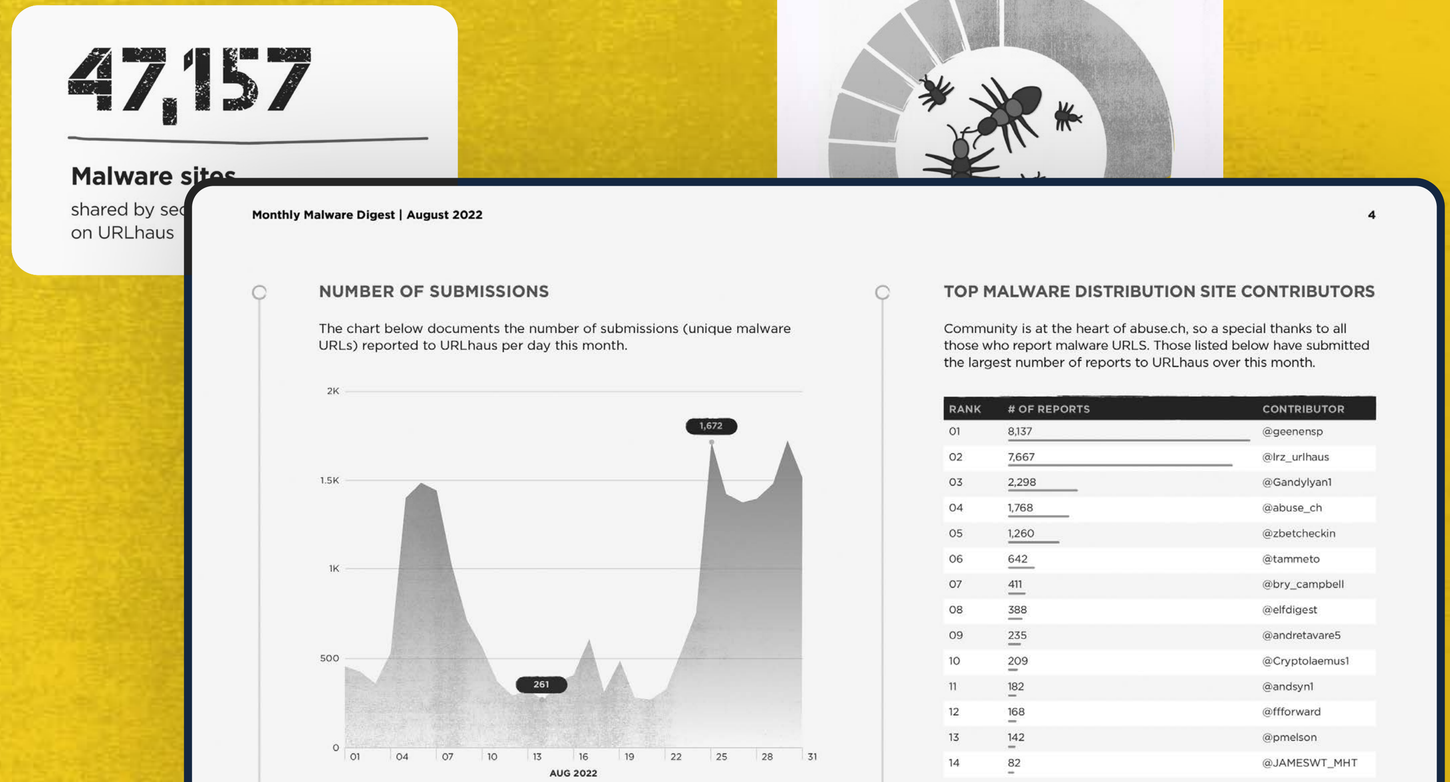
AUGUST 2022

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

23,950

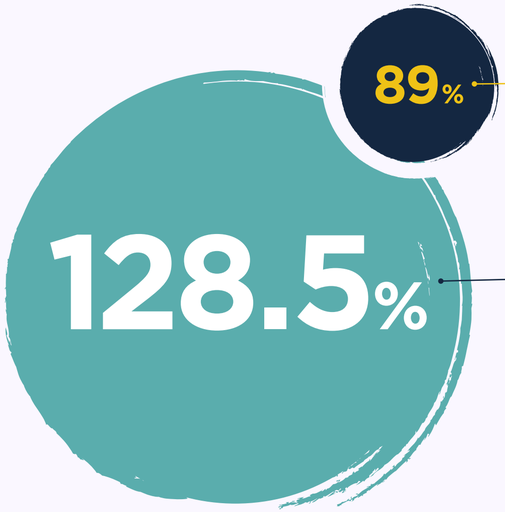
Malware sites

shared by security researchers on URLhaus

29,946

Abuse reports

sent out to hosting providers and network owners

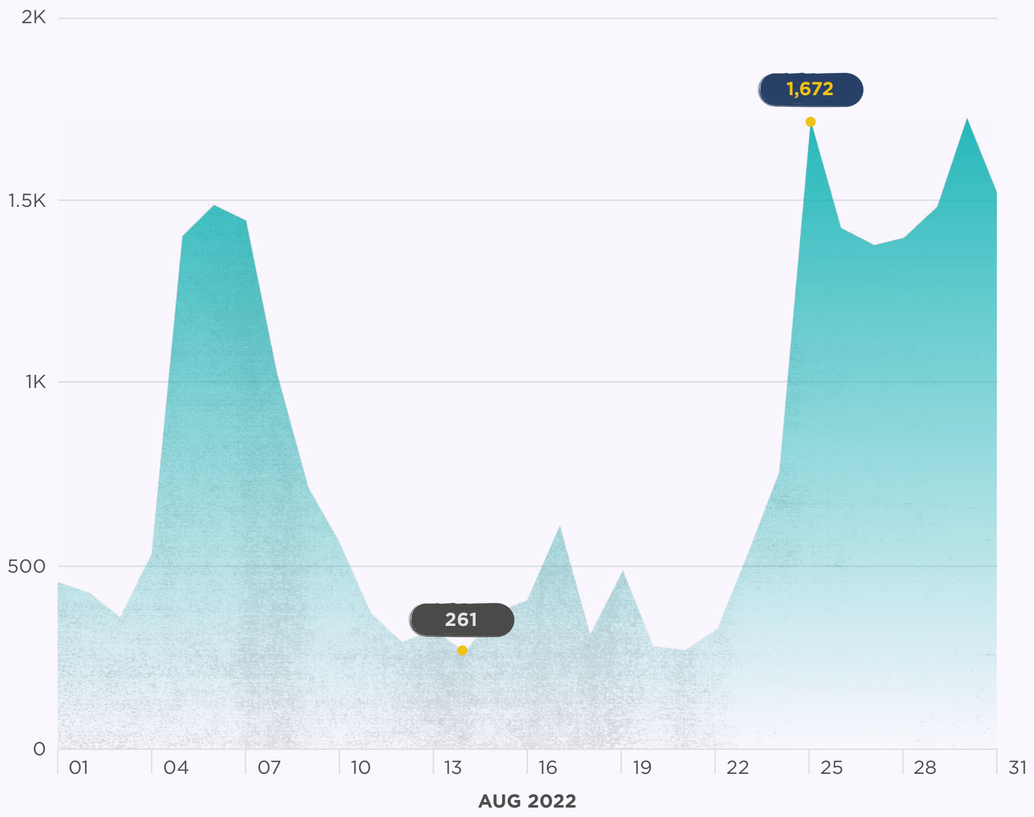


of abuse reports have been acted upon

increase in malware sites shared compared with the previous month

NUMBER OF SUBMISSIONS

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

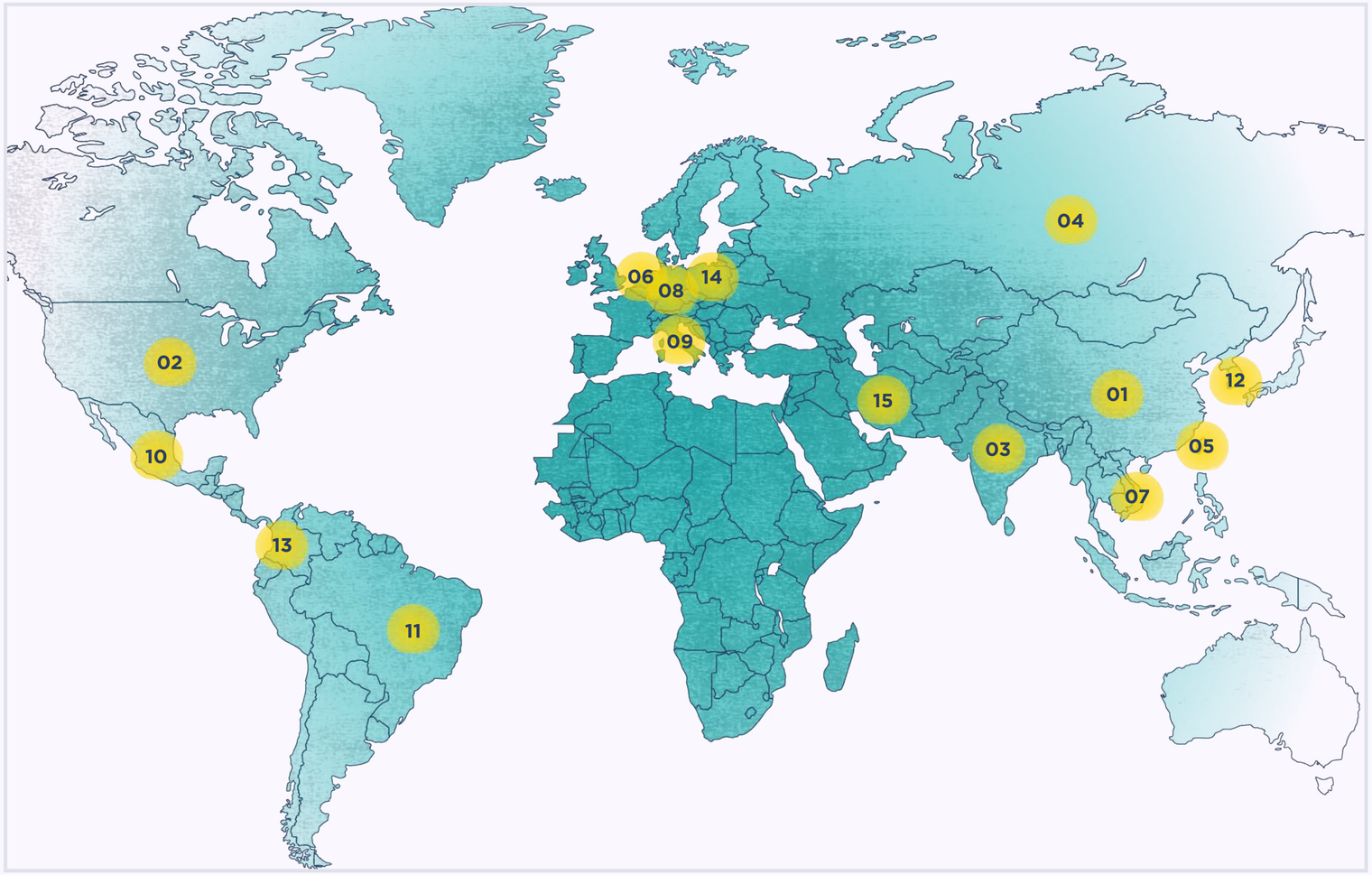


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	8,137	@geenensp
02	7,667	@lrz_urlhaus
03	2,298	@Gandylyan1
04	1,768	@abuse_ch
05	1,260	@zbetcheckin
06	642	@tammeto
07	411	@bry_campbell
08	388	@elfdigest
09	235	@andretavare5
10	209	@Cryptolaemus1
11	182	@andsyn1
12	168	@ffforward
13	142	@pmelson
14	82	@JAMESWT_MHT
15	71	@AndreGironda

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	COUNTRY
01	3,965	China
02	2,669	United States
03	1,429	India
04	464	Russia
05	363	Taiwan
06	296	Netherlands
07	287	Vietnam
08	171	Germany
09	150	Italy
10	130	Mexico
11	113	Brazil
12	107	Korea
13	81	Columbia
14	68	Poland
15	66	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	2,446	AS4134	No.31,Jin-rong Street	China
02	1,494	AS211252	Delis LLC	United States
03	1,443	AS4837	China Unicom - China169 Backbone	China
04	1,310	AS9829	National Internet Backbone	India
05	384	AS15169	Google LLC	United States
06	322	AS3462	Data Communication Business Group	Taiwan
07	174	AS36352	ColoCrossing	United States
08	172	AS14061	DigitalOcean, LLC	United States
09	154	AS13335	Cloudflare, Inc.	United States
10	120	AS8151	Uninet S.A. de C.V.	Mexico
11	109	AS7552	Viettel Group	Vietnam
12	104	AS52000	MIRholding B.V.	Netherlands
13	91	AS4766	Korea Telecom	Korea
14	88	AS53667	FranTech Solutions	United States
15	86	AS47541	VKontakte Ltd	Russia

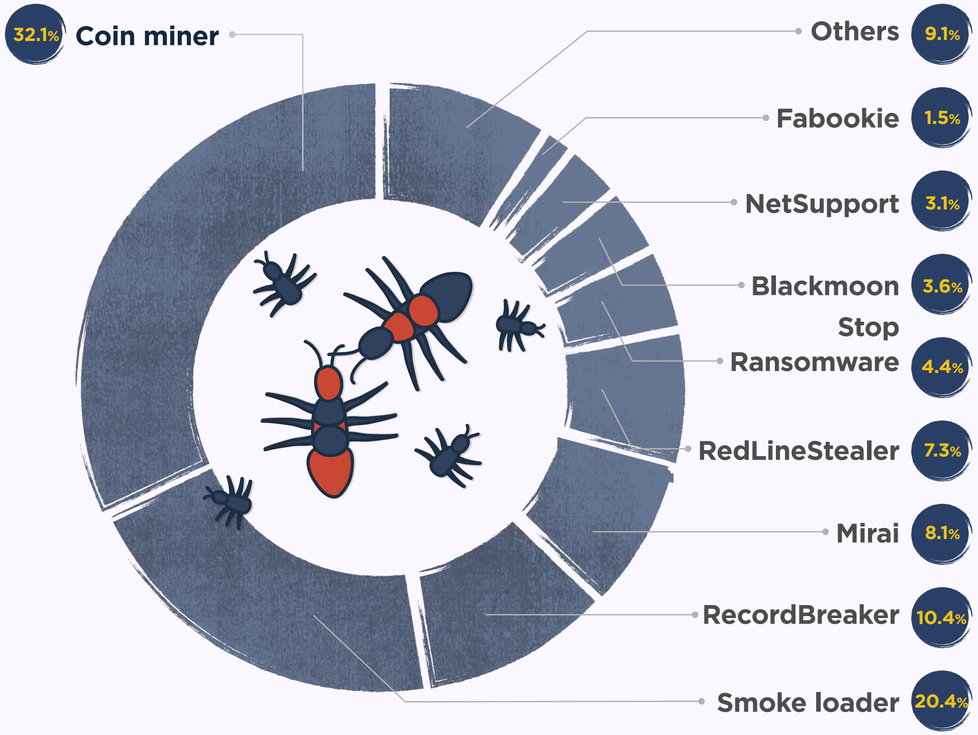
TOP MALWARE HOSTS

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	654	109.206.241.81	Serverion B.V.	Netherlands
02	525	drive.google.com	Google	United States
03	420	37.139.129.142	Serverion B.V.	Netherlands
04	201	1drv.ms	Microsoft	United States
05	121	cdn.discordapp.com	Discord	United States
06	90	storage.googleapis.com	Google	United States
07	86	vk.com	VK	Russia
08	69	163.123.142.131	Serverion B.V.	Netherlands
09	63	pasteio.com	PasteIO	n/a
10	50	pastebin.com	Pastebin	n/a
11	45	141.98.6.211	Serverion B.V.	Netherlands
12	45	50.115.170.112	Virpus	United States
13	40	208.67.107.247	Serverion B.V.	Netherlands
14	38	192.3.108.11	ColoCrossing	United States
15	33	107.182.129.240	Serverion B.V.	Netherlands

TOP MALWARE FAMILIES ASSOCIATED WITH MALWARE SITES

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



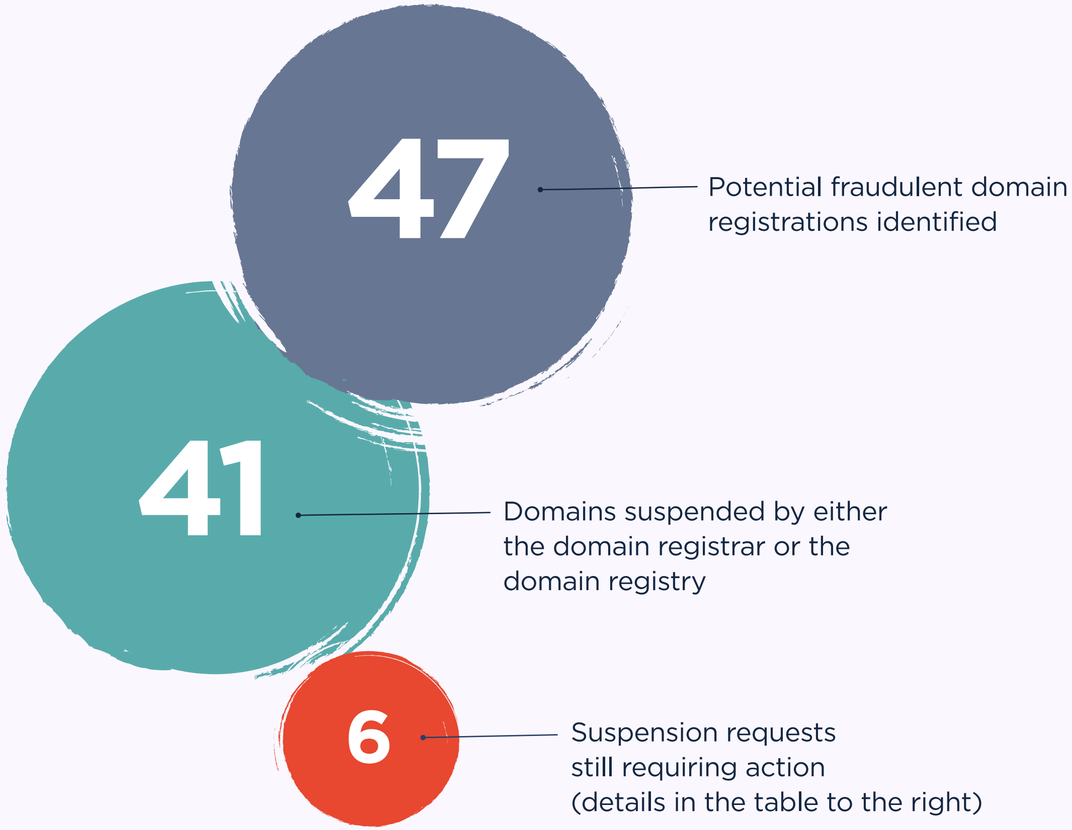
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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

RANK	% CHANGE	MALWARE FAMILY	# OF DISTINCT PAYLOADS
01	1,640%	RecordBreaker	1,340
02	888%	DanaBot	89
03	493%	Gafgyt	89
04	205%	AsyncRAT	113
05	188%	Stop Ransomware	562
06	167%	Fabookie	187
07	166%	RemcosRAT	136
08	100%	Blackmoon	466
09	100%	NetSupport	404
10	84%	Mirai	1,049
11	68%	Smoke Loader	2,624
12	37%	ArkeiStealer	131
13	11%	CoinMiner	4,135
14	10%	AgentTesla	134
15	-7%	SnakeKeylogger	76

FRAUDULENT DOMAIN REGISTRATIONS

URLhaus determines if a domain name used for malware distribution has been set up by threat actors with the sole intention of spreading malware. If this is the case, an automated abuse report is sent to the sponsoring domain registry (top-level domain operator) and domain registrar, requesting action against the domain name, e.g., suspending it.



OUTSTANDING SUSPENSION REQUESTS

The following table outlines the details of the domains that are still waiting for suspension requests to be actioned.

TIMESTAMP	DOMAIN	REGISTRAR	REGISTRY
Aug 30, 2022, 5:55:02 AM	connect2me.hopto.org	No-IP	n/a
Aug 29, 2022, 1:26:02 PM	cthulhu-world.app	Tucows	n/a
Aug 21, 2022, 6:30:01 AM	the-end.ga	Freenom	n/a
Aug 10, 2022, 9:40:02 AM	safetygear.pk	n/a	PKNIC
Aug 10, 2022, 9:40:02 AM	scientific.pk	n/a	PKNIC
Aug 4, 2022, 6:10:02 AM	marnersstyler.ug	n/a	Uganda Online

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

16,803

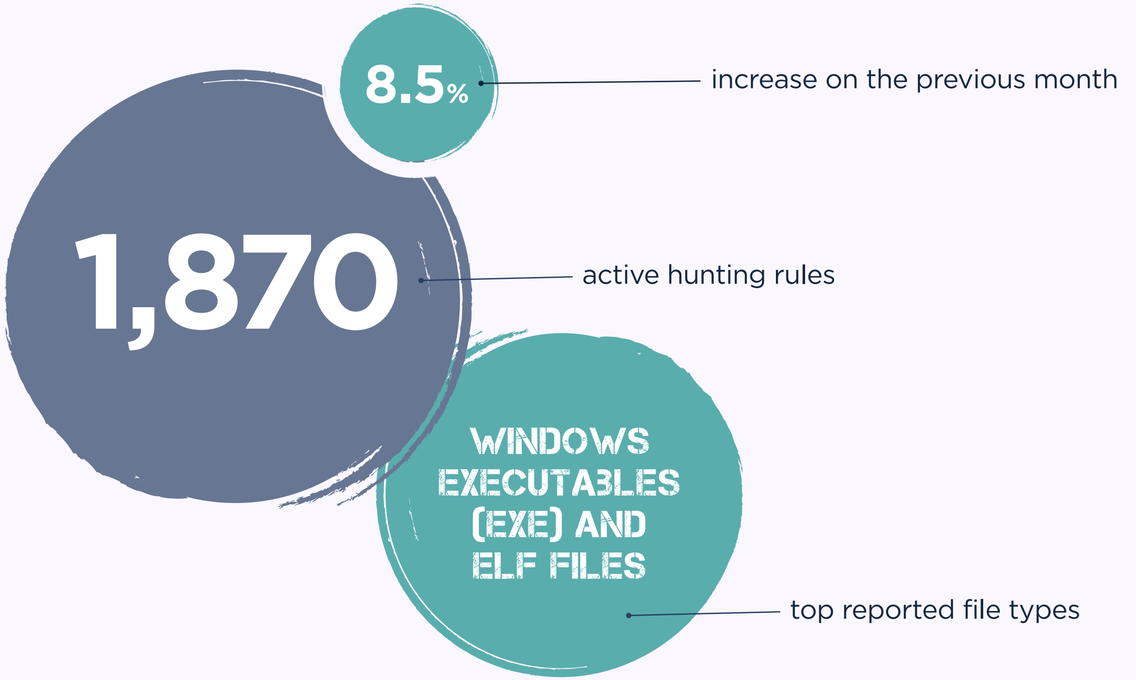
Malware samples

shared by security researchers on MalwareBazaar

663KB

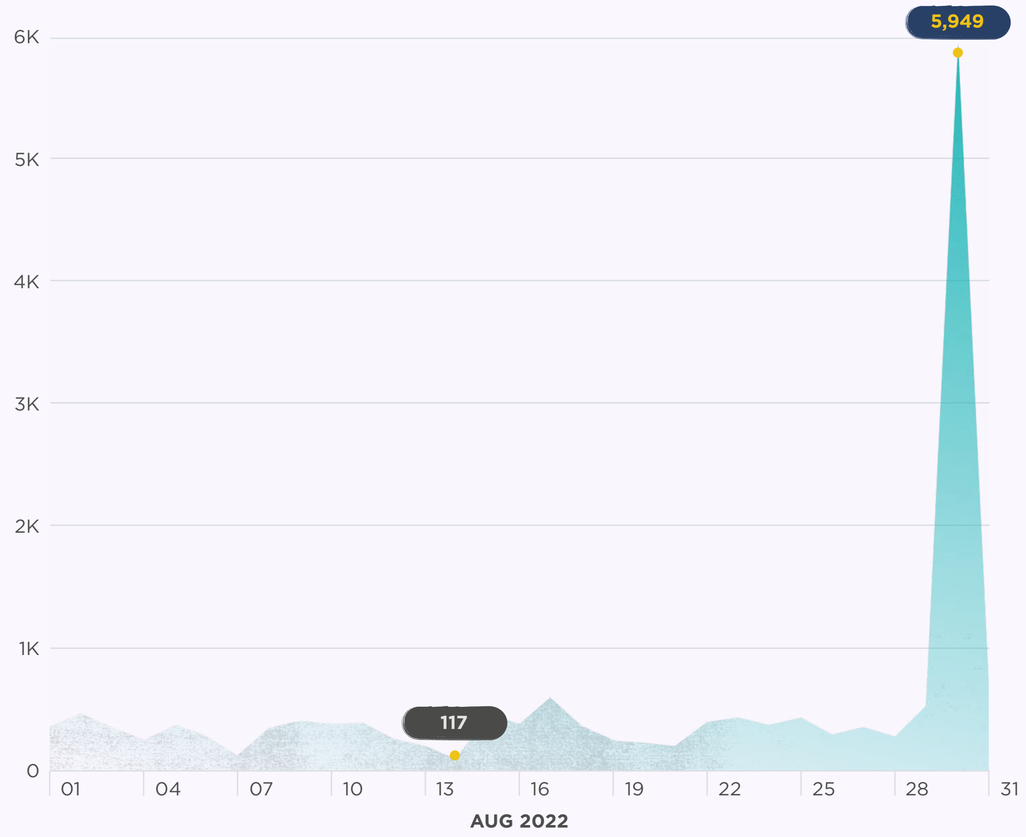
Average size

of a malware sample



MALWARE SAMPLES

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



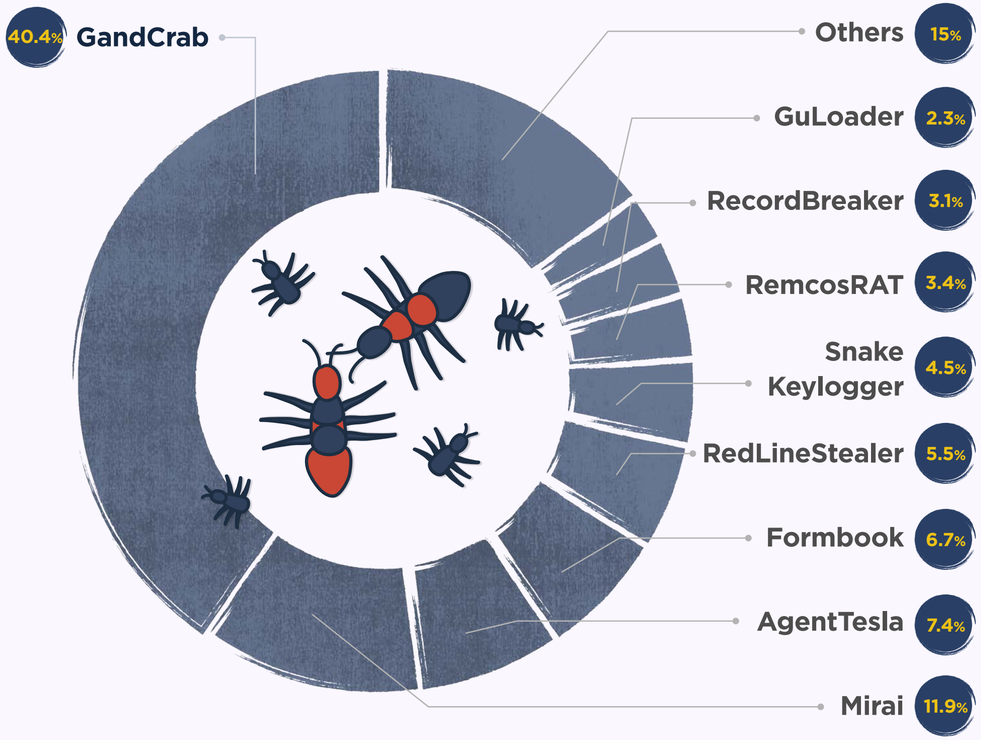
TOP SAMPLE CONTRIBUTORS

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	CONTRIBUTOR
01	5,660	@OSimao
02	1,885	@zbetcheckin
03	1,105	@SecuriteInfoCom
04	492	@GovCERT_CH
05	441	@cocaman
06	376	@JAMESWT_MHT
07	367	@elfdigest
08	362	@andretavare5
09	306	@lowmal3
10	260	@TeamDreier
11	201	@0xToxin
12	174	@adrian__luca
13	158	@James_inthe_box
14	128	@malwarelabnet
15	109	@pmelson

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



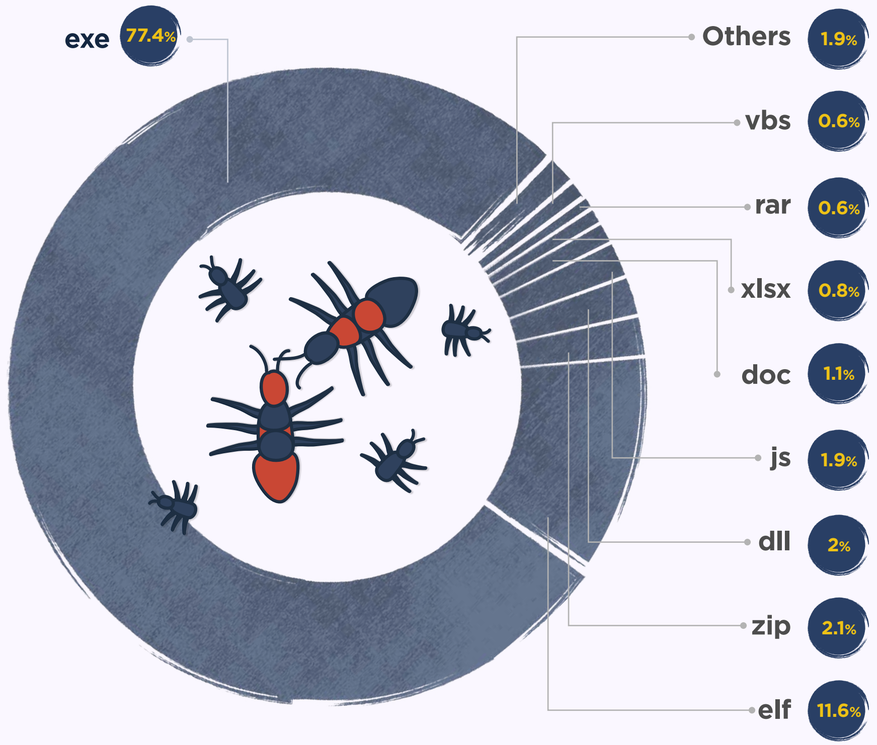
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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

RANK	% CHANGE	MALWARE FAMILY	# OF SAMPLES
01	129%	RemcosRAT	458
02	100%	GandCrab	5,483
03	100%	RecordBreaker	417
04	100%	Stop Ransomware	161
05	100%	NetSupport	147
06	42%	DCRat	158
07	29%	AsyncRAT	196
08	19%	IcedID	238
09	15%	SnakeKeylogger	604
10	14%	Formbook	904
11	11%	ArkeiStealer	126
12	9%	Smoke Loader	240
13	9%	NanoCore	180
14	-1%	AgentTesla	1007
15	-1%	AveMariaRAT	186

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	5,474	win_gandcrab_auto	Felix Bilstein
02	5,418	SUSP_RANSOMWARE_ Indicator_Jul20	Florian Roth
03	5,418	SUSP_RANSOMWARE_I ndicator_Jul20_RID31A2	Florian Roth
04	5,418	Gandcrab	kevoreilly
05	3,452	ReflectiveLoader	n/a
06	3,452	INDICATOR_SUSPICIOUS_ ReflectiveLoader	ditekshen
07	1,611	Win32_Ransomware_GandCrab	ReversingLabs
08	998	linux_generic_ipv6_catcher	@_lubiedo
09	977	myMirai	n/a
10	810	unixredflags3	@timb_machine
11	671	cobalt_strike_tmp01925d3f	The DFIR Report
12	457	MALWARE_Win_RedLine	ditekshen
13	366	setsockopt	@timb_machine
14	356	HeavensGate	kevoreilly
15	329	win_smokeloader_a2	pnx

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.

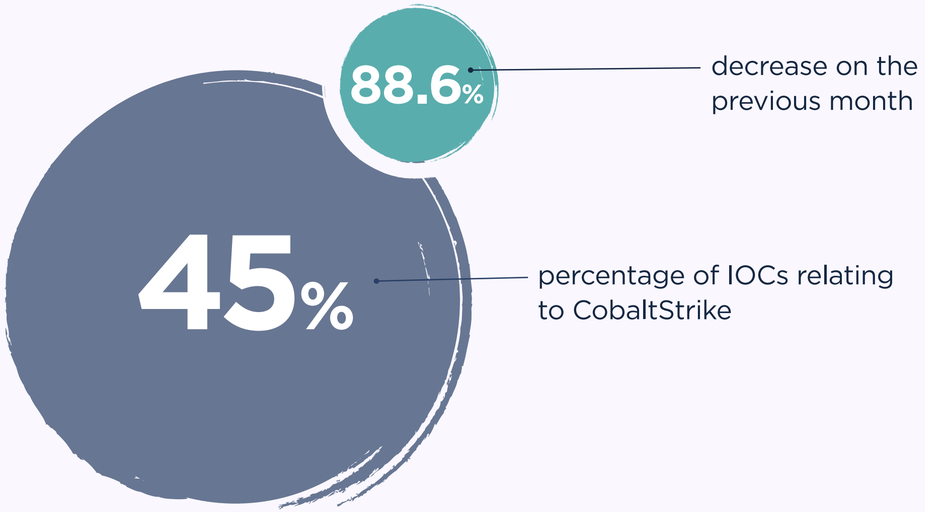
Explore ThreatFox

INDICATERS OF COMPROMISE (IOCs)

6,220

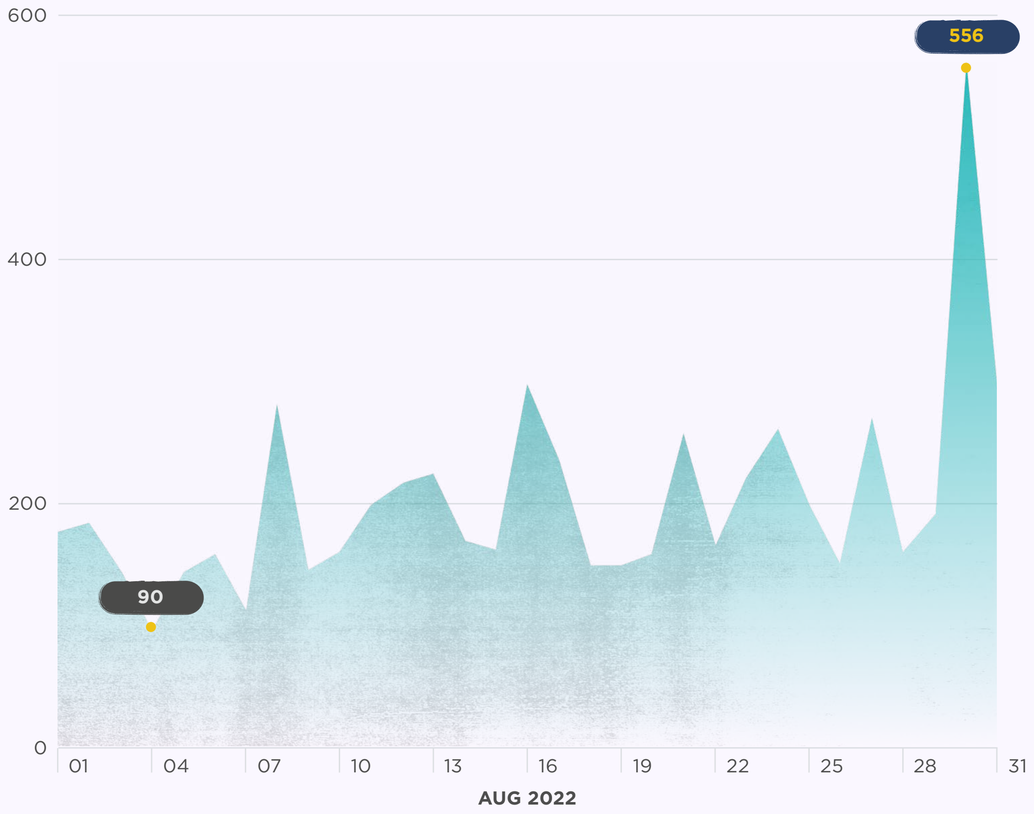
Indicators of compromise (IOCs)

shared on ThreatFox



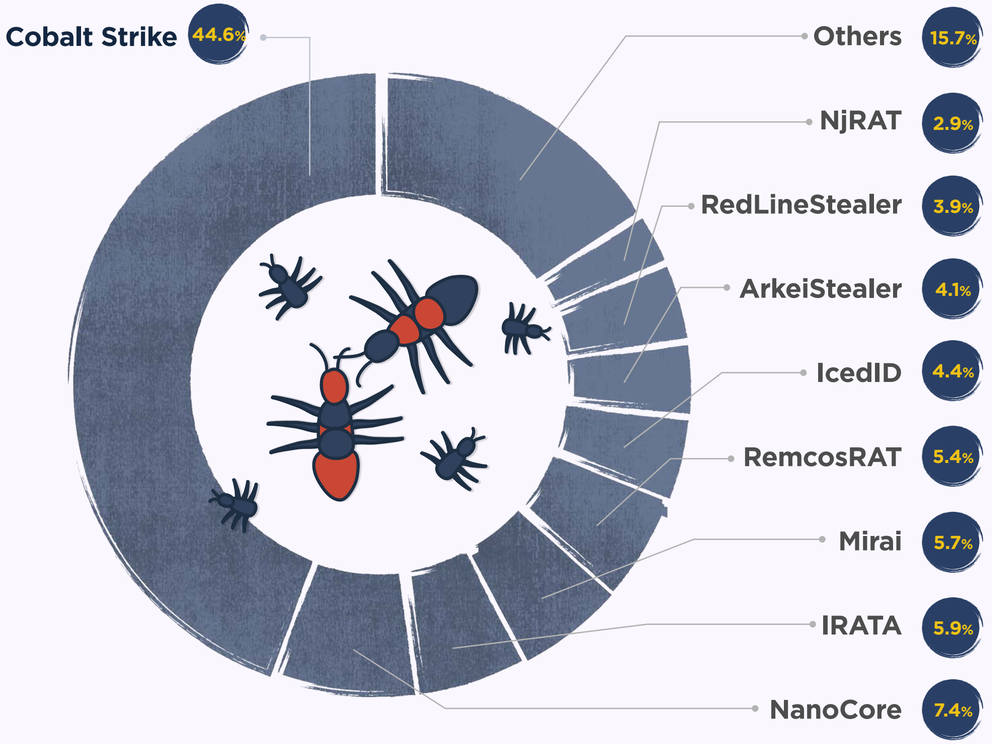
NUMBER OF IOCs SHARED PER DAY

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



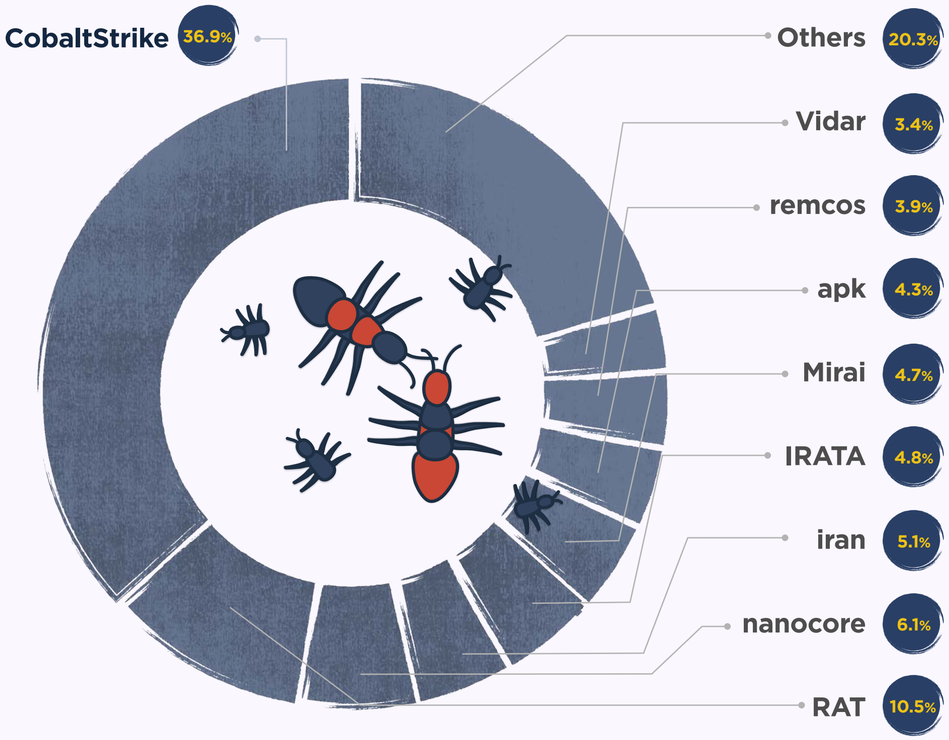
TOP MALWARE FAMILIES

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



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.



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	2,281	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
02	2,213	url	botnet_cc	URL that is used for botnet Command&control (C&C)
03	647	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
04	593	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
05	206	md5_hash	payload	MD5 hash of a malware sample (payload)
06	162	url	payload_ delivery	URL that delivers a malware payload
07	94	domain	payload_ delivery	Domain name that delivers a malware payload
08	19	ip:port	payload_ delivery	ip:port combination that delivery a malware payload
09	5	domain	cc_skimming	Domain used for credit card skimming (usually related to Magecart attacks)

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

2,340,781

File scans

conducted on YARAify

1,989,678

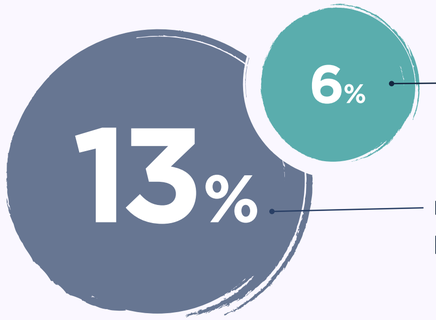
Distinct files

that had scans performed on them

4,262

YARA rules

deployed on YARAify and available for hunting

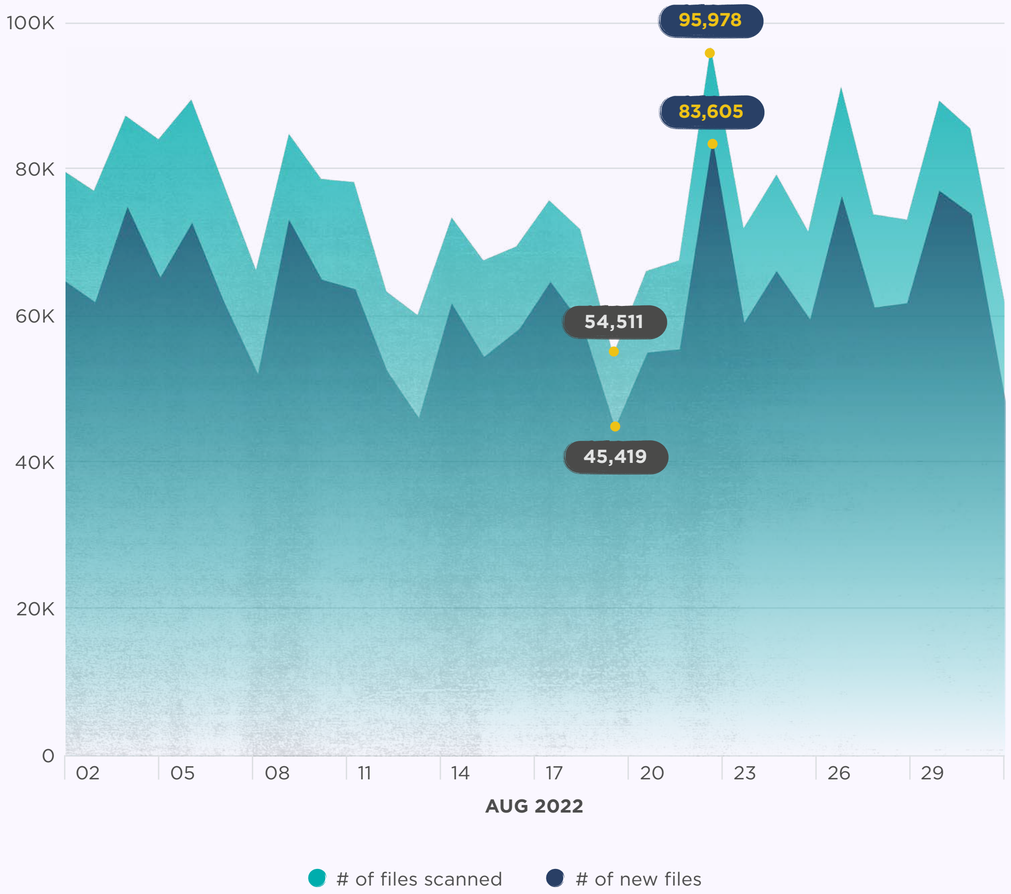


increase in distinct files on the previous month

reduction in file scans on the previous month

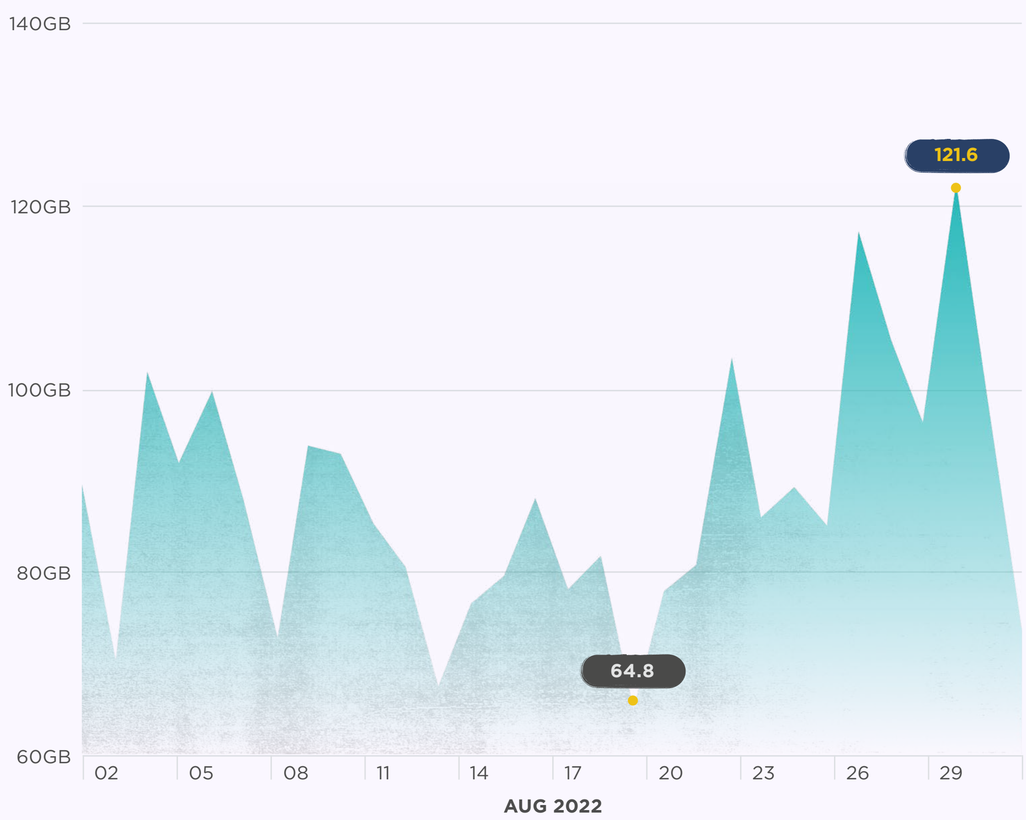
FILES SCANNED PER DAY

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 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	61,588	command_and_control	CD_R0M_
02	28,162	win_sality_auto	Felix Bilstein
03	24,462	malware_shellcode_hash	JPCERT/CC
04	23,122	MALWARE_Win_RedLine	ditekSHen
05	22,592	MALWARE_Win_BlackMoon	ditekSHen
06	20,499	cobalt_strike_tmp01925d3f	The DFIR Report
07	19,746	INDICATOR_EXE_ Packed_MPress	ditekSHen
08	18,902	AutoIT_Compiled	@bartblaze
09	16,637	reverse_http	CD_R0M_
10	15,254	win_vobfus_auto	Felix Bilstein
11	14,794	SUSP_XORed_URL_in_EXE	Florian Roth
12	14,794	SUSP_XORed_URL_in_EXE_ RID2E46	Florian Roth
13	14,427	win_xfilesstealer_auto	Felix Bilstein
14	13,729	INDICATOR_EXE_Packed_ SmartAssembly	ditekSHen
15	12,971	INDICATOR_SUSPICIOUS_ EXE_NoneWindowsUA	ditekSHen

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	146,780	PUA.Win.Packer.Upx-4
02	33,964	PUA.Win.Packer.Pequake-4
03	28,190	PUA.Win.Packer.AcprotectUltraprotect-1
04	25,104	PUA.Win.Packer.Lccwin-2
05	22,422	Win.Malware.Dqqw-9951425-0
06	22,383	Win.Trojan.QQPass-5710308-0
07	22,382	Win.Malware.Zusy-6804618-0
08	21,316	Win.Malware.Nevereg-9916351-0
09	21,141	Win.Dropper.Tiggre-9845940-0
10	20,893	Win.Malware.Generickdz-9938530-0
11	20,256	Win.Trojan.Qukart-6874817-0
12	19,778	Win.Trojan.Cosmu-1058
13	18,787	PUA.Win.Packer.Pseudosigner-36
14	16,100	Multios.Coinminer.Miner-6781728-2
15	15,754	PUA.Win.Packer.Asprotect-3

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN OCTOBER

Remember, sharing is caring.