Malware Landscape 2023

A Study of the Scope and Distribution of Malware

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

14 March 2023

Interisle
Consulting Group

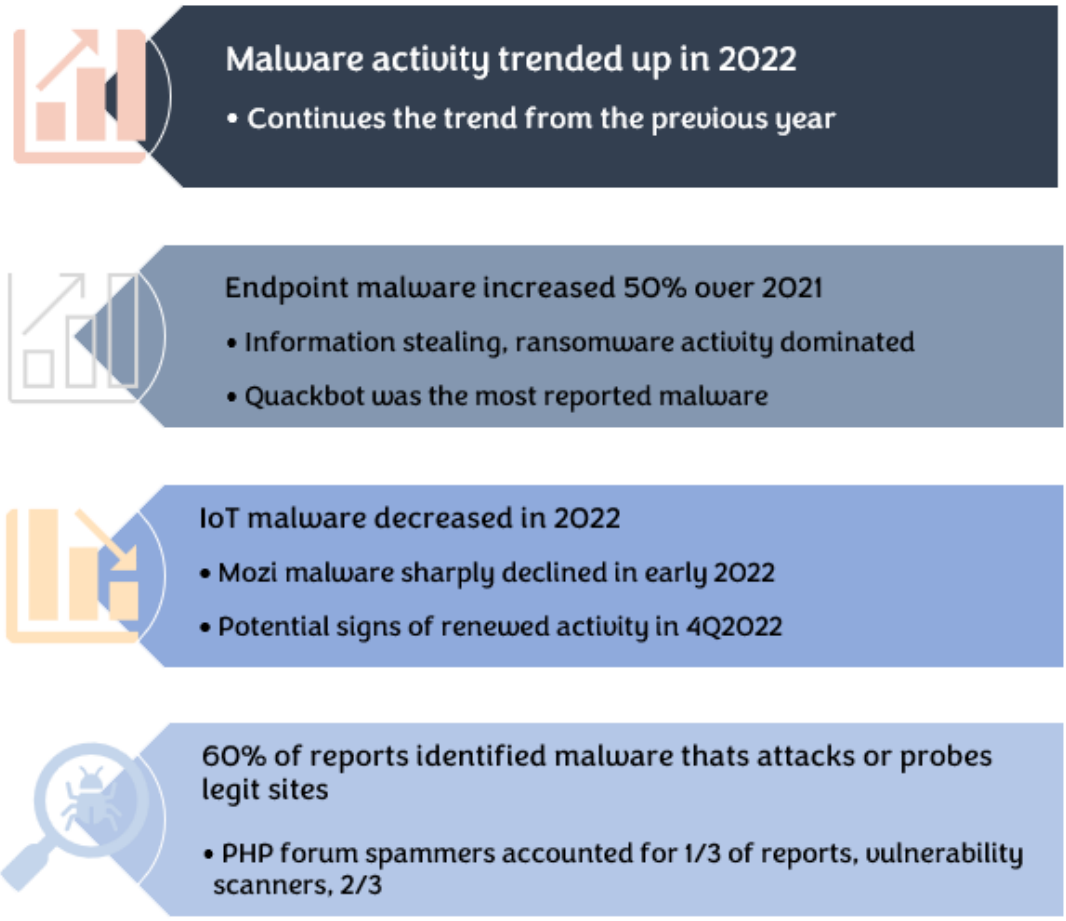
Executive Summary

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

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

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

Principal Findings



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

- Malware hosting tends to be regionalized

Use of domain names for malware distribution grew sharply

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

Future Opportunities

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

HOSTING & CLOUD SERVICE PROVIDERS

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

DOMAIN REGISTRARS & REGISTRIES

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

ALL OPERATORS

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

TARGETS OF MALWARE

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

Introduction

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 used threat intelligence data collected and curated at the Cybercrime Information Center. We captured and analyzed over 7 million malware reports during a 12-month study period (January 2022 to December 2022) from four widely used and respected threat intelligence sources: Malware Patrol, MalwareURL, Spamhaus, and URLhaus. We removed duplicates from this set of malware reports, resulting in nearly 4 million records of distinct malware events. These malware 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.

The malware landscape is extraordinarily diverse. 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 or *endpoint device* malware is commonly used for financial fraud, data exfiltration or theft; IoT device malware is commonly used for denial-of-service attacks, to create criminal infrastructures ("botnets"), or as launch points for deeper network infiltration.

In 2022, we began processing reports that identified origins or sources of malicious traffic, *e.g.,* form and forum traffic injectors, scanners, and other forms of attackware. This new sub-family, *Malicious Traffic Sources* (aka Malicious IPs), accounted for 61% of the malware records for which we had sufficient information to classify the malware.

We studied each sub-family of malware separately.

The Malware Study: 2022 Year in Review

572
Top-level domains where we observed malware hosting

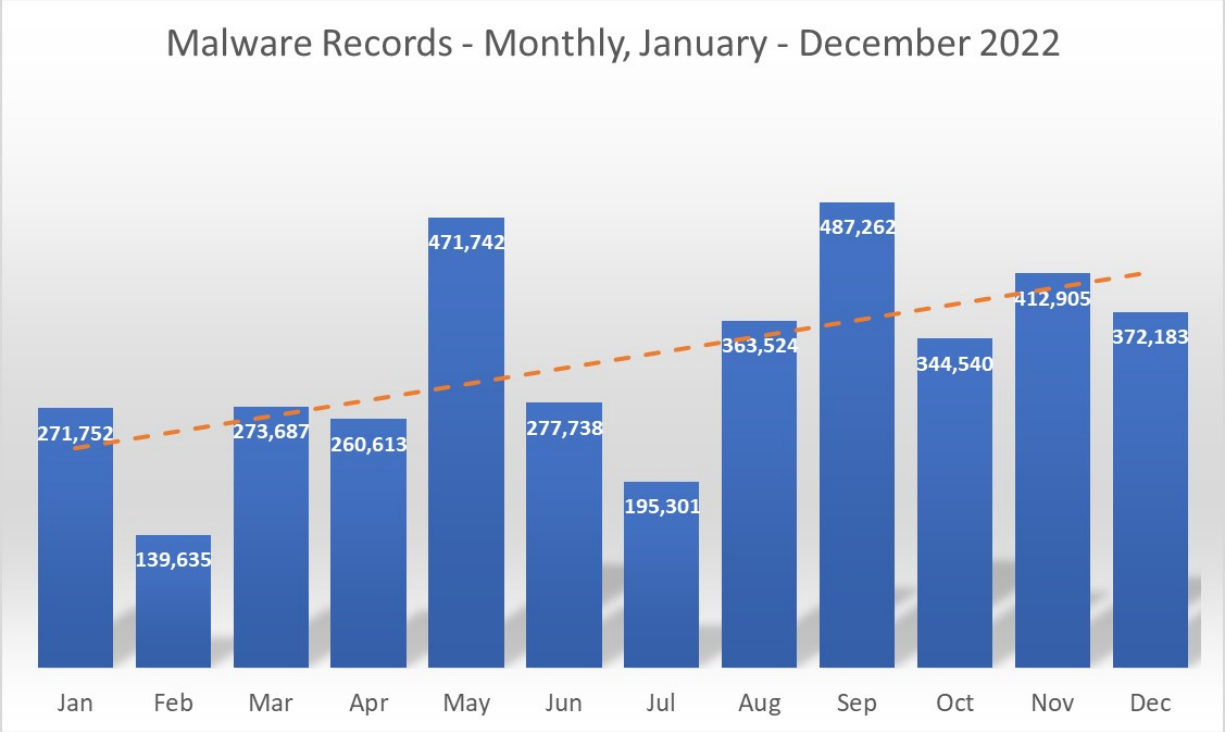
116,639
Domain names reported for serving up malware

1,168
Registrars with gTLD domains reported for serving malware

2,973,858
IPv4 addresses reported as serving or distributing malware

27,791
ASNs where we observed malware hosting

Malware activity trended up in 2022



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) and address prefixes within autonomous systems in this study; we identify the hosting services or cloud services that criminals misuse to serve or distribute malware by Autonomous System Number (ASN).

We extracted the IP addresses of hosts reported for hosting malware and malicious traffic sources from address-based URLs that were reported for serving or distributing malware. We 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.

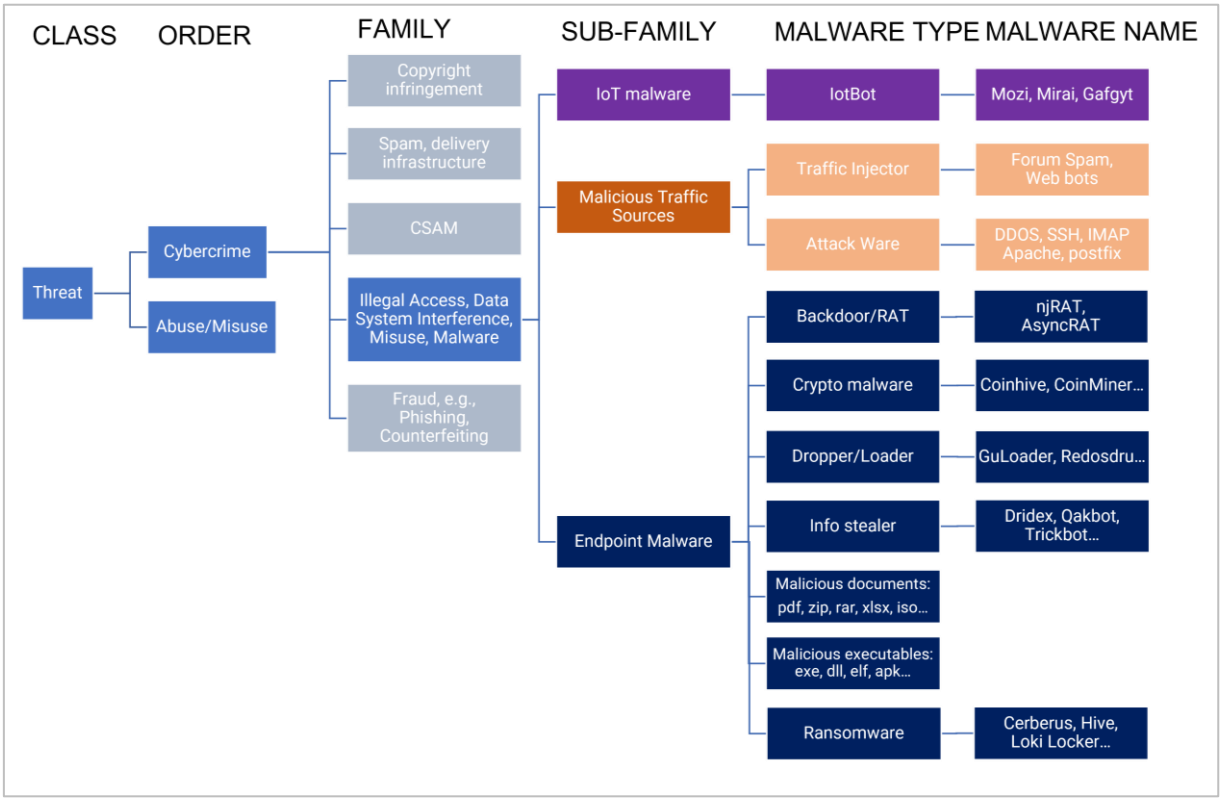
An IP address prefix, also known as a subnet, is the portion of an IP address that is used to identify a contiguous block of IP addresses. Here we include IP address prefixes that were identified as having a minimum of 10,000 malware reports. Here, we list the most reported malware, by IP address prefixes, hosting network and geolocation:

IPv4 addresses assigned to networks in the United States and China have the highest malware report figures

IP prefix	# Malware Records	Assigned to	IP Prefix Geolocation
36.248.0.0/14	72,433	UNICOM China169 Backbone	China
104.17.0.0/20	69,260	Cloudflare	California, US
115.48.0.0/12	40,718	UNICOM China169 Backbone	Henan, China
182.112.0.0/12	40,404	Unicom Henan Province	Henan, China
52.217.64.0/20	38,610	Amazon	Virginia, US
13.225.64.0/21	36,352	Amazon	New Jersey, US
42.224.0.0/12	32,516	Unicom Henan Province	Henan, China
157.185.146.0/24	23,227	Quantil Networks	California, US
125.40.0.0/13	20,037	Unicom Henan Province	China
27.40.0.0/13	17,117	Unicom Guangdong Province	China
123.8.0.0/13	16,306	Unicom Henan Province	China
222.136.0.0/13	15,973	Unicom Henan Province	China
112.224.0.0/11	13,127	Unicom Shandong Province	China
27.192.0.0/11	12,747	Unicom Shandong Province	China
61.162.0.0/16	10,970	Unicom Shandong Province	China
61.52.0.0/15	10,101	Unicom Henan Province	China

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. Refer to the Cybercrime Information Center, Measurements, for a mapping of the Convention's Articles and Guidelines onto cyber threats, including malware.



In our taxonomy, we identify three 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)

Malicious IP Sources are IPv4 addresses of hosts that were determined to be origins of malicious traffic including attackware (such as vulnerability scanners) and traffic injectors (such as forum or form spammers and web bots)

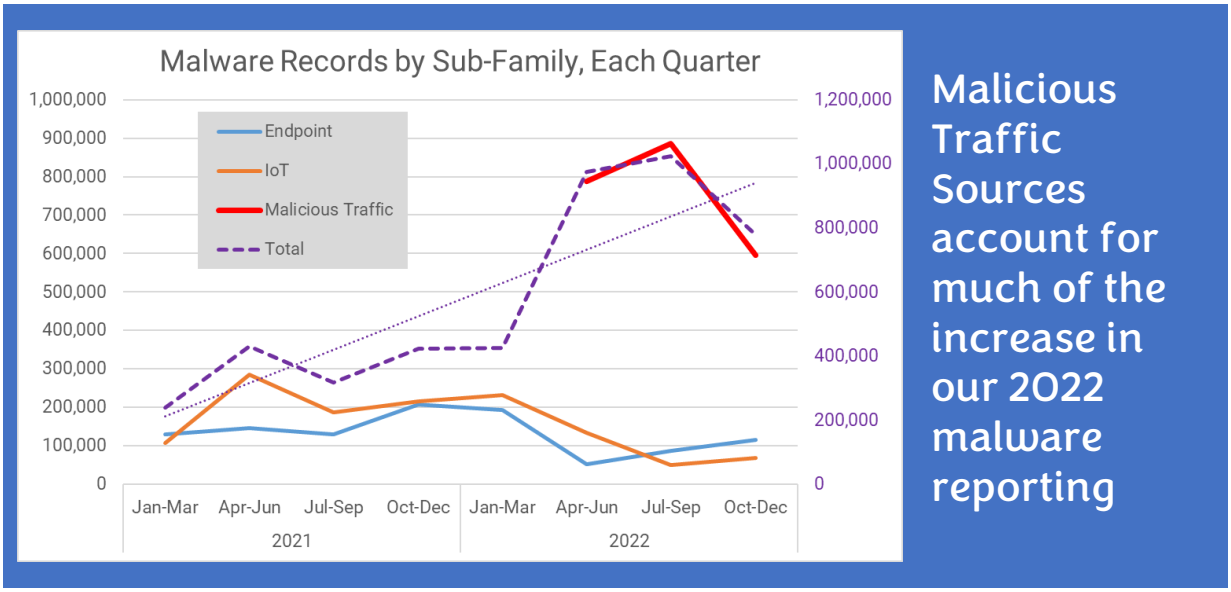
Two of our threat intelligence feeds identify malware URLs, IP addresses, or domain names, but do not identify malware by name nor provide the metadata that we require to assign malware to a Malware sub-family.

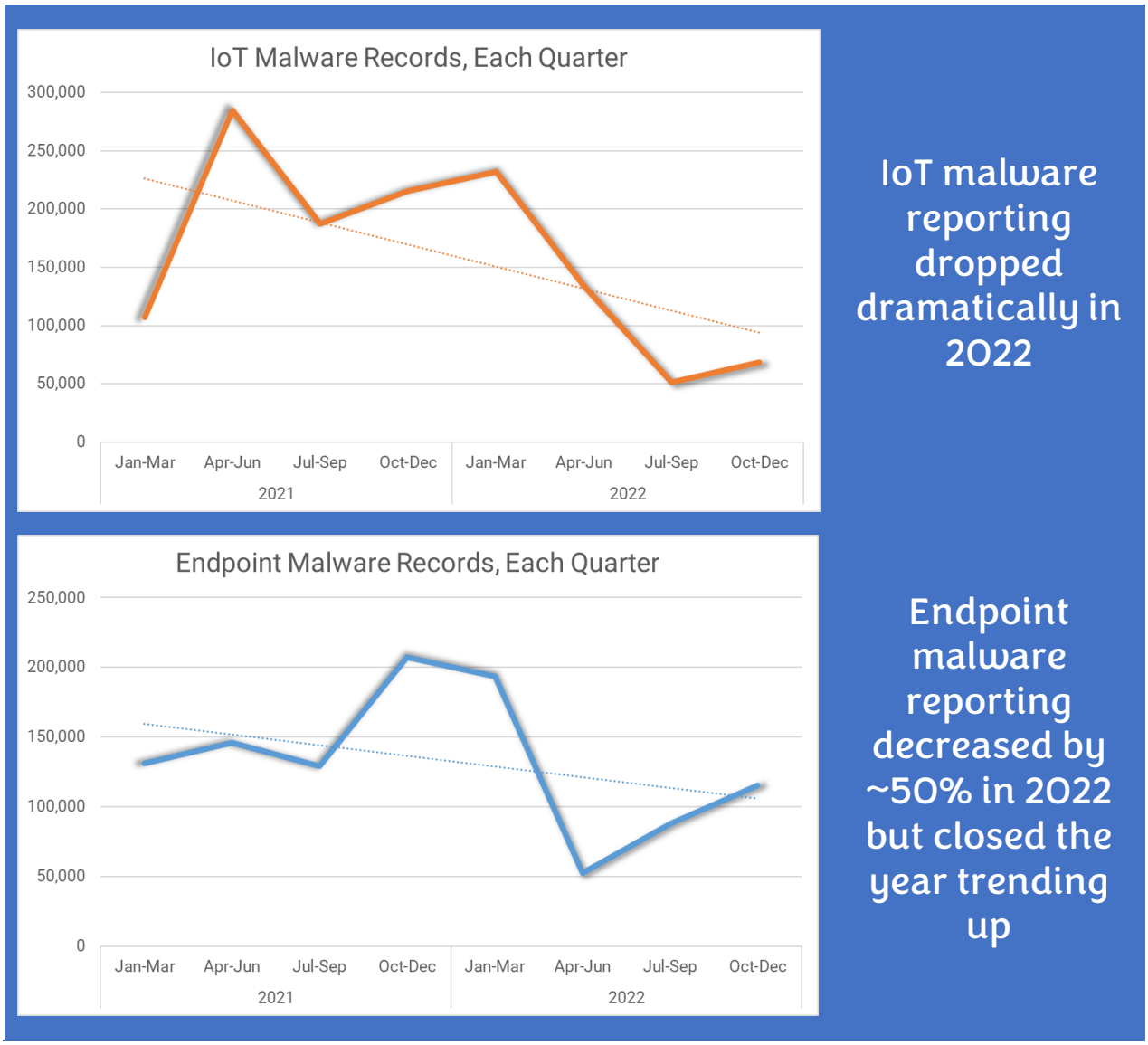
We further attempted to apply our classification to reports that did not provide metadata by submitting URLs to one or more of three malware analysis services: Virus Total, Hybrid Analysis, and ANY.RUN. Where available, we augmented our metadata with information from these reports.

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

Where insufficient information existed to determine if a report was *IoT Malware*, *Endpoint Malware,* or *Malicious Traffic Sources* we considered that report to be *Uncategorized*. Uncategorized malware reporting is important in understanding overall malware activity. We include all malware reports – IoT, Endpoint, Malicious Traffic Sources, 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 following tables, charts, and analyses in this study focus on the IoT, Endpoint, and Malicious Traffic Sources sub-families.





Quarterly and quarter-over-quarter counts of Malware Activity are published at the [Cybercrime Information Center's Malware Activity pages](#).

Our analyses of each of these sub-families follow.

IoT Malware

Internet of Things (IoT) Malware targets devices – routers, sensors, DVR or IP cameras, wearables, and embedded technologies. We processed 467,319 IoT Malware records in 2022, a marked reduction from 2021. We attribute much of the decrease to a decline in Mozi malware reporting.

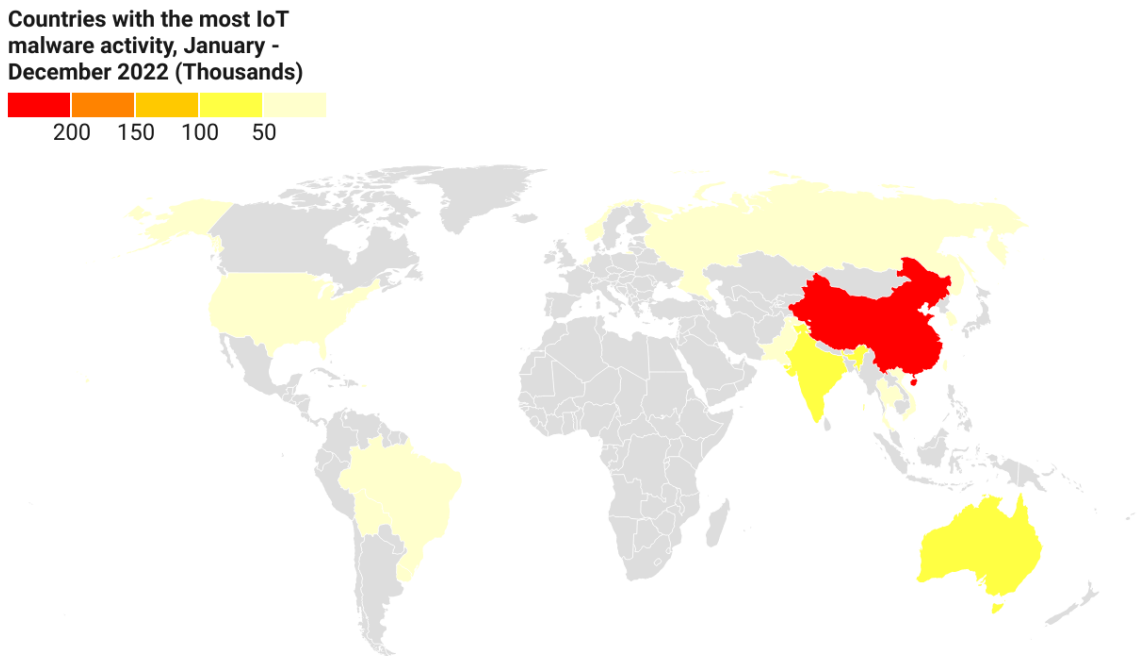
Counts (raw numbers) of reported IoT Malware reveal the intended misuse of infected devices. Large numbers (often thousands) of infected IoT devices are used to conduct volumetric denial of service attacks; in such attacks, these devices send traffic at a target, intending to overwhelm ("flood") the targeted server or network and disrupt its services. In some cases, denial of service attackers may try to extort the target, but in other cases, their 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.

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 advanced persistent threat presence (APT), poses problems for parties who report or measure malware: some reporters name the initial stage malware, some report subsequent stages, and others report everything they find. The introduction of the malicious traffic sources sub-family introduces the possibility of more reporting diversity, as malware-infected devices may be reported as scanners or injectors. We continue to believe that our malware counts are underreported generally.

We determined the countries where the most IoT malware was reported, by number of malware records and by percent of the malware records for which we could determine a country used. By representing these in this heat map, we illustrate where IoT malware activity was most intense, by total IoT records.

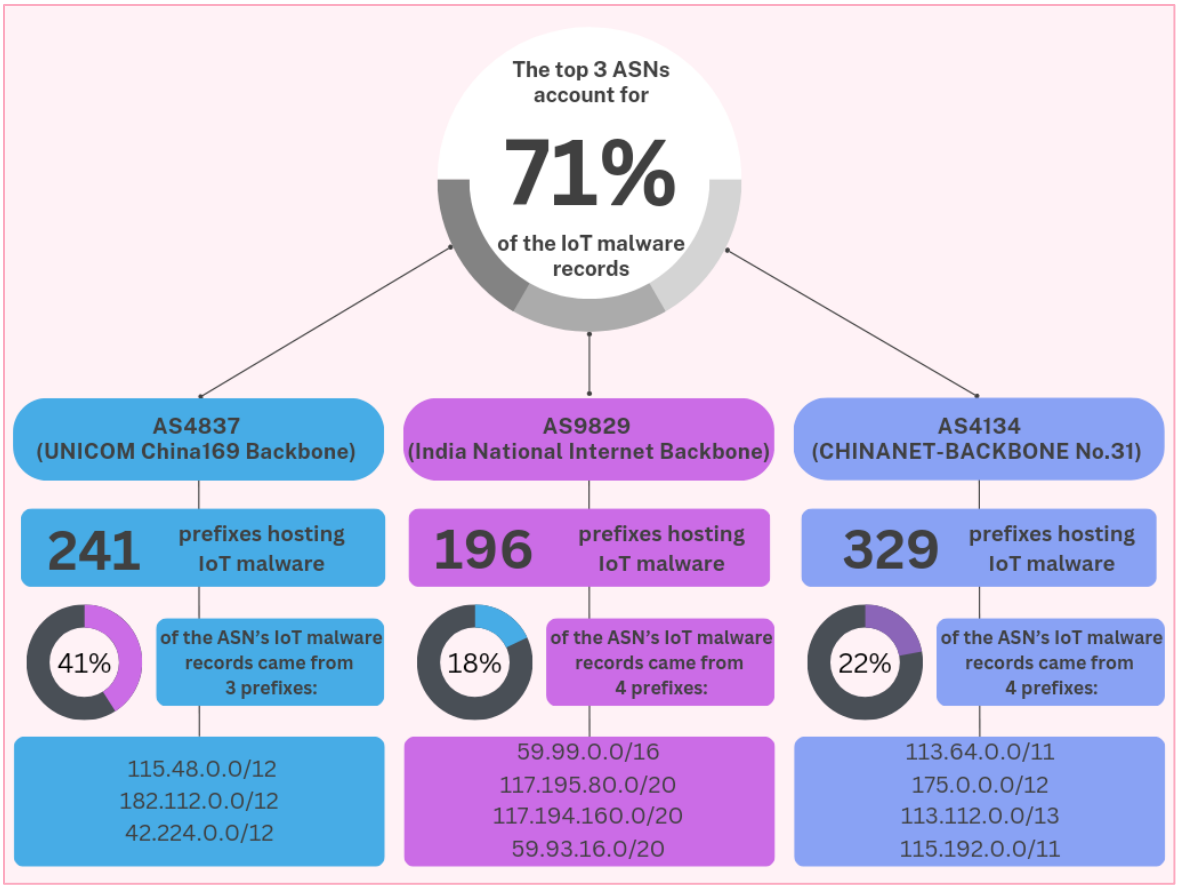
Heat map: IoT malware reported



Source: Cybercrime Information Center • Created with Datawrapper

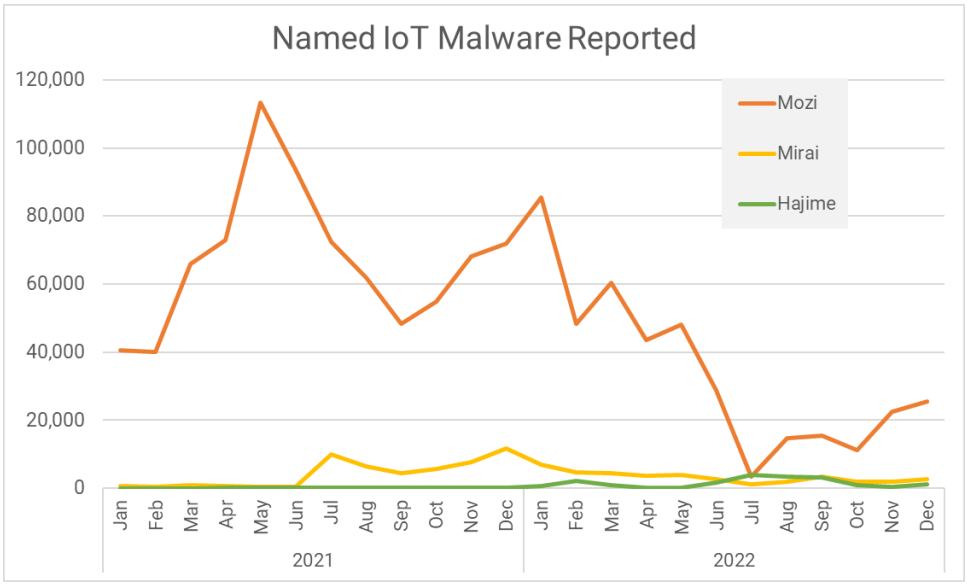
The top 10 hosting networks most frequently reported for hosting IoT malware are operated in China and India

Rank	AS Name	AS number	Country	Unique IoT Malware Addresses	Total IoT Malware Records ▼
1	UNICOM China169 Backbone	4837	China	110,827	**204,060**
2	National Internet Backbone	9829	India	41,971	**65,542**
3	CHINANET-BACKBONE No.31	4134	China	35,773	**63,112**
4	China169 Guangdong province	17816	China	18,784	**31,742**
5	Hathway IP Over Cable Internet	17488	India	3,550	**5,093**
6	HINET Data Communications	3462	China	3,487	**4,740**
7	China Unicom Shenzen network	17623	China	2,078	**3,334**
8	Netplus Broadband Services	133661	India	1,932	**3,172**
9	Mahanagar Telephone Nigam Ltd	17813	India	1,988	**3,032**
10	China Unicom Guangzhou network	17622	China	2,010	**2,751**



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.

Mozi malware reports show a decline in early 2022 but potential signs of renewed activity in 4Q2022

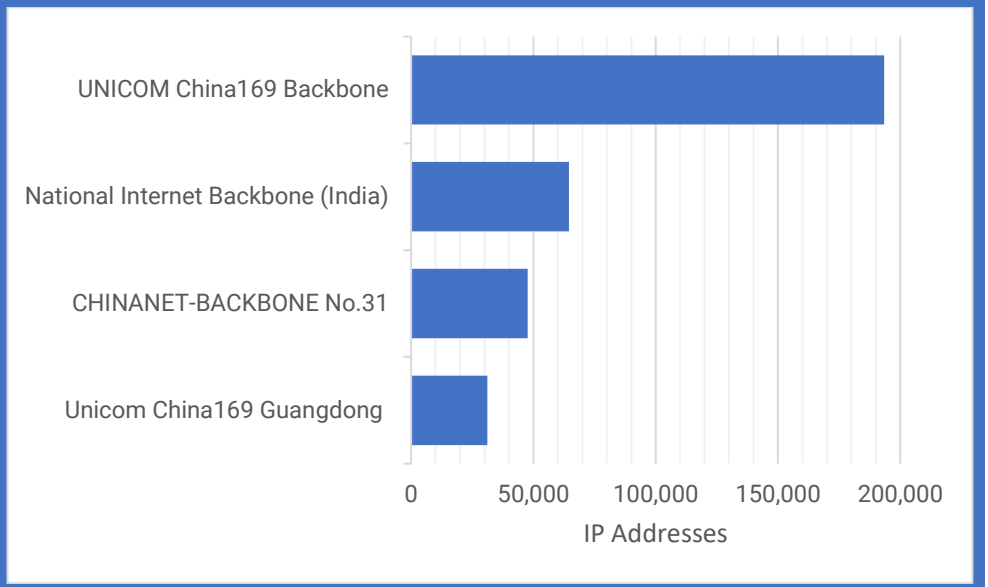


Mozi Malware

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.

In our 2022 Malware Landscape study, covering April 2021 through March 2022, we reported that the 10 ASNs accounted for 89% of the addresses reported as hosting Mozi and the top 30 ASNs account for 94%. We observed nearly the same concentration for this landscape study: covering January through December 2022, where 5 ASNs accounted for 83% of the addresses reported as hosting Mozi, ten ASNs accounted for 87%, and the top 30 ASNs for 94%.

IPv4 addresses most frequently reported for hosting Mozi malware were in China and India

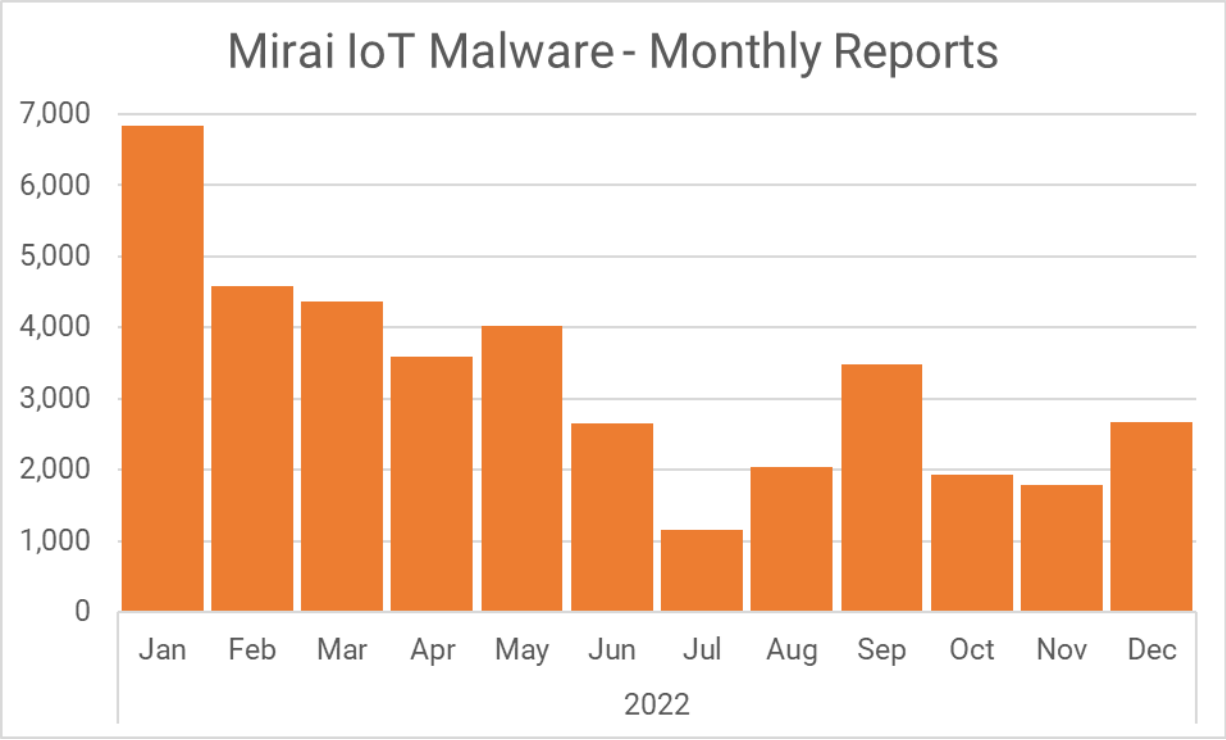


IP prefix	Mozi reports	ASN	IP Prefix Geolocation
115.48.0.0/12	29,005	4837	Henan, China
182.112.0.0/12	28,979	4837	Henan, China
42.224.0.0/12	23,470	4837	Henan, China
125.40.0.0/13	14,796	4837	Henan, China
27.40.0.0/13	13,602	17816	Guangdong, China
123.8.0.0/13	11,037	4837	Henan, China
222.136.0.0/13	10,908	4837	Henan, China
61.52.0.0/15	8,158	4837	Henan, China
27.192.0.0/11	7,605	4837	Shandong, China
112.224.0.0/11	7,389	4837	Shandong, China

The ten IPv4 address prefixes most frequently reported for hosting Mozi malware are in three China provinces

Mirai Malware

Mirai malware variants appeared throughout our 2022 study period and were among the IoT malware that was associated with botnet-based DDoS attacks against Ukraine.

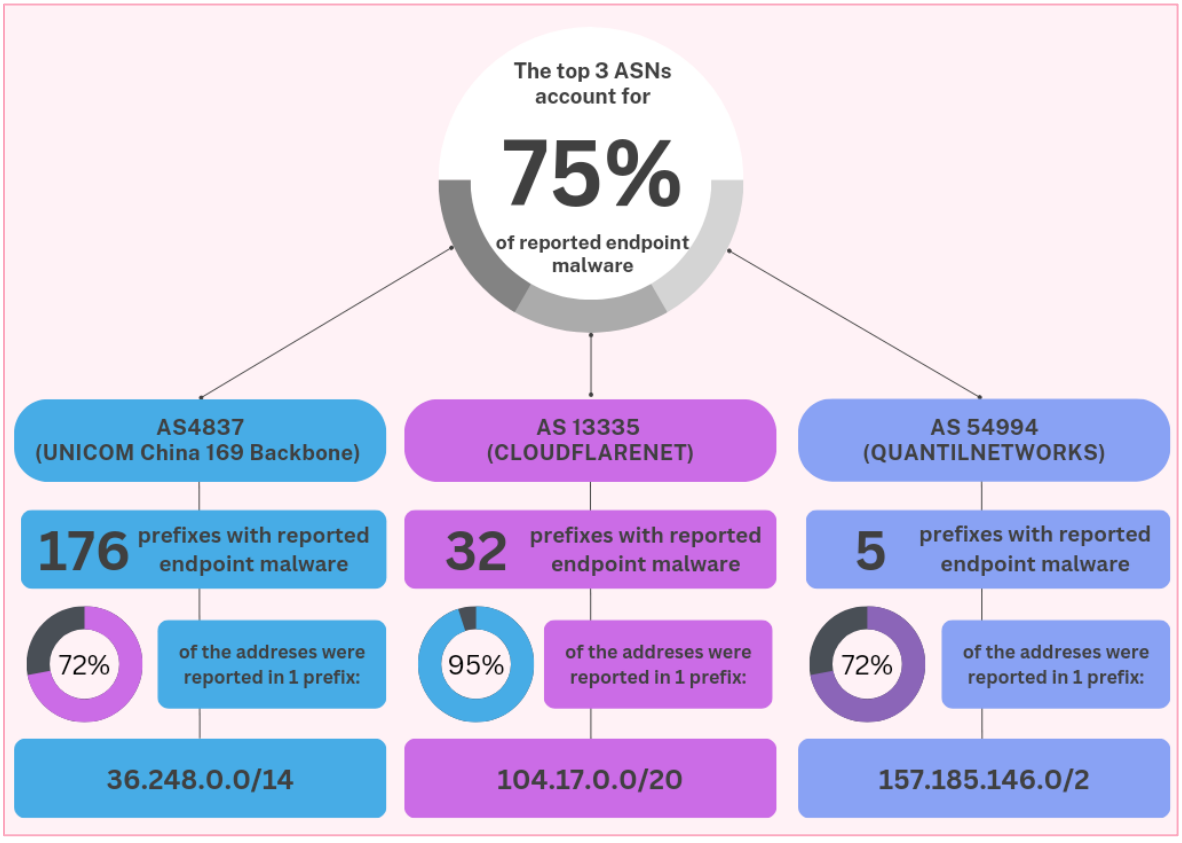


Endpoint Malware

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. For example, 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. Here, we report on the malware types that we classify as endpoint malware.

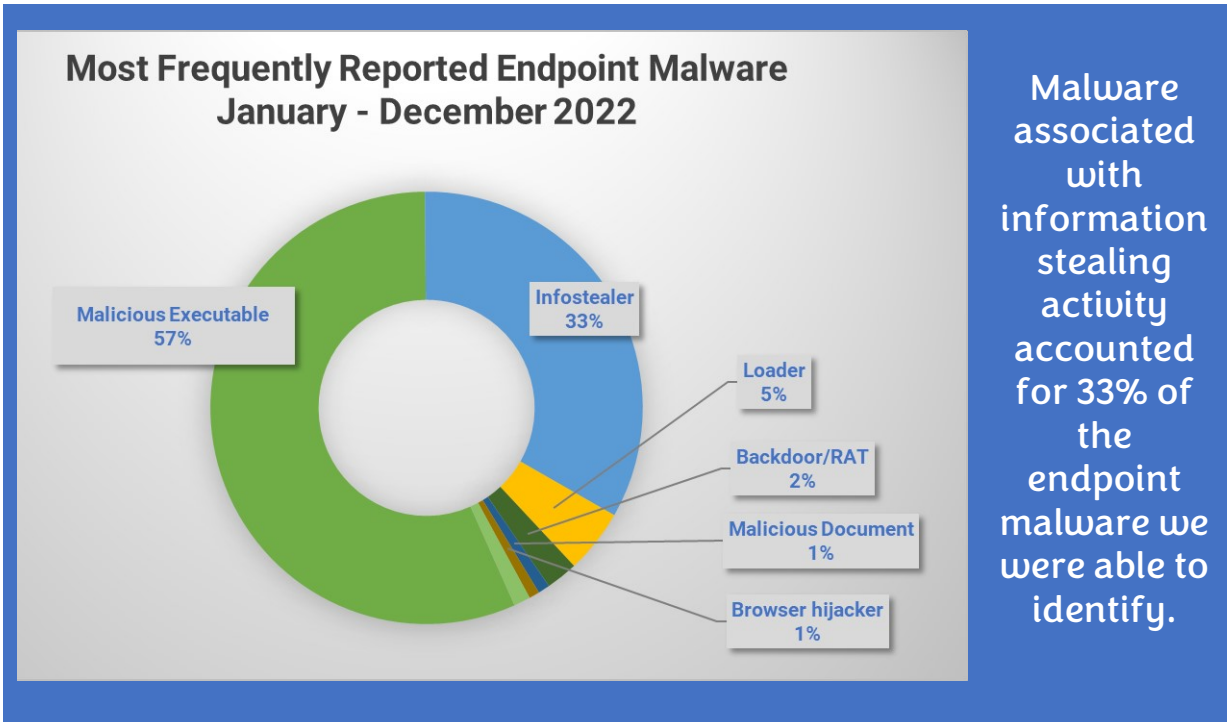
Classifying Endpoint Malware by Malware Type

Malicious Executable was the most reported endpoint malware type in our Malware Landscape 2022 study at 51% and is again in this 2023 landscape study, at 56%. 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.



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”.

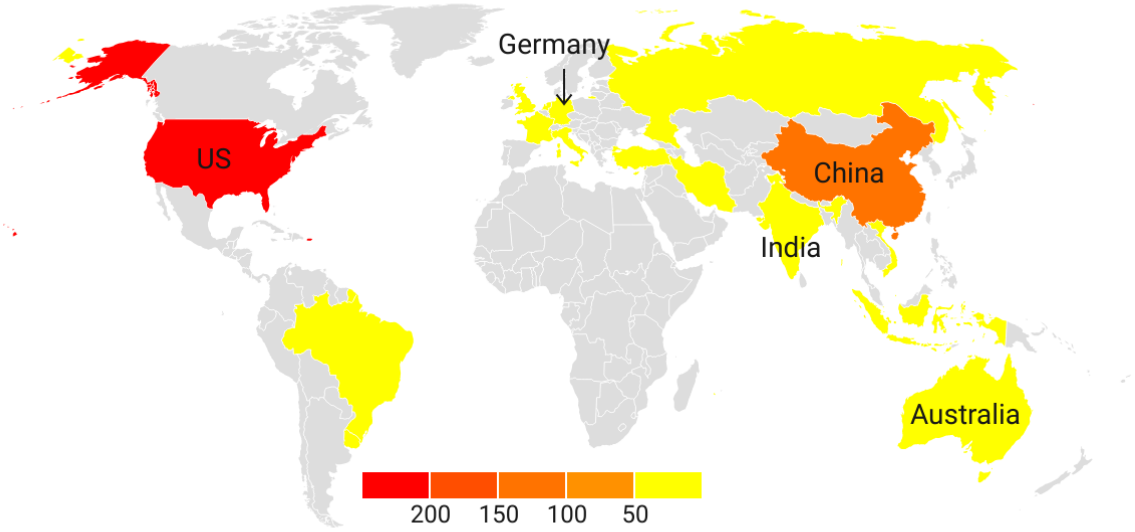
The Infostealer portion of endpoint malware increased dramatically from our 2021 study, from 16% to 33%.



Ransomware receives the most attention, particularly where attacks by criminal groups, *e.g.*, Hive, have victimized healthcare IT systems for millions of dollars. These are appropriately prosecuted aggressively by law enforcement. Financial losses attributed to information stealers are typically smaller, but prominent malware gangs are combining banking trojan with ransomware in a multi-stage attack sequence called big game hunting.

We determined the countries where the most endpoint malware was reported, by number of malware records and by percent of the malware records for which we could determine a country used. By representing these in this heat map, we illustrate where endpoint malware activity was most intense, by total endpoint records.

Heat map: endpoint malware reported (thousands)



Source: Cybercrime Information Center • Created with Datawrapper

Endpoint malware was most frequently reported against networks in China and the United States

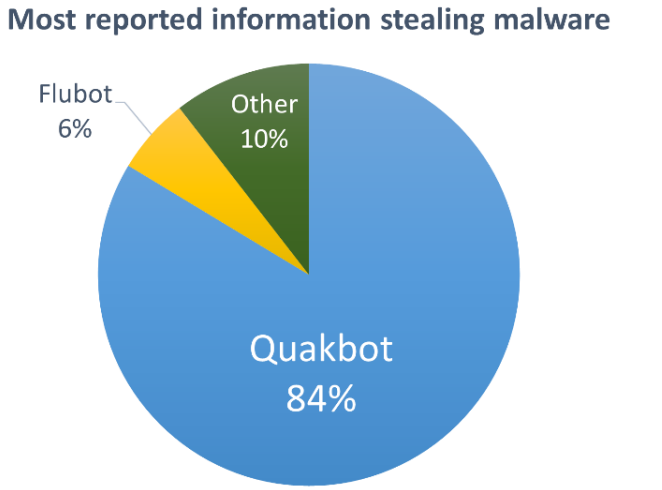
Rank	AS Name	AS number	Country	Unique Endpoint Malware Addresses	Total Endpoint Malware Records ▼
1	UNICOM China169 Backbone	4837	China	15,739	**99,955**
2	CLOUDFLARENET	13335	United States	4,805	**53,491**
3	UNIFIEDLAYER	46606	United States	4,298	**36,012**
4	QUANTILNETWORKS	54994	United States	7	**31,449**
5	NAMECHEAP	22612	United States	1,733	**9,129**
6	National Internet Backbone	9829	India	6,394	**6,954**
7	NETWORK-SOLUTIONS	19871	United States	1,282	**6,772**
8	China Unicom IP network	133119	China	3	**5,956**
9	OVH SAS	16276	France	1,151	**5,664**
10	CHINANET-BACKBONE No.31	4134	China	5,149	**5,539**

To identify endpoint malware by name, we used tags provided by our feeds. As we did for IoT malware, we submitted samples of these URLs to community malware analysis services to see these could be classified by name.

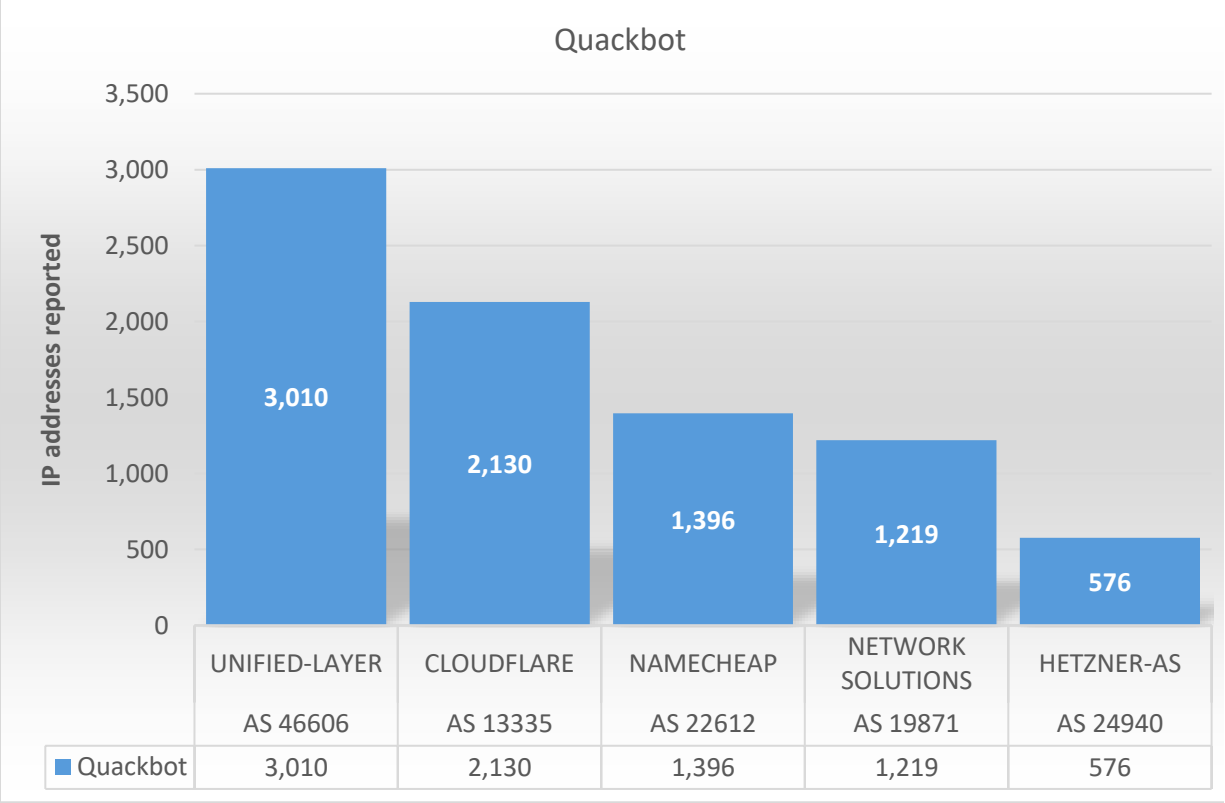
Quackbot was the most reported information stealing malware...

Quackbot

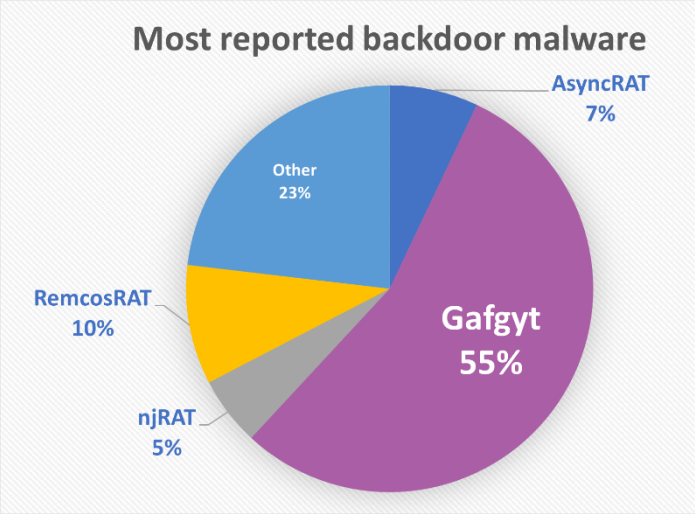
is a banking trojan that has persisted in the wild since 2007, largely due to stealth and self-propagating characteristics. It behaves as a man-in-the-middle browser – it alters what victims see when they visit a bank web site and captures bank credentials and online session information.



... and the hosting networks with the most IPv4 addresses reported for hosting Quakbot were



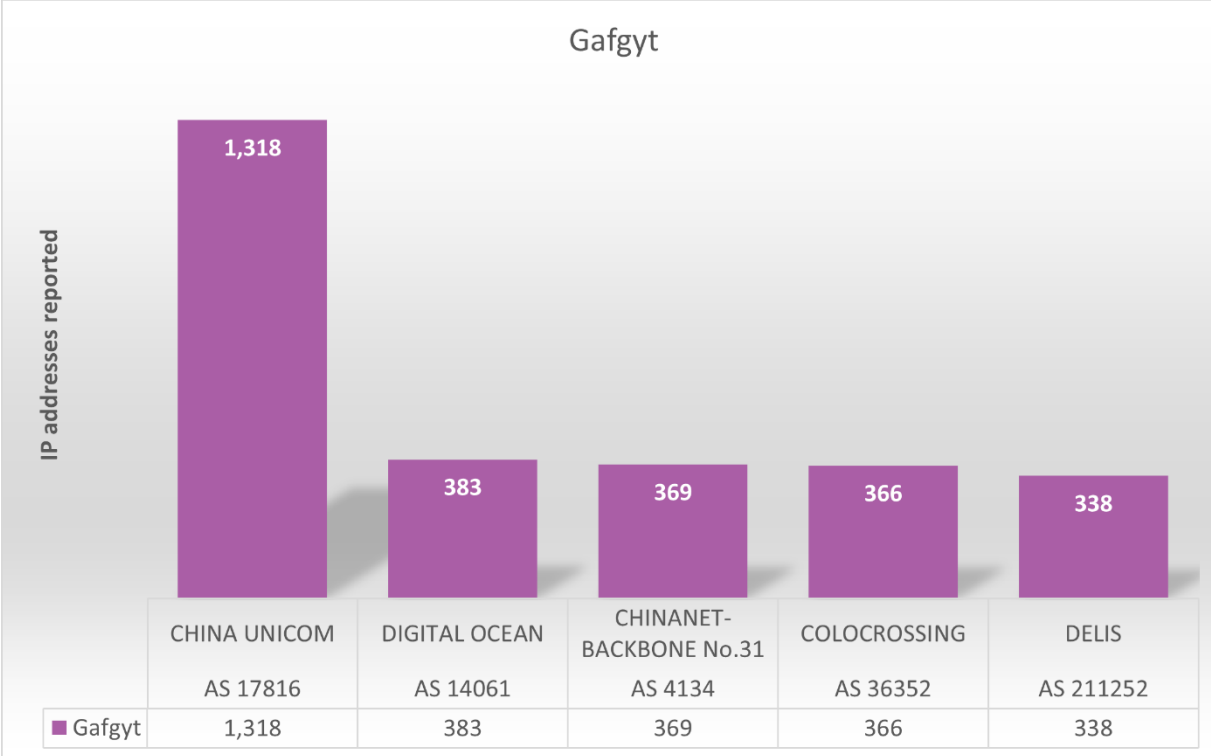
Gafgyt was the most reported backdoor malware...



Gafgyt

targets Linux devices. Infected devices are often used in large scale DDoS attacks.
Under constant evolution since 2014, Gafgyt uses Shellshock for its initial compromise, and like Mirai, it propagates by brute-forcing weak Telnet passwords.

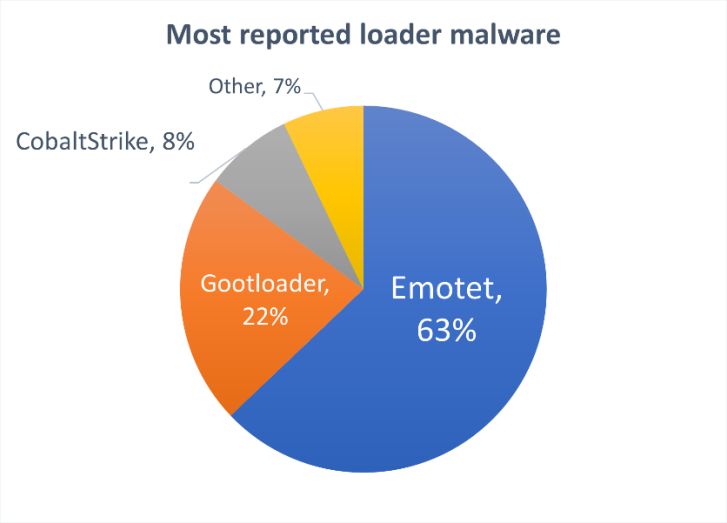
... and the hosting networks with the most IPv4 addresses reported for hosting Gafgyt were



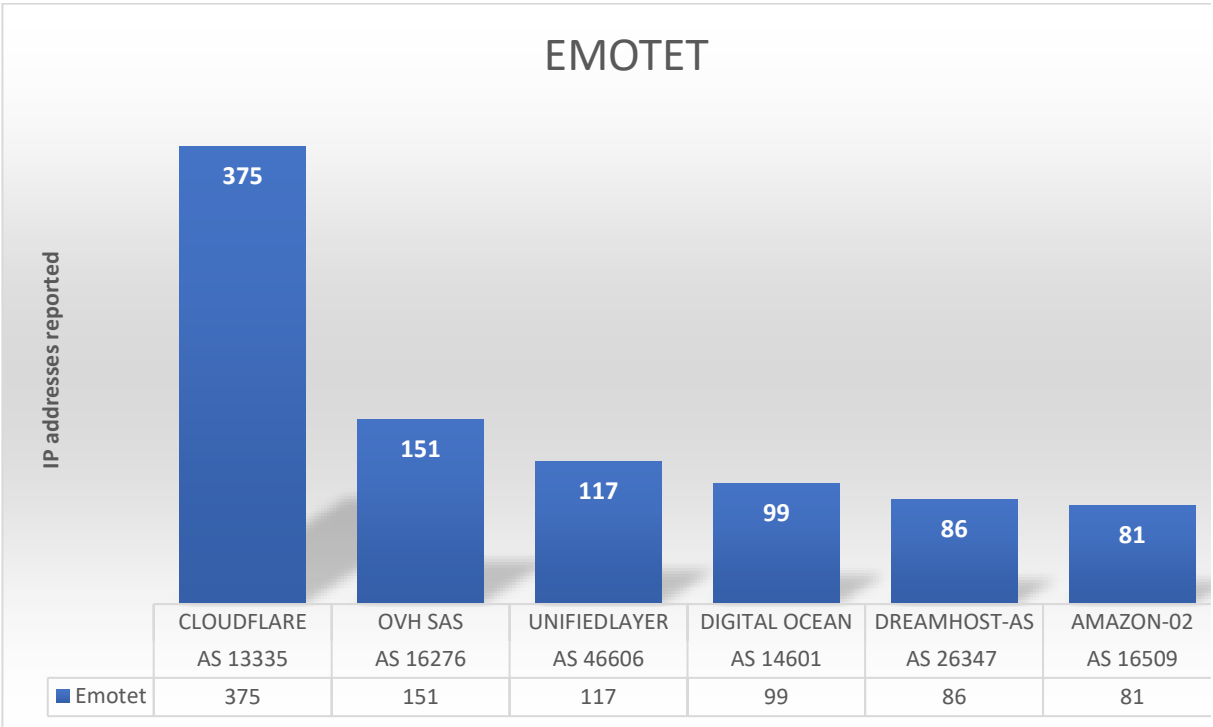
Emotet was the most reported loader malware...

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.



... and the hosting networks with the most IPv4 addresses reported for hosting Emotet were



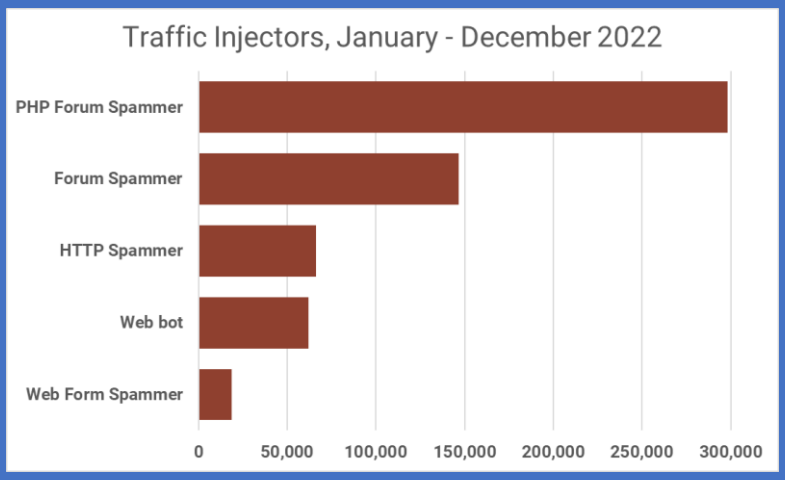
Malicious Traffic Sources

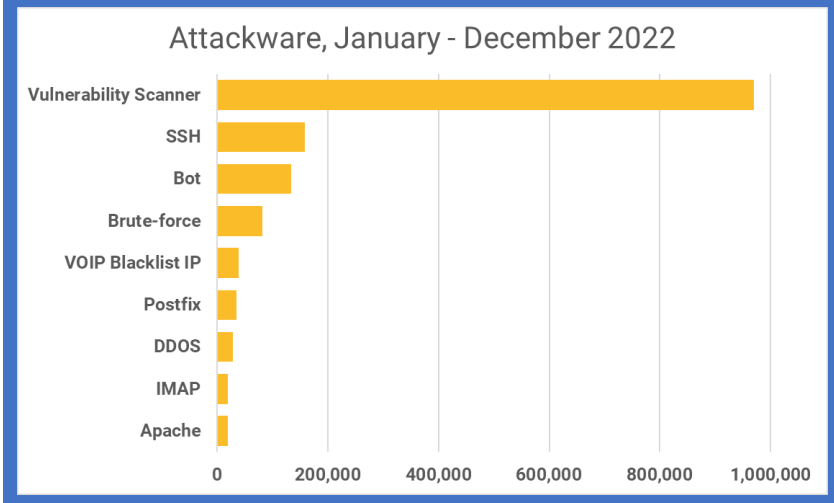
In the Malicious traffic sources sub-family, we include IP addresses of scripts or executables that are identified as hosting malware that was used "offensively" for malicious purposes. Reports of such malware identify the origins of these attacks. This sub-family includes:

Traffic injectors – malicious executables that operate from infected devices (the sources) to insert unwanted or malicious content into web forms or computer processes. Some injectors, *e.g.*, PHP, HTTP, or Web form spammers, visit web sites, copy or "scrape" forms from that site, and then submit advertisements (aka malvertising), malicious URLs, or inappropriate data into such forms. Some traffic injectors perform process injection. We also included here infected devices that host credential-stuffing bots or captcha bypass bots, or bots that disrupt merchant services (bidding snipers, download stat boosters).

Attackware – malicious executables that have been reported for targeting systems with traffic that scan for ways to disrupt or break into targeted systems or services. Here, we include reports of attacker IP addresses that scan target services – *e.g.*, Apache, IMPA, FTP, Postfix, SSH – for vulnerabilities that may be subsequently exploited. We also include reports of IPs that are participating in DDOS.

PHP forum spammers accounted for 35% of reported traffic injectors



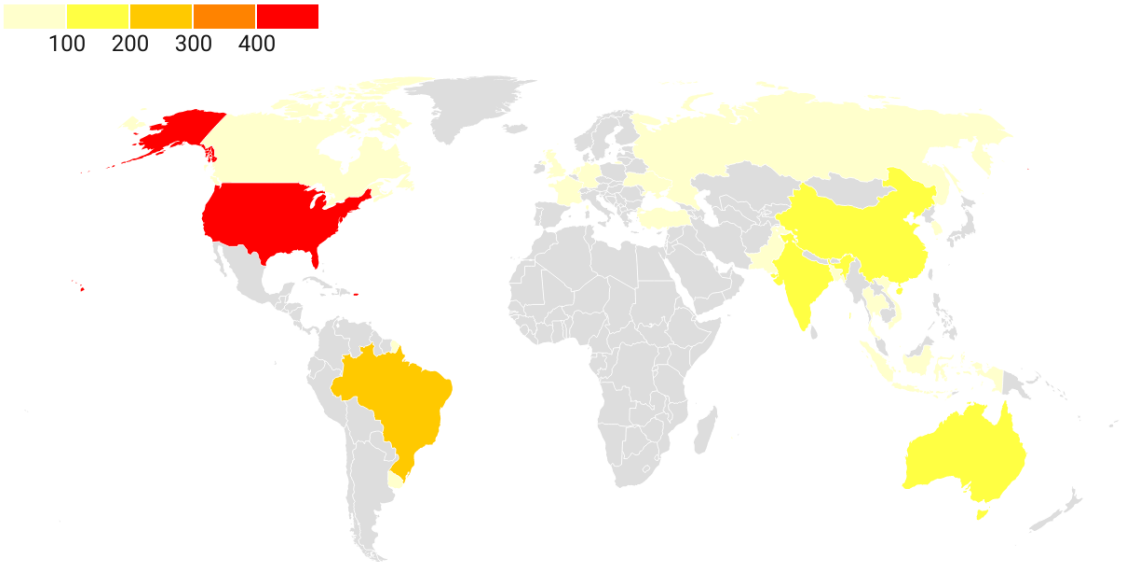


64% of reported attackware was identified as vulnerability scanners

We determined the countries where the most malicious traffic sources were reported, by number of malware records and by the percent of malware records for which we could determine a country used. By representing these in this heat map, we illustrate where malicious traffic origins were most frequently reported, by total malicious traffic source records.

Heat map: attacks and probes reported

Countries with most reports of malicious traffic sources, January - December, 2022 (thousands)



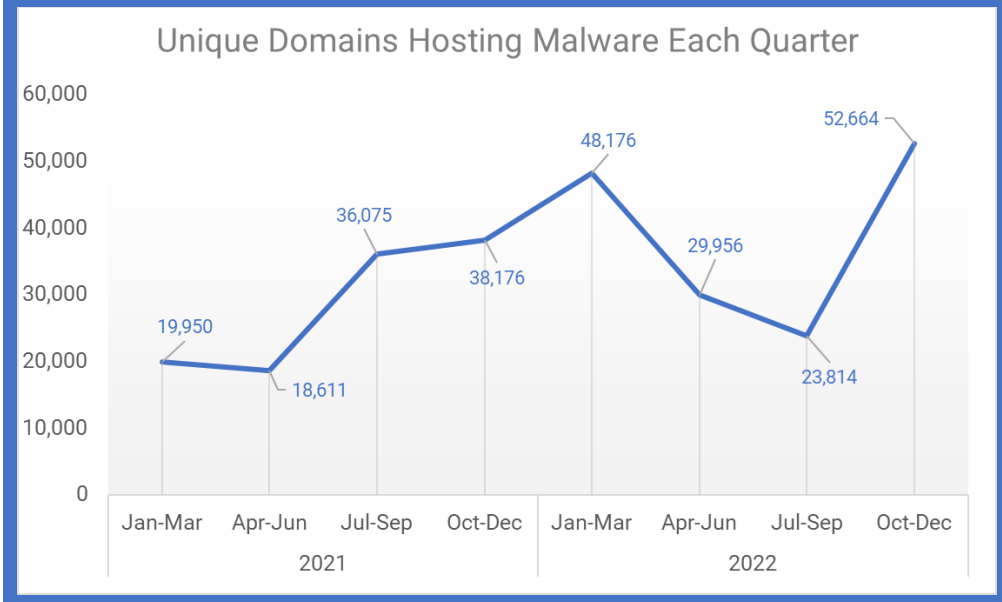
Source: Cybercrime Information Center • Created with Datawrapper

China and the United States have 7 of the 10 hosting networks (ASNs) with the most (unique) IPv4 Addresses reported for hosting malware (January to December 2022, minimum 20,000 addresses). We note that we typically found one malware hosted at each of these addresses.

Rank	AS Name	AS number	Country	Unique Malicious Traffic Addresses ▼	Total Malicious Traffic Records
1	CHINANET-BACKBONE No.31	4134	China	**123,057**	123,057
2	DIGITALOCEAN	14061	United States	**73,960**	73,961
3	CHINA UNICOM China169 Backbone	4837	China	**58,082**	58,082
4	AMAZON-02	16509	United States	**44,511**	44,511
5	Korea Telecom	4766	Republic of Korea	**33,332**	33,332
6	LG DACOM Corporation	3786	Republic of Korea	**30,000**	30,000
7	MICROSOFT-CORP-MSN	8075	United States	**26,503**	26,503
8	HINET Data Communication	3462	China	**21,897**	21,897
9	Link3 Technologies Ltd.	23688	Bangladesh	**21,119**	21,119
10	COLOCROSSING	36352	United States	**20,481**	20,481

Domain Names and Malware

Domain names are essential resources for spam and phishing attacks. However, of the 3,870,882 malware records that we examined for this study, only 116,639 unique domain names were reported for serving up malware. While the data we collected reveal that domain names are less commonly used for serving malware or for malware distribution, we observed several patterns over time.



Use of domain names to identify malware hosting increased 121% in 4Q 2022

The following table shows the gTLD registrars where endpoint malware domains were most often registered (considering registrars with a minimum of 1,500 domains under management).

Rank	IANA_ID	Registrar	Total Endpoint Malware Domains ▼
1	146	GoDaddy.com, LLC	**9,613**
2	1068	NameCheap, Inc.	**6,193**
3	303	PDR Ltd. d/b/a PublicDomainRegistry.com	**4,564**
4	48	eNom, LLC	**1,143**
5	69	Tucows Domains Inc.	**1,039**

The following table shows the Top-level domains where endpoint malware domains were most often registered (where TLDs have at least 4,500 domains under management). The COM TLD had the most reported endpoint malware domains but the 30,141 of 116,639 reported domains is proportionately below COM's market share (26% of endpoint malware versus 44% of registered domains)?

Rank	TLD	Total Endpoint Malware Domains ▼	Total URLs reported	Ratio of URLs to domains reported
1	com	**30,141**	180,643	5.99
2	br	**3,038**	9,692	3.19
3	in	**2,715**	8,667	3.19
4	org	**1,957**	7,454	3.81
5	net	**1,766**	4,955	2.81

When we do see domain names reported for hosting malware, we often see amplification: a many-to-one use of host names to domain names. We also see many-to-one relationships in URL paths, where hundreds of URLs have the same domain name or host name in common. In such cases, we count the domain name once. Some host names or registered domain names have extraordinary numbers of URLs reported for hosting endpoint malware. COM's ratio of URLs to unique registered domain names reported for serving malware may indicate that many legitimate domain names are being exploited to host malware.

We found domains of seven file sharing services and code repositories that rank high in user popularity (*e.g.*, Alexa ranked, registered to Fortune 100 companies, profiled at Crunchbase or similar sites) but also have very large numbers of URLs reported for hosting endpoint malware: of these, 6 are registered in the COM TLD.

Our data for this study show that malware attackers continue to misuse file sharing services and code repositories to distribute source code, attack code, and files containing compromised credentials or cryptographic keys. We also observed that web sites that offer mobile app downloads, serve as Internet archives, and IT professional portals were misused to serve malware.

Malware attackers continue to misuse file sharing services and code repositories

83,117 zol.com.cn	**zol.com.cn**, a Chinese technology and science portal for professionals acquired by CNET Networks in 2004, had the most reported malicious URLs. We classified nearly all the 83,117 URLs as malicious Windows executables or Android APKs. VirusTotal tags these as application/x-msdownload or application/octet-stream.
69,258 usinenovelle.com	**usinenovelle.com**, a French business magazine, had 69,258 reported malicious URLs, all in 1Q2022. These were reported as malicious executables, suspicious java scripts, or URL redirectors. Our tests of a sample set of URLs indicate that the content has been removed.
40,041 amazonaws.com	**amazonaws.com** is a domain used for the cloud service Amazon Web Services. 38,600 of the 40,041 malicious URLs were flagged at VirusTotal as suspicious xml files.
36,332 strikinglycdn.com	**strikinglycdn.com** is a web site builder and hosting service located in Sunnyvale. These 36,332 reported malicious URLs were found in `http://uploads.strikinglycdn.com/files/` directory. The names appear to be automatically generated. We attempted to submit these for analysis but were challenged for a login.
4,390 live.com	**live.com** is used by Microsoft for Outlook.com and OneDrive products. 97% of the 2,545 reported URLs were Quakbot infostealer. VirusTotal reported the URLs that we couldn't classify as malicious. Our tests of a sample set of URLs indicate that the content has been removed.
3,514 drive.google.com	**drive.google.com** is a cloud storage service operated by Google, Inc. We were able to identify 794 infostealers: 600 were Quackbot. The sample set of URLs that we investigated were identified in the VirusTotal database as malicious by several antivirus software. All returned page not found errors (http/404)
3,511 filefactory.com	**filefactory.com** is a storage service located in Hong Kong. 3,511 malicious URLs reported in the January-May 2022 period were in a single directory. The file names appear to be automatically generated. We did not have sufficient data to classify the malware. Our tests of a sample set of URLs indicate that the content has been removed.

Malware Mitigation Opportunities

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

Hosting services, cloud services, registrars, and registries should adopt 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. Given the agility that malware actors exhibit, it is imperative that hosting services, cloud services, registrars, and registries have the tools to respond quickly and legally.

Hosting or cloud service providers should scan their IP address spaces for malware and act quickly to remove malware when detected or when reported by investigators.
These operators are best positioned to identify the origin addresses of users who upload malware to file sharing repositories, 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.

Domain registrars and registries are best positioned to identify and suspend domains reported for serving malware.
These parties possess key information – contact data and billing data – that is available to no one else. 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. When malware actors include domain names in URL composition, they can change the DNS to resolve their domain names to newly acquired hosting resources when their malicious content is taken down. Suspension activities should thus be coordinated with hosting providers as well as 3rd party DNS providers.

Legislation or regulation may be necessary to effectively mitigate malware threats.
Calls for regulations that require Internet as a Service operators to collect and maintain accurate contact information (such as the US Executive Order 13984 of January 19, 2021), or that oblige domain registrars or registries to "lock and suspend" 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.

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 ANSI and ISO standards groups. 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), 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 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

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

About the Cybercrime Information Center

The Cybercrime Information Center (CIC) is a repository for measurements and analysis of global security threats involving the Internet's names and numbers—the Domain Name System (DNS), Internet Protocol (IP) addresses, and Autonomous System (AS) numbers. Its mission is to document abuse and the context in which it occurs, enabling investigators and researchers to discover where criminals obtain the resources for their attacks, to observe and analyze criminal behavior over time, and to quantify the role that individual registries, registrars, and service providers play in criminal abuse of the Internet's names and numbers.

The Cybercrime Information Center collects and processes malware reports from these sources:

Malware Patrol. 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. 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. 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). 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).

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, Spamhaus, 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.