EMAIL ANALYSIS REPORT

Analysis URL https://app.phishtool.com/analysis/68f8cfae370b6cd6b3e67695

Email subject Binance Cybersecurity

RESOLUTION

Resolved by madhavgarg679 (madhavgarg679@gmail.com)

Resolved on 2025-10-22T12:51:25Z

Disposition Malicious

CLASSIFICATION CODES

RECON The email is attempting to solicit a response (either an automatic response or a reply) to establish if the target mailbox is active and/or if a target user is present. Reconnaissance is often used to generate a list of target email addresses for future phishing.

SPOOF The email is attempting to convince the target that it originated from a legitimate source, when it did not. Spoofing is often used as a means to gain the authenticity of the spoofed sender, to persuade the target that email is genuine.

AUTO ANALYSIS

2 Malcious indicators **1 Safe indicators**

SPF: FAIL

The SPF record published on the **libreriacies.es** domain has a policy that designates the IP address **217.18.161.43** as **not permitted** to send emails on behalf of the **libreriacies.es** domain.

The IP address 217.18.161.43 is not a legitimate origin for the email.

VirusTotal hit on URL

A VirusTotal hit has been detected for this URL:

URL https://axobox.com/vt/wp-track.php

VirusTotal 11/98

Consistent Return-Path domain

The 'Return-Path' domain **libreriacies.es** is consistent with the 'From' domain **libreriacies.es**. The 'Return-Path' will not cause a misleading SPF result.

DETAILS

From info@libreriacies.es

Display name *None*

Sender *None*

To jdgelok@gmail.com

CC *None*

In-Reply-To *None*

Timestamp Tue, 25 Jul 2023 12:47:32 +0300

Reply-To *None*

Message-ID <C2C067AE.1670873@libreriacies.es>

Return-Path info@libreriacies.es

Originating IP 217.18.161.43 (Received-SPF)

rDNS serlogal.arnoia.com

AUTHENTICATION

SPF

Result FAIL

Originating IP 217.18.161.43 (Received-SPF)

rDNS serlogal.arnoia.com

Return-Path domain libreriacies.es

SPF record v=spf1 +a +mx -all +a:serlogal.arnoia.com

DKIM

Result *NONE*

Verification(s) 0 Signatures

DMARC

Result *NONE*

From domain libreriacies.es

DMARC record *None*

URLS

URL https://axobox.com/vt/wp-track.php

VirusTotal 11/98

TRANSMISSION

HOP 1

Timestamp 25 Jul 2023 11:47:28 +0200

Received from smtp.gmail.com ((unknown [43.230.161.16])by serlogal.arnoia.com (Postfix))

With ESMTPSA

ID EAB66C1C49;Tue,

```
from smtp.gmail.com (unknown [43.230.161.16])by serlogal.arnoia.com (Postfix) with ESMTPSA id EAB66C1C49;Tue, 25 Jul 2023 11:47:28 +0200 (CEST)
```

HOP 2

Timestamp Tue, 25 Jul 2023 09:47:34 +0000

Received from serlogal.arnoia.com ((217.18.161.43))

Received by BN8NAM12FT011.mail.protection.outlook.com ((10.13.183.146))

Via Frontend Transport

With Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))

ID 15.20.6631.25

```
from serlogal.arnoia.com (217.18.161.43) by BN8NAM12FT011.mail.protection.outlook.com (10.13.183.146) with Microsoft SMTP Server (version=TLS1_2,
```

HOP 3

Timestamp Tue, 25 Jul 2023 09:47:35 +0000

Received from BN8NAM12FT011.eop-nam12.prod.protection.outlook.com ((2603:10b6:408:106:cafe::a0))

Received by BN9PR03CA0616.outlook.office365.com ((2603:10b6:408:106::21))

Via Frontend Transport

With Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))

ID 15.20.6609.33

```
from BN8NAM12FT011.eop-nam12.prod.protection.outlook.com (2603:10b6:408:106:cafe::a0) by BN9PR03CA0616.outlook.office365.com (2603:10b6:408:106::
```

HOP 4

Timestamp Tue, 25 Jul 2023 09:47:35 +0000

Received from BN9PR03CA0616.namprd03.prod.outlook.com ((2603:10b6:408:106::21))

Received by PH0PR19MB5396.namprd19.prod.outlook.com ((2603:10b6:510:fa::20))

With Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))

ID 15.20.6609.25

```
from BN9PR03CA0616.namprd03.prod.outlook.com (2603:10b6:408:106::21) by PH0PR19MB5396.namprd19.prod.outlook.com (2603:10b6:510:fa::20) with Micros
```

HOP 5

Timestamp	Tue, 25 Jul 2023 09:47:37 +0000
Received from	PH0PR19MB5396.namprd19.prod.outlook.com ((::1))
Received by	MN0PR19MB6312.namprd19.prod.outlook.com
With	HTTPS

```
from PH0PR19MB5396.namprd19.prod.outlook.com (::1) by MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 25 Jul 2023 09:47:37 +0000
```

RECIPIENT MAILBOX

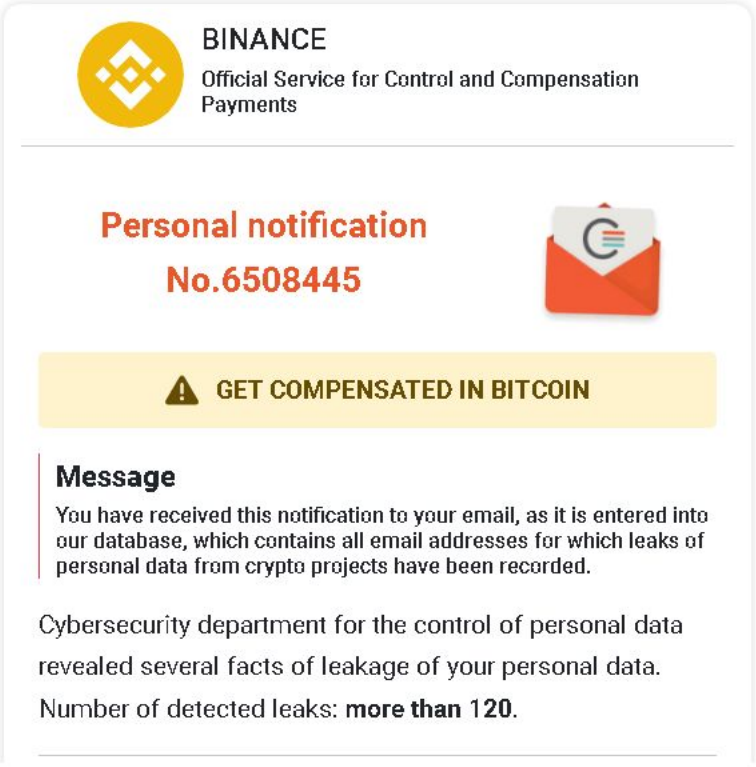
Timestamp Tue, 25 Jul 2023 12:47:32 +0300

X-HEADERS

x-incomingtopheadermarker	OriginalChecksum:03D66726AC96B4D53504E4CBC2EFB9D7A17A4AAD2C31D06BB9DBAD877449FEFA;UpperCasedChecksum:33A442CCC36B2DDC58E83CE0B5755C98F6793354CE07FEFEF9AF2645081EA269;SizeAsReceived:878;Count:13
x-ppp-message-id	<169027845306.115385.17798998159970521909@serlogal.arnoia.com>
x-ppp-vhost	libreriacies.es
x-incomingheadercount	13
x-ms-exchange-organization-expirationstarttime	25 Jul 2023 09:47:34.8480 (UTC)
x-ms-exchange-organization-expirationstarttimereason	OriginalSubmit
x-ms-exchange-organization-expirationinterval	1:00:00:00.0000000
x-ms-exchange-organization-expirationintervalreason	OriginalSubmit
x-ms-exchange-organization-network-message-id	9fc50159-6c91-4ae2-a5a1-08db8cf42c6f
x-eopattributedmessage	0
x-eoptenantattributedmessage	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
x-ms-exchange-organization-messagedirectionality	Incoming
x-ms-publictraffictype	Email
x-ms-traffictypediagnostic	BN8NAM12FT011:EE_|PH0PR19MB5396:EE_|MN0PR19MB6312:EE_
x-ms-exchange-organization-authsource	BN8NAM12FT011.eop-nam12.prod.protection.outlook.com
x-ms-exchange-organization-authas	Anonymous
x-ms-userlastlogontime	7/25/2023 9:39:39 AM
x-ms-office365-filtering-correlation-id	9fc50159-6c91-4ae2-a5a1-08db8cf42c6f
x-ms-exchange-eopdirect	true
x-sender-ip	217.18.161.43
x-sid-pra	INFO@LIBRERIACIES.ES
x-sid-result	PASS
x-ms-exchange-organization-pcl	2
x-ms-exchange-organization-scl	9
x-microsoft-antispam	BCL:0;
x-ms-exchange-crosstenant-originalarrivaltime	25 Jul 2023 09:47:34.7074 (UTC)
x-ms-exchange-crosstenant-network-message-id	9fc50159-6c91-4ae2-a5a1-08db8cf42c6f
x-ms-exchange-crosstenant-id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
x-ms-exchange-crosstenant-authsource	BN8NAM12FT011.eop-nam12.prod.protection.outlook.com
x-ms-exchange-crosstenant-authas	Anonymous
x-ms-exchange-crosstenant-fromentityheader	Internet
x-ms-exchange-crosstenant-rms-persistedconsumerorg	00000000-0000-0000-0000-000000000000
x-ms-exchange-transport-crosstenantheadersstamped	PH0PR19MB5396
x-ms-exchange-transport-endtoendlatency	00:00:02.4161998
x-ms-exchange-processed-by-bccfoldering	15.20.6609.030
x-microsoft-antispam-mailbox-delivery	abwl:0;wl:0;pcwl:0;kl:0;dwl:0;dkl:0;rwl:0;ucf:0;jmr:0;ex:0;auth:1;dest:J;OFR:SpamFilterAuthJ;ENG:(5062000305)(90000117)(90005022)(91005020)(91035115)(9050020)(9100338)(944500132)(2008001134)(2008121020)(4810010)(4910033)(8820095)(10005027)(9710001)(9610025)(9520007)(10115022)(9320005)(9245025);RF:JunkEmail;
x-message-delivery	Vj0xLjE7dXM9MDtsPTA7YT0xO0Q9MjtHRD0xO1NDTD02
x-microsoft-antispam-message-info	g7cU7g7e0YXYgqBmgo6Zoi2Jii+RQpT2nJQaDwoRpSI4U7ntAKjmq2RXPHxLwFm0DBAOvmkRoupqZeEiEVDH5jS2cIav1jnN+sqvLtmY+QBph35gi4o5EHEnaaGbh67/i7usY/hxqw5EbnPRBY68u392htv2zsfecF6Gmsr38MdgeoBIOGCxWgPcEOrhBISFJw6qo0NUWV5pqx2c3/VlzkAoHIJ2InfOqJRwaNsGT+fPvUZBjT7wFAlFuTwsdkECF5MJf+cuSVyWD/Twcj7+uItp3EmvyFGU3wjJJ5xsDCxWfFnhx5uBquIJ8ufk6XnjThLr7VNAqkGzWvwZYxPkyl2hGFXKRhWvvPGB++qM9wWLRbJcsw5lsPJRfs1jkULL+NNuaXQBaIS2sRb2ciIWU

Oul/5UM8/105UT7hcNt1YkPqxKo1xYnDK8z6w8OzfSUpB0zbS4GV1Fo4igS59MsBUjJkBcs/NjfzjbkBreXdmZeMk2cwIpPvxGLLWj
ssELsvnYmim/5M0X56BNRMgDTU1ooqNiCAUf4m/WJDx2ZJgzh/IyRNngLooDnwxIhYbKRlcWipTasZT09CkoY7Jv06O6qP0lyywkO
9VPXYTXgkeLgQ5/27p4WgqEGUCSvRFsFBOgjI30k6GCzwyV4NnsDxS0K6JQvr6JuAt7qvsr/xHe7kYCvbSZyJh0nKLwFC/lf6Vo3NA
90f8oXcHoPKWWxlWe2fF3rJI5h8UygnX9ysXg9vk6O232gxkr7sFpGjGKeLIGGVpiREHZ1TNQ+BxHLnCQkqFYpgdeI9vJ4nC9qTpVf
7/jo334NIwHYpZ9XmJ00qVbfwSP0XrYSBkfemDoNb9qhWXNyBEObGLBriFDR6S7nlH1C1ZwkQnH3QQlsqoe4J8ryW8jstcI0fVMuL
Q5qkI/tQPi22lAGgcbElCHOzy070I5dYaDrXfUQg0+WITn4Dd43mnK1kpth6BC+FNnc3VTCd4v/z4RjCJAxXjamDj0jEKqdXHOe1f9G
np1NrOQRJ75byDmJl2TMLWfWsFb+aEc9bye+LiY2gknAl0hD/+IL/Y5KCD2C1PkPmK9gUmWyi693f4wJjNP7/4TP9ebtQe6AvC5R
ZLFJhHV0iihwbJds/EivNZEbIi+pcphyKgBseWSmpeoPmiigAG7Rmq/YlRaDxrR3V491XeMD8EzObSPwCLDxZWRWMAX3rb20rP8U
2qg7BX8BdJN260COEwAn3Z/Kb3LOQQjL9QHn0KJCV61xXcNoAnMF1AlVmpYbTgNFNsTQhNlqcC7XBxcXkRE1WjKyyvYbFDRQAy
nbes65ltzRzox8xj+AHQLOnAV1PBQicfnqHkEGv+DrplbzZk2mJkYgme7KW9dpmzdY0YvU/WkrYV3SxUR6RYdZjniP4MZhH8Lxg7E
QJDEPgba9RZZ14XyxdKKahupREKNGuTyNKDwVRYyuuZ6GgjPw+whMvxIucQhC3qbGdn0qWuxbgL3z24o1cBwrAyXIAwtbnRSze
dRmfEmdYYt0s+aiU3ys5xENGmelv4tE2VLErHLeWhAUWYZRIlL4DQlpwGZtkjKoaL57bO8nWBdYjCha/uyt8U7rgwFOnvjproICcR+O
TMhjJnJbS/RXfVe5SS+PZ5gWyKYRrPt9oaQlSwQOWM4nKybe4YFCrO7Y0sQW7L/ncOBNeN24AzEUdBKYokTX5J6PQsm2B5a4+t
NtdYw9tHQpIiB+mmJyUeYlcQMCu5IoNWADUpkczPo53Aw/XsRVmLwdoX8p8f9oczR8g3mv/MJ9YAYLxzs15+DpoSDJPzn66iukt+
/RV7qGqhLXiltGwbWT3Z6HLx0xd7M4vPvWkuFy34/kyJIKeaRmYZGYgHwh+8FL20itCl7L9bD61M7tZC1wm7Eflur2fX6yfS8cmq8H
oujdGXnsuQcW+LNiHE+JJFfPfu24OqkYkkY310SnwJSsyZzzae58v1R4SgdBjB3yEP8CxwpyXHvSHjFbU6zXoj3WxkuMvhrJ4yZdUNj
3v9P6ptBluU45fqky56xL/VT6nPcud8V73fLlMnVcevg6+Y/TzEqyAEaQVOVyN6Igv53pjimltOZSNi8ZWqdb1HXo7EbZTN+4807pWU
mUOEA+WCd9B4EVEI5k9f0ZSAztWTa7i9C5pX0ueFRujodDZzHV2lGDMFq4gZHJy+fUgIcMV2ikNvv7YNzxuIQ+6L2K3SwaPMSACd
3+EY1UYRXe51hmSKX5w/PR+qwfUt/c+o1dnn6+IrPZtA0eaU2dyb8GmzuxiIleDUc8BkhiUj8QFIh6S0KWH8knlqkTpB1bxdgQyLOS
Oyu3jQ6PRQlODIP51d2Pcr63i6AbJ+DkrutLGFbUMFs

MESSAGE RENDER



Open the official website

_____ ialozfapprnttjwkcgzdvio
ypulylsluvxruhawhvuasqxfrkxnalqshzvzojkhytqjwffe
dkusggodswwhcbmqgznokowyqkblujxrsqnryprudmew

MESSAGE PLAINTEXT

https://axobox.com/vt/wp-track.php

FLAGGED ARTIFACTS

Message URL	https://axobox.com/vt/wp-track.php
Message URL domain	axobox.com

OPEN SOURCE INTELLIGENCE

DNS - AXOBOX.COM

A	192.185.145.93
MX	0 axobox.com
TXT	v=spf1 include:websitewelcome.com -all
SOA	ns831.websitewelcome.com. dnsadmin.vr6.websitewelcome.com. 2025092201 86400 7200 3600000 86400
NS	ns831.websitewelcome.com ns832.websitewelcome.com

WHOIS - AXOBOX.COM

Registrant	REDACTED FOR PRIVACY
Registrar	IONOS SE
Registered on	2009-01-08
Expires on	2027-01-08
Updated on	2025-10-09
Domain age	6131 days
Status	clientTransferProhibited

AUDIT LOG

2025-10-22T12:51:25Z	Resolved as "Malicious" by madhavgarg679@gmail.com
2025-10-22T12:35:58Z	Manually uploaded by madhavgarg679@gmail.com