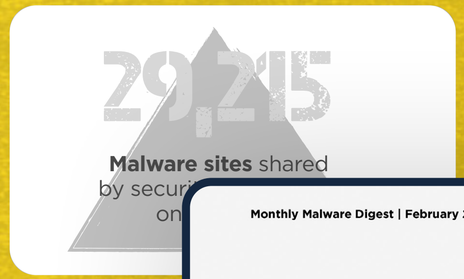
FEBRUARY 2023

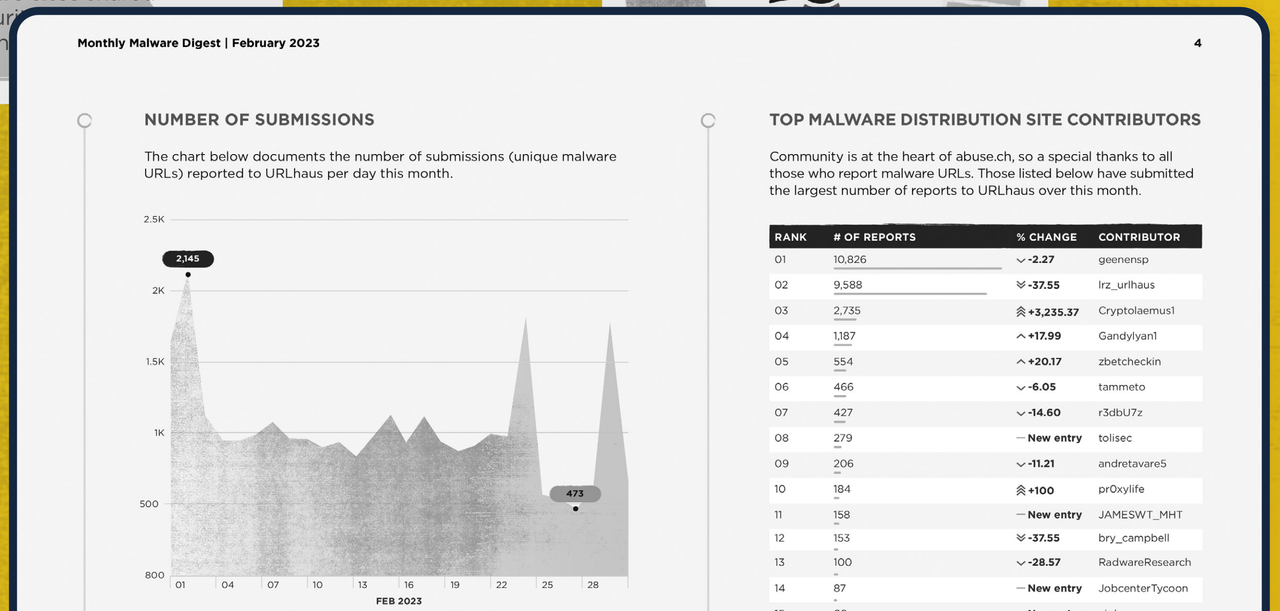
SPAMHAUS ABUSE.ch

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

29,215

Malware sites shared by security researchers on URLhaus

-7.5%

Decrease month on month

29,099

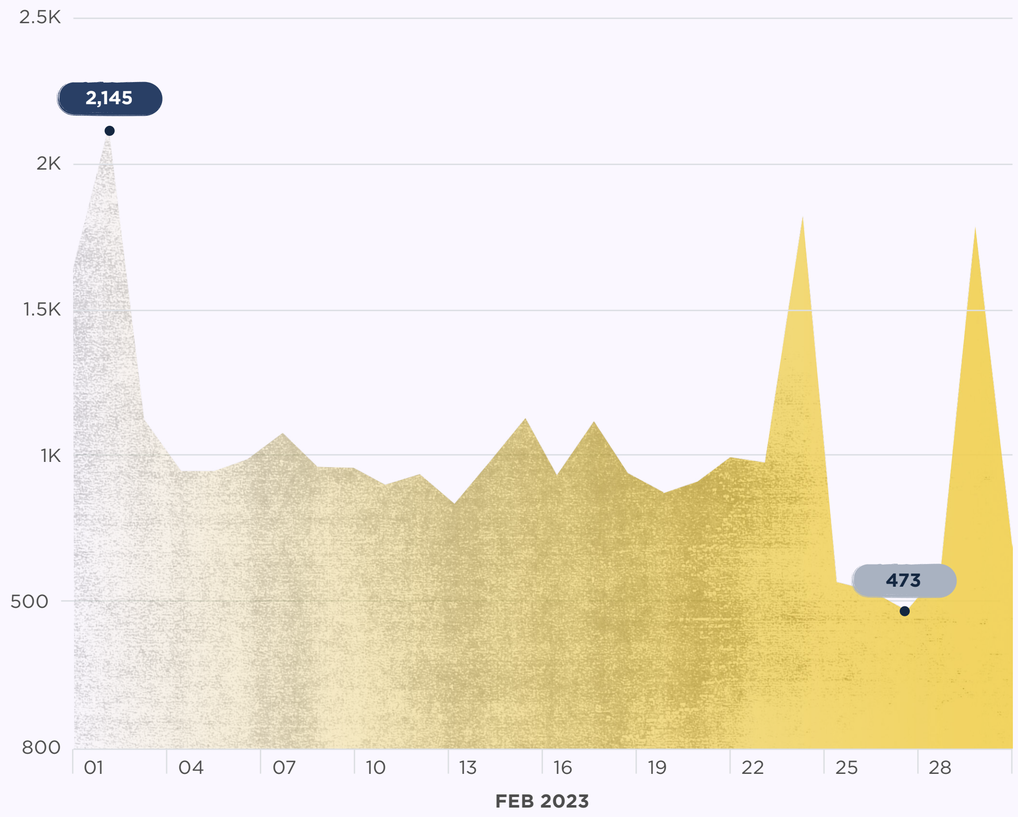
Abuse reports sent out to hosting providers and network owners

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.

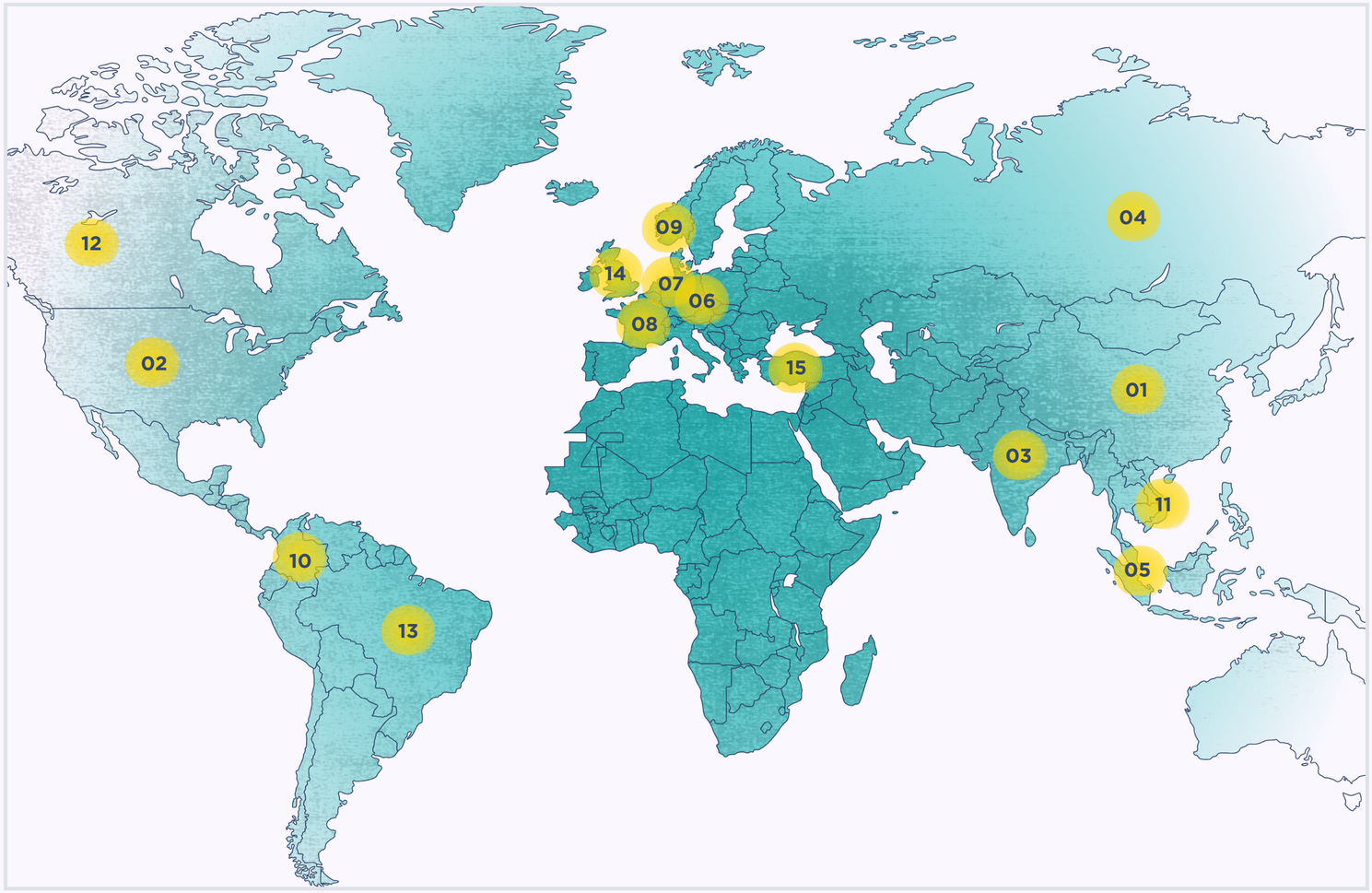


TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

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	10,826	-2.27	geenensp
02	9,588	-37.55	lrz_urlhaus
03	2,735	+3,235.37	Cryptolaemus1
04	1,187	+17.99	Gandylyan1
05	554	+20.17	zbetcheckin
06	466	-6.05	tammeto
07	427	-14.60	r3dbU7z
08	279	New entry	tolisec
09	206	-11.21	andretavare5
10	184	+100	pr0xylife
11	158	New entry	JAMESWT_MHT
12	153	-37.55	bry_campbell
13	100	-28.57	RadwareResearch
14	87	New entry	JobcenterTycoon
15	66	New entry	viql

GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES



RANK	# OF SITES	% CHANGE	COUNTRY
01	7,332	+16.99	China
02	3,333	+447.29	United States
03	2,359	+9.57	India
04	417	-48.83	Russia
05	305	+609.30	Singapore
06	297	+47.03	Germany
07	219	+180.77	Netherlands
08	168	+69.70	France
09	163	+409.38	Norway
10	158	New entry	Colombia
11	127	+101.59	Viet Nam
12	97	+223.33	Canada
13	81	+55.77	Brazil
14	75	-50	United Kingdom
15	74	New entry	Turkey

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	5,366	4837	CHINA169	China
02	2,129	9829	BSNL-NIB	India
03	1,860	4134	CHINANET	China
04	1,027	29802	HVC-AS	United States
05	716	22612	NAMECHEAP	United States
06	645	26496	GO-DADDY*	United States
07	362	13335	CLOUDFLARE	United States
08	172	36352	COLOCROSSING	United States
09	152	24940	HETZNER	Germany
10	118	211252	DELIS	Netherlands
11	97	16276	OVH	France
12	81	17813	MTNL-AP	India
13	68	51167	CONTABO	Germany
14	51	59425	HORIZONMSK-AS	Russia
15	48	210644	AEZA-AS	Russia

*GO-DADDY is a total number for ASN 26496, 398101, 21499

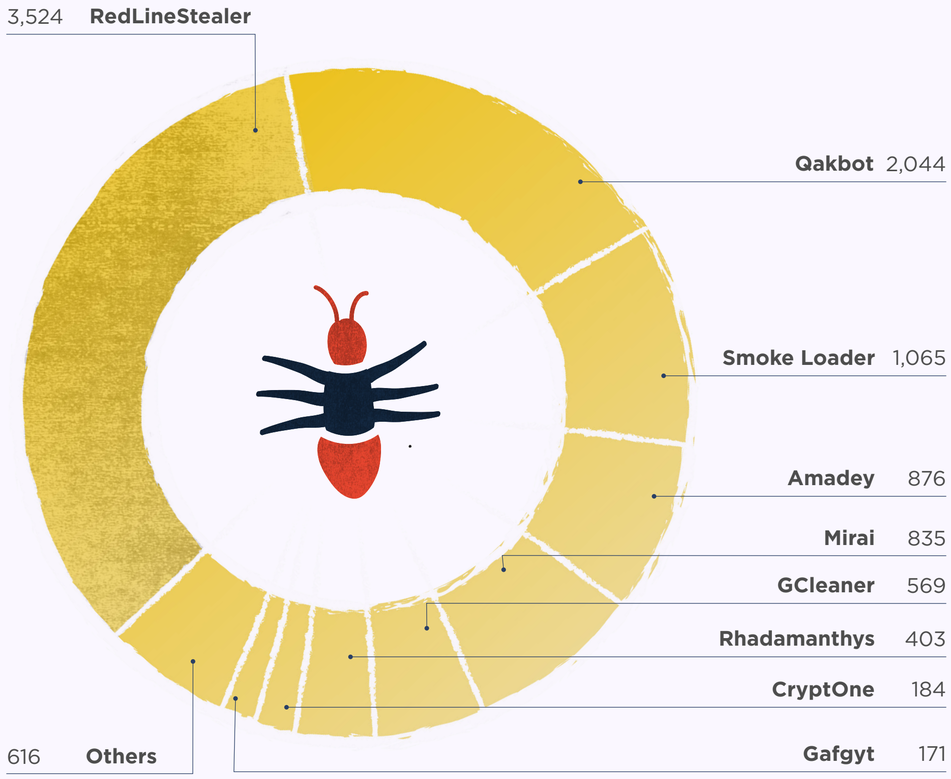
TOP MALWARE HOSTS

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	155	vk.com	VK	Russia
02	26	cdn.discordapp.com	Discord	United States
03	25	drive.google.com	Google	United States
04	21	bitbucket.org	Atlassian	Australia
05	18	pastebin.com	Pastebin	United States
06	15	www.4sync.com	4Sync	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	Amadey	+689.19		876
02	Qakbot	+648.72		2,044
03	Rhadamanthys	+172.30		403
04	RedLineStealer	+67.97		3,524
05	Mirai	+30.67		835
06	AgentTesla	+23.64		136
07	Gafgyt	+0.59		171
08	GCleaner	-26.01		569
09	TeamBot	-37.50		75
10	Smoke Loader	-46.16		1,065
11	CoinMiner	-59.66		119
12	CryptOne	New entry		184
13	LaplasClipper	New entry		100
14	Loki	New entry		95
15	SnakeKeylogger	New entry		91

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

14,477

Malware samples shared by security researchers on MalwareBazaar

+17.7%

Increase on the previous month

1,123

Active hunting rules

+4.8%

increase on the previous month

12.46MB

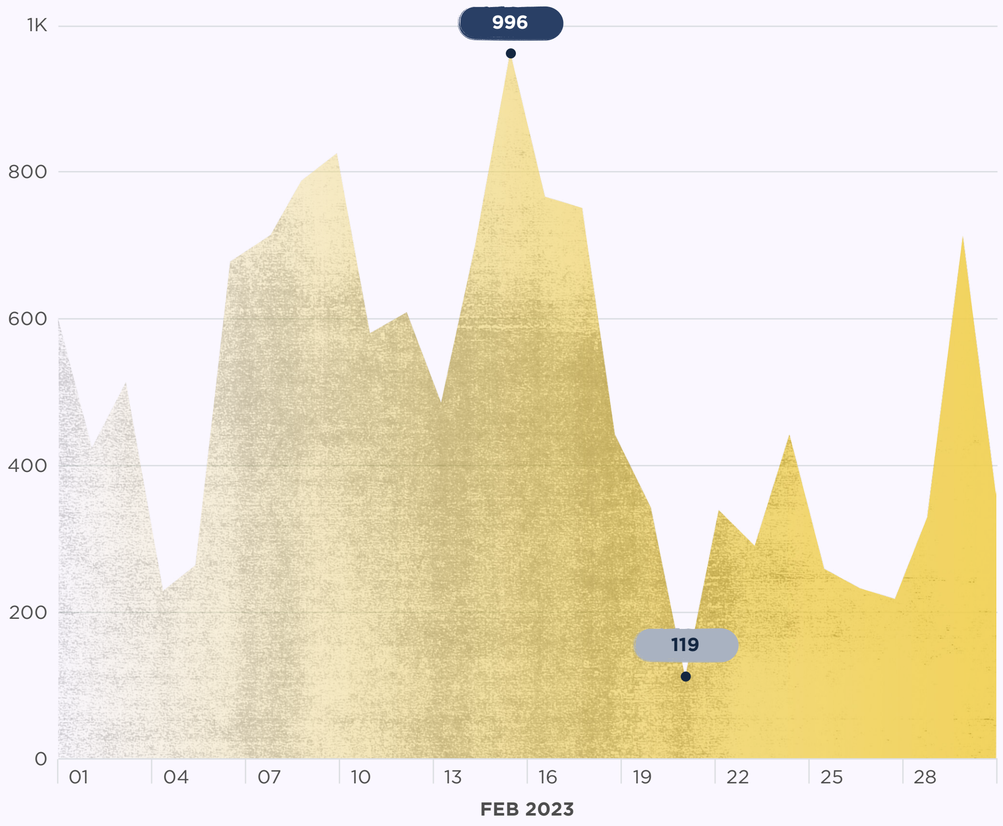
Avarage size of a malware sample

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.



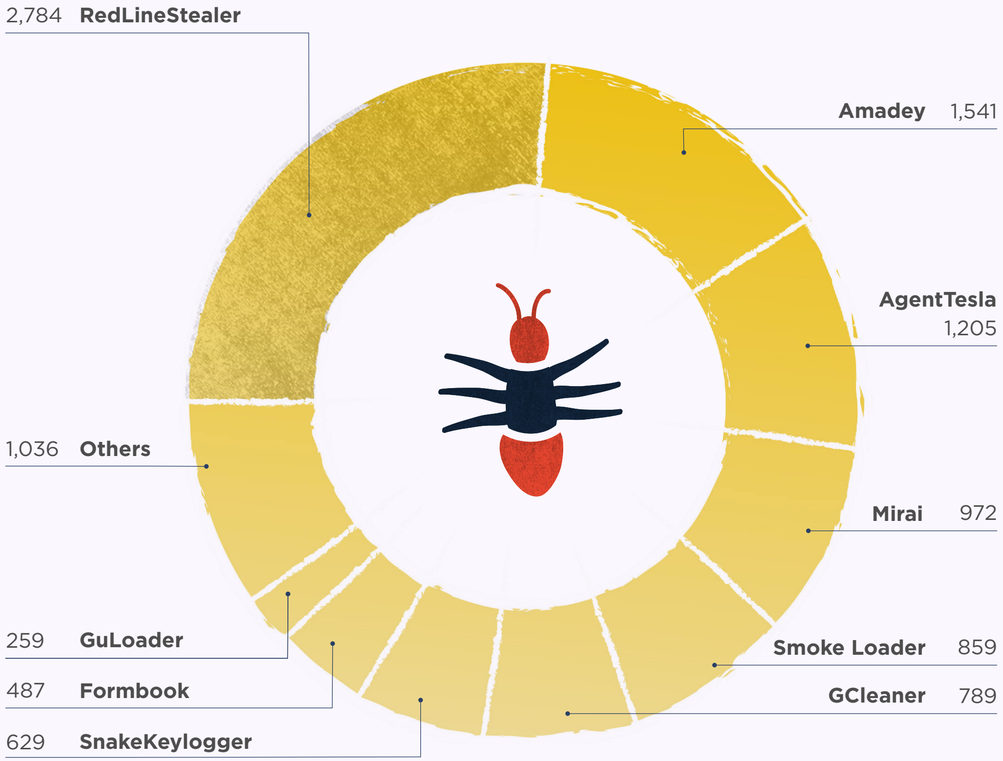
TOP SAMPLE CONTRIBUTORS

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	5,170	+3.65	@andretavare5
02	1,444	+24.48	@zbetcheckin
03	500	+81.16	@cocaman
04	333	+66.50	@lowmal3
05	314	+14.18	@adrian__luca
06	210	+77.97	@James_inthe_box
07	205	+0	@JAMESWT_MHT
08	204	-56.78	@SecuriteInfoCom
09	182	+111.63	@petikvx
10	171	-44.30	@jstrosch
11	165	-34.78	@atomiczsec
12	161	New entry	@elfdigest
13	142	-24.47	@0xToxin
14	138	New entry	@TeamDreier
15	121	+45.78	@pr0xylife

TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

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



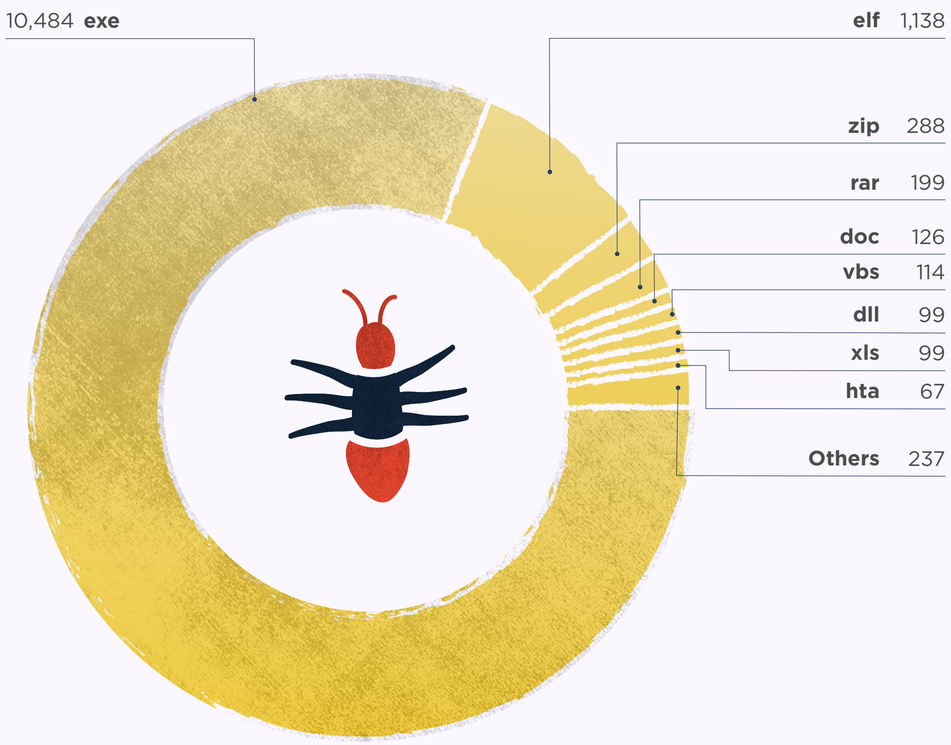
TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

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	RedLineStealer	+119.39		2,784
02	SnakeKeylogger	+116.15		629
03	Loki	+42.57		211
04	Mirai	+42.31		972
05	AgentTesla	+33.44		1,205
06	RemcosRAT	+24.39		204
07	Gafgyt	+9.86		156
08	Formbook	+6.10		487
09	DCRat	-5.84		145
10	GCleaner	-42.99		789
11	Smoke Loader	-44.83		859
12	CoinMiner	-50.72		171
13	Amadey	New entry		1,541
14	GuLoader	New entry		259
15	Gozi	New entry		149

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	2,962	Windows_Trojan_ Smokeloader_3687686f	Elastic Security
02	2,242	MALWARE_Win_RedLine	ditekSHen
03	1,325	shellcode	Nex
04	1,278	cobalt_strike_tmp01925d3f	The DFIR Report
05	930	win_smokeloader_a2	pnx
06	784	win_nymaim_g0	mak, msm, CERT.pl
07	774	win_gcleaner_auto	Felix Bilstein
08	548	unixredflags3	Tim Brown @timb_machine
09	542	MyMirai	n/a
10	534	linux_generic_ipv6_catcher	@_lubiedo
11	343	INDICATOR_SUSPICIOUS_ Binary_References_Browsers	ditekSHen
12	289	Linux_Trojan_Gafgyt_ 28a2fe0c	Elastic Security
13	277	setsockopt	Tim Brown @timb_ machine
14	256	meth_stackstrings	Willi Ballenthin
15	234	INDICATOR_SUSPICIOUS_ EXE_TelegramChatBot	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)

9,031

Indicators of compromise (IOCS) shared on ThreatFox

-21%

Decrease on the previous month

3,275

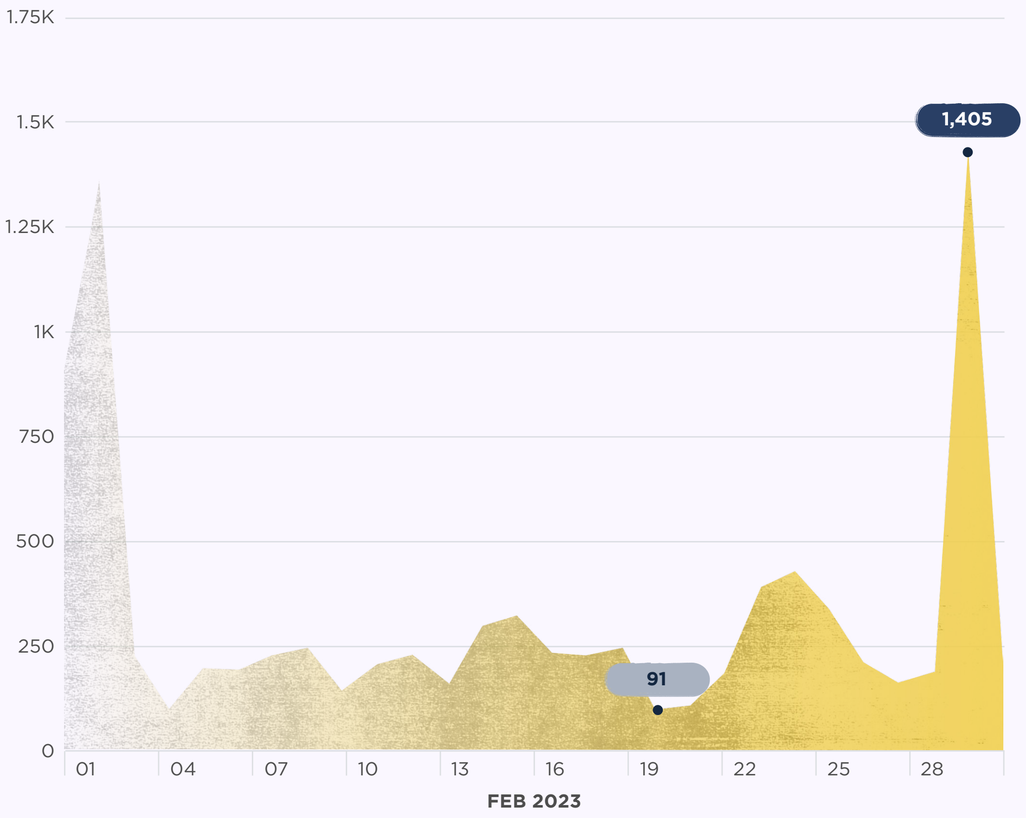
IOCs relating to Qakbot

NEW ENTRY

In February

NUMBER OF IOCs SHARED PER DAY

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



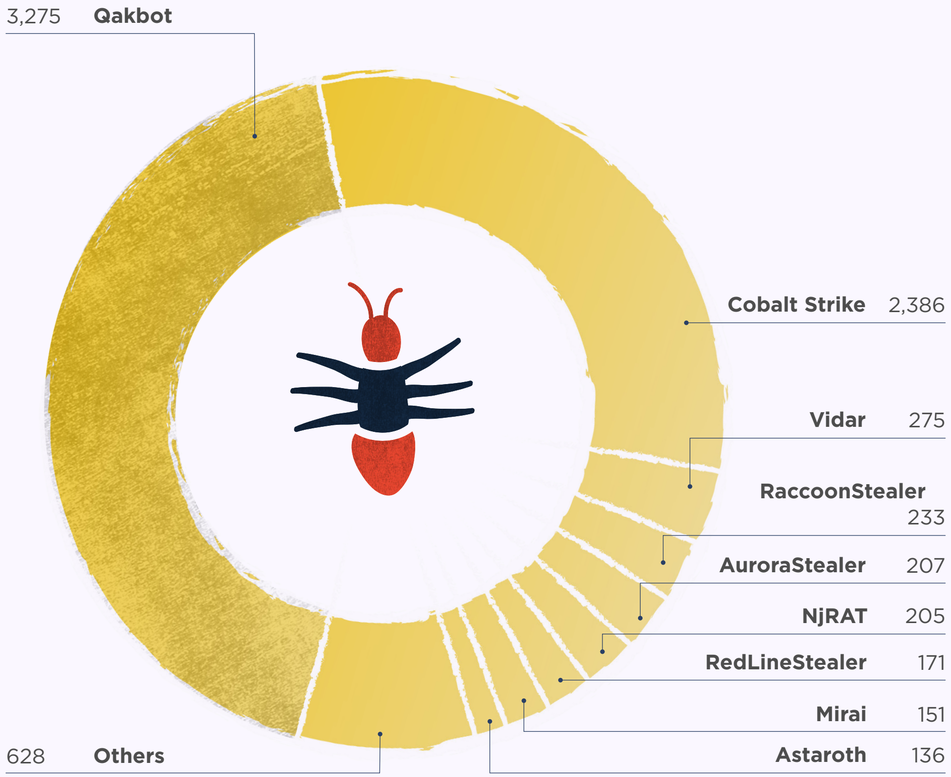
IOC TYPE

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	2,984	url	payload_delivery	URL that delivers a malware payload
02	2,825	ip:port	botnet_cc	ip:port combination that is used for botnet Command&control (C&C)
03	2,307	url	botnet_cc	URL that is used for botnet Command&control (C&C)
04	463	domain	botnet_cc	Domain that is used for botnet Command&control (C&C)
05	210	md5_hash	payload	MD5 hash of a malware sample (payload)
06	164	domain	payload_delivery	Domain name that delivers a malware payload
07	69	sha256_ hash	payload	SHA256 hash of a malware sample (payload)
08	6	ip:port	payload_delivery	ip:port combination that delivery a malware payload
09	2	domain	cc_skimming	Domain used for credit card skimming (usually re-lated to Magecart attacks)
10	1	payload	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.



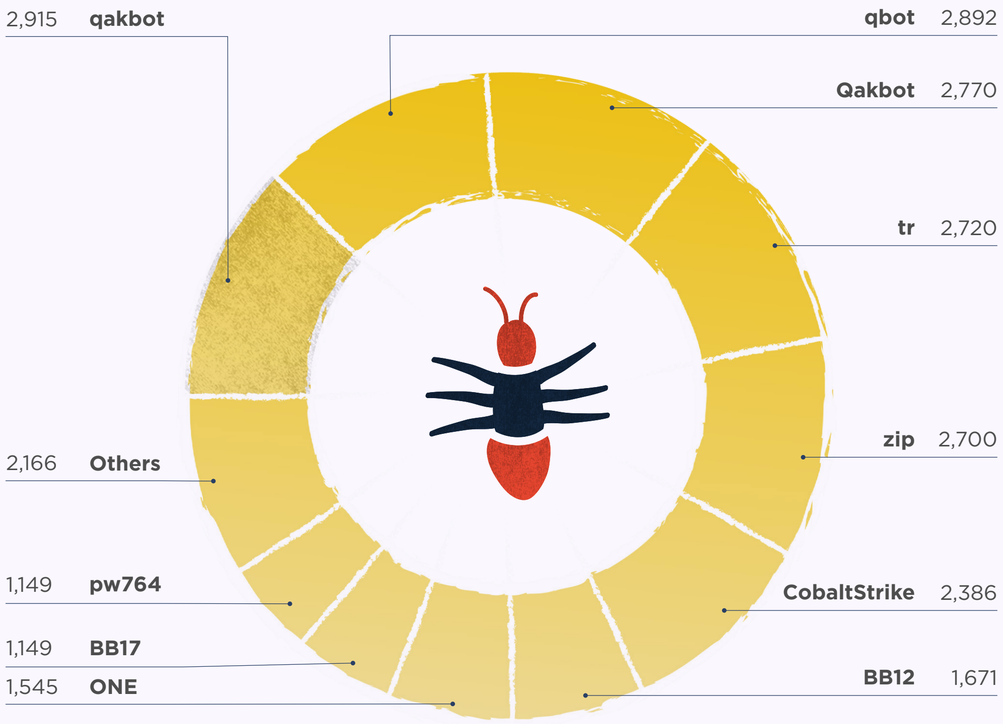
TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

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	Cobalt Strike	+62.31		2,386
02	AuroraStealer	+32.69		207
03	RedLineStealer	-3.93		171
04	NjRAT	-25.18		205
05	BianLian	-37.75		127
06	Astaroth	-39.01		136
07	IcedID	-45.21		120
08	RaccoonStealer	-63.25		233
09	Vidar	-87.90		275
10	Mirai	-90.44		151
11	Qakbot	New entry		3,275
12	Stealc	New entry		131
13	RecordBreaker	New entry		100
14	DCRat	New entry		75
14	Bumblebee	New entry		75

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	⌃⌃ **+63.65**	2,386
02	RedPacketSecurity	⌃ **+20**	258
03	RecordBreaker	⌄ **-15.38**	275
03	Vidar	⌄⌄ **-87.82**	275
04	zip	— **New entry**	2,700
05	tr	— **New entry**	2,720
06	BB12	— **New entry**	1,671
07	ONE	— **New entry**	1,545
08	BB17	— **New entry**	1,149
08	img	— **New entry**	1,149
08	pw764	— **New entry**	1,149
09	Qakbot	— **New entry**	2,770
10	qbot	— **New entry**	2,892
11	qakbot	— **New entry**	2,915
12	APT	— **New entry**	209

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

2,323,892

File scans conducted
on YARAify

1,928,350

Distinct files
that had scans performed on them

+5.1%

increase in
file scans on the previous month

+5.9%

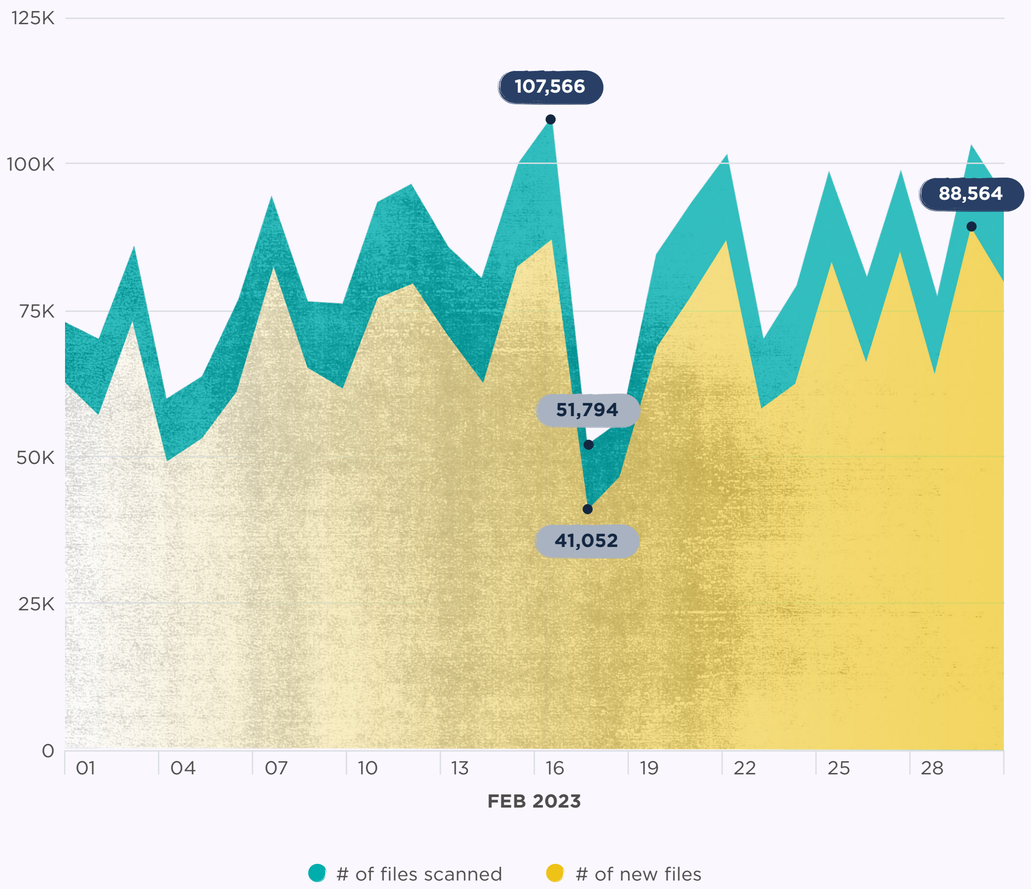
increase in
files on the previous month

14,733

YARA rules deployed
on YARAify and available for hunting

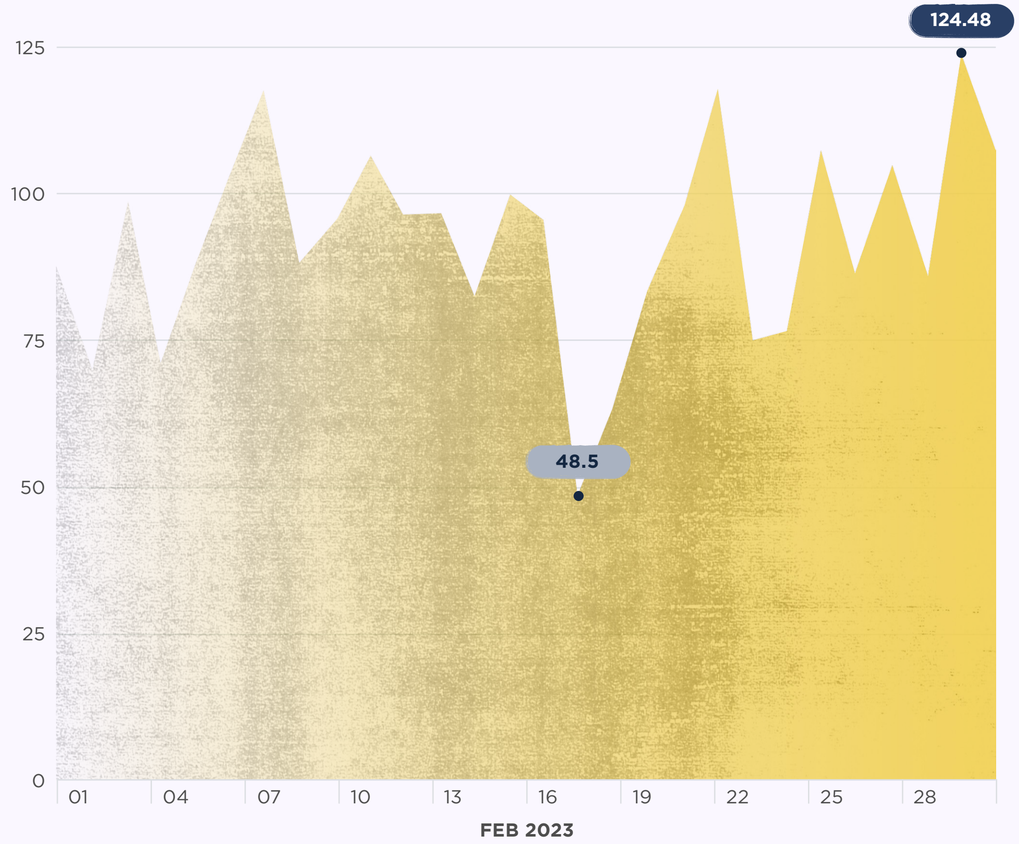
FILES SCANNED PER DAY

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	67,179	— New entry	Shellcode	nex
02	56,303	^ +13.34	BitcoinAddress	Didier Stevens (@DidierStevens)
03	50,011	^^ +48.85	TeslaCryptPackedMalware	n/a
04	47,865	^^ +98.79	malware_shellcode_hash	JPCERT/CC Incident Response Group
05	40,847	— New entry	shad0w_beacon_16June	Sbousseaden
06	32,641	— New entry	MALWARE_Win_RedLine	DitekSHen
07	31,600	v -2.45	win_sality_auto	Felix Bilstein
08	31,072	v -9.54	Disable_Defender	Iam-py-test
09	29,530	vv -56.84	INDICATOR_EXE_Packed_MPress	DitekSHen
10	25,545	— New entry	MALWARE_Win_BlackMoon	DitekSHen
11	20,029	^ -28.18	cobalt_strike_tmp01925d3f	The DFIR Report
12	19,922	^ -7.95	INDICATOR_SUSPICIOUS_EXE_RawPaste_URL	DitekSHen
13	19,784	— New entry	Windows_Trojan_Smokeloader_3687686f	Elastic Security
14	17,390	^ -23.63	SUSP_XORed_URL_in_EXE_RID2E46	n/a
15	17,307	— New entry	Adonunix2	Tim Brown @ timb_machine

YARAify

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	61,802	vv -40.99	PUA.Win.Packer.PeQake-4
02	57,048	^ +23.88	PUA.Win.Packer.Lccwin-2
03	56,628	^^ +51.81	PUA.Win.Packer.AcprotectUltraprotect-1
04	34,756	^ +18.05	Win.Trojan.Qukart-6874817-0
05	34,291	^^ +34.83	PUA.Win.Packer.Embedpe-3
06	30,828	^ +32.16	PUA.Win.Packer.Ep-7
07	29,928	^ +27.30	Win.Malware.Qukart-6838239-0
08	29,484	^ +15.05	Win.Trojan.Obfus-38
09	27,236	^^ +38.26	Win.Malware.Scar-9946848-0
10	26,729	^^ +37.56	PUA.Win.Packer.Acprotect-2
10	26,729	^^ +37.54	PUA.Win.Packer.Acprotect-5
10	26,729	— New entry	PUA.Win.Packer.Acprotect-3
10	26,729	— New entry	PUA.Win.Packer.AcprotectUltrap-1
10	26,729	^^ +37.56	PUA.Win.Packer.Acprotect-4
11	26,689	— New entry	Win.Trojan.Agent-1192165

SPAMHAUS ABUSE|ch

LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN APRIL

Remember, sharing is caring.