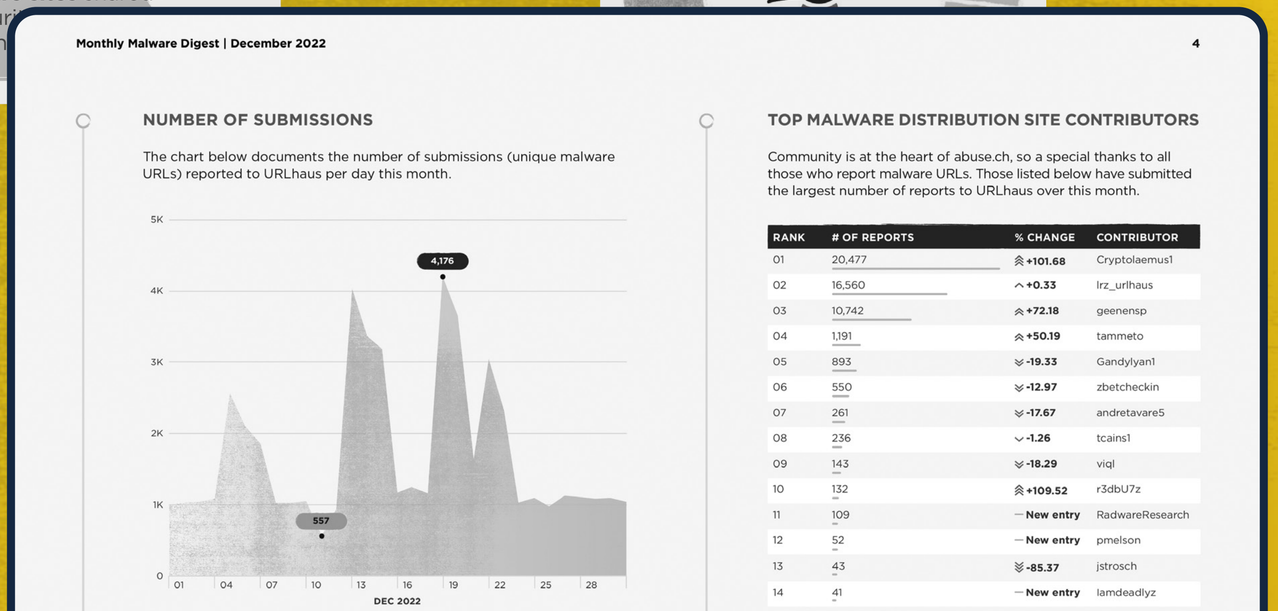
DECEMBER 2022

SPAMHAUS ABUSE.ch

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.



Monthly Malware Digest | December 2022 4

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	% CHANGE	CONTRIBUTOR
01	20,477	+101.68	Cryptolaemus1
02	16,560	+0.33	lrz_urlhaus
03	10,742	+72.18	geenensp
04	1,191	+50.19	tammeto
05	893	-19.33	Gandylyan1
06	550	-12.97	zbetcheckin
07	261	-17.67	andretavare5
08	236	-1.26	tcains1
09	143	-18.29	viql
10	132	+109.52	r3dbU7z
11	109	New entry	RadwareResearch
12	52	New entry	pmelson
13	43	-85.37	jstrosch
14	41	New entry	lamdeadlyz

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.

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	**Malware Bazaar**
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	**Malware Bazaar**
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

52,523

Malware sites shared by security researchers on URLhaus

+29.2%

Increase on the previous month

54,709

Abuse reports sent out to hosting providers and network owners

97%

Of abuse reports **have been acted upon**

NUMBER OF SUBMISSIONS

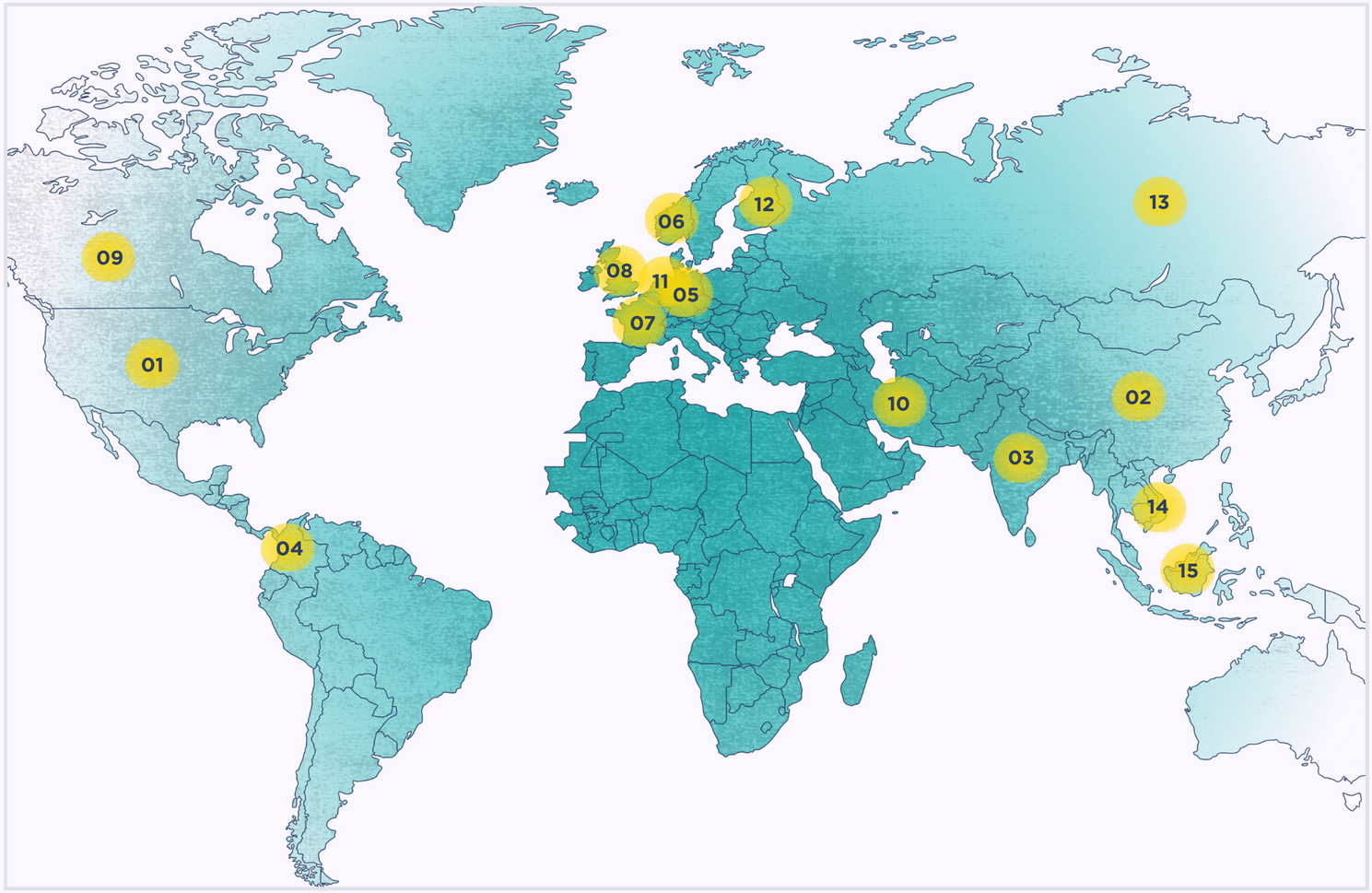
The chart below documents the number of submissions (unique malware URLs) reported to URLhaus per day this month.

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	% CHANGE	CONTRIBUTOR
01	20,477	+101.68	Cryptolaemus1
02	16,560	+0.33	lrz_urlhaus
03	10,742	+72.18	geenensp
04	1,191	+50.19	tammeto
05	893	-19.33	Gandylyan1
06	550	-12.97	zbetcheckin
07	261	-17.67	andretavare5
08	236	-1.26	tcains1
09	143	-18.29	viql
10	132	+109.52	r3dbU7z
11	109	New entry	RadwareResearch
12	52	New entry	pmelson
13	43	-85.37	jstrosch
14	41	New entry	lamdeadlyz
15	38	New entry	bjornruberg

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	13,148	+52.76	United States
02	6,681	+87.41	China
03	3,008	+74.88	India
04	1,124	+210.50	Colombia
05	1,095	+45.42	Germany
06	741	New entry	Norway
07	576	+115.73	France
08	483	+67.71	United Kingdom
09	341	+125.83	Canada
10	315	+108.61	Iran
11	308	-39.96	Netherlands
12	289	+73.05	Finland
13	274	+12.76	Russia
14	267	New entry	Viet Nam
15	247	+48.80	Indonesia

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	4,247	AS4837	CHINA 169	China
02	3,990	AS46606	UNIFIEDLAYER	United States
03	3,323	AS22612	NAMECHEAP	United States
04	2,237	AS4134	CHINANET	China
05	2,119	AS13335	CLOUDFLARENET	United States
06	1,693	AS394695	PUBLIC-DOMAIN-REGISTRY	United States
07	1,441	AS9829	BSNL	India
08	829	AS19871	NETWORK-SOLUTIONS-HOSTING	United States
09	793	AS24940	HETZNER	Germany
10	625	AS16276	OVH	France
11	357	AS51167	CONTABO	Germany
12	336	AS23352	SERVERCENTRAL	United States
13	314	AS33182	DIMENOC	United States
14	280	AS36352	COLOCROSSING	United States
15	212	AS32244	LIQUIDWEB	United States

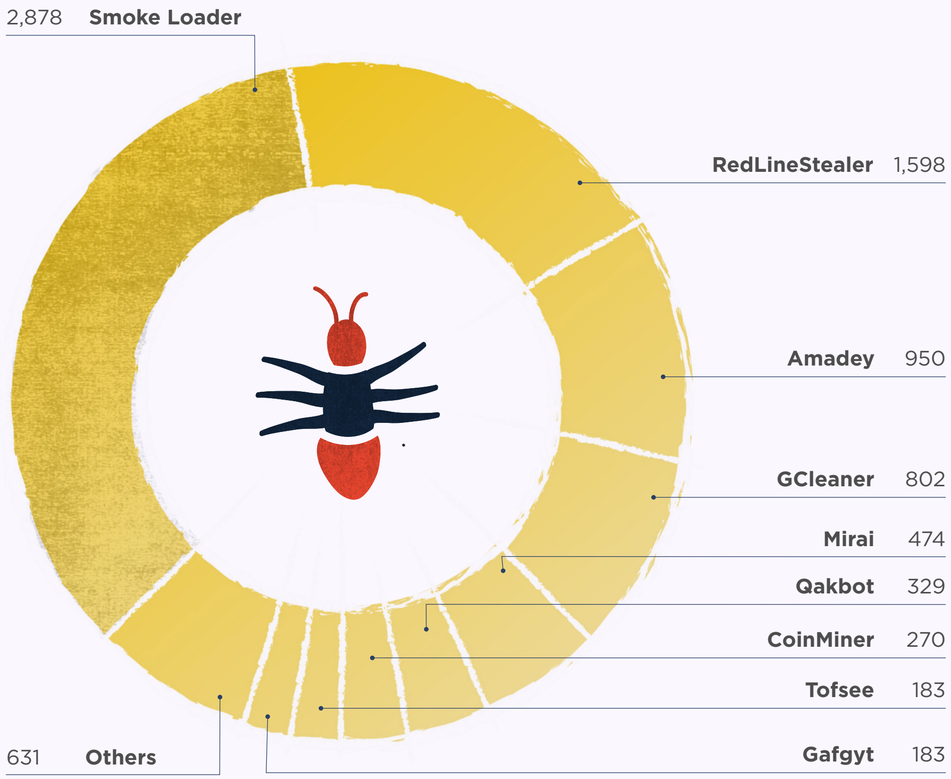
TOP MALWARE HOSTS

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	254	cdn.discordapp.com	Discord	United States
02	215	vk.com	VK	Russia
03	61	github.com	Github	United States
04	56	transfer.sh	n/a	Germany
05	41	bitbucket.org	Atlassian	United States
06	24	pasteio.com	n/a	n/a
07	20	pastebin.com	pastebin.com	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 - % CHANGES MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

RANK	MALWARE FAMILY	% CHANGE	LAST 3 MONTHS	# OF SAMPLES
01	RedLineStealer	+62.23		1,598
02	Tofsee	+28.87		183
03	GCleaner	+10.47		802
04	ArkeiStealer	+0.94		107
05	SnakeKeylogger	-7.92		93
06	Amadey	-10.88		950
07	CoinMiner	-14.01		270
08	Mirai	-16.11		474
09	Smoke Loader	-21.17		2,878
10	AgentTesla	-27.11		121
11	Formbook	-53.13		90
12	Qakbot	New entry		329
12	Gafgyt	New entry		183
12	DanaBot	New entry		123
12	Ransomware.Stop	New entry		97

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

13,583

Malware samples shared by security researchers on MalwareBazaar

-19.8%

Decrease on the previous month

1,045

Active hunting rules

-46.8%

Decrease on the previous month

1.3MB

Avarage 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 MawareBazaar per day this month.

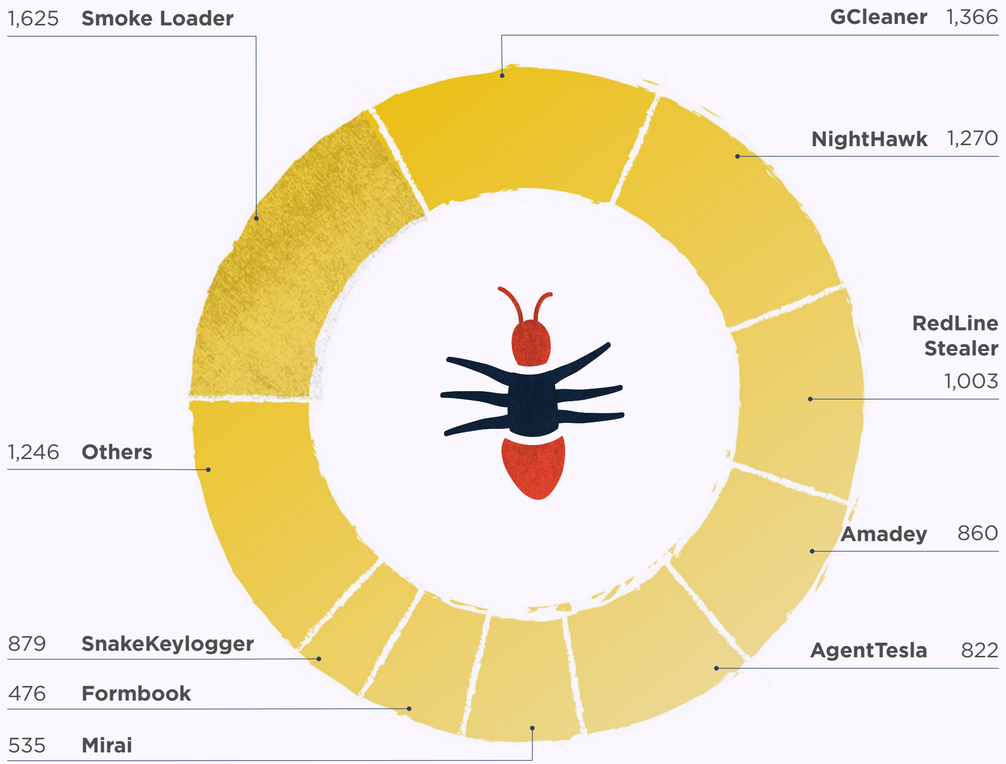
TOP SAMPLE CONTRIBUTORS

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	% CHANGE	CONTRIBUTOR
01	5,502	— New entry	@andretavare5
02	1,249	— New entry	@summontoxic
03	1,076	⌄⌄ -40.78	@zbetcheckin
04	778	⌄ -28.88	@SecuriteInfoCom
05	225	⌄⌄ -76.61	@jstrosch
06	205	⌄⌄ -43.84	@cocaman
07	192	⌄ -9.86	@lowmal3
08	190	⌄ -12.84	@adrian__luca
09	181	⌃ +27.46	@petikvx
10	157	⌄⌄ -52.57	@JAMESWT_MHT
11	151	⌄ -8.48	@pr0xylife
12	103	⌄ -21.97	@James_inthe_box
13	102	— New entry	@atomiczsec
14	92	— New entry	@0xToxin
15	88	— New entry	@r3dbU7z

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



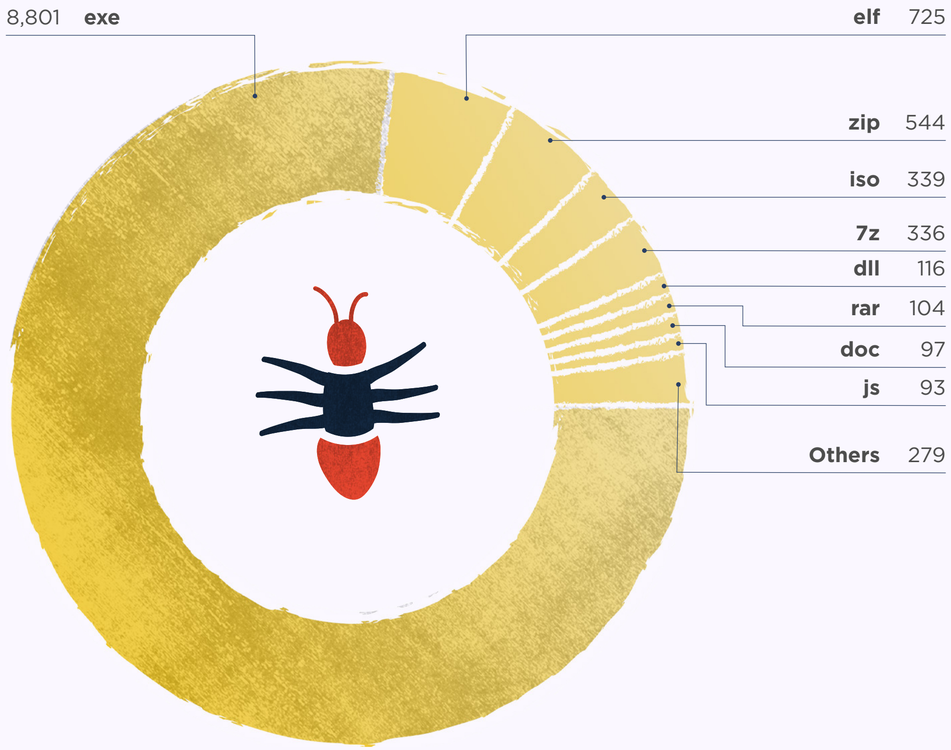
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

RANK	MALWARE FAMILY	% CHANGE	LAST 3 MONTHS	# OF SAMPLES
01	Smoke Loader	**+49.22**		1,625
02	Tofsee	**+17.92**		283
03	GCleaner	**+3.56**		1,366
04	Amadey	**-8.90**		860
05	CoinMiner	**-18.48**		300
06	RedLineStealer	**-24.87**		1,003
07	Mirai	**-25.90**		535
08	SnakeKeylogger	**-27.25**		363
09	AgentTesla	**-35.28**		822
10	Formbook	**-45.85**		476
11	RemcosRAT	**-55.65**		149
12	NightHawk	**New entry**		1,270
12	ArkeiStealer	**New entry**		185
12	Gafgyt	**New entry**		179
12	Quakbot	**New entry**		168

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	# OF MALWARE SAMPLES	YARA RULE	AUTHOR
01	1,996	Windows_Trojan_ Smokeloader_3687686f	Elastic Security
02	1,803	cobalt_strike_tmp01925d3f	The DFIR Report
03	1,706	win_smokeloader_a2	pnx
04	680	MALWARE_Win_RedLine	ditekSHen
05	647	win_nymaim_g0	CERT.pl
06	644	win_gcleaner_auto	Felix Bilstein
07	485	myMirai	n/a
08	472	unixredflags3	Tim Brown @timb_ machine
09	443	linux_generic_ipv6_catcher	@_lubiedo
10	430	CAS_Malware_Hunting	Michael Reinprecht
11	425	win_amadey_a9f4	Johannes Bader
12	353	SUSP_XORed_URL_in_EXE_ RID2E46	Florian Roth
13	342	tofsee_yhub	Billy Austin
13	342	MALWARE_Win_Tofsee	ditekSHen
13	342	win_tofsee_w0	akrasuski1

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)

35,397

Indicators of compromise (IOCS) shared on ThreatFox

-50.9%

Decrease on the previous month

30,611

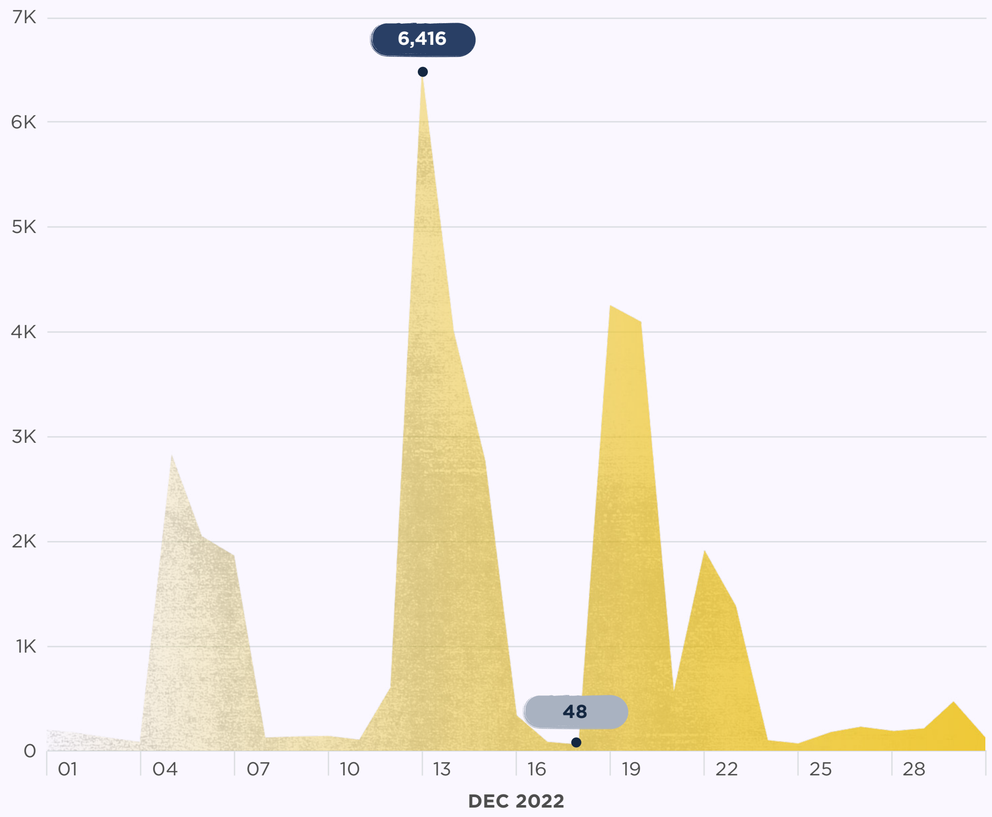
IOCs relating to Qakbot

NEW ENTRY

In December

NUMBER OF IOCs SHARED PER DAY

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



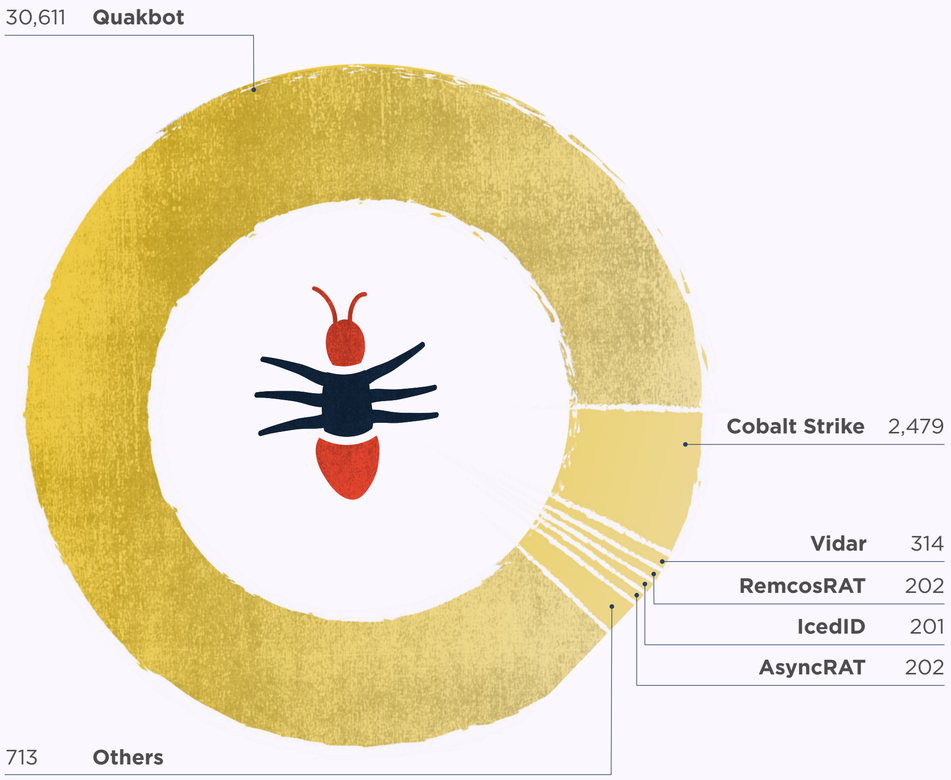
IOC TYPE

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	20,506	url	payload_delivery	URL that delivers a malware payload
02	10,017	domain	payload_delivery	Domain name that delivers a malware payload
03	1,927	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
04	1,781	url	botnet_cc	URL that is used for botnet Command&control (C&C)
05	892	domain	botnet_cc	Domain that is used for botnet Command &control (C&C)
06	236	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
07	25	md5_hash	payload	MD5 hash of a malware sample (payload)
08	13	ip:port	payload_delivery	ip:port combination that delivery a malware payload

TOP MALWARE FAMILIES

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



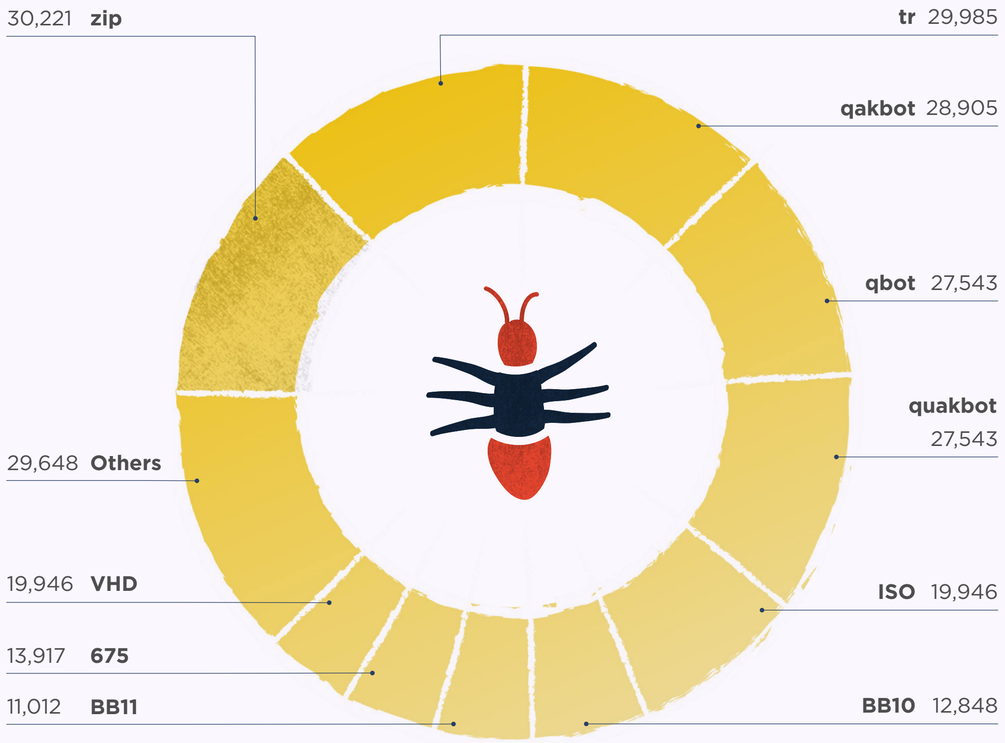
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

RANK	MALWARE FAMILY	% CHANGE	LAST 3 MONTHS	# OF IOCS
01	Quakbot	+57.45		30,611
02	IcedID	+15.43		202
03	RemcosRAT	+12.22		202
04	BumbleBee	+6		106
05	Alien	+4.41		71
06	Cobalt Strike	-3.16		2,479
07	RedLineStealer	-38.43		133
08	NjRAT	-56.43		61
09	Mirai	-68.27		66
10	Vidar	-68.85		314
11	AsyncRAT	New entry		202
11	AuroraStealer	New entry		155
11	NetSupport RAT	New entry		51
11	Gozi	New entry		47
11	Mozi	New entry		45

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 - % CHANGES MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

RANK	MALWARE FAMILY	% CHANGE	# OF IOCS
01	zip	⇈ **+61.10**	30,221
02	tr	⇈ **+59.84**	29,985
03	qakbot	⇈ **+53.39**	28,905
04	quakbot	⇈ **+46.83**	27,543
05	qbot	⇈ **+46.82**	27,543
06	ISO	— **New entry**	19,946
06	BB10	— **New entry**	12,848
06	BB11	— **New entry**	11,012
06	675	— **New entry**	10,388
06	VHD	— **New entry**	10,251
06	nt005	— **New entry**	9,902
06	BB09	— **New entry**	6,036
06	IMG	— **New entry**	5,496
06	RR17	— **New entry**	4,215
06	TR23	— **New entry**	3,999

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

2,419,399

File scans conducted on YARAify

2,009,978

Distinct files that had scans performed on them

+16.2%

Increase in file scans on the previous month

+14.9%

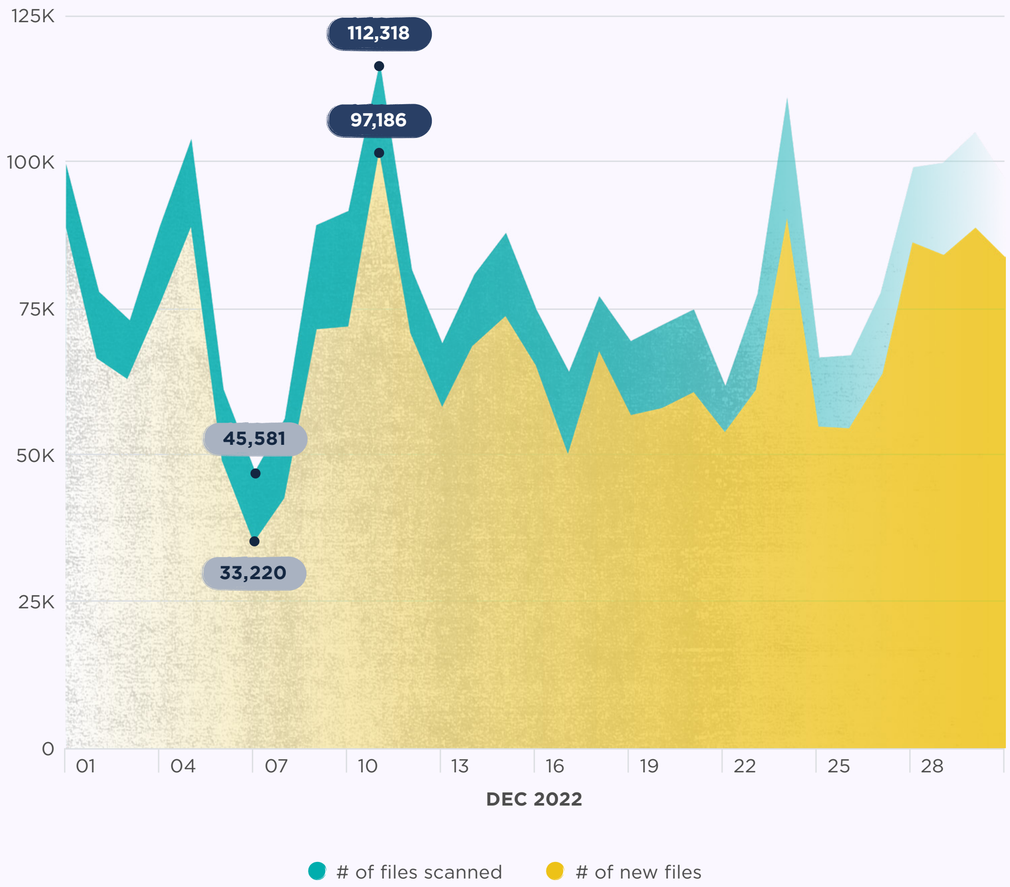
Increase in files on the previous month

14,442

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	% CHANGE	YARA RULE	AUTHOR
01	66,033	^ +14.20	command_and_control	CD_R0M_
02	27,944	— New entry	AsyncRat_Detection_ Dec_2022	n/a
03	26,043	^ +1.40	cobalt_strike_tmp01925d3f	The DFIR Report
04	24,683	— New entry	TeslaCryptPackedMalware	n/a
05	24,343	^^ +34.02	SUSP_XORed_URL_in_ EXE_RID2E46	n/a
06	22,915	— New entry	EnigmaStub	@bartblaze
07	22751	v -27.33	INDICATOR_EXE_Packed_ MPress	ditekSHen
08	21,840	^ +27.40	SUSP_XORed_URL_in_EXE	Florian Roth
09	21,187	v -19.82	win_sality_auto	Felix Bilstein
10	18,547	— New entry	AutoIT_Compiled	@bartblaze
11	17,923	^ +13.24	win_vobfus_auto	Felix Bilstein
12	17,208	^ +32.69	malware_shellcode_hash	JPCERT/CC
13	15,115	— New entry	Mimikatz_Generic	Still
14	13,144	— New entry	win_trickbot_auto	Felix Bilstein
15	12,511	— New entry	MALWARE_Win_RedLine	ditekSHen

TOP MATCHING CLAMAV SIGNATURES

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

RANK	TASK COUNT	% CHANGE	CLAMAV SIGNATURE
01	143,465	v -28.57	Win.Malware.Zusy-6878655-0
02	136,698	v -30.34	Win.Malware.Midie-6847893-0
03	128,828	v -31.27	Win.Malware.Midie-6847981-0
04	124,999	v -31.40	Win.Malware.Midie-6848630-0
05	124,826	v -31.36	Win.Malware.Midie-6847894-0
06	102,702	vv -40.12	Win.Malware.Midie-6847892-0
06	102,702	vv -40.12	Win.Malware.Midie-6848784-0
08	84,801	v -27.26	Win.Packed.Generic-9967832-0
09	39,427	^^ +35.80	PUA.Win.Packer.ProtectSharewar-2
09	39,427	^^ +35.80	PUA.Win.Packer.ProtectSharewar-3
11	70,390	— New entry	PUA.Win.Packer.Pequake-4
11	39,515	— New entry	PUA.Win.Packer.AcprotectUltraprotect-1
11	27,490	— New entry	PUA.Win.Packer.Embedpe-3
11	27,305	— New entry	Win.Malware.Swisyn-9942393-0
11	26,833	— New entry	PUA.Win.Packer.Ep-7

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN FEBRUARY

Remember, sharing is caring.