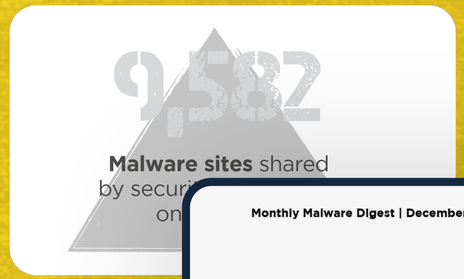
DECEMBER 2023

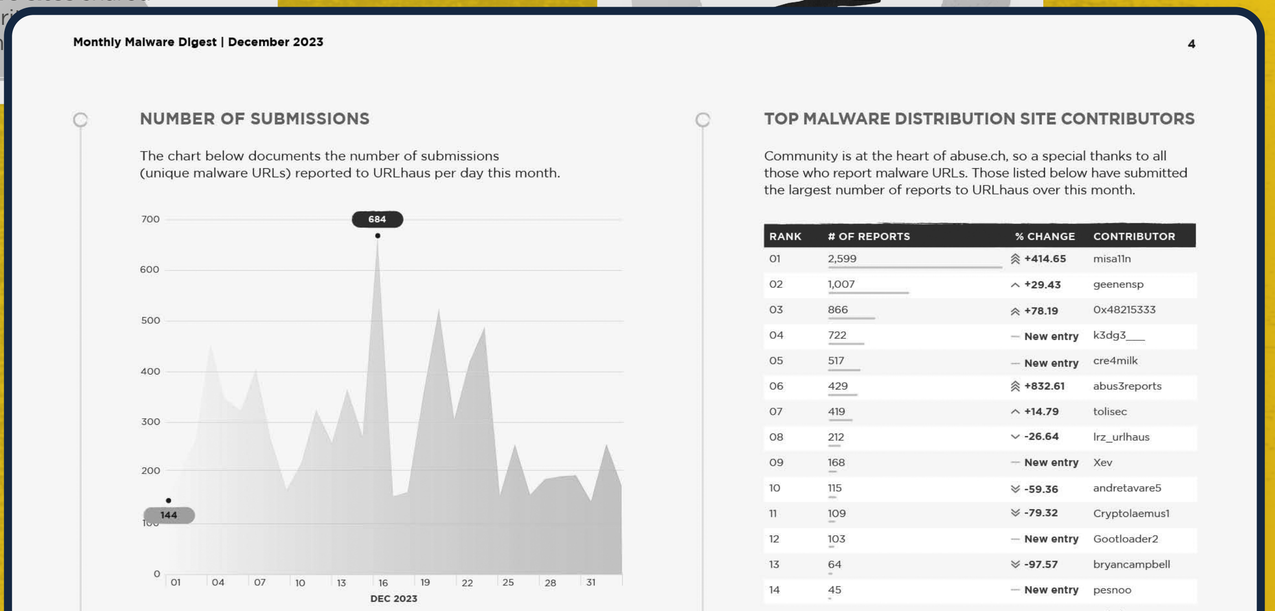
SPAMHAUS ABUSE.ch

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.





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	**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

9,100

Malware sites shared by security researchers on URLhaus

-5%

decrease on the previous month

14,376

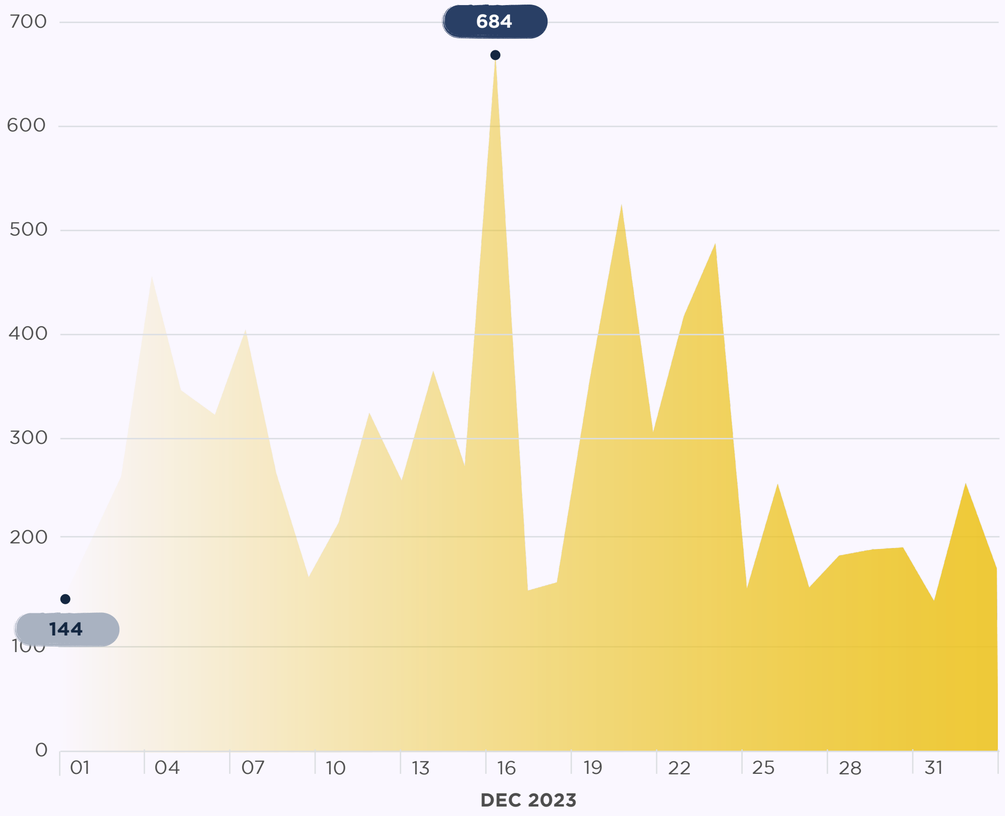
Abuse reports sent out to hosting providers and network owners

90.7%

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.

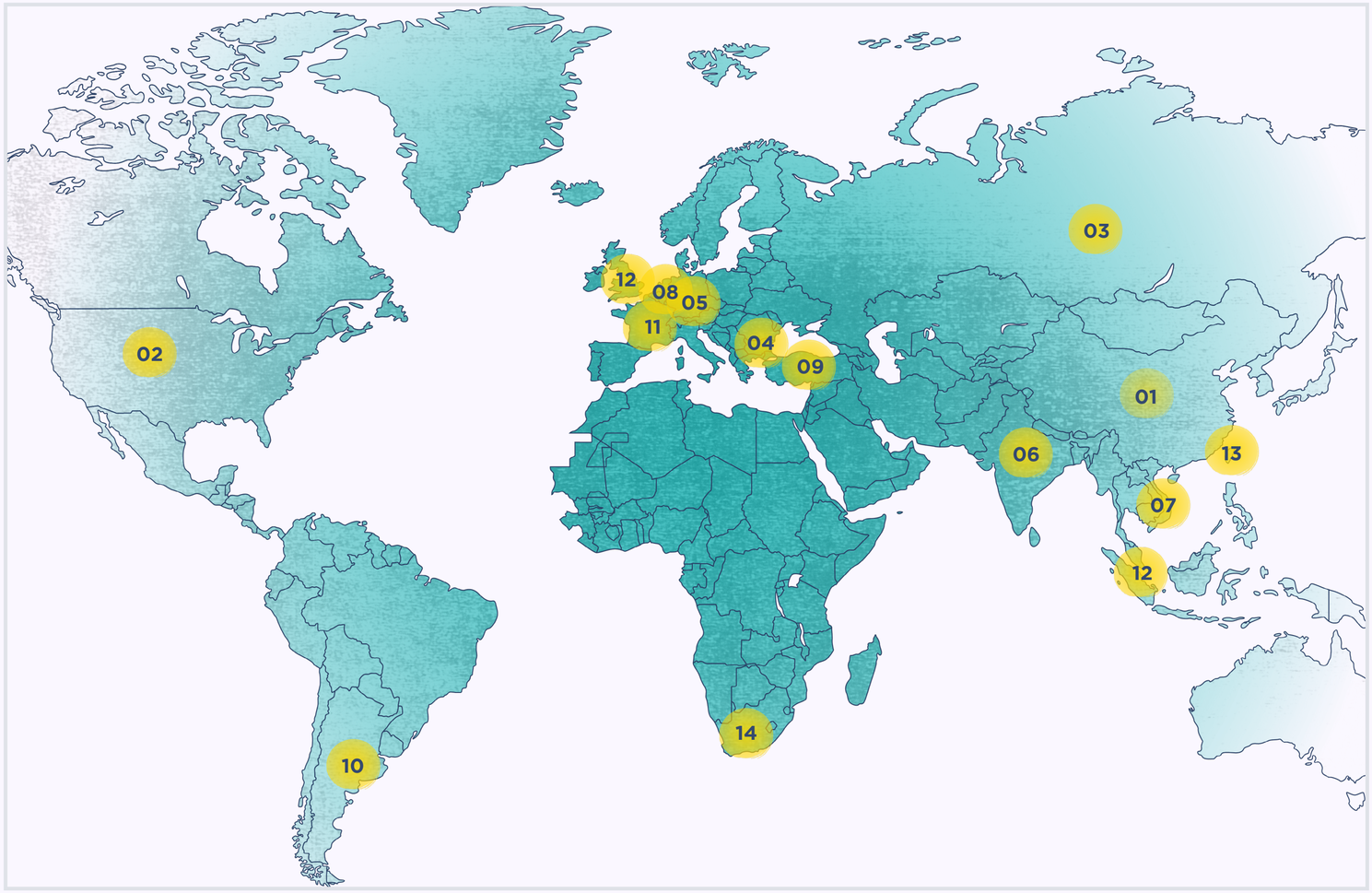


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	2,599	+414.65	misa11n
02	1,007	+29.43	geenensp
03	866	+78.19	0x48215333
04	722	New entry	k3dg3___
05	517	New entry	cre4milk
06	429	+832.61	abus3reports
07	419	+14.79	tolisec
08	212	-26.64	lrz_urlhaus
09	168	New entry	Xev
10	115	-59.36	andretavare5
11	109	-79.32	Cryptolaemus1
12	103	New entry	Gootloader2
13	64	-97.57	bryancampbell
14	45	New entry	pesnoo
15	35	New entry	redrabytes

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	3,005	+360.18	China
02	784	+71.93	United States
03	297	+45.59	Russia
04	291	+25.43	Bulgaria
05	265	-50.37	Germany
06	212	New entry	India
07	207	+64.29	Vietnam
08	202	-57.29	Netherlands
09	146	New entry	Turkey
10	139	+18.80	Argentina
11	132	-54.79	France
12	95	+265.38	Singapore
12	95	-64.55	United Kingdom
13	77	+102.63	Taiwan
14	76	+90.00	South Africa

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	2,419	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
02	554	AS4837	CHINA169-BACK-BONE,CHINA UNICOM China 169 Backbone	China
03	550	AS13335	CLOUDFLARENET	United States
04	246	AS14061	DIGITALOCEAN-ASN	United States
05	229	AS10617	SION S.A	Argentina
06	204	AS24940	HETZNER-AS	Germany
07	186	AS216240	MORTALSOFT	United Kingdom
08	131	AS47583	AS-HOSTINGER	United States
08	131	AS55293	A2HOSTING	United States
09	127	AS394711	LIMENET	United States
10	121	AS16276	OVH	France
11	111	AS19871	NETWORK-SOLU-TIONS-HOSTING	United States
12	91	AS51559	NETINTERNET Bilisim Teknolojileri AS	Tokelau
13	82	AS47541	VKONTAKTE-SPB-AS vk.com	Russia
14	79	AS20473	AS-CHOOPA	United States

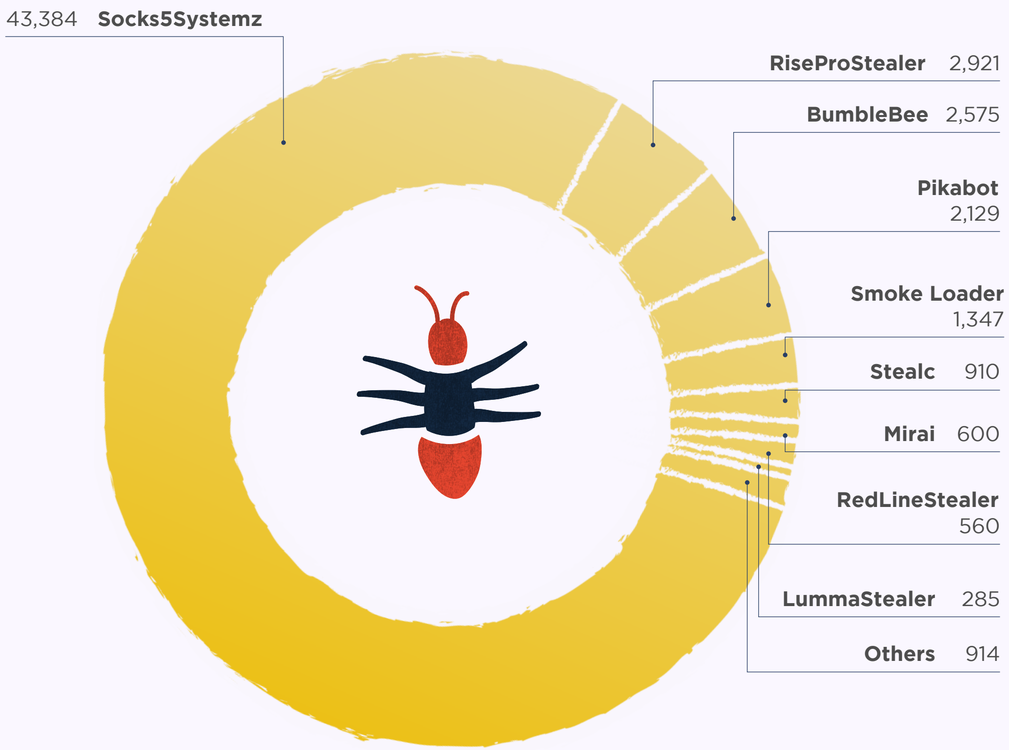
TOP MALWARE HOSTS

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	149	cdn.discordapp.com	Discord	United States
02	82	vk.com	VK	Russia
03	62	wtools.io	WTOOLS	null
04	27	paste.ee	Paste.ee	null
05	19	drive.google.com	Google	United States
05	19	github.com	Github	United States
06	18	pastebin.com	Pastebin	null

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	Socks5Systemz	+2,966.01		43,384
02	Stealc	+147.28		910
03	RiseProStealer	+121.29		2,921
04	LummaStealer	+2.52		285
05	Mirai	+0.67		600
06	BumbleBee	-0.23		2,575
07	Smoke Loader	-1.61		1,347
08	Amadey	-25.09		206
09	RedLineStealer	-61.06		560
10	Pikabot	New entry		2,129
10	CoinMiner	New entry		276
10	Gafgyt	New entry		170
10	Ransomware.Stop	New entry		112
10	AgentTesla	New entry		87
10	Tofsee	New entry		63

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

10,416

Malware samples shared by security researchers on MalwareBazaar

+4.9%

increase on the previous month

1,426

Active hunting rules

+2.4%

increase on the previous month

37.14MB

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.

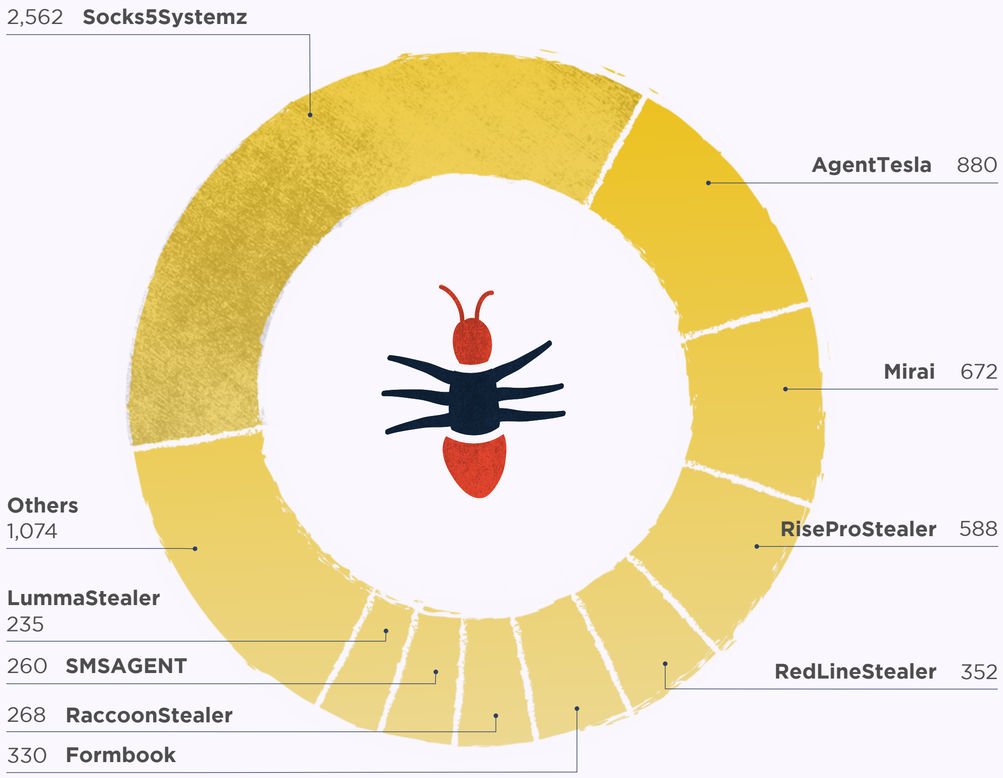
TOP SAMPLE CONTRIBUTORS

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	% CHANGE	CONTRIBUTOR
01	2,164	— New entry	Xev
02	1,089	^ +5.93	andretavare5
03	383	^^ +76.50	elfdigest
04	309	v -30.41	cocaman
05	192	v -28.36	adrian__luca
06	190	v -29.89	lowmal3
07	171	^ +8.23	smica83
08	150	^^ +219.15	adm1n_usa32
09	87	^^ +27.94	Porcupine
09	87	v -29.84	TeamDreier
10	69	^ +1.47	pr0xylife
11	61	v -79.60	JAMESWT_MHT
12	59	v -45.37	malwarelabnet
13	52	— New entry	jstrosch
14	31	— New entry	V3n0mStrike

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



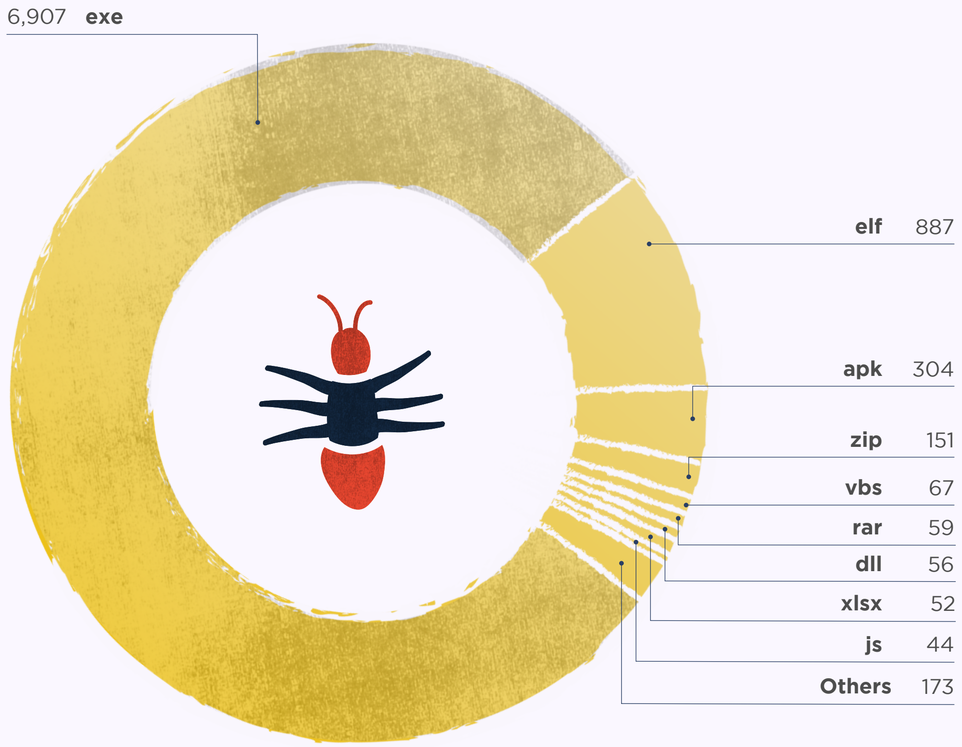
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	RiseProStealer	**+114.60**		588
02	LummaStealer	**+16.92**		235
03	Mirai	**+6.67**		672
04	Stealc	**-0.88**		225
05	GuLoader	**-12.23**		165
06	Smoke Loader	**-14.81**		230
07	AgentTesla	**-32.15**		880
08	Formbook	**-35.80**		330
09	RedLineStealer	**-46.01**		352
10	RemcosRAT	**-61.82**		147
11	Socks5Systemz	**New entry**		2,562
11	RaccoonStealer	**New entry**		268
11	SMSAGENT	**New entry**		260
11	Gafgyt	**New entry**		180
11	DCRat	**New entry**		127

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	2,145	shellcode	nex
02	1,952	MD5_Constants	phoul
03	1,523	DebuggerCheck__API	n/a
04	1,246	maldoc_find_kernel32_base_method_1	Didier Stevens
05	1,075	NET	malware-lu
06	555	NETexecutableMicrosoft	malware-lu
07	539	pe_no_import_table	n/a
08	475	INDICATOR_EXE_Packed_VMProtect	ditekSHen
09	443	Check_OutputDebugStringA_iat	n/a
10	423	Windows_Trojan_Smokeload-er_3687686f	Elastic Security
11	399	maldoc_getEIP_method_1	Didier Stevens
12	359	DebuggerCheck__QueryInfo	n/a
13	341	PE_Digital_Certificate	albertzsigovits
14	287	unixredflags3	Tim Brown
15	281	myMirai	n/a

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)

14,555

Indicators of compromise (IOCS) shared on ThreatFox

+35.1%

increase on the previous month

2,883

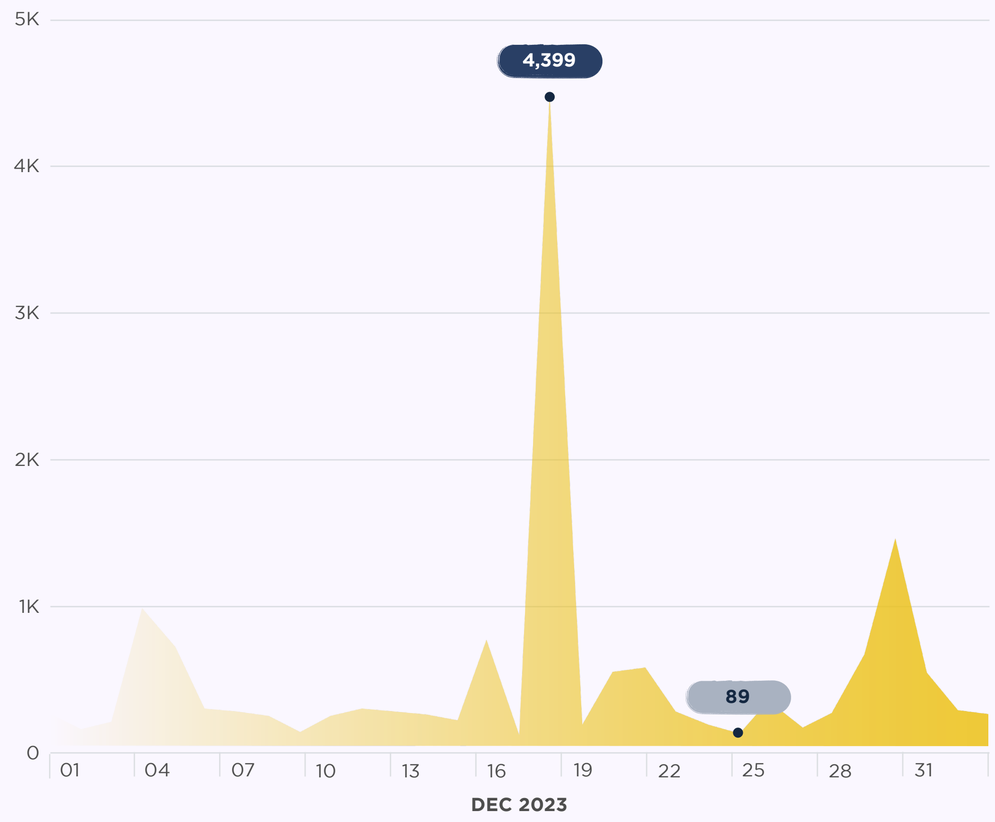
IOCs relating to Cybergate

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.



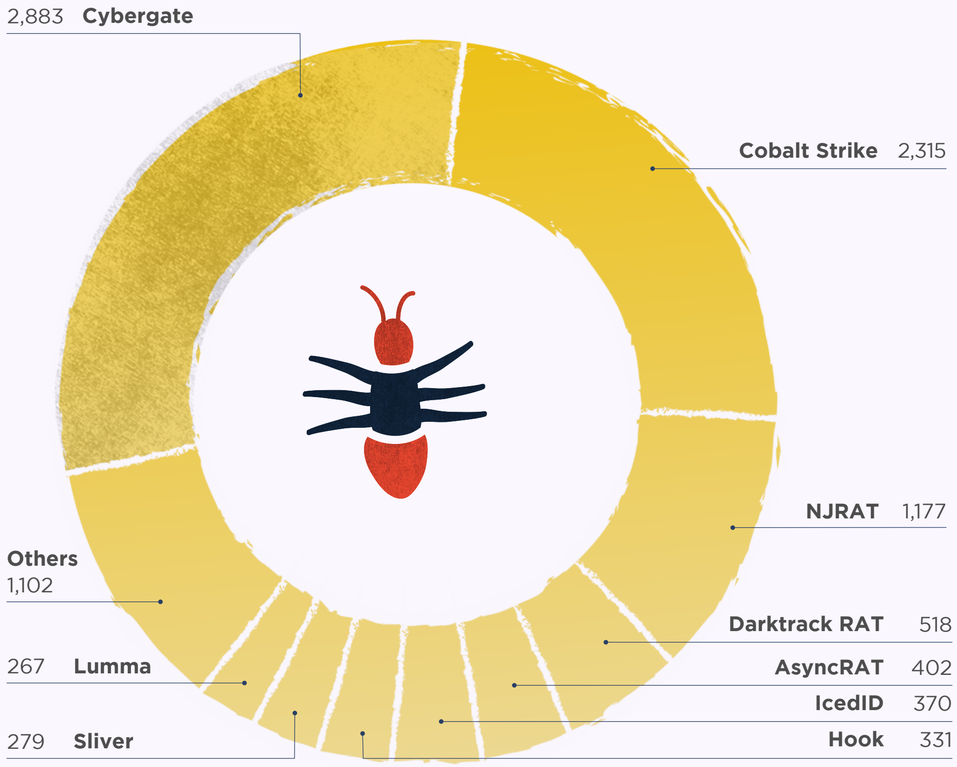
IOC TYPE

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	6,948	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
02	5,659	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
03	1,609	url	botnet_cc	URL that is used for botnet Command&control (C&C)
04	314	url	payload_ delivery	URL that delivers a malware payload
05	175	domain	payload_ delivery	Domain name that delivers a malware payload
06	35	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
07	28	md5_hash	payload	MD5 hash of a malware sample (payload)
08	16	ip:port	payload_ delivery	ip:port combination that delivers a malware payload
09	9	sha1_hash	payload	SHA1 hash of a malware sample (payload)
10	4	domain	cc_skimming	Domain used for credit card skimming (usually related to Magecart attacks)

TOP MALWARE FAMILIES

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



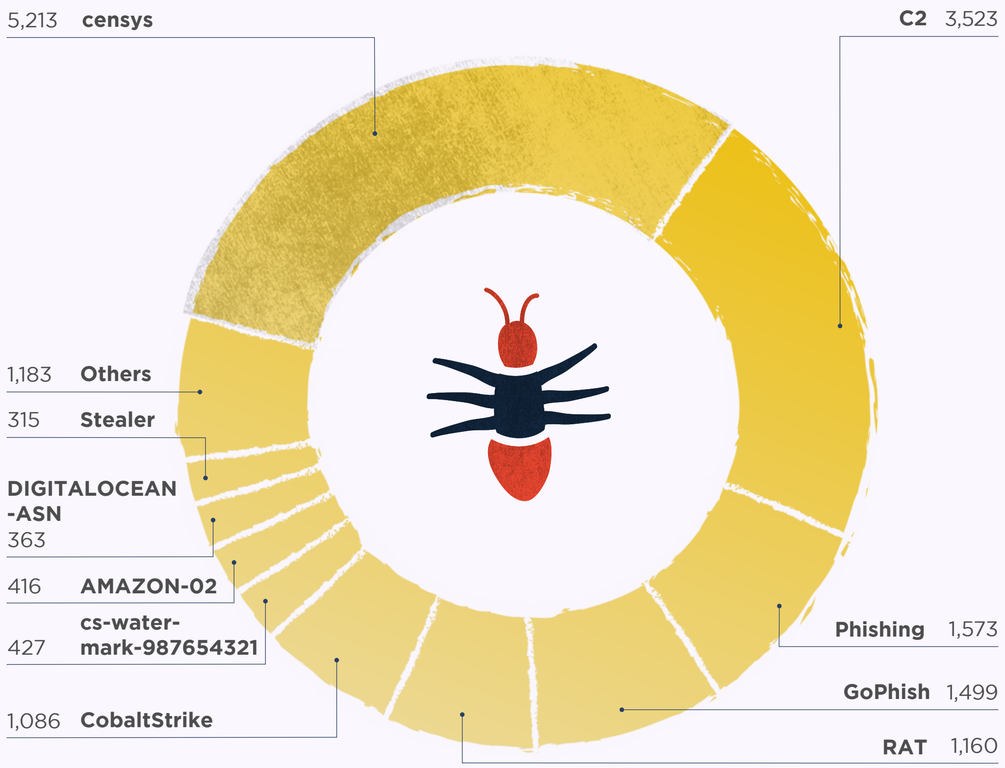
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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	Lumma	**+64.81**		267
02	AsyncRAT	**+19.29**		402
03	Cobalt Strike	**+7.67**		2,315
04	Coper	**+3.33**		155
05	Qakbot	**-17.83**		258
06	Hook	**-62.73**		331
07	Cybergate	**New entry**		2,883
07	NJRAT	**New entry**		1,177
07	Darktrack RAT	**New entry**		518
07	IcedID	**New entry**		370
07	Sliver	**New entry**		279
07	NanoCore	**New entry**		194
07	Pikabot	**New entry**		189
07	DCRat	**New entry**		163
07	Socks5Systemz	**New entry**		143

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	DIGITALOCEAN-ASN	**+159.29**	363
02	AMAZON-02	**+127.32**	416
03	cs-watermark-987654321	**+44.26**	427
04	Supershell	**+20.09**	269
05	CobaltStrike	**+17.79**	1,086
06	censys	**+11.25**	5,213
07	Qakbot	**-26.23**	225
08	C2	**-29.21**	3,523
09	RAT	**-52.54**	1,160
10	Phishing	**New entry**	1,573
10	GoPhish	**New entry**	1,499
10	Stealer	**New entry**	315
10	BLNWX	**New entry**	283
10	MICROSOFT-CORP-MSN-AS-BLOCK	**New entry**	217
10	lummastealer	**New entry**	189

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

8,517,913

File scans conducted on YARAify

7,654,362

Distinct files that had scans performed on them

-7.8%

decrease in file scans on the previous month

-6%

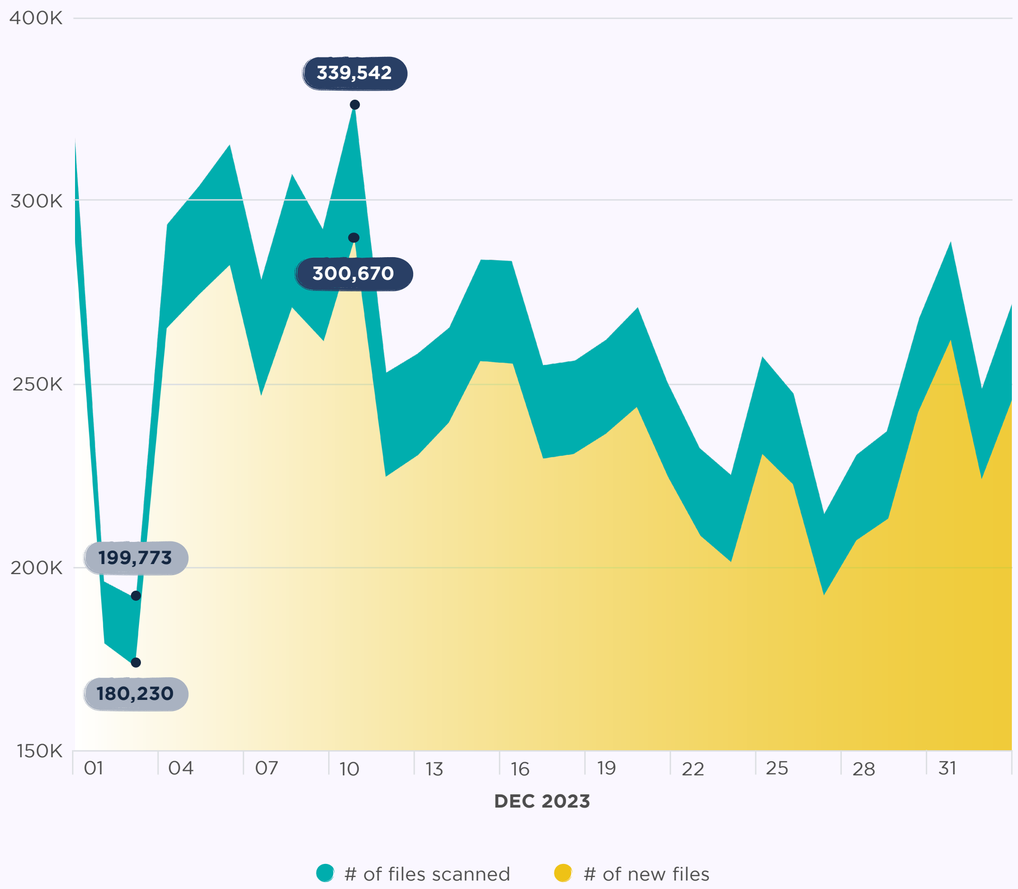
decrease in distinct files on the previous month

19,079

YARA rules deployed on YARAify and available for hunting

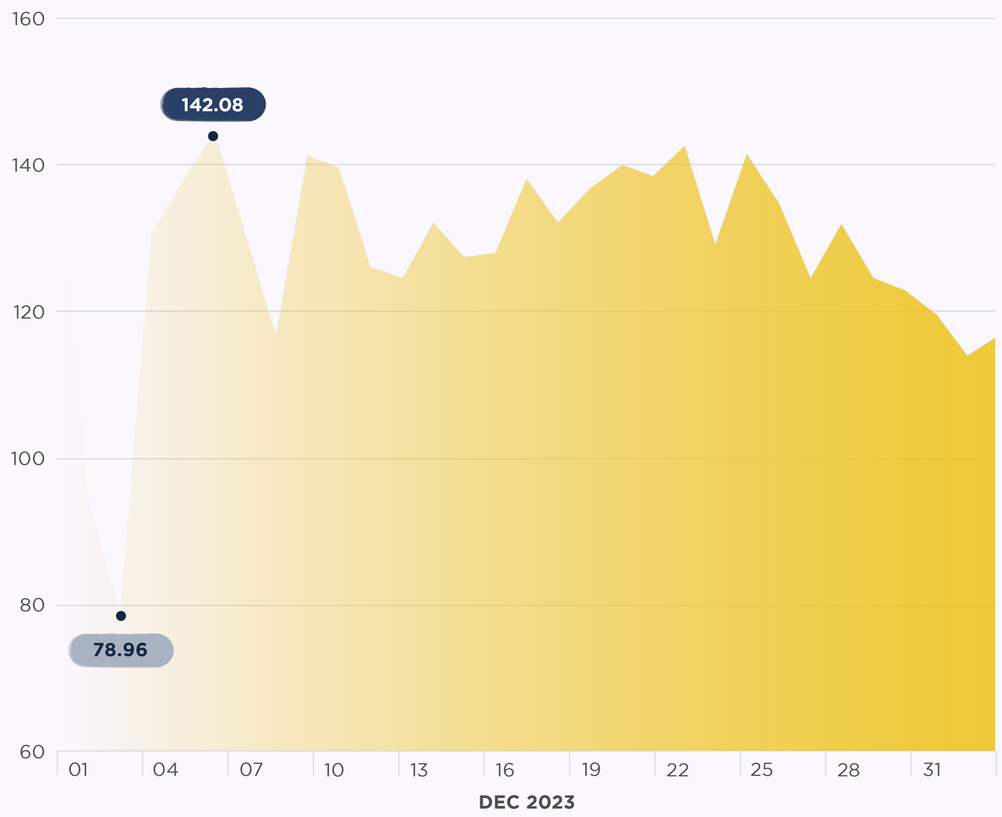
FILES SCANNED PER DAY

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	3,009,683	-56.75	maldoc_getEIP_method_1	Didier Stevens
02	188,899	-55.99	DebuggerCheck__API	n/a
03	133,961	-54.11	maldoc_find_kernel32_base_method_1	Didier Stevens
04	113,743	-57.31	Check_Dlls	n/a
05	108,434	-61.85	NET	malware-lu
06	99,398	-13.27	SHA512_Constants	phoul
07	98,602	-12.80	malware_shellcode_hash	JPCERT/CC Incident Response Group
08	86,970	-60.22	SUSP_XORed_URL_in_EXE_RID2E46	n/a
09	86,930	-60.22	SUSP_XORed_URL_In_EXE	Florian Roth
10	70,248	-50.63	MD5_Constants	phoul
11	67,342	-62.52	UPXV200V290MarkusOberhumerLaszloMolnarJohnReiser	malware-lu
12	62,079	-31.87	vmdetect	nex
13	59,428	-58.77	SHA1_Constants	phoul
13	59,428	-58.77	RIPEMD160_Constants	phoul
14	58,185	-63.81	UPXv20MarkusLaszloReise	malware-lu

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	5,828,582	-10.23	PUA.Win.Packer.Lccwin-2
02	3,915,573	-9.59	Win.Trojan.Obfus-38
03	3,468,021	+24.32	Win.Trojan.Qukart-6874817-0
04	2,481,022	+24.57	Win.Malware.Qukart-6838239-0
05	2,444,099	New entry	Win.Trojan.Padodor-10016488-0
06	1,815,524	New entry	null
07	1,058,312	-45.72	Win.Trojan.Padodor-9877164-0
08	668,979	+21.90	Win.Packed.Razy-10010080-0
09	664,166	+33.93	Win.Trojan.Berbew-9845290-1
10	577,147	-27.77	Win.Trojan.Berbew-10013977-0
11	541,130	-25.59	Win.Trojan.Crypted-29
12	535,036	-26.15	Win.Trojan.Crypted-30
13	468,868	New entry	Win.Trojan.Packz-10015071-0
14	378,944	New entry	Win.Trojan.Razy-10015064-0
15	367,452	-30.37	Win.Malware.Padodor-10012877-0

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN FEBRUARY

Remember, sharing is caring.