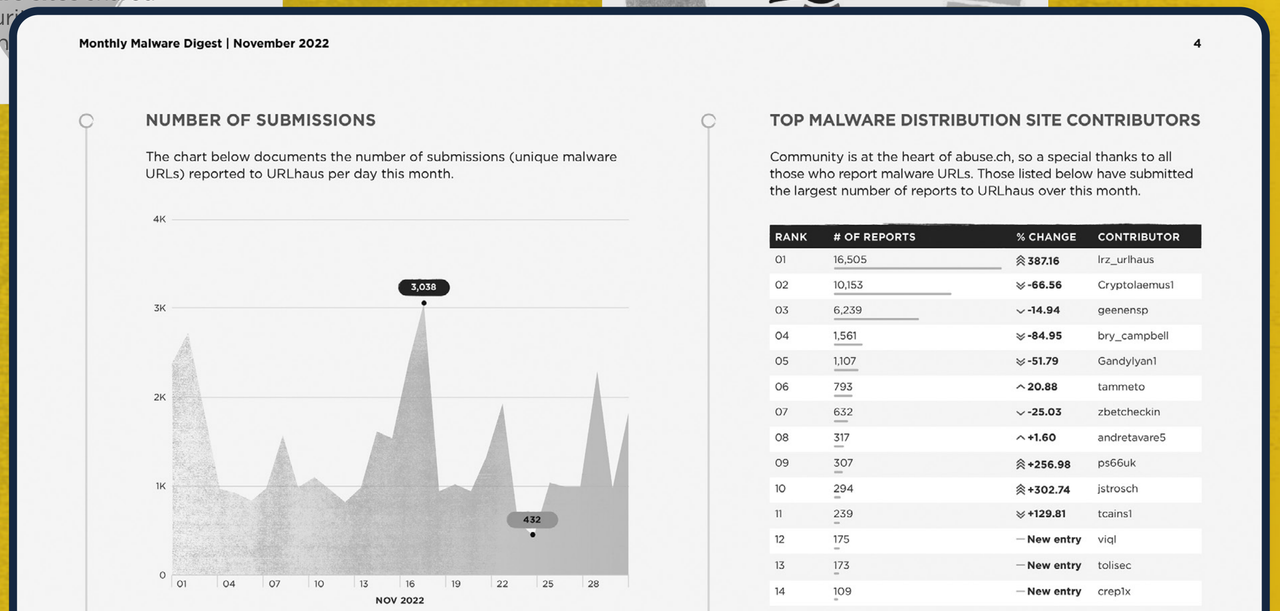
NOVEMBER 2022

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.



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

40,650

Malware sites shared by security researchers on URLhaus

-15.5%

Decrease on the previous month

45,151

Abuse reports sent out to hosting providers and network owners

85%

Of abuse reports **have been acted upon**

NUMBER OF SUBMISSIONS

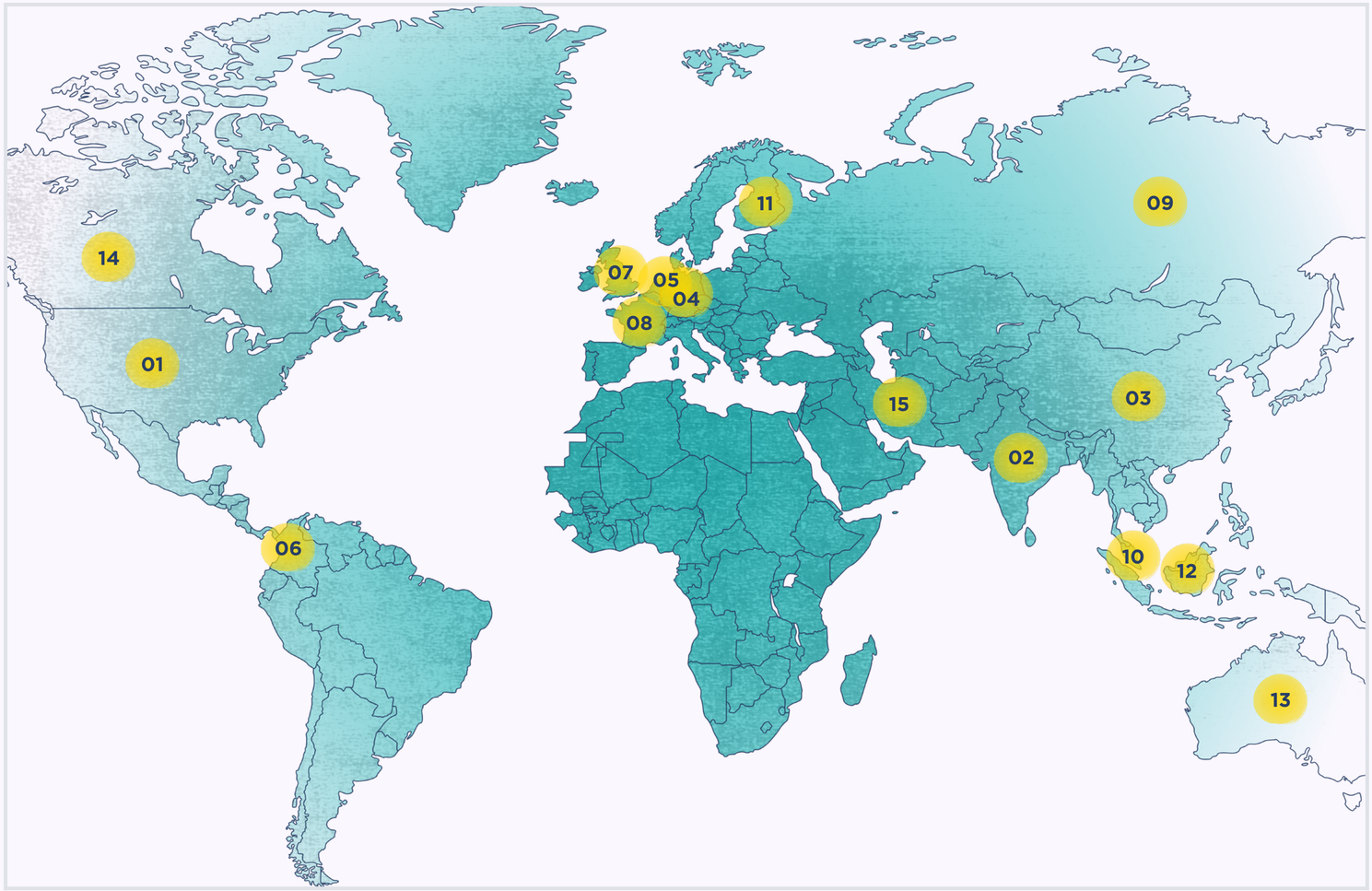
The chart below documents the number of submissions (unique malware URLs) reported to URLhaus per day this month.

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	16,505	**387.16**	lrz_urlhaus
02	10,153	**-66.56**	Cryptolaemus1
03	6,239	**-14.94**	geenensp
04	1,561	**-84.95**	bry_campbell
05	1,107	**-51.79**	Gandylyan1
06	793	**+20.88**	tammeto
07	632	**-25.03**	zbetcheckin
08	317	**+1.60**	andretavare5
09	307	**+256.98**	ps66uk
10	294	**+302.74**	jstrosch
11	239	**+129.81**	tcains1
12	175	**New entry**	viql
13	173	**New entry**	tolisec
14	109	**New entry**	crep1x
15	63	**-3.08**	r3dbU7z

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	8607	-51.74	United States
02	3565	-17.44	China
03	1720	-61.13	India
04	753	-48.42	Germany
05	513	-60.66	Netherlands
06	362	New entry	Colombia
07	288	-57.71	United Kingdom
08	267	-70.82	France
09	243	-40.00	Russia
10	176	-74.89	Singapore
11	167	New entry	Finland
12	166	-80.45	Indonesia
13	151	New entry	Australia
14	151	73.60	Canada
15	151	-58.52	Iran

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	2,650	AS22612	NAMECHEAP	United States
02	2,248	AS4837	CHINA169	China
03	1,797	AS46606	UNIFIEDLAYER	United States
04	1,194	AS4134	CHINANET	China
05	1,107	AS394695	PUBLIC-DOMAIN-REGISTRY	India
06	917	AS13335	CLOUDFLARE	United States
07	730	AS9829	BSNL	India
08	688	AS8068	MICROSOFT	United States
09	473	AS24940	HETZNER	Germany
10	271	AS23352	SERVERCENTRAL	United States
11	269	AS19871	NETWORK-SOLUTIONS	United States
12	243	AS16276	OVH	France
13	219	AS51167	CONTABO	Germany
14	177	AS36352	COLOCROSSING	United States
15	173	AS16509	AMAZON	United States

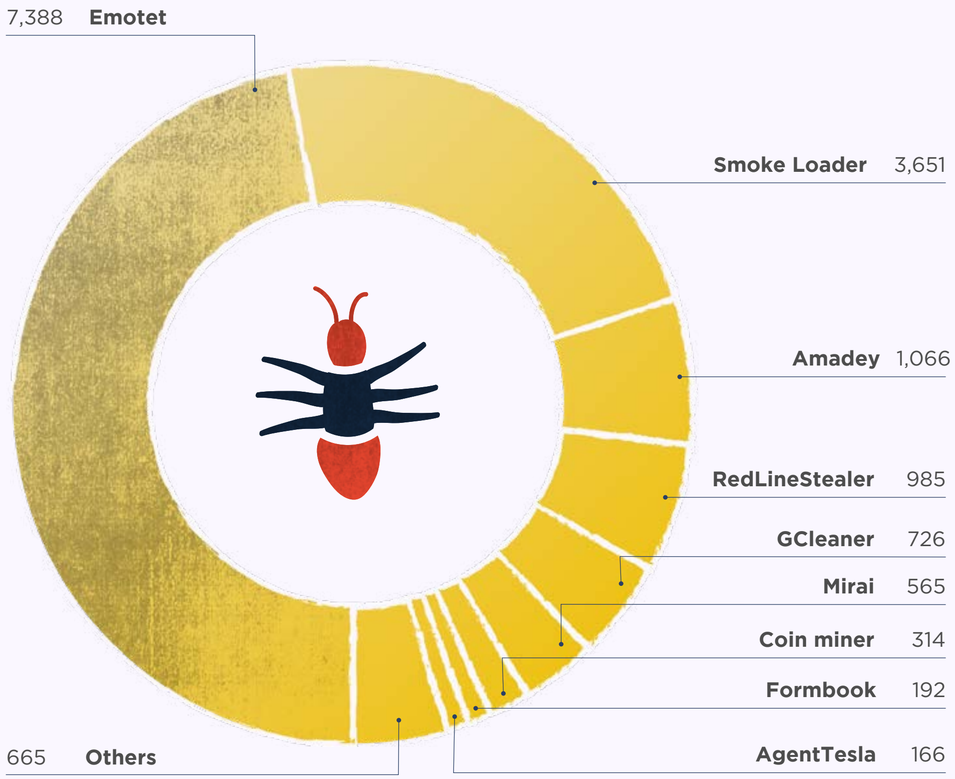
TOP MALWARE HOSTS

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	690	onedrive.live.com	Microsoft	United States
02	251	vk.com	VK	Russia
03	148	cdn.discordapp.com	Discord	United States
04	56	raw.githubusercontent.com	Github	United States
05	43	transfer.sh	n/a	Netherlands
06	34	bitbucket.org	Bitbucket	United States
07	31	194.180.48.22	n/a	n/a
08	29	github.com	Github	United States

TOP MALWARE FAMILIES ASSOCIATED WITH MALWARE SITES

This chart shows, by percentage, 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	Amadey	+620.27		1,066
02	AgentTesla	+30.71		166
03	RedLineStealer	+21.16		985
04	Loki	+5.56		133
05	Smoke Loader	+2.96		3,651
06	Mirai	-15.80		565
07	GCleaner	-25.39		726
08	RecordBreaker	-36.62		90
09	ArkeiStealer	-41.76		106
10	CoinMiner	-53.96		314
11	Tofsee	New entry		142
12	Formbook	New entry		192
13	SnakeKeylogger	New entry		101
14	RemcosRAT	New entry		93
15	Emotet	New entry		7,388

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

16,931

Malware samples shared by security researchers on MalwareBazaar

+23.2%

Increase on the previous month

1,964

Active hunting rules

+1.08%

Increase on the previous month

1.1MB

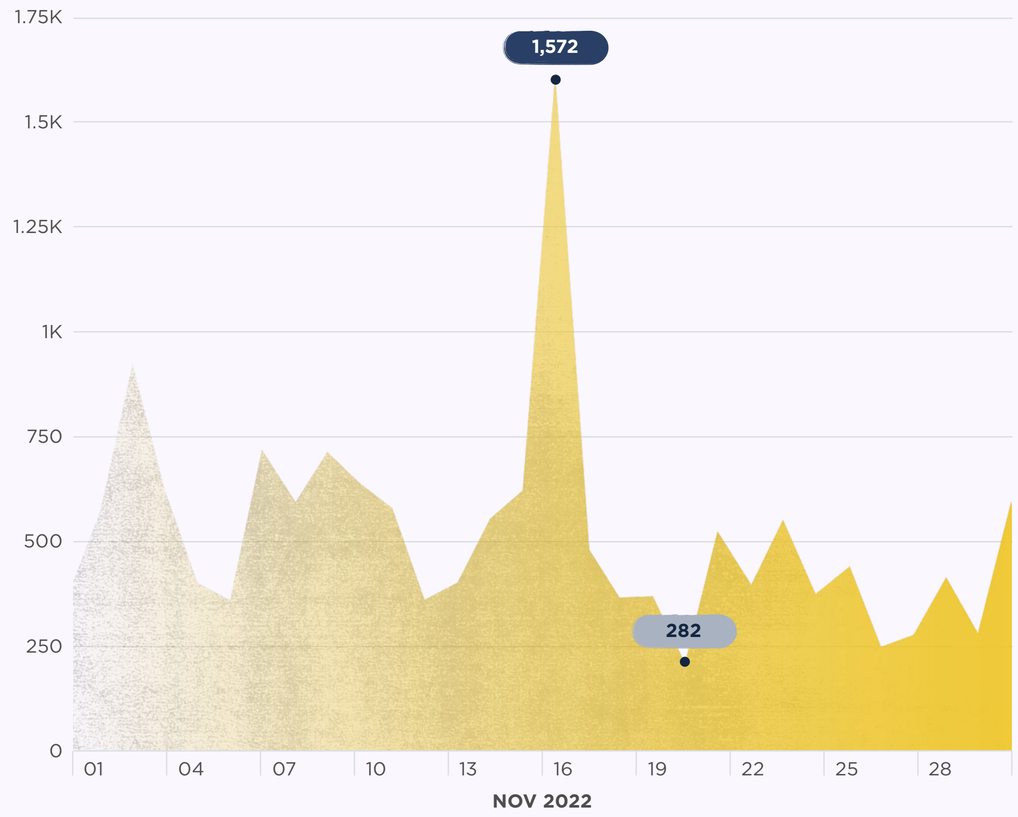
Avarage size of a malware sample

EXE & ELF FILES

Windows executables (exe) and ELF 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.



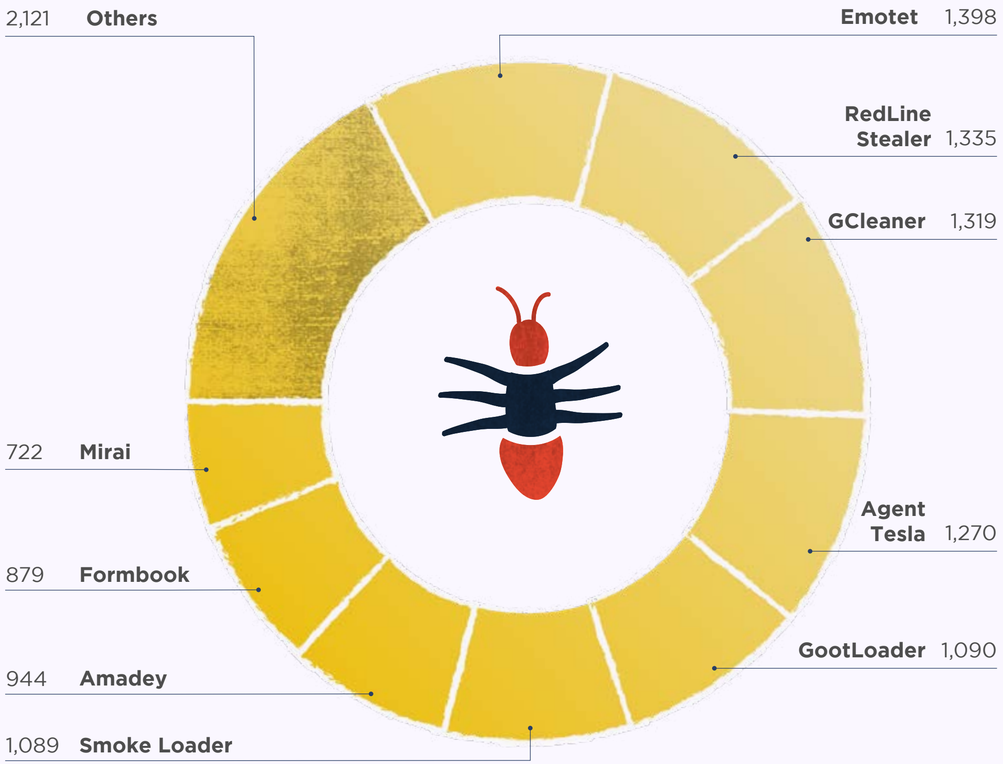
TOP SAMPLE CONTRIBUTORS

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	1,817	+54.24	@zbetcheckin
02	1,094	+49.25	@SecuriteInfoCom
03	1,085	+474.07	@GootLoaderSites
04	962	+607.35	@jstrosch
05	365	-12.26	@cocaman
06	331	-30.46	@JAMESWT_MHT
07	254	-54.48	@GovCERT_CH
08	218	-24.57	@adrian__luca
09	213	-29.70	@lowmal3
10	165	+2.48	@pr0xylife
11	156	-4.29	@malwarelabnet
12	142	-80.60	@petikvx
13	132	-11.41	@James_inthe_box
14	114	New entry	@EstisRemiel
15	101	New entry	@elfdigest

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



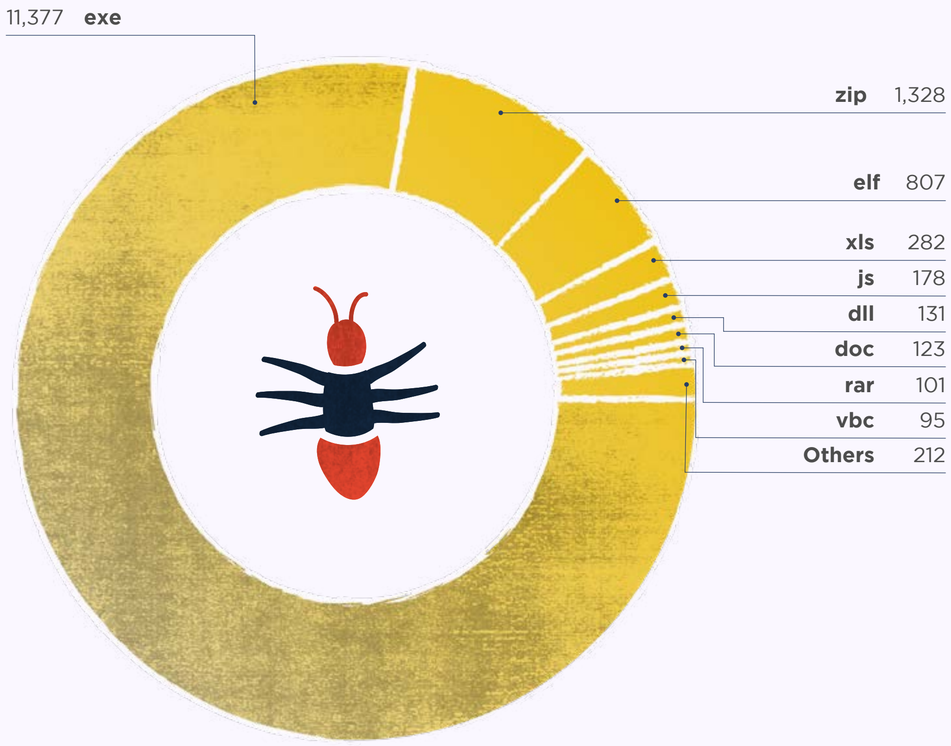
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	GootLoader	+426.57		1,090
02	GCleaner	+34.87		1,319
03	AgentTesla	+20.38		1,270
04	RemcosRAT	+20		336
05	RedLineStealer	+15.58		1,335
06	Formbook	+14.30		879
07	Smoke Loader	+3.03		1,089
08	GuLoader	-2.20		311
09	Loki	-4.43		367
10	Mirai	-13.01		722
11	SnakeKeylogger	-32.11		499
12	CoinMiner	New entry		368
13	Amadey	New entry		944
14	Emotet	New entry		1,398
15	Tofsee	New entry		240

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	2,424	Windows_Trojan_ Smokeloader_3687686f	Elastic Security
02	1,900	cobalt_strike_tmp01925d3f	The DFIR Report
03	1,087	win_smokeloader_a2	pnx
04	821	MALWARE_Win_RedLine	ditekshen
05	745	win_heodo	n/a
06	744	win_emotet_a3	SWITCH-CERT
07	707	meth_stackstrings	Felix Bilstein
08	548	win_emotet_auto	Willi Ballenthin
09	539	crime_win64_emotet_ unpacked	r0ny_123
10	449	win_nymaim_g0	CERT.pl
11	446	win_gcleaner_auto	Felix Bilstein
12	424	myMirai	n/a
13	407	linux_generic_ipv6_catcher	@_lubiedo
14	405	unixredflags3	@timb_machine
15	311	tofsee_yhub	Billy Austin

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)

72,053

Indicators of compromise (IOCS) shared on ThreatFox

-20.1%

Decrease on the previous month

46,814

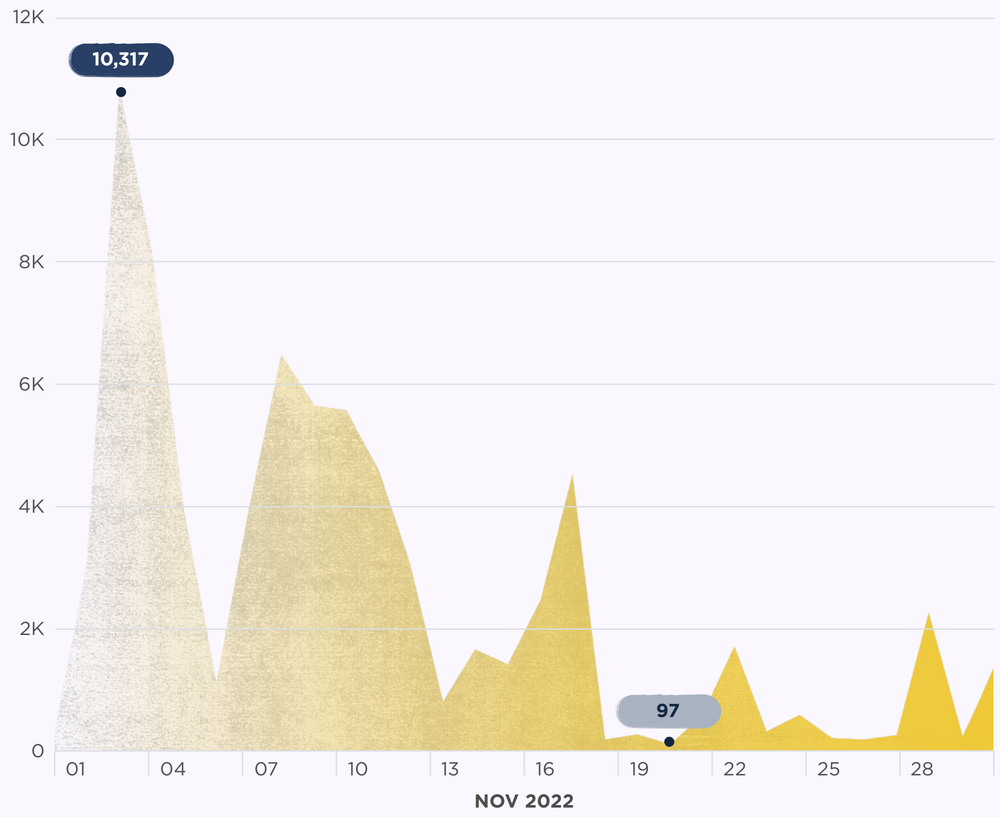
IOCs relating to Emotet

NEW ENTRY

In November

NUMBER OF IOCs SHARED PER DAY

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



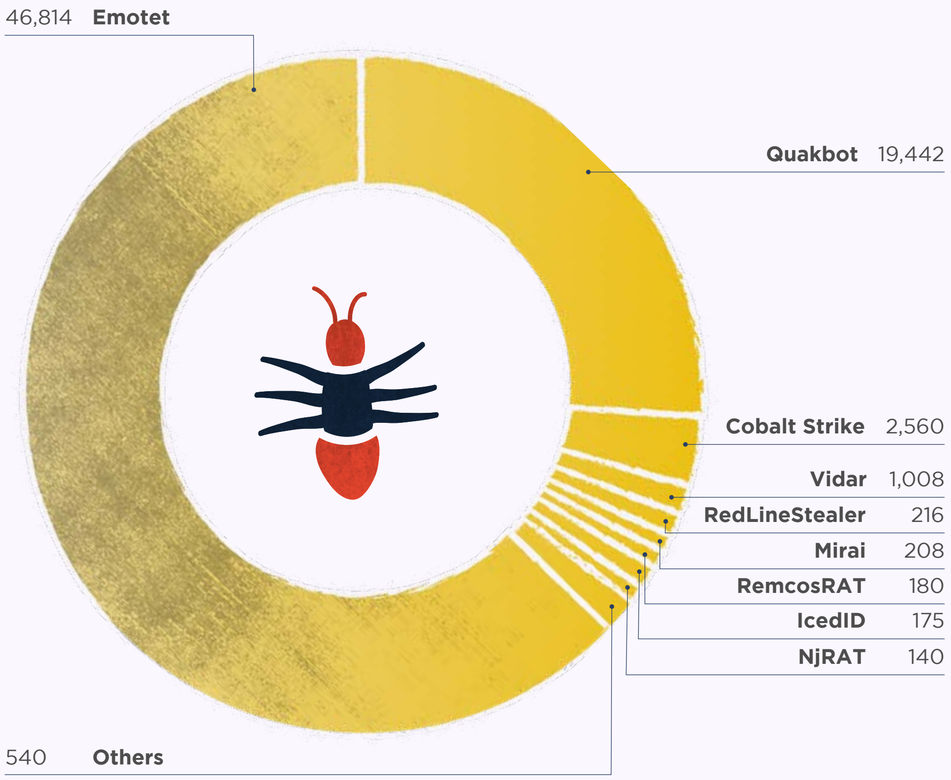
IOC TYPE

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	46,809	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
02	11,812	url	payload_delivery	URL that delivers a malware payload
03	7,637	domain	payload_delivery	Domain name that delivers a malware payload
04	2,582	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
05	2,531	url	botnet_cc	URL that is used for botnet Command&control (C&C)
06	619	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
07	36	md5_hash	payload	MD5 hash of a malware sample (payload)
08	26	ip:port	payload_delivery	ip:port combination that delivery a malware payload
09	1	domain	cc_skimming	Domain used for credit card skimming (usually related to Magecart attacks)

TOP MALWARE FAMILIES

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



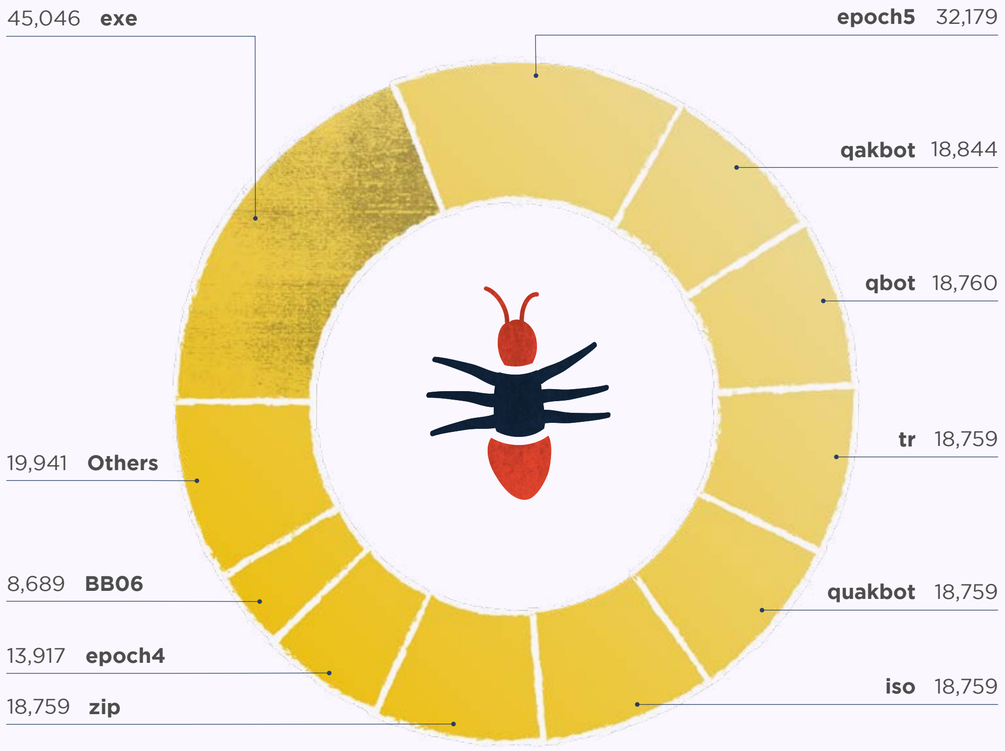
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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	IcedID	**+40**		175
02	Mirai	**+8.33**		208
03	Alien	**+6.25**		68
04	RedLineStealer	**0**		216
05	Loki	**-9.57**		85
06	Cobalt Strike	**-16.29**		2,560
07	RecordBreaker	**-21.98**		71
08	RemcosRAT	**-36.40**		180
09	BumbleBee	**-37.50**		100
10	NjRAT	**-38.86**		140
11	Quakbot	**-76.89**		19,442
12	CryptBot	**New entry**		134
13	Grandoreiro	**New entry**		82
14	Vidar	**New entry**		1,008
15	Emotet	**New entry**		46,814

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	iso	**-76.21**	18759
02	zip	**-77.25**	18,759
03	qakbot	**-77.42**	18,844
04	qbot	**-77.42**	18,760
05	quakbot	**-77.51**	18,759
06	epoch5	**New entry**	32,179
07	tr	**New entry**	18,759
08	exe	**New entry**	45,046
09	epoch4	**New entry**	13,917
10	BB06	**New entry**	8,689
11	SK16	**New entry**	6,134
12	BB05	**New entry**	5,306
13	W19	**New entry**	3004,
14	BB08	**New entry**	2,962
15	CobaltStrike	**New entry**	2,535

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

2,082,475

File scans conducted
on YARAify

1,748,898

Distinct files
that had scans performed on them

-9.1%

Decrease in
file scans on the previous month

-6.6%

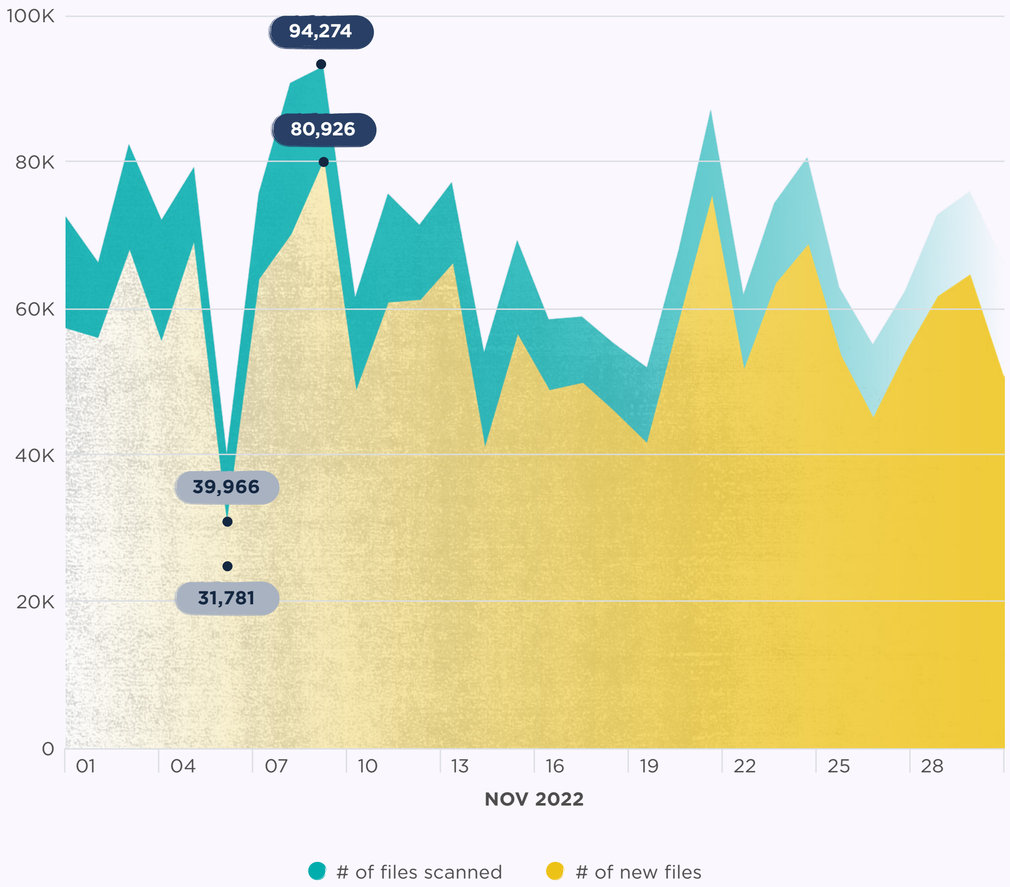
Decrease in
files on the previous month

14,233

YARA rules deployed
on YARAify and available for hunting

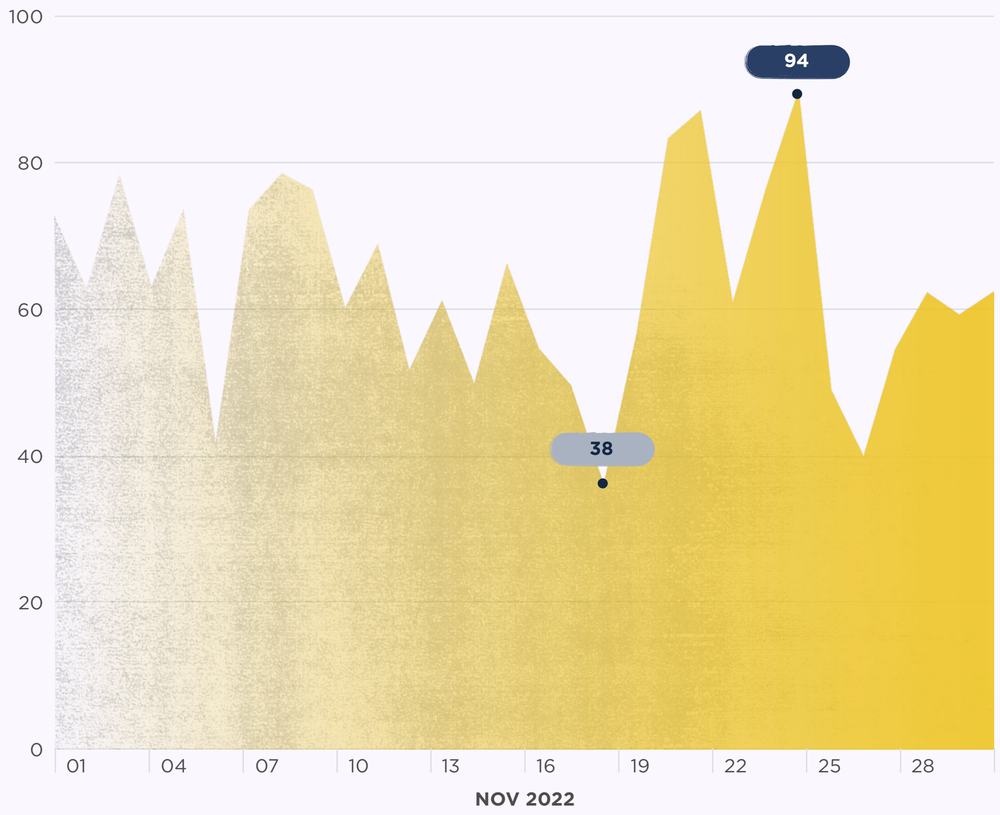
FILES SCANNED PER DAY

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	83,816	— New entry	QbotStuff	anonymous
02	78,981	— New entry	BitcoinAddress	DidierStevens
03	57,823	⌄⌄ -13.07	command_and_control	CD_R0M_
04	31,309	⌄ -6.79	INDICATOR_EXE_Packed_MPress	ditekSHen
05	26,423	⌄⌄ -35.41	win_sality_auto	Felix Bilstein
06	25,683	⌃⌃ +28.54	cobalt_strike_tmp01925d3f	The DFIR Report
07	23,029	— New entry	win_heodo	n/a
08	23,029	— New entry	win_emotet_a3	SWITCH-CERT
09	18,679	— New entry	crime_win64_emotet_unpacked	r0ny_123
10	18,164	⌃ +2.59	SUSP_XORed_URL_in_EXE_RID2E46	n/a
11	18,158	— New entry	win_emotet_auto	Felix Bilstein
12	17,143	⌄ -0.33	SUSP_XORed_URL_in_EXE	Florian Roth
13	16,490	— New entry	with_urls	n/a
14	15,827	⌃ +9.26	win_vobfus_auto	Felix Bilstein
15	13,330	⌄⌄ -14.88	win_smokeloader_a2	pnx

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	200,847	— New entry	Win.Malware.Zusy-6878655-0
02	196,229	— New entry	Win.Malware.Midie-6847893-0
03	187,433	— New entry	Win.Malware.Midie-6847981-0
04	182,210	— New entry	Win.Malware.Midie-6848630-0
05	181,869	— New entry	Win.Malware.Midie-6847894-0
06	171,506	— New entry	Win.Malware.Midie-6848784-0
07	171,506	— New entry	Win.Malware.Midie-6847892-0
08	116,580	— New entry	Win.Packed.Generic-9967832-0
09	38,431	⌄⌄ -36.83try	PUA.Win.Packer.Lccwin-2
10	34,725	⌄⌄ -37.31	Win.Trojan.Qukart-6874817-0
11	29,757	— New entry	Win.Trojan.Generic-9959068-0
12	25,537	⌄⌄ -35.80	Win.Trojan.Obfus-38
13	23,963	— New entry	PUA.Win.Packer.Asprotect-3
14	23,963	— New entry	PUA.Win.Packer.ProtectSharewar-2
15	23,963	— New entry	PUA.Win.Packer.ProtectSharewar-3

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN JANUARY

Remember, sharing is caring.