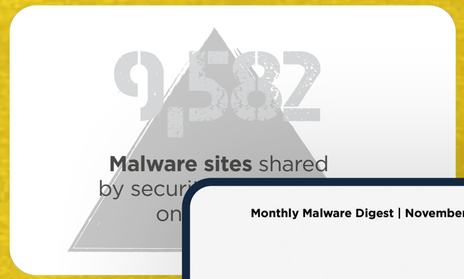
NOVEMBER 2023

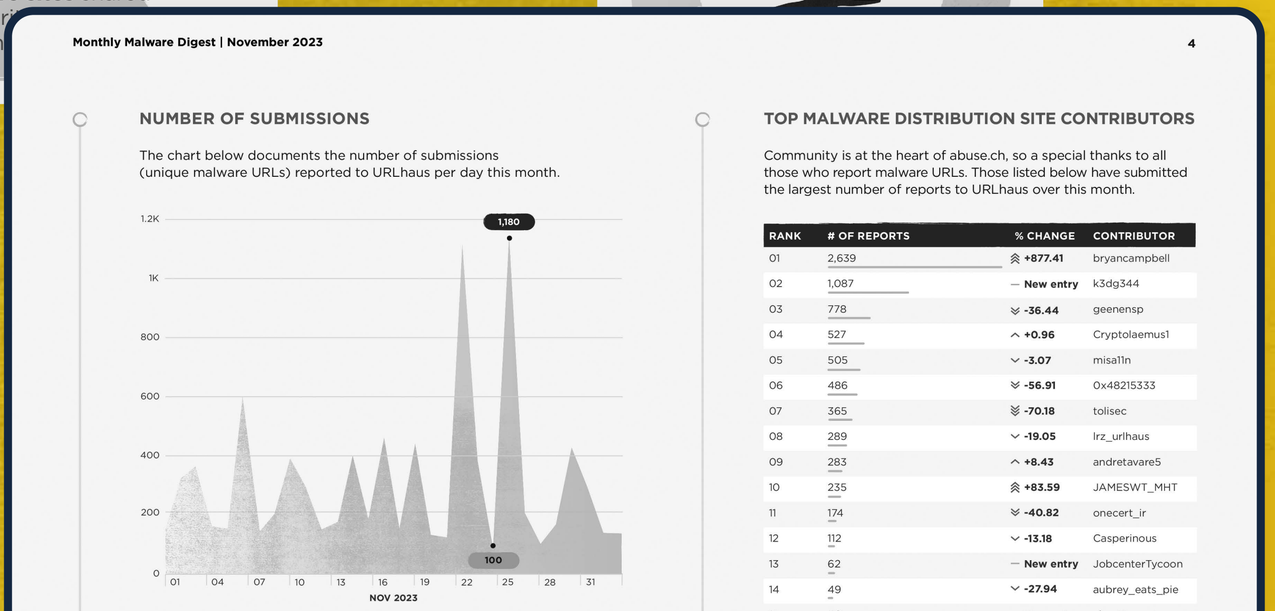
SPAMHAUS ABUSE.ch

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

9,582

Malware sites shared by security researchers on URLhaus

-16.5%

decrease on the previous month

15,134

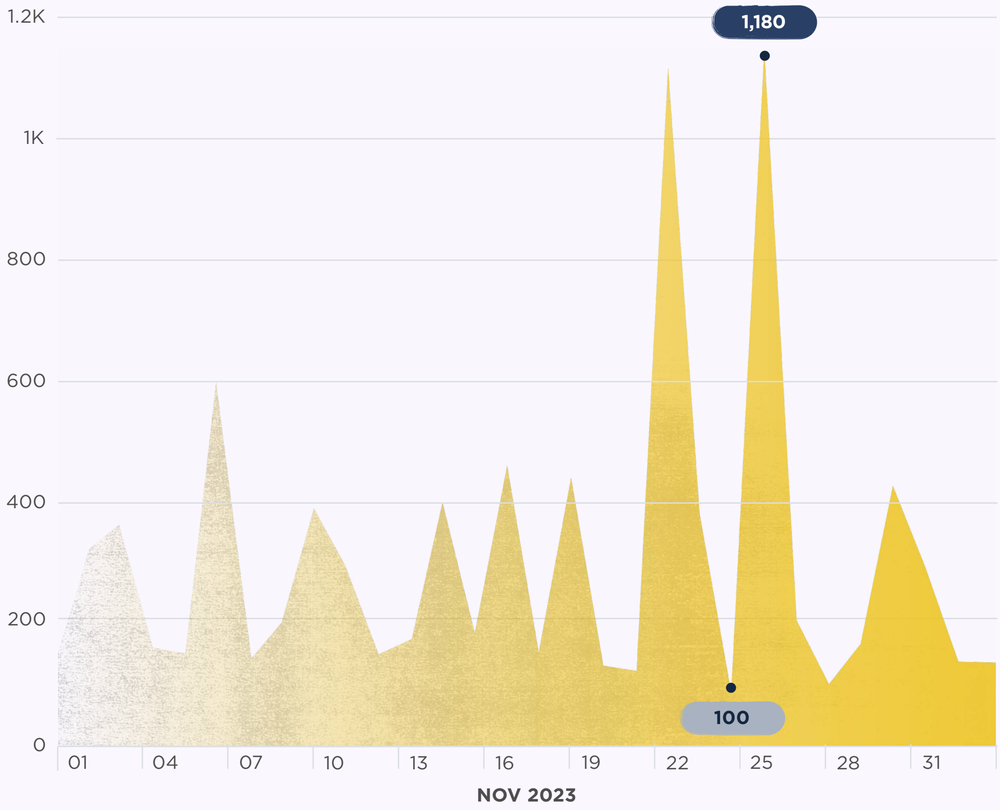
Abuse reports sent out to hosting providers and network owners

93.1%

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.

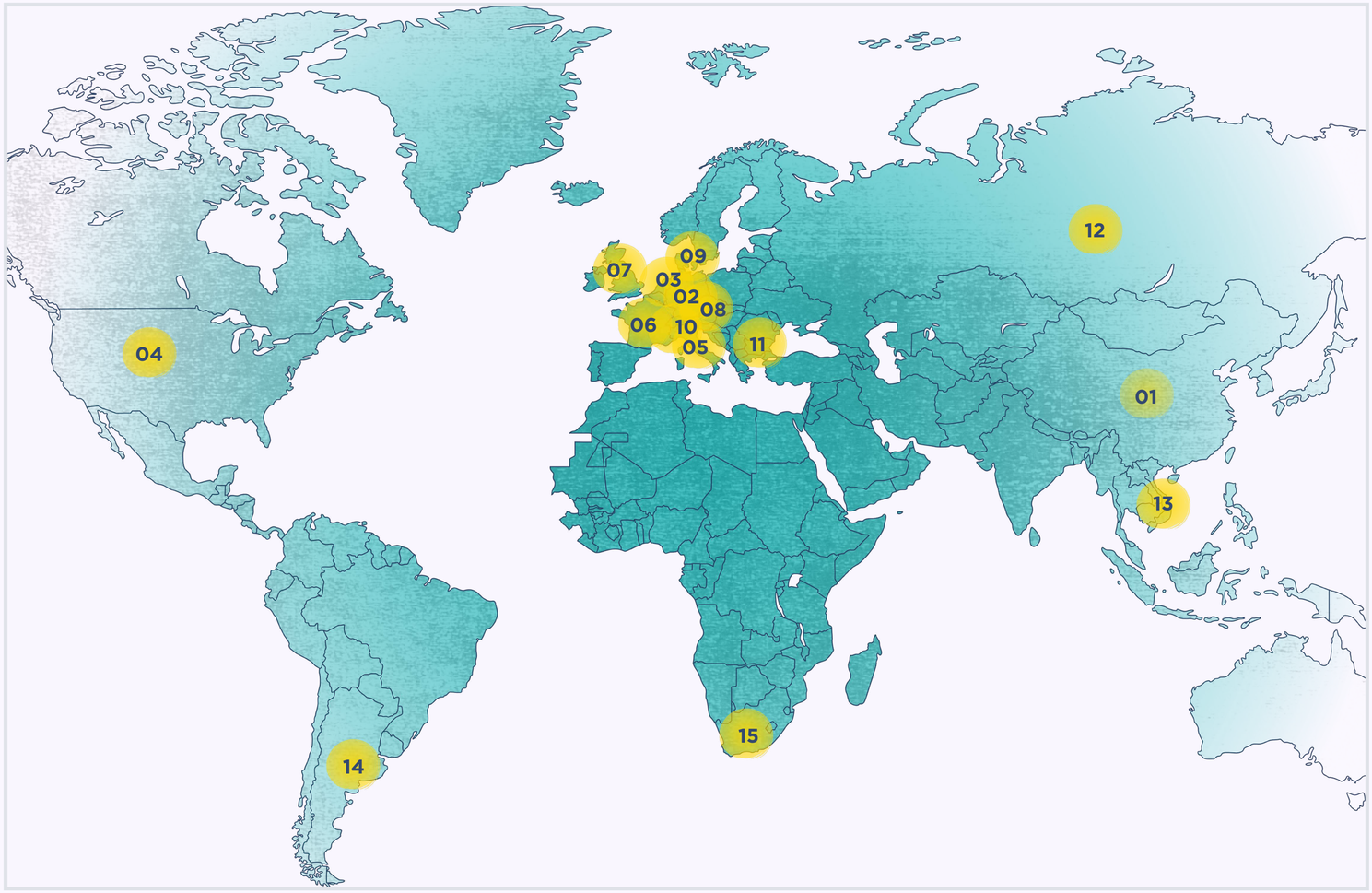


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	2,639	+877.41	bryancampbell
02	1,087	New entry	k3dg344
03	778	-36.44	geenensp
04	527	+0.96	Cryptolaemus1
05	505	-3.07	misa11n
06	486	-56.91	0x48215333
07	365	-70.18	tolisec
08	289	-19.05	lrz_urlhaus
09	283	+8.43	andretavare5
10	235	+83.59	JAMESWT_MHT
11	174	-40.82	onecert_ir
12	112	-13.18	Casperinous
13	62	New entry	JobcenterTycoon
14	49	-27.94	aubrey_eats_pie
15	46	New entry	abus3reports

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	653	-31.91	China
02	534	-33.08	Germany
03	473	-50.00	Netherlands
04	456	-89.79	United States
05	306	+152.89	Italy
06	292	+64.04	France
07	268	+46.45	United Kingdom
08	257	New entry	Austria
09	248	New entry	Denmark
10	247	New entry	Switzerland
11	232	+105.31	Bulgaria
12	204	-55.56	Russia
13	126	-47.06	Vietnam
14	117	-50.21	Argentina
15	40	-70.37	South Africa

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	2,269	AS15169	GOOGLE	United States
02	662	AS13335	CLOUDFLARENET	United States
03	479	AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	China
04	362	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
05	252	AS10617	SION S.A	Argentina
06	249	AS16625	AKAMAI-AS	United States
06	249	AS20940	AKAMAI-ASN1	Netherlands
07	232	AS19871	NETWORK-SOLUTIONS-HOSTING	United States
08	225	AS24940	HETZNER-AS	Germany
09	217	AS36352	AS-COLOCROSSING	United States
10	197	AS19679	DROPBOX	United States
11	196	AS47541	VKONTAKTE-SPB-AS vk.com	Russia
12	163	AS394711	LIMENET	United States
13	160	AS19557	CHANGEIP-01	United States
14	137	AS216240	MORTALSOFT	null

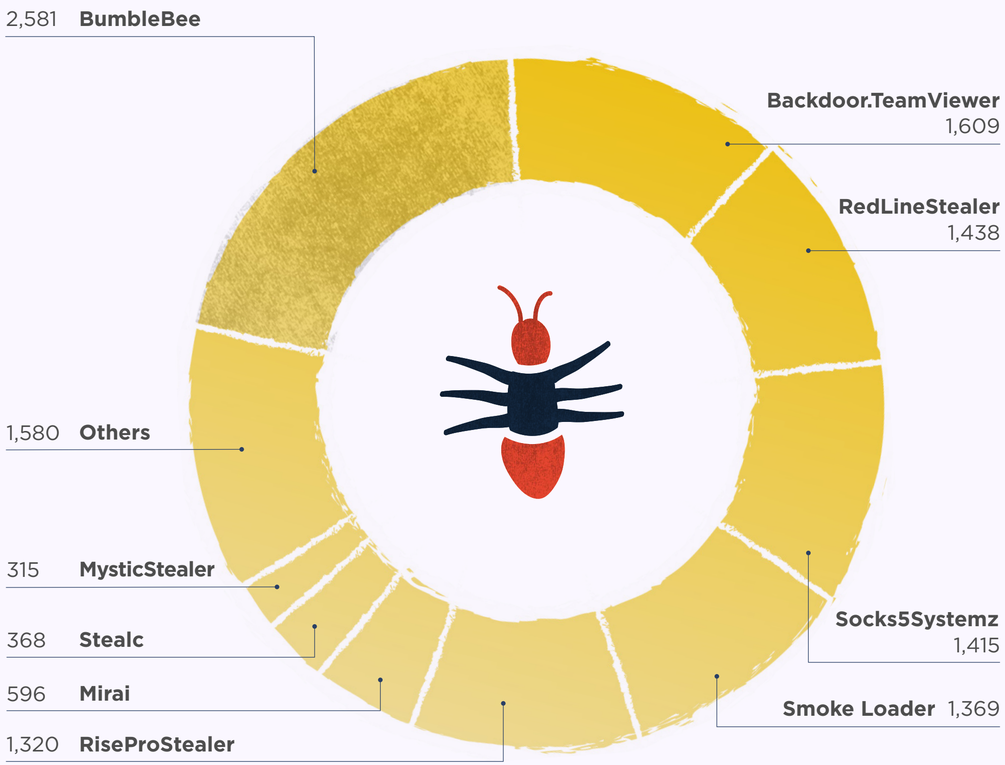
TOP MALWARE HOSTS

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	196	vk.com	VK	Russia
02	191	www.dropbox.com	Dropbox	United States
03	170	cdn.discordapp.com	Discord	United States
04	139	drive.google.com	Google	United States
05	96	wtools.io	n/a	null
06	72	pastebin.com	Pastebin	United States
07	41	paste.ee	Paste.ee	null
08	21	docs.google.com	Google	United States
08	21	transfer.sh	n/a	null
09	17	pasteio.com	n/a	null

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	BumbleBee	+71.50		2,581
02	Smoke Loader	0.00		1,369
03	UACModuleSmokeLoader	-15.79		208
04	Stealc	-33.81		368
05	RedLineStealer	-38.70		1,438
06	MarsStealer	-52.61		200
07	Mirai	-55.02		596
08	MysticStealer	-58.22		315
09	Amadey	-87.09		275
10	Backdoor.TeamViewer	New entry		1,609
10	Socks5Systemz	New entry		1,415
10	RiseProStealer	New entry		1,320
10	RemcosRAT	New entry		314
10	IcedID	New entry		305
10	LummaStealer	New entry		278

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

9,928

Malware samples shared by security researchers on MalwareBazaar

-9.9%

decrease on the previous month

1,393

Active hunting rules

+3%

increase on the previous month

28.40MB

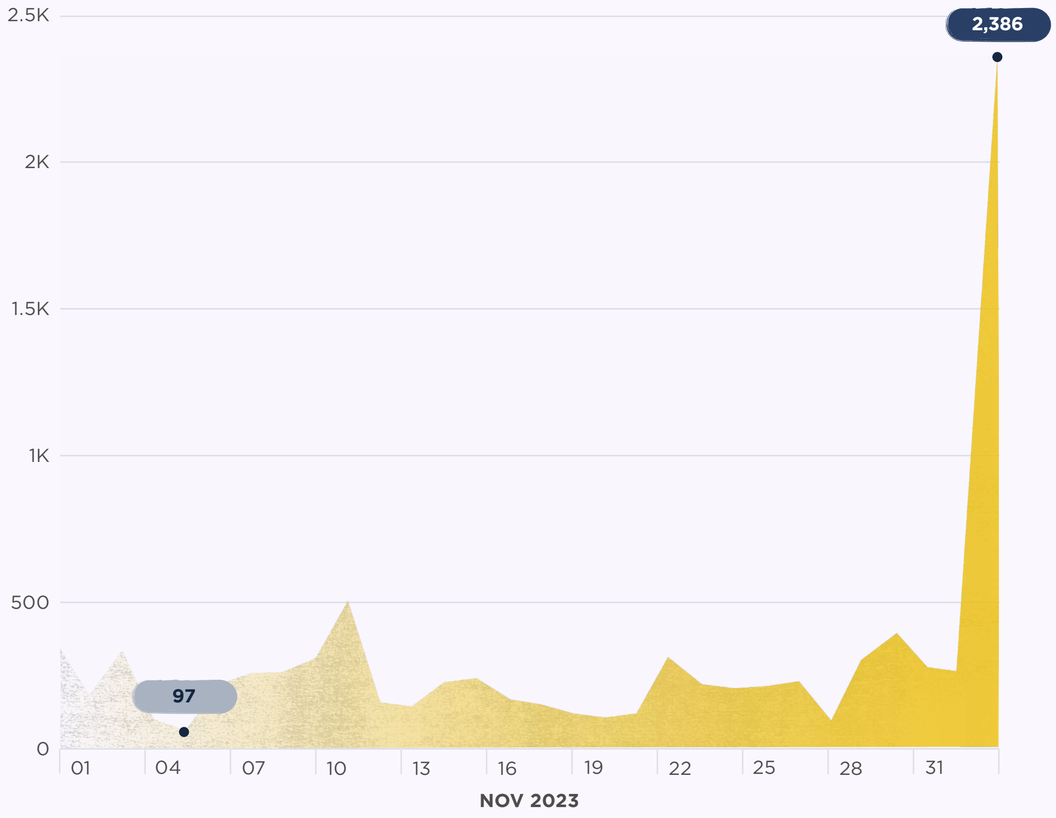
Average size of a malware sample

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.



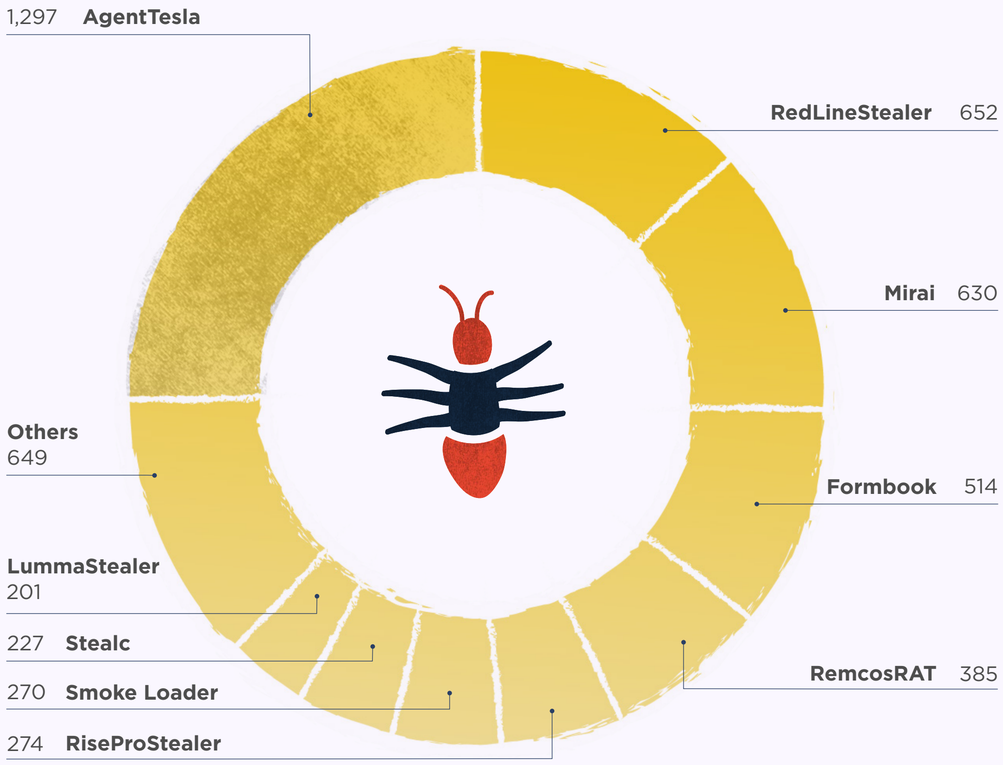
TOP SAMPLE CONTRIBUTORS

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	1,028	-56.99	@andretavare5
02	444	-18.68	@cocaman
03	299	-26.35	@JAMESWT_MHT
04	271	+1.50	@lowmal3
05	268	+54.02	@adrian__luca
06	217	-56.25	@elfdigest
07	158	+44.95	@smica83
08	124	-31.49	@TeamDreier
09	120	New entry	@NIXLovesCooper
10	108	-12.20	@malwarelabnet
10	108	-28.48	@onecert_ir
11	68	New entry	@Porcupine
11	68	-27.66	@pr0xylife
12	47	New entry	@adm1n_usa32
13	40	New entry	@1ZRR4H

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



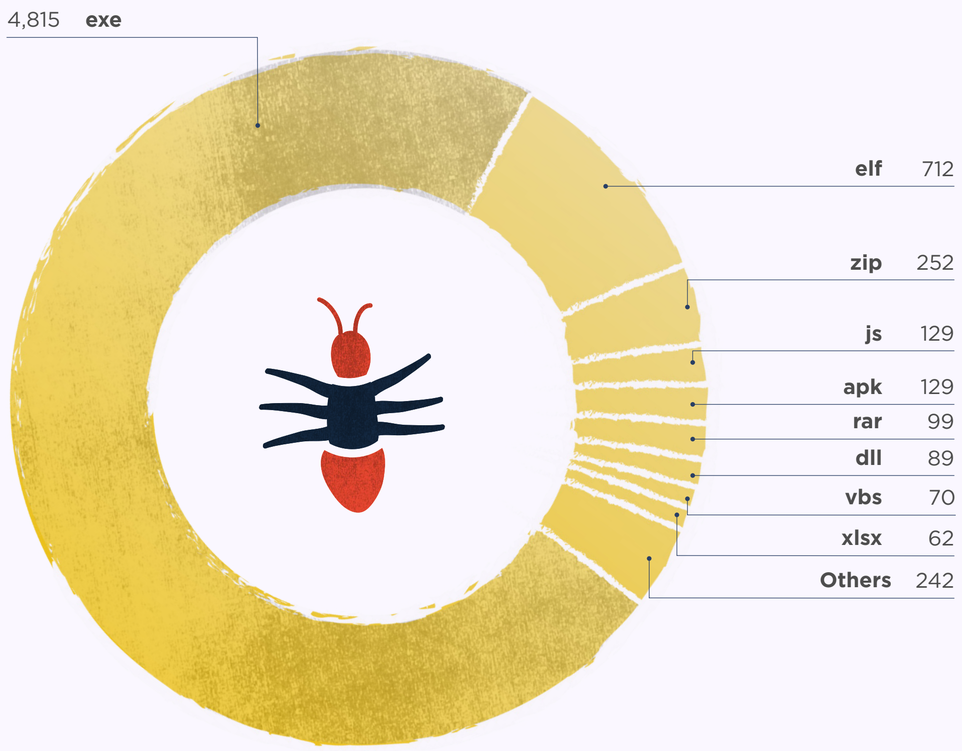
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	GuLoader	^ +26.17		188
02	Formbook	^ +15.51		514
03	Stealc	v -13.36		227
04	LummaStealer	v -15.55		201
05	AgentTesla	v -20.58		1,297
06	SnakeKeylogger	v -24.66		110
07	IRATA	v -28.48		108
08	Smoke Loader	vv -45.45		270
09	Mirai	vv -56.16		630
10	RedLineStealer	vv -58.44		652
11	RemcosRAT	— New entry		385
11	RiseProStealer	— New entry		274
11	MarsStealer	— New entry		86
11	Loki	— New entry		83
11	njrat	— New entry		74

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	1,972	NET	malware-lu
02	1,533	DebuggerCheck__API	n/a
03	1,198	maldoc_find_kernel32_base_method_1	Didier Stevens
04	993	NETexecutableMicrosoft	malware-lu
05	728	MD5_Constants	phoul (@phoul)
06	714	DebuggerCheck__QueryInfo	n/a
07	580	pe_no_import_table	n/a
08	542	INDICATOR_EXE_Packed_ConfuserEx	ditekSHen
09	497	INDICATOR_SUSPICIOUS_Binary_References_Browsers	ditekSHen
10	451	redline_stealer_1	Nikolaos 'n0t' Totosis
11	450	maldoc_getEIP_method_1	Didier Stevens
12	447	RIPEMD160_Constants	phoul (@phoul)
12	447	SHA1_Constants	phoul (@phoul)
13	437	shellcode	nex
14	408	INDICATOR_EXE_Packed_GEN01	ditekSHen

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)

10,771

Indicators of compromise (IOCS) shared on ThreatFox

-30.5%

decrease on the previous month

2,150

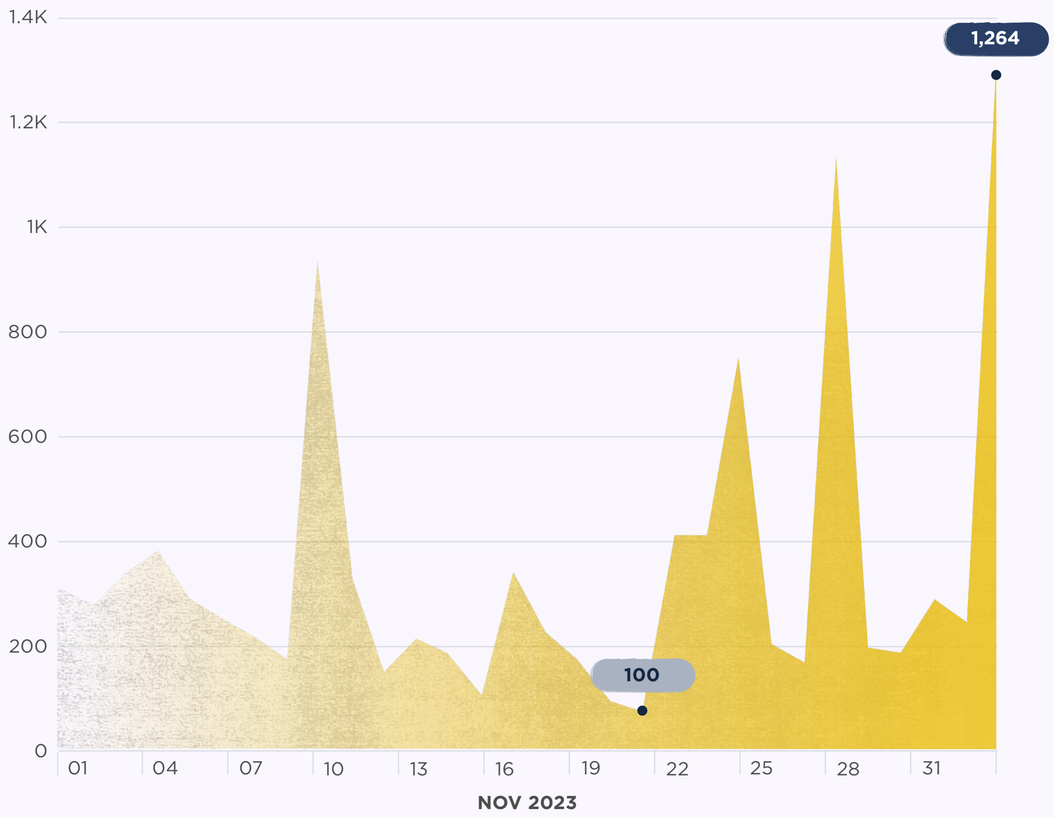
IOCs relating to Cobalt Strike

-43.18%

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.



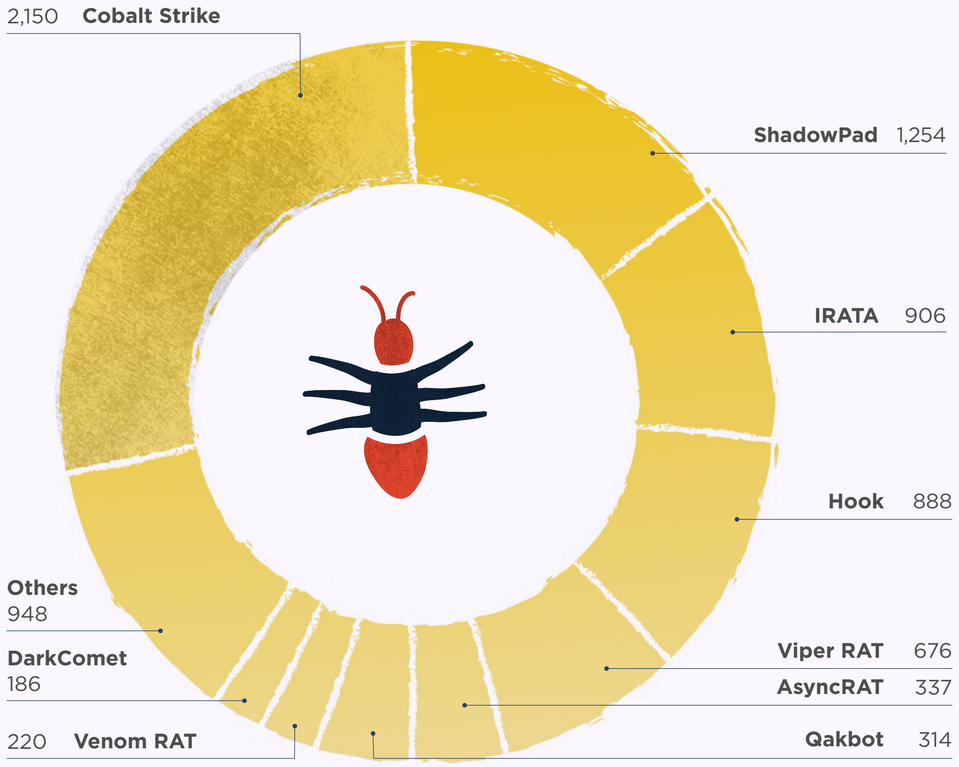
IOC TYPE

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	6,557	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
02	1,810	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
03	1,588	url	botnet_cc	URL that is used for botnet Command&control (C&C)
04	337	url	payload_ delivery	URL that delivers a malware payload
05	317	domain	payload_ delivery	Domain name that delivers a malware payload
06	114	md5_hash	payload	MD5 hash of a malware sample (payload)
06	114	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
07	38	ip:port	payload_ delivery	ip:port combination that delivers a malware payload
08	6	sha1_hash	payload	SHA1 hash of a malware sample (payload)

TOP MALWARE FAMILIES

This chart shows the malware families that were associated with the largest number of IOCs this month.



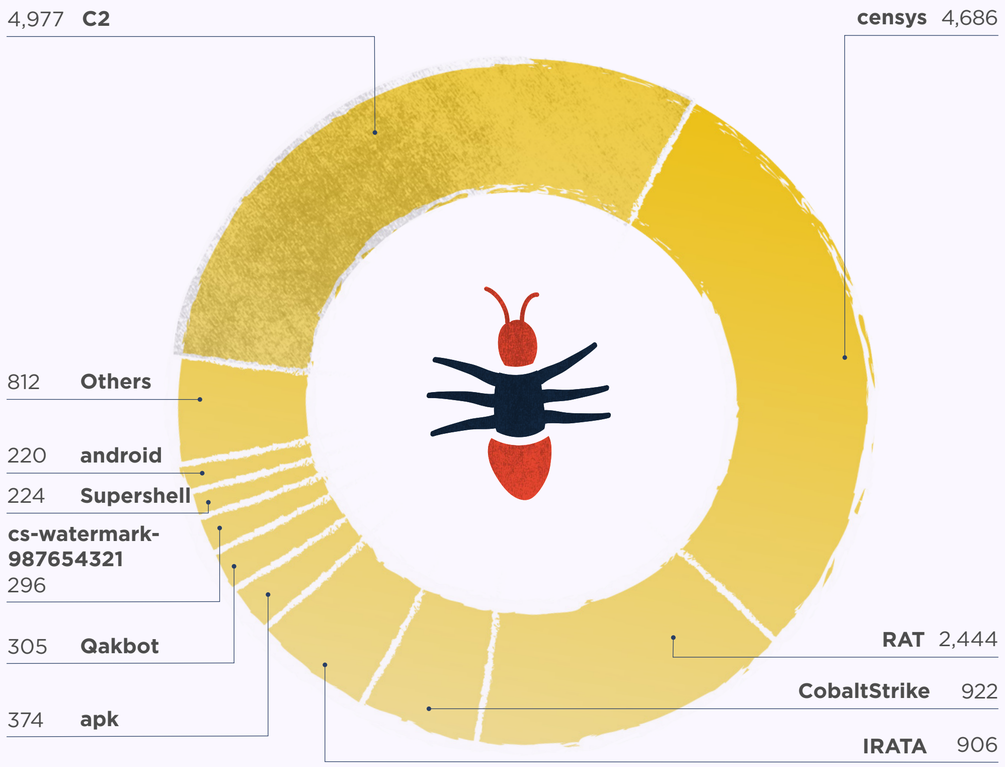
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

RANK	MALWARE FAMILY	% CHANGE	LAST 3 MONTHS	# OF IOCS
01	ShadowPad	+459.82		1,254
02	Lumma	+1.89		162
03	Qakbot	-24.52		314
04	IRATA	-29.66		906
05	Cobalt Strike	-43.18		2,150
06	Havoc	-44.19		173
07	AsyncRAT	-49.40		337
08	Quasar RAT	-53.90		183
09	Hook	New entry		888
09	Viper RAT	New entry		676
09	Venom RAT	New entry		220
09	DarkComet	New entry		186
09	Coper	New entry		150
09	Vidar	New entry		146
09	BianLian	New entry		134

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	RAT	^ +165.08	2,444
02	Qakbot	v -26.33	305
03	IRATA	v -29.66	906
04	censys	v -32.50	4,686
05	CobaltStrike	vv -36.11	922
06	cs-watermark-987654321	vv -36.21	296
07	C2	vv -44.91	4,977
08	AMAZON-02	vv -49.86	183
09	DIGITALOCEAN-ASN	vv -91.93	140
10	apk	— New entry	374
10	Supershell	— New entry	224
10	android	— New entry	220
10	stealer	— New entry	183
10	Shadowpad	— New entry	156
10	Coper	— New entry	150

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

9,242,368

File scans conducted on YARAify

8,141,645

Distinct files that had scans performed on them

+137.5%

increase in file scans on the previous month

+153.4%

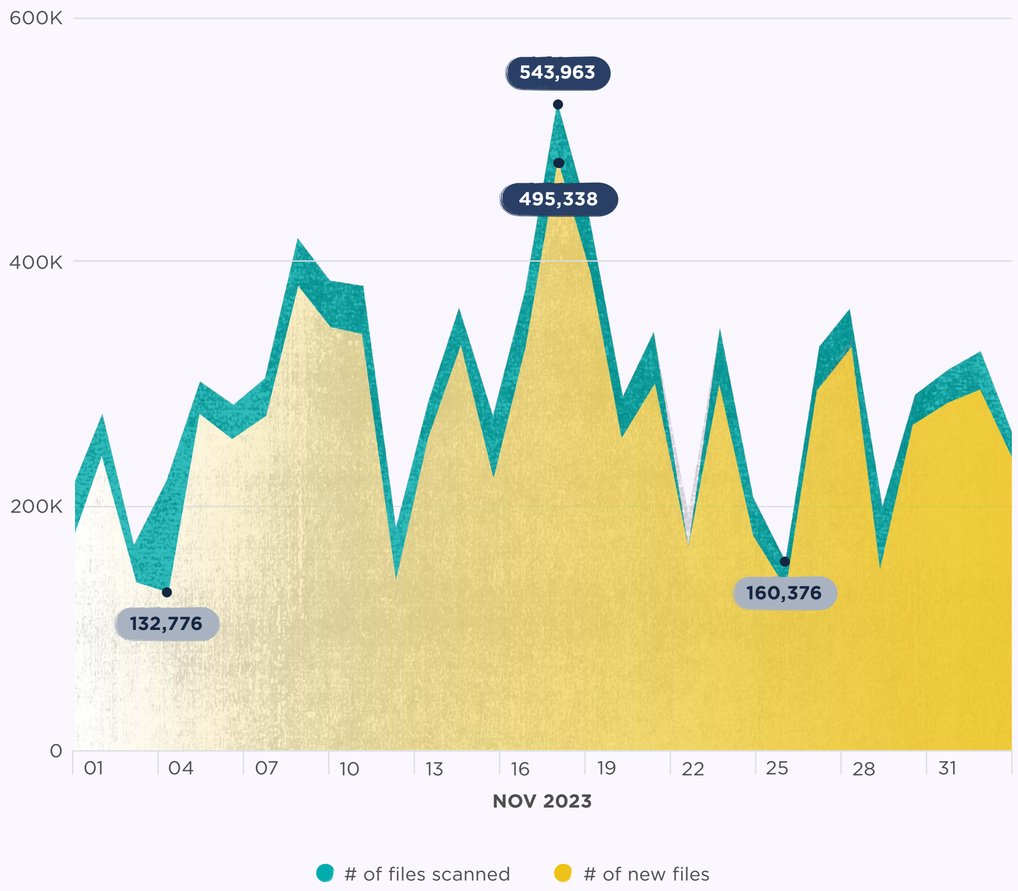
increase in distinct files on the previous month

18,558

YARA rules deployed on YARAify and available for hunting

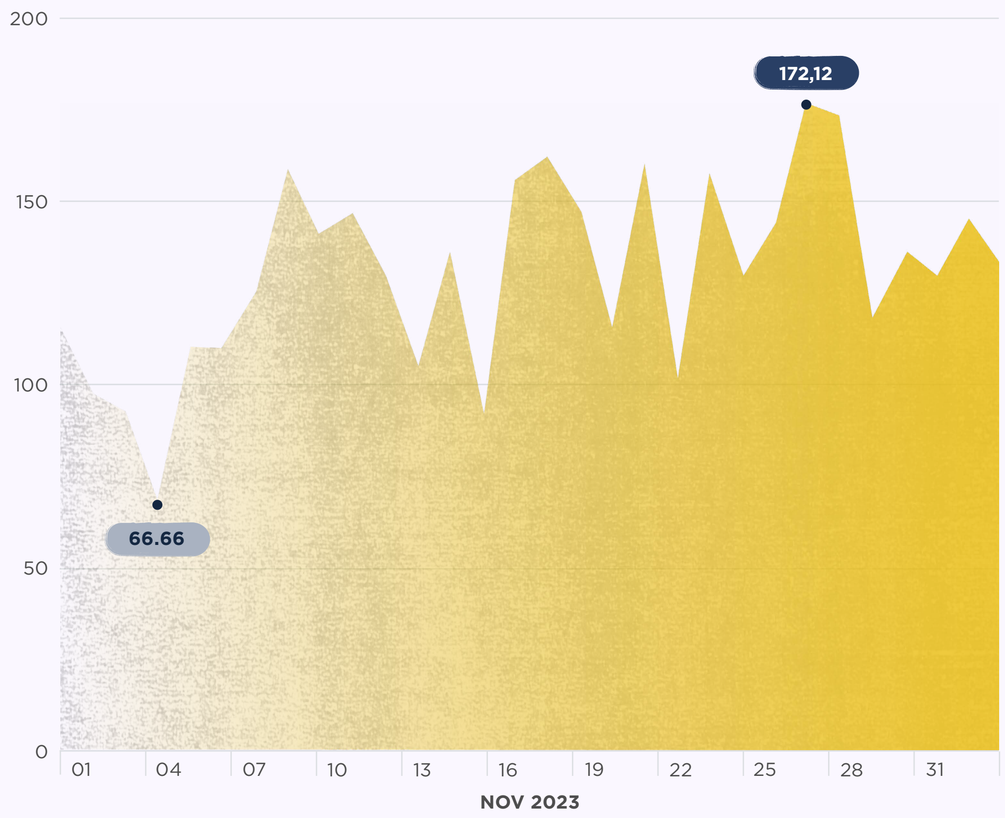
FILES SCANNED PER DAY

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	6,958,802	+146.48	maldoc_getEIP_method_1	Didier Stevens
02	429,208	+48.16	DebuggerCheck__API	n/a
03	291,934	+93.51	maldoc_find_kernel32_base_method_1	Didier Stevens
04	284,252	+61.99	NET	malware-lu
05	266,441	+191.08	Check_Dlls	n/a
06	218,638	+162.56	SUSP_XORed_URL_in_EXE_RID2E46	n/a
07	218,531	New entry	SUSP_XORed_URL_In_EXE	Florian Roth (Nextron Systems)
08	179,669	+15.16	UPXV200V290MarkusOberhumerLaszloMolnar-JohnReiser	malware-lu
09	160,780	+18.59	UPXv20MarkusLaszloReiser	malware-lu
10	144,123	+96.07	SHA1_Constants	phoul (@phoul)
10	144,123	+96.08	RIPEMD160_Constants	phoul (@phoul)
11	142,293	+62.42	MD5_Constants	phoul (@phoul)
12	121,309	+78.83	DebuggerException__SetConsoleCtrl	n/a
13	114,610	+102.08	SHA512_Constants	phoul (@phoul)
14	113,077	+137.61	malware_shellcode_hash	JPCERT/CC Incident Re-sponse Group

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	6,492,788	+263.87	PUA.Win.Packer.Lccwin-2
02	4,330,723	+258.09	Win.Trojan.Obfus-38
03	2,789,518	+265.55	Win.Trojan.Qukart-6874817-0
04	1,991,715	+270.78	Win.Malware.Qukart-6838239-0
05	1,949,548	+232.75	Win.Trojan.Padodor-9877164-0
06	799,052	New entry	Win.Trojan.Berbew-10013977-0
07	727,240	+259.24	Win.Trojan.Crypted-29
08	724,479	+257.69	Win.Trojan.Crypted-30
09	548,802	+338.99	Win.Packed.Razy-10010080-0
10	527,729	New entry	Win.Malware.Padodor-10012877-0
11	495,897	+472.15	Win.Trojan.Berbew-9845290-1
12	455,936	+236.28	Win.Packed.Razy-10009896-0
13	442,112	+274.34	Win.Trojan.Crypted-28
14	400,406	+283.95	Win.Packed.Lazy-10005437-0
15	399,014	New entry	Win.Packed.Razy-10012935-0

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN JANUARY

Remember, sharing is caring.