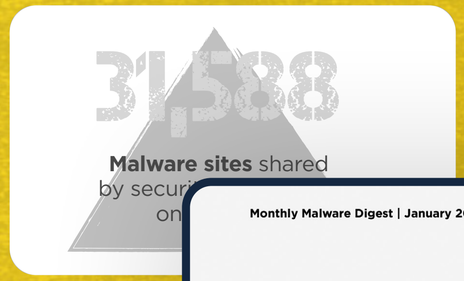
JANUARY 2023

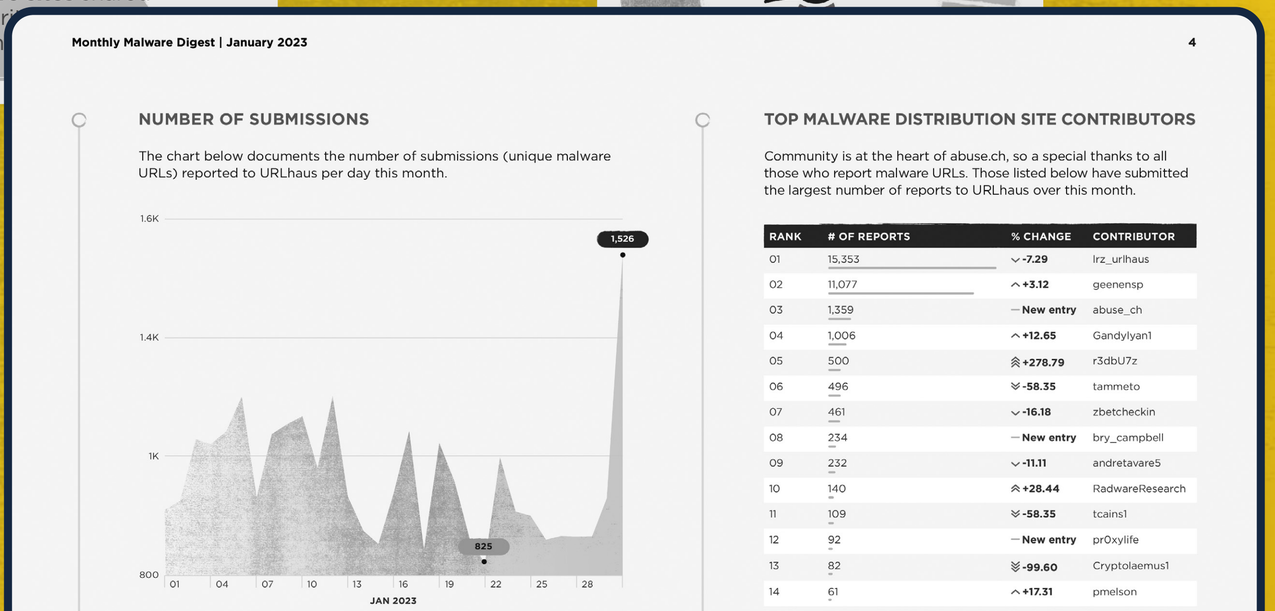
SPAMHAUS ABUSE.ch

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	**Malware Bazaar**
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	**Malware Bazaar**
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

31,588

Malware sites shared by security researchers on URLhaus

-40%

Decrease month on month

34,412

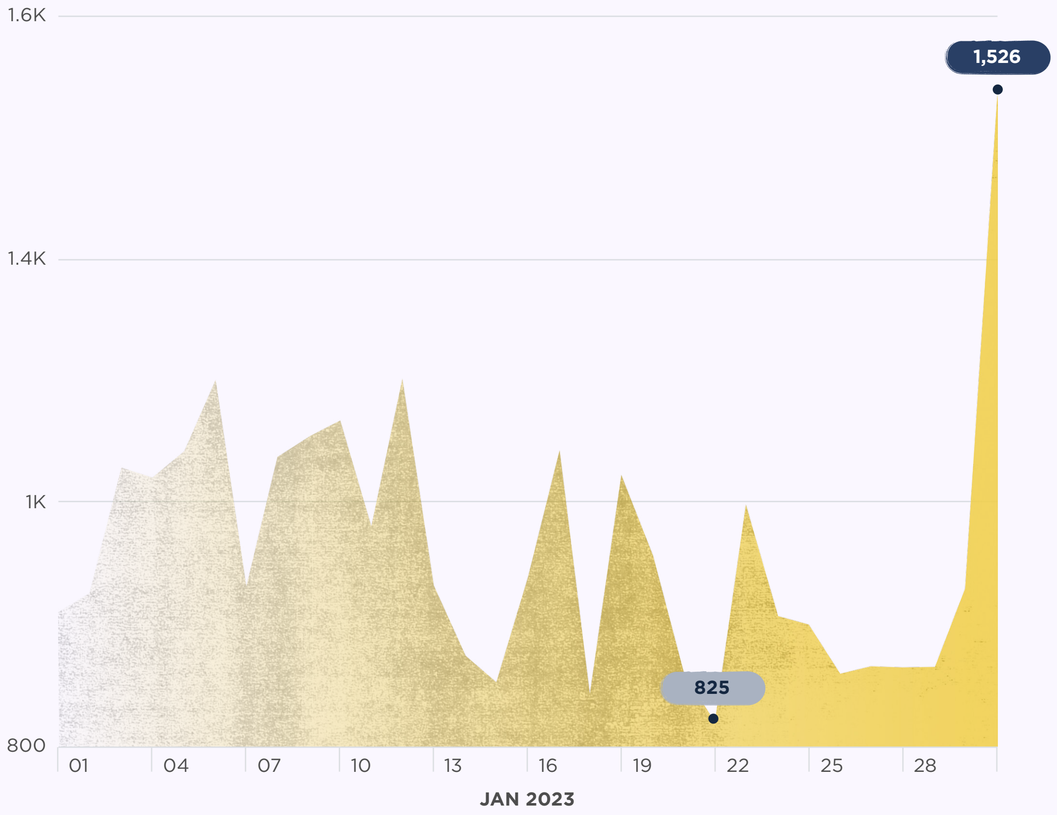
Abuse reports sent out to hosting providers and network owners

93%

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.

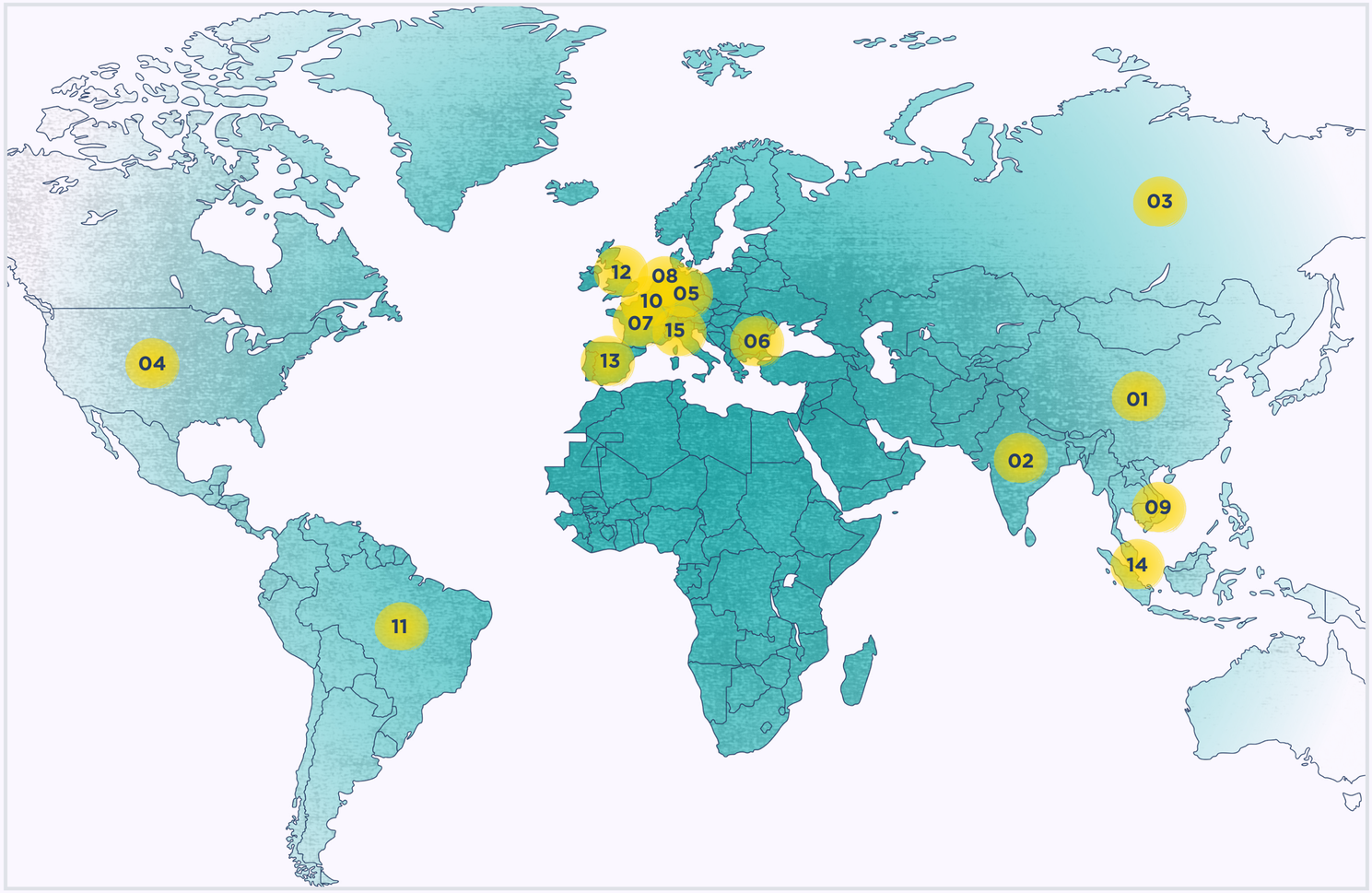


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	15,353	-7.29	lrz_urlhaus
02	11,077	+3.12	geenensp
03	1,359	New entry	abuse_ch
04	1,006	+12.65	Gandylyan1
05	500	+278.79	r3dbU7z
06	496	-58.35	tammeto
07	461	-16.18	zbetcheckin
08	234	New entry	bry_campbell
09	232	-11.11	andretavare5
10	140	+28.44	RadwareResearch
11	109	-58.35	tcains1
12	92	New entry	pr0xylife
13	82	-99.60	Cryptolaemus1
14	61	+17.31	pmelson
15	41	New entry	crep1x

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	6,267	-6.20	China
02	2,153	-28.42	India
03	815	+197.45	Russia
04	609	-95.37	United States
05	202	-81.55	Germany
06	140	New entry	Bulgaria
07	99	-82.81	France
08	78	-74.68	Netherlands
09	63	-76.40	Viet Nam
10	52	New entry	Luxembourg
11	52	-77.78	Brazil
12	50	-89.65	United Kingdom
13	44	New entry	Spain
14	43	-73.78	Singapore
15	38	New entry	Switzerland

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	4,498	AS4837	CHINA 169-BACKBONE	China
02	2,049	AS9829	BSNL-NIB	India
03	1,573	AS4134	CHINANET-BACKBONE	China
04	505	AS49943	ITRESHENIYA	Russia
05	179	AS211252	DELIS	Netherlands
06	132	AS59425	HORIZONMSK	Russia
07	80	AS3462	HINET	Taiwan
08	79	AS53667	PONYNET	United States
09	69	AS15169	GOOGLE	United States
10	66	AS36352	COLOCROSSING	United States
11	65	AS61272	IST-AS	Lithuania
12	62	AS17813	MTNL-AP	India
13	57	AS210644	AEZA	Russia
14	56	AS36459	GITHUB	United States
15	51	AS13335	CLOUDFLARENET	United States

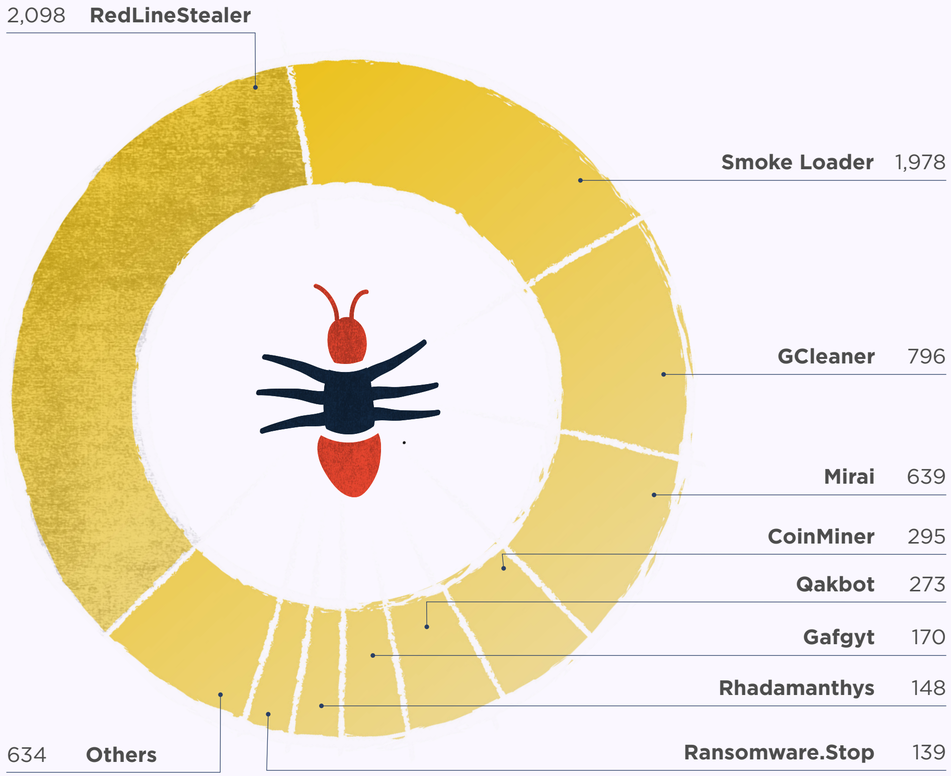
TOP MALWARE HOSTS

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	177	vk.com	VK	Russia
02	172	cdn.discordapp.com	Discord	United States
03	58	github.com	Github	United States
04	37	pastebin.com	Pastebin	New entry
05	20	dropbox.com	Dropbox	United States
06	15	onedrive.live.com	Microsoft	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	Ransomware.Stop	**+43.30**		139
02	Mirai	**+34.81**		639
03	RedLineStealer	**+31.29**		2,098
04	CoinMiner	**+9.26**		295
05	GCleaner	**-4.11**		769
06	Gafgyt	**-7.10**		170
07	ArkeiStealer	**-8.41**		98
08	AgentTesla	**-9.09**		110
09	Quakbot	**-17.02**		273
10	Smoke Loader	**-31.27**		1,978
11	Tofsee	**-42.62**		105
12	Amadey	**-88.32**		111
13	TeamBot	**New entry**		120
14	Rhadamanthys	**New entry**		148
15	LummaStealer	**New entry**		90

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

12,296

Malware samples shared by security researchers on MalwareBazaar

-9.5%

Decrease on the previous month

1,072

Active hunting rules

+2.6%

increase on the previous month

1.5MB

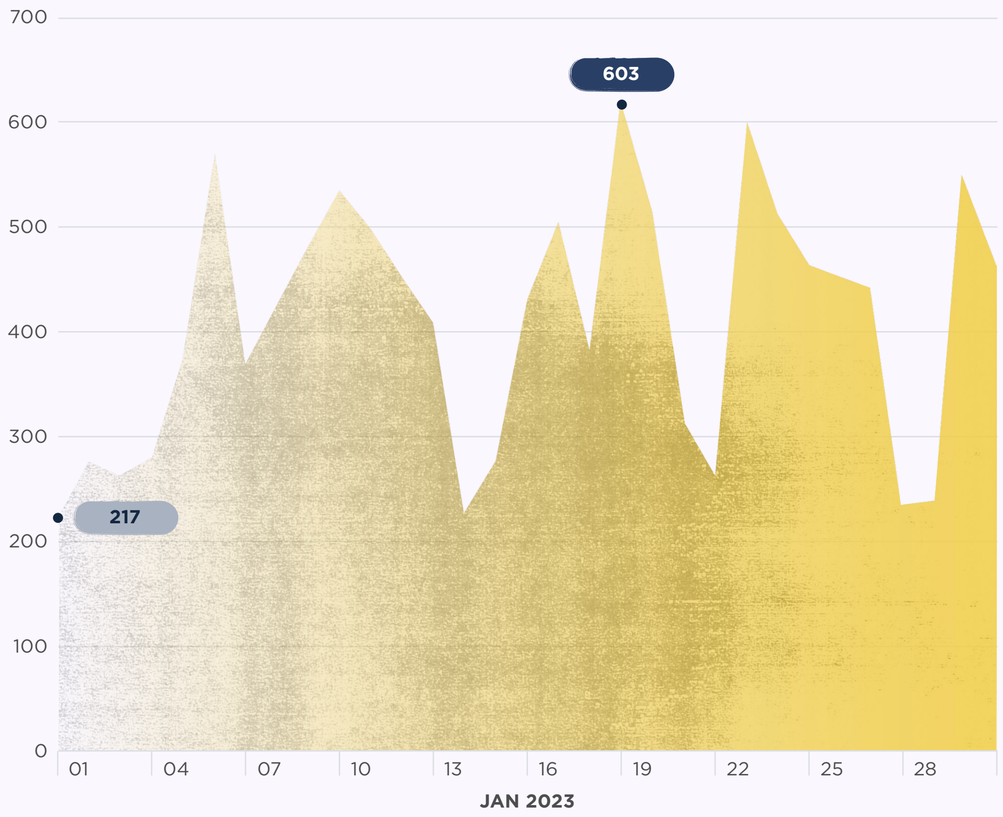
Avarage size of a malware sample

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 MawareBazaar per day this month.



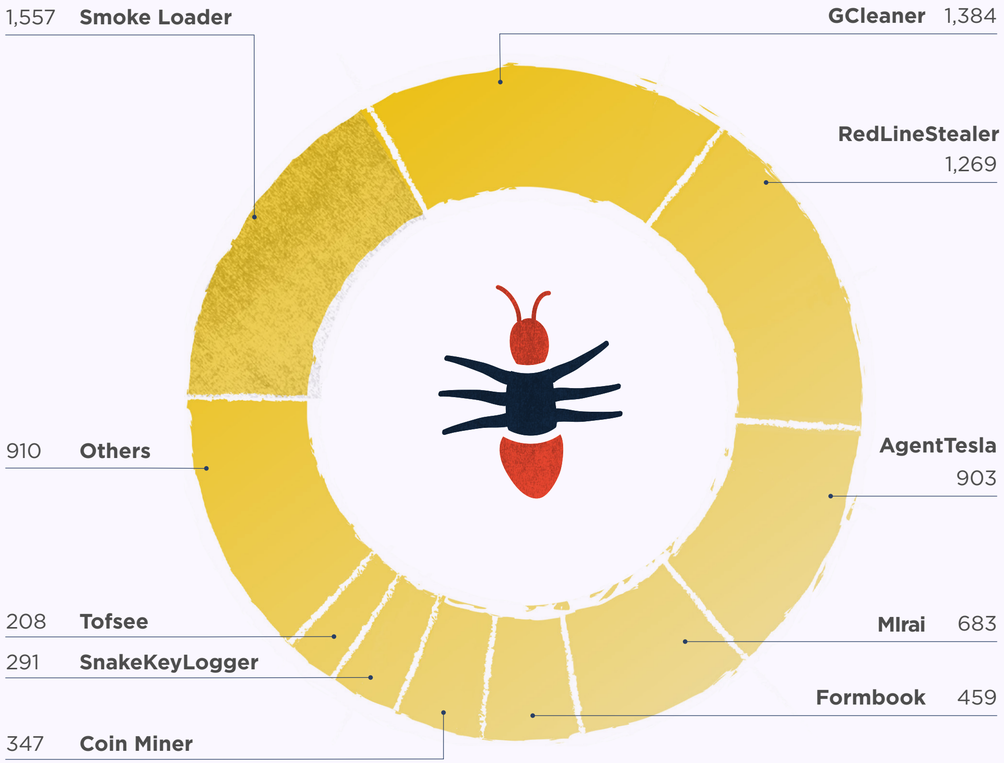
TOP SAMPLE CONTRIBUTORS

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	% CHANGE	CONTRIBUTOR
01	4,988	-9.34	@andretavare5
02	1,160	+7.81	@zbetcheckin
03	472	-39.33	@SecuriteInfoCom
04	307	+36.44	@jstrosch
05	276	+34.63	@cocaman
06	275	+44.74	@adrian__luca
07	253	+148.04	@atomiczsec
08	205	+30.57	@JAMESWT_MHT
09	200	+4.17	@lowmal3
10	188	+104.35	@0xToxin
11	118	+14.56	@James_inthe_box
12	86	-52.49	@petikvx
13	84	New entry	@adm1n_usa32
14	83	-45.03	@pr0xylife
15	82	-6.82	@r3dbU7z

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



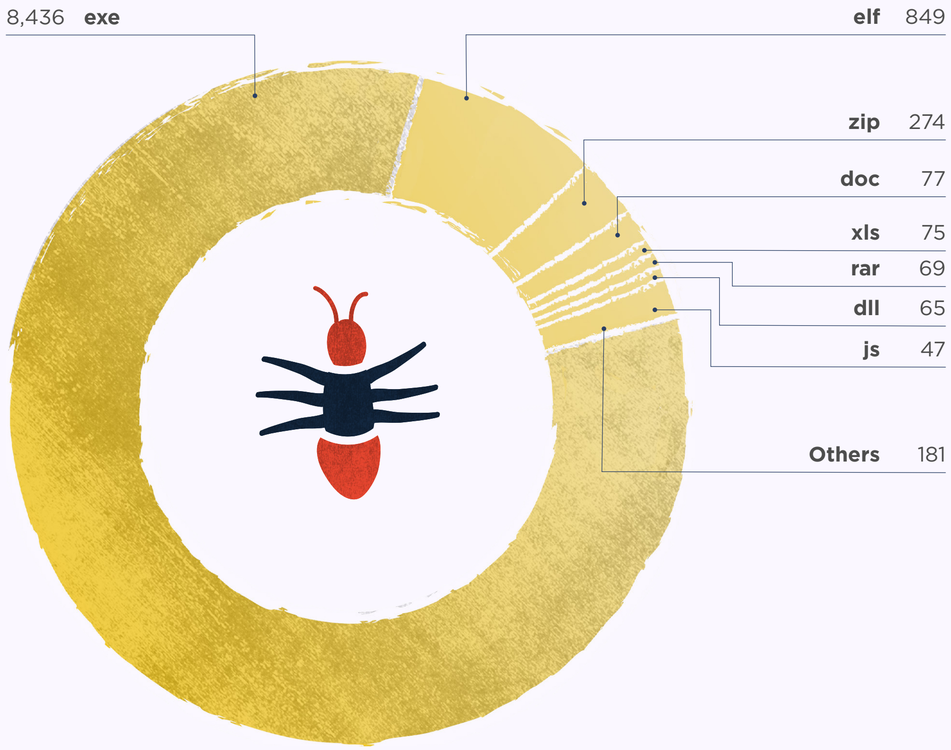
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	Mirai	^ **+27.66**		683
02	RedLineStealer	^ **+26.52**		1,269
03	CoinMiner	^ **+15.67**		347
04	RemcosRAT	^ **+10.07**		164
05	AgentTesla	^ **+9.85**		903
06	GCleaner	^ **+1.32**		1,384
07	Formbook	v **-3.57**		459
08	Smoke Loader	v **-4.18**		1,557
09	ArkeiStealer	vv **-19.46**		149
10	SnakeKeylogger	v **-19.83**		291
11	Gafgyt	v **-20.67**		142
12	Tofsee	v **-26.50**		208
15	DCRat	— **New entry**		154
13	AsyncRAT	— **New entry**		153
14	Loki	— **New entry**		148

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	2061	Windows_Trojan_ Smokeloader_3687686f	Elastic Security
02	1924	cobalt_strike_tmp01925d3f	The DFIR Report
03	1721	win_smokeloader_a2	Pnx
04	1345	win_nymaim_g0	CERT.pl
05	1334	win_gcleaner_auto	Felix Bilstein
06	1184	shellcode	nex
07	990	MALWARE_Win_RedLine	ditekshen
08	661	yara_template	n/a
09	621	CAS_Malware_Hunting	Michael Reinprecht
10	569	myMirai	n/a
11	520	unixredflags3	Tim Brown
12	471	linux_generic_ipv6_catcher	@_lubiedo
13	333	Windows_Trojan_ Tofsee_26124fe4	Elastic Security
13	333	tofsee_yhub	Billy Austin
13	333	win_tofsee_w0	akrasuski1

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)

11,435

Indicators of compromise (IOCS) shared on ThreatFox

-67.7%

Decrease on the previous month

2,272

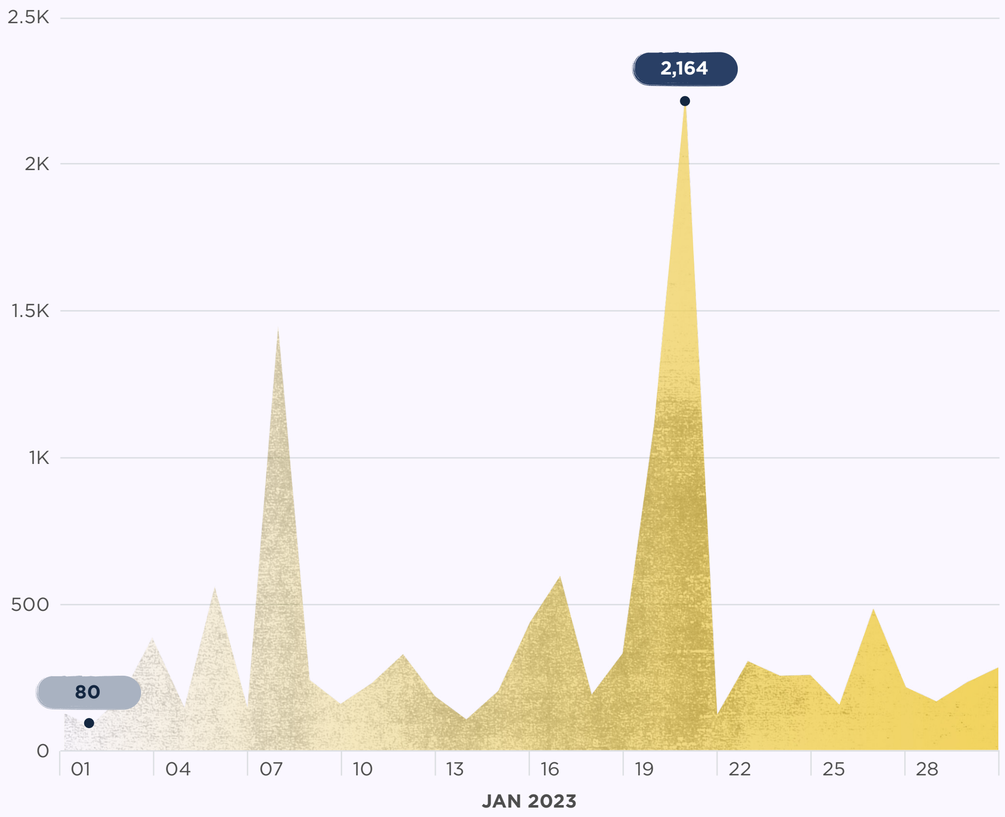
IOCs relating to Vidar

NEW ENTRY

In January

NUMBER OF IOCs SHARED PER DAY

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



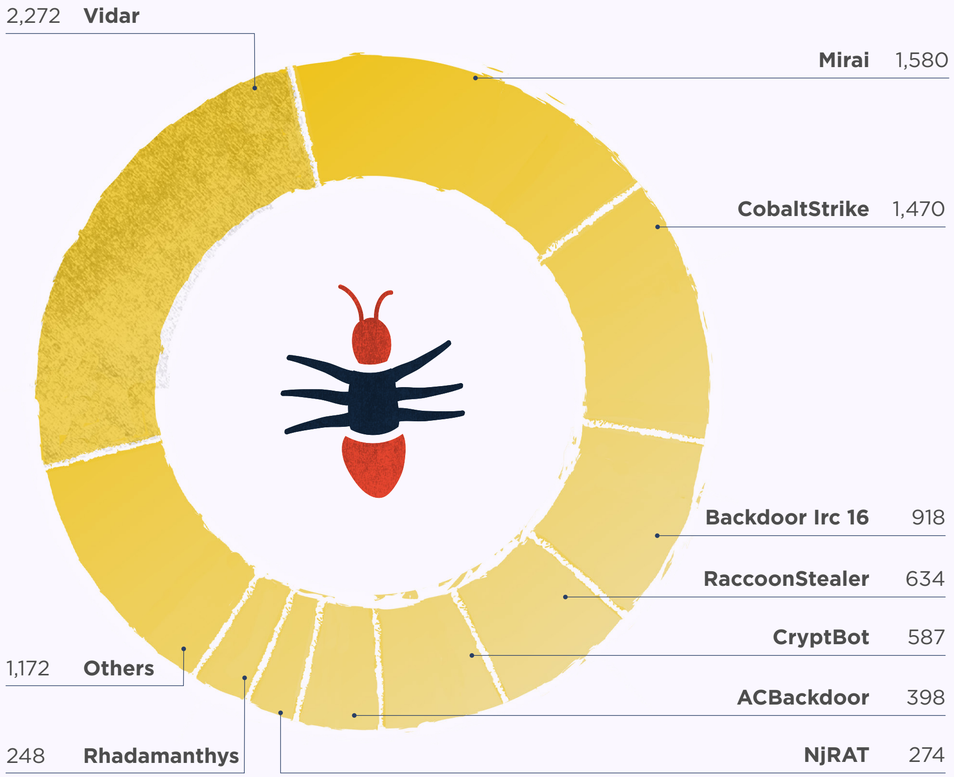
IOC TYPE

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	3,047	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
02	2,943	sha256_hash	payload	SHA256 hash of a malware sample (payload)
03	2,057	url	botnet_cc	URL that is used for botnet Command&control (C&C)
04	2,004	domain	payload_delivery	Domain name that delivers a malware payload
05	1,147	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
06	101	url	payload_delivery	URL that delivers a malware payload
07	82	md5_hash	payload	MD5 hash of a malware sample (payload)
08	46	ip:port	payload_delivery	ip:port combination that delivery a malware payload
09	8	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.



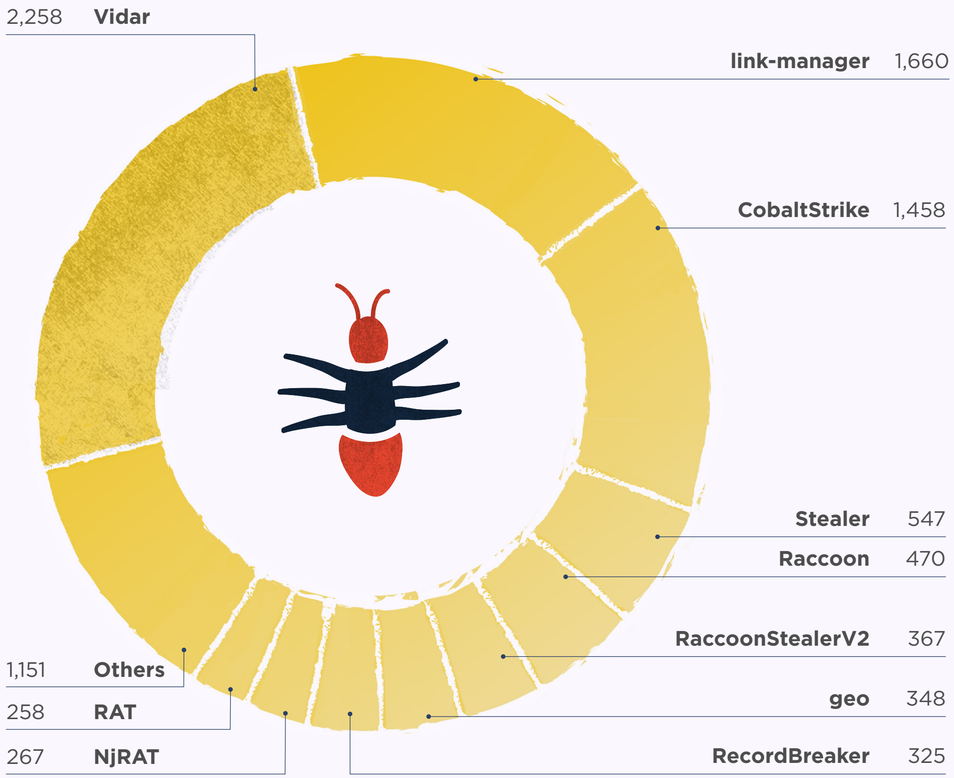
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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	Mirai	**+2,293.94**		1,580
02	Vidar	**+623.57**		2,272
03	NjRAT	**+349.18**		274
04	RedLineStealer	**+33.83**		178
05	IcedID	**+8.42**		219
06	AuroraStealer	**+0.65**		156
07	Cobalt Strike	**-40.70**		1,470
08	Backdoor Irc 16	**New entry**		918
08	RaccoonStealer	**New entry**		634
08	CryptBot	**New entry**		587
08	ACBackdoor	**New entry**		398
08	Rhadamanthys	**New entry**		248
08	Astaroth	**New entry**		223
08	BianLian	**New entry**		204
08	Sliver	**New entry**		192

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	Vidar	— **New entry**	2,258
02	link-manager	— **New entry**	1,660
03	CobaltStrike	— **New entry**	1,458
04	Stealer	— **New entry**	547
05	Raccoon	— **New entry**	470
06	RaccoonStealerV2	— **New entry**	367
06	geo	— **New entry**	348
06	RecordBreaker	— **New entry**	325
06	NjRAT	— **New entry**	267
06	RAT	— **New entry**	258
06	Rhadamanthys	— **New entry**	249
06	BRA	— **New entry**	236
06	RaccoonStealer	— **New entry**	228
06	Astaroth	— **New entry**	223
06	RedPacketSecurity	— **New entry**	215

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

2,210,611

File scans conducted
on YARAify

1,820,230

Distinct files
that had scans performed on them

-8.6%

Decrease in
file scans on the previous month

-9.4%

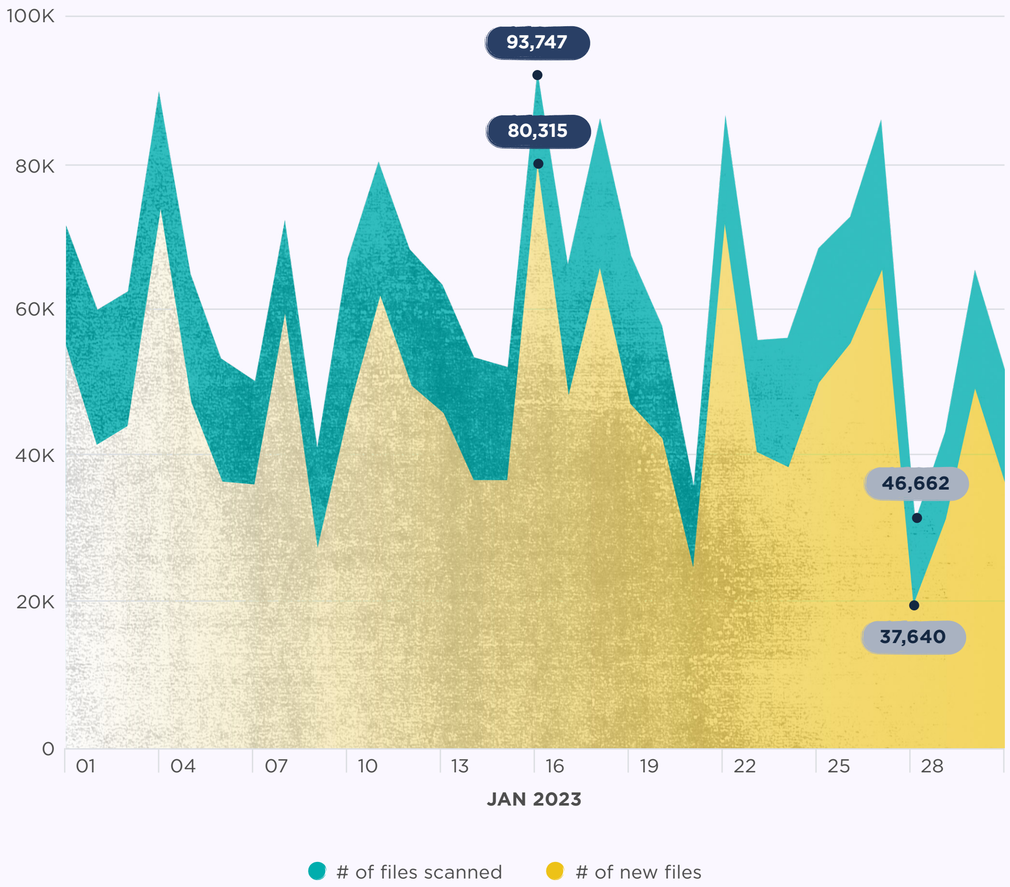
Decrease in
files on the previous month

14,442

YARA rules deployed
on YARAify and available for hunting

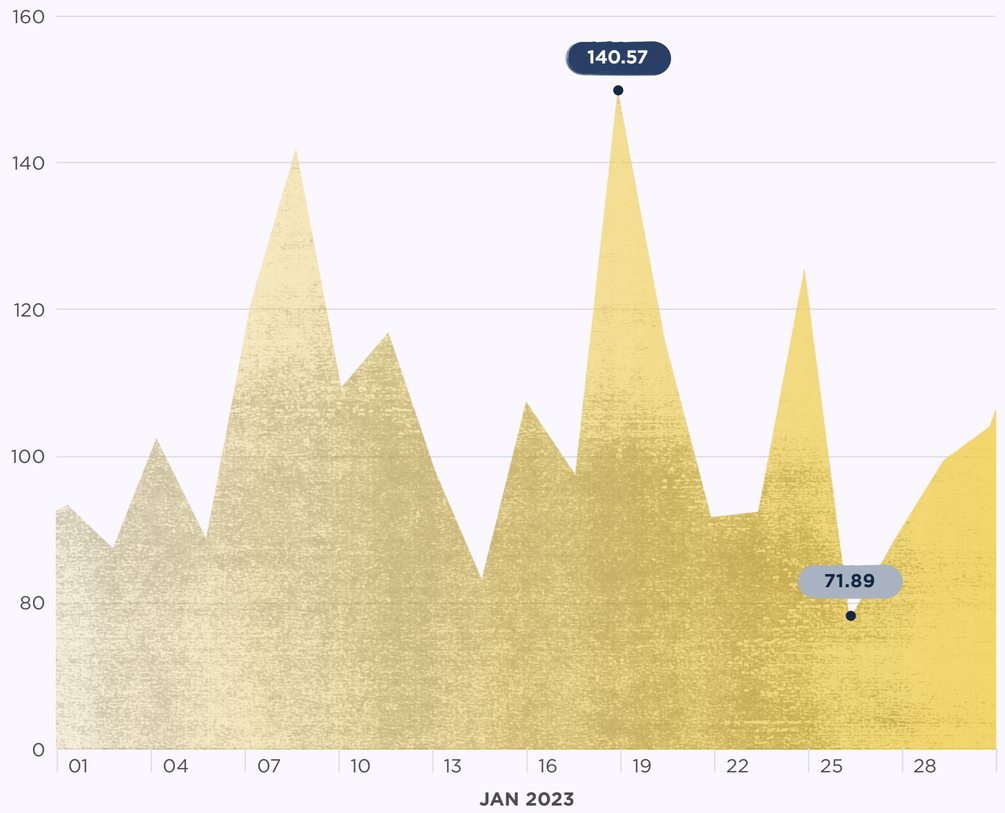
FILES SCANNED PER DAY

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	112,413	— New entry	QbotStuff	anonymous
02	97,764	⇈ +296.08	TeslaCryptPackedMalware	n/a
03	75,847	^ +14.86	command_and_control	CD_R0M_
04	68,424	⇈ +200.75	INDICATOR_EXE_Packed_MPress	ditekSHen
05	65,202	— New entry	yara_template	n/a
06	64,970	— New entry	BitcoinAddress	Didier Stevens (@DidierStevens)
07	50,856	⇊ -81.99	AsyncRat_Detection_Dec_2022	NULL
08	40,563	— New entry	shellcode	nex
09	34,349	— New entry	Disable_Defender	iam-py-test
10	32,395	⇈ +52.90	win_sality_auto	Felix Bilstein
11	27,886	^ +7.08	cobalt_strike_tmp01925d3f	The DFIR Report
12	26,267	— New entry	with_urls	n/a
13	26,127	— New entry	without_attachments	n/a
14	24,078	⇈ +52.90	malware_shellcode_hash	JPCERT/CC
15	23,684	— New entry	SUSP_Websites	Falcon Team

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	104,723	⇈ +48.78	PUA.Win.Packer.Pequake-4
02	58,381	— New entry	Win.Dropper.Tinba-9943147-2
03	46,052	— New entry	PUA.Win.Packer.Lccwin-2
04	41,654	— New entry	Win.Malware.Midie-9878132-0
05	37,303	v -5.60	PUA.Win.Packer.AcprotectUltraprotect-1
06	29,443	— New entry	Win.Trojan.Qukart-6874817-0
07	25,627	— New entry	Win.Trojan.Obfus-38
08	25,433	v -7.48	PUA.Win.Packer.Embedpe-3
09	23,510	— New entry	Win.Malware.Qukart-6838239-0
10	23,327	v -13.07	PUA.Win.Packer.Ep-7
11	22,510	— New entry	Win.Malware.Convagent-9979654-0
12	19,699	— New entry	Win.Malware.Scar-9946848-0
13	19,434	— New entry	PUA.Win.Packer.Acprotect-5
14	19,431	— New entry	PUA.Win.Packer.Acprotect-2
14	19,431	— New entry	PUA.Win.Packer.Acprotect-4

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN MARCH

Remember, sharing is caring.