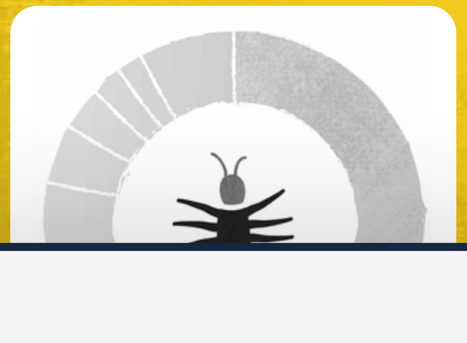
OCTOBER 2023

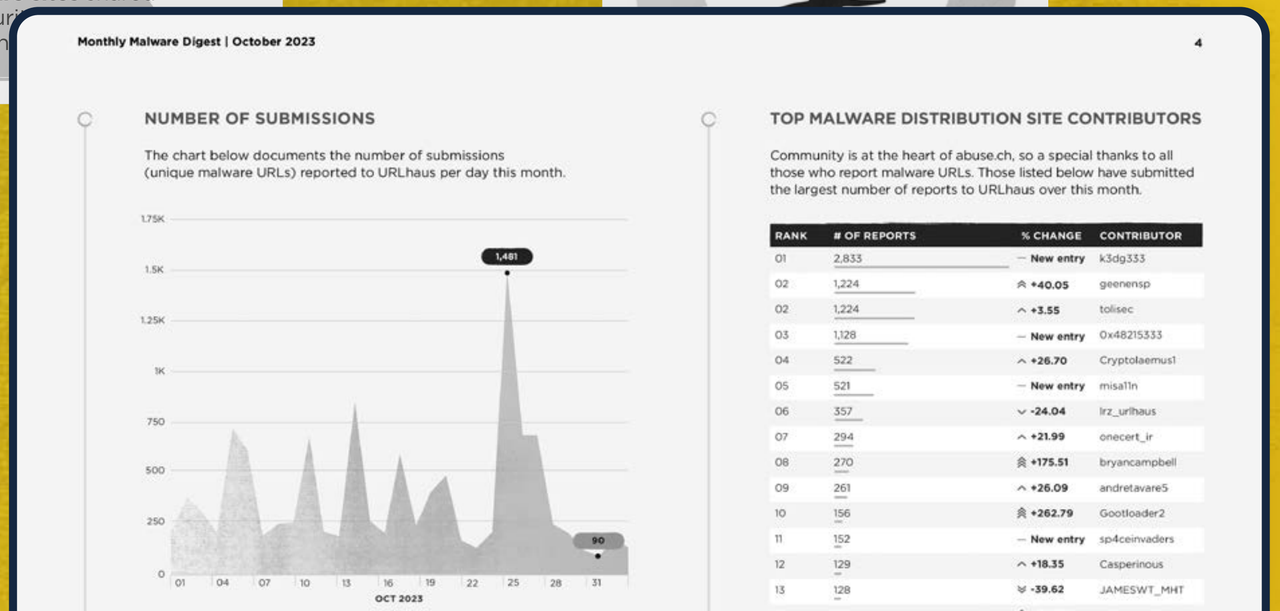
SPAMHAUS ABUSE.ch

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.





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	**MalwareBazaar**
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	**MalwareBazaar**
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

11,471

Malware sites shared by security researchers on URLhaus

+72.5%

increase on the previous month

18,274

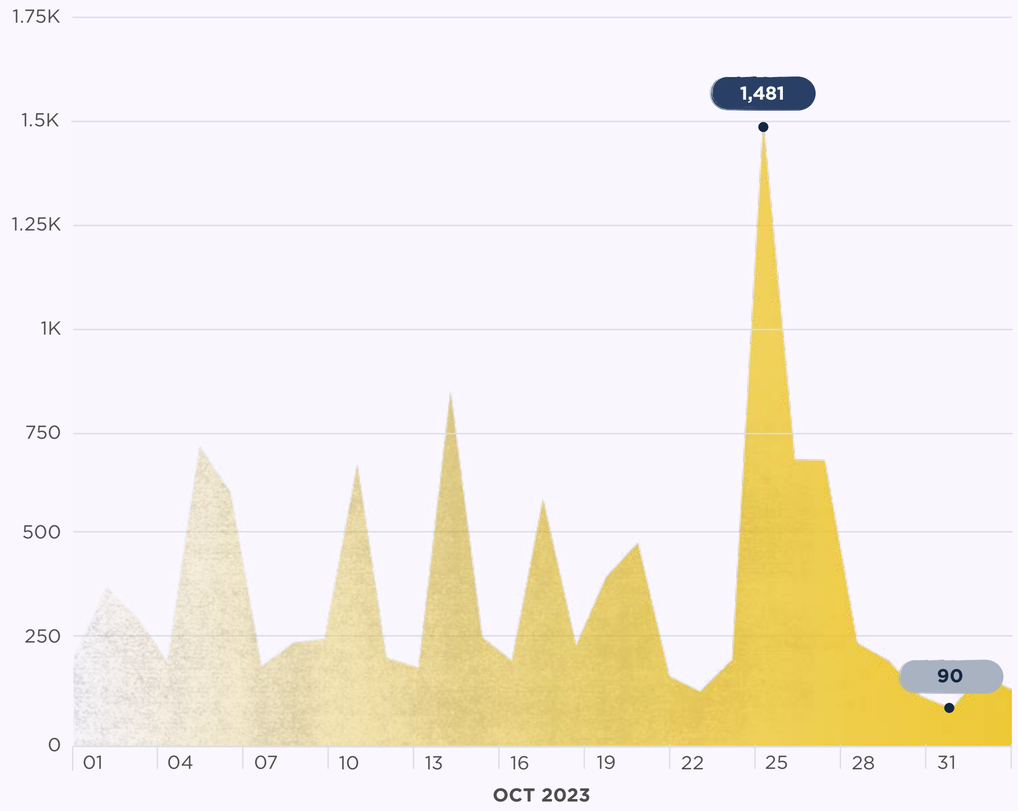
Abuse reports sent out to hosting providers and network owners

94.1%

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.

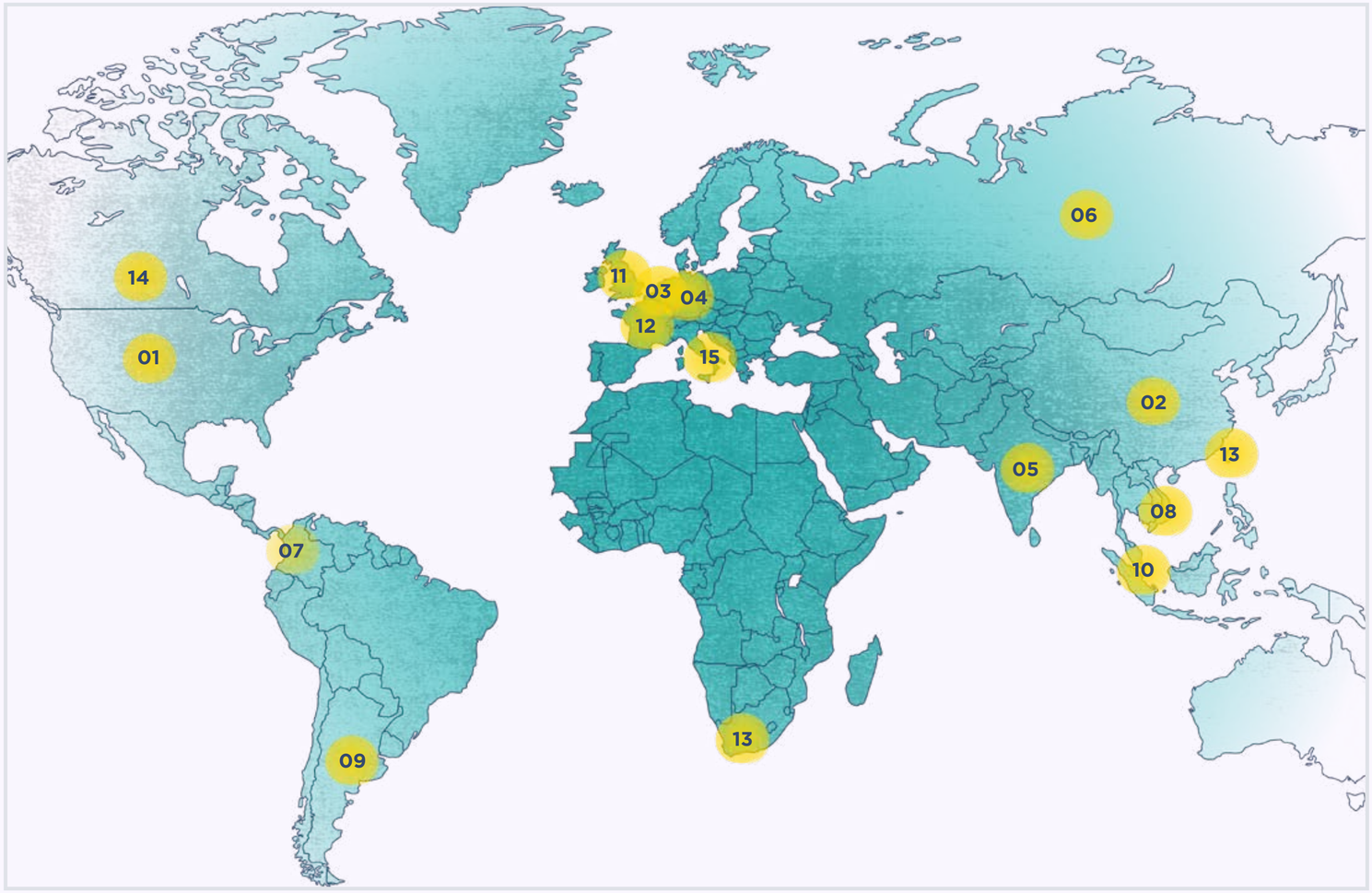


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	2,833	— New entry	k3dg333
02	1,224	⌃⌃ +40.05	geenensp
02	1,224	⌃ +3.55	tolisec
03	1,128	— New entry	0x48215333
04	522	⌃ +26.70	Cryptolaemus1
05	521	— New entry	misa11n
06	357	⌄ -24.04	lrz_urlhaus
07	294	⌃ +21.99	onecert_ir
08	270	⌃⌃ +175.51	bryancampbell
09	261	⌃ +26.09	andretavare5
10	156	⌃⌃ +262.79	Gootloader2
11	152	— New entry	sp4ceinvaders
12	129	⌃ +18.35	Casperinous
13	128	⌄⌄ -39.62	JAMESWT_MHT
14	68	⌃⌃ +94.29	aubrey_eats_pie

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	4,467	+126.18	United States
02	959	+85.85	China
03	946	-2.67	Netherlands
04	798	+111.11	Germany
05	527	+181.82	India
06	459	+8.77	Russia
07	339	+132.19	Colombia
08	238	+5.31	Vietnam
09	235	+76.69	Argentina
10	199	+139.76	Singapore
11	183	+40.77	United Kingdom
12	178	+111.90	France
13	135	+80.00	South Africa
14	127	New entry	Canada
15	121	New entry	Italy

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	832	AS22612	NAMECHEAP-NET	United States
02	750	AS13335	CLOUDFLARENET	United States
03	660	AS211252	AS_DELIS	Netherlands
04	646	AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	China
05	597	AS46606	UNIFIEDLAYER-AS-1	United States
06	368	AS36352	AS-COLOCROSSING	United States
07	291	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
08	280	AS19871	NETWORK-SOLUTIONS-HOSTING	United States
09	269	AS19557	CHANGEIP-01	United States
10	267	AS26496	AS-26496-GO-DADDY-COM-LLC	United States
11	228	AS24940	HETZNER-AS	Germany
12	217	AS10617	SION S.A	Argentina
13	209	AS49581	FERDINANDZINK	Germany
14	203	AS47541	VKONTAKTE-SPB-AS vk.com	Russia
15	200	AS9829	BSNL-NIB National Internet Backbone	India

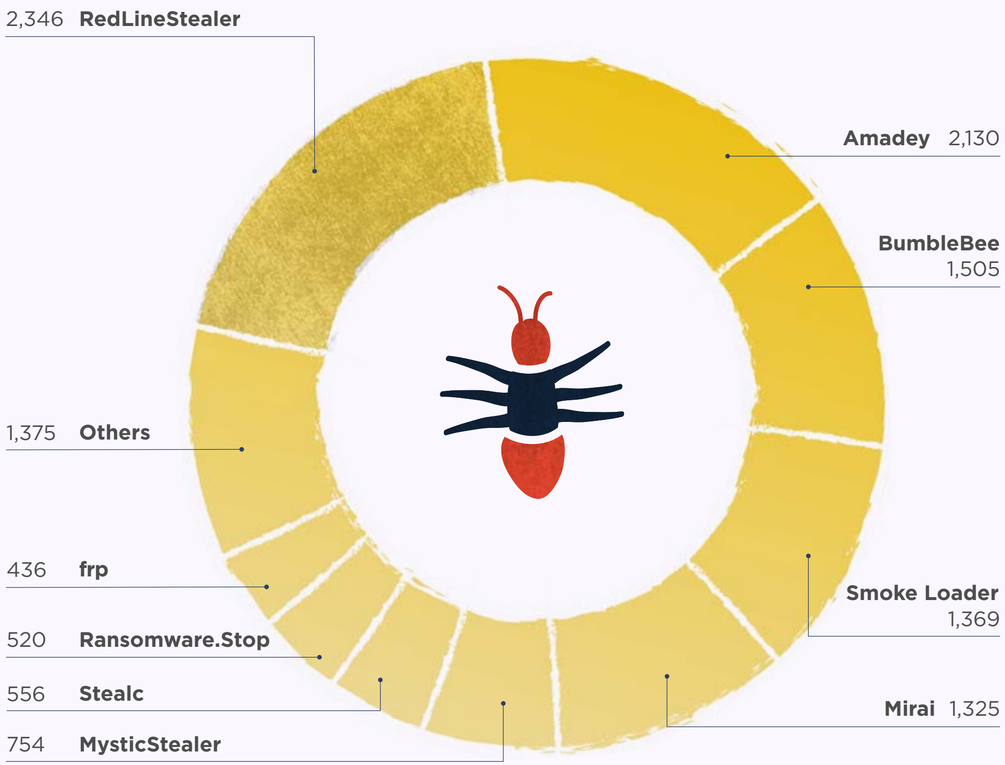
TOP MALWARE HOSTS

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	203	vk.com	VK	Russia
02	106	drive.google.com	Google	United States
03	100	www.dropbox.com	Dropbox	United States
04	97	wtools.io	n/a	null
05	48	transfer.sh	n/a	null
06	19	paste.ee	n/a	null
07	14	pasteio.com	n/a	null
07	14	docs.google.com	Google	United States
09	13	pastebin.com	Pastebin	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	Stealc	+84.72		556
02	UACModuleSmokeLoader	+14.35		247
03	Mirai	+5.58		1,325
04	CoinMiner	-3.43		225
05	BumbleBee	-7.38		1,505
06	Ransomware.Stop	-13.62		520
07	Smoke Loader	-17.23		1,369
08	Amadey	-30.48		2,130
09	frp	-42.86		436
10	MysticStealer	-48.04		754
11	RedLineStealer	-48.92		2,346
12	MarsStealer	New entry		422
12	AgentTesla	New entry		168
12	RecordBreaker	New entry		158
12	IRATA	New entry		155

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

11,015

Malware samples shared by security researchers on MalwareBazaar

+12.9%

increase on the previous month

1,353

Active hunting rules

+2.7%

increase on the previous month

14.17MB

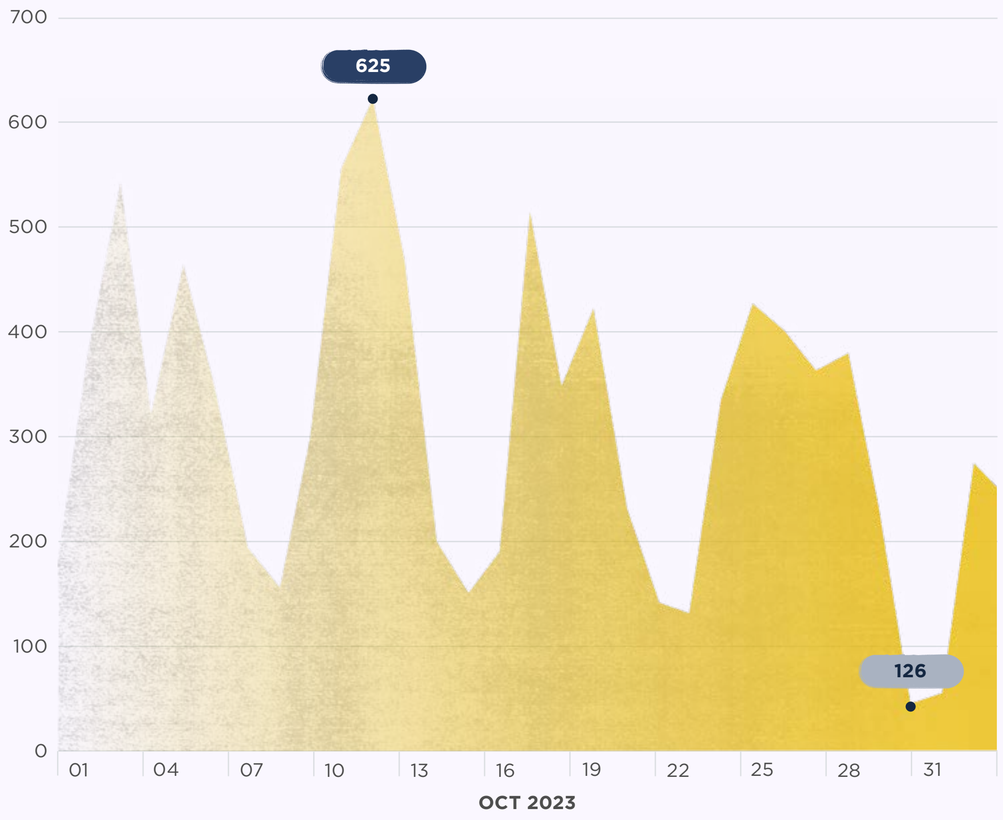
Average size of a malware sample

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.



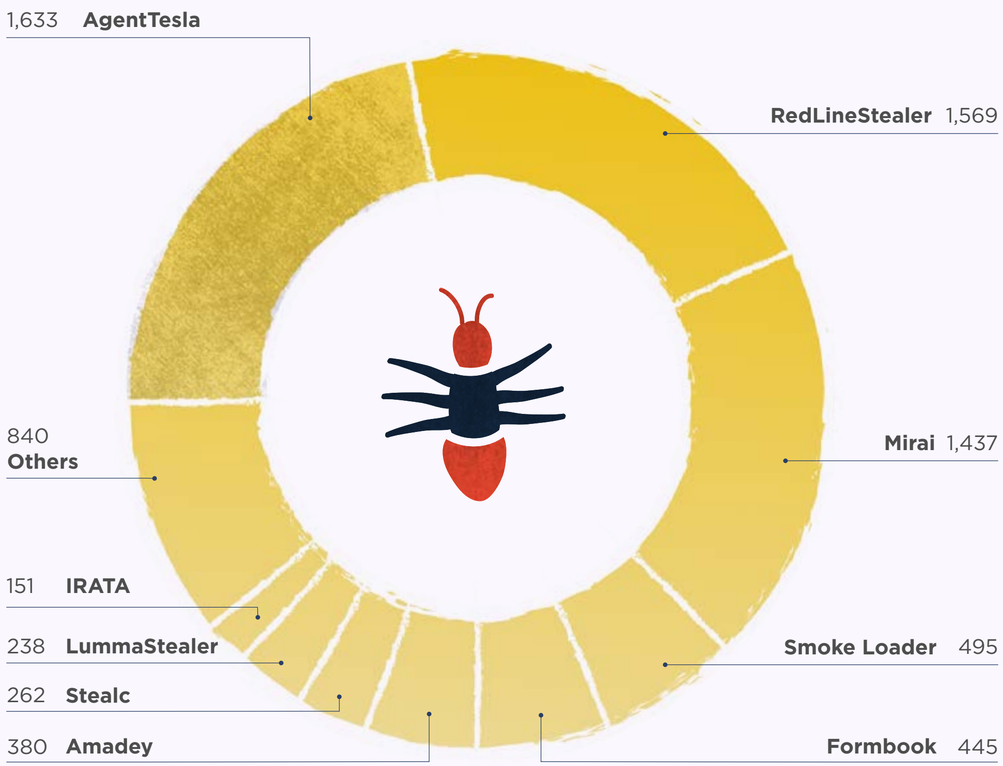
TOP SAMPLE CONTRIBUTORS

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	2,390	+85.70	@andretavare5
02	546	+27.57	@cocaman
03	496	+4.42	@elfdigest
04	406	-12.88	@JAMESWT_MHT
05	267	-32.91	@lowmal3
06	237	+16.18	@r3dbU7z
07	181	+38.17	@TeamDreier
08	174	-18.31	@adrian__luca
09	151	+11.03	@onecert_ir
10	123	+35.16	@malwarelabnet
11	122	New entry	@g0njxa
12	109	+7.92	@smica83
13	94	New entry	@pr0xylife
14	55	-35.29	@jstrosch
14	55	New entry	@vovaan

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



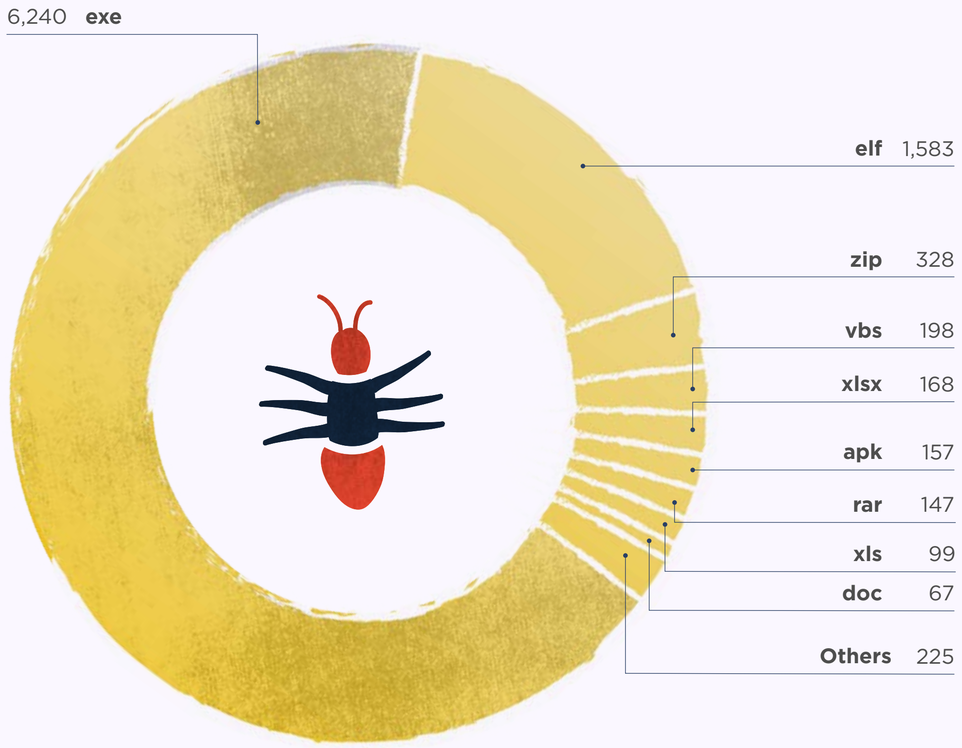
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	AsyncRAT	+39.58		134
02	RedLineStealer	+38.48		1,569
03	Formbook	+36.50		445
04	Stealc	+34.36		262
05	Smoke Loader	+33.42		495
06	AgentTesla	+11.24		1,633
07	SnakeKeylogger	+8.15		146
08	IRATA	+7.86		151
09	Amadey	+4.97		380
10	Mirai	-4.26		1,437
11	LummaStealer	New entry		238
11	GuLoader	New entry		149
11	RecordBreaker	New entry		140
11	Gafgyt	New entry		138
11	Tofsee	New entry		133

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	2,792	NET	malware-lu
02	1,914	NETexecutableMicrosoft	malware-lu
03	1,834	DebuggerCheck__API	n/a
04	1,440	maldoc_find_kernel32_base_method_1	Didier Stevens
05	1,127	detect_Redline_Stealer	Varp0s
06	1,060	INDICATOR_EXE_Packed_ConfuserEx	ditekSHen
07	911	redline_stealer_1	Nikolaos 'n0t' Totosis
08	841	win_smokeloader_a2	pnx
09	792	pe_no_import_table	qux
10	571	linux_generic_ipv6_catcher	@_lubiedo
11	554	myMirai	n/a
12	553	MD5_Constants	phoul (@phoul)
13	529	INDICATOR_SUSPICIOUS_EXE_RegKeyComb_DisableWinDefender	ditekSHen
14	528	mal_healer	Nikos 'n0t' Totosis
15	526	cobalt_strike_tmp01925d3f	The DFIR Report

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)

15,493

Indicators of compromise (IOCS) shared on ThreatFox

-43.4%

decrease on the previous month

3,784

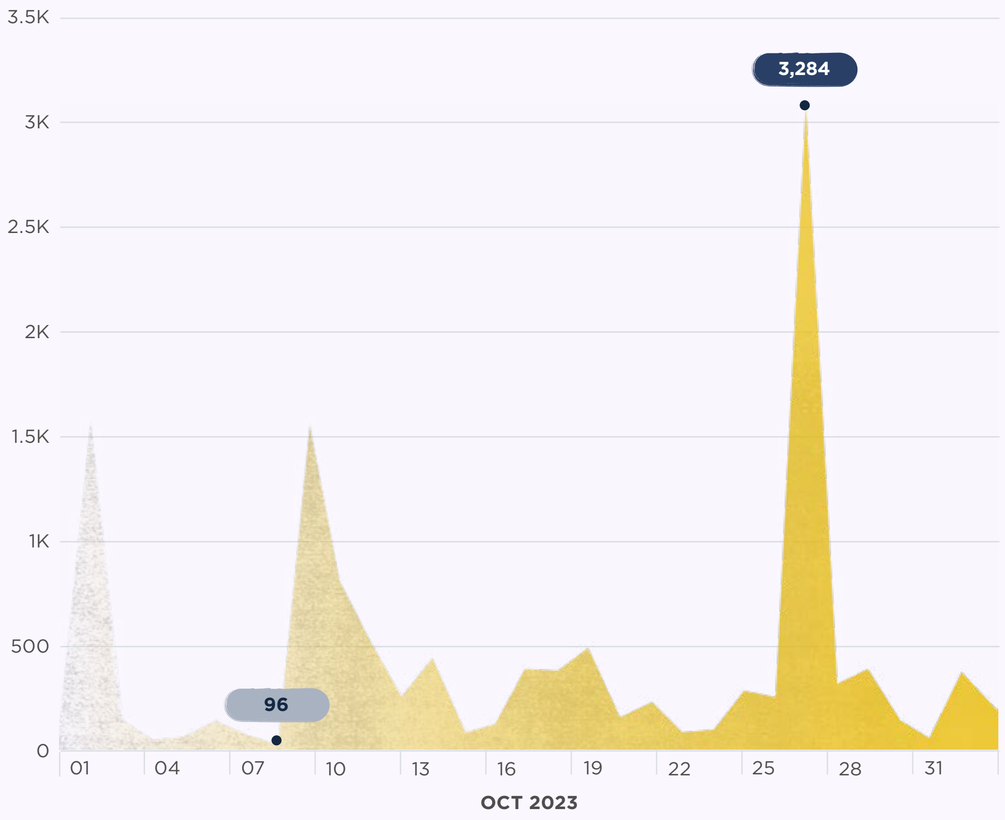
IOCs relating to Cobalt Strike

+99.89%

increase on the previous 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.



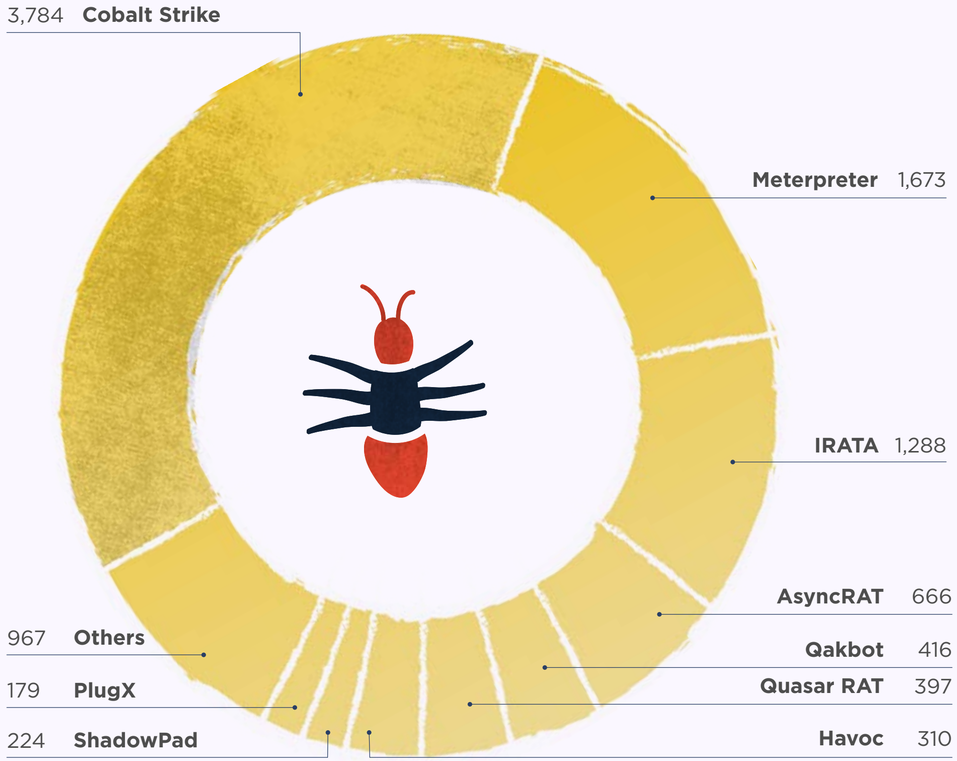
IOC TYPE

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	7,475	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
02	2,644	url	botnet_cc	URL that is used for botnet Command&control (C&C)
03	2,595	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
04	1,138	ip:port	payload_ delivery	ip:port combination that delivers a malware payload
05	705	domain	payload_ delivery	Domain name that delivers a malware payload
06	648	url	payload_ delivery	URL that delivers a malware payload
07	199	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
08	174	md5_hash	payload	MD5 hash of a malware sample (payload)
09	7	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.



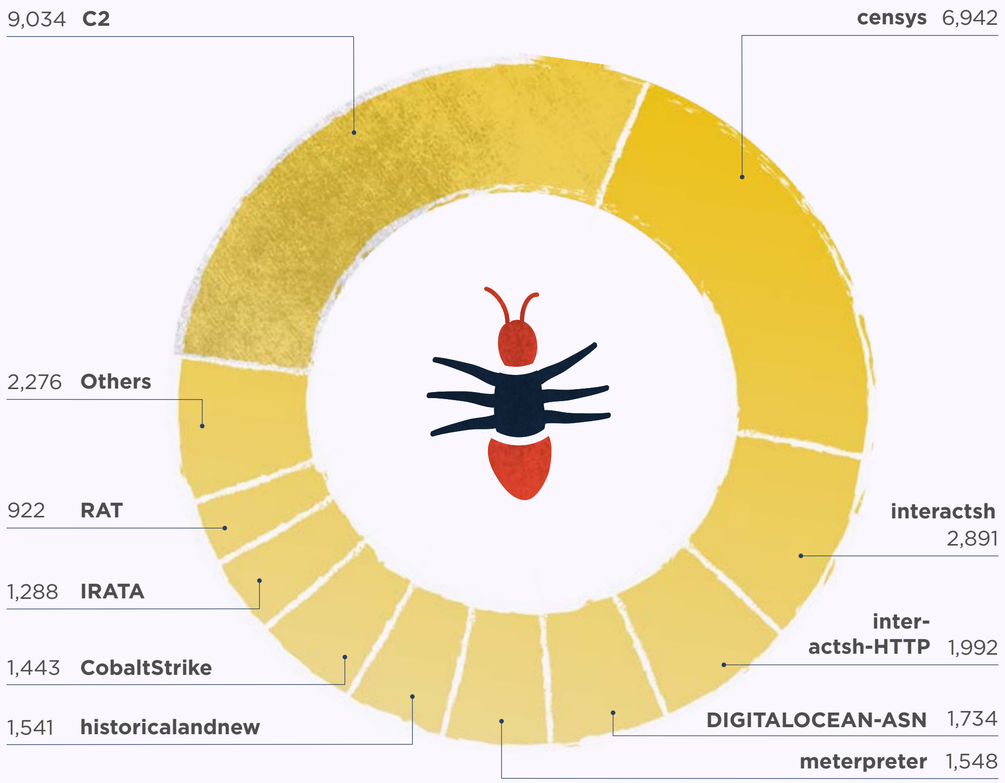
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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	Cobalt Strike	**+99.89**		3,784
02	IRATA	**+17.95**		1,288
03	Quasar RAT	**-65.08**		397
04	AsyncRAT	**-72.33**		666
05	Meterpreter	**New entry**		1,673
05	Qakbot	**New entry**		416
05	Havoc	**New entry**		310
05	ShadowPad	**New entry**		224
05	PlugX	**New entry**		179
05	RedlineStealer	**New entry**		174
05	Sliver	**New entry**		169
05	GootLoader	**New entry**		164
05	Lumma	**New entry**		159
05	DarkGate	**New entry**		156
05	Pikabot	**New entry**		145

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	IRATA	^ +18.60	1,288
02	CobaltStrike	v -17.45	1,443
03	C2	vv -55.96	9,034
04	RAT	vv -74.41	922
05	AsyncRAT	vv -84.92	359
06	historicalandnew	vv -91.74	1,541
07	censys	— New entry	6,942
07	interactsh	— New entry	2,891
07	interactsh-HTTP	— New entry	1,992
07	DIGITALOCEAN-ASN	— New entry	1,734
07	meterpreter	— New entry	1,548
07	interactsh-SMTP	— New entry	674
07	cs-watermark-987654321	— New entry	464
07	Qakbot	— New entry	414
07	AMAZON-02	— New entry	365

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

3,891,584

File scans conducted
on YARAify

3,212,843

Distinct files
that had scans performed on them

+29.3%

increase in
file scans on the previous month

+26.9%

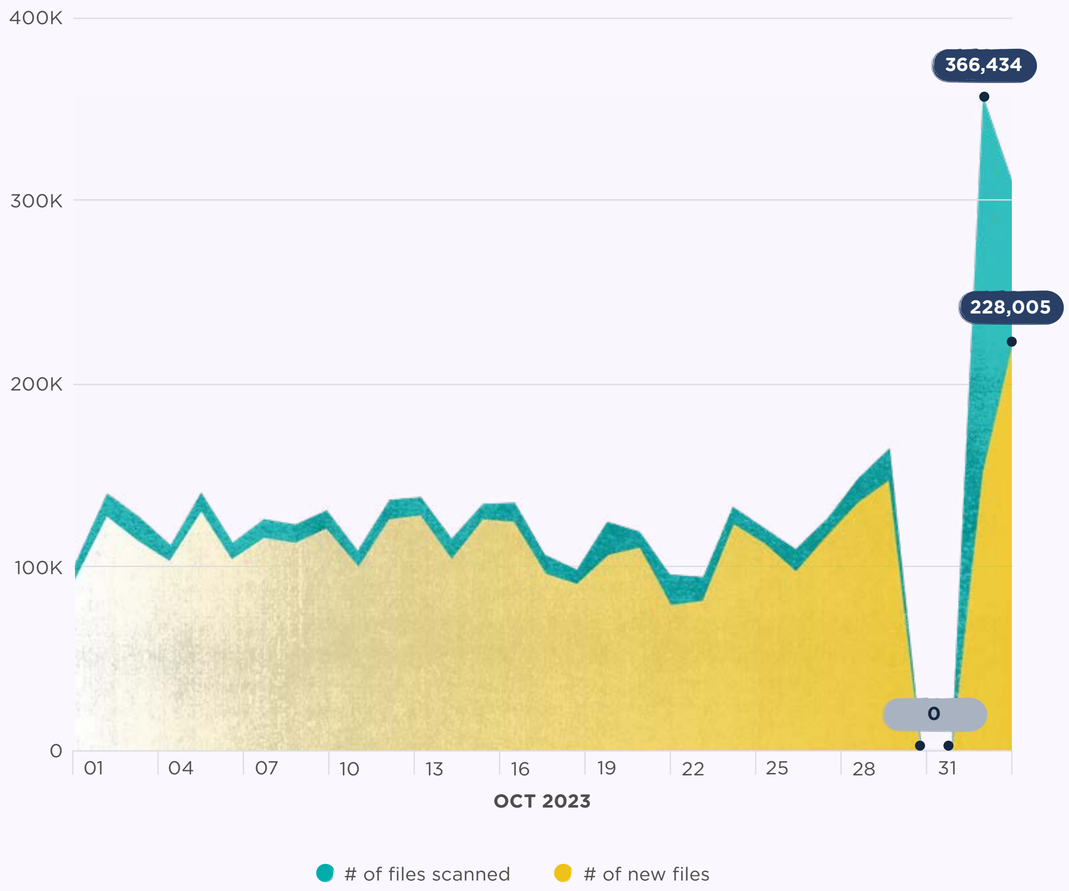
increase in distinct
files on the previous month

18,422

YARA rules deployed
on YARAify and available for hunting

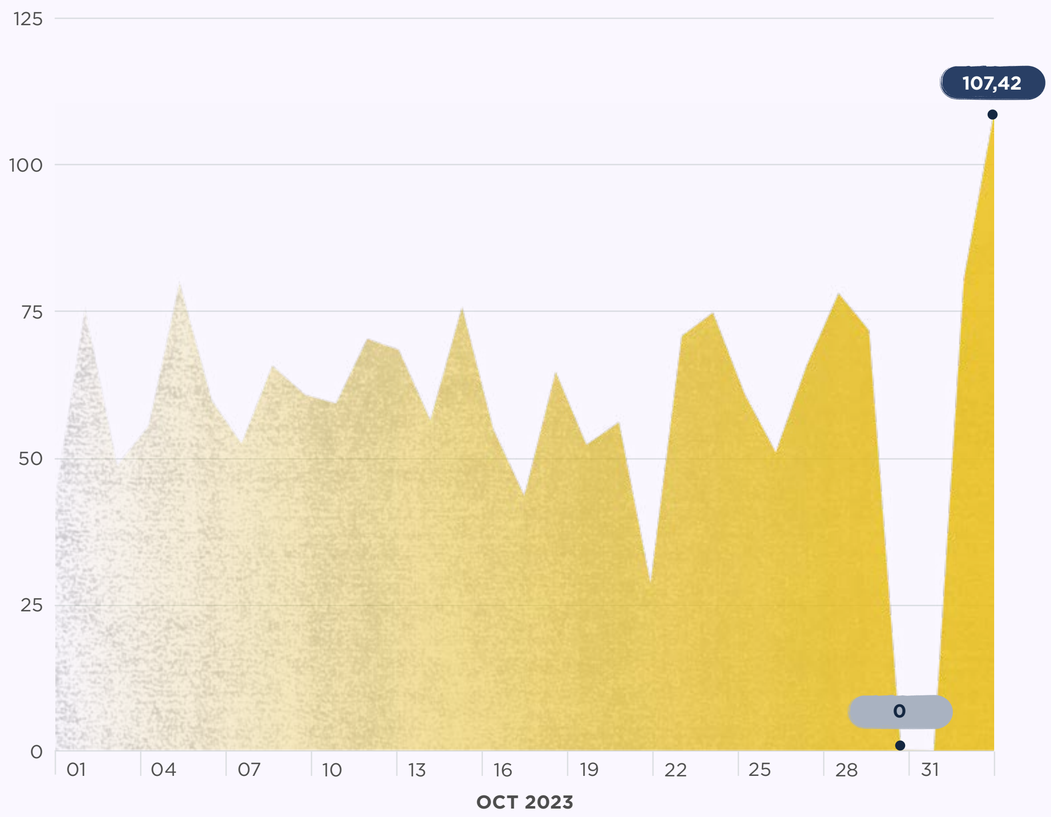
FILES SCANNED PER DAY

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	2,823,220	+133.67	maldoc_getEIP_method_1	Didier Stevens
02	289,692	-6.65	DebuggerCheck__API	n/a
03	175,476	-17.55	NET	malware-lu
04	156,012	-15.60	UPXV200V290MarkusOberhumerLaszloMolnar-JohnReiser	malware-lu
05	150,859	-15.99	maldoc_find_kernel32_base_method_1	Didier Stevens (https://Didier-Stevens.com)
06	135,572	-19.44	UPXv20MarkusLaszloReiser	malware-lu
07	91,536	New entry	Check_Dlls	n/a
08	87,609	-18.10	MD5_Constants	phoul (@phoul)
09	83,271	New entry	SUSP_XORed_URL_in_EXE_RID2E46	n/a
10	83,107	New entry	SUSP_XORed_URL_in_EXE	Florian Roth (Nextron Systems)
11	73,941	+19.17	SEH__vba	n/a
12	73,505	-33.98	SHA1_Constants	phoul (@phoul)
13	73,504	-33.98	RIPEMD160_Constants	phoul (@phoul)
14	67,836	-8.79	DebuggerException__SetConsoleCtrl	n/a
15	57,966	+2.86	Borland	malware-lu

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	1,784,353	+86.03	PUA.Win.Packer.Lccwin-2
02	1,209,379	+85.85	Win.Trojan.Obfus-38
03	763,099	+58.27	Win.Trojan.Qukart-6874817-0
04	585,881	+112.46	Win.Trojan.Padodor-9877164-0
05	537,173	+131.56	Win.Malware.Qukart-6838239-0
06	202,545	-4.73	Win.Trojan.Crypted-30
07	202,440	-4.47	Win.Trojan.Crypted-29
08	135,581	New entry	Win.Packed.Razy-10009896-0
09	125,014	New entry	Win.Packed.Razy-10010080-0
10	118,103	+15.49	Win.Trojan.Crypted-28
11	112,100	+190.74	Win.Malware.Renos-10003934-0
12	104,287	+88.01	Win.Packed.Lazy-10005437-0
13	100,302	+260.57	Win.Packed.Zpack-10001780-0
14	86,673	+56.81	Win.Trojan.Berbew-9845290-1
15	63,210	-17.55	Win.Trojan.Crypted-31

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN DECEMBER

Remember, sharing is caring.