SEPTEMBER 2022

SPAMHAUS ABUSE|ch

MONTHLY MALWARE DIGEST

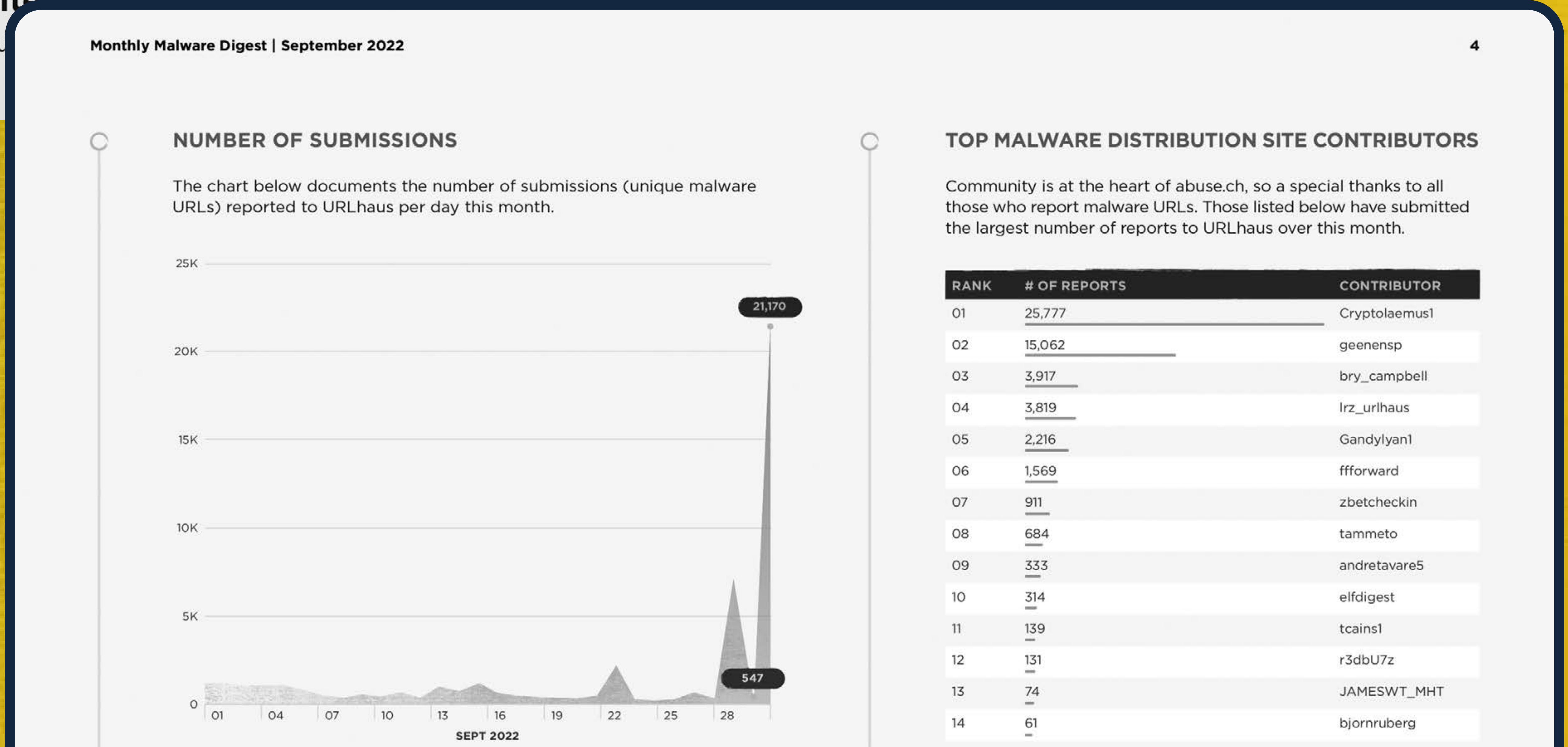
In this report, we highlight malware trends utilizing data from abuse.ch's open platforms. These collect, track and share resources relating to malware campaigns, including the URLs of malware distribution sites, malware samples, and indicators of compromise.

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.

57,227

Malware sites

shared by secu
on URLhaus



Monthly Malware Digest | September 2022 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	CONTRIBUTOR
01	25,777	Cryptolaemus1
02	15,062	geenensp
03	3,917	bry_campbell
04	3,819	lrz_urlhaus
05	2,216	Gandylyan1
06	1,569	ffforward
07	911	zbetcheckin
08	684	tammeto
09	333	andretavare5
10	314	elfdigest
11	139	tcains1
12	131	r3dbU7z
13	74	JAMESWT_MHT
14	61	bjornruberg

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

Malware Bazaar

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/

Malware Bazaar

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

57,227

Malware sites

shared by security researchers on URLhaus

45,028

Abuse reports

sent out to hosting providers and network owners

70%

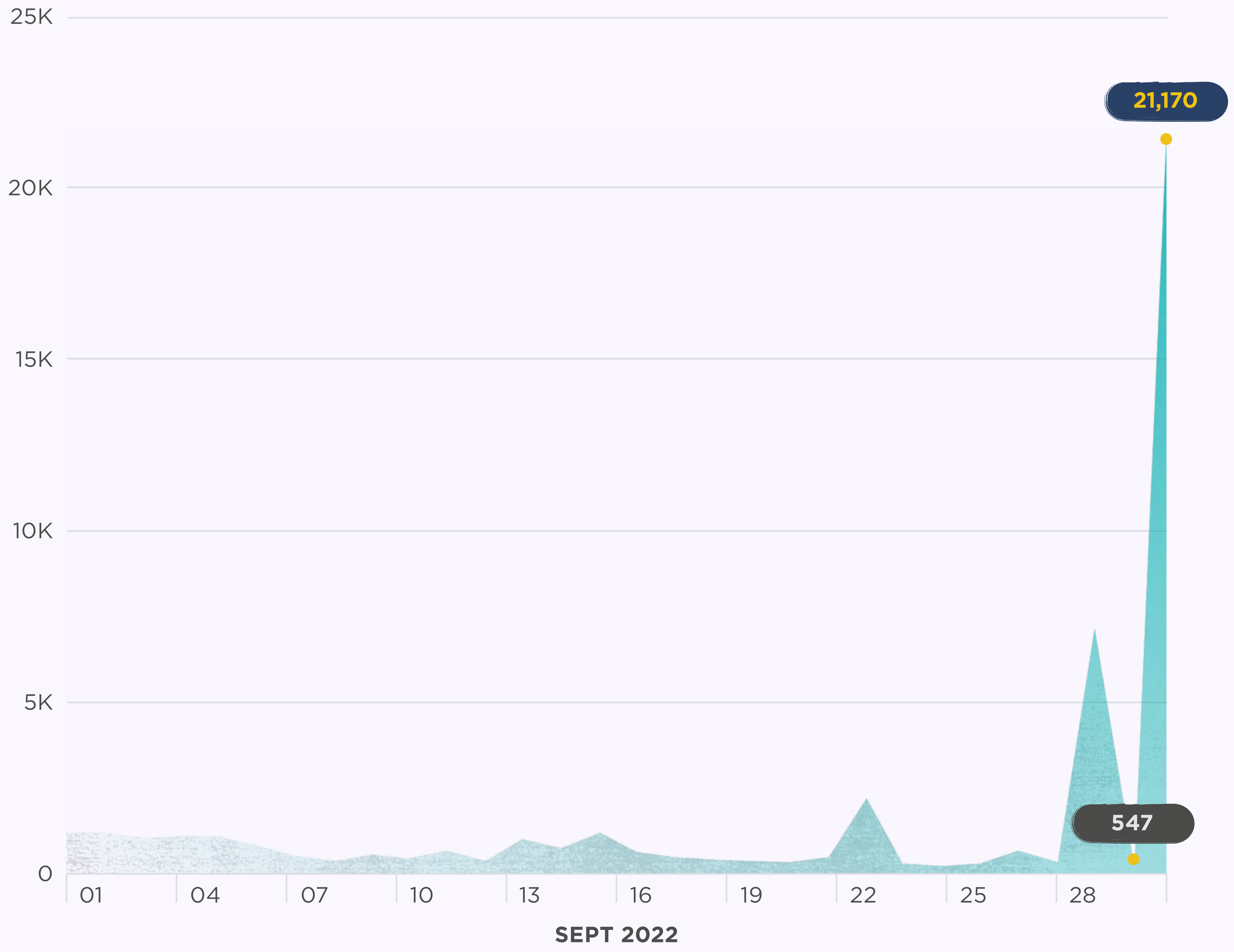
of abuse reports have been acted upon

138.9%

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.

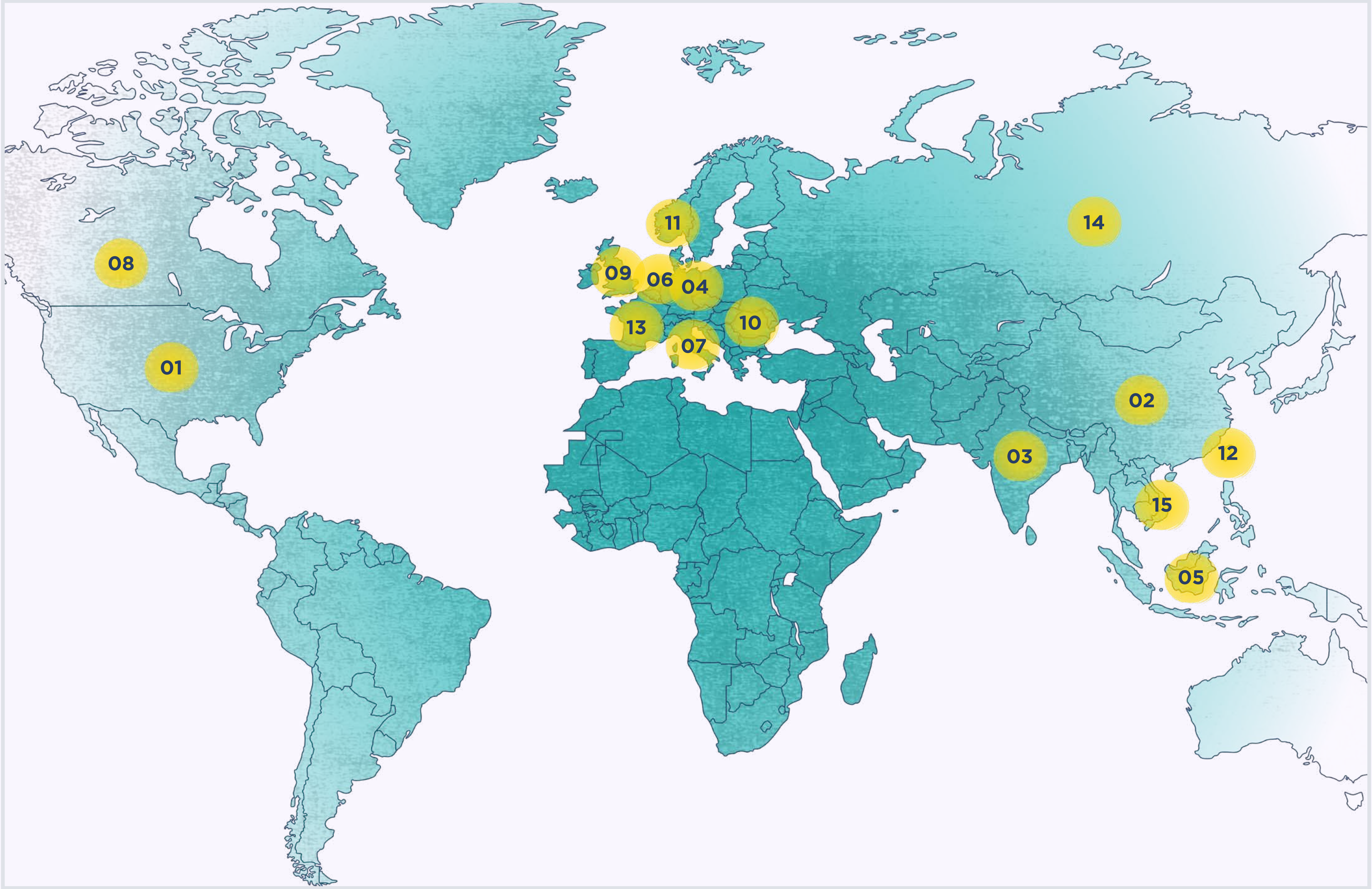


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	25,777	Cryptolaemus1
02	15,062	geenensp
03	3,917	bry_campbell
04	3,819	lrz_urlhaus
05	2,216	Gandylyan1
06	1,569	ffforward
07	911	zbetcheckin
08	684	tammeto
09	333	andretavare5
10	314	elfdigest
11	139	tcains1
12	131	r3dbU7z
13	74	JAMESWT_MHT
14	61	bjornruberg
15	50	tcains2

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	COUNTRY
01	23,264	United States
02	7,505	China
03	5,750	India
04	1,030	Germany
05	1,009	Indonesia
06	809	Netherlands
07	512	Italy
08	500	Canada
09	485	United Kingdom
10	430	Romania
11	421	Norway
12	406	Taiwan
13	376	France
14	372	Russia
15	316	Vietnam

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	12,770	AS46606	UNIFIEDLAYER	United States
02	3,732	AS4134	CHINANET	China
03	3,593	AS4837	CHINA169	China
04	3,063	AS9829	BSNL-NIB	India
05	2,834	AS394695	PUBLIC-DOMAIN-REGISTRY	United States
06	937	AS22612	NAMECHEAP	United States
07	889	AS211252	DELIS	Netherlands
08	871	AS13335	CLOUDFLARE	United States
09	855	AS36352	COLOCROSSING	United States
10	630	AS16276	OVH	France
11	618	AS24940	HETZNER	Germany
12	502	AS23352	SERVERCENTRAL	United States
13	487	AS19871	NETWORK-SOLUTIONS	United States
14	444	AS53755	IOFLOOD	United States
15	409	AS26337	OIS1	United States

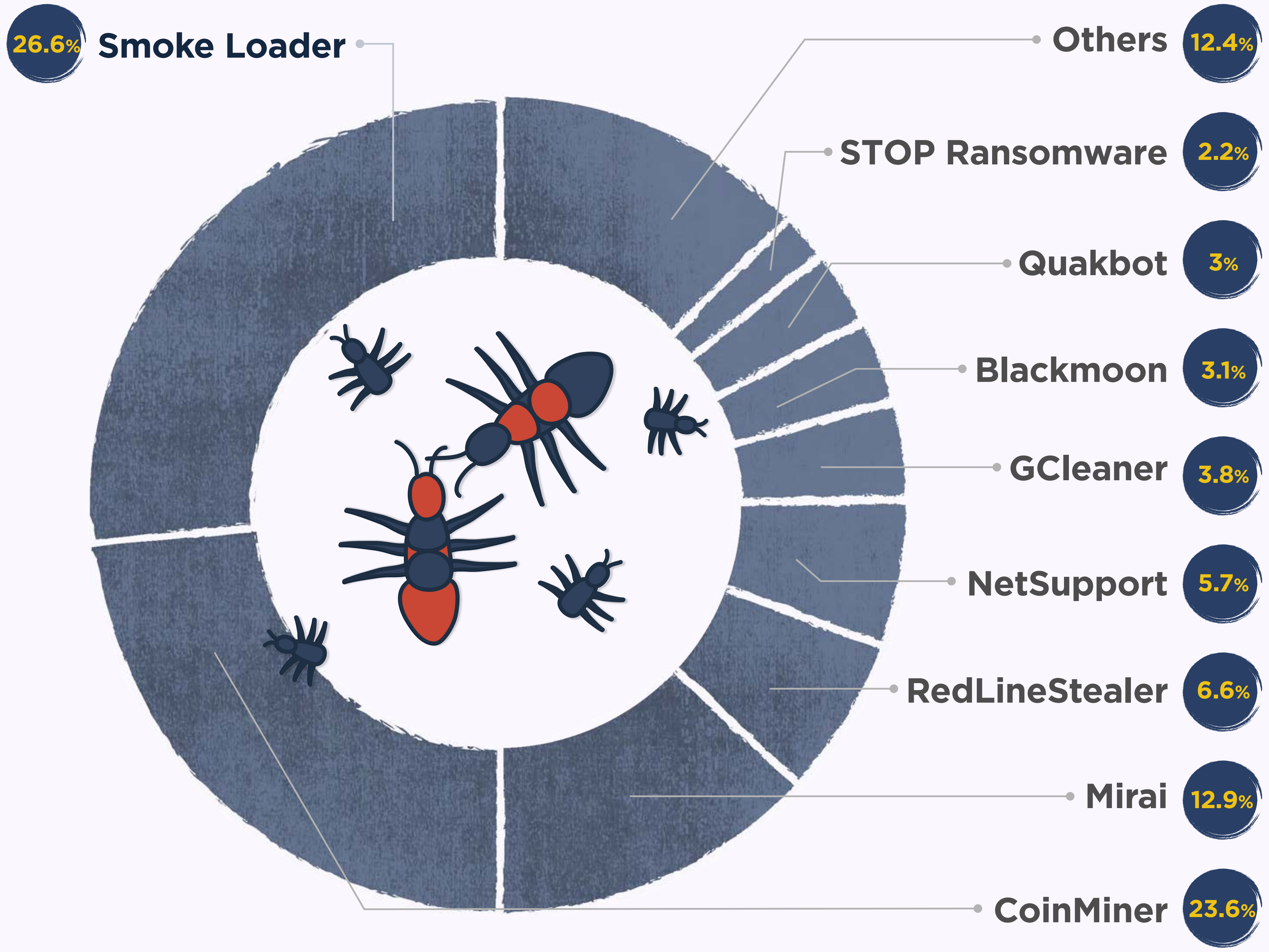
TOP MALWARE HOSTS

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	1,455	drive.google.com	Google	United States
02	465	81.161.229.110	Severion	Netherlands
03	278	vk.com	VKontakte	Russia
04	175	45.155.165.62	Severion	Netherlands
05	93	onedrive.live.com	Microsoft	United States
06	52	46.19.141.122	Private Layer	China
07	48	cdn.discordapp.com	Discord	United States
08	46	194.38.23.170	NT Service	Ukraine
09	43	195.178.120.115	Severion	Netherlands
10	30	81.161.229.7	Severion	Netherlands
11	28	185.216.71.116	Severion	Netherlands
12	28	81.161.229.46	Severion	Netherlands
13	28	45.138.16.201	1337 Services GmbH	Germany
14	27	79.110.62.20	Severion	Netherlands
15	26	46.23.109.212	Severion	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 SAMPLES
01	196%	GCleaner	370
02	93.26%	Gafgyt	172
03	82.02%	DanaBot	162
04	37.38%	NetSupport	555
05	20.59%	Mirai	1265
06	8.40%	ArkeiStealer	142
07	-0.99%	Smoke Loader	2598
08	-7.89%	SnakeKeylogger	70
09	-20.15%	AgentTesla	107
10	-30.70%	RedLineStealer	648
11	-34.55%	Blackmoon	305
12	-43.85%	Fabookie	105
13	-44.23%	CoinMiner	2306
14	-61.76%	RemcosRAT	52
15	-86.34%	RecordBreaker	183

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

11,530

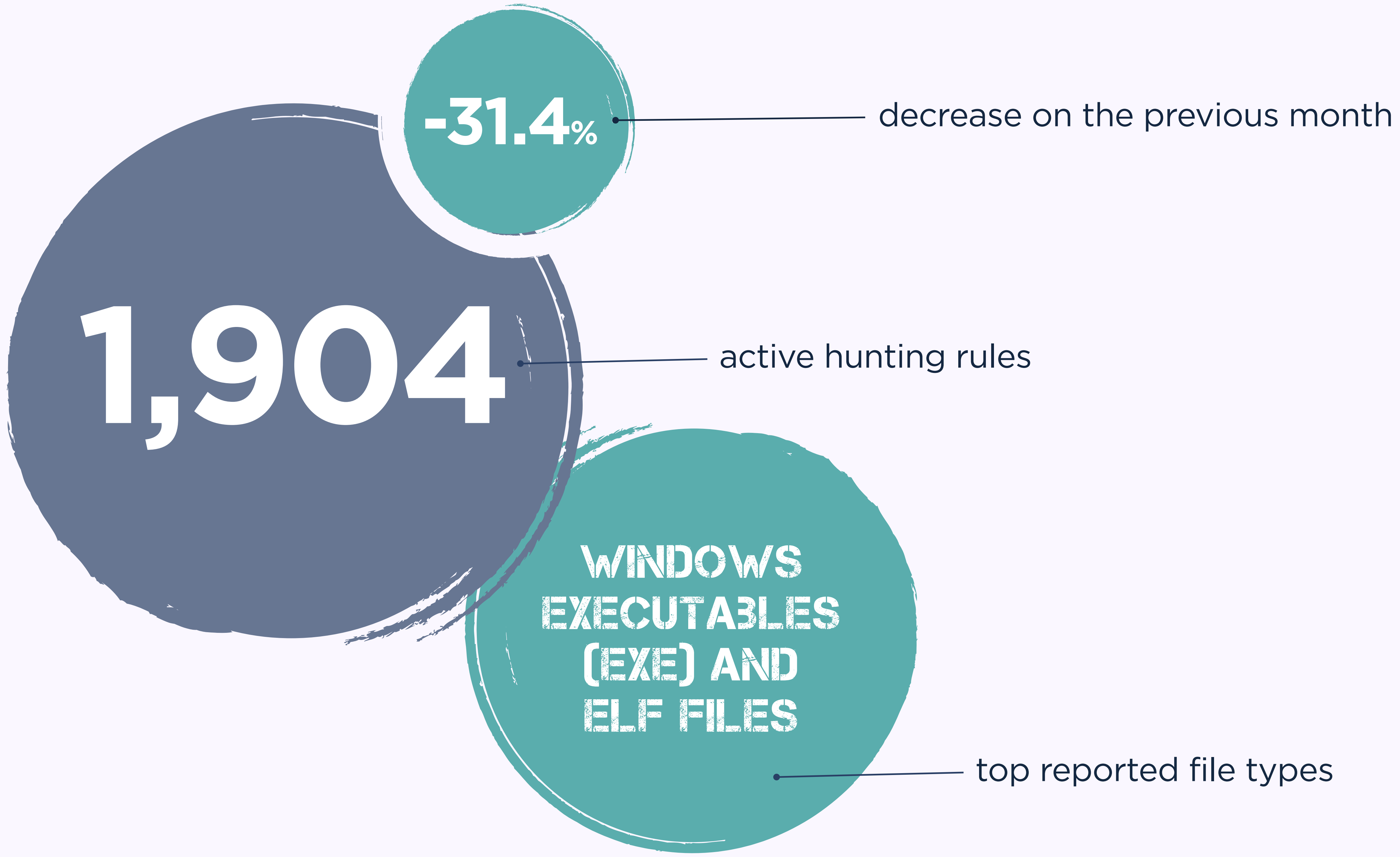
Malware samples

shared by security researchers on MalwareBazaar

1.1MB

Average size

of a malware sample



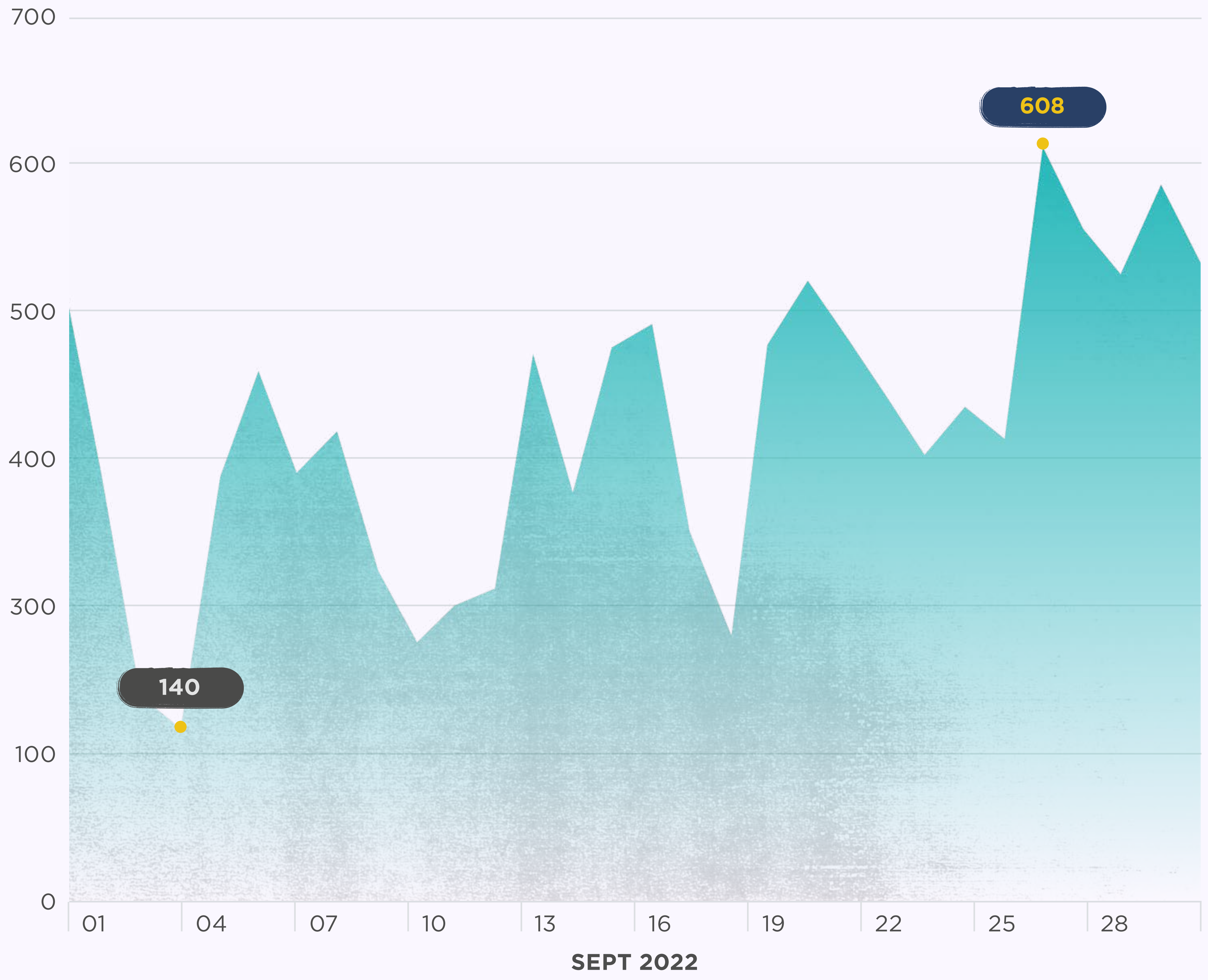
-31.4% decrease on the previous month

1,904 active hunting rules

WINDOWS EXECUTABLES (EXE) AND ELF FILES top reported file types

MALWARE SAMPLES

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



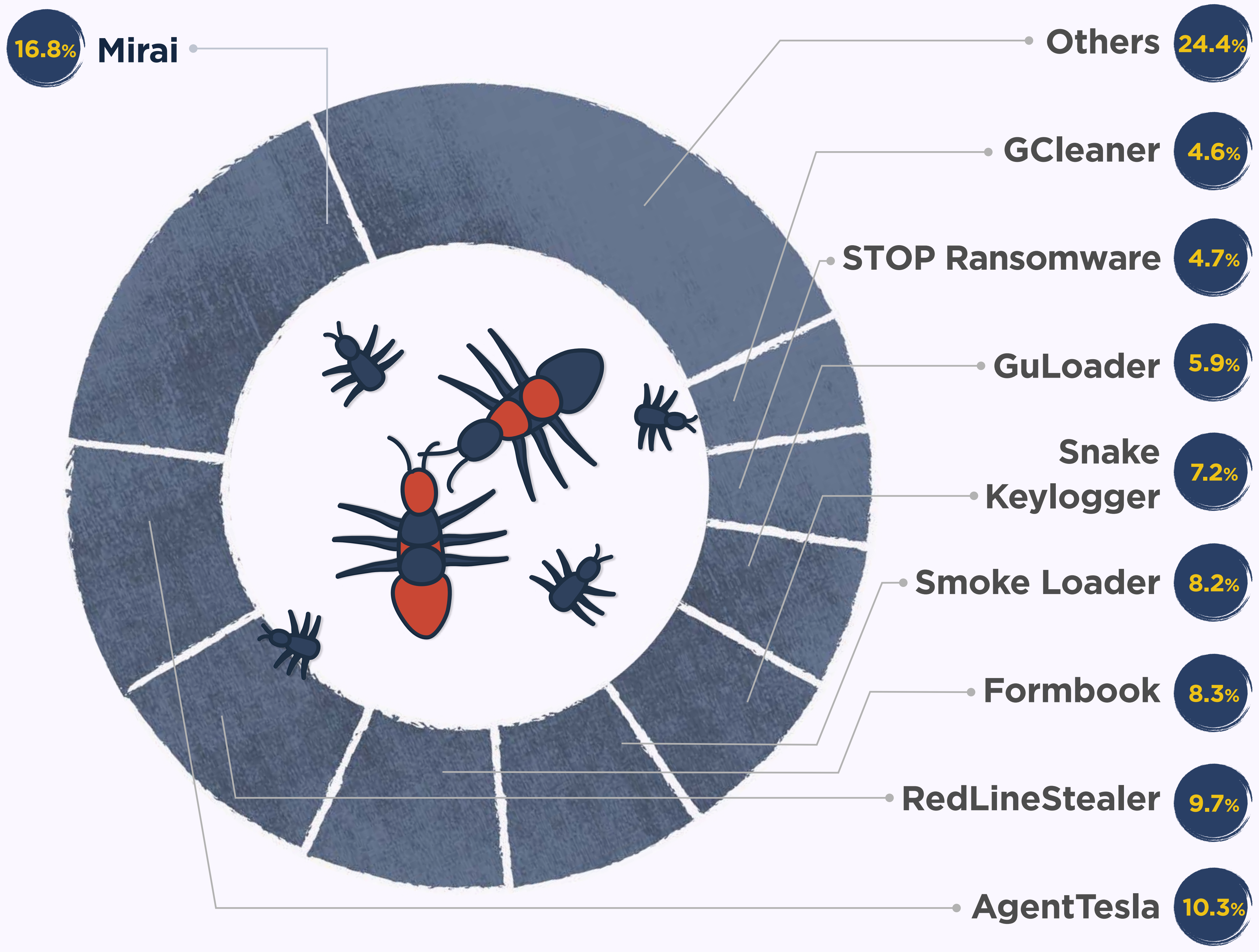
TOP SAMPLE CONTRIBUTORS

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	CONTRIBUTOR
01	1,898	@andretavare5
02	1,438	@zbetcheckin
03	832	@SecuriteInfoCom
04	479	@JAMESWT_MHT
05	452	@GovCERT_CH
06	440	@elfdigest
07	315	@cocaman
08	281	@petikvx
09	272	@lowmal3
10	249	@TeamDreier
11	201	@0xToxin
12	189	@adrian__luca
13	169	@pr0xylife
14	134	@malwarelabnet
15	127	@James_inthe_box

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



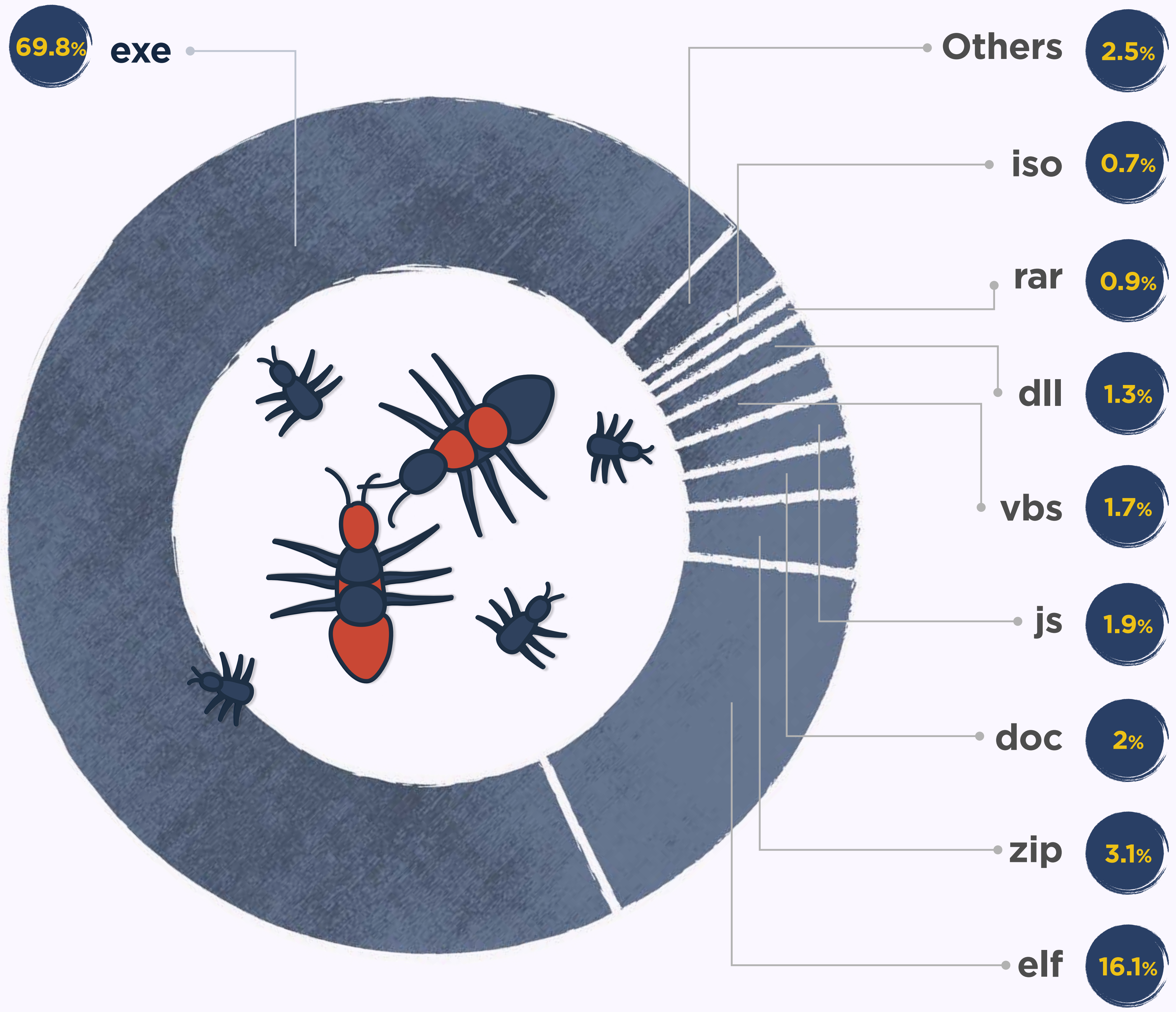
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	173.75%	Smoke Loader	657
02	131.68%	Stop Ransomware	373
03	54.90%	GuLoader	474
04	28.57%	ArkeiStealer	162
05	18.07%	IcedID	281
06	8.18%	Loki	291
07	5.12%	RedLineStealer	780
08	0.63%	DCRat	159
09	-4.97%	SnakeKeylogger	574
10	-16.57%	Mirai	1,344
11	-17.97%	AgentTesla	826
12	-26.22%	Formbook	667
13	-31.18%	AveMariaRAT	128
14	-32.65%	AsyncRAT	132
15	-49.13%	RemcosRAT	233

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	788	myMirai	n/a
02	698	linux_generic_ipv6_catcher	@_lubiedo
03	692	unixredflags3	@timb_machine
04	566	cobalt_strike_tmp01925d3f	The DFIR Report
05	538	win_smokeloader_a2	pnx
06	370	win_nymaim_g0	CERT.pl
07	368	MALWARE_Win_RedLine	ditekshen
08	337	setsockopt	@timb_machine
09	314	SUSP_XORed_URL_in_EXE_RID2E46	Florian Roth
10	314	SUSP_XORed_URL_in_EXE	Florian Roth
11	285	win_stop_auto	Felix Bilstein
12	285	MALWARE_Win_STOP	ditekSHen
13	270	INDICATOR_SUSPICIOUS_Binary_References_Browsers	ditekSHen
14	222	SUSP_XORed_Mozilla_RID2DB4	Florian Roth
15	222	SUSP_XORed_Mozilla	Florian Roth

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.

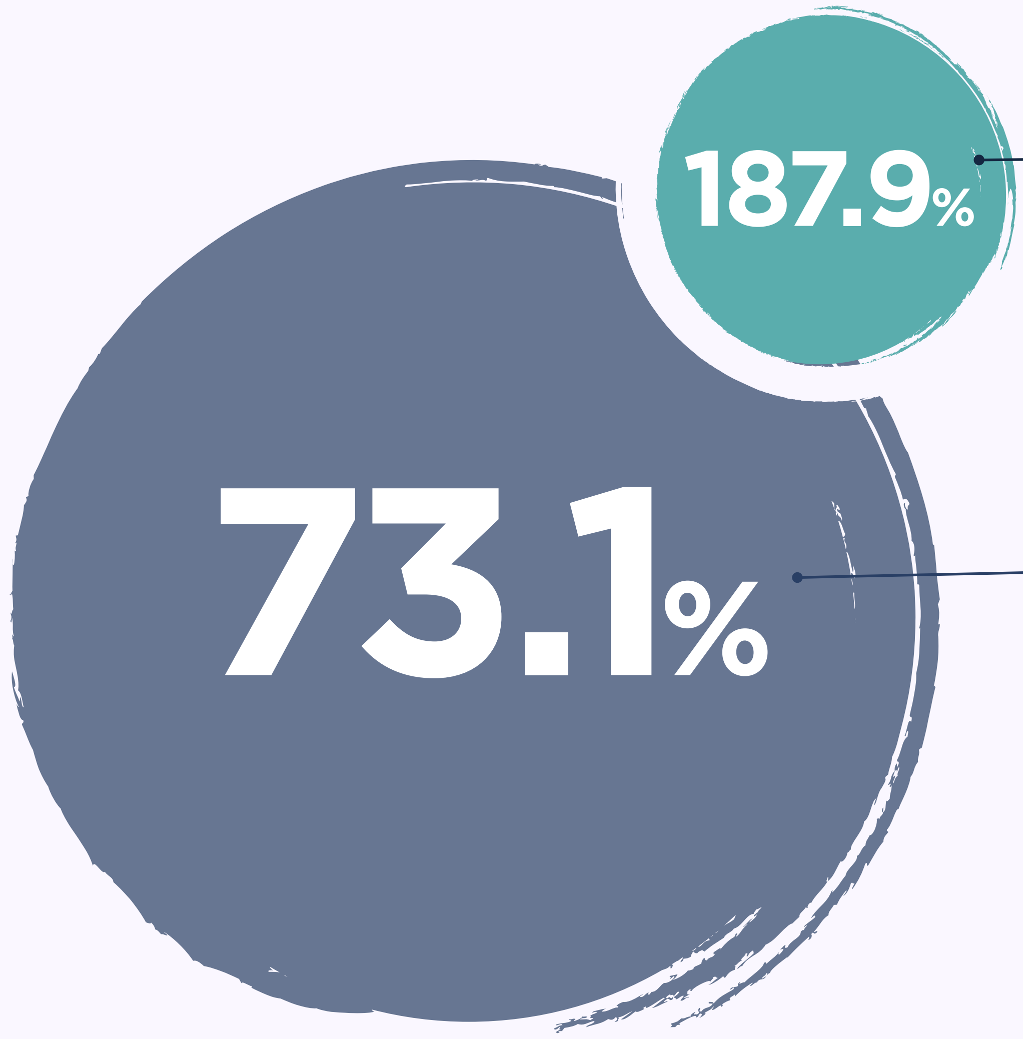
Explore ThreatFox

INDICATERS OF COMPROMISE (IOCs)

17,910

Indicators of compromise (IOCs)

shared on ThreatFox

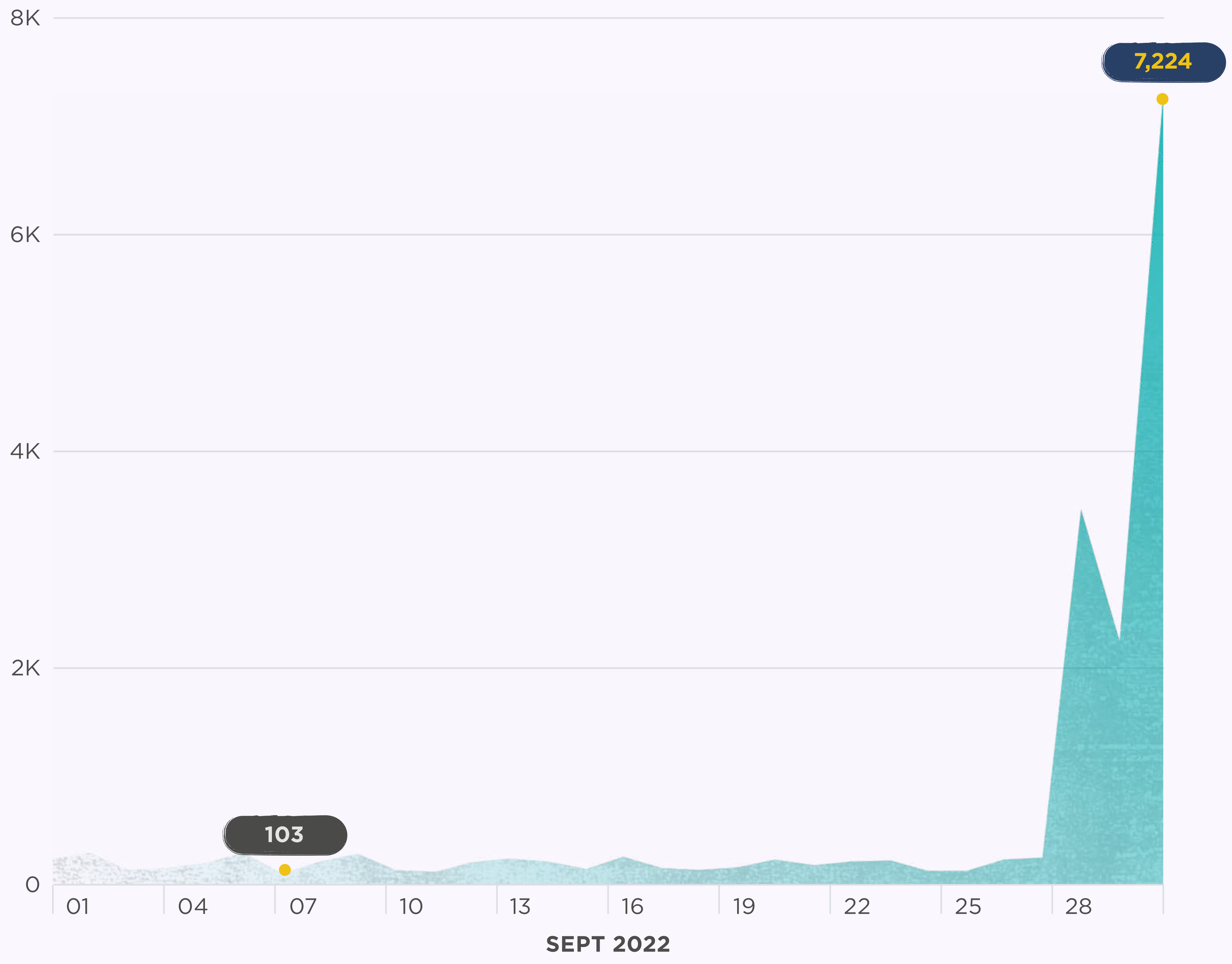


187.9% increase on the previous month

73.1% percentage of IOCs relating to Quakbot

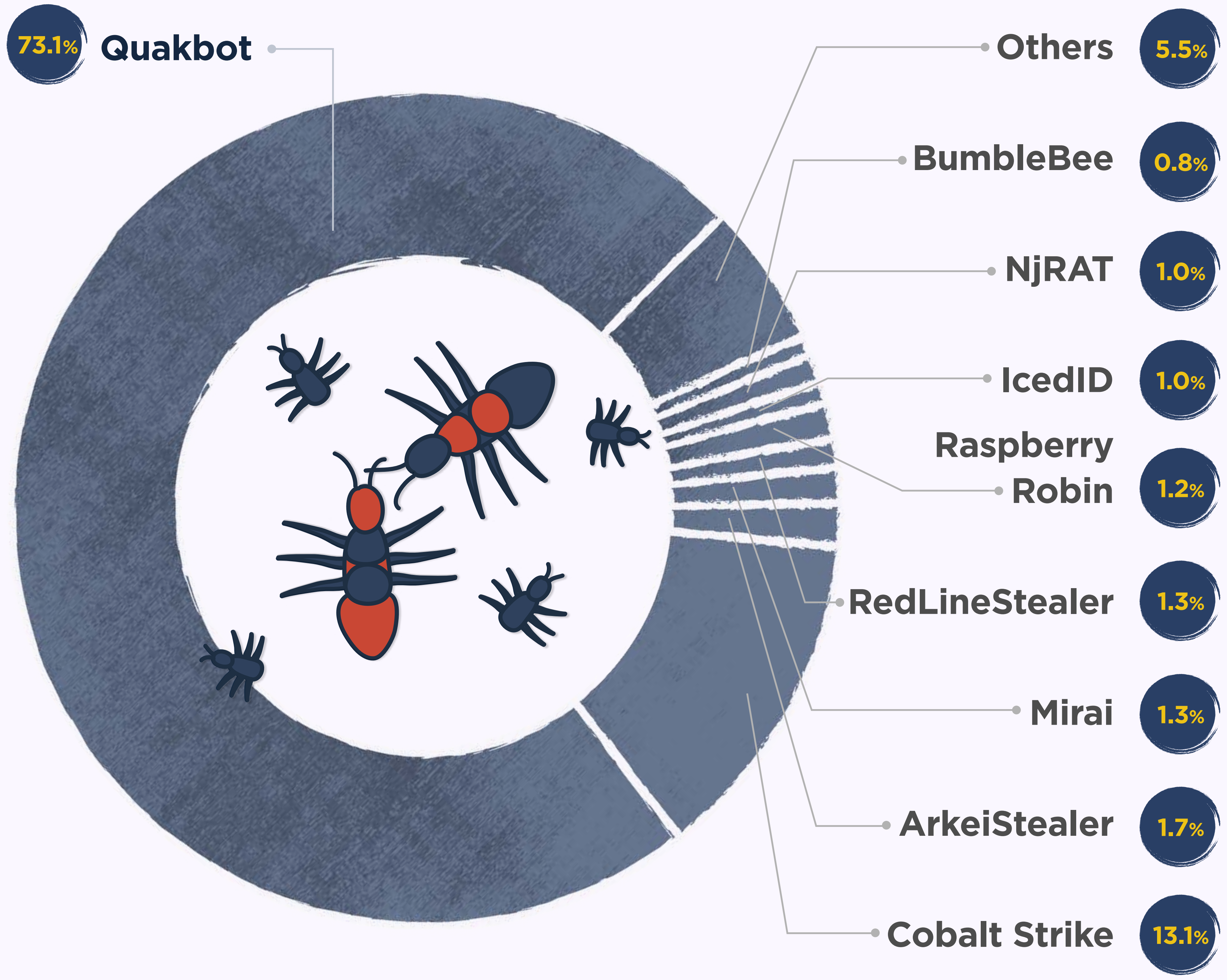
NUMBER OF IOCs SHARED PER DAY

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



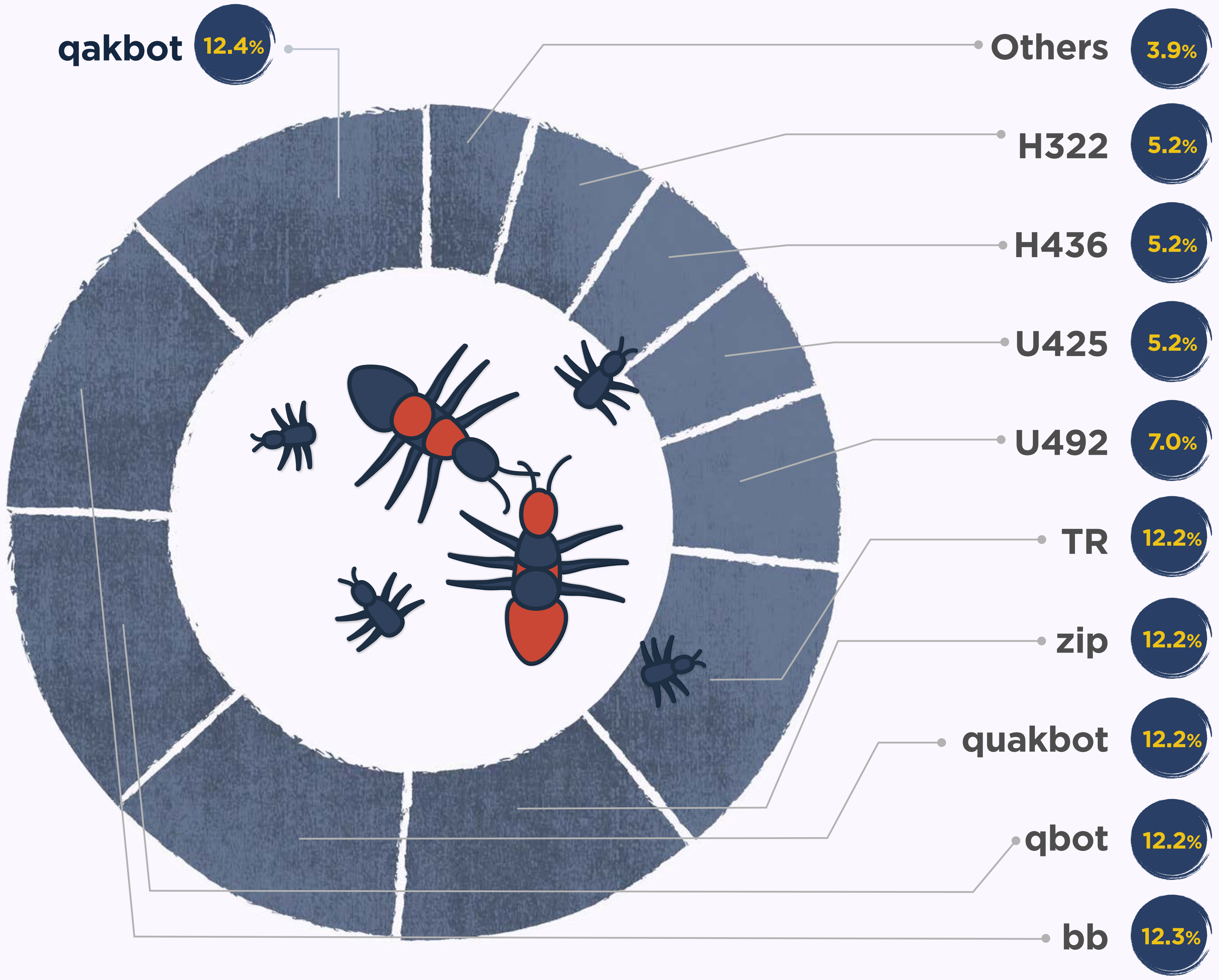
TOP MALWARE FAMILIES

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	12,147	url	payload_ delivery	URL that delivers a malware payload
02	2,557	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
03	2,217	url	botnet_cc	URL that is used for botnet Command&control (C&C)
04	380	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
05	269	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
06	158	md5_hash	payload	MD5 hash of a malware sample (payload)
07	151	domain	payload_ delivery	Domain name that delivers a malware payload
08	31	ip:port	payload_ delivery	ip:port combination that delivery a malware payload

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

2,206,463

File scans

conducted on YARAify

1,856,394

Distinct files

that had scans performed on them

4,304

YARA rules

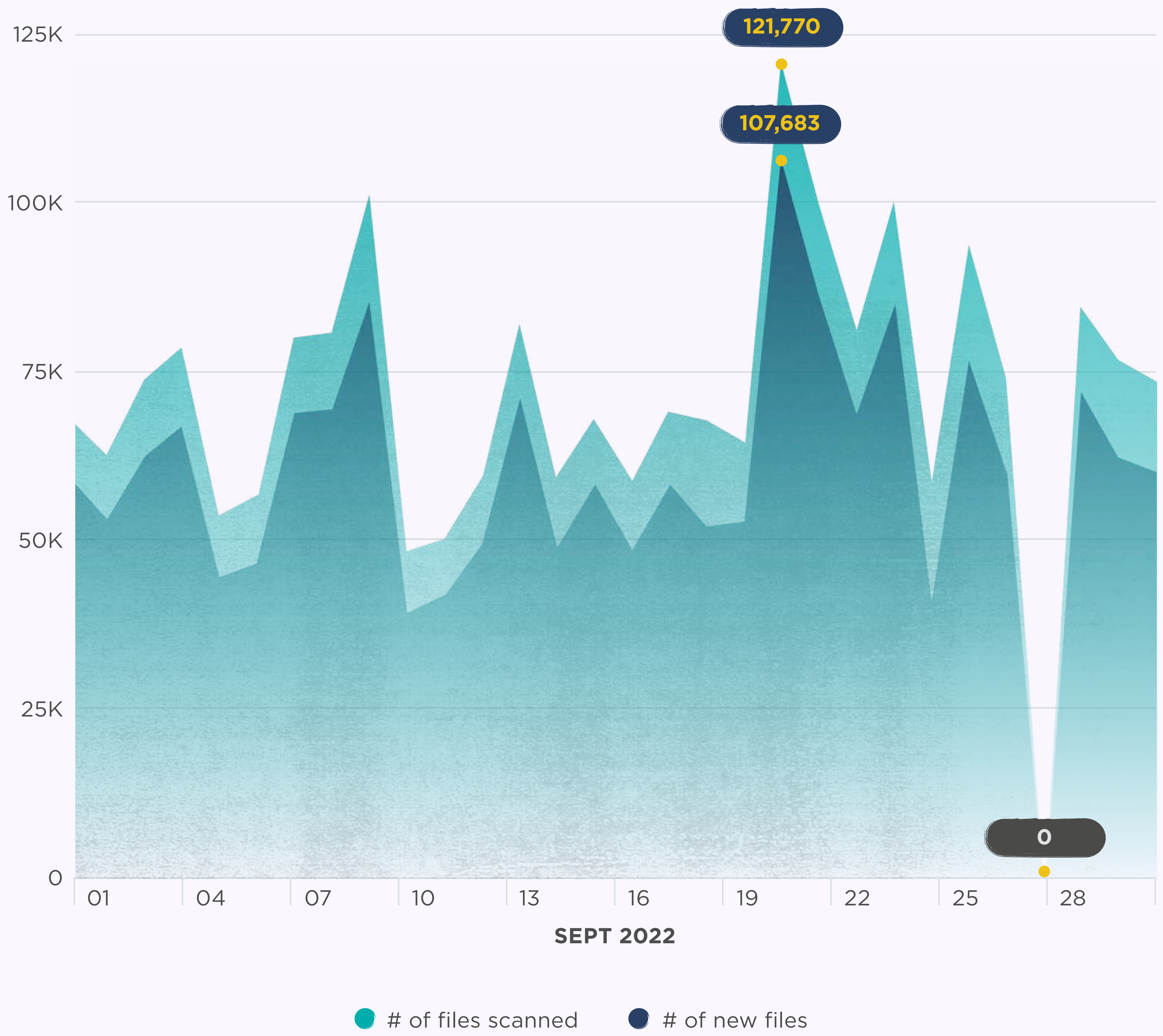
deployed on YARAify and available for hunting

-1.2% reduction in distinct files on the previous month

-2.2% decrease in file scans on the previous month

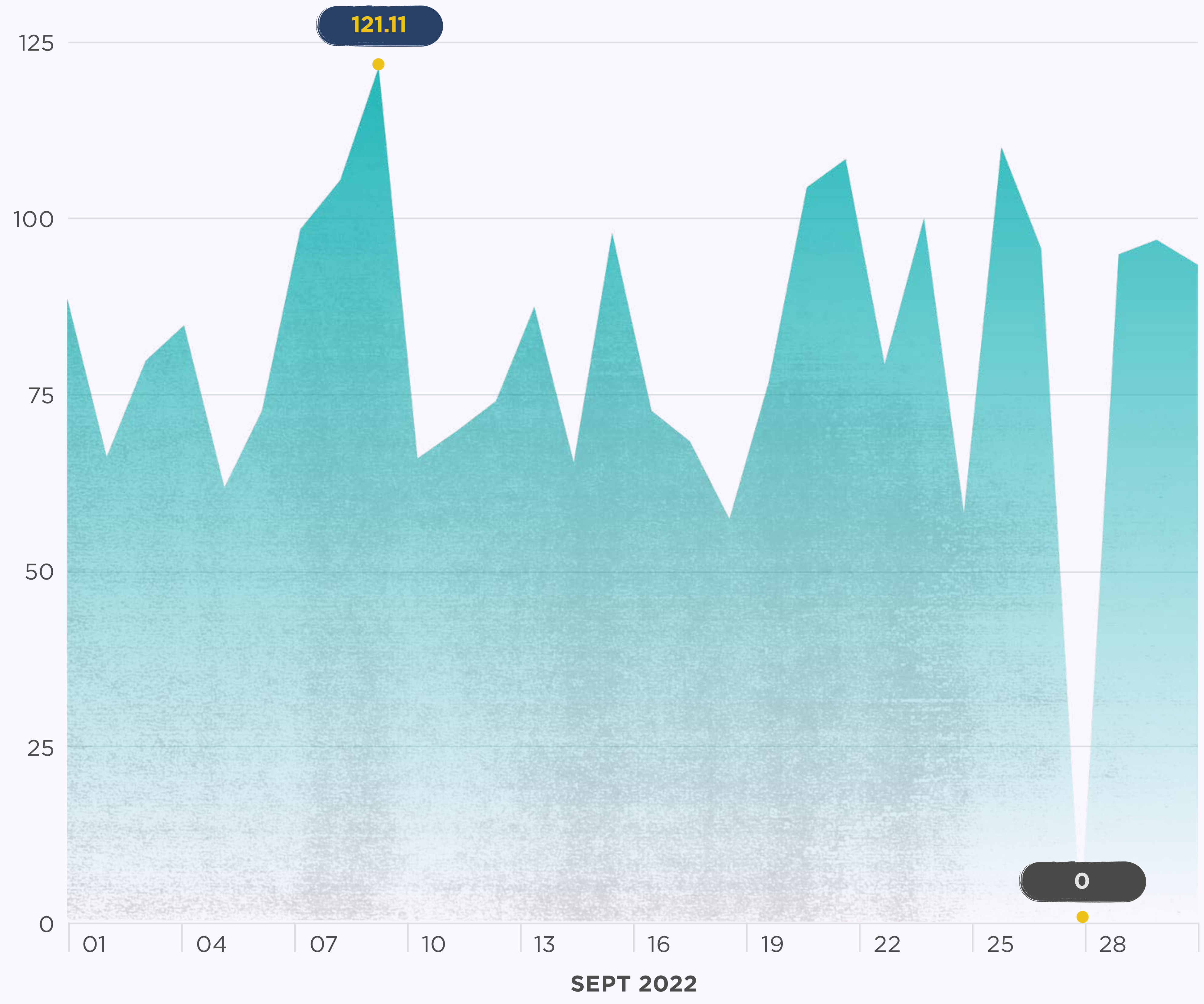
FILES SCANNED PER DAY

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	68,369	command_and_control	CD_R0M_
02	43,116	win_win_sality_auto	Felix Bilstein
03	24,758	INDICATOR_EXE_Packed_MPress	ditekSHen
04	24,462	malware_shellcode_hash	JPCERT/CC
05	24,233	malware_shellcode_hash	JPCERT/CC
06	23,675	MALWARE_Win_RedLine	ditekshen
07	19,357	MAL_XMR_Miner_May19_1	Florian Roth
08	19,357	MAL_XMR_Miner_May19_1_RID2E1B	Florian Roth
09	19,356	cobalt_strike_tmp01925d3f	DFIR Report
10	16,674	AutoIT_Compiled	@bartblaze
11	14,760	win_vobfus_auto	Felix Bilstein
12	14,107	SUSP_XORed_URL_in_EXE_RID2E46	Florian Roth
13	14,107	SUSP_XORed_URL_in_EXE	Florian Roth
14	13,677	SUSP_Websites	ditekSHen
15	13,656	win_xfilesstealer_auto	Felix Bilstein

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	123,469	PUA.Win.Packer.Lccwin-2
02	120,175	PUA.Win.Packer.Upx-4
03	111,643	Win.Trojan.Qukart-6874817-0
04	88,269	Win.Malware.Midie-6847981-0
05	86,574	Win.Malware.Zusy-6878655-0
06	77,638	Win.Trojan.Obfus-38
07	71,660	Win.Malware.Midie-6847893-0
08	67,557	Win.Malware.Midie-6847892-0
09	67,557	Win.Malware.Midie-6848784-0
10	61,864	PUA.Win.Packer.Pequake-4
11	50,166	Win.Malware.Qukart-6838239-0
12	49,819	Win.Malware.Midie-6848630-0
13	48,127	Win.Trojan.Crypted-30
14	47,986	Win.Trojan.Crypted-29
15	44,895	Win.Malware.Midie-6847894-0

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN NOVEMBER

Remember, sharing is caring.