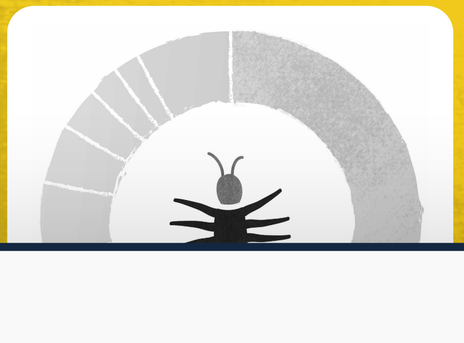
JANUARY 2024

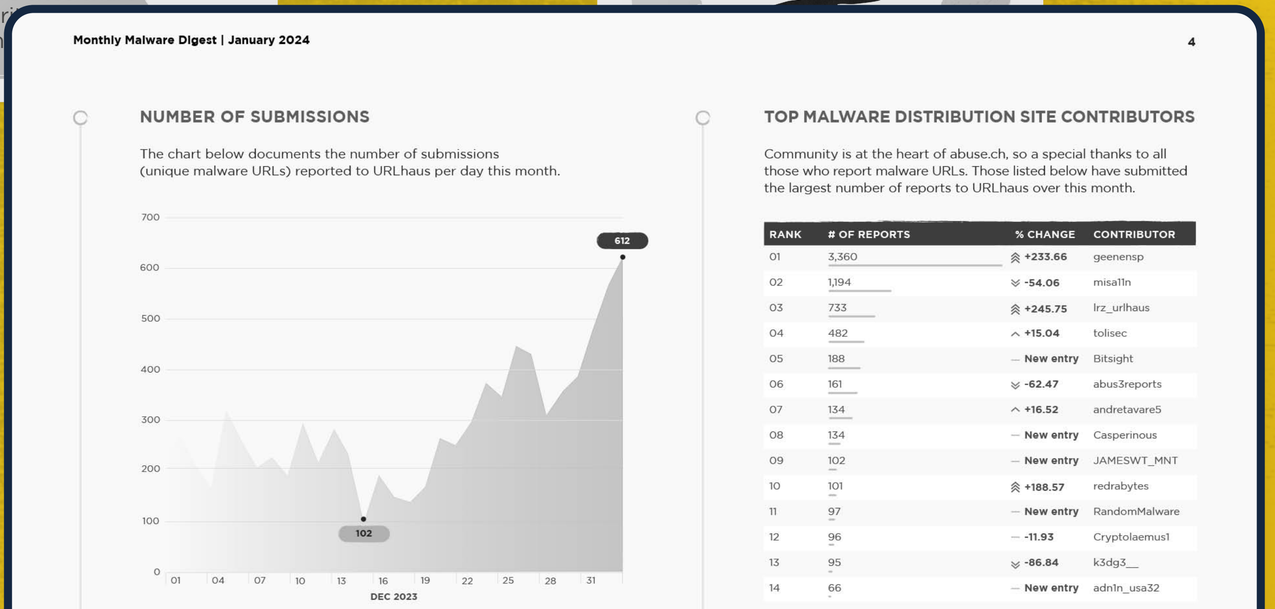
SPAMHAUS ABUSE.ch

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

8,864

Malware sites shared by security researchers on URLhaus

-2.6%

decrease on the previous month

15,079

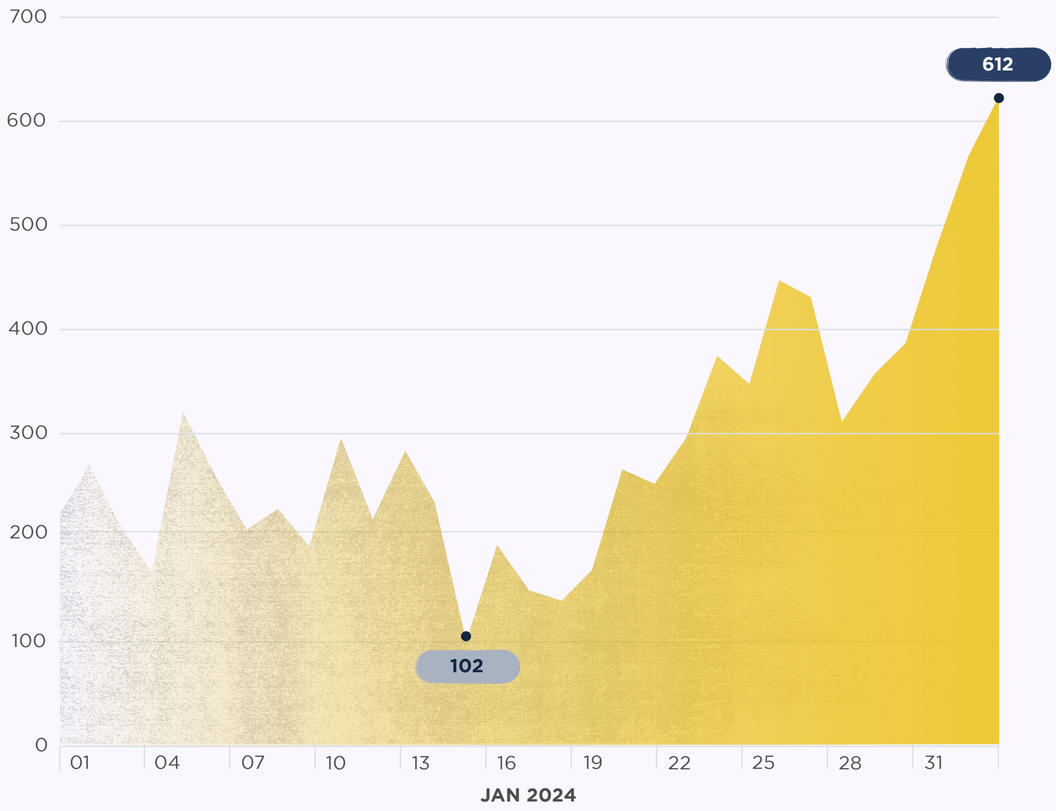
Abuse reports sent out to hosting providers and network owners

90.6%

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.

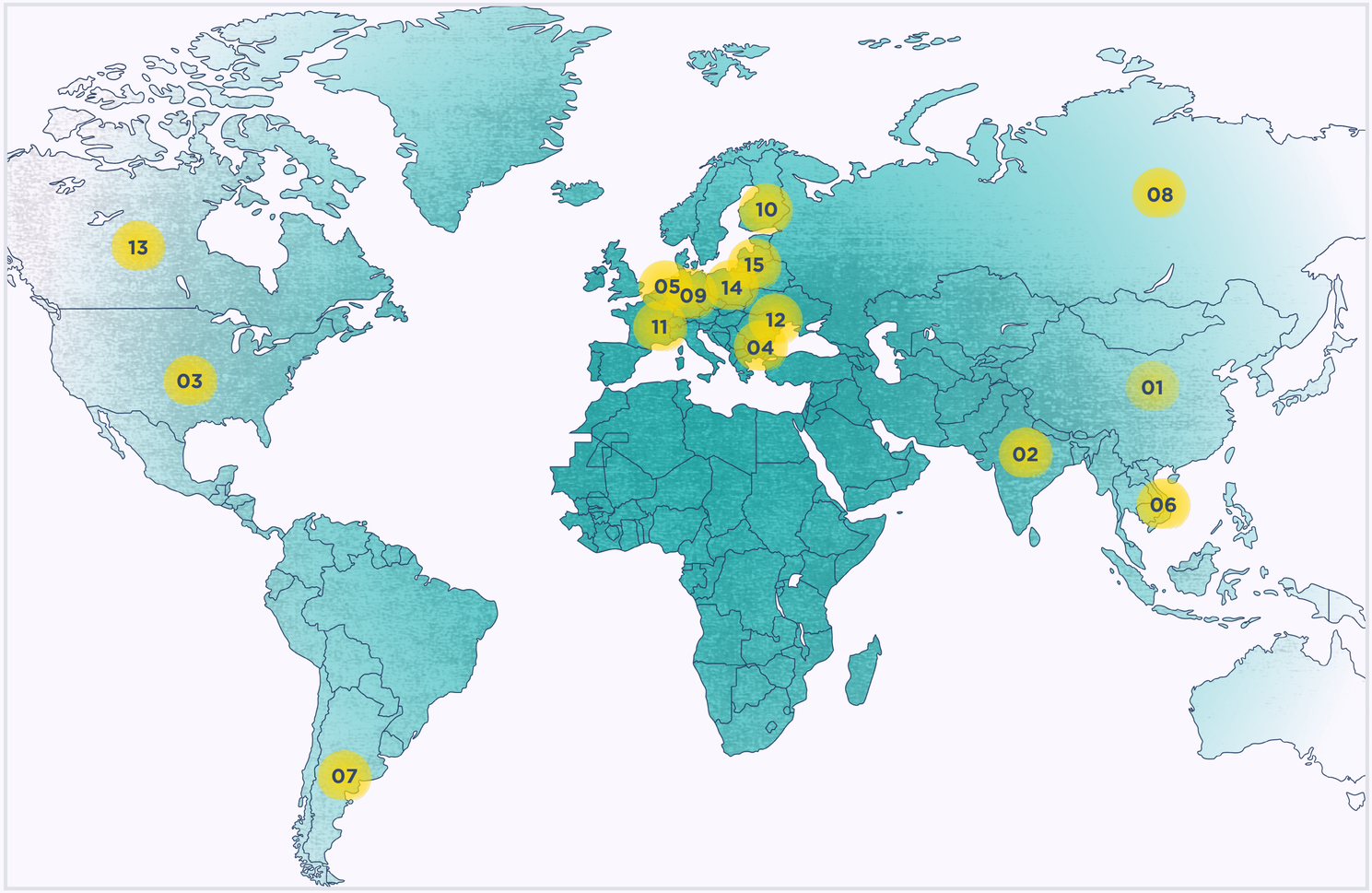


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	3,360	+233.66	geenensp
02	1,194	-54.06	misa11n
03	733	+245.75	lrz_urlhaus
04	482	+15.04	tolisec
05	188	New entry	Bitsight
06	161	-62.47	abus3reports
07	134	+16.52	andretavare5
08	134	New entry	Casperinous
09	102	New entry	JAMESWT_MNT
10	101	+188.57	redrabytes
11	97	New entry	RandomMalware
12	96	-11.93	Cryptolaemus1
13	95	-86.84	k3dg3__
14	66	New entry	adn1n_usa32
15	57	-66.07	Xev

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	3,673	+22.23	China
02	578	+172.64	India
03	464	-40.82	United States
04	372	+27.84	Bulgaria
05	369	+82.67	Netherlands
06	317	+53.14	Vietnam
07	240	+72.66	Argentina
08	197	-33.67	Russia
09	187	-29.43	Germany
10	120	New entry	Finland
11	91	-31.06	France
12	53	New entry	Moldova
13	52	+10.64	Canada
14	51	New entry	Poland
15	50	New entry	Lithuania

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	2,844	AS4837	CHINA169	China
02	1,295	AS4134	CHINANET	China
03	544	AS9829	BSNL-NIB	India
04	495	AS13335	CLOUDFLARENET	United States
05	306	AS10617	SION S.A	Argentina
06	185	AS47541	VKONTAKTE-SPB-AS vk.com	Russia
07	163	AS216240	MORTALSOFT	United Kingdom
08	146	AS49870	Alsycon-BV	Netherlands
09	131	AS394711	LIMENET	United States
10	118	AS203727	ALTAWK	Ukraine
11	96	AS36352	AS-COLOCROSSING	United States
12	92	AS51396	PFCLOUD	Germany
13	85	AS15169	Google	United States
14	84	AS63737	VIETSERVER SERVICES TECHNOLOGY	Vietnam
15	83	AS49581	FERDINANDZINK	Germany

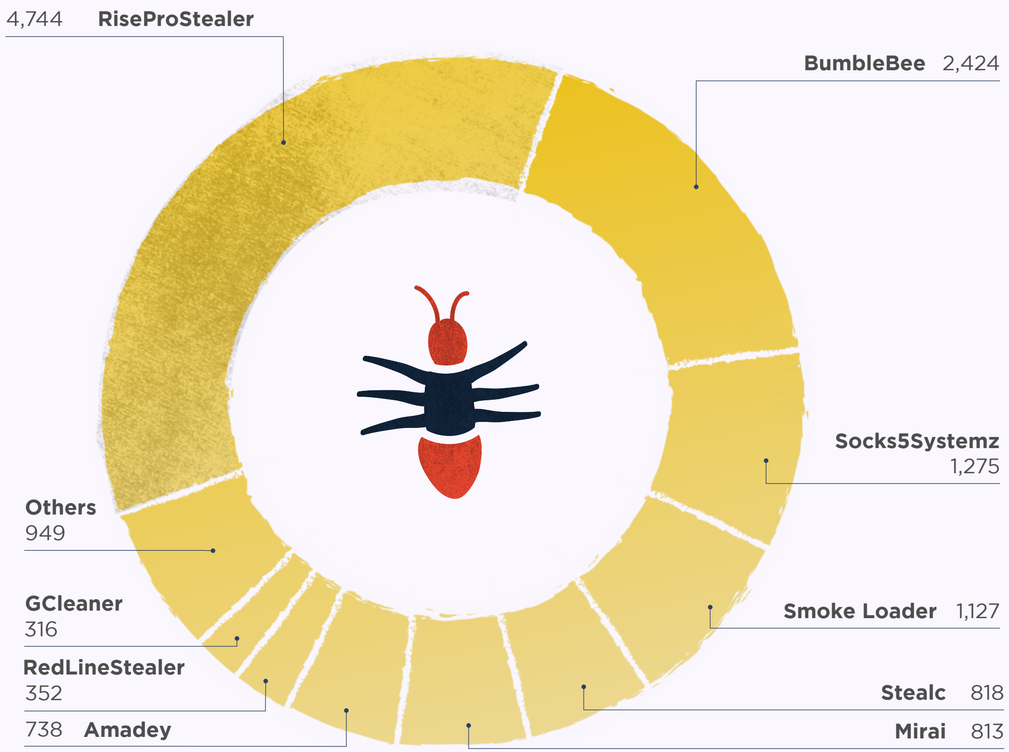
TOP MALWARE HOSTS

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	183	vk.com	VK	Russia
02	165	cdn.discordapp.com	Discord	United States
03	92	wtools.io	WTOOLS	null
04	38	paste.ee	Paste.ee	null
05	35	drive.google.com	Google	United States
06	31	github.com	Github	United States
07	22	transfer.sh	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	Amadey	+258.25		738
02	Ransomware.Stop	+124.11		251
03	Tofsee	+112.70		134
04	RiseProStealer	+62.41		4744
05	Mirai	+35.50		813
06	Gafgyt	+1.76		173
07	BumbleBee	-5.86		2424
08	CoinMiner	-6.16		259
09	Stealc	-10.11		818
10	Smoke Loader	-16.33		1127
11	RedLineStealer	-37.14		352
12	LummaStealer	-74.39		73
13	Socks5Systemz	-97.06		1275
14	GCleaner	New entry		316
14	Arechclient2	New entry		59

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

6,751

Malware samples shared by security researchers on MalwareBazaar

-35.2%

decrease on the previous month

1,472

Active hunting rules

+3.2%

increase on the previous month

31.12MB

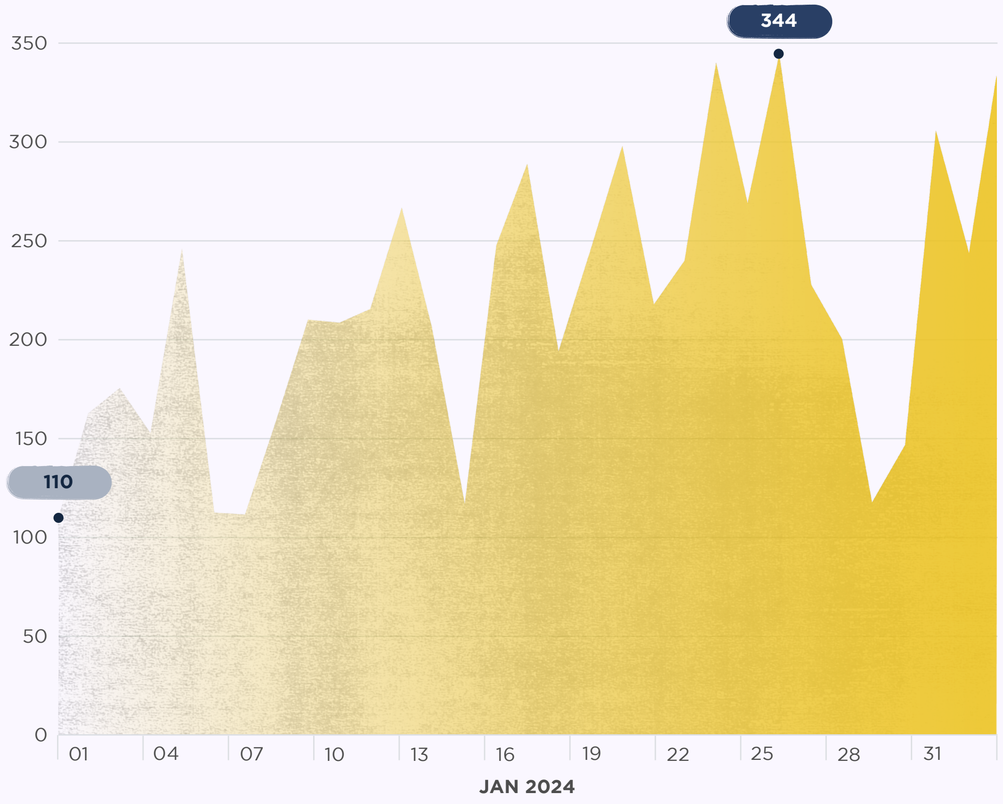
Average size of a malware sample

.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.



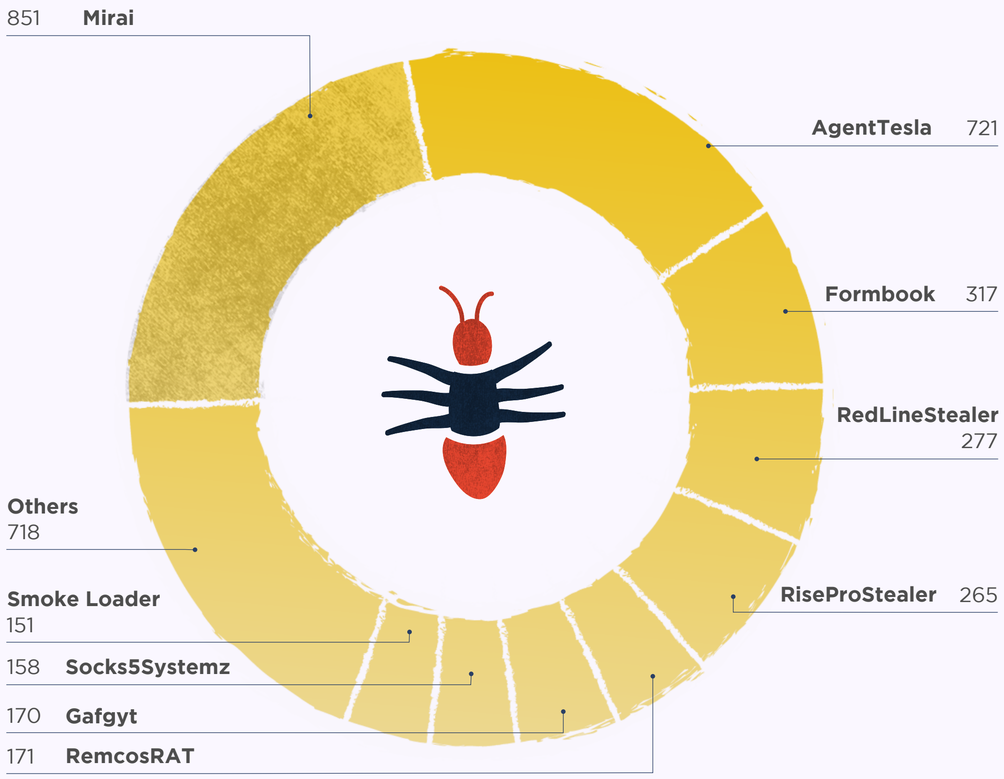
TOP SAMPLE CONTRIBUTORS

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	470	+213.33	adm1n_usa32
02	365	-4.70	elfdigest
03	280	+45.83	adrian__luca
04	209	+22.22	smica83
05	204	New entry	Bitsight
06	157	-49.19	cocaman
07	141	-87.05	andretavare5
08	122	-35.79	lowmal3
09	117	New entry	RandomMalware
10	103	+18.39	Porcupine
11	87	+67.31	jstrosch
12	72	+18.03	JAMESWT_MHT
13	61	+3.39	malwarelabnet
13	61	-29.89	TeamDreier
15	45	New entry	UkyKnight

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



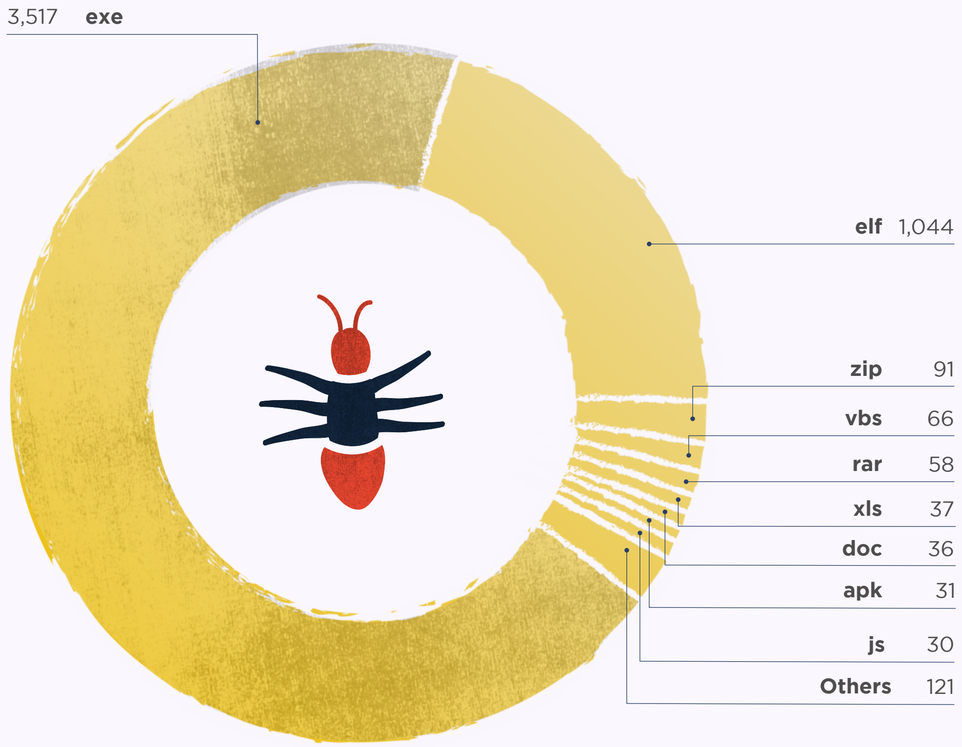
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	^ +26.64		851
02	RemcosRAT	^ +16.33		171
03	DCRat	^ +4.72		133
04	Formbook	v -3.94		317
05	Gafgyt	v -5.56		170
06	AgentTesla	v -18.07		721
07	RedLineStealer	v -21.31		277
08	Smoke Loader	vv -34.35		151
09	LummaStealer	vv -40.85		139
10	GuLoader	vv -41.82		96
11	Stealc	vv -48.44		116
12	RiseProStealer	vv -54.93		265
13	Socks5Systemz	vv -93.83		158
14	njrat	— New entry		151
14	AsyncRAT	— New entry		83

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	1865	NET	malware-lu
02	1815	DebuggerCheck__API	n/a
03	1250	MD5_Constants	phoul
04	987	maldoc_find_kernel32_base_method_1	Didier Stevens
05	937	NETexecutableMicrosoft	malware-lu
06	743	unixredflags3	Tim Brown
07	716	linux_generic_ipv6_catcher	@_lubiedo
08	714	myMirai	n/a
09	682	maldoc_getEIP_method_1	Didier Stevens
10	620	PE_Digital_Certificate	albertzsigovits
11	617	SHA1_Constants	phoul
11	617	RIPEMD160_Constants	phoul
13	584	PE_Potentially_Signed_Digital_Certif-icate	albertzsigovits
14	560	DebuggerException__SetConsoleCtrl	n/a
15	492	DebuggerCheck__QueryInfo	n/a

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)

8,048

Indicators of compromise (IOCS) shared on ThreatFox

-44.7%

decrease on the previous month

234

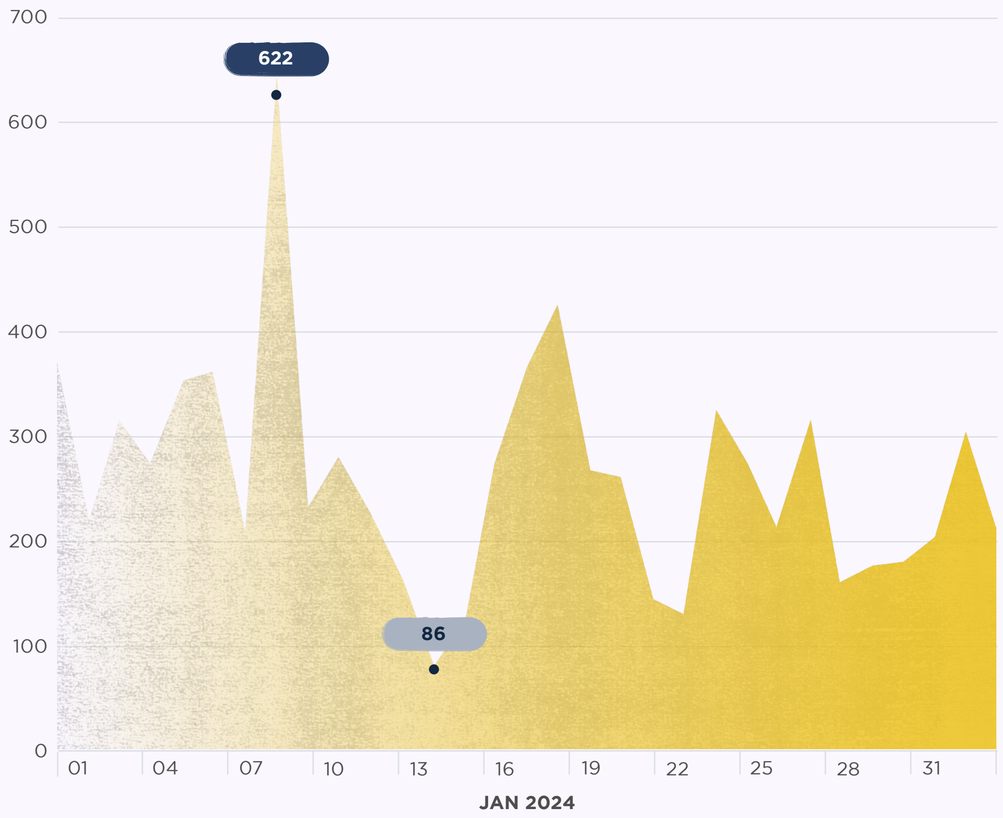
IOCs relating to AsyncRAT

-41.79%

decrease 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.



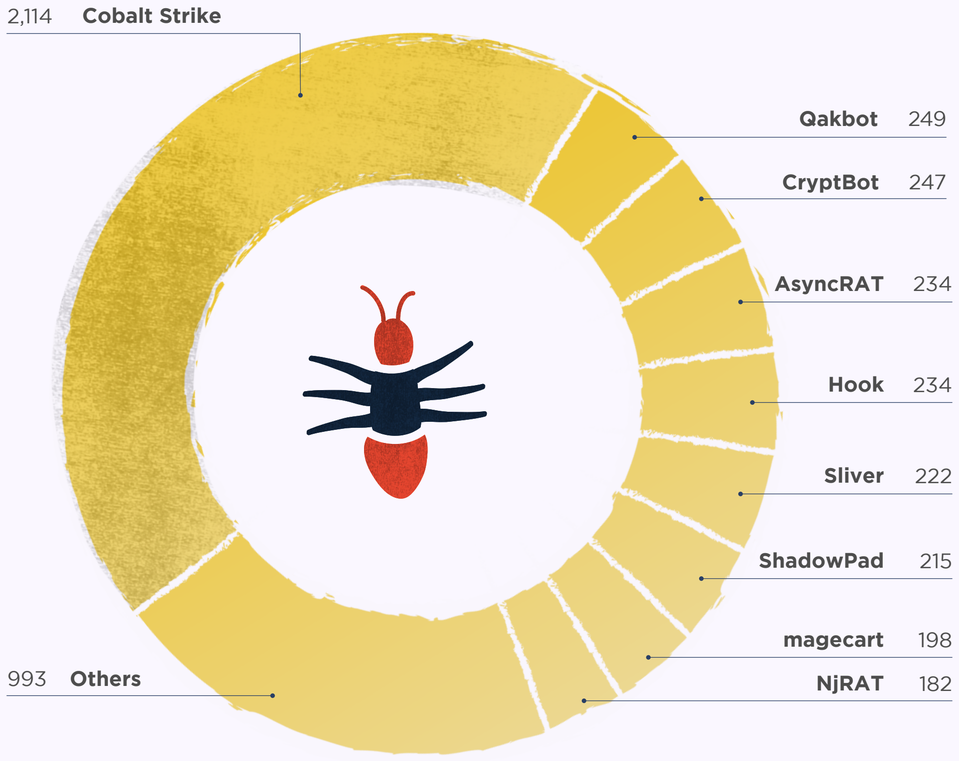
IOC TYPE

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	4,639	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
02	1,350	url	botnet_cc	URL that is used for botnet Command&control (C&C)
03	1,317	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
04	253	url	payload_ delivery	URL that delivers a malware payload
05	198	domain	cc_skimming	Domain used for credit card skimming (usually related to Magecart attacks)
06	138	sha1_hash	payload	SHA1 hash of a malware sample (payload)
07	67	domain	payload_ delivery	Domain name that delivers a malware payload
08	49	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
09	41	ip:port	payload_ delivery	ip:port combination that delivers a malware payload
10	23	md5_hash	payload	MD5 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.



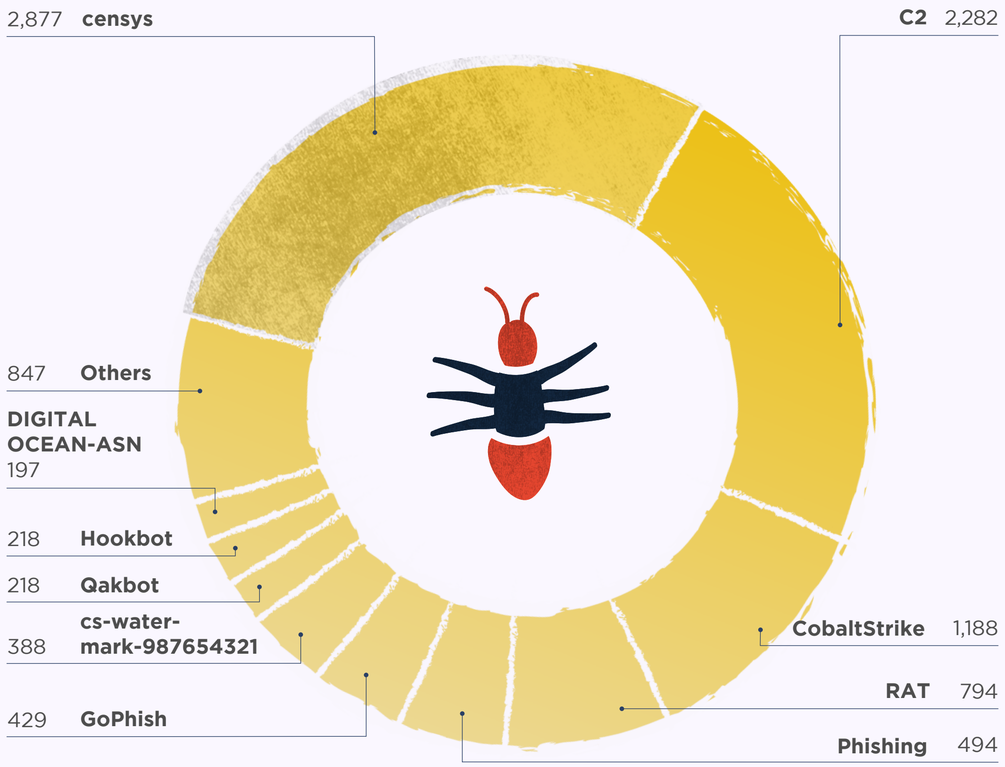
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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	Qakbot	-3.49		249
02	Cobalt Strike	-8.68		2114
03	Sliver	-20.43		222
04	Hook	-29.31		234
05	AsyncRAT	-41.79		234
06	CryptBot	New entry		247
06	ShadowPad	New entry		215
06	magecart	New entry		198
06	NjRAT	New entry		182
06	Havoc	New entry		176
06	Mirai	New entry		173
06	DarkComet	New entry		166
06	FakeUpdates	New entry		164
06	Venom	New entry		163
06	Quasar RAT	New entry		151

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	CobaltStrike	^ +9.39	1188
02	Qakbot	v -3.11	218
03	cs-watermark-987654321	v -9.13	388
04	RAT	v -31.55	794
05	C2	vv -35.23	2282
06	censys	vv -44.81	2877
07	DIGITALOCEAN-ASN	vv -45.73	197
08	Stealer	vv -49.84	158
09	AMAZON-02	vv -54.81	188
10	Phishing	vvv -68.60	494
11	GoPhish	vvv -71.38	429
12	Mirai	— New entry	173
12	NjRAT	— New entry	168
12	fofa	— New entry	160
12	Hookbot	— New entry	218

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

5,355,747

File scans conducted on YARAify

4,778,735

Distinct files that had scans performed on them

-37.1%

decrease in file scans on the previous month

-37.6%

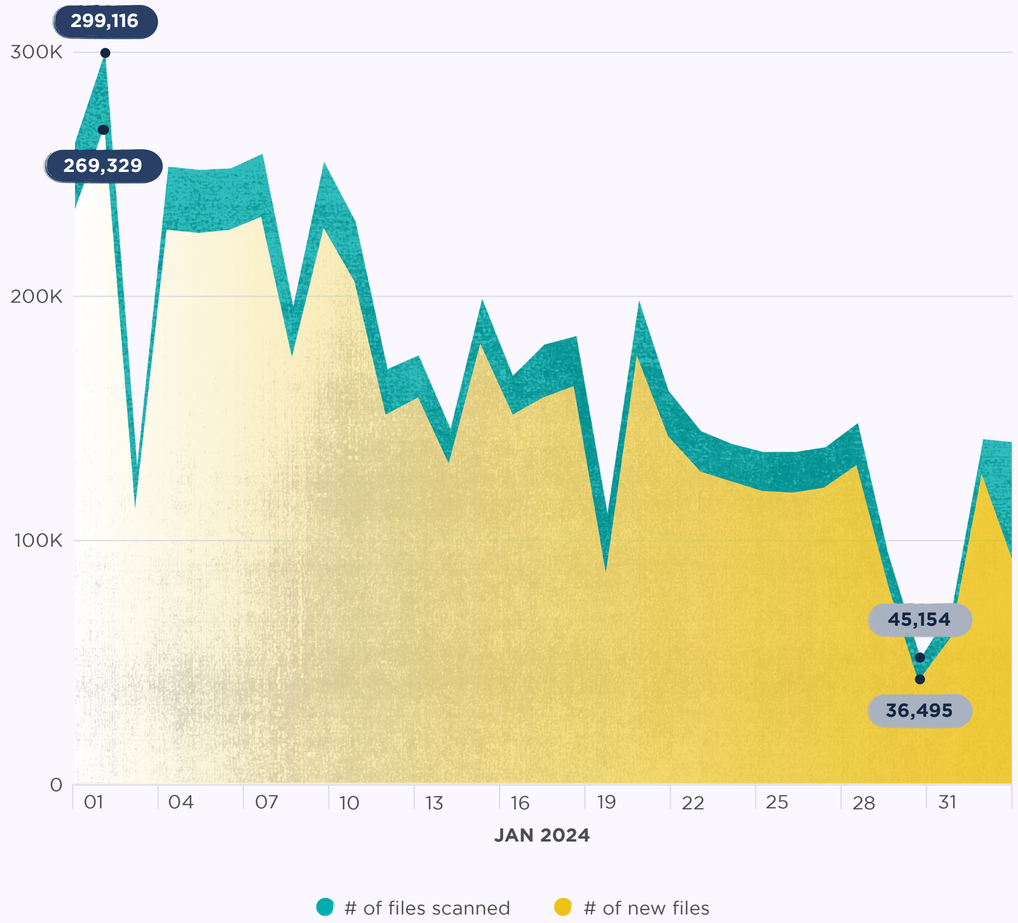
decrease in distinct files on the previous month

19,292

YARA rules deployed on YARAify and available for hunting

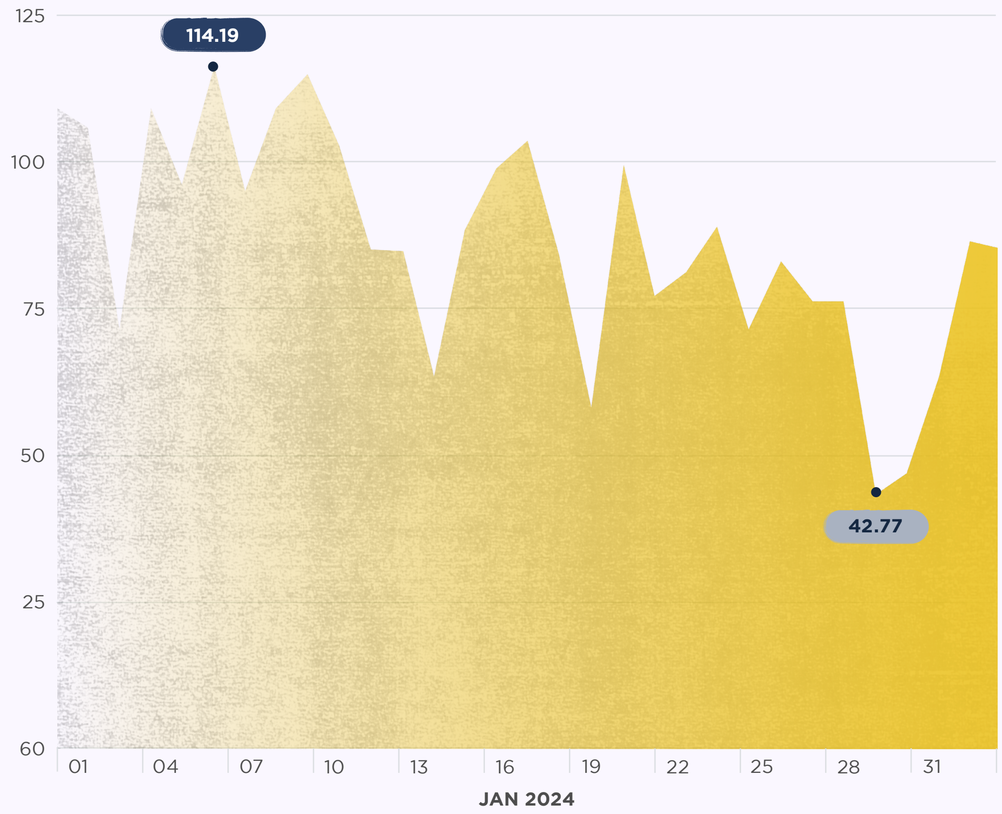
FILES SCANNED PER DAY

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	3,400,562	^ +12.99	maldoc_getEIP_method_1	Didier Stevens
02	520,905	— New Entry	win_berbew_strings	Matthew
03	486,903	^^ +157.76	DebuggerCheck__API	n/a
04	250,466	^^ +151.98	SHA512_Constants	phoul
05	242,077	^^ +80.71	maldoc_find_kernel32_base_method_1	Didier Stevens
06	237,320	^^ +118.86	NET	malware-lu
07	234,250	^^ +137.57	malware_shellcode_hash	JPCERT/CC Incident Response Group
08	227,048	^^ +237.16	UPXV200V290MarkusOberhumerLaszloMolnarJohnReiser	malware-lu
09	208,583	^^ +258.48	UPXv20MarkusLaszloReiser	malware-lu
10	148,035	^^ +138.46	vmdetect	nex
11	118,657	^^ +68.91	MD5_Constants	phoul
12	118,342	^^ +146.82	win_m0yv_auto	Felix Bilstein
13	115,705	^^ +126.25	DebuggerException__SetConsoleCtrl	n/a
14	108,783	^^ +83.05	RIPEMD160_Constants	phoul
15	108,782	^^ +83.05	SHA1_Constants	phoul

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	3,008,897	vv -48.38	PUA.Win.Packer.Lccwin-2
02	2,015,648	vv -48.52	Win.Trojan.Obfus-38
03	1,681,019	vv -51.53	Win.Trojan.Qukart-6874817-0
04	1,680,614	vv -31.24	Win.Trojan.Padodor-10016488-0
05	1,308,651	vv -47.25	Win.Malware.Qukart-6838239-0
06	700,312	vv -33.83	Win.Trojan.Padodor-9877164-0
07	342,904	vv -40.59	Win.Trojan.Berbew-10013977-0
08	258,905	— New entry	Win.Packed.Lazy-10005437-0
09	249,396	vv -34.19	Win.Trojan.Razy-10015064-0
10	248,934	vv -62.79	Win.Packed.Razy-10010080-0
11	236,074	vv -64.46	Win.Trojan.Berbew-9845290-1
12	216,846	vv -59.93	Win.Trojan.Crypted-29
13	216,448	vv -41.09	Win.Malware.Padodor-10012877-0
14	213,946	vv -60.01	Win.Trojan.Crypted-30
15	195,050	— New entry	Win.Trojan.Razy-10016933-0

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN MARCH

Remember, sharing is caring.