| Registrars that had domains under management reported for malware | 7 | 5 | 4 | 7 |
| Number of Internet Addresses (IPv4) where malware was hosted | 182,145 | 143,654 | 146,754 | 128,972 |
| Hosting Networks (ASNs) where malware web sites were reported | 2,143 | 1,878 | 1,907 | 2,898 |

*Table 8 Key IoT Malware Statistics for April 2021 – March 2022*

# Appendix C – 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.[58, 59, 60, 61, 62] 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.

We chose the following sources of malware reporting 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.[63, 64, 65]

**Malware Patrol.**[66] We use Malware Patrol's Business Protect feed for 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.**[67] The MalwareURL database uses proprietary software and analytic techniques to locate, assess and monitor suspected sources of web criminality, malware, Trojans and other web-related threats. The feed offers metadata that assists us in identifying malware types and families.

**URLhaus.**[68] Operated by abuse.ch, the URLhaus MalwareURL 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).**[69] 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 collected data covering the period April 1, 2021 to March 31, 2022. 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.[70] We relied upon RIPE-NCC's WHOIS [71] 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.[72] We used the Public Suffix List [73] 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 [74] for normalization. Some gTLD registries severely rate-limited [75] 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.

## 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 4). 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 original MalwareURL Type and URLhaus Tag fields as appropriate).

## About the Authors

**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-Phishing 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

## 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.
- Malware subject matter experts at Malware Patrol, URLhaus, MalwareURL, and at Netenrich and Bambenek Labs for their assistance with our effort to create a taxonomic ranking of malware.
- The Virus Total. ANY.RUN and Hybrid Analysis communities and teams who provide exceptional malicious code analysis tools or services.
- All the security personnel who fight malware.

# Citations

[1] 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.

[2] The SolarWinds Cyber-Attack: What You Need to Know, Center for Internet Security https://www.cisecurity.org/solarwinds

[3] Kaseya: Incident Overview & Technical Details https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961

[4] Understanding Russia’s Cyber Strategy, Foreign Policy Research Institute https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/

[5] The World Joins the Full-Scale Cyber War as Russia Invades Ukraine https://socprime.com/blog/latest-threats/the-world-joins-the-full-scale-cyber-war-as-russia-invades-ukraine/

[6] Malware-as-a-Service is a Booming Business, Info Security https://www.infosecurity-magazine.com/opinions/malware-service-booming-business/

[7] 2022 Unit 42 Ransomware Threat Report, Palo Alto Networks https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/

[8] 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).

[9] 2022 State Of Financial Crime Report, ComplyAdvantage https://complyadvantage.com/press-media/complyadvantage-releases-2022-state-of-financial-crime-report/

[10] 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

[11] 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

[12] 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

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

[14] Phishing Landscape 2021: An Annual Study of the Scope and Distribution of Phishing https://interisle.net/PhishingLandscape2021.html

[15] Definition of hosting network (ASN), Cybercrime Information Center https://www.cybercrimeinfocenter.org/terminology#hostingnetwork

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

[17] 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

[18] Virus Total https://virustotal.com

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

[20] ANY.RUN Interactive malware hunting service https://any.run/

[21] Cybercrime Information Center, Malware Activity Reports https://cybercrimeinfocenter.org/malware-activity

[22] Cyberattacks Targeting Latin America, January through March 2021 https://www.f5.com/labs/articles/threat-intelligence/cyberattacks-targeting-latin-america-january-through-march-2021

[23] https://urlhaus.abuse.ch/statistics/#top_malware

[24] Breaking Down Mirai: An IoT DDoS Botnet Analysis https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/

[25] Some details of the DDoS attacks targeting Ukraine and Russia in recent days https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/

[26] CVE-2021-44228 Detail, National Vulnerability Database https://nvd.nist.gov/vuln/detail/CVE-2021-44228

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

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

[29] CISA Alert (TA18-201A) Emotet Malware https://www.cisa.gov/uscert/ncas/alerts/TA18-201A#:~:text=Emotet%20Malware%201%20Systems%20Affected%202%20Overview.%20Emotet,SLTT%20governments.%20...%204%20Impact%205%20Solution.%20

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

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

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

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

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

[35] Gafgyt, Trend Micro Threat Encyclopedia
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/GAFGYT/

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

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

[38] DomainTools
https://www.domaintools.com/

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

[40] Malware Landscape 2021: A Study of the Scope and Distribution of Malware
https://interisle.net/MalwareLandscape2021.html

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

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

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

[44] H.R. 6352: DRUGS Act
https://www.govtrack.us/congress/bills/117/hr6352

[45] Executive Order 13984 of January 19, 2021, Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities
https://www.federalregister.gov/executive-order/13984

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

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

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

[49] 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/

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

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

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

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

[54] 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

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

[56] Remote code execution (RCE), explained: what it is and how to prevent it

https://blog.sqreen.com/remote-code-execution-rce-explained

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

[58] 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

[59] 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

[60] 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

[61] 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/

[62] 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

[63] 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

[64] 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

[65] 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

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

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

[68] URLhaus MalwareURL Exchange
https://urlhaus.abuse.ch/

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

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

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

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

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

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

[75] 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