

Verdicts

SpamAssassin (score: 5)

- RBL: ADMINISTRATOR NOTICE: The query to zen.spamhaus.org was blocked due to usage of an open resolver. See <https://www.spamhaus.org/returnc/oub/> [2603:10a6:10:130:0:0:0:24 listed in] [zen.spamhaus.org] (score: N/A)
- RBL: ADMINISTRATOR NOTICE: The query to DNSWL was blocked. See <http://wiki.apache.org/spamassassin/DnsBlocklists#DnsBlocklists-dnsbl-block> for more information. [2603:10a6:10:130:0:0:0:24 listed in] [list.dnswl.org] (score: N/A)
- ADMINISTRATOR NOTICE: The query to dbf.spamhaus.org was blocked due to usage of an open resolver. See <https://www.spamhaus.org/returnc/pub/> [URI: thebandallsty.com] (score: N/A)
- No valid author signature and domain not in DNS (score: 0.8)
- To: has a malformed address (score: 0.1)
- BODY: Message only has text/html MIME parts (score: 0.1)
- BODY: HTML included in message (score: N/A)
- HTML-only message, but there is no HTML tag (score: 0.6)
- Multiple header formatting problems (score: N/A)
- Freemail in Reply-To, but not From (score: 2.5)
- Message body is only a URI in one line of text or for an image (score: 0.9)

oleid (score: N/A)

- There is no suspicious OLE file in attachments. (score: N/A)

Headers

Basic headers

Message ID <032672b4-77ca-42f8-a036-9711e91bd1f3@DB8EUR06FT032.eop-eur06.prod.protection.outlook.com>

Subject Microsoft account unusual signin activity

Activate Windows
Go to Settings to activate Windows.

Phishing Email Analy... (63) Phishing Analy... 42 Phishing Email E... CaniPhish: The Free CaniPhish: The Free EML Analyzer phishing_pot/email/

eml-analyzer.herokuapp.com/#/

EML Analyzer

Home Cache API GitHub

Cache EmailRep VirusTotal InQuest urlscan.io

ratio_50p_0,
reto,
auftreten,
juniors,
aussehen,
dahl,
facilit,
natures,
witte,
d909</style>

Extracted URLs

http://thebandalisty.com/track/o43062rdzGz18708448Gdrw1821750... ▾

Extracted emails

sotrecognizd@gmail.com ▾

Extracted domains

gmail.com ▾ sign.in ▾ thebandalisty.com ▾

Extracted IPv4s

103.225.77.255 ▾

Activate Windows

Go to Settings to activate Windows.

Type here to search

35°C Haze

ENG 5:47 PM

Scanned with OKEN Scanner

EML Analyzer

Home Cache API GitHub

Cache EmailRep VirusTotal InQuest urlscan.io

Subject Microsoft account unusual signin activity
Date (UTC) 2023-09-08T05:47:04Z
From no-reply@access-accsecurity.com
To phishing@pot

Hops

Hop	From	By	With	Date (UTC)
1	thcultarfdes.co.uk, 89.144.44.2	db8eur06ft032.mail.protection.outlook.com, 10.233.253.34	microsoft smtp server id 15.20.6768.30 via frontend transport	2023-09-08T05:47:04Z
2	db8eur06ft032.eop- eur06.prod.protection.outlook.com, 2603:10a6:10:130:cafe::9b	db8p191ca0014.outlook.office365.com, 2603:10a6:10:130::24	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha384) id 15.20.6768.30 via frontend transport	2023-09-08T05:47:04Z
3	db8p191ca0014.eurp191.prod.outlook.com, 2603:10a6:10:130::24	2603:10b6:a03:477::19, sj0pr19mb6679.namprd19.prod.outlook.com	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha384) id 15.20.6768.30	2023-09-08T05:47:04Z
4	::1, sj0pr19mb6679.namprd19.prod.outlook.com	mn0pr19mb6312.namprd19.prod.outlook.com	https	2023-09-08T05:47:06Z

Security headers

authentication-results spf=none (sender IP is 89.144.44.2) smtp.mailfrom=thcultarfdes.co.uk; dkim=none (message not signed)
header.d=none; dmarc=pererror action=none header.from=access-accsecurity.com;

X headers

x- 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0

Activate Windows
Go to Settings to activate Windows.



EML Analyzer

Home Cache API GitHub

Cache EmailRep VirusTotal InQuest urlscan.io

Security headers

authentication-results

spt=none (sender IP is 89.144.44.2) smtp.mailfrom=thculturalrdes.co.uk; dkim=none (message not signed)
header.d=none;dmARC=perMerror action=none header.from=access-accsecurity.com;

X headers

x- 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0

eoptenantattributedmessage

x-ms-exchange-crosstenant-originalarrivaltime 08 Sep 2023 05:47:04.2458 (UTC)

x-incomingheadercount 12

x-ms-exchange-processed-by-bccfoldering 15.20.6745.026

x-ms-exchange-organization-expirationinterval 1:00:00:00.0000000

x-ms-userlastlogontime 9/8/2023 5:43:16 AM

x-microsoft-antispam BCL:6;

x-ms-exchange-organization-scl 5

x-sid-result NONE

x-message-flag Flag

x-microsoft-antispam-mailbox-delivery wl:1;pcwl:1;ucf:0;jmr:0;ex:0;auth:0;dest:I;OFR:TrustedSenderList;ENG:(5062000305)(920221119095)(90000117)(920221120095)(9000200

Activate Windows
Go to Settings to activate Windows.

Phishing Email Analysis Guide

(63) Phishing Analysis with real

VirusTotal - URL

EML Analyzer

phishing_pot/email/sample-10

virustotal.com/gui/url/d0f0b1d739b21ea0f1d2cdfd1df92e20ce9311965af46b2a0ca7b29e518ee83f

http://thebandalisty.com/track/o43062rdrGz18708448Gdrw1821750fYo33632d5jh176

4
/ 97

Community Score

4/97 security vendors flagged this URL as malicious

Reanalyze

Search

More

http://thebandalisty.com/track/o43062rdrGz18708448Gdrw1821750fYo33632d5jh176

thebandalisty.com

Last Analysis Date

5 days ago

DETECTION

DETAILS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

BitDefender	Phishing	Fortinet	Phishing
G-Dat	Phishing	Sophos	Phishing
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BlockList	Clean	Blueliv	Clean
Cortego	Clean	Chong Lua Dao	Clean
CINIS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Criminal IP	Clean

Activate Windows
Go to Settings to activate Windows

Phishing Email Analysis Guide(63) Phishing Analysis with realVirusTotal - IP address - 103.225.77.255EML Analyzerphishing_pot/email/sample-10

virustotal.com/gui/ip-address/103.225.77.255

103.225.77.255

0/94

Community Score

1 detected file embedding this IP address

103.225.77.255INLast Analysis Date6 days ago

ReanalyzeSimilarMore

DETECTIONDETAILSRELATIONSCOMMUNITY10

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abuse	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Criminal IP	Clean	Cyble	Clean
CyRadar	Clean	desenmascara.me	Clean
DNSB	Clean	Dc3Web	Clean
EmergingThreats	Clean	Femtocore	Clean

Type here to search

34°C HazeENG6:03 PM

Activate Windows

Go to Settings to activate Windows



Header Analyzed

Email Subject: Microsoft account unusual signin activity

[Analyze New Header](#)

Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

Delivery Information

- DMARC Compliant (No DMARC Record Found)
 - SPF Alignment
 - SPF Authenticated
 - DKIM Alignment
 - DKIM Authenticated

Relay Information

Received Delay: 2 seconds

