AUGUST 2023

SPAMHAUS ABUSE.ch

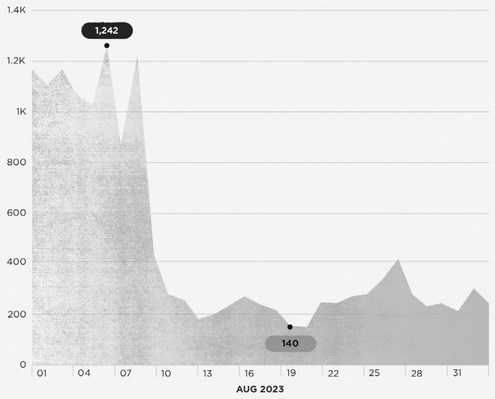
MONTHLY MALWARE DIGEST

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.

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	4,701	-62.21	geenensp
02	4,409	+773.07	lrz_urlhaus
03	280	+4,566.67	Gootloader2
04	150	-23.47	andretavare5
05	107	+127.66	Cryptolaemus1
06	93	-50.53	JAMESWT_MHT
07	88	+66.04	Casperinous
08	36	+300	wonderhoi39
09	31	-71.82	bry_campbell
10	26	-35	dms1899
11	21	-41.67	viql
12	20	— New entry	ffforward
13	13	-40.91	ULTRAFRAUD
14	13	— New entry	MDMCk10

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

14,455

Malware sites shared by security researchers on URLhaus

-25.9%

decrease on the previous month

16,329

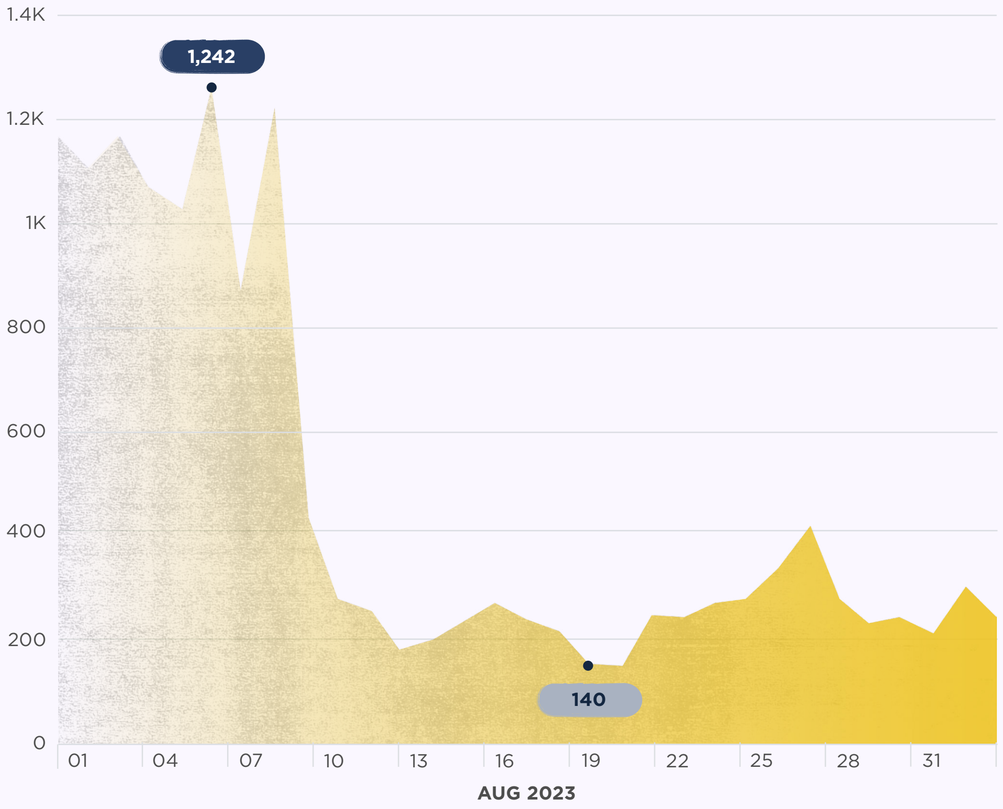
Abuse reports sent out to hosting providers and network owners

92.3%

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.

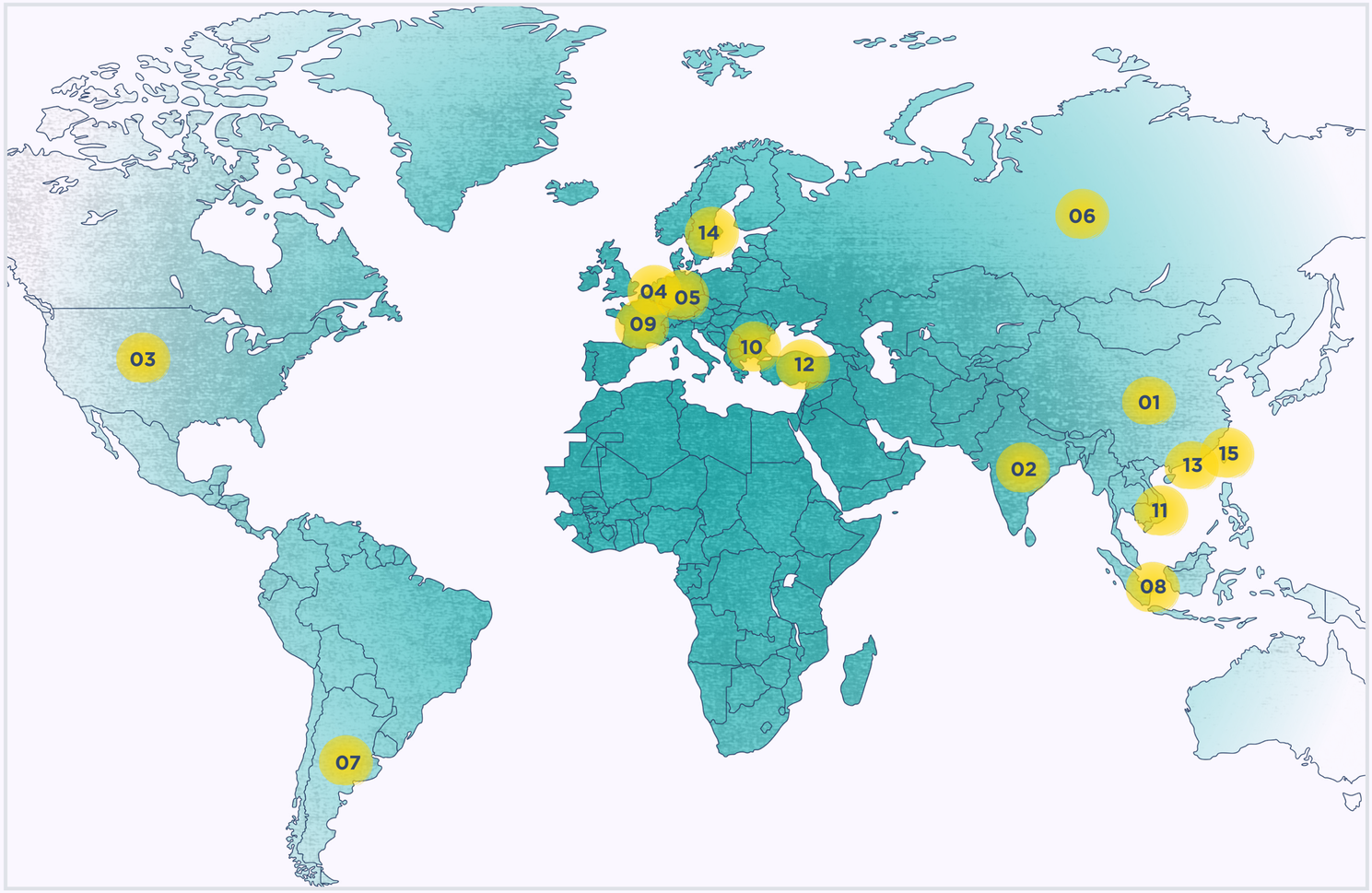


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	4,701	-62.21	geenensp
02	4,409	+773.07	lrz_urlhaus
03	280	+4,566.67	Gootloader2
04	150	-23.47	andretavare5
05	107	+127.66	Cryptolaemus1
06	93	-50.53	JAMESWT_MHT
07	88	+66.04	Casperinous
08	36	+300	wonderhoi39
09	31	-71.82	bry_campbell
10	26	-35	dms1899
11	21	-41.67	viql
12	20	New entry	ffforward
13	13	-40.91	ULTRAFRAUD
13	13	New entry	MDMCk10
14	12	-85.37	JobcenterTycoon

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	5,524	-44.55	China
02	2,700	-36.26	India
03	1,339	-9.59	United States
04	772	+284.08	Netherlands
05	550	+60.35	Germany
06	450	-28.00	Russia
07	425	+13.03	Argentina
08	199	+220.97	Singapore
09	192	+42.22	France
10	188	-53.58	Bulgaria
11	173	-20.64	Vietnam
12	123	+33.70	Turkey
13	122	+48.78	Hong Kong
14	108	New entry	Sweden
15	101	-15.13	Taiwan (PoC)

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	3,112	AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	China
02	2,375	AS9829	BSNL-NIB National Internet Backbone	India
03	1,681	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
04	512	AS211252	AS_DELIS	Netherlands
05	355	AS17816	CHINA169-GZ China Unicom IP network China169 Guangdong	China
06	273	AS14061	DIGITALOCEAN-ASN	United States
07	269	AS13335	CLOUDFLARENET	United States
08	227	AS24547	CMNET-V4HEBEI-AS-AP Hebei Mobile Communication Company	China
09	213	AS52495	Cotel Ltda.	Bolivia
10	197	AS10617	SION S.A	Argentina
11	131	AS47541	VKONTAKTE-SPB-AS vk.com	Russia
12	126	AS17447	NET4-IN Net4India Ltd	India
13	125	AS36352	AS-COLOCROSSING	United States
14	118	AS49581	FERDINANDZINK	Germany
15	112	AS16276	OVH	France

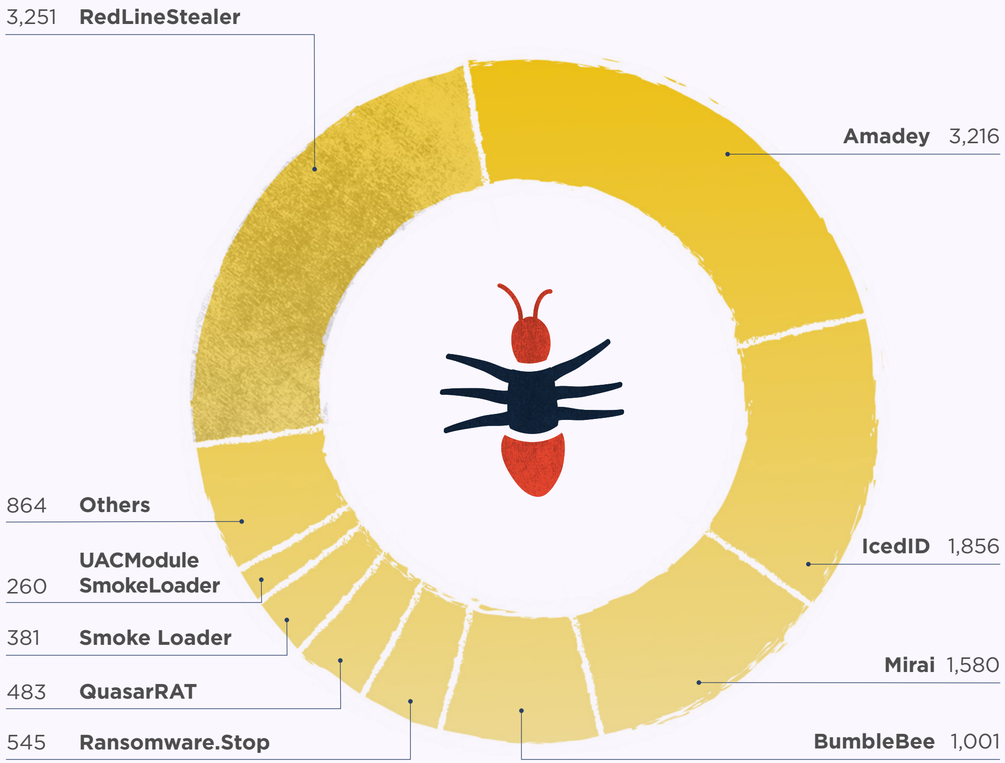
TOP MALWARE HOSTS

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	127	vk.com	VK	Russia
02	85	wtools.io	n/a	null
03	63	cdn.discordapp.com	Discord	United States
04	32	transfer.sh	n/a	null
05	31	pasteio.com	n/a	null
06	18	pastebin.com	Pastebin	United States
07	12	files.catbox.moe	n/a	null
08	8	uploaddeimagens.com.br	n/a	Brazil
08	8	github.com	Github	United States
09	7	drivegoogle.com	Google	United States
10	6	bitbucket.org	Atlassian	Australia

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	# OF SAMPLES
01	Mirai	^ +12.30	1,580
02	CoinMiner	v -3.53	246
03	Amadey	v -13.71	3,216
04	Ransomware.Stop	v -18.90	545
05	BumbleBee	v -21.24	1,001
06	Smoke Loader	v -22.72	381
07	UACModuleSmokeLoader	v -24.20	260
08	AgentTesla	vv -33.50	137
09	IcedID	vv -39.84	1,856
10	RedLineStealer	vv -40.06	3,251
11	QuasarRAT	— New entry	483
11	DarkTortilla	— New entry	162
11	Tofsee	— New entry	119
11	Formbook	— New entry	104
11	Fabookie	— New entry	96

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

9,580

Malware samples shared by security researchers on MalwareBazaar

-23.5%

decrease on the previous month

1,314

Active hunting rules

+1.5%

increase on the previous month

9.93MB

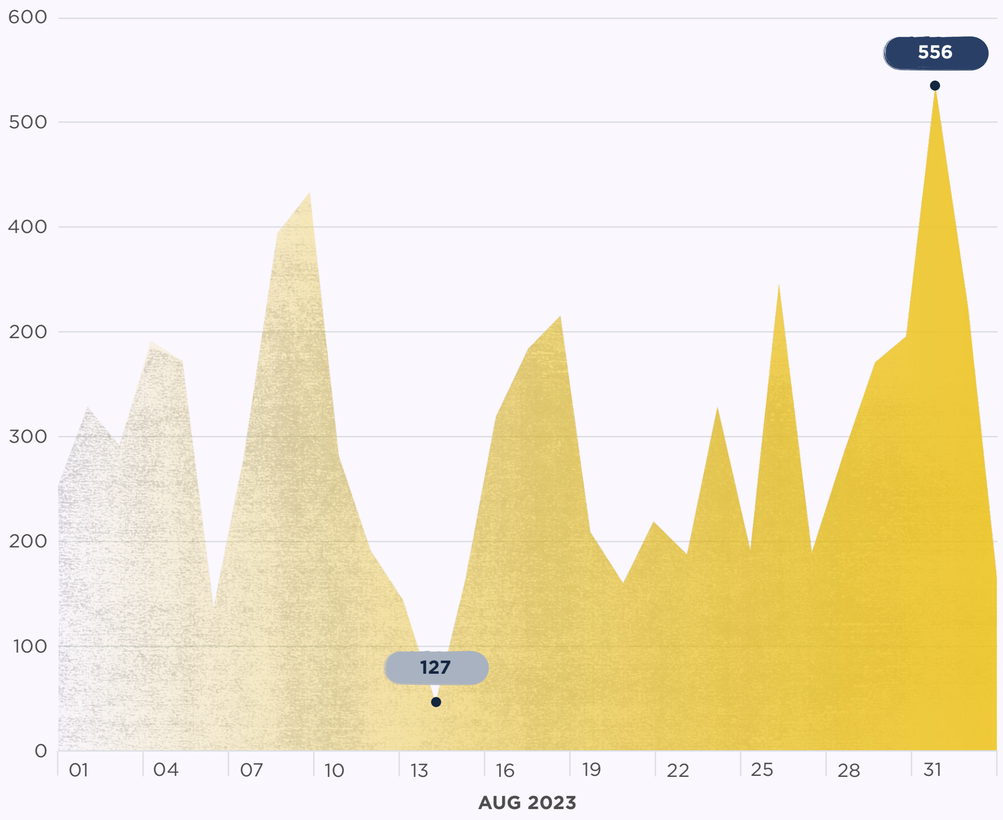
Average size of a malware sample

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.



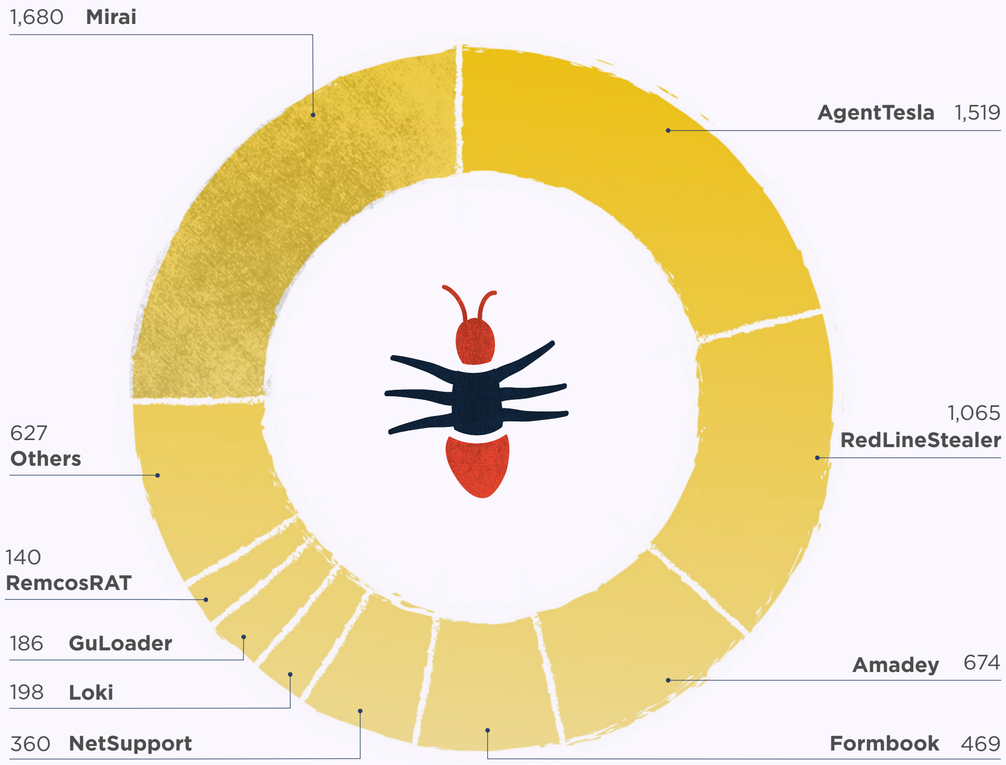
TOP SAMPLE CONTRIBUTORS

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	515	-37.27	@cocaman
02	294	-66.21	@andretavare5
03	292	-17.75	@lowmal3
04	248	-20.51	@adrian__luca
05	189	-63.93	@JAMESWT_MHT
06	135	New entry	@smica83
07	111	-18.38	@malwarelabnet
08	108	New entry	@dancho_danchev
09	91	-15.74	@TeamDreier
10	74	New entry	@rmceoin
11	71	-29.00	@Porcupine
12	62	+129.63	@jstrosch
13	56	+7.69	@ULTRAFRAUD
14	47	New entry	@petikvx
15	26	-16.13	@1ZRR4H

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



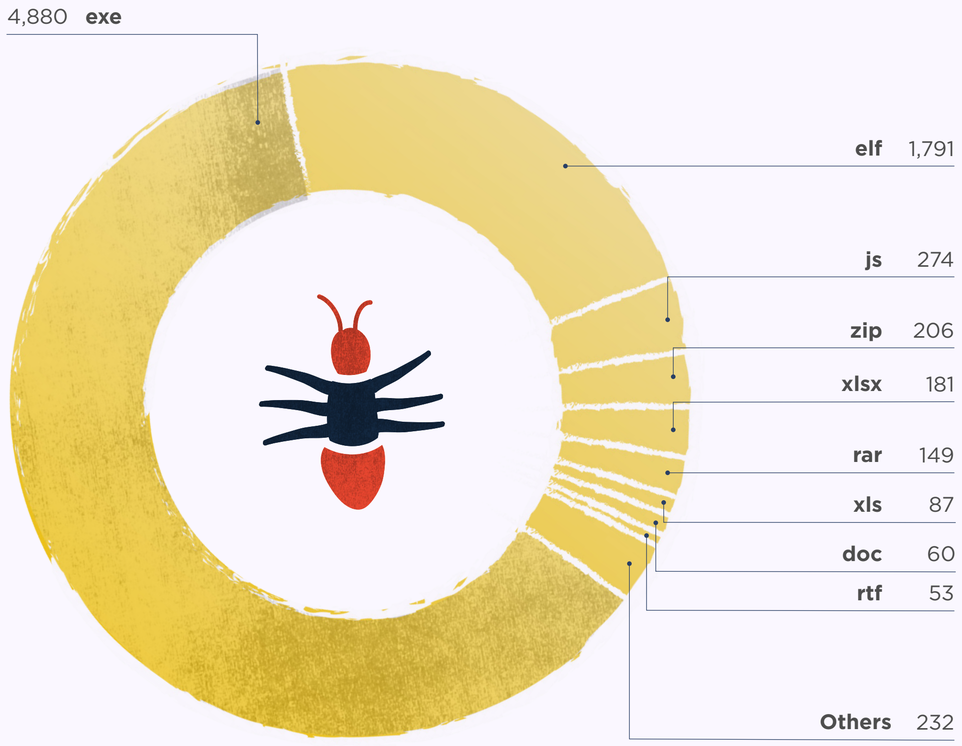
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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

RANK	MALWARE FAMILY	% CHANGE	# OF SAMPLES
01	Mirai	^ +19.15	1,680
02	AgentTesla	^ +3.33	1,519
03	DCRat	^ +3.20	129
04	njrat	v -1.68	117
05	GuLoader	v -12.26	186
06	DarkCloud	v -21.24	89
07	RemcosRAT	v -21.35	140
08	Loki	v -22.35	198
09	Formbook	v -26.60	469
10	Gafgyt	vv -40.13	91
11	SnakeKeylogger	vv -43.27	118
12	Amadey	vv -54.34	674
13	RedLineStealer	vv -57.45	1,065
14	NetSupport	— New entry	360
14	AsyncRAT	— New entry	83

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	1,788	NET	malware-lu
02	1,231	DebuggerCheck__API	n/a
03	1,043	detect_Redline_Stealer	Varp0s
04	861	linux_generic_ipv6_catcher	@_lubiedo
05	838	maldoc_find_kernel32_base _method_1	Didier Stevens
06	814	myMirai	n/a
07	812	NETexecutableMicrosoft	malware-lu
08	605	unixredflags3	Tim Brown @ timb_machine
09	428	PE_Digital_Certificate	albertzsigovits
10	398	MD5_Constants	phoul (@phoul)
11	371	RIPEMD160_Constants	phoul (@phoul)
11	371	SHA1_Constants	phoul (@phoul)
12	361	DebuggerException__SetConsoleCtrl	n/a
13	340	PE_Potentially_Signed_Digital _Certificate	albertzsigovits
14	315	shellcode	nex

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)

8,944

Indicators of compromise (IOCS) shared on ThreatFox

+2.1%

increase on the previous month

2,225

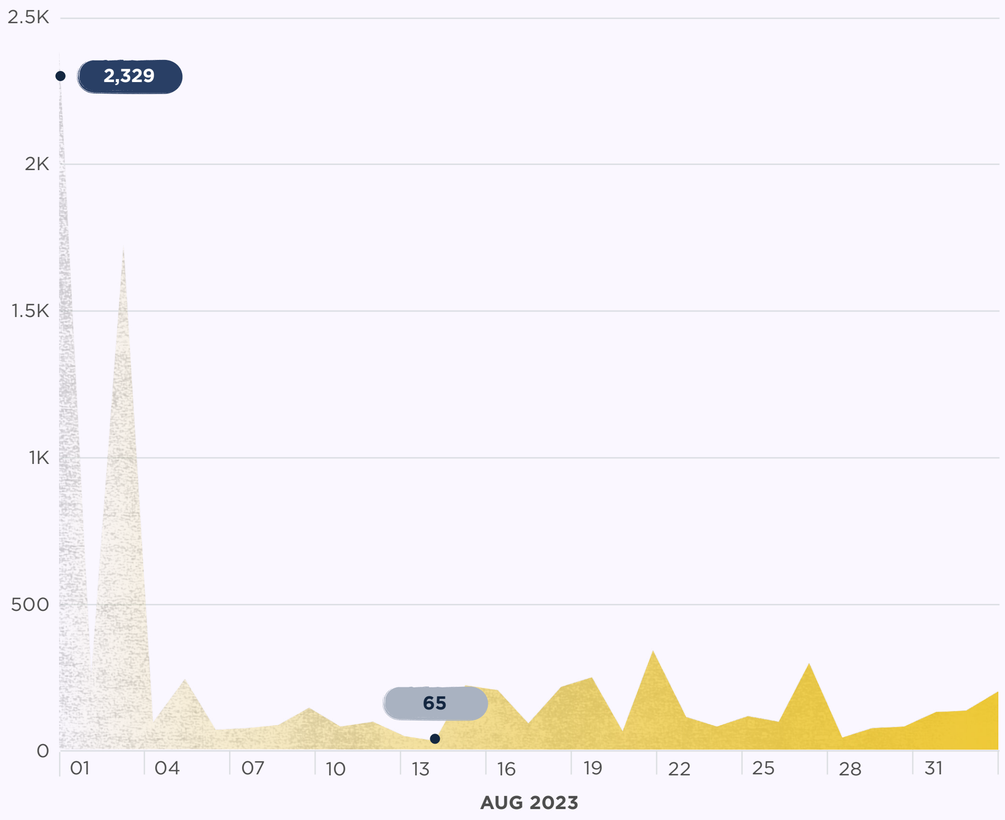
IOCs relating to RedlineStealer

+1,403.4%

increase on the previous month

NUMBER OF IOCs SHARED PER DAY

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



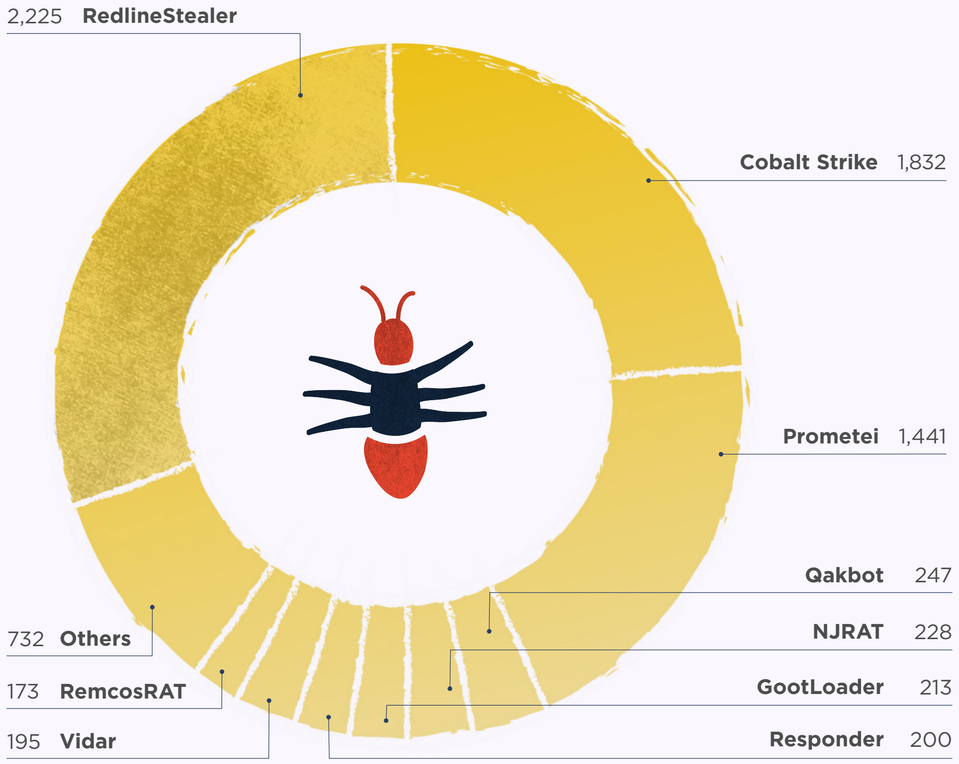
IOC TYPE

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	3,872	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
02	2,784	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
03	1,741	url	botnet_cc	URL that is used for botnet Command&control (C&C)
04	272	url	payload_ delivery	URL that delivers a malware payload
05	119	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
06	106	domain	payload_ delivery	Domain name that delivers a malware payload
07	43	md5_hash	payload	MD5 hash of a malware sample (payload)
08	9	domain	cc_skimming	Domain used for credit card skimming (usually related to Magecart attacks)
08	9	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.



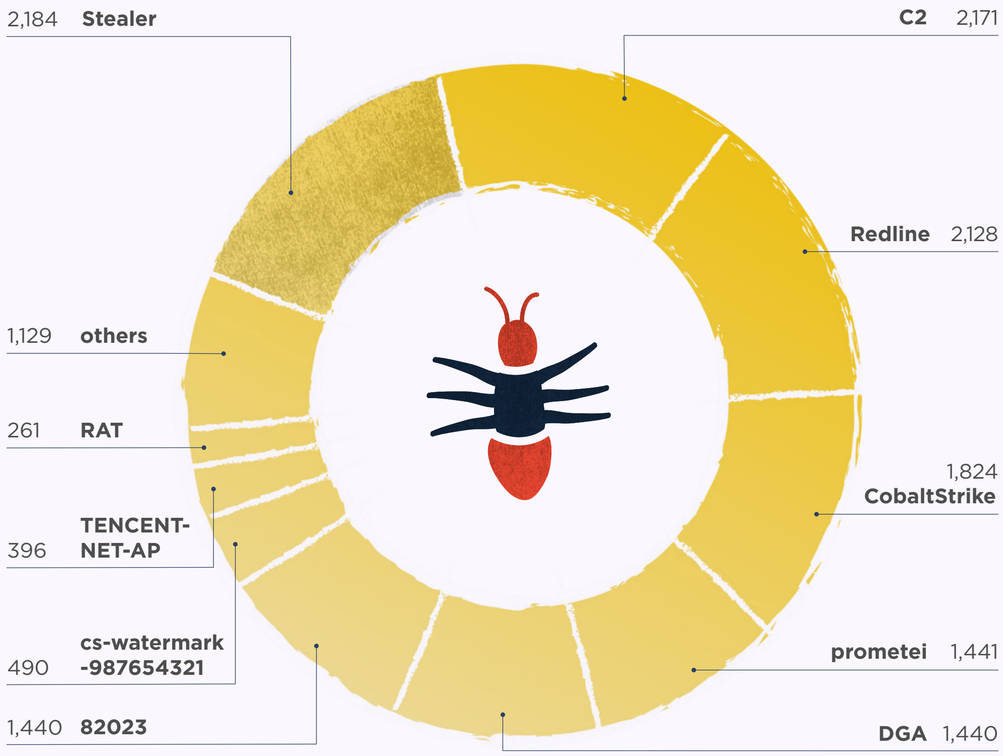
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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

RANK	MALWARE FAMILY	% CHANGE	# OF IOCS
01	RedlineStealer	**+1,403.38**	2,225
02	Vidar	**+105.26**	195
03	RemcosRAT	**+92.22**	173
04	IRATA	**+80**	162
05	NJRAT	**+20**	228
06	IcedID	**+14.38**	167
07	BianLian	**-2.94**	99
08	Responder	**-16.67**	200
09	DCRat	**-20.51**	124
10	Qakbot	**-28.82**	247
11	Cobalt Strike	**-37.35**	1,832
12	Prometei	**New entry**	1,441
12	GootLoader	**New entry**	213
12	CryptBot	**New entry**	101
12	Sliver	**New entry**	79

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	RAT	^ +14.47	261
02	cs-watermark-100000	v -26.30	241
03	cs-watermark-987654321	vv -34.32	490
04	CobaltStrike	vv -37.38	1,824
05	Stealer	— New entry	2,184
05	C2	— New entry	2,171
05	Redline	— New entry	2,128
05	prometei	— New entry	1,441
05	82023	— New entry	1,440
05	DGA	— New entry	1,440
05	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	— New entry	396
05	ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.Ltd.	— New entry	239
05	Njrat	— New entry	228
05	gootloader	— New entry	211
05	gating	— New entry	210

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

2,402,852

File scans conducted on YARAify

1,969,910

Distinct files that had scans performed on them

+7.2%

increase in file scans on the previous month

+16.3%

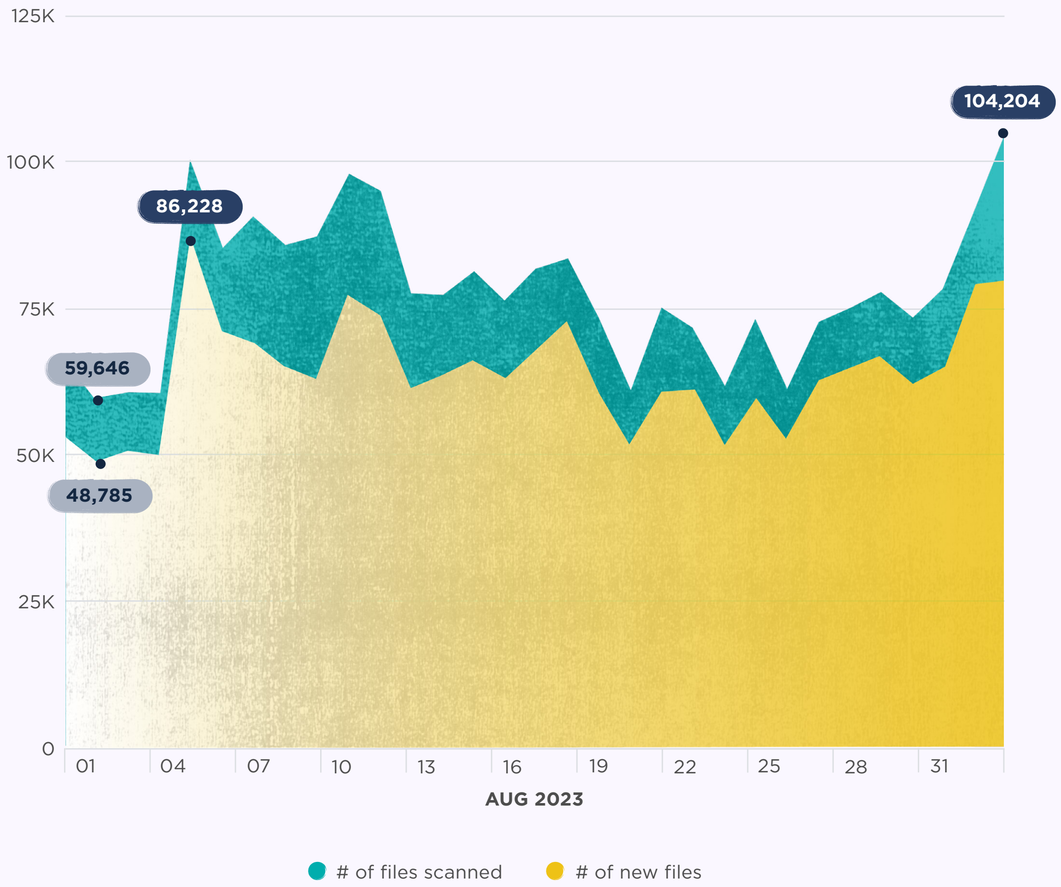
increase in files on the previous month

17,774

YARA rules deployed on YARAify and available for hunting

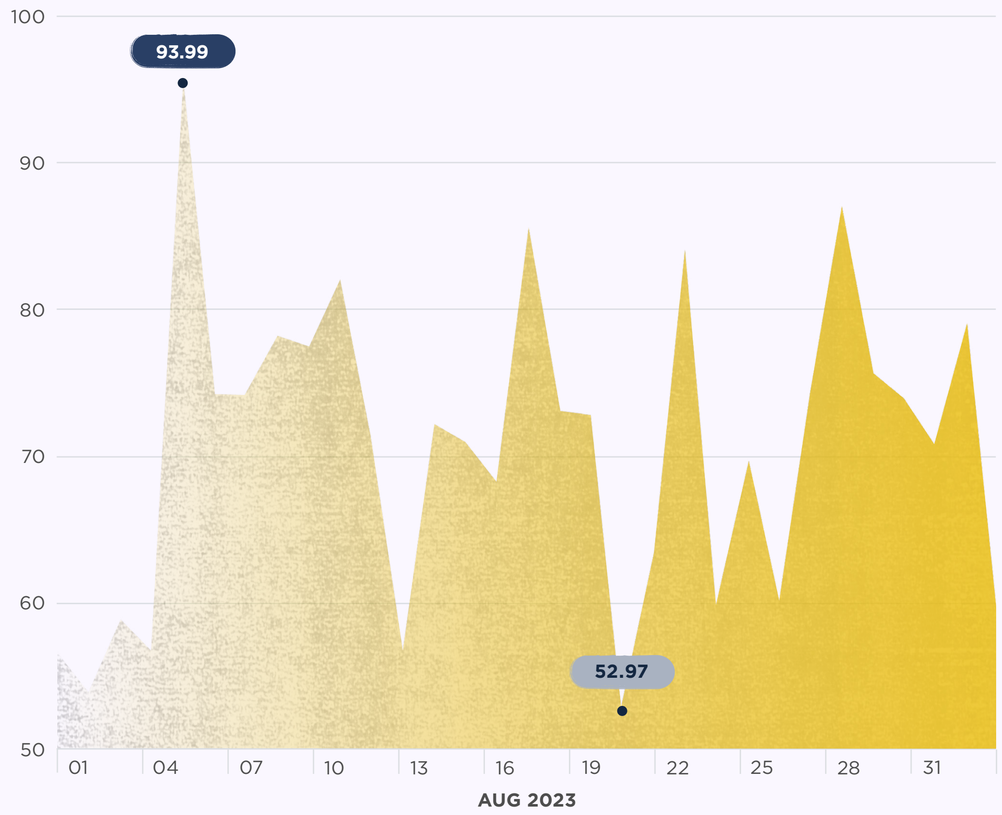
FILES SCANNED PER DAY

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	643,608	— New entry	maldoc_getEIP_method_1	Didier Stevens
02	379,825	— New entry	DebuggerCheck__API	n/a
03	277,546	— New entry	NET	malware-lu
04	229,704	— New entry	UPXV200V290MarkusO-berhumerLaszloMolnar-JohnReiser	malware-lu
05	198,712	— New entry	UPXv20MarkusLaszloReiser	malware-lu
06	197,853	— New entry	maldoc_find_kernel32_base_method_1	Didier Stevens
07	126,649	— New entry	RIPEMD160_Constants	phoul (@phoul)
07	126,649	— New entry	SHA1_Constants	phoul (@phoul)
08	110,353	— New entry	DebuggerException__SetConsoleCtrl	n/a
09	108,616	— New entry	MD5_Constants	phoul (@phoul)
10	78,649	— New entry	Borland	malware-lu
11	77,295	— New entry	Check_OutputDebugStrin-gA_iat	n/a
12	77,279	— New entry	SEH__vectored	n/a
13	73,974	— New entry	ThreadControl__Context	n/a
14	67,664	— New entry	DebuggerCheck__QueryInfo	n/a

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	358,701	⌃⌃ +501.78	PUA.Win.Packer.Lccwin-2
02	241,514	⌃⌃ +507.60	Win.Trojan.Obfus-38
03	154,678	⌃⌃ +549.99	Win.Trojan.Qukart-6874817-0
04	123,340	⌄ -17.69	Win.Malware.Dqqw-9951425-0
05	122,582	⌄ -17.89	Win.Malware.Zusy-6804618-0
06	122,576	⌄ -17.90	Win.Trojan.QQPass-5710308-0
07	120,461	⌃⌃ +451.41	Win.Trojan.Crypted-29
08	120,454	⌃⌃ +444.11	Win.Trojan.Crypted-30
09	103,732	— New entry	Win.Trojan.Padodor-9877164-0
10	80,072	— New entry	Win.Malware.Qukart-6838239-0
11	53,289	— New entry	Win.Trojan.Crypted-28
12	49,483	— New entry	PUA.Win.Packer.Pequake-4
13	49,209	— New entry	Win.Trojan.Crypted-31
14	41,610	⌄⌄ -75.97	Win.Packed.Lazy-10005437-0
15	40,832	— New entry	Win.Trojan.Berbew-9845290-1

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN OCTOBER

Remember, sharing is caring.