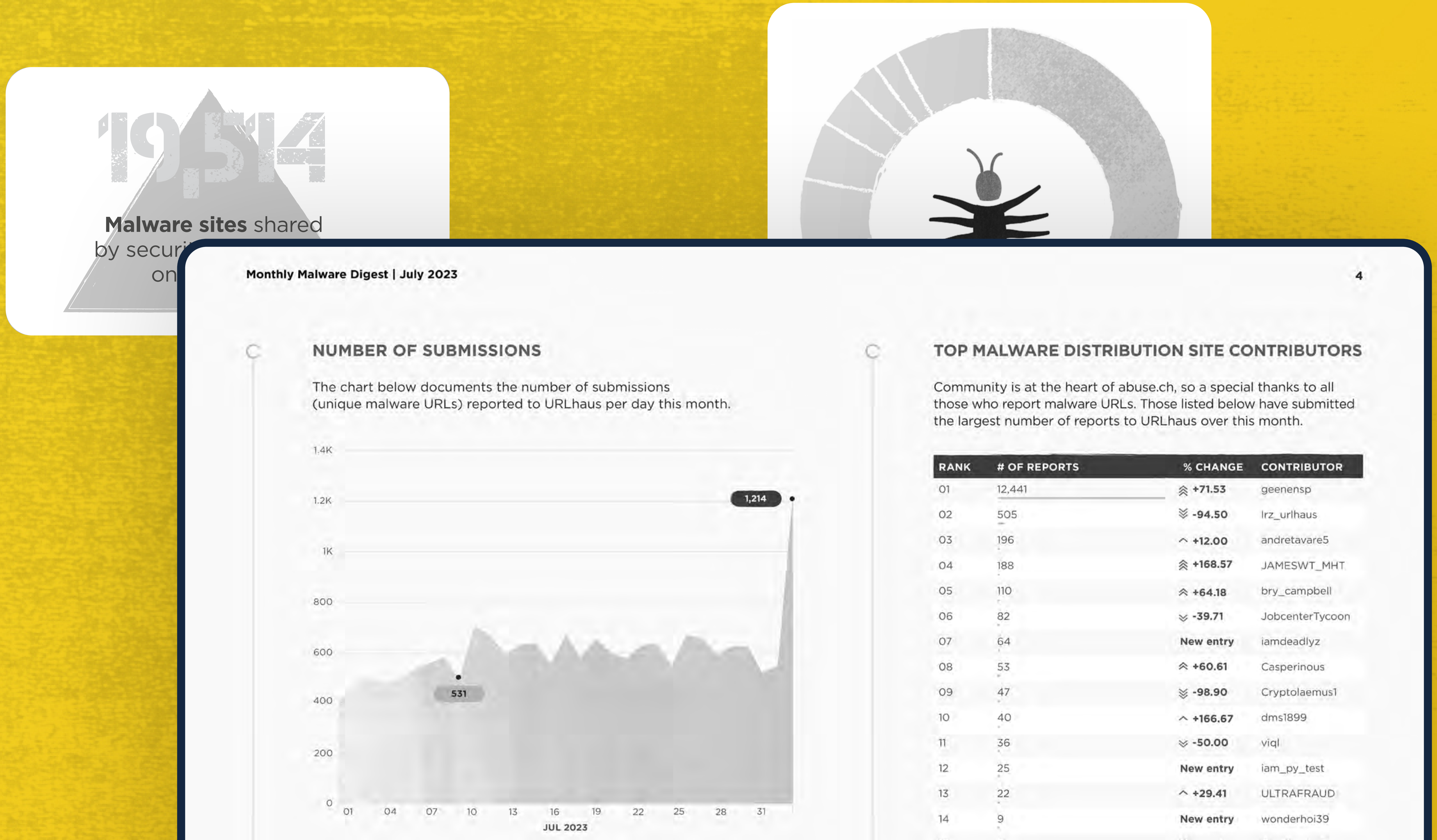
JULY 2023

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.



19,514

Malware sites shared by securi

on

Monthly Malware Digest | July 2023

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	12,441	+71.53	geenensp
02	505	-94.50	lrz_urlhaus
03	196	+12.00	andretavare5
04	188	+168.57	JAMESWT_MHT
05	110	+64.18	bry_campbell
06	82	-39.71	JobcenterTycoon
07	64	New entry	iamdeadlyz
08	53	+60.61	Casperinous
09	47	-98.90	Cryptolaemus1
10	40	+166.67	dms1899
11	36	-50.00	viql
12	25	New entry	iam_py_test
13	22	+29.41	ULTRAFRAUD
14	9	New entry	wonderhoi39

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.

Due to various issues related to Twitter API authentication, inbound data contributions were disrupted in May, resulting in no three months comparison figures.

Our thanks go out to all abuse.ch users and contributors for your continued support and patience.

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
https://urlhaus.abuse.ch

MalwareBazaar
https://bazaar.abuse.ch

ThreatFox
https://threatfox.abuse.ch

YARAify
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
https://urlhaus.abuse.ch/api/

MalwareBazaar
https://bazaar.abuse.ch/api/

ThreatFox
https://threatfox.abuse.ch/api/

YARAify
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

19,514

Malware sites shared by security researchers on URLhaus

-25.8%

Decrease on the previous month

23,167

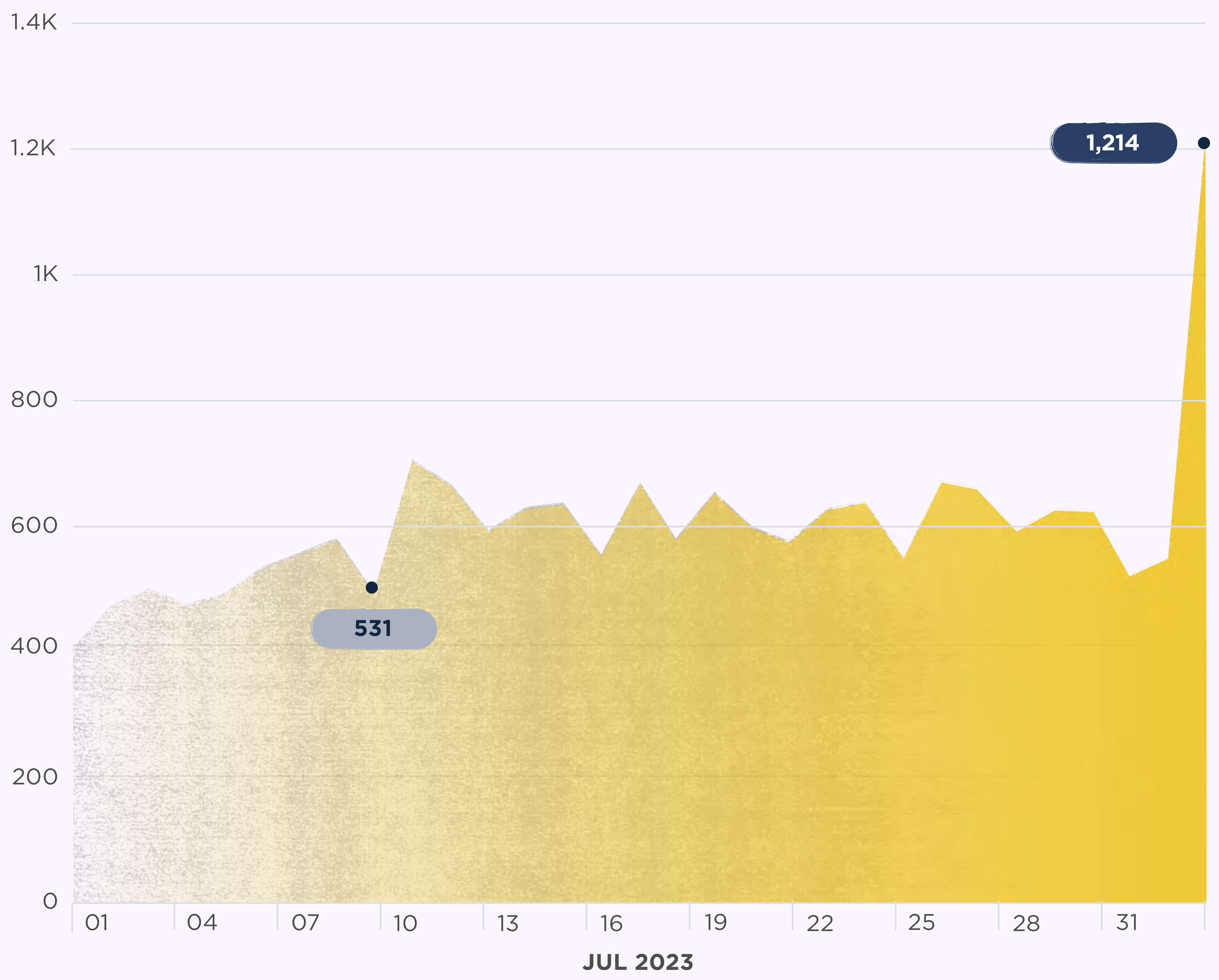
Abuse reports sent out to hosting providers and network owners

86.7%

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.

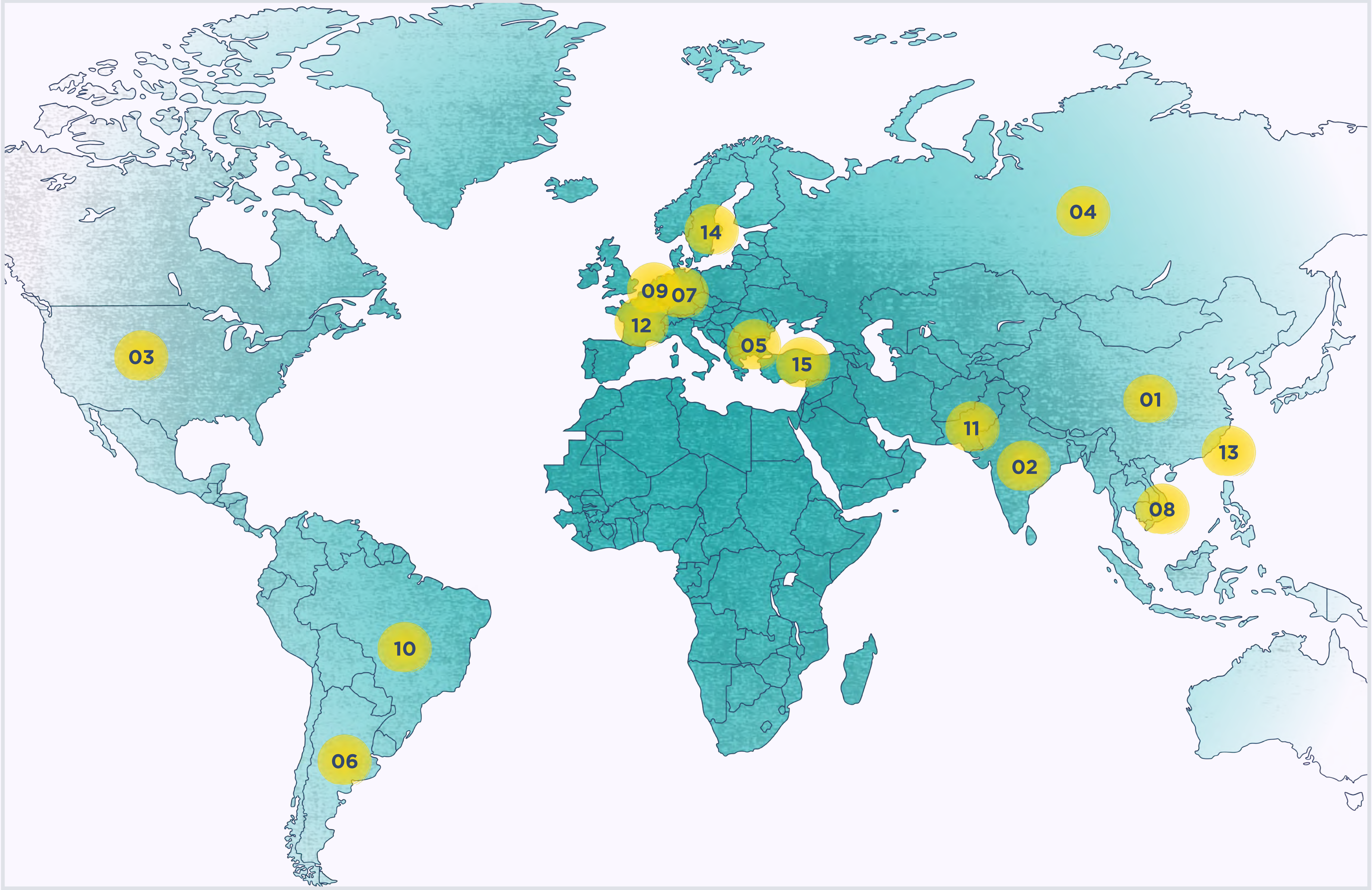


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	12,441	+71.53	geenensp
02	505	-94.50	lrz_urlhaus
03	196	+12.00	andretavare5
04	188	+168.57	JAMESWT_MHT
05	110	+64.18	bry_campbell
06	82	-39.71	JobcenterTycoon
07	64	New entry	iamdeadlyz
08	53	+60.61	Casperinous
09	47	-98.90	Cryptolaemus1
10	40	+166.67	dms1899
11	36	-50.00	viql
12	25	New entry	iam_py_test
13	22	+29.41	ULTRAFRAUD
14	9	New entry	wonderhoi39
15	6	New entry	Gootloader2

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	9,963	+271.62	China
02	4,236	+65.08	India
03	1,481	-54.75	United States
04	625	+89.97	Russia
05	405	+387.95	Bulgaria
06	376	+182.71	Argentina
07	343	+68.97	Germany
08	218	+225.37	Vietnam
09	201	0.00	Netherlands
10	167	+169.35	Brazil
11	162	New entry	Pakistan
12	135	-17.18	France
13	119	New entry	Taiwan (PoC)
14	108	New entry	Sweden
15	92	+46.03	Turkey

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	8,233	4837	CHINA169-BACKBONE	China
02	3,548	9829	BSNL-NIB	India
03	1,362	4134	CHINANET-BACKBONE	China
04	334	46308	SUKHOI-SU-57-LLC	Russia
05	331	52495	Cotel Ltda.	Bolivia
06	304	211252	AS_DELIS	Netherlands
07	257	13335	CLOUDFLARENET	United States
08	168	36352	AS-COLOCROSSING	United States
09	152	17816	CHINA169-GZ	China
10	151	47541	VKONTAKTE-SPB-AS	Russia
11	141	23888	NTC-AS-AP	Pakistan
12	111	133661	NETPLUS-AS	India
12	111	133696	FASTWAY-AS	India
13	106	16276	OVH	France
14	100	210644	AEZA-AS	Russia

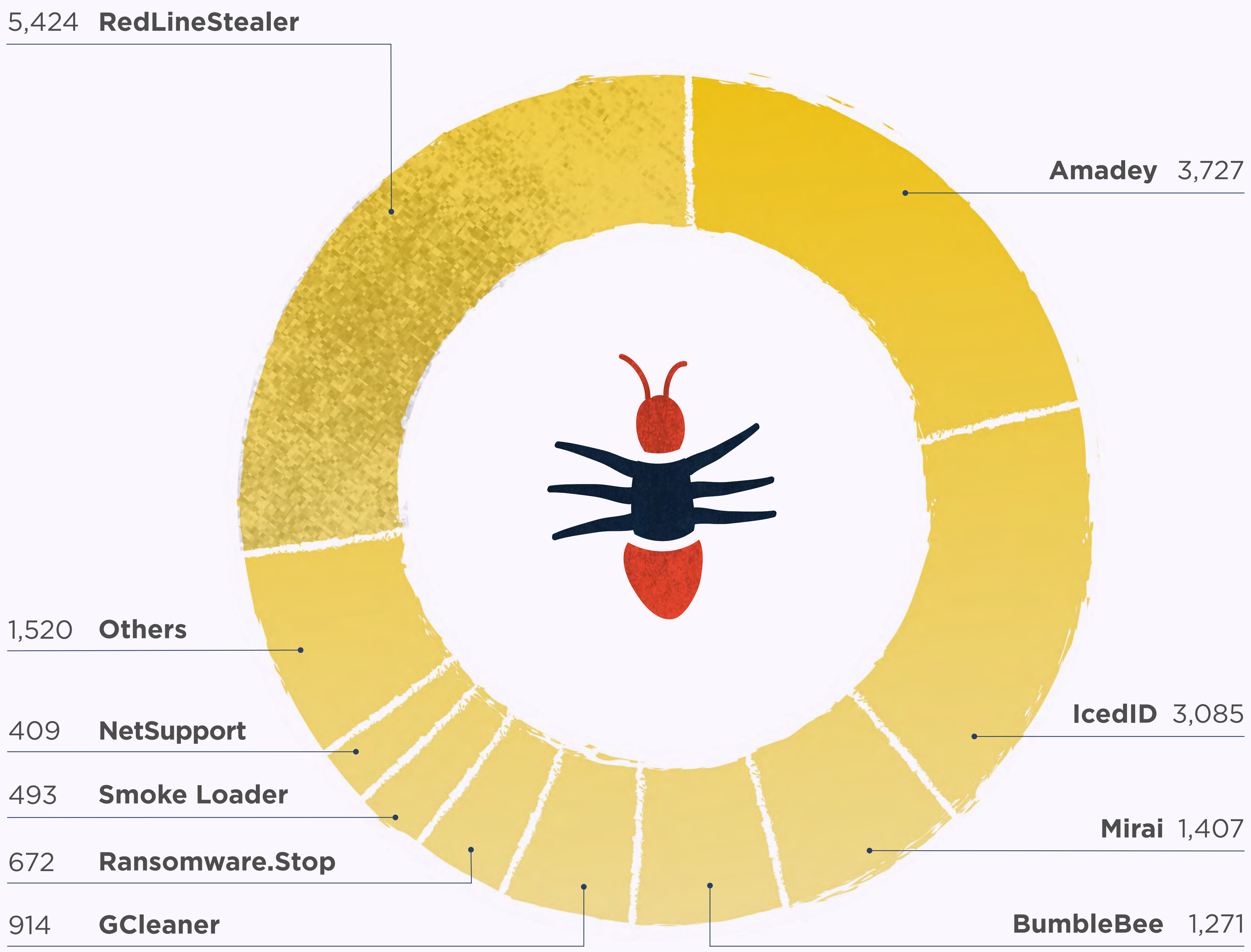
TOP MALWARE HOSTS

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	147	vk.com	VK	Russia
02	76	wtools.io	WTOOLS	United States
03	62	cdn.discordapp.com	Discord	United States
04	54	github.com	Github	United States
05	40	transfer.sh	n/a	n/a
06	31	pasteio.com	n/a	n/a

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	Ransomware.Stop	+218.48	672
02	Amadey	+91.03	3,727
03	Smoke Loader	+69.42	493
04	NetSupport	+60.39	409
05	RedLineStealer	+54.31	5,424
06	AgentTesla	+45.07	206
07	GCleaner	+39.33	914
08	UACModuleSmokeLoader	+35.04	343
09	BumbleBee	+31.71	1,271
10	CoinMiner	+23.79	255
11	Mirai	+15.23	1,407
12	Rhadamanthys	-34.76	214
13	Quakbot	-97.85	351
14	IcedID	New entry	3,085
14	CryptOne	New entry	151

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

12,528

Malware samples shared by security researchers on MalwareBazaar

+25.6%

Increase on the previous month

1,295

Active hunting rules

+3.4%

Increase on the previous month

10.29MB

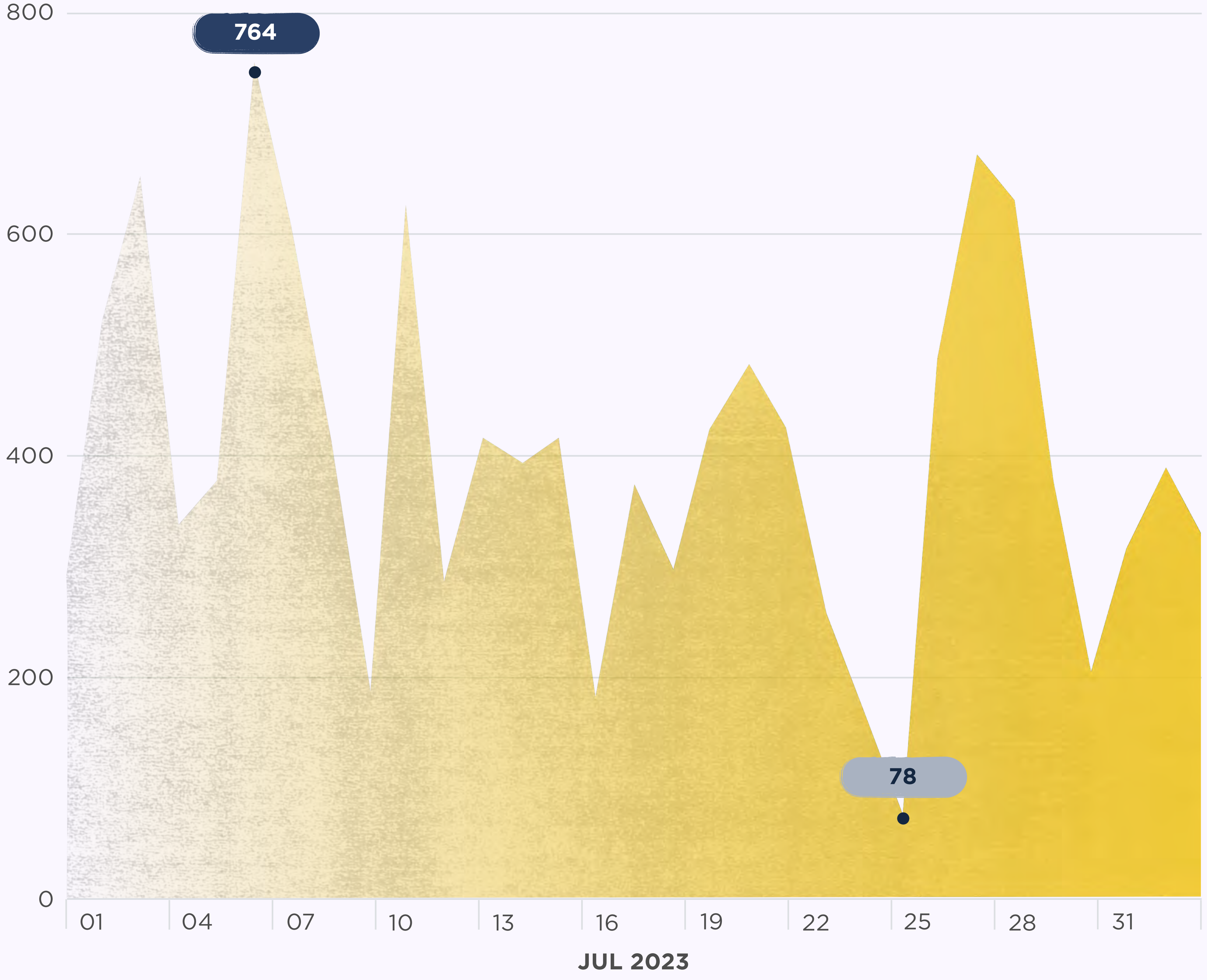
Average size of a malware sample

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.



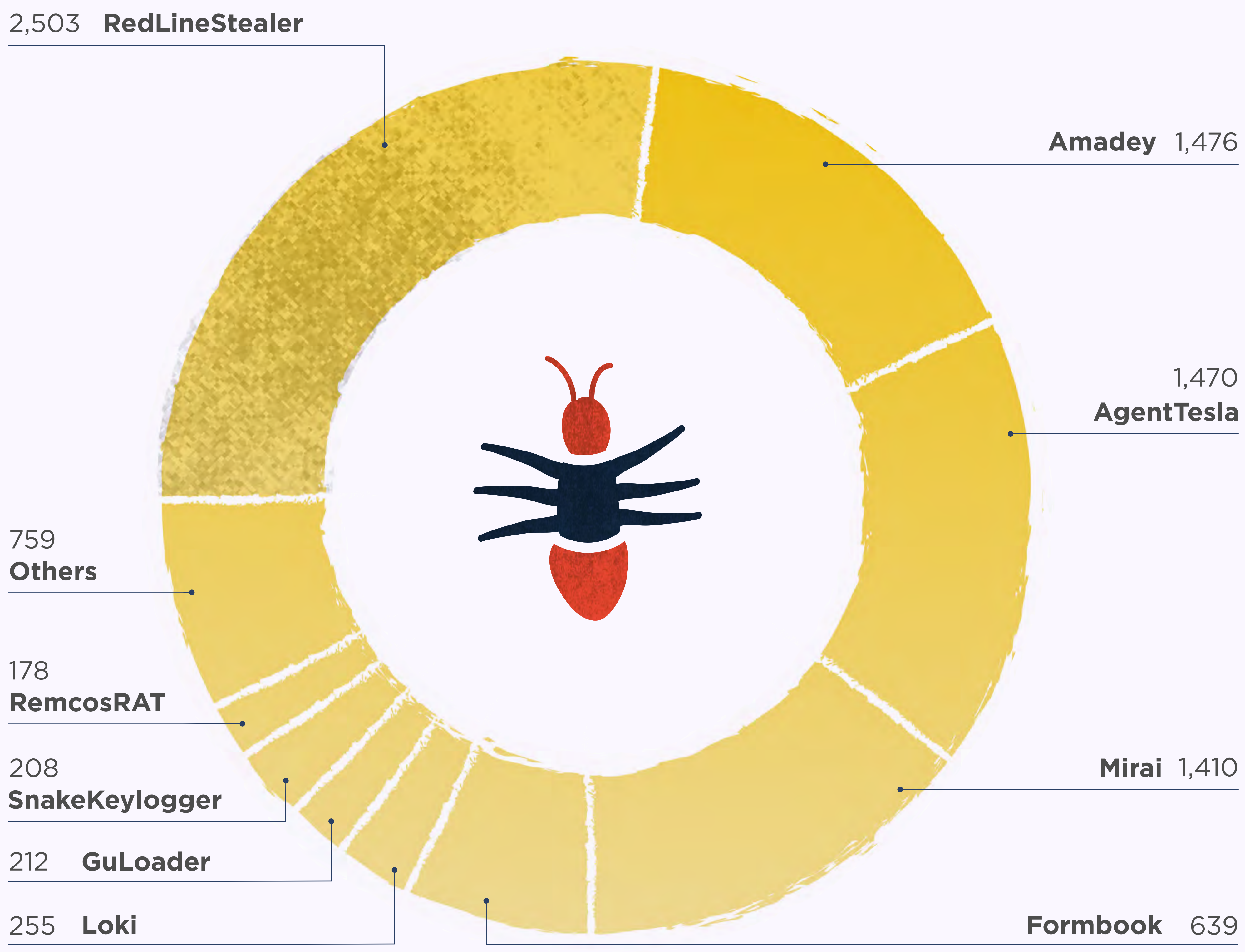
TOP SAMPLE CONTRIBUTORS

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	870	+57.04	@andretavare5
02	821	+1.73	@cocaman
03	524	+57.36	@JAMESWT_MHT
04	355	+13.78	@lowmal3
05	312	+18.18	@adrian__luca
06	223	+129.90	@obfusor
07	136	+56.32	@malwarelabnet
08	108	-28.48	@TeamDreier
09	100	-5.66	@Porcupine
10	58	New entry	@iamdeadlyz
11	52	New entry	@ULTRAFRAUD
12	50	-51.46	@pr0xylife
13	44	New entry	@johnk3r
14	31	New entry	@1ZRR4H
15	27	-90.91	@jstrosch

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



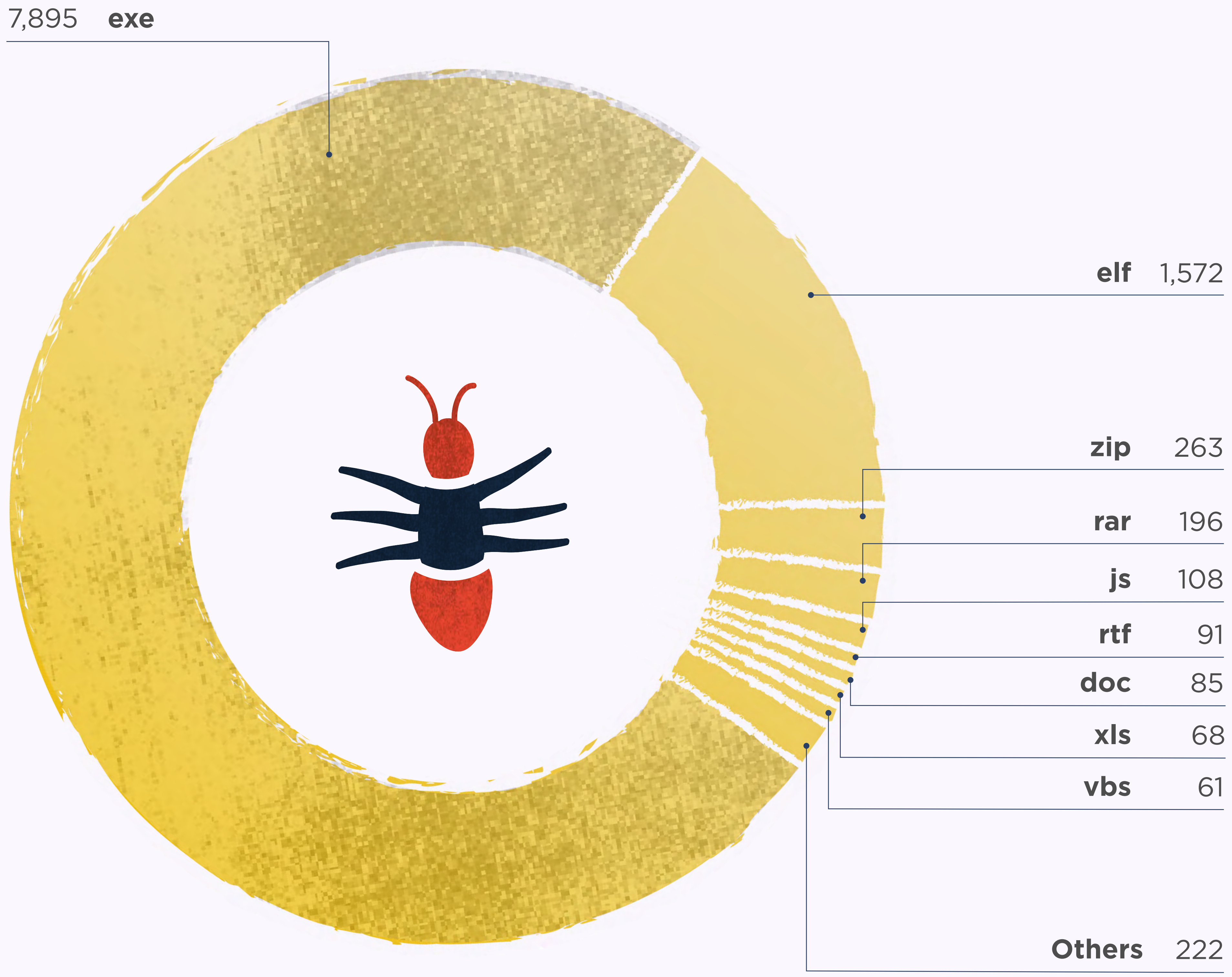
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	Amadey	⇈ +110.86	1,476
02	RedLineStealer	⇈ +77.64	2,503
03	Formbook	⇈ +51.78	639
04	GuLoader	⇈ +40.40	212
05	Loki	↑ +22.01	255
06	SnakeKeylogger	↑ +9.47	208
07	AgentTesla	↑ +7.69	1,470
08	RemcosRAT	↑ +5.95	178
09	Mirai	↓ -1.88	1,410
10	Gafgyt	↓ -11.11	152
11	GCleaner	⇊ -36.21	148
12	DCRat	— New entry	125
12	njrat	— New entry	119
12	DarkCloud	— New entry	113
12	Smoke Loader	— New entry	102

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	2,858	detect_Redline_Stealer	Varp0s
02	2,001	MALWARE_Win_RedLine	ditekSHen
03	1,739	INDICATOR_EXE_Packed_ConfuserEx	ditekSHen
04	1,709	PE_Digital_Certificate	albertzsigovits
05	1,625	redline_stealer_1	Nikolaos 'n0t' Totosis
06	1,573	PE_Potentially_Signed_Digital_Certificate	albertzsigovits
07	1,076	INDICATOR_SUSPICIOUS_EXE_RegKeyComb_DisableWinDefender	ditekSHen
08	945	myMirai	n/a
09	906	INDICATOR_SUSPICIOUS_EXE_B64_Encoded_UserAgent	ditekSHen
10	803	unixredflags3	@timb_machine
11	784	linux_generic_ipv6_catcher	@_lubiedo
12	702	cobalt_strike_tmp01925d3f	The DFIR Report
13	599	shellcode	nex
14	424	Windows_Trojan_Smokeloader_3687686f	Elastic Security
15	394	setsockopt	@timb_machine

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)

8,764

Indicators of compromise (IOCS) shared on ThreatFox

-14.1%

Decrease on the previous month

1,620

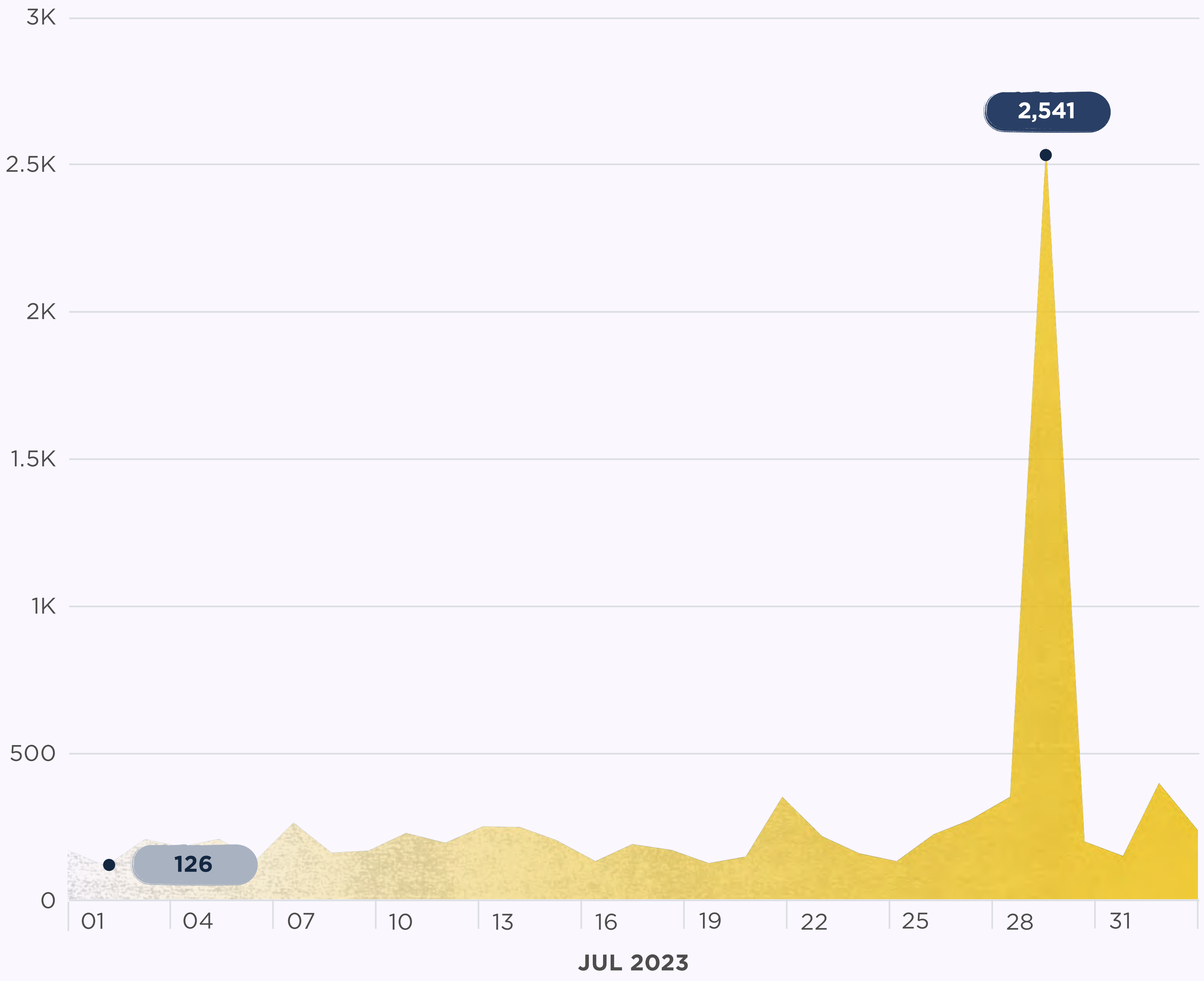
IOCs relating to DBatLoader

NEW ENTRY

in July

NUMBER OF IOCs SHARED PER DAY

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



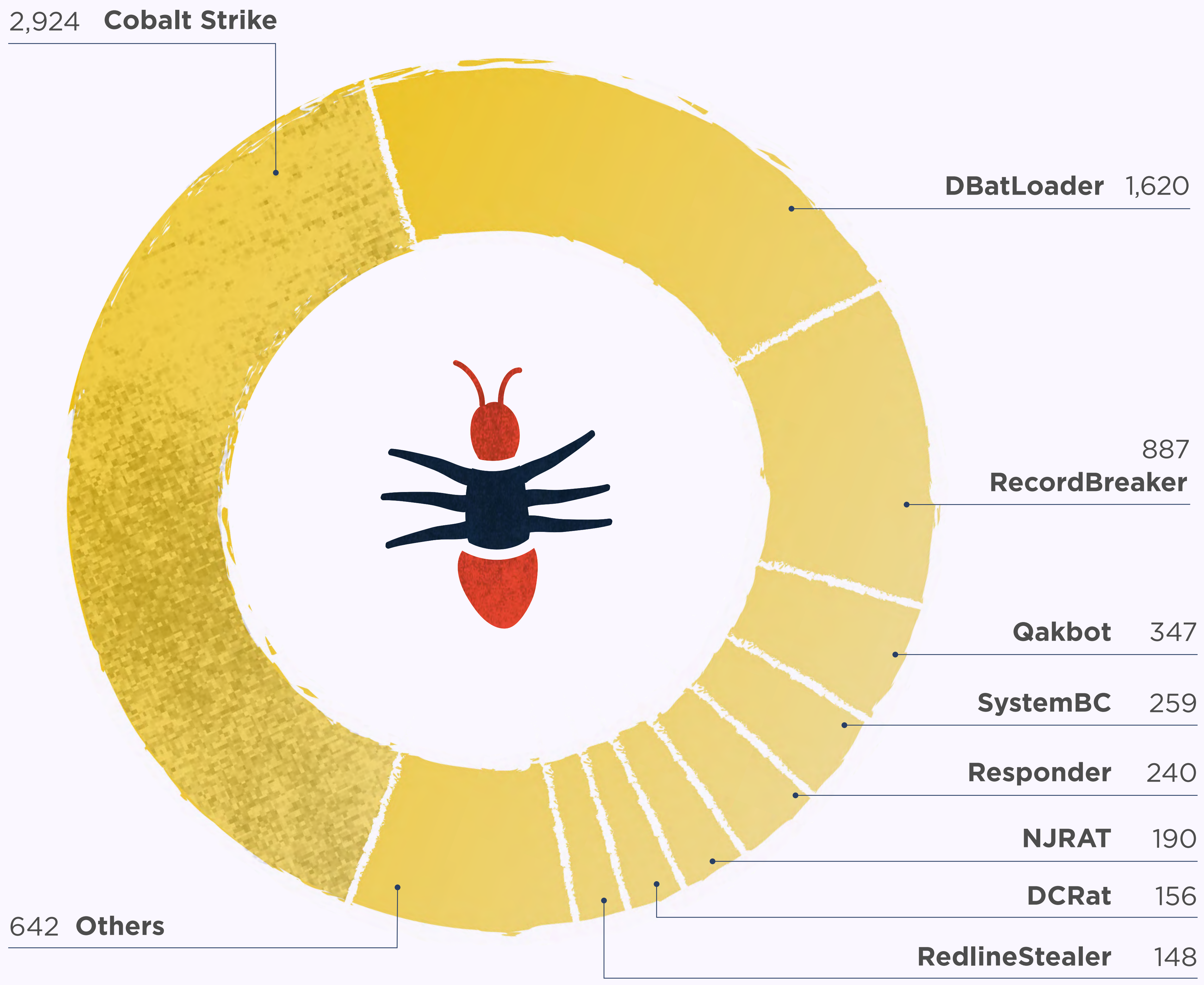
IOC TYPE

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	3,328	url	botnet_cc	URL that is used for botnet Command&control (C&C)
02	2,827	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
03	1,716	url	payload _delivery	URL that delivers a malware payload
04	685	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
05	126	md5_hash	payload	MD5 hash of a malware sample (payload)
06	72	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
07	55	domain	payload _delivery	Domain name that delivers a malware payload
08	12	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.



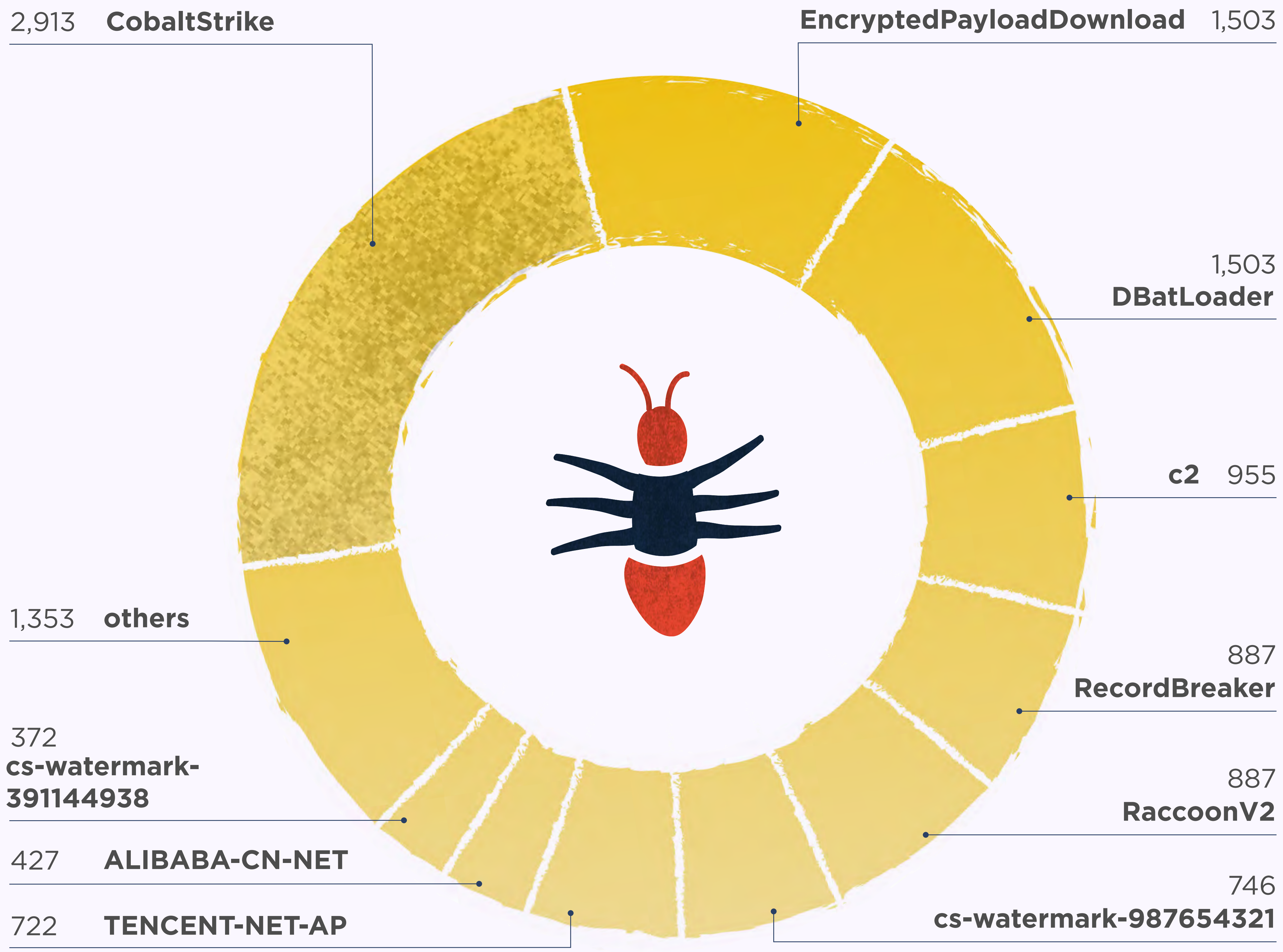
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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	RecordBreaker	+833.68	887
02	NJRAT	+123.53	190
03	DCRat	+64.21	156
04	Cobalt Strike	-4.10	2,924
05	Responder	-11.76	240
06	BianLian	-25.00	102
07	Mirai	-26.99	119
08	Vidar	-45.09	95
09	RemcosRAT	-60.00	90
10	Qakbot	-91.66	347
11	IcedID	— New entry	146
11	RedlineStealer	— New entry	148
11	SystemBC	— New entry	259
11	IRATA	— New entry	90
11	DBatLoader	— New entry	1,620

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	cs-watermark-987654321	⇈ +65.78	746
02	cs-watermark-391144938	↑ +12.39	372
03	CobaltStrike	↓ -4.27	2,913
04	cs-watermark-100000	↓ -10.66	327
05	RAT	↓ -16.18	228
06	RaccoonV2	— New entry	877
06	RecordBreaker	— New entry	887
06	TENCENT-NET-AP	— New entry	722
06	ALIBABA-CN-NET	— New entry	427
06	c2	— New entry	955
06	cs-watermark-1234567890	— New entry	338
06	EncryptedPayloadDownload	— New entry	1,503
06	Responder	— New entry	240
06	DBatLoader	— New entry	1,503
06	cs-watermark-0	— New entry	220

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

2,240,443

File scans conducted on YARAify

+4.3%

increase in file scans on the previous month

1,694,070

Distinct files that had scans performed on them

+2.5%

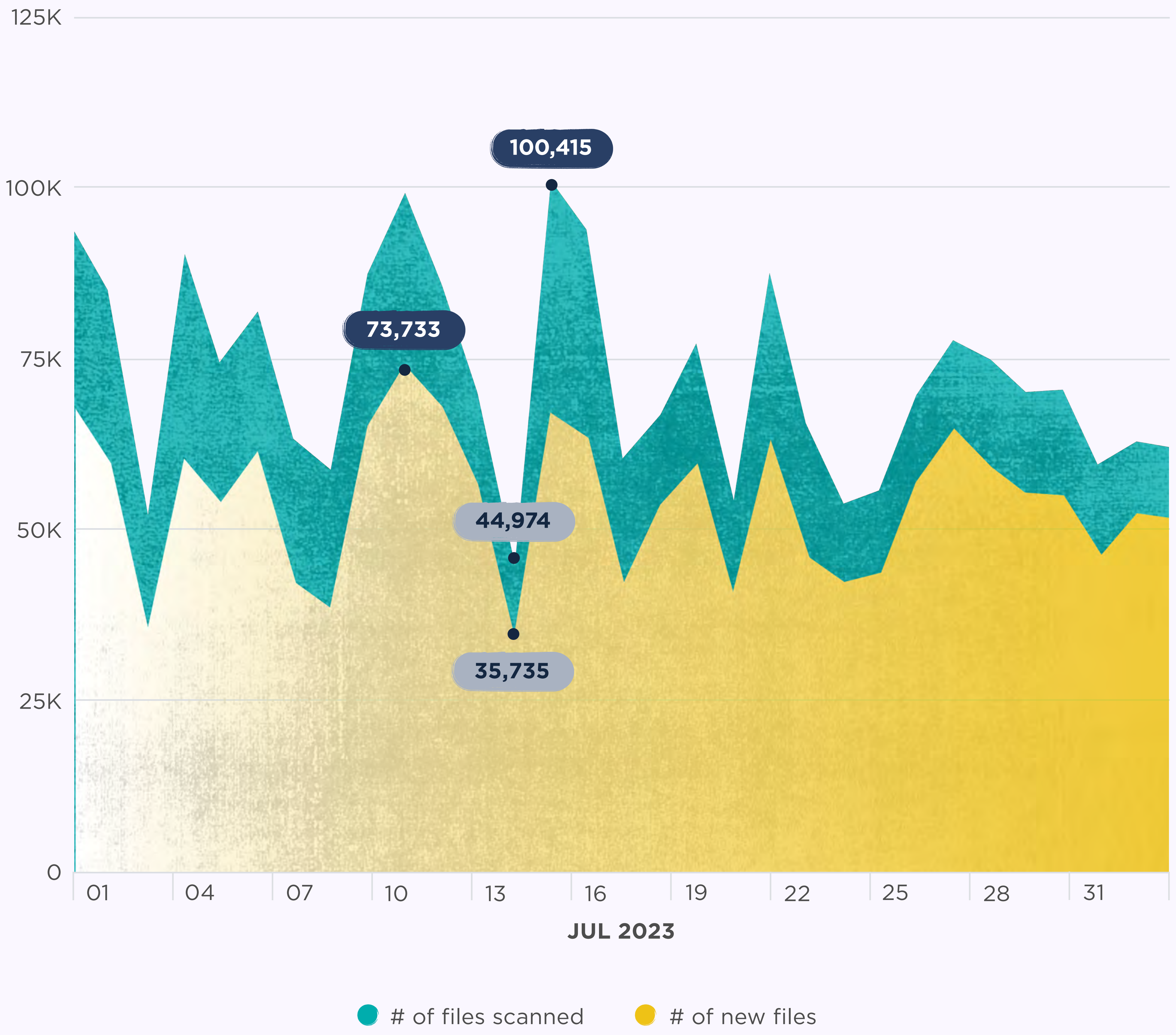
increase in files on the previous month

15,524

YARA rules deployed on YARAify and available for hunting

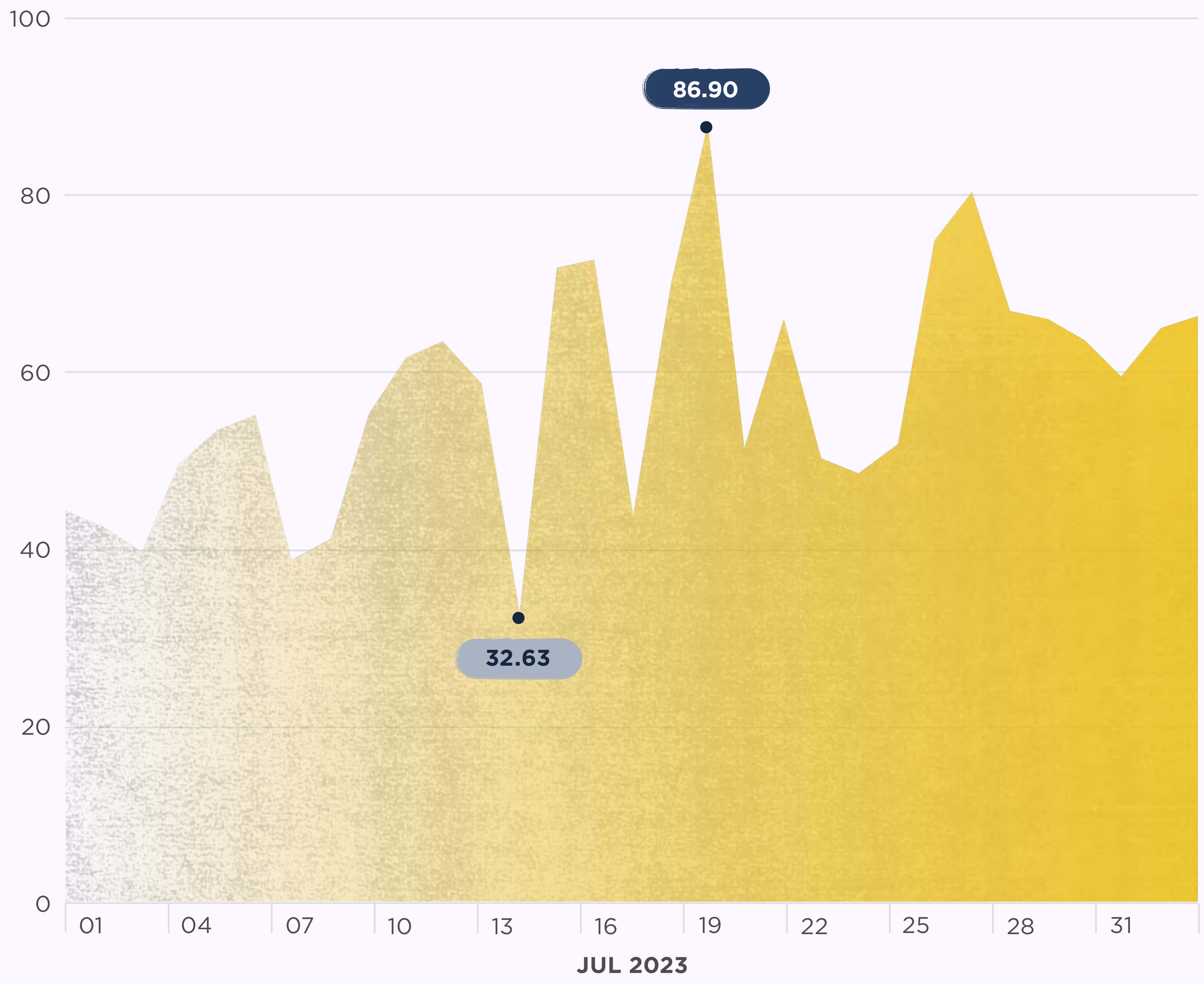
FILES SCANNED PER DAY

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	69,453	-16.06	SUSP_Imphash_Mar23_2	Arnim Rupp
02	61,419	New entry	shellcode	nex
03	60,892	+131.59	PE_Potentially_Signed_Digital_Certificate	n/a
04	50,010	+78.32	PE_Digital_Certificate	albertzsigovits
05	48,067	+93.43	BitcoinAddress	Didier Stevens (@DidierStevens)
06	43,069	+35.80	win_qakbot_malped	Felix Bilstein
06	43,069	+35.80	win_qakbot_auto	Felix Bilstein
07	43,057	+37.95	QakBot	kevoreilly
08	43,026	+38.52	qakbot_api_hashing	@Embee_Research
09	43,015	+35.78	MAL_QakBot_ConfigExtraction_Feb23	kevoreilly
09	43,015	+37.90	unpacked_qbot	n/a
10	41,394	+37.90	Windows_Trojan_Qbot_1ac22a26	Elastic Security
11	36,592	+35.95	cobalt_strike_tmp01925d3f	The DFIR Report
12	32,982	+82.77	win_qakbot_api_hashing_oct_2022	@Embee_Research
13	27,523	New entry	TeslaCryptPackedMalware	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	149,846	-0.86	Win.Malware.Dqqw-9951425-0
02	149,295	-1.06	Win.Malware.Zusy-6804618-0
03	149,293	-1.06	Win.Trojan.QQPass-5710308-0
04	59,607	New entry	PUA.Win.Packer.Lccwin-2
05	47,571	-7.31	Win.Malware.Gepys-9770177-0
06	42,942	New entry	Win.Trojan.Qbot-10002723-0
07	39,749	New entry	Win.Trojan.Obfus-38
08	34,655	New entry	PUA.Win.Packer.AcprotectUltraprotect-1
09	25,049	New entry	Sanesecurity.Malware.28840.BadO.UNOFFICIAL
10	23,797	New entry	Win.Trojan.Qukart-6874817-0
11	23,646	New entry	Win.Packed.Lazy-10005437-0
12	22,138	New entry	Win.Trojan.Crypted-30
13	21,846	New entry	Win.Trojan.Crypted-29
14	21,245	New entry	Win.Malware.Nevereg-9916351-0
15	20,176	-90.86	Win.Malware.Midie-6847893-0

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN SEPTEMBER

Remember, sharing is caring.