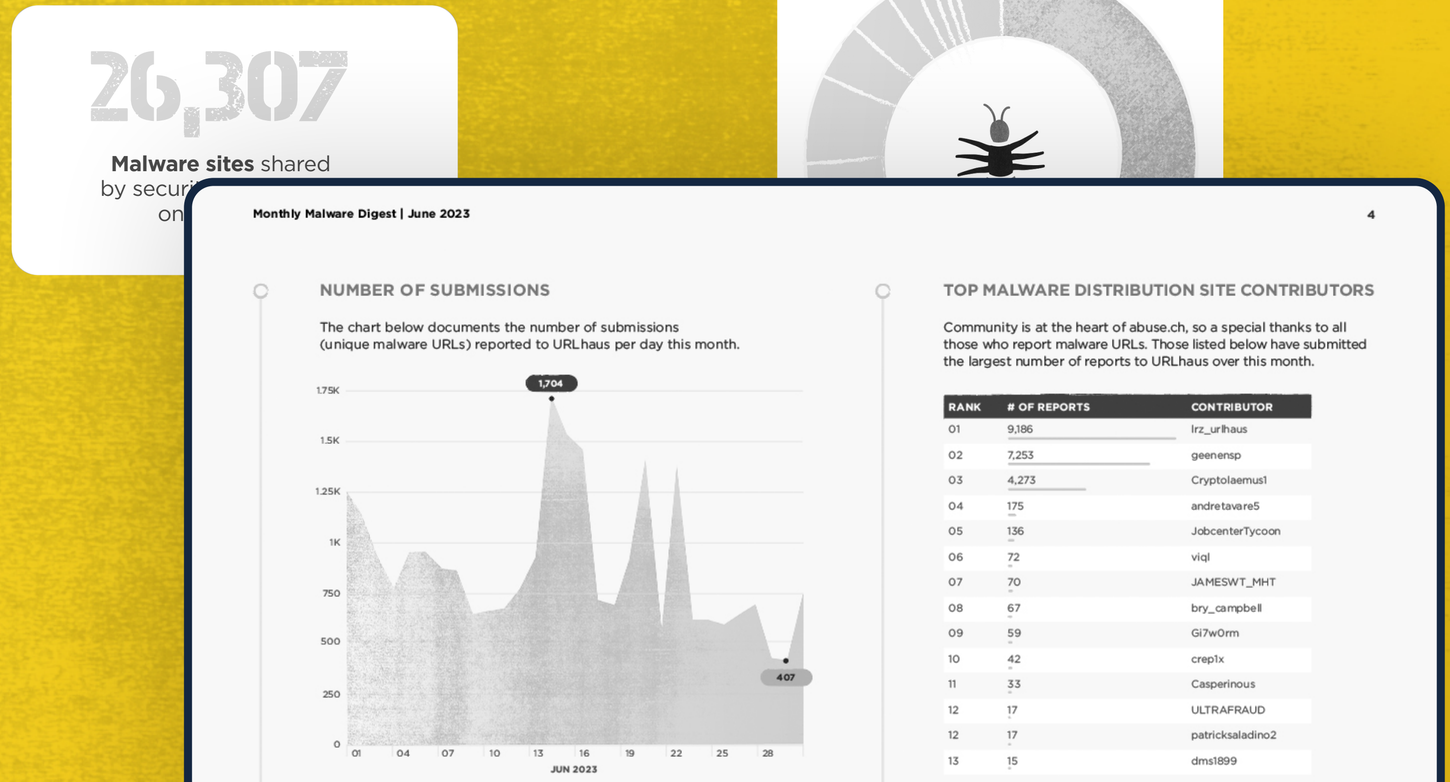
JUNE 2023

MONTHLY MALWARE DIGEST

In this report, we highlight malware trends utilizing data from abuse.ch's open platforms. These collect, track and share resources relating to malware campaigns, including the URLs of malware distribution sites, malware samples, and indicators of compromise.

Each section will provide you with a detailed look at who and what data has been shared in the past month showing possible trends in malware operations.



ABOUT THE DATA

All the data in this report is provided by **abuse.ch**, a project committed to fighting abuse on the internet.

abuse.ch operates multiple community driven platforms which are open to everyone to both contribute and consume cyber threat intelligence data.

Security researchers, internet service providers and network operators trust in data provided by abuse.ch to protect their infrastructure from malware and botnet threats.

Due to various issues related to Twitter API authentication, inbound data contributions were disrupted in May, resulting in no comparison figures.

Our thanks go out to all abuse.ch users and contributors for your continued support and patience.

HOW TO BECOME A CONTRIBUTOR

If you would like to contribute URLs of sites distributing malware, malware samples, IOCs or YARA files, then please go to the relevant platform and register by validating with a Twitter account.

Once you have proved to be a trustworthy contributor, you will then be invited to become a trusted member of the abuse.ch community.

URLhaus	**MalwareBazaar**
https://urlhaus.abuse.ch	https://bazaar.abuse.ch
ThreatFox	**YARAify**
https://threatfox.abuse.ch	https://yaraify.abuse.ch

HOW TO CONSUME THE DATA

Currently, all data available via abuse.ch's platforms is free. Below are the links to the relevant APIs:

URLhaus	**MalwareBazaar**
https://urlhaus.abuse.ch/api/	https://bazaar.abuse.ch/api/
ThreatFox	**YARAify**
https://threatfox.abuse.ch/api/	https://yaraify.abuse.ch/api/

URLHAUS

This platform focuses on collecting, tracking and sharing actionable threat intelligence on active malware distribution sites.

Trusted third parties, including security researchers, are continually reporting sites hosting malware to URLhaus. This community-led approach enables hosting companies and network owners to take rapid action on harmful content. Additionally, it provides organizations with actionable threat intelligence data to protect against malware threats.

Explore URLhaus

ACTIVE MALWARE DISTRIBUTION SITES

26,307

Malware sites shared by security researchers on URLhaus

25,782

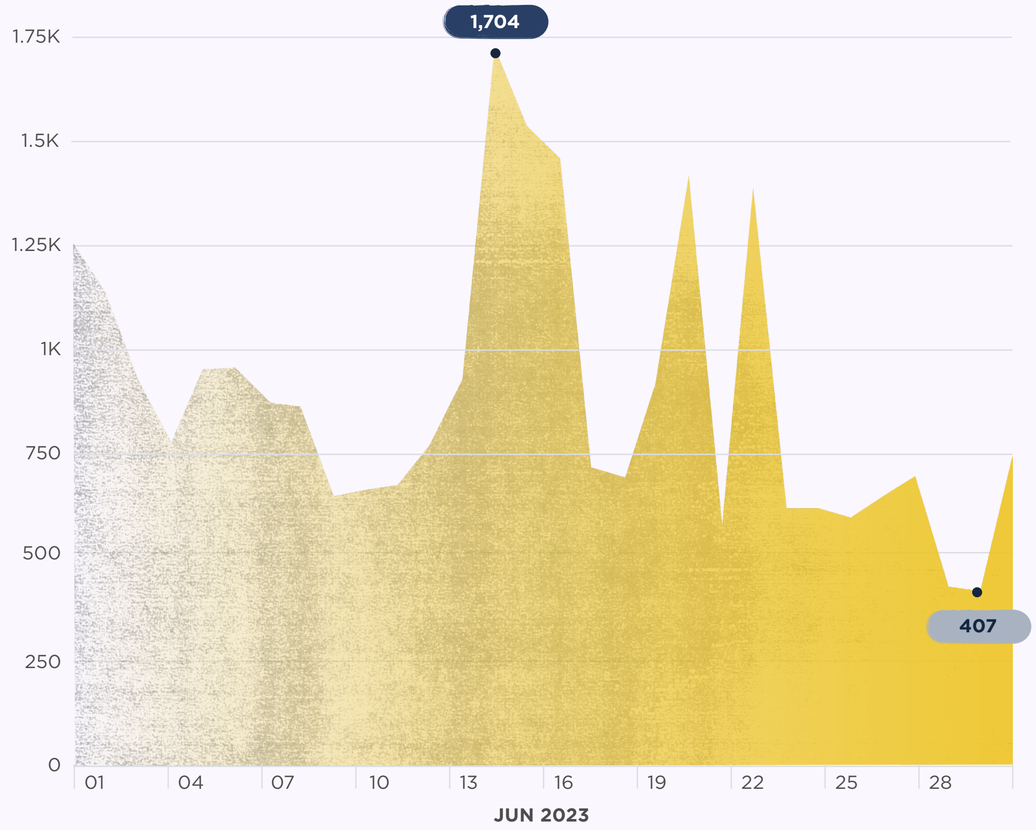
Abuse reports sent out to hosting providers and network owners

92%

Of abuse reports **have been acted upon**

NUMBER OF SUBMISSIONS

The chart below documents the number of submissions (unique malware URLs) reported to URLhaus per day this month.

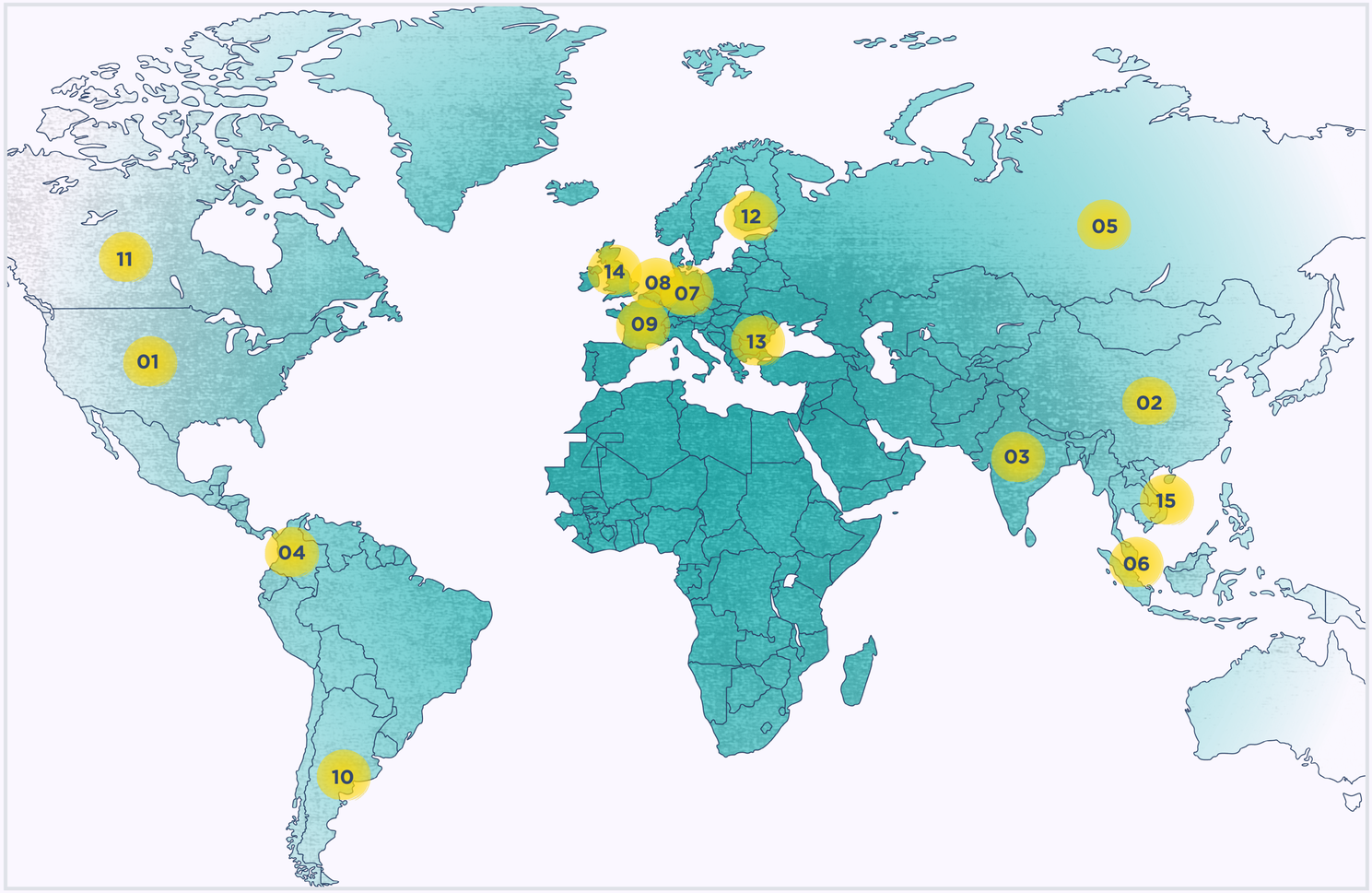


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

Community is at the heart of abuse.ch, so a special thanks to all those who report malware URLs. Those listed below have submitted the largest number of reports to URLhaus over this month.

RANK	# OF REPORTS	CONTRIBUTOR
01	9,186	lrz_urlhaus
02	7,253	geenensp
03	4,273	Cryptolaemus1
04	175	andretavare5
05	136	JobcenterTycoon
06	72	viql
07	70	JAMESWT_MHT
08	67	bry_campbell
09	59	Gi7w0rm
10	42	crep1x
11	33	Casperinous
12	17	ULTRAFRAUD
12	17	patricksaladino2
13	15	dms1899

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	COUNTRY
01	3,273	United States
02	2,681	China
03	2,566	India
04	365	Colombia
05	329	Russia
06	214	Singapore
07	203	Germany
08	201	Netherlands
09	163	France
10	133	Argentina
11	127	Canada
12	104	Finland
13	83	Bulgaria
14	70	United Kingdom
15	67	Vietnam

TOP NETWORKS HOSTING MALWARE DISTRIBUTION SITES

The following table shows the networks hosting the largest number of malware distribution sites this month.

RANK	# OF URLs	AS NUMBER	ORGANIZATION NAME	COUNTRY
01	2,367	9829	BSNL	India
02	1,735	4837	CHINA169	China
03	877	4134	CHINANET	China
04	699	13335	CLOUDFLARE	United States
05	680	46606	UNIFIEDLAYER	United States
06	565	22612	NAMECHEAP	United States
07	360	19871	NETWORK-SOLUTIONS	United States
08	269	26496	GO-DADDY	United States
09	158	24940	HETZNER	Germany
10	141	204603	PARTNER	Russia
11	140	211252	DELIS	Netherlands
12	135	16276	OVH	France
13	111	36352	COLOCROSSING	United States
14	110	52495	Cotel	Bolivia
15	95	23352	SERVERCENTRAL	United States

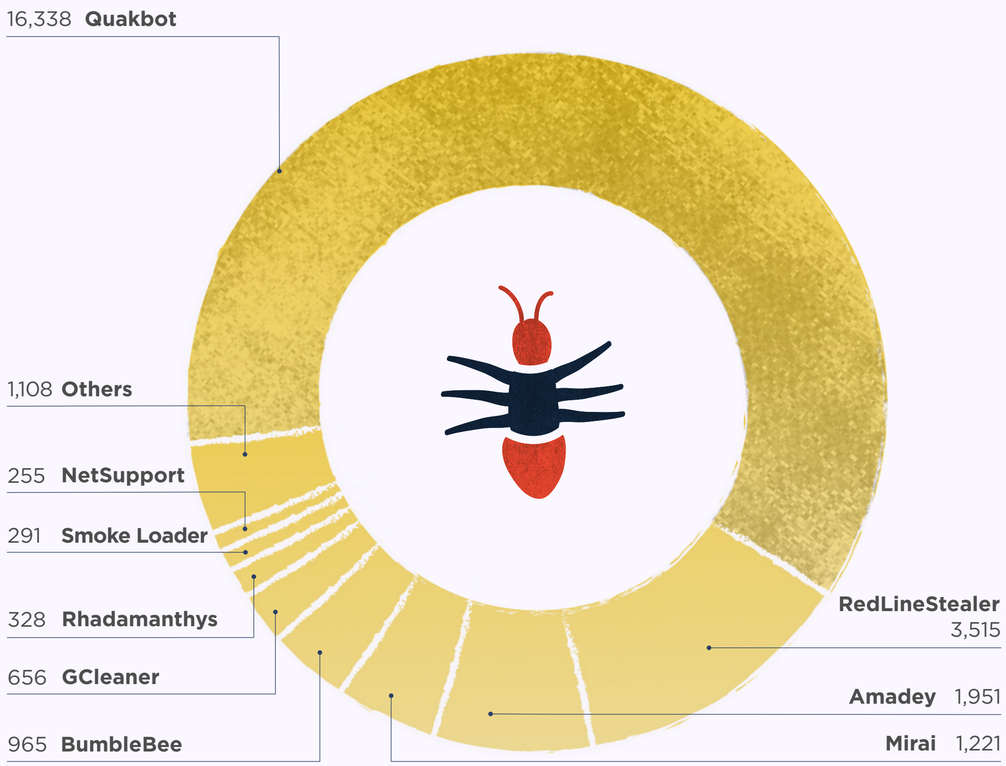
TOP MALWARE HOSTS

The following table shows the details of the top malware hosts and their associated providers this month.

RANK	# OF MALWARE SITES	HOST	PROVIDER	COUNTRY
01	130	vk.com	VK	Russia
02	118	pasteio.com	n/a	n/a
03	26	wtools.io	n/a	n/a
03	26	cdn.discordapp.com	Discord	United States
04	23	github.com	Microsoft	United States
05	19	pastebin.com	Pastebin	United States

TOP MALWARE FAMILIES ASSOCIATED WITH MALWARE SITES

This chart shows the malware families associated with the largest number of reported sites.



TOP MALWARE FAMILIES

The following table shows the top 15 malware families this month.

RANK	MALWARE FAMILY	# OF SAMPLES
01	Quakbot	16,338
02	RedLineStealer	3,515
03	Amadey	1,951
04	Mirai	1,221
05	BumbleBee	965
06	GCleaner	656
07	Rhadamanthys	328
08	Smoke Loader	291
09	NetSupport	255
10	UACModuleSmokeLoader	254
11	Ransomware.Stop	211
12	CoinMiner	206
13	Gafgyt	179
14	AgentTesla	142
15	Fabookie	116

MALWARE BAZAAR

Through this platform security researchers and the wider industry can share, classify and hunt for confirmed malware samples.

The platform allows security researchers to hunt for malware samples by deploying custom hunting rules, e.g., using the power of vendor-based threat detections.

Explore MalwareBazaar

MALWARE SAMPLES

9,977

Malware samples shared by security researchers on MalwareBazaar

1,252

Active hunting rules

11MB

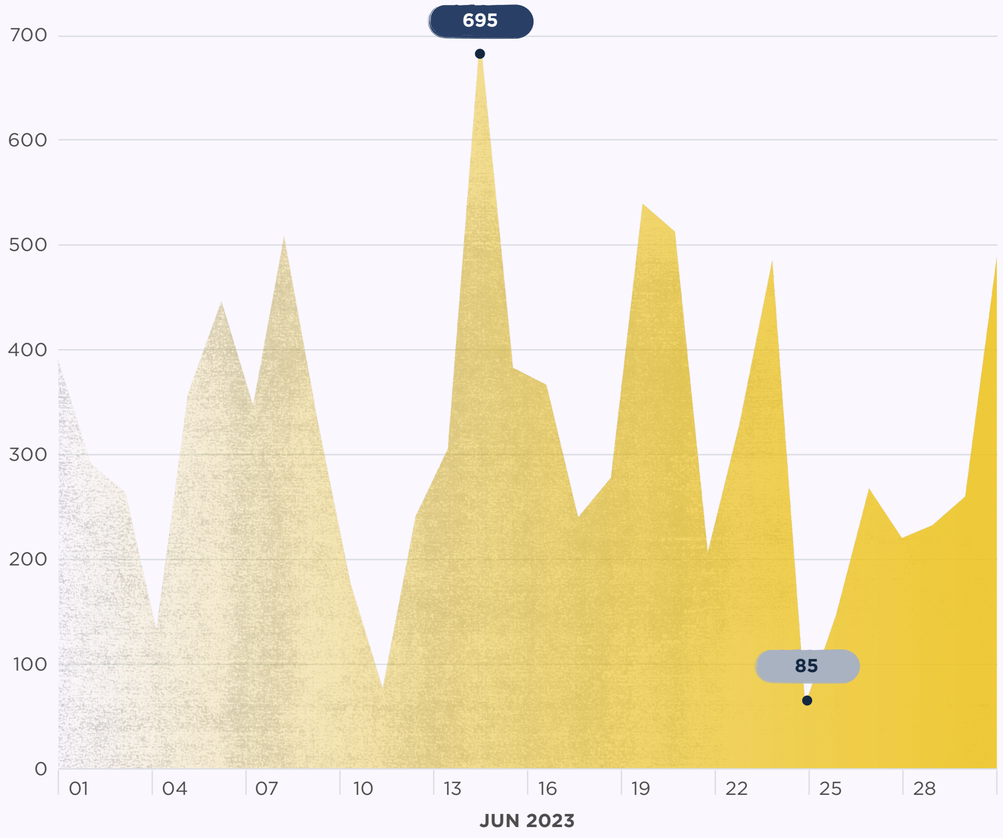
Average size of a malware sample

EXE FILES

Windows executables (exe) are the **top reported file types**

MALWARE SAMPLES

The chart below shows the number of unique malware samples shared on MalwareBazaar per day this month.



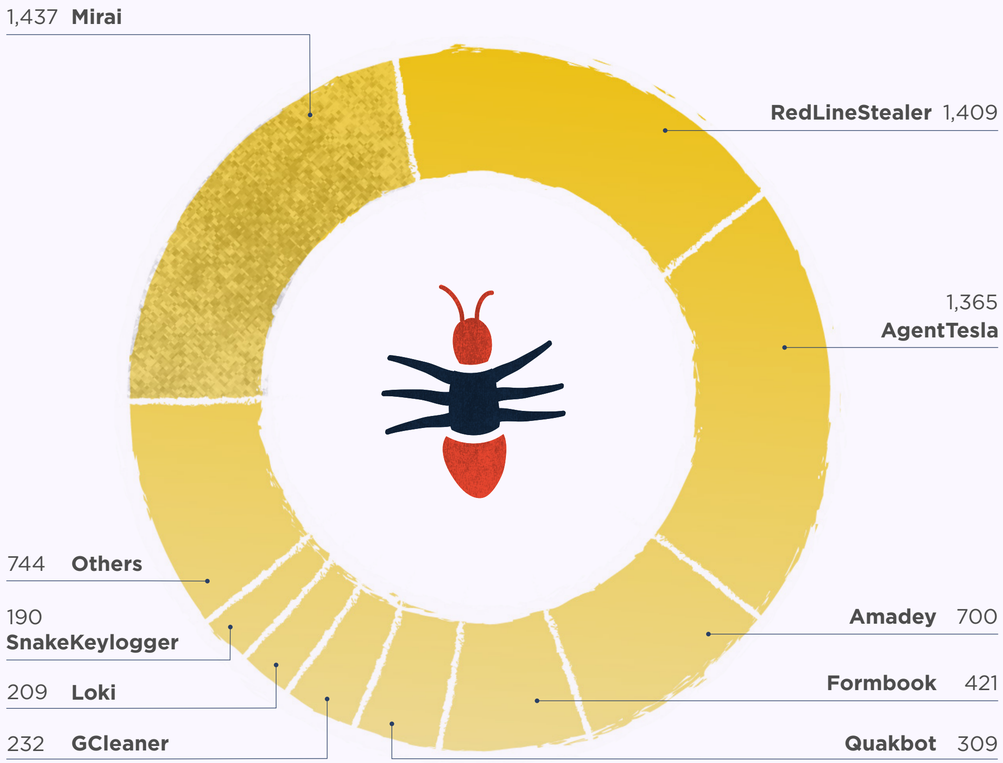
TOP SAMPLE CONTRIBUTORS

Community is at the heart of abuse.ch, so a special thanks to all those who provide malware samples. Those listed below have submitted the largest number of samples to MalwareBazaar over this month.

RANK	# OF MALWARE SAMPLES	CONTRIBUTOR
01	807	@cocaman
02	554	@andretavare5
03	333	@JAMESWT_MHT
04	312	@lowmal3
05	297	@jstrosch
06	296	@Chainskilabs
07	264	@adrian__luca
08	174	@r3dbU7z
09	151	@TeamDreier
10	114	@threatcat_ch
11	106	@Porcupine
12	105	@Neiki__
13	103	@pr0xylife
14	97	@obfusor
15	87	@malwarelabnet

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

This chart shows the malware families that were associated with the largest number of samples.



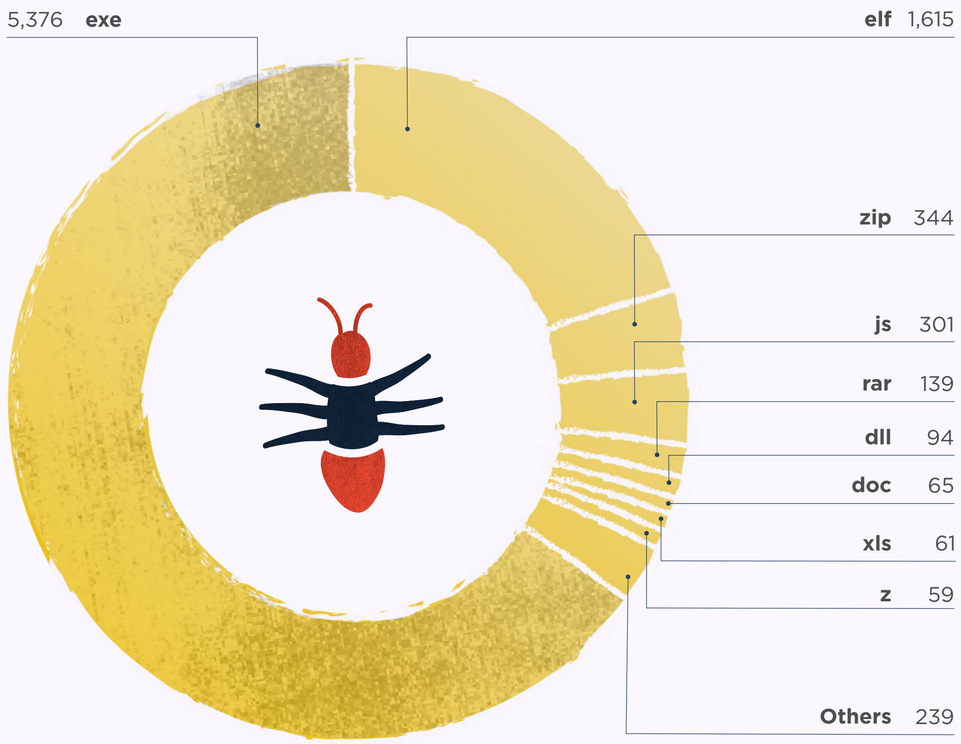
TOP MALWARE FAMILIES

The following table shows the top 15 malware families this month.

RANK	MALWARE FAMILY	# OF SAMPLES
01	Mirai	1,437
02	RedLineStealer	1,409
03	AgentTesla	1,365
04	Amadey	700
05	Formbook	421
06	Quakbot	309
07	GCleaner	232
08	Loki	209
09	SnakeKeylogger	190
10	Gafgyt	171
11	RemcosRAT	168
12	GuLoader	151
13	AsyncRAT	90
14	AveMariaRAT	83
15	Rhadamanthys	81

TOP FILE TYPES

This chart shows the most popular tags related to the reported IOCs.



TOP MATCHING YARA RULES

Community is at the heart of abuse.ch, so a special thanks to all those who contribute. The following table lists the YARA rules and their authors associated with the largest number of samples submitted.

RANK	# MALWARE SAMPLES	YARA RULE	AUTHOR
01	1,260	MALWARE_Win_RedLine	ditekSHen
02	1,163	INDICATOR_EXE_Packed_ConfuserEx	ditekSHen
03	1,155	detect_Redline_Stealer	Varp0s
04	1,027	redline_stealer_1	n0t
05	880	linux_generic_ipv6_catcher	_lubiedo
06	862	MyMirai	n/a
07	829	PE_Digital_Certificate	albertzsigovits
08	756	INDICATOR_SUSPICIOUS_EXE_RegKeyComb_DisableWinDefender	ditekSHen
09	750	unixredflags3	timb_machine
10	745	PE_Potentially_Signed_Digital_Certificate	albertzsigovits
11	556	cobalt_strike_tmp01925d3f	The DFIR Report
12	439	Shellcode	nex
13	381	Linux_Trojan_Gafgyt_28a2fe0c	Elastic Security
14	341	setsockopt	timb_machine
15	306	Windows_Trojan_Smokeloader_3687686f	Elastic Security

THREATFOX

This platform enables organizations and security researchers to consume and contribute technical indicators connected to cyber attacks in a structured way. The shared indicators of compromise (IOCs) help others to detect potential cyber attacks within their environment.

Explore ThreatFox

INDICATORS OF COMPROMISE (IOCs)

10,199

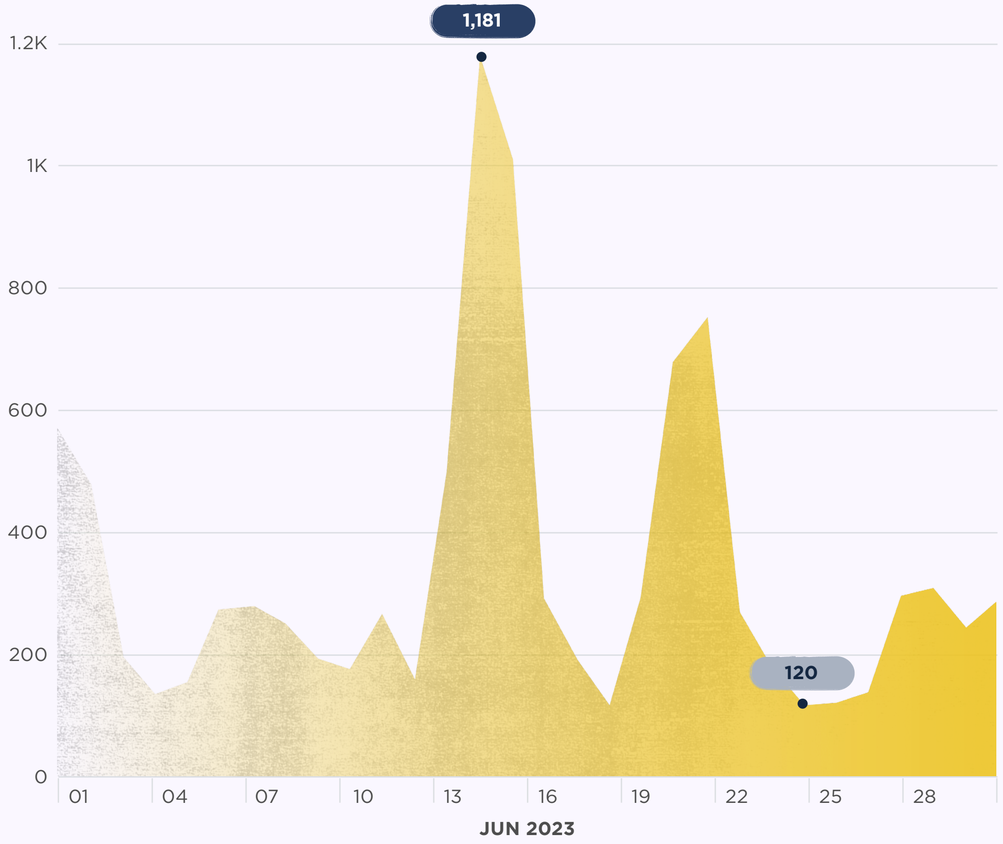
Indicators of compromise (IOCS) shared on ThreatFox

4,160

IOCs relating to Qakbot

NUMBER OF IOCs SHARED PER DAY

The chart below shows the number of indicators of comprimise (IOCs) shared on ThreatFox per day this month.



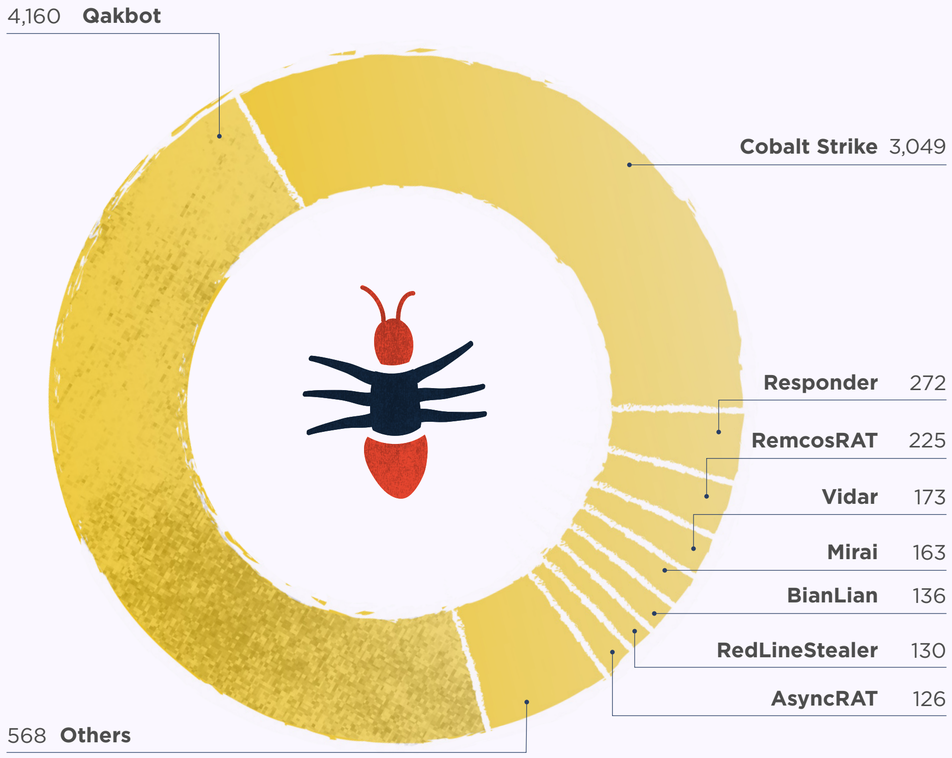
IOC TYPE

An IOC can be a domain name, IP address, or file hash. The following table identifies and explains the most common IOC types reported this month.

RANK	# OF IOCS	IOC TYPE	THREAT TYPE	EXPLANATION
01	3,681	url	payload_ delivery	URL that delivers a malware payload
02	3,193	ip_port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
03	2,234	url	botnet_cc	URL that is used for botnet Command&control (C&C)
04	654	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
05	217	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
06	143	domain	payload_ delivery	Domain name that delivers a malware payload
07	57	md5_hash	payload	MD5 hash of a malware sample (payload)
08	47	ip:port	payload_ delivery	ip:port combination that delivers a malware payload

TOP MALWARE FAMILIES

This chart shows the malware families that were associated with the largest number of IOCs this month.



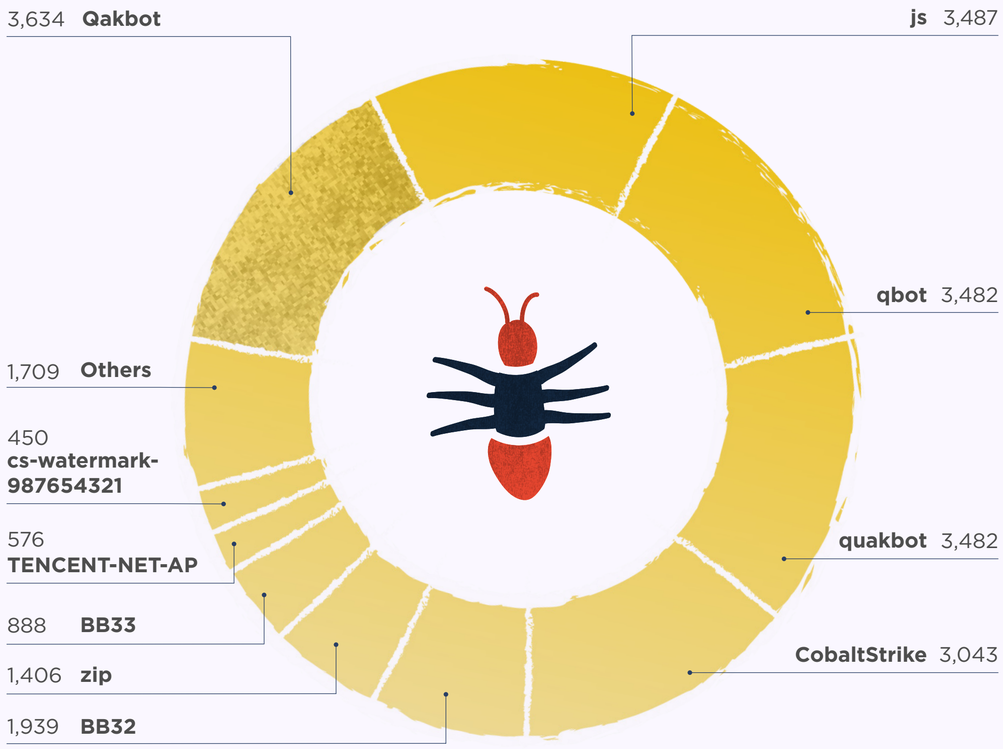
TOP MALWARE FAMILIES

The following table shows the top 15 malware families this month.

RANK	MALWARE FAMILY	# OF IOCS
01	Qakbot	4,160
02	Cobalt Strike	3,049
03	Responder	272
04	RemcosRAT	225
05	Vidar	173
06	Mirai	163
07	BianLian	136
08	RedLineStealer	130
09	AsyncRAT	126
10	Havoc	100
11	RaccoonStealer	99
12	DCRat	95
12	RecordBreaker	95
13	FakeUpdates	94
14	NJRAT	85

TOP TAGS

Tags allow the contributer of an IOC to provide additional context about a threat. This chart shows the most popular tags used this month.



TOP TAGS

The following table shows the top 15 most popular tags of the malware families this month.

RANK	MALWARE FAMILY	# OF IOCS
01	Qakbot	3,634
02	js	3,487
03	quakbot	3,482
03	qbot	3,482
04	CobaltStrike	3,043
05	BB32	1,939
06	zip	1,406
07	BB33	888
08	TENCENT-NET-AP	576
09	cs-watermark-987654321	450
10	BB30	400
11	cs-watermark-100000	366
12	ALIBABA-CN-NET	340
13	cs-watermark-391144938	331
14	RAT	272

YARAIFY

A platform for threat hunters and security researchers to be able to hunt for suspicious files using YARA. Additionally, this community-based platform allows users to share their own YARA rules in structured way.

[**YARA rules** are used to identify malware based on certain characteristics]

Explore YARAify

YARAIFY STATISTICS

2,148,128

File scans conducted on YARAify

1,652,956

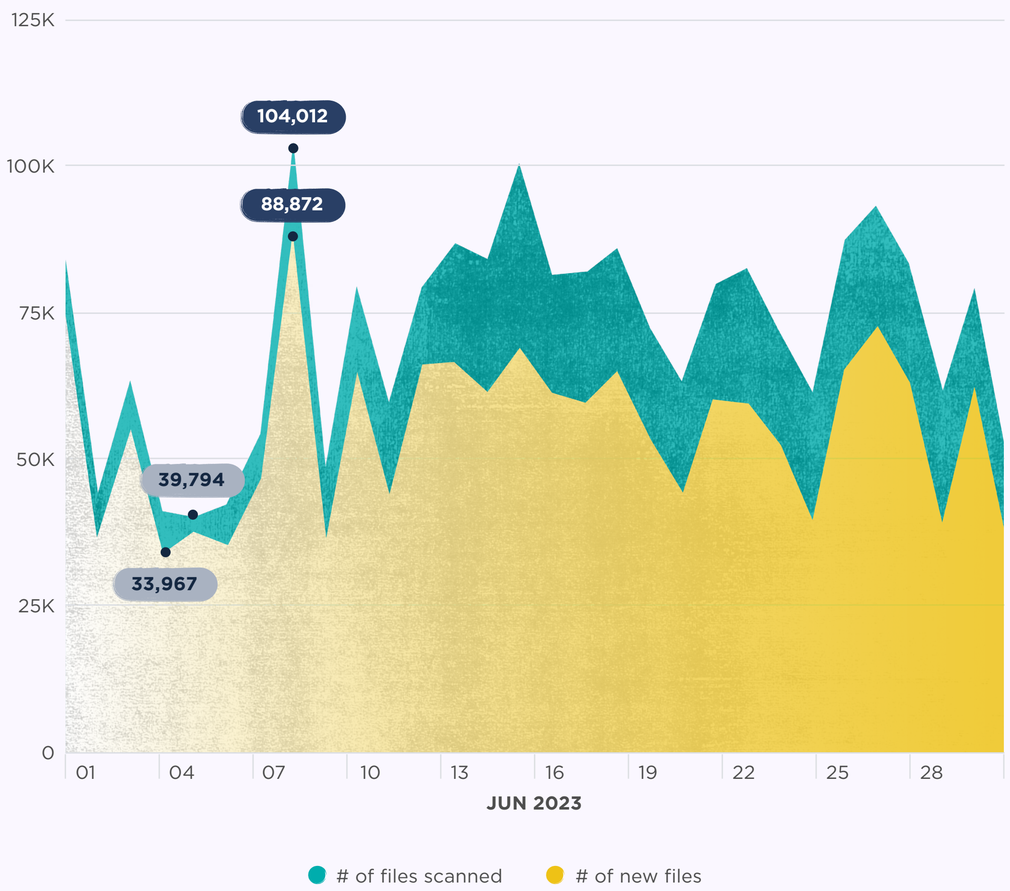
Distinct files that had scans performed on them

15,073

YARA rules deployed on YARAify and available for hunting

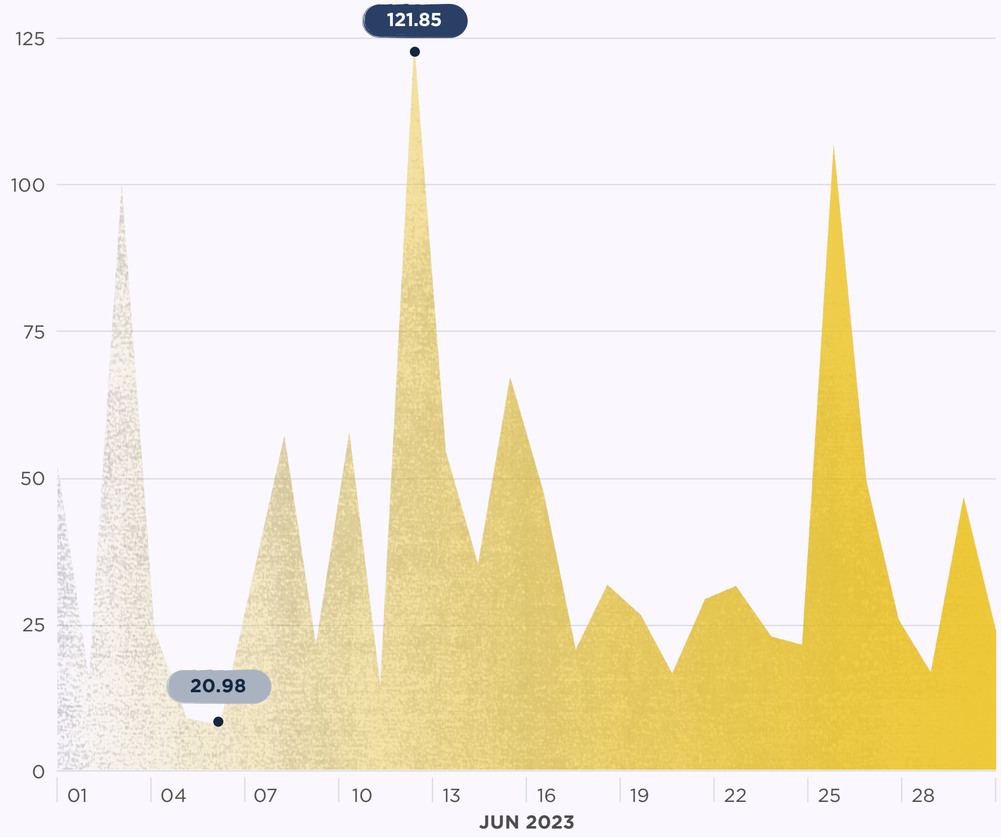
FILES SCANNED PER DAY

The chart below shows the number of file scans conducted by YARAify this month.



DATA SCANNED PER DAY

The chart below shows the amount of data scanned in gigabytes (GB) this month.



TOP MATCHING YARA RULES

The following table lists the YARA rules and their authors associated with the largest number of files matched.

RANK	# OF FILES MATCHED	YARA RULE	AUTHOR
01	82,740	SUSP_Imphash_Mar23_2	Arnim Rupp
02	38,001	Shellcode	nex
03	31,714	win_qakbot_auto	Felix Bilstein
03	31,714	win_qakbot_malped	Felix Bilstein
04	31,688	qakbot_api_hashing	Embee_Research
05	31,213	QakBot	kevoreilly
06	31,193	MAL_QakBot_ ConfigExtraction_Feb23	kevoreilly
06	31,193	unpacked_qbot	n/a
07	30,449	Windows_Trojan_Qbot_ 1ac22a26	Elastic Security
08	30,016	SUSP_Imphash_Mar23_3	Arnim Rupp
09	28,045	PE_Digital_Certificate	albertzsigovits
10	26,293	PE_Potentially_Signed_Digital_ Certificate	n/a
11	24,850	BitcoinAddress	Didier Stevens
12	24,440	MALWARE_Win_RedLine	ditekSHen
13	24,373	APT_NK_Methodology_ Artificial_UserAgent_IE_Win7	stvemillertime

TOP MATCHING CLAMAV SIGNATURES

The following table lists the Clam AntiVirus signatures that were used in the most tasks.

RANK	TASK COUNT	CLAMAV SIGNATURE
01	220,634	Win.Malware.Midie-6847893-0
02	220,374	Win.Malware.Zusy-6878655-0
03	188,580	Win.Malware.Midie-6847894-0
04	184,343	Win.Malware.Midie-6848630-0
05	182,636	Win.Malware.Midie-6847892-0
06	182,634	Win.Malware.Midie-6848784-0
07	151,270	Win.Malware.Midie-6847981-0
08	151,146	Win.Malware.Dqqw-9951425-0
09	150,888	Win.Malware.Zusy-6804618-0
09	150,888	Win.Trojan.QQPass-5710308-0
10	80,554	PUA.Win.Packer.Pequake-4
11	61,874	Win.Malware.Generickdz-10004857-0
12	51,323	Win.Malware.Gepys-9770177-0
13	50,482	Win.Packed.Generic-9967832-0
14	48,218	Win.Trojan.Generic-9959068-0

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN AUGUST

Remember, sharing is caring.