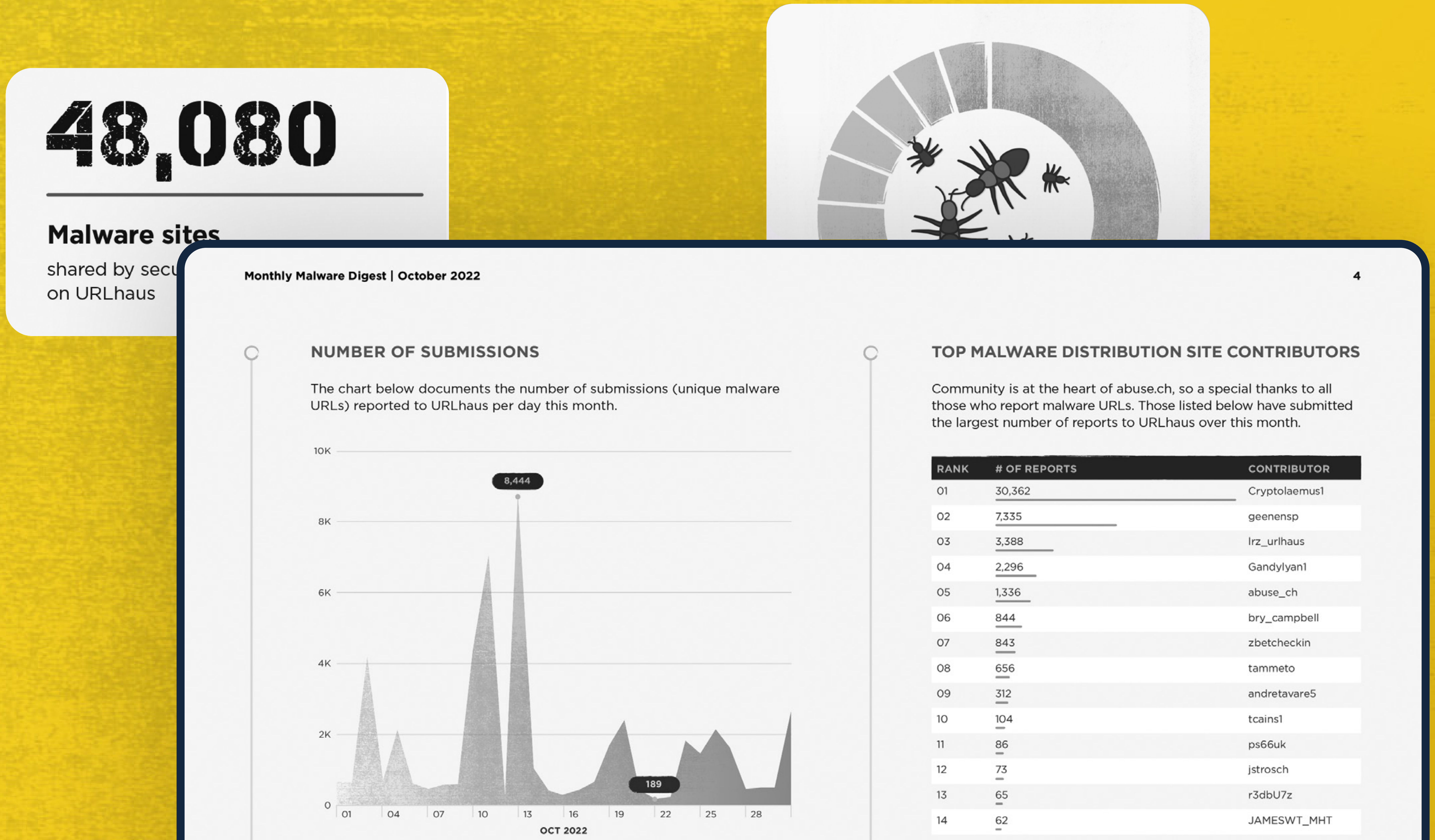
OCTOBER 2022

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.



48,080

Malware sites

shared by secu

on URLhaus

Monthly Malware Digest | October 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	30,362	Cryptolaemus1
02	7,335	geenensp
03	3,388	lrz_urlhaus
04	2,296	Gandylyan1
05	1,336	abuse_ch
06	844	bry_campbell
07	843	zbetcheckin
08	656	tammeto
09	312	andretavare5
10	104	tcains1
11	86	ps66uk
12	73	jstrosch
13	65	r3dbU7z
14	62	JAMESWT_MHT

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

48,080

Malware sites

shared by security researchers on URLhaus

50,455

Abuse reports

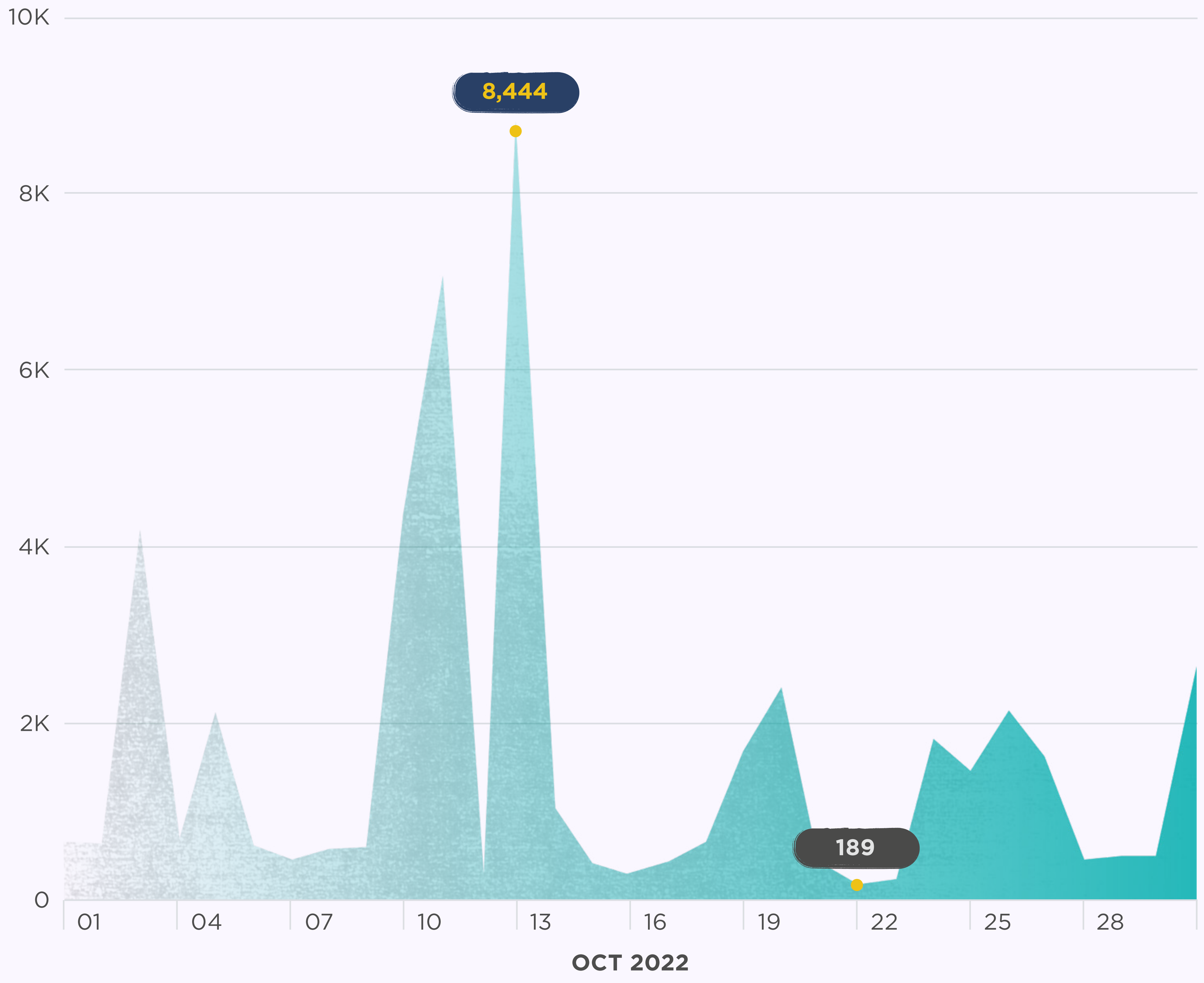
sent out to hosting providers and network owners

54% of abuse reports have been acted upon

-16% decrease 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.

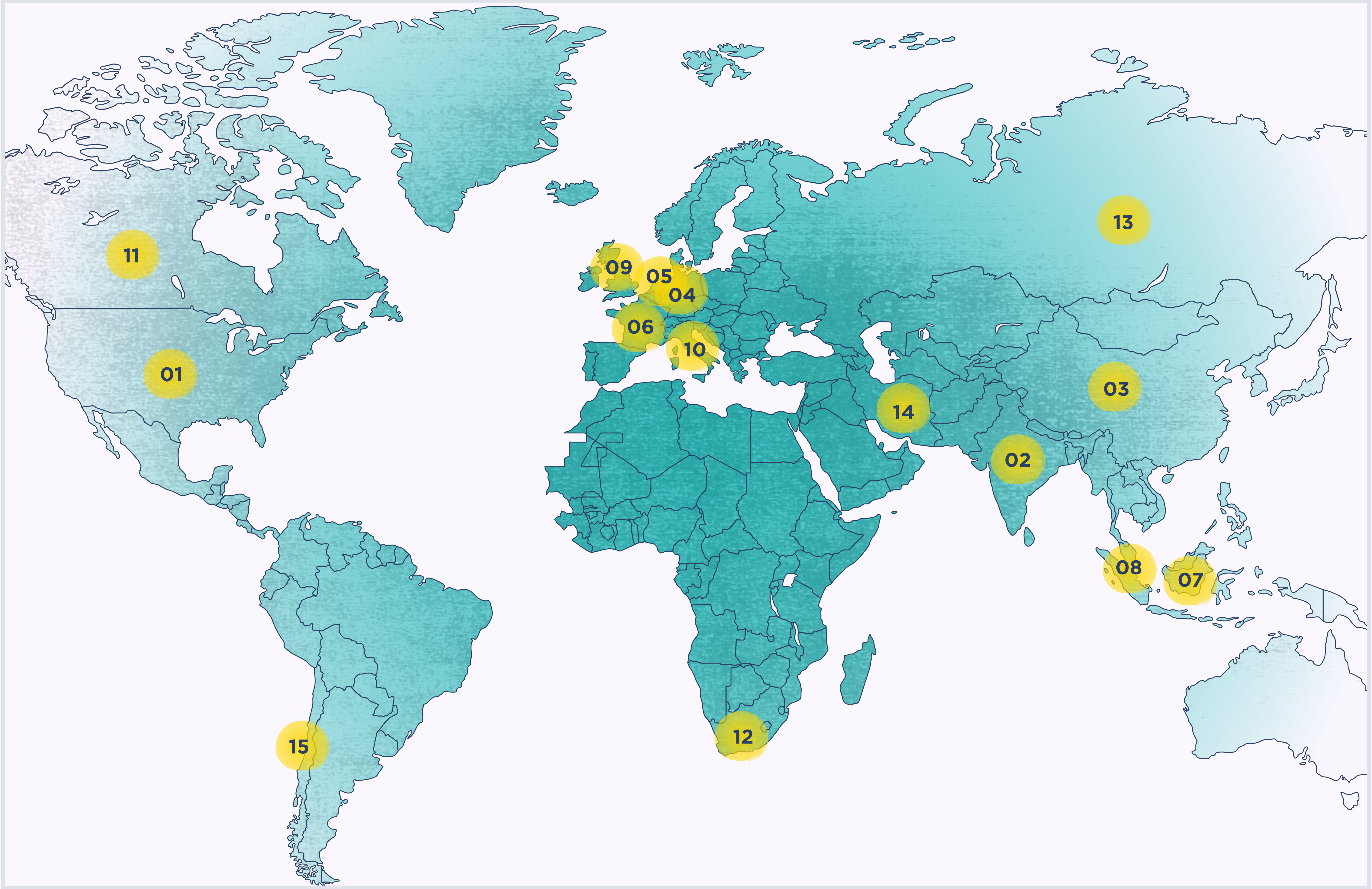


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	30,362	Cryptolaemus1
02	7,335	geenensp
03	3,388	lrz_urlhaus
04	2,296	Gandylyan1
05	1,336	abuse_ch
06	844	bry_campbell
07	843	zbetcheckin
08	656	tammeto
09	312	andretavare5
10	104	tcains1
11	86	ps66uk
12	73	jstrosch
13	65	r3dbU7z
14	62	JAMESWT_MHT
15	38	pmelson

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	COUNTRY
01	17,833	United States
02	4,425	India
03	4,318	China
04	1,460	Germany
05	1,304	Netherlands
06	915	France
07	849	Indonesia
08	701	Singapore
09	681	United Kingdom
10	638	Italy
11	572	Canada
12	439	South Africa
13	405	Russia
14	364	Iran
15	335	Chile

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	8,757	AS46606	UNIFIEDLAYER	United States
02	3,615	AS394695	PUBLIC-DOMAIN-REGISTRY	India
03	2,874	AS4837	CHINA169	China
04	2,039	AS13335	CLOUDFLARENET	United States
05	1,354	AS4134	CHINANET	China
06	1,186	AS16276	OVH	France
07	1,026	AS9829	BSNL	India
08	989	AS24940	HETZNER	Germany
09	674	AS36352	COLOCROSSING	United States
10	582	AS135222	MWNASHIK	India
11	571	AS23352	SERVERCENTRAL	United States
12	416	AS26496	GO-DADDY-COM	United States
13	393	AS51167	CONTABO	Germany
14	334	AS29802	HVC	United States
15	321	AS36943	1-Grid	South Africa

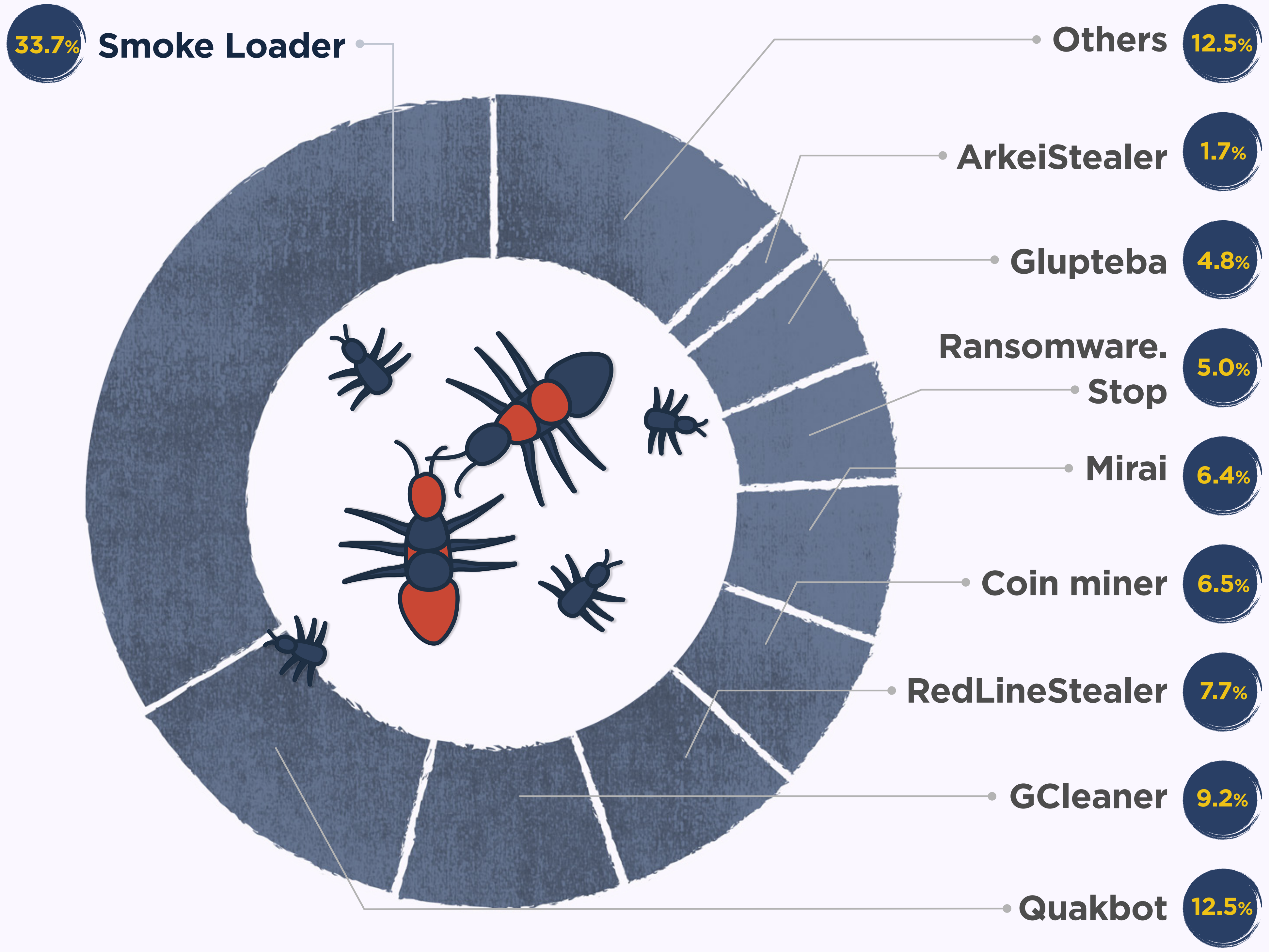
TOP MALWARE HOSTS

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	268	vk.com	VK	Russia
02	267	drive.google.com	Google	United States
03	187	www.theodoraross.com	n/a	null
04	133	www.lohevisto.com	n/a	null
05	132	www.thomadaneau.com	n/a	null
06	129	www.theairtrekstory.com	n/a	null
07	120	www.liparicasa.it	n/a	null
08	118	drc.co.th	n/a	null
09	114	www.losgaucos.cz	n/a	null
10	113	ankaraopl.com	n/a	null
11	113	fisioterapiabios.ch	n/a	null
12	113	www.tavernelentrepot.be	n/a	null
13	110	gvscolombia.com	n/a	null
14	108	sh4r3dfilesoncl0ud9.cf	n/a	null
15	107	ap-locksmith.com	n/a	null

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	344.75%	Quakbot	1,312
02	162.97%	GCleaner	973
03	143.78%	Ransomware.Stop	529
04	62.86%	SnakeKeylogger	114
05	36.49%	Smoke Loader	3,546
06	28.17%	ArkeiStealer	182
07	25.46%	RedLineStealer	813
08	23.40%	Tofsee	116
09	18.69%	AgentTesla	127
10	-22.40%	RecordBreaker	142
11	-29.07%	Gafgyt	122
12	-46.96%	Mirai	671
13	-47.54%	Blackmoon	160
14	-54.32%	DanaBot	74
15	-70.42%	CoinMiner	682

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

13,740

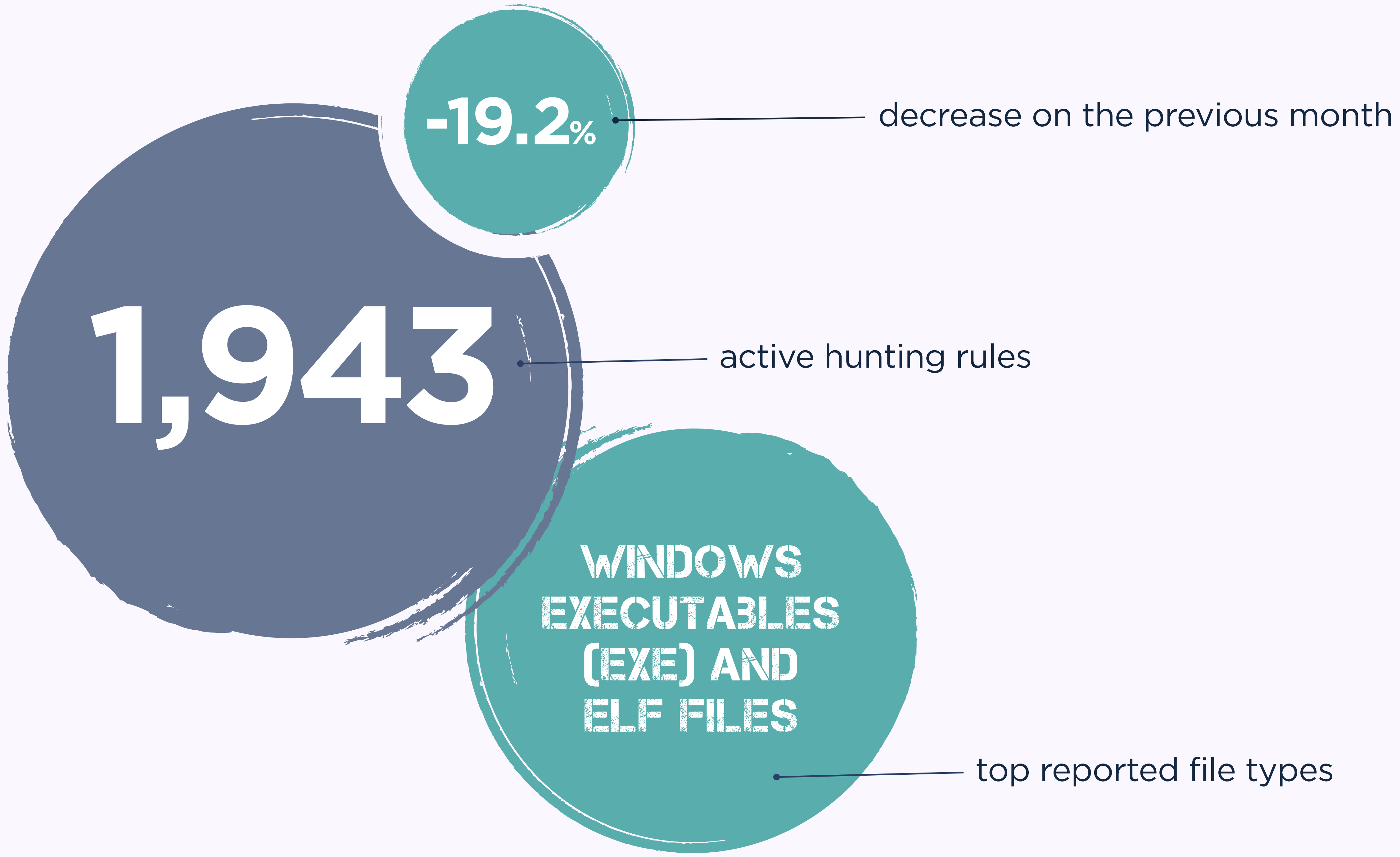
Malware samples

shared by security researchers on MalwareBazaar

1.5MB

Average size

of a malware sample



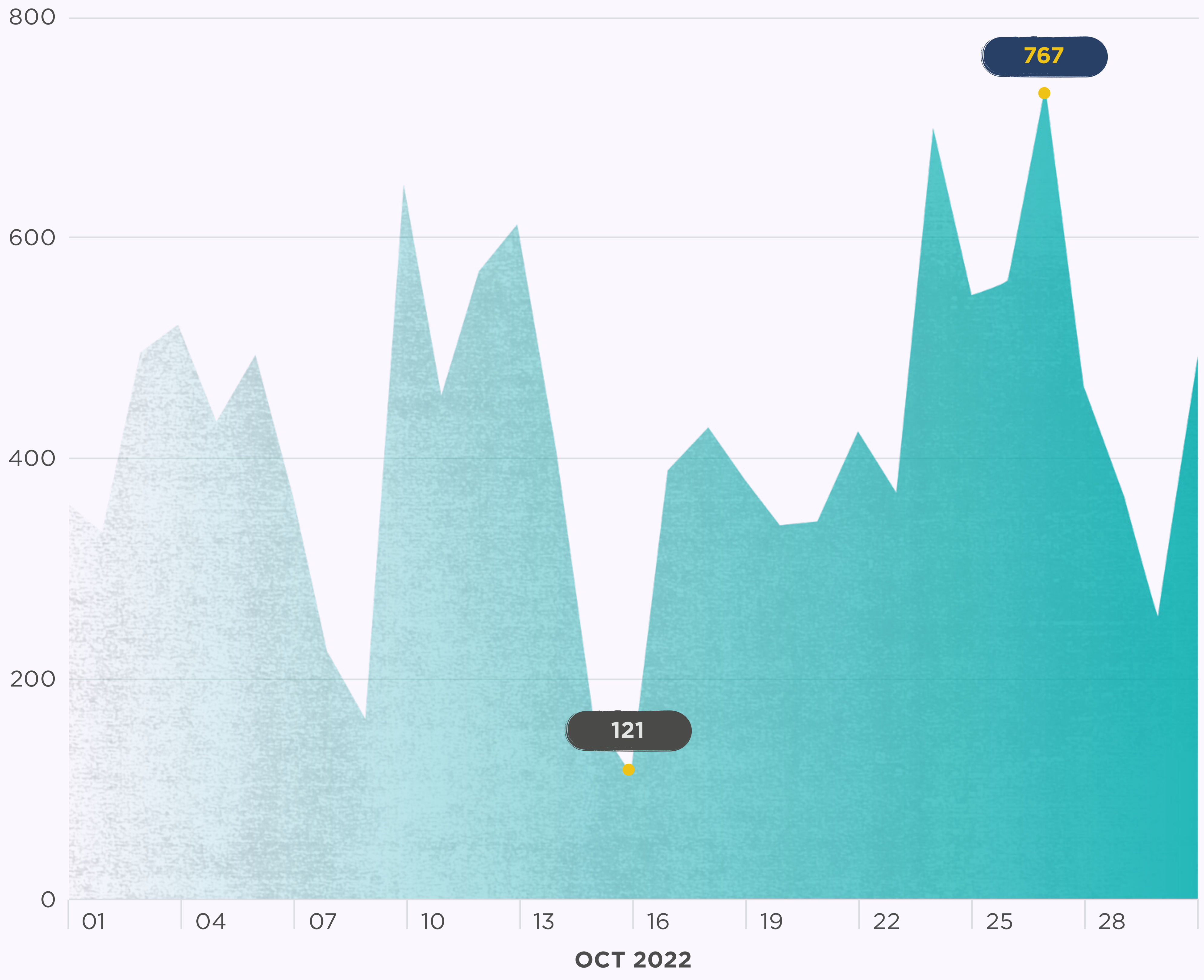
-19.2% decrease on the previous month

1,943 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.



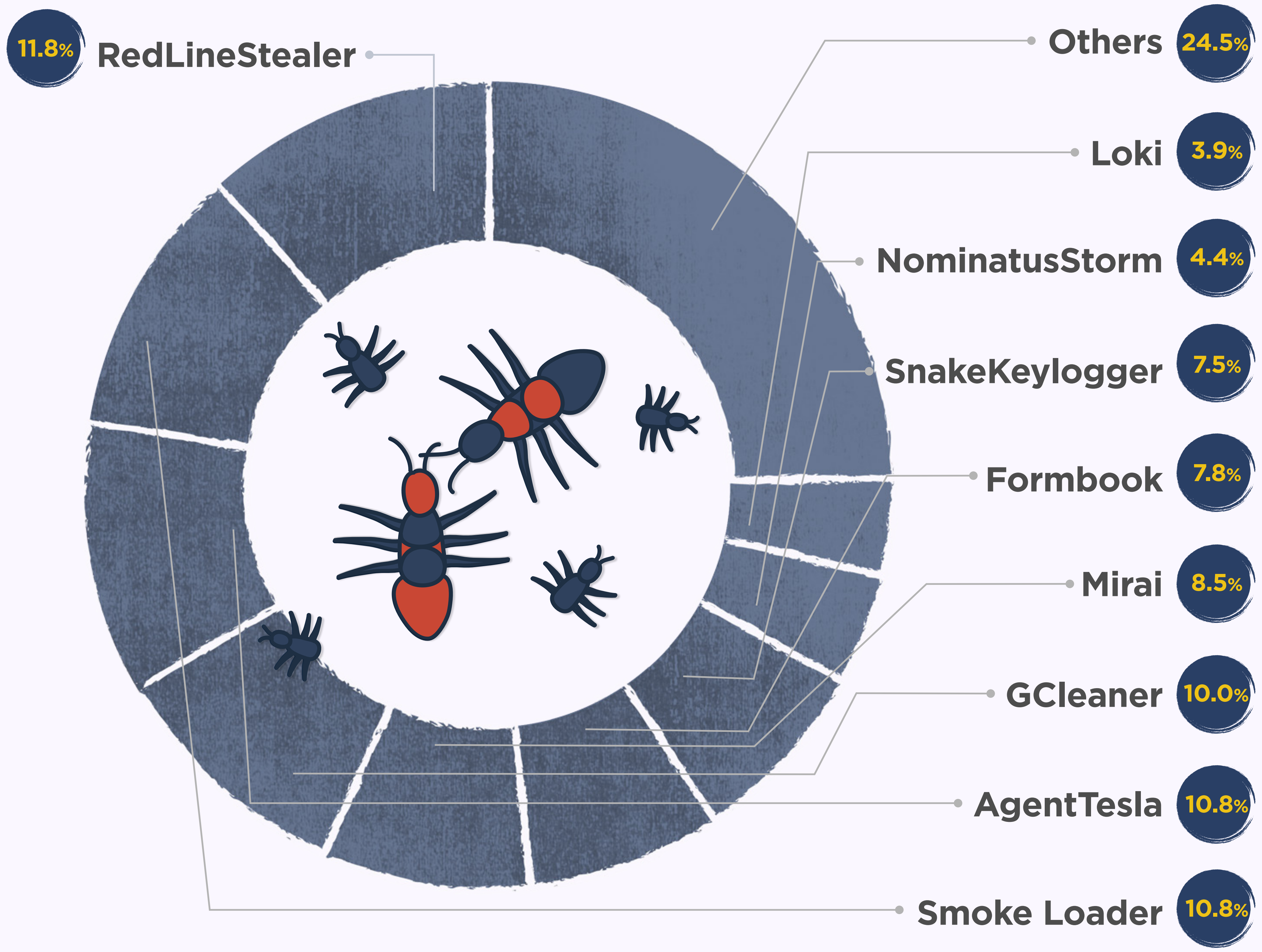
TOP SAMPLE CONTRIBUTORS

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	3,821	@andretavare5
02	1,178	@zbetcheckin
03	733	@SecuriteInfoCom
04	732	@petikvx
05	558	@GovCERT_CH
06	476	@JAMESWT_MHT
07	416	@cocaman
08	303	@lowmal3
09	289	@adrian__luca
10	189	@GootLoaderSites
11	182	@0xToxin
12	163	@malwarelabnet
13	161	@pr0xylife
14	149	@James_inthe_box
15	136	@jstrosch

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



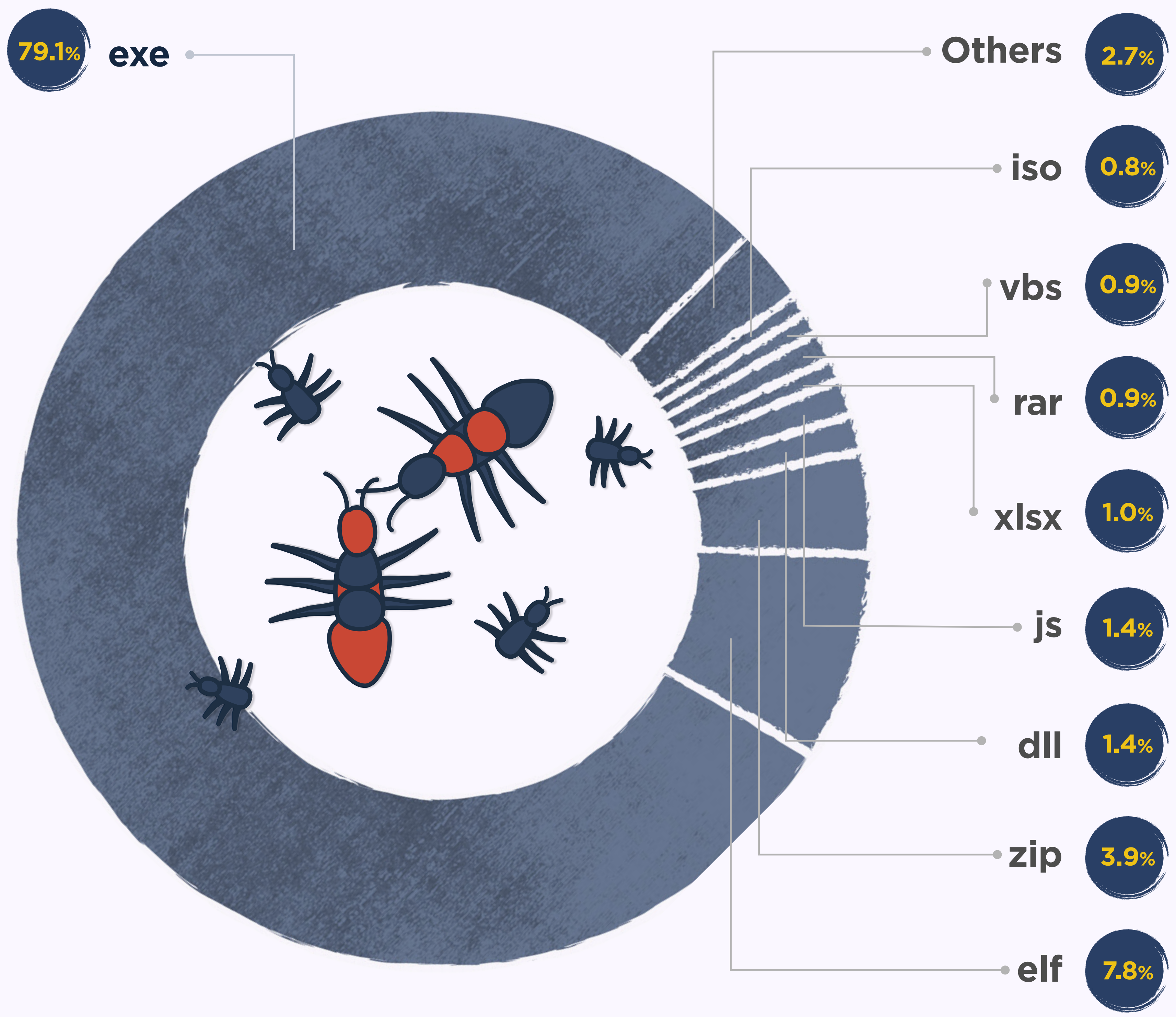
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	167.95%	GCleaner	978
02	78.77%	Quakbot	261
03	73.46%	ArkeiStealer	281
04	60.88%	Smoke Loader	1,057
05	56.44%	njrat	158
06	48.08%	RedLineStealer	1,155
07	31.96%	Loki	384
08	31.03%	RecordBreaker	228
09	28.05%	SnakeKeylogger	735
10	27.72%	AgentTesla	1,055
11	20.17%	RemcosRAT	280
12	15.29%	Formbook	769
13	10.69%	DCRat	176
14	-32.91%	GuLoader	318
15	-38.24%	Mirai	830

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	1,405	cobalt_strike_tmp01925d3f	The DFIR Report
02	1,232	win_smokeloader_a2	pnx
03	884	win_nymaim_g0	CERT.pl
04	742	MALWARE_Win_RedLine	ditekSHen
05	594	win_gcleaner_auto	Felix Bilstein
06	577	Windows_Trojan_ Smokeloader_3687686f	Elastic Security
07	549	CAS_Malware_Hunting	Michael Reinprecht
08	520	unixredflags3	Tim Brown
09	511	linux_generic_ipv6_catcher	@_lubiedo
10	505	myMirai	n/a
11	407	INDICATOR_SUSPICIOUS_ GENRansomware	ditekSHen
12	372	INDICATOR_SUSPICIOUS_ Binary_References_Browsers	ditekSHen
13	323	QbotStuff	n/a
14	271	MALWARE_Win_AgentTeslaV3	ditekSHen
15	264	setsockopt	Tim Brown

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)

90,162

Indicators of compromise (IOCs)

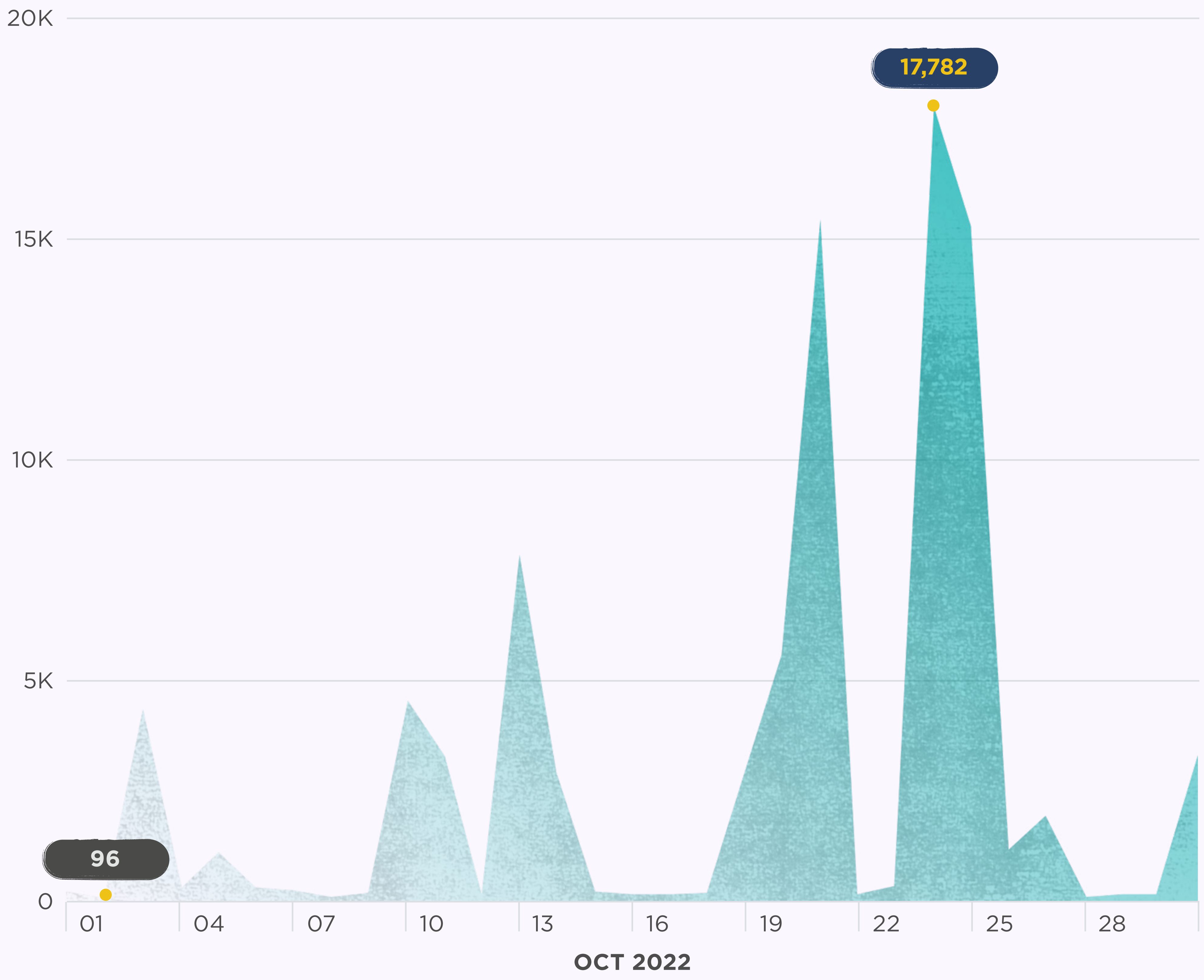
shared on ThreatFox

403.4% increase on the previous month

93.9% percentage of IOCs relating to Quakbot

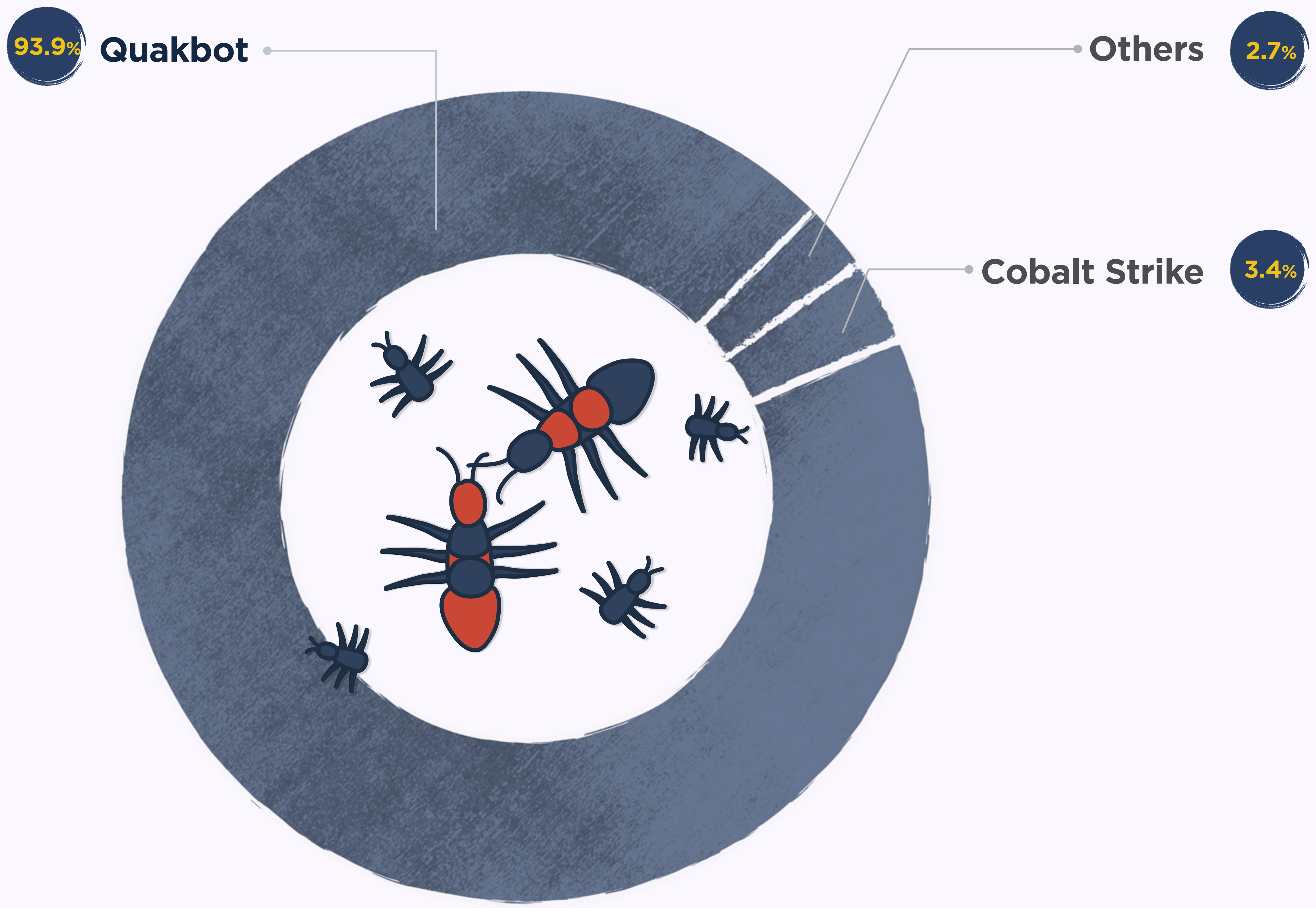
NUMBER OF IOCs SHARED PER DAY

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



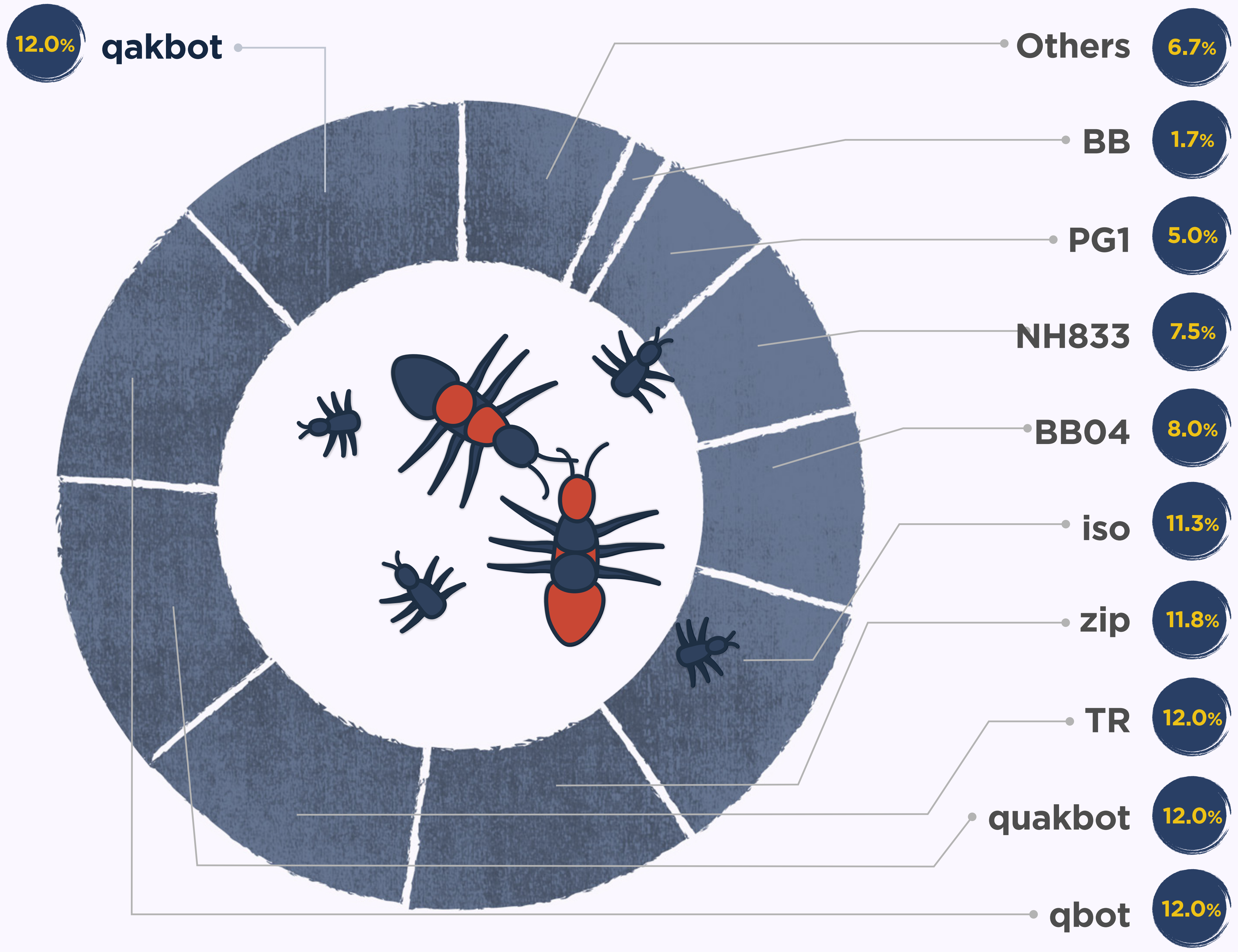
TOP MALWARE FAMILIES

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	80,809	url	payload_delivery	URL that delivers a malware payload
02	2,852	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
03	2,813	url	botnet_cc	URL that is used for botnet Command&control (C&C)
04	2,543	domain	payload_delivery	Domain name that delivers a malware payload
05	591	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
06	430	sha256_hash	payload	SHA256 hash of a malware sample (payload)
07	118	md5_hash	payload	MD5 hash of a malware sample (payload)
08	5	ip:port	payload_delivery	ip:port combination that delivery a malware payload
09	1	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

2,291,618

File scans

conducted on YARAify

1,872,318

Distinct files

that had scans performed on them

4,917

YARA rules

deployed on YARAify and available for hunting

0.9%

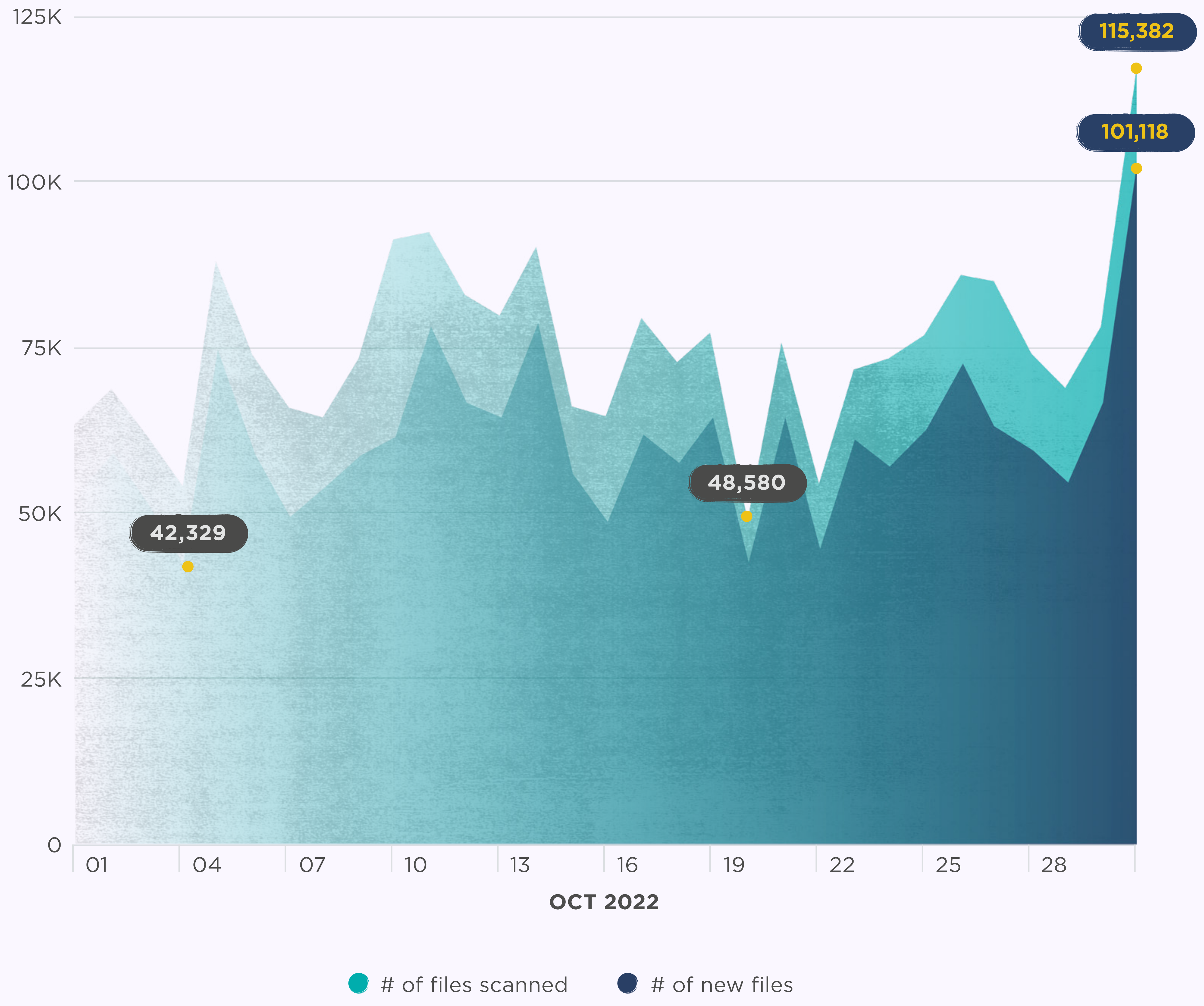
increase in distinct files on the previous month

3.9%

increase in file scans on the previous month

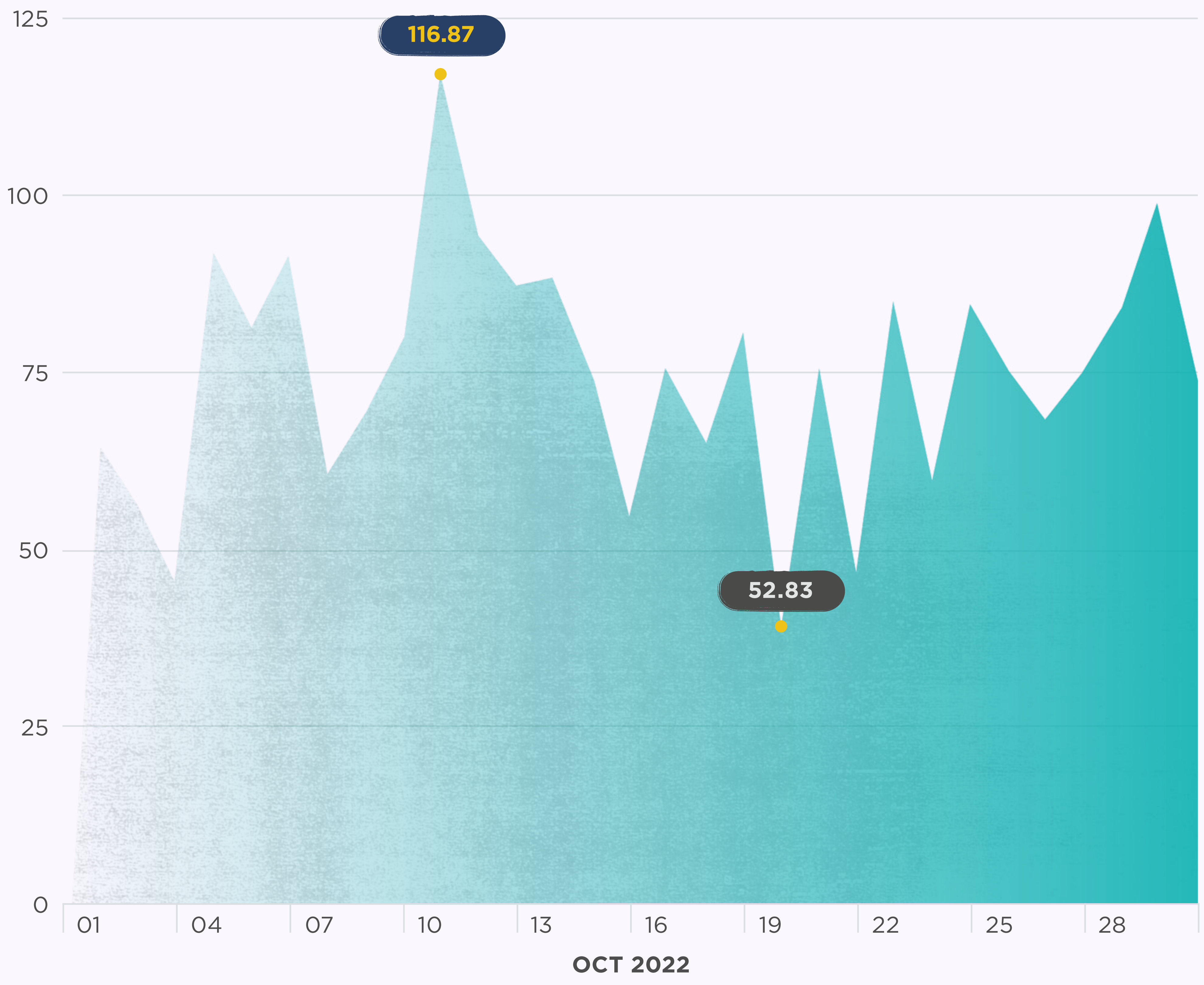
FILES SCANNED PER DAY

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 (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	YARA RULE	AUTHOR
01	66,520	command_and_control	CD_R0M_
02	40,906	win_sality_auto	Felix Bilstein
03	33,591	INDICATOR_EXE_Packed_MPress	ditekSHen
04	24,216	malware_shellcode_hash	JPCERT/CC
05	19,981	cobalt_strike_tmp01925d3f	The DFIR Report
06	17,705	SUSP_XORed_URL_in_EXE_RID2E46	Florian Roth
07	17,200	SUSP_XORed_URL_in_EXE	Florian Roth
08	16,922	AutoIT_Compiled	@bartblaze
09	15,660	win_smokeloader_a2	pnx
10	14,485	win_vobfus_auto	Felix Bilstein
11	12,362	MALWARE_Win_BlackMoon	ditekSHen
12	12,083	MALWARE_Win_RedLine	ditekSHen
13	11,522	GoBinTest	n/a
14	10,770	INDICATOR_EXE_Packed_ASPack	ditekSHen
15	10,642	adonunix2	Tim Brown

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	134,351	PUA.Win.Packer.Upx-4
02	60,840	PUA.Win.Packer.Lccwin-2
03	55,390	Win.Trojan.Qukart-6874817-0
04	39,780	Win.Trojan.Obfus-38
05	35,803	Win.Malware.Qukart-6838239-0
06	30,049	PUA.Win.Packer.AcprotectUltraprotect-1
07	23,934	Win.Worm.Moonlight-9779178-0
08	23,934	Win.Worm.Ulise-9778387-0
09	23,864	Win.Malware.Moonlight-9934254-0
10	23,853	Win.Malware.Moonlight-9890813-0
11	23,853	Win.Trojan.Moonlight-9881795-0
12	23,853	Win.Malware.Moonlight-9934996-0
13	23,396	Win.Trojan.Crypted-30
14	23,296	Win.Trojan.Crypted-29
15	20,587	Win.Packed.Moonlight-9934265-0

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN DECEMBER

Remember, sharing is caring.