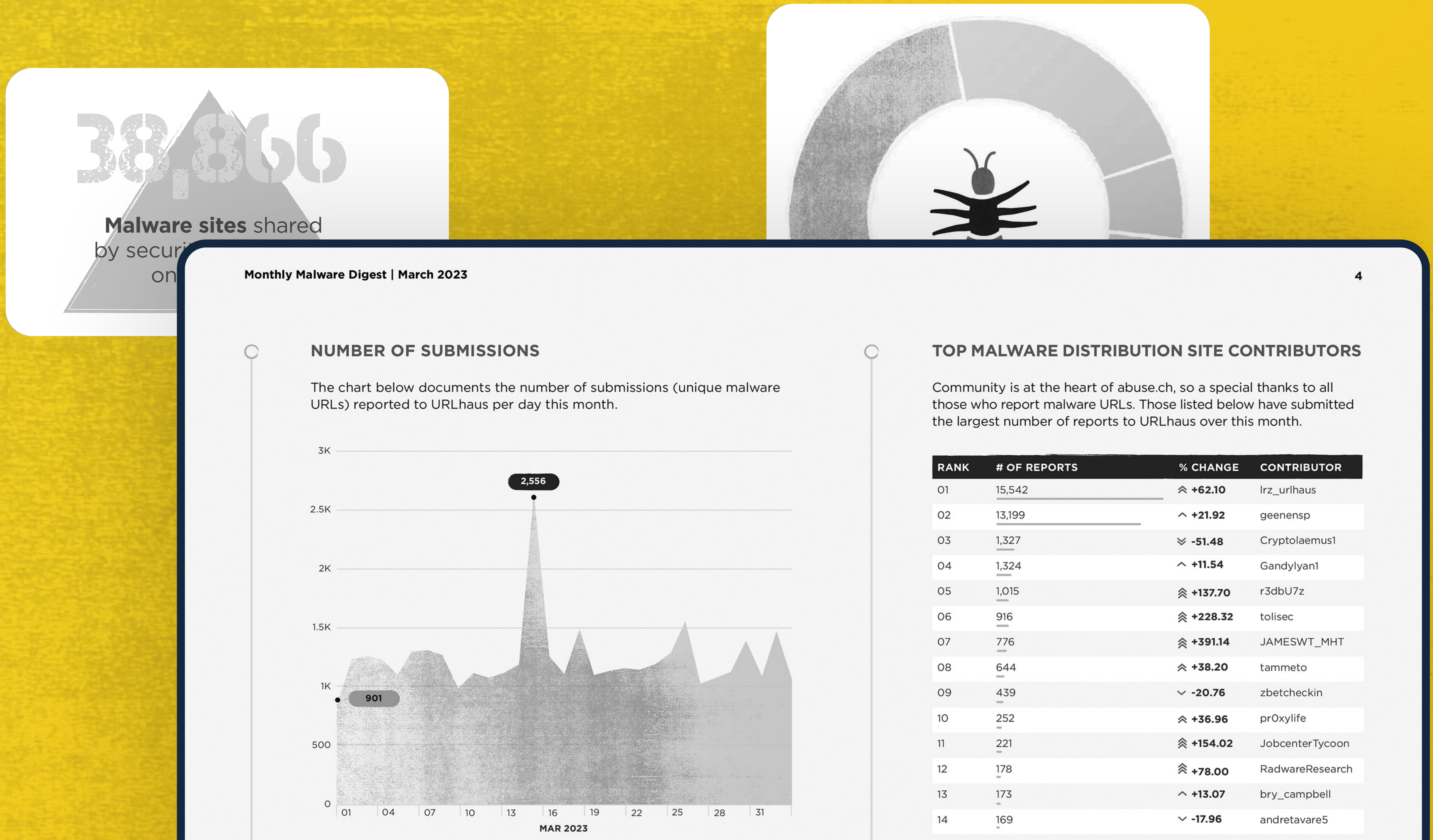
MARCH 2023

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.



Monthly Malware Digest | March 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	15,542	⌃⌃ +62.10	lrz_urlhaus
02	13,199	⌃ +21.92	geenensp
03	1,327	⌄⌄ -51.48	Cryptolaemus1
04	1,324	⌃ +11.54	Gandylyan1
05	1,015	⌃⌃⌃ +137.70	r3dbU7z
06	916	⌃⌃⌃ +228.32	tolisec
07	776	⌃⌃⌃ +391.14	JAMESWT_MHT
08	644	⌃⌃ +38.20	tammeto
09	439	⌄ -20.76	zbetcheckin
10	252	⌃⌃ +36.96	pr0xylife
11	221	⌃⌃⌃ +154.02	JobcenterTycoon
12	178	⌃⌃⌃ +78.00	RadwareResearch
13	173	⌃ +13.07	bry_campbell
14	169	⌄ -17.96	andretavare5

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
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

38,866

Malware sites shared by security researchers on URLhaus

+33%

Increase month on month

39,213

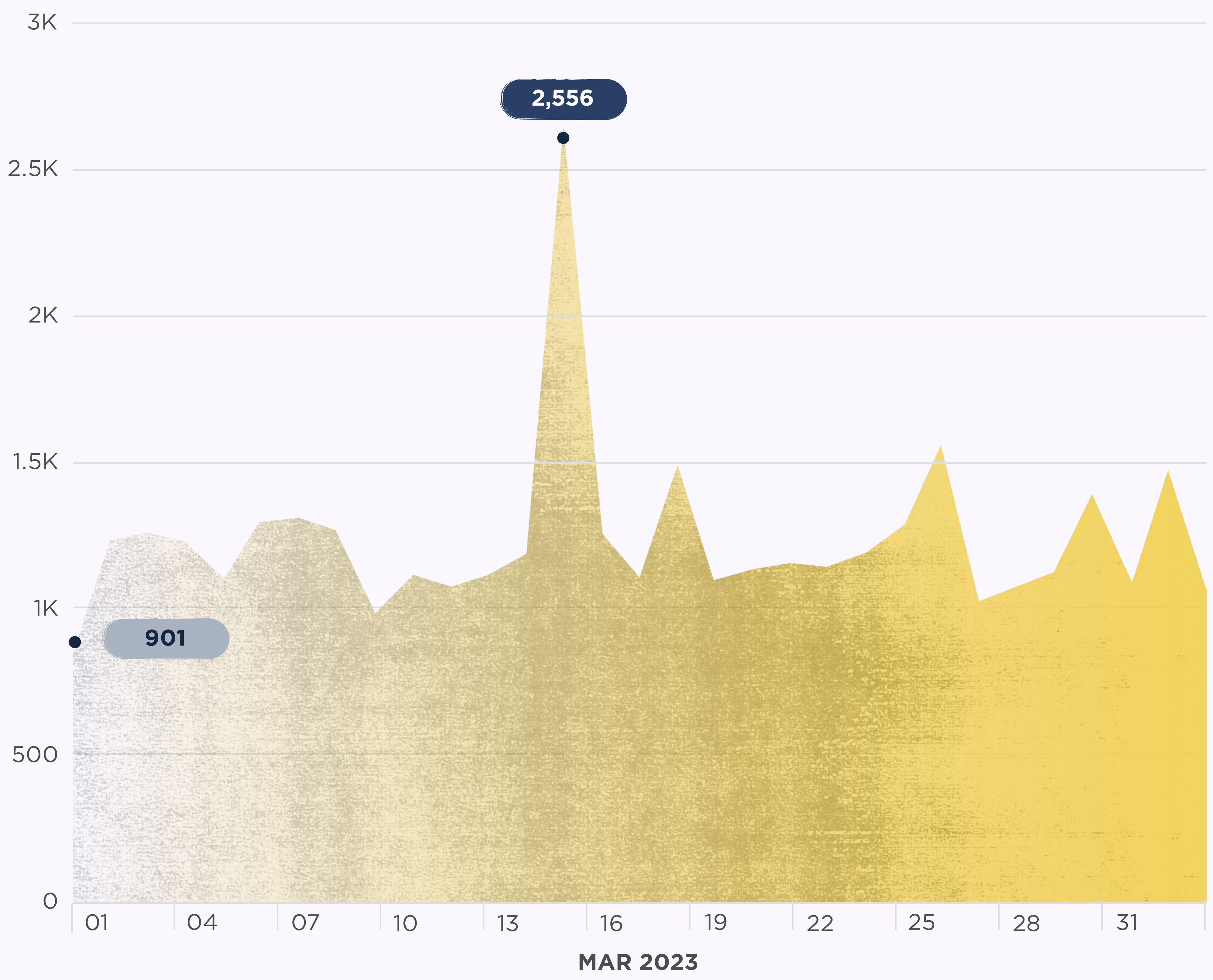
Abuse reports sent out to hosting providers and network owners

92%

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.

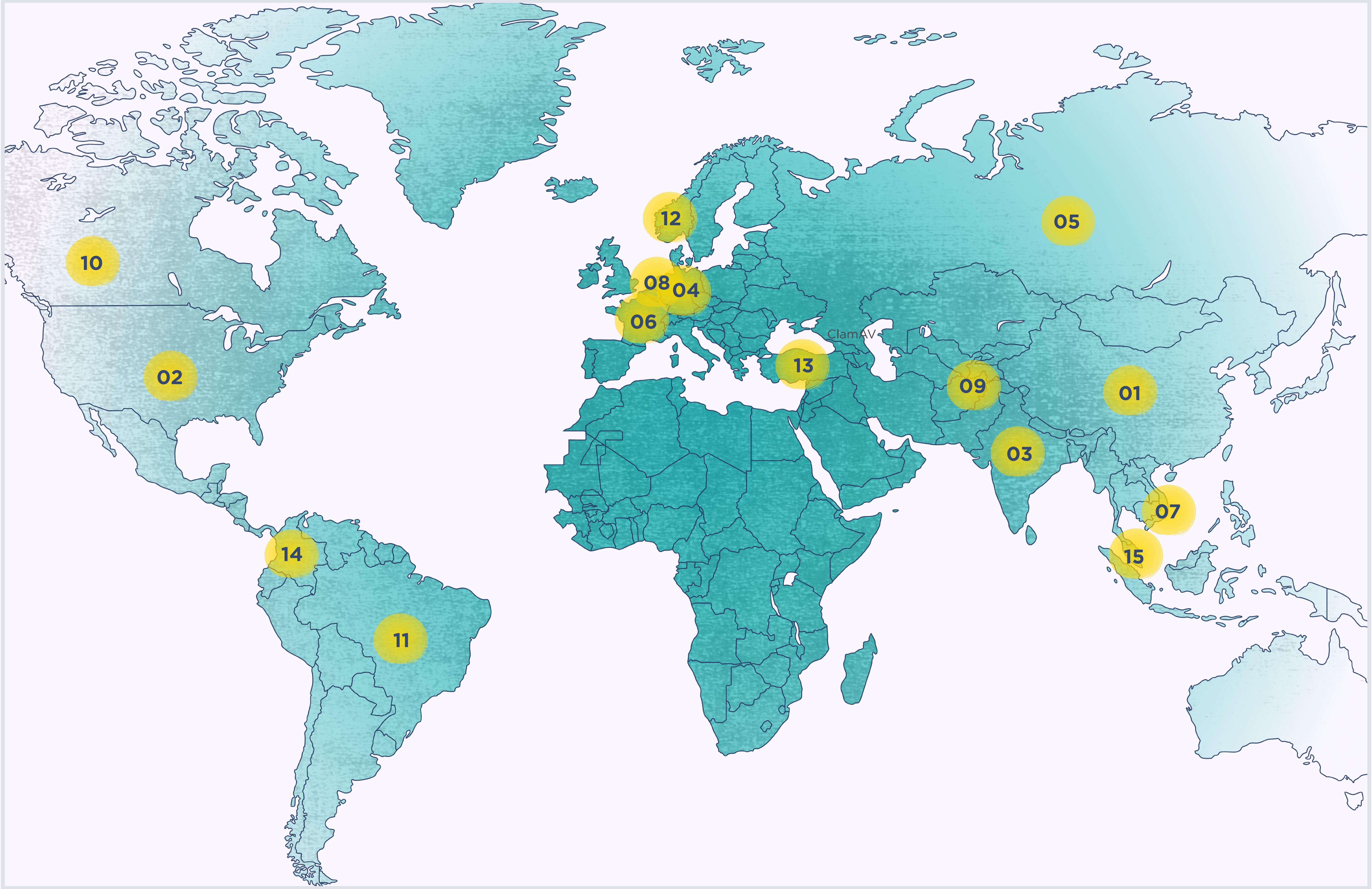


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	15,542	⌃⌃ +62.10	lrz_urlhaus
02	13,199	⌃ +21.92	geenensp
03	1,327	⌄⌄ -51.48	Cryptolaemus1
04	1,324	⌃ +11.54	Gandylyan1
05	1,015	⌃⌃⌃ +137.70	r3dbU7z
06	916	⌃⌃⌃ +228.32	tolisec
07	776	⌃⌃⌃ +391.14	JAMESWT_MHT
08	644	⌃⌃ +38.20	tammeto
09	439	⌄ -20.76	zbetcheckin
10	252	⌃⌃ +36.96	pr0xylife
11	221	⌃⌃⌃ +154.02	JobcenterTycoon
12	178	⌃⌃⌃ +78.00	RadwareResearch
13	173	⌃ +13.07	bry_campbell
14	169	⌄ -17.96	andretavare5

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	8,822	▲ +20.32	China
02	2,333	▼ -30.00	United States
03	2,202	▼ -6.66	India
04	370	▲ +24.58	Germany
05	369	▼ -11.51	Russia
06	269	▲▲ +60.12	France
07	264	▲▲▲ +107.87	Viet Nam
08	246	▲ +12.33	Netherlands
09	226	▲▲▲ +380.85	Pakistan
10	178	▲▲▲ +83.51	Canada
11	146	▲▲▲ +80.25	Brazil
12	131	▼ -19.63	Norway
13	113	▲▲ +52.70	Turkey
14	98	▼▼ -37.97	Colombia
15	90	▼▼▼ -70.49	Singapore

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	6,423	4837	CHINA169	China
02	2,084	4134	CHINANET	China
03	2,017	9829	BSNL	India
04	479	22612	NAMECHEAP	United States
05	215	13335	CLOUDFLARENET	United States
06	214	17557	PKTELECOM-AS	Pakistan
07	202	36352	COLOCROSSING	United States
08	196	211252	DELIS	Netherlands
09	188	24940	HETZNER	Germany
10	186	46606	UNIFIEDLAYER	United States
11	171	24547	CMNET	China
12	154	16276	OVH	France
13	152	47583	HOSTINGER	United States
14	102	15169	GOOGLE	United States
15	99	26496	GO-DADDY-COM	United States

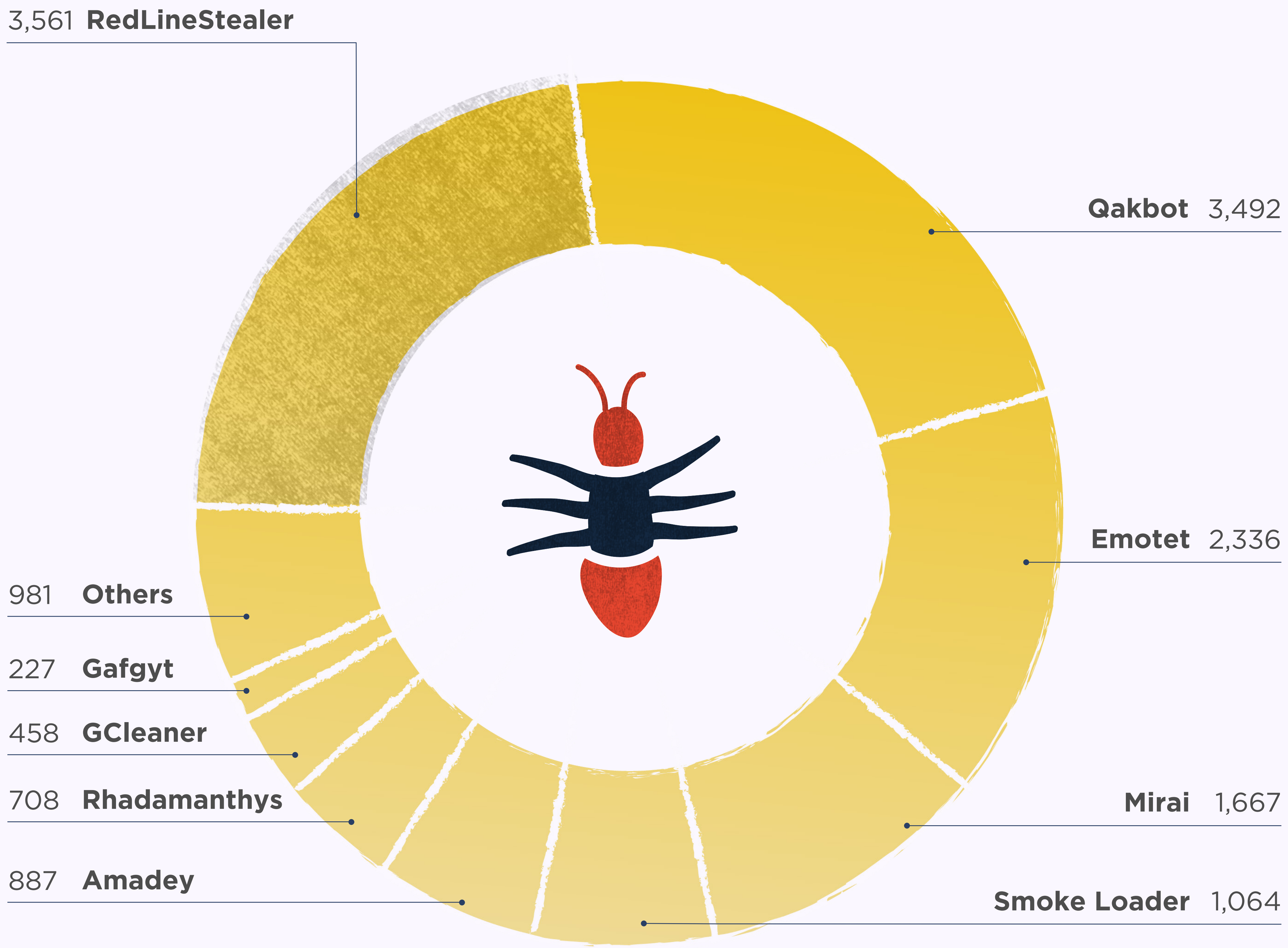
TOP MALWARE HOSTS

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	102	vk.com	VK	Russia
02	93	cdn.discordapp.com	Discord	United States
03	70	transfer.sh	n/a	n/a
04	51	wtools.io	WTOOLS	United States
05	41	github.com	Github	United States
06	36	onedrive.live.com	Microsoft	United States
07	36	pastebin.com	Pastebin	United States
08	34	bitbucket.org	Atlassian	Australia
09	26	drive.google.com	Google	United States

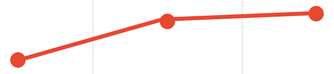
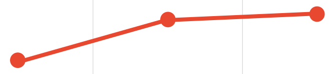
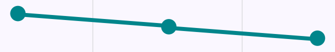
TOP MALWARE FAMILIES ASSOCIATED WITH MALWARE SITES

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	Mirai	⇈ +99.64		1,667
02	LaplasClipper	⇈ +92.00		192
03	Rhadamanthys	⇈ +75.68		708
04	Qakbot	⇈ +70.84		3,492
05	CoinMiner	⇈ +37.82		164
06	Gafgyt	^ +32.75		227
07	AgentTesla	^ +27.21		173
08	RedLineStealer	^ +1.05		3,561
09	Amadey	^ +0.11		877
10	Smoke Loader	∨ -0.09		1,064
11	GCleaner	∨ -19.51		458
12	Emotet	— New entry		2,336
13	Ransomware.Stop	— New entry		185
14	Tofsee	— New entry		151
15	Stealc	— New entry		116

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

12,076

Malware samples shared by security researchers on MalwareBazaar

-16.6%

Decrease on the previous month

1,109

Active hunting rules

-1.2%

Decrease on the previous month

10.85MB

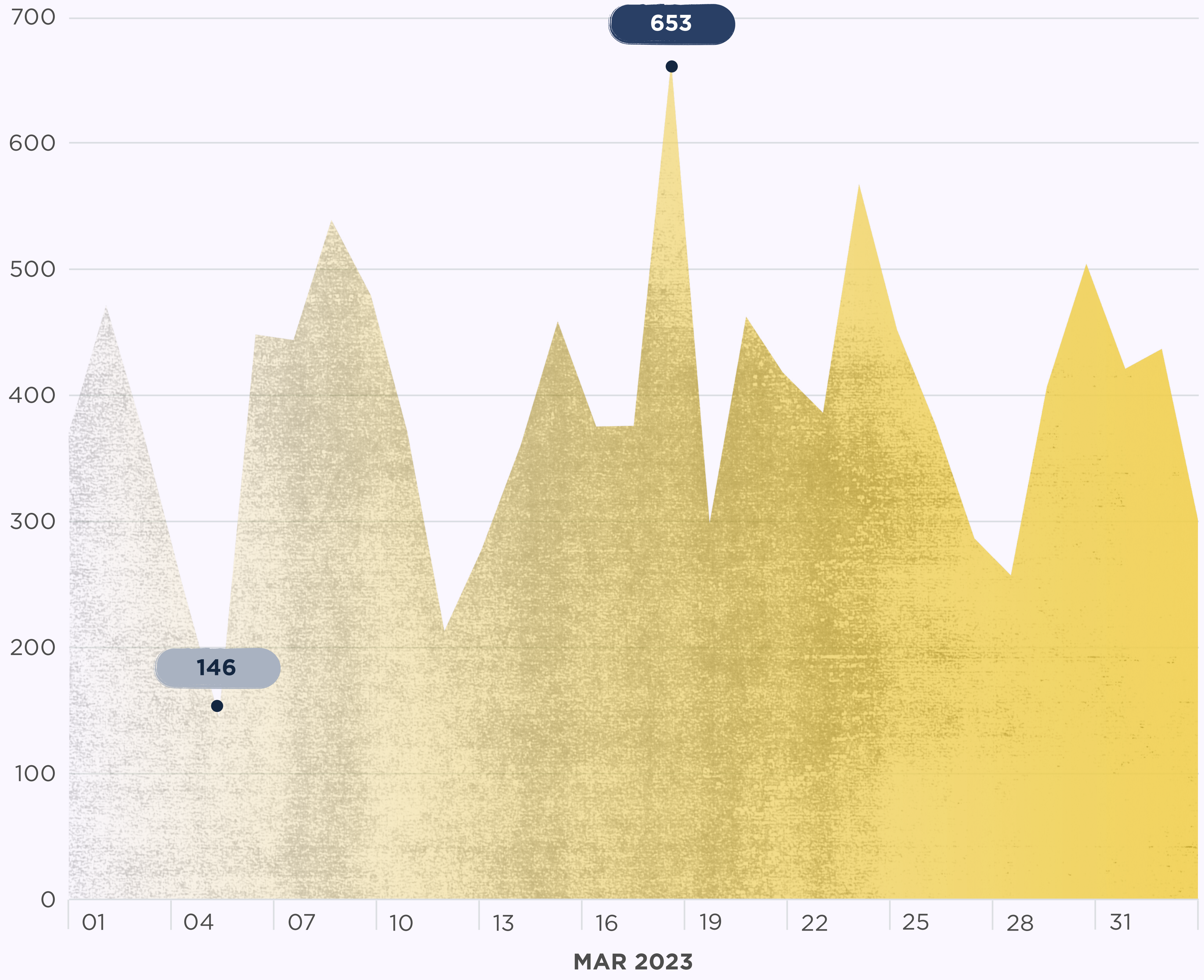
Average size of a malware sample

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.



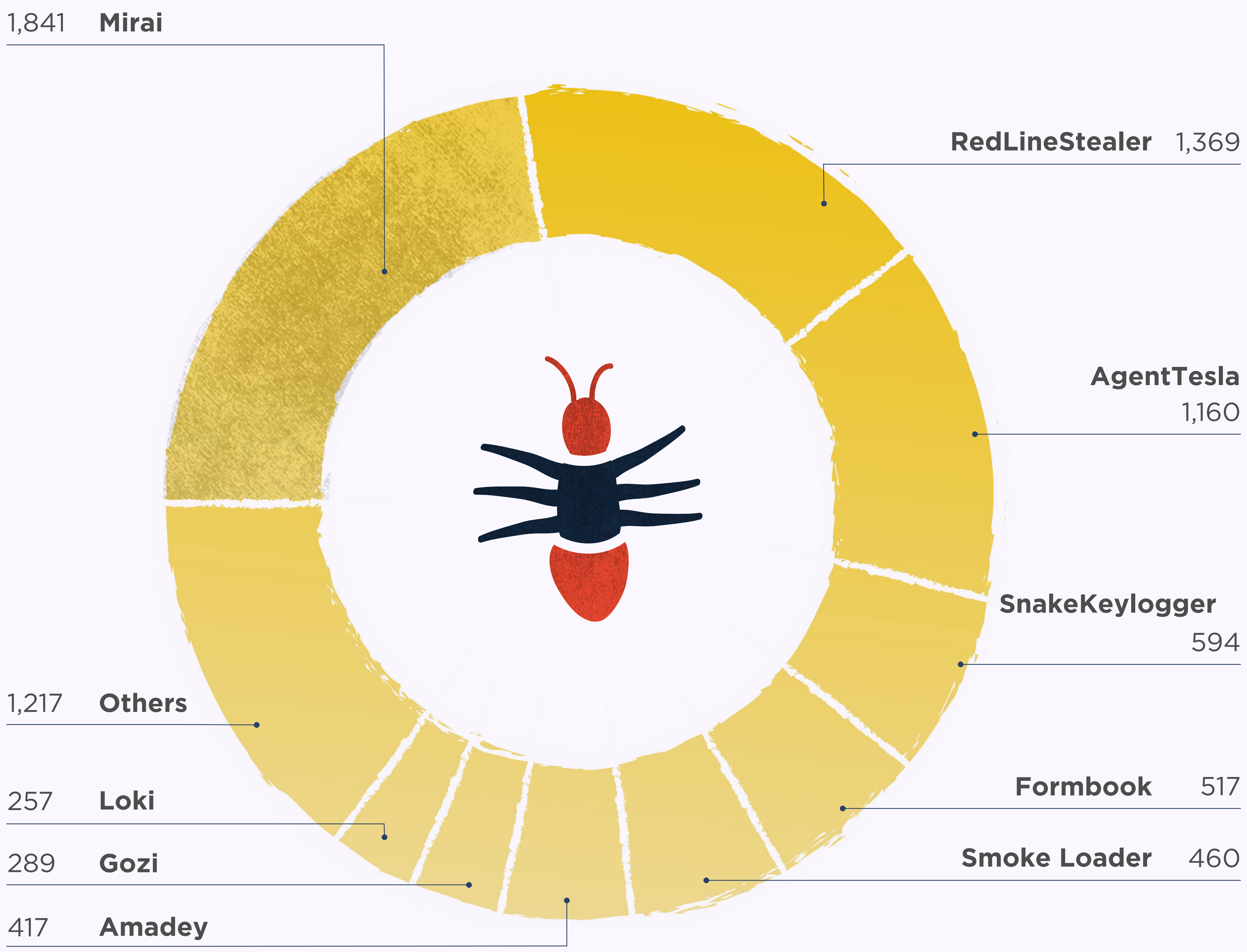
TOP SAMPLE CONTRIBUTORS

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	2,043	**+41.48**	@zbetcheckin
02	858	— **New entry**	@ChainskiLabs
03	615	**-88.10**	@andretavare5
04	524	**+155.61**	@JAMESWT_MHT
05	458	**+184.47**	@elfdigest
06	444	**-11.20**	@cocaman
07	351	**+92.86**	@petikvx
08	281	**-15.62**	@lowmal3
09	279	**+36.76**	@SecuriteInfoCom
10	253	**-19.43**	@adrian__luca
11	239	**+39.77**	@jstrosch
12	194	**-7.62**	@James_inthe_box
13	161	**+33.06**	@pr0xylife
14	153	**+10.87**	@TeamDreier
15	137	— **New entry**	@fabiodemartin

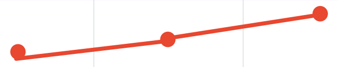
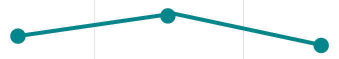
TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



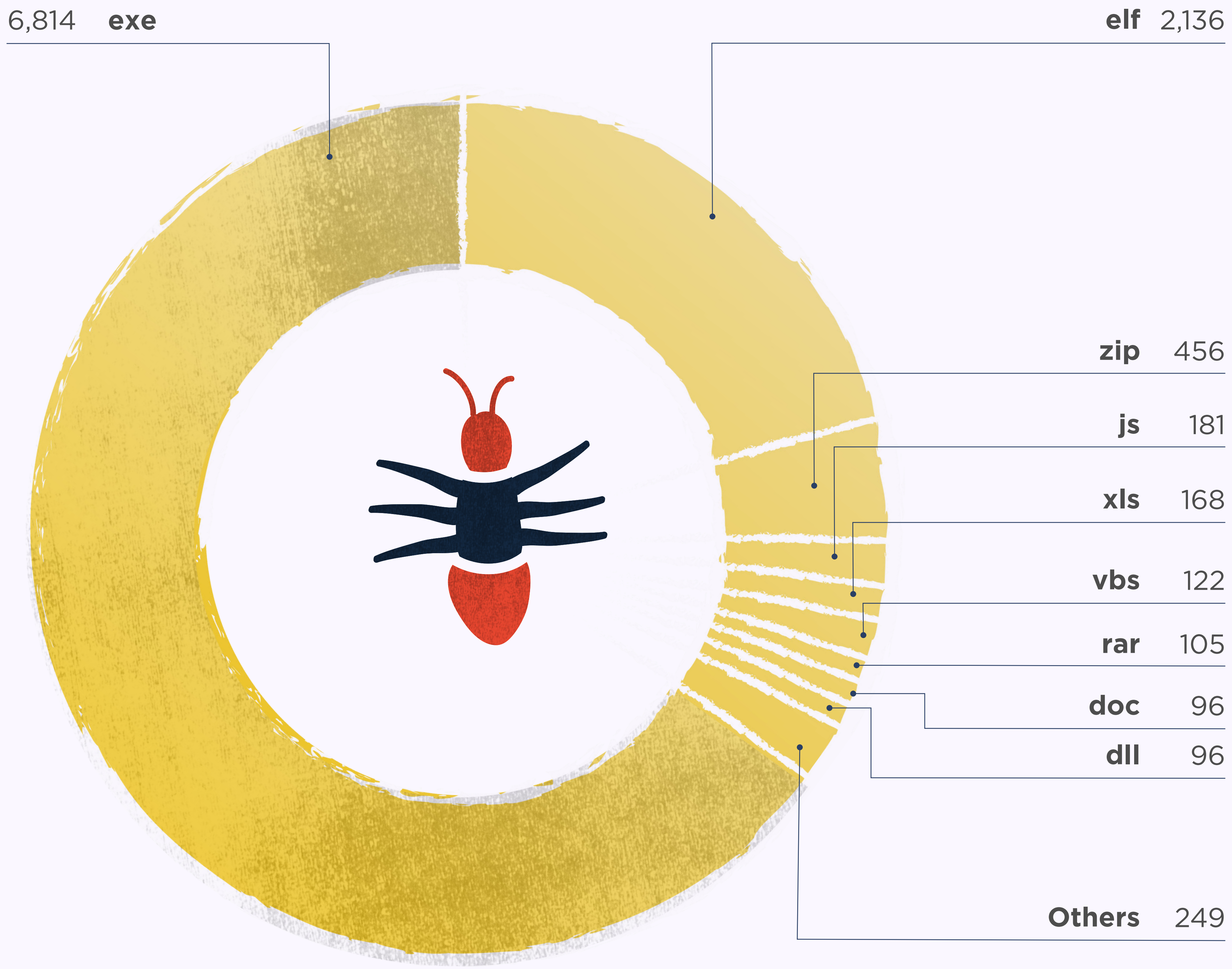
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	Gozi	⇈ +93.96		289
02	Mirai	⇈ +89.40		1,841
03	Gafgyt	⇈ +57.05		245
04	Loki	↑ +21.80		257
05	Formbook	↑ +6.16		517
06	AgentTesla	↓ -3.73		1,160
07	SnakeKeylogger	↓ -5.56		594
08	RemcosRAT	↓ -16.18		171
09	GuLoader	↓ -20.08		207
10	Smoke Loader	⇊ -46.45		460
11	RedLineStealer	⇊ -50.83		1,369
12	Amadey	⇊ -72.94		417
13	Heodo	— New entry		222
14	Rhadamanthys	— New entry		219
15	Stop	— New entry		153

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	1,653	Windows_Trojan_Smokeloader_3687686f	Elastic Security
02	1,323	MALWARE_Win_RedLine	ditekshen
03	1,314	myMirai	New entry
04	1,287	linux_generic_ipv6_catcher	@_lubiedo
05	1,139	unixredflags3	@timb_machine
06	1,082	Excel_Hidden_Macro_Sheet	New entry
07	708	Linux_Trojan_Gafgyt_28a2fe0c	Elastic Security
08	691	shellcode	nex
09	588	setsockopt	@timb_machine
10	517	PE_Digital_Certificate	albertzsigovits
11	482	cobalt_strike_tmp01925d3f	The DFIR Report
12	444	PE_Potentially_Signed_Digital_Certificate	albertzsigovits
13	378	Microsoft_XLSX_with_Macrosheet	New entry
14	329	Linux_Gafgyt_Generic_A	albertzsigovits
15	313	golang	New entry

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)

11,571

Indicators of compromise (IOCS) shared on ThreatFox

+28.1%

Increase on the previous month

2,734

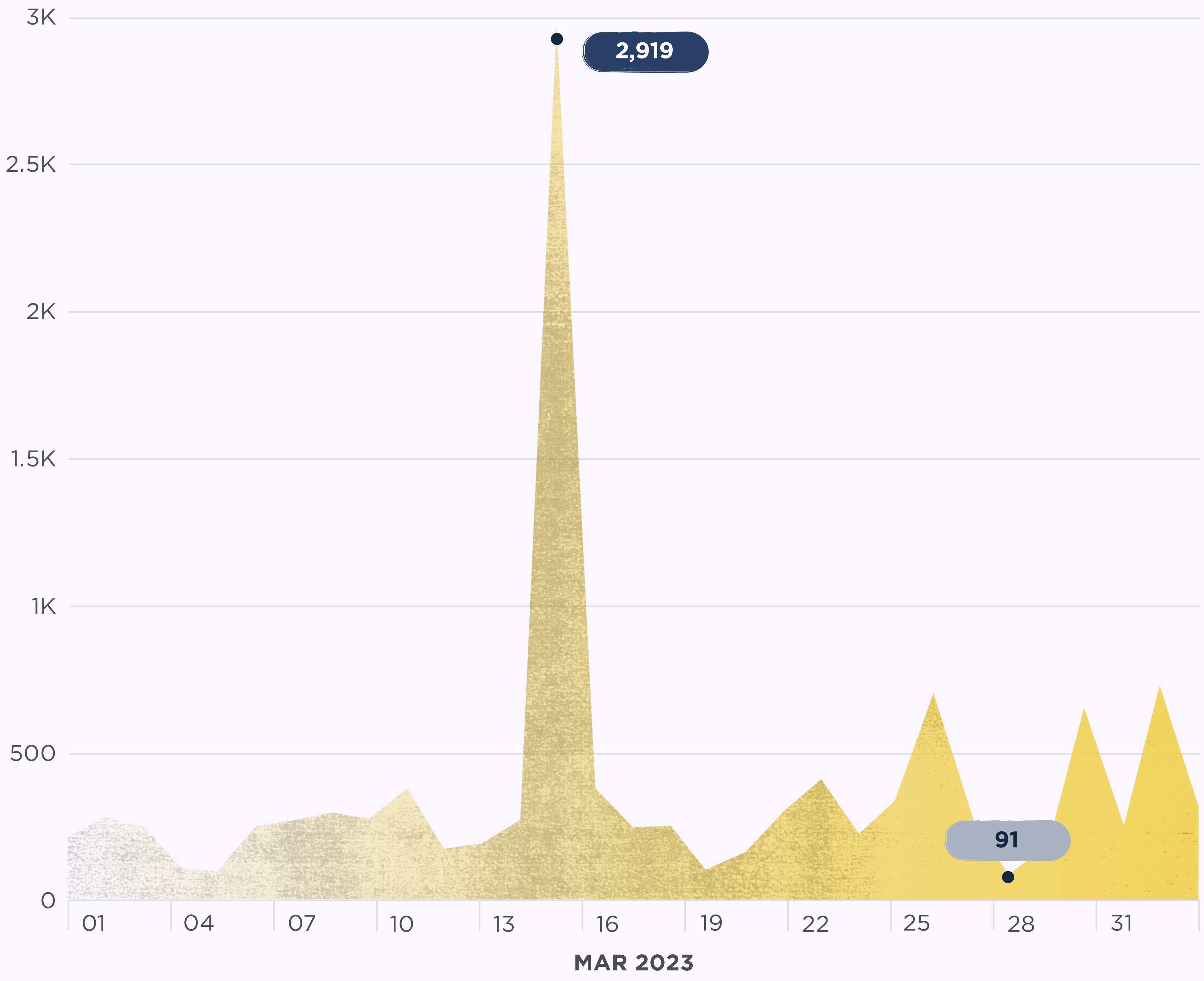
IOCs relating to Mirai

1,711%

Increase month on 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.



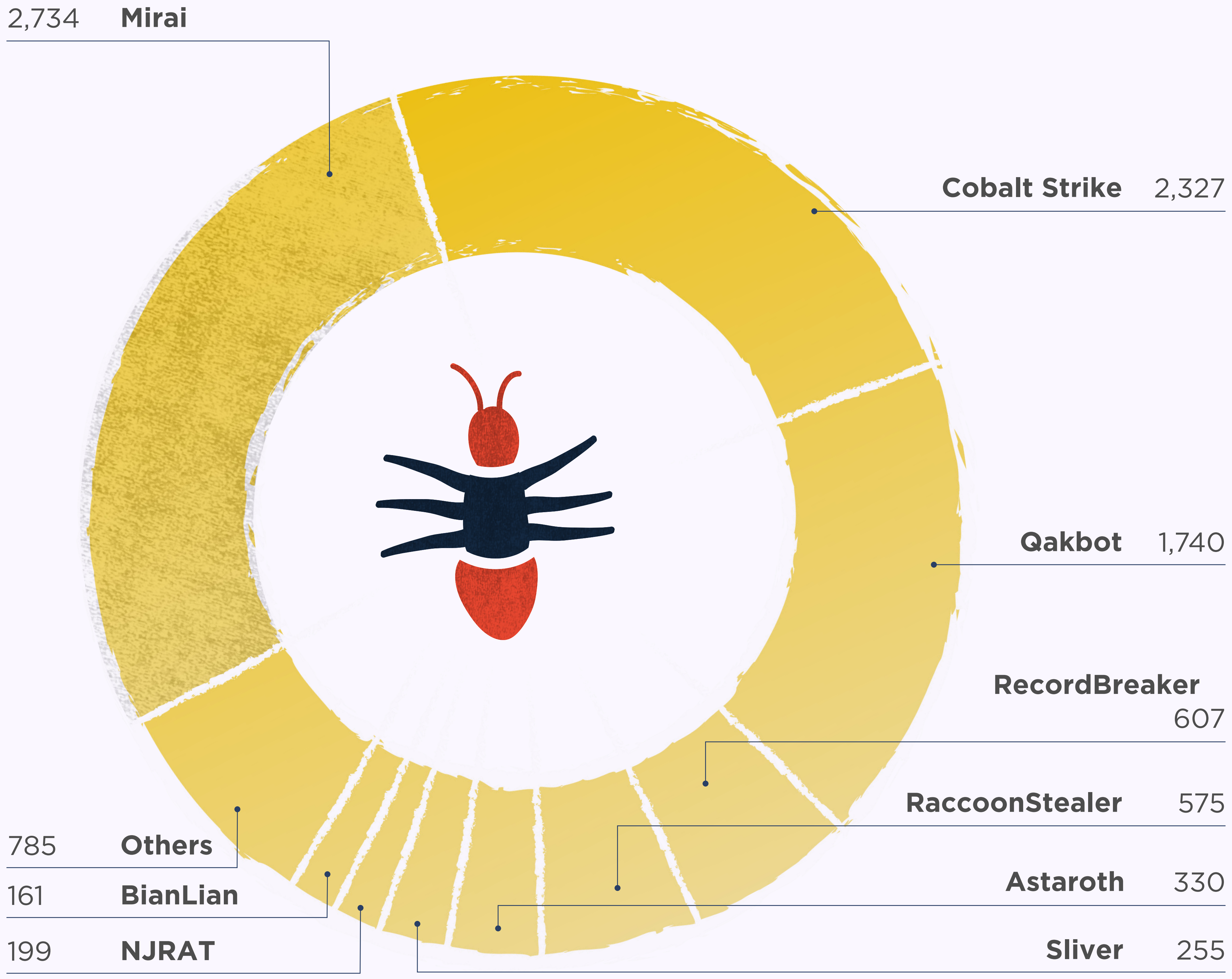
IOC TYPE

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	6,378	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
02	2,478	url	botnet_cc	URL that is used for botnet Command&control (C&C)
03	1,478	url	payload_delivery	URL that delivers a malware payload
04	650	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
05	267	sha256_hash	payload	SHA256 hash of a malware sample (payload)
06	203	domain	payload_delivery	Domain name that delivers a malware payload
07	74	md5_hash	payload	MD5 hash of a malware sample (payload)
08	31	ip:port	payload_delivery	ip:port combination that delivery a malware payload
09	11	sha1_hash	payload	SHA1 hash of a malware sample (payload)
10	1	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.



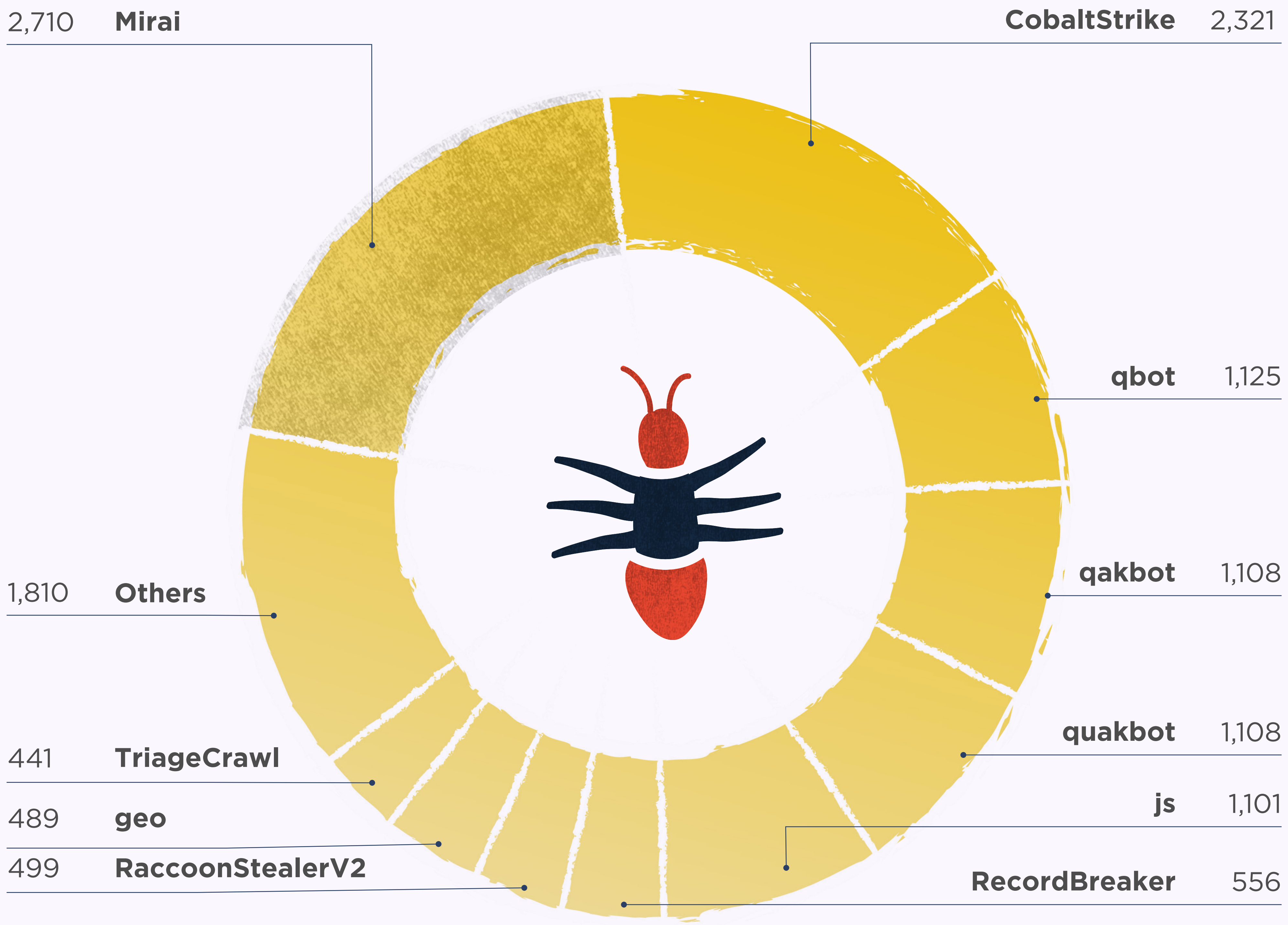
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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	Mirai	︽ +1,710.60		2,734
02	RecordBreaker	︽ +507.00		607
03	RaccoonStealer	︽ +146.78		575
04	Astaroth	︽ +142.65		330
05	BianLian	︿ +26.77		161
06	IcedID	︿ +24.17		149
07	Cobalt Strike	﹀ -2.47		2,327
08	RedLineStealer	﹀ -14.04		147
09	Stealc	﹀ -23.66		100
10	AuroraStealer	︾ -43.96		116
11	Qakbot	︾ -46.87		1,740
12	Sliver	— New entry		255
13	NJRAT	— New entry		199
14	ISFB	— New entry		149
15	RemcosRAT	— New entry		124

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	RecordBreaker	102.18	556
02	CobaltStrike	-2.72	2,321
03	qbot	-61.10	1,125
04	qakbot	-61.99	1,108
05	tr	-87.02	353
06	Mirai	— New entry	2,710
07	quakbot	— New entry	1,108
08	js	— New entry	1,101
09	RaccoonStealerV2	— New entry	499
10	geo	— New entry	489
11	TriageCrawl	— New entry	441
12	BB20	— New entry	430
13	cs-watermark -391144938	— New entry	349
14	BB21	— New entry	345
15	BRA	— New entry	333

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

2,557,200

File scans conducted on YARAify

+10%

increase in file scans on the previous month

2,155,576

Distinct files that had scans performed on them

+11.8%

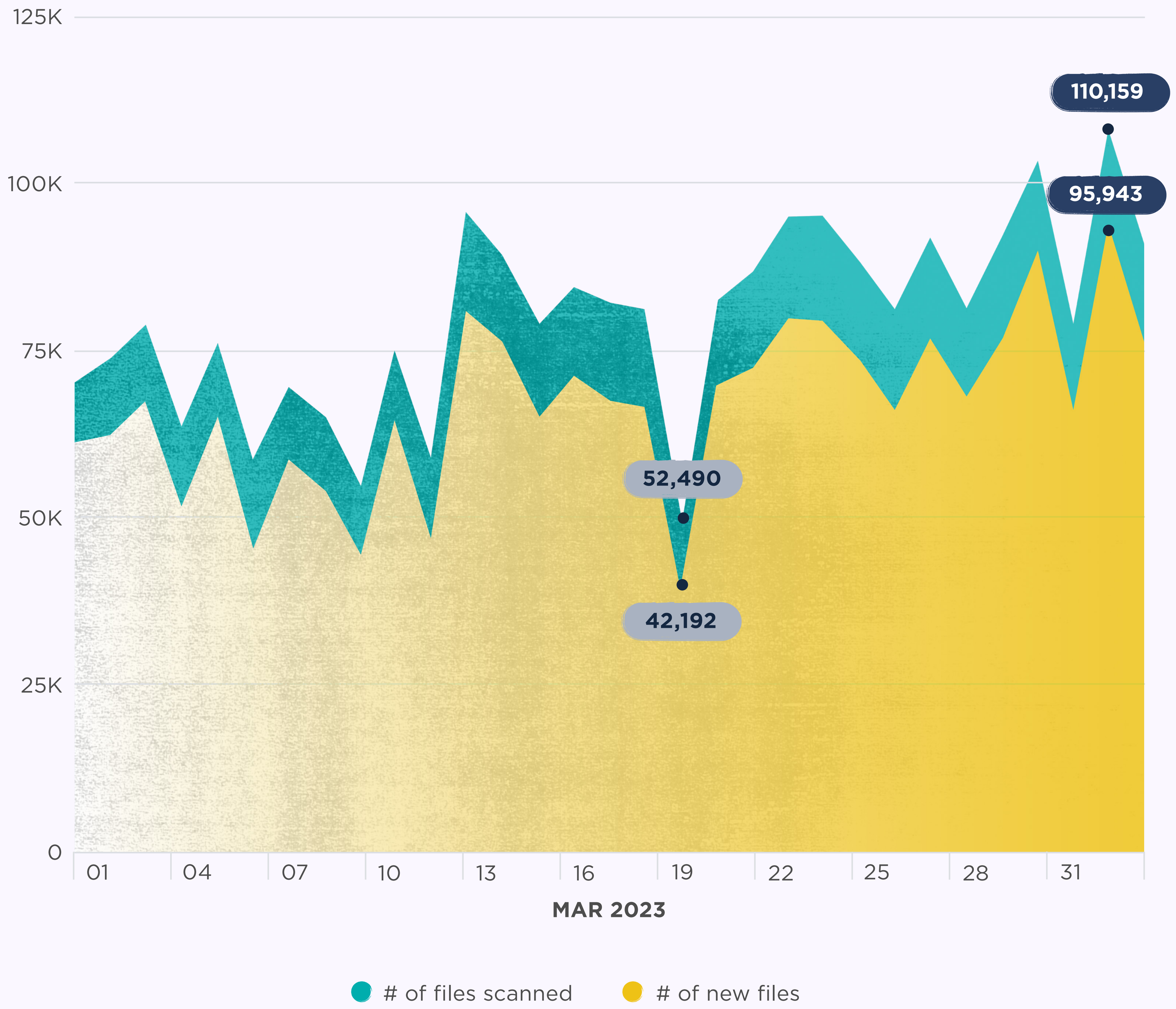
increase in files on the previous month

14,819

YARA rules deployed on YARAify and available for hunting

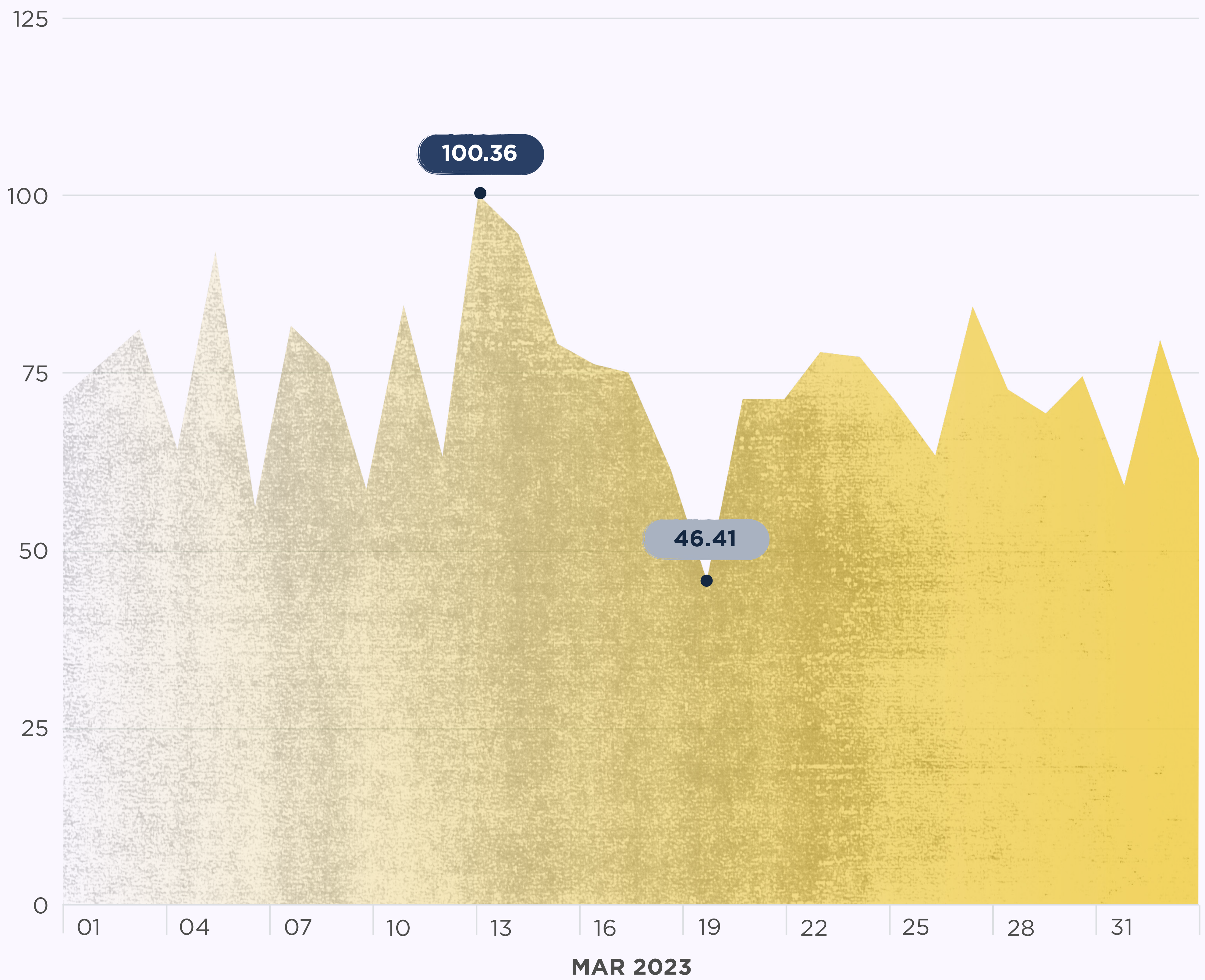
FILES SCANNED PER DAY

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	77,424	New entry	shellcode	nex
02	63,137	+31.91	malware_shellcode_hash	JPCERT/CC
03	61,463	+94.50	win_sality_auto	Felix Bilstein
04	58,688	+275.70	PE_Potentially_Signed_Digital_Certificate	n/a
05	57,108	+14.19	TeslaCryptPackedMalware	n/a
06	54,090	-3.93	BitcoinAddress	@DidierStevens
07	46,127	+41.32	MALWARE_Win_RedLine	ditekSHen
08	41,402	New entry	PE_Digital_Certificate	albertzsigovits
09	40,905	+38.52	INDICATOR_EXE_Packed_MPress	ditekSHen
10	32,430	+63.92	Windows_Trojan_Smokeloader_3687686f	Elastic Security
11	30,756	-24.70	shad0w_beacon_16June	SBousseaden
12	22,438	New entry	RedLine_Campaign_June2021	bartblaze
13	20,229	+16.33	SUSP_XORed_URL_in_EXE_RID2E46	n/a
14	19,884	+25.84	SUSP_XORed_URL_in_EXE	Florian Roth
15	19,810	-36.24	Disable_Defender	iam-py-test

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	195,010	New entry	Win.Malware.Dqqw-9951425-0
02	194,736	New entry	Win.Malware.Zusy-6804618-0
03	194,735	New entry	Win.Trojan.QQPass-5710308-0
04	110,335	+93.41	PUA.Win.Packer.Lccwin-2
05	81,404	+43.75	PUA.Win.Packer.AcprotectUltraprotect-1
06	73,840	+150.44	Win.Trojan.Obfus-38
07	57,692	+65.99	Win.Trojan.Qukart-6874817-0
08	50,391	+46.95	PUA.Win.Packer.Embedpe-3
09	48,208	+56.38	PUA.Win.Packer.Ep-7
10	45,154	+50.88	Win.Malware.Qukart-6838239-0
11	43,265	+58.85	Win.Malware.Scar-9946848-0
12	42,366	+58.50	PUA.Win.Packer.Acprotect-4
12	42,366	+58.50	PUA.Win.Packer.Acprotect-3
13	42,365	+58.50	PUA.Win.Packer.AcprotectUltrap-1
13	42,365	+58.50	PUA.Win.Packer.Acprotect-2

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN MAY

Remember, sharing is caring.