EMAIL ANALYSIS REPORT

Analysis URL https://app.phishtool.com/analysis/68f8cd956e0f6d90b97f3ae5

Email subject [URGENT] Verify Your Trust Wallet.

RESOLUTION

Resolved by madhavgarg679 (madhavgarg679@gmail.com)

Resolved on 2025-10-22T12:29:55Z

Disposition Malicious

CLASSIFICATION CODES

CRED_HARV The email is attempting to persuade the target to enter a user name and password though an illegitimate mechanism, so that the user name and password can be harvested for malicious purposes.

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

4 Malcious indicators **1 Notable indicators** **1 Safe indicators**

Inconsistent Return-Path domain

The 'Return-Path' domain **pot=hotmail.com** is inconsistent with the 'From' domain **itpro.net.br**.

SPF: FAIL

The SPF record published on the **pot=hotmail.com** domain has a policy that designates the IP address **149.72.240.56** as **not permitted** to send emails on behalf of the **pot=hotmail.com** domain.

The IP address 149.72.240.56 is not a legitimate origin for the email.

DMARC: FAIL

The DMARC tests have **failed**. The authentication mechanisms (SPF and/or DKIM) have not passed with an authenticated identifier that is in sufficient alignment with the 'From' domain **itpro.net.br**, as specified by the domain's DMARC policy.

The authenticity of the email cannot be relied upon.

DKIM: BODY HASH DID NOT VERIFY - s1._domainkey.itpro.net.br

The message body hash **did not** verify.

Inconsistent display-name

The 'From' email address local-part **claudia** is **inconsistent** with the display-name **Trust Wallet** provided in the email.

The local-part of an email address is the part of an email address before the '@' symbol.

Consistent Reply-To email address

The 'Reply-To' email address **claudia@itpro.net.br** is consistent with the 'From' email address **claudia@itpro.net.br**. The sender is not attempting to deceive the recipient with a different reply email address.

DETAILS

From claudia@itpro.net.br

Display name Trust Wallet

Sender *None*

To phishing@pot

CC *None*

In-Reply-To *None*

Timestamp Tue, 03 Oct 2023 23:47:34 +0000 (UTC)

Reply-To claudia@itpro.net.br

Message-ID <VV04DMpGRPOoJ3UAgRlDaw@geopod-ismtpd-16>

Return-Path bounces+14043109-f56e-phishing@pot=hotmail.com@alavancandominhacarreira.itpro.net.br

Originating IP 149.72.240.56 (Received-SPF)

rDNS	wrqvfhpv.outbound-mail.sendgrid.net

AUTHENTICATION

SPF

Result	FAIL
Originating IP	149.72.240.56 (Received-SPF)
rDNS	wrqvfhpv.outbound-mail.sendgrid.net
Return-Path domain	pot=hotmail.com
SPF record	v=spf1 ip4:167.89.80.139 ip4:168.245.100.63 -all

DKIM

Result	NEUTRAL
Verification(s)	1 Signature - 1 NEUTRAL

SIGNATURE 1

Selector	s1._domainkey.itpro.net.br
Signing domain	itpro.net.br
Algorithm	rsa-sha256
Verification	**NEUTRAL**

DMARC

Result	FAIL
From domain	itpro.net.br
DMARC record	v=DMARC1; p=none;

URLS

URL	https://t.rdsv1.net/ls/click?upn=QJHDLu6c7joILAshEaWRB90ZvG3MeB7stfqQoNfEMaoKnttIpVYuRKEo8ASi9sTkYTGqKsbrHulqBqCo6R83H-2BMPpTZ-2FPFQPHNxCWnvt06OfPqj6vFBieRdLd63IeEdddn-2BtNZ15bfQjITLRr2eDqnuV-2BpwBQ9ZHfBRMwYi5ADY-3Dd1Ac_Ee7nT2ZQdJ749eAGxVv-2FHN3XNBqa48KbYVWhgkx4gPmq9lJRJyAOpJGecmhmqQ-2BOzEdxpPZTG3-2FcbtSAK-2BaUclKhX3UXigAovFtamcPLixidlDIa9dezstz6DOOZsPHpelYCac1FQPgsvVUSZ0w6dS2L5Idr282b2EFYRQJJsGe1vbi7ptE4Mqirpmltc1Qah43s-2BHvwh5IvmVRP-2FHUgrXo5kOW39-2BayhRLSI3vJxMWy3tZvn-2BYJZ3CLiwjSEDblXyvlyOt9-2BjQAzVEVQ-2FkiOVieZmwidMbDKsMWYmJ5uGhHB-2FXgtDgecz6UlzvkA0I7-2FD-2BgZ6StBCBMzARh-2FmeYTGt49pPRR2zjL2YDZwP3z-2FOmPw-2BcTqQ3fbQnHxooO-2FsFZPsul1fyi0vwtBEOVQJl2Hv1nQ4AtlYiJnis5gBiAZnTLy0EcwXvMPfUVjUQMh-2B8wMG3Rl1mbOuD8vAkSIBVFkRmXKNRmfyapSxfbwDDC310leXSC-2FPkhx0EjfK3EWFfHkte6cZrqCLMo97-2B-2BhHHnlG3onU06lWwIJpKDM6L-2FXt-2Fv47iMTkLsQ1vQ7nEFWXTJUUn04y6nVxzwxPno-2BMYjdPUgM8ePCz7NYCYlF0-2BJ4ydDs87pZA597K9g-2FD3X29Oqubab1cI-2FXku0PfJEV4ClQ-3D-3D
VirusTotal	*None*

URL	https://t.rdsv1.net/ls/click?upn=vmZSPIdvJlJEjv0U0GmezzhgBNOgVLg9sDeuRDN5ukD7iD-2BC6wItpoab0w8mupO6waJpEZth-2BtTrjDkzM7HN6lhXslcf7Nsr3HgKHQ0R6YkcaZ3kRyrEbBP3te6oriuV82YL_Ee7nT2ZQdJ749eAGxVv-2FHN3XNBqa48KbYVWhgkx4gPmq9lJRJyAOpJGecmhmqQ-2BOzEdxpPZTG3-2FcbtSAK-2BaUclKhX3UXigAovFtamcPLixidlDIa9dezstz6DOOZsPHpelYCac1FQPgsvVUSZ0w6dS2L5Idr282b2EFYRQJJsGe1vbi7ptE4Mqirpmltc1Qah43s-2BHvwh5IvmVRP-2FHUgrXo5kOW39-2BayhRLSI3vJxMWy3tZvn-2BYJZ3CLiwjSEDblXyvlyOt9-2BjQAzVEVQ-2FkiOVieZmwidMbDKsMWYmJ5uGhHB-2FXgtDgecz6UlzvkA0I7-2FD-2BgZ6StBCBMzARh-2FmeYTGt49pPRR2zjL2YDZwP3z-2FOmPw-2BcTqQ3fbQnHxooO-2FsFZPsul1fyi0vwtBEOVQJl2Hv1nQ4AtlYiJnis5gBiAZnTLy0EcwXvMPfUVjUQMh-2B8wMG3Rl1mbOuD8vAkSIBVFkRmXKNRmfyapSxfbwDDC310leXSC-2FPkhx0EjfK3EWFfSrEqfYV0ZBiB89I8uGETYnuz8R4wfWmDbJ8qpRQHsHKrLxtOvDYueffXyo2XFgoXHG6JZeDhn46BruNuzVWT61tNvAekpGZ0MRLMyQ-2BNHkDd05PTEXs0QocYLF4evJEH5NLD6aKVT-2BQkA8uiyfLlCA-3D-3D
VirusTotal	*None*

URL	https://t.rdsv1.net/ls/click?upn=vmZSPIdvJlJEjv0U0GmezzhgBNOgVLg9sDeuRDN5ukCmxB0gOkbPaEUNBnkMB8m0K-2FHJcmcVhcGhylkzsTK033PE0rSCtUwRyDIlEv-2BV0gE-3DxYSV_Ee7nT2ZQdJ749eAGxVv-2FHN3XNBqa48KbYVWhgkx4gPmq9lJRJyAOpJGecmhmqQ-2BOzEdxpPZTG3-2FcbtSAK-2BaUclKhX3UXigAovFtamcPLixidlDIa9dezstz6DOOZsPHpelYCac1FQPgsvVUSZ0w6dS2L5Idr282b2EFYRQJJsGe1vbi7ptE4Mqirpmltc1Qah43s-2BHvwh5IvmVRP-2FHUgrXo5kOW39-2BayhRLSI3vJxMWy3tZvn-2BYJZ3CLiwjSEDblXyvlyOt9-2BjQAzVEVQ-2FkiOVieZmwidMbDKsMWYmJ5uGhHB-2FXgtDgecz6UlzvkA0I7-2FD-2BgZ6StBCBMzARh-2FmeYTGt49pPRR2zjL2YDZwP3z-2FOmPw-2BcTqQ3fbQnHxooO-2FsFZPsul1fyi0vwtBEOVQJl2Hv1nQ4AtlYiJnis5gBiAZnTLy0EcwXvMPfUVjUQMh-2B8wMG3Rl1mbOuD8vAkSIBVFkRmXKNRmfyapSxfbwDDC310leXSC-2FPkhx0EjfK3EWFfJT00gmPN-2Bdxjxbt6JsF5kZAIKzyo4cFEZGI5onSkHVpX9krvevSCJkVP-2BFZkv-2BzRih3-2FnDjNeftoNTCJTRhhrl1ILaSlqo6OcMTP-2Fdelh9XZ51NFTwK3-2FdBvIpusxy1G14P8i-2BfYE0pHKEph5ZtC-2Fg-3D-3D
VirusTotal	*None*

TRANSMISSION

HOP 1

Timestamp	03 Oct 2023 23:47:28.650 +0000
Received from	MTQwNDMxMDk ((unknown)by geopod-ismtpd-16 (SG))
With	HTTPid VV04DMpGRPOoJ3UAgRlDawTue,

```
from MTQwNDMxMDk (unknown)by geopod-ismtpd-16 (SG) with HTTPid VV04DMpGRPOoJ3UAgRlDawTue, 03 Oct 2023 23:47:28.650 +0000 (UTC)
```

HOP 2

Timestamp	2023-10-03 23:47:29.023676208 +0000 UTC m=+5295985.815374256
Received by	filterdrecv-56867d48f6-6q7fq
With	SMTP
ID	filterdrecv-56867d48f6-6q7fq-1-651CA810-5E

```
by filterdrecv-56867d48f6-6q7fq with SMTP id filterdrecv-56867d48f6-6q7fq-1-651CA810-5E        2023-10-03 23:47:29.023676208 +0000 UTC m=+5295985
```

HOP 3

Timestamp	Tue, 3 Oct 2023 23:47:35 +0000
Received from	wrqvfhpv.outbound-mail.sendgrid.net ((149.72.240.56))
Received by	CO1NAM11FT080.mail.protection.outlook.com ((10.13.174.99))
Via	Frontend Transport
With	Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))
ID	15.20.6863.25

```
from wrqvfhpv.outbound-mail.sendgrid.net (149.72.240.56) by CO1NAM11FT080.mail.protection.outlook.com (10.13.174.99) with Microsoft SMTP Server (v
```

HOP 4

Timestamp	Tue, 3 Oct 2023 23:47:35 +0000
Received from	CO1NAM11FT080.eop-nam11.prod.protection.outlook.com ((2603:10b6:303:85:cafe::8e))
Received by	MW4PR04CA0162.outlook.office365.com ((2603:10b6:303:85::17))
Via	Frontend Transport
With	Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))
ID	15.20.6838.31

```
from CO1NAM11FT080.eop-nam11.prod.protection.outlook.com (2603:10b6:303:85:cafe::8e) by MW4PR04CA0162.outlook.office365.com (2603:10b6:303:85::17)
```

HOP 5

Timestamp	Tue, 3 Oct 2023 23:47:36 +0000
Received from	MW4PR04CA0162.namprd04.prod.outlook.com ((2603:10b6:303:85::17))
Received by	PH7PR19MB6657.namprd19.prod.outlook.com ((2603:10b6:510:1ab::6))
With	Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))
ID	15.20.6813.20

```
from MW4PR04CA0162.namprd04.prod.outlook.com (2603:10b6:303:85::17) by PH7PR19MB6657.namprd19.prod.outlook.com (2603:10b6:510:1ab::6) with Microso
```

HOP 6

Timestamp	Tue, 3 Oct 2023 23:47:38 +0000
Received from	PH7PR19MB6657.namprd19.prod.outlook.com ((::1))
Received by	MN0PR19MB6312.namprd19.prod.outlook.com
With	HTTPS

```
from PH7PR19MB6657.namprd19.prod.outlook.com (::1) by MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 3 Oct 2023 23:47:38 +0000
```

RECIPIENT MAILBOX

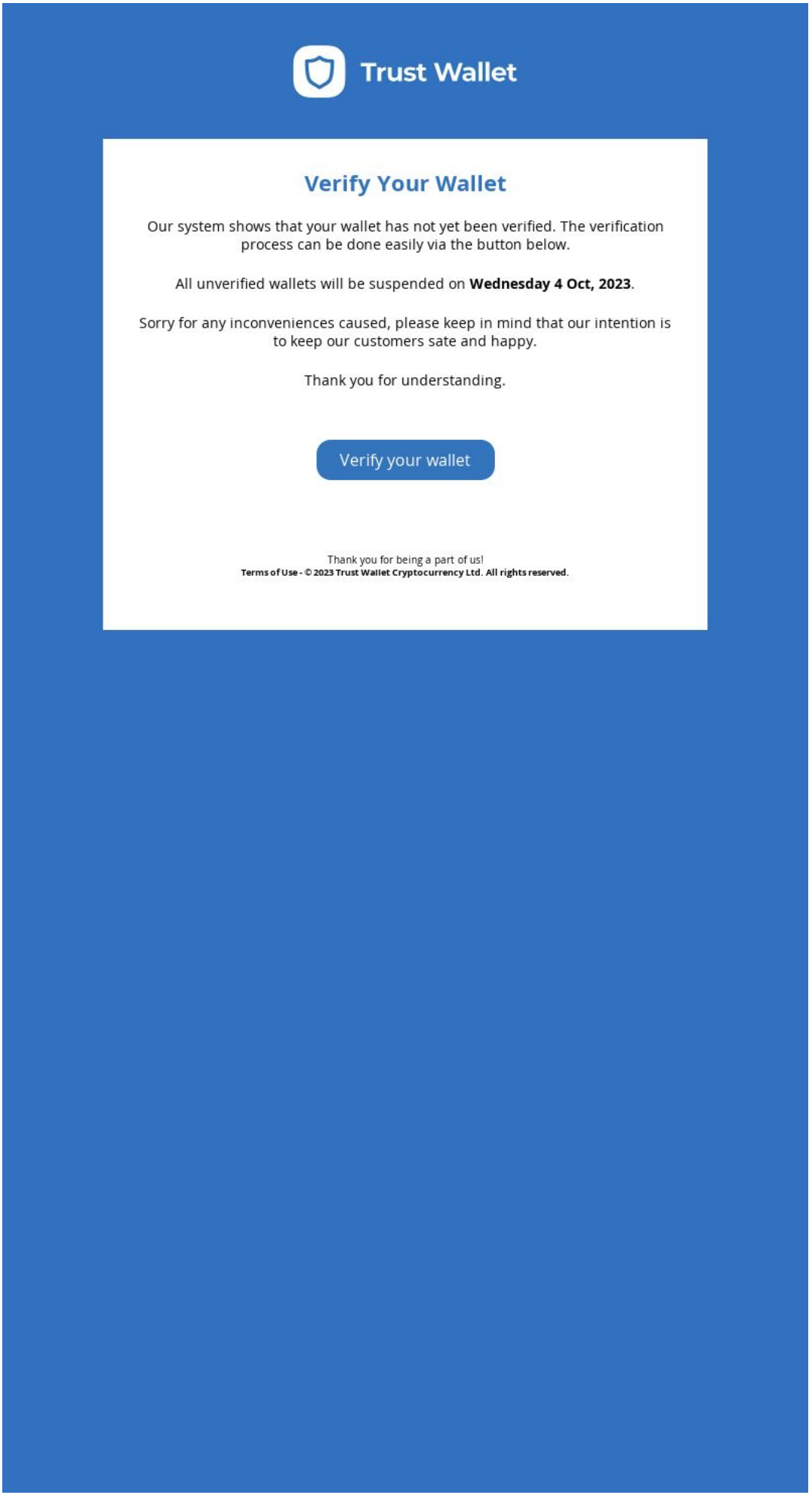
Timestamp	Tue, 03 Oct 2023 23:47:34 +0000 (UTC)

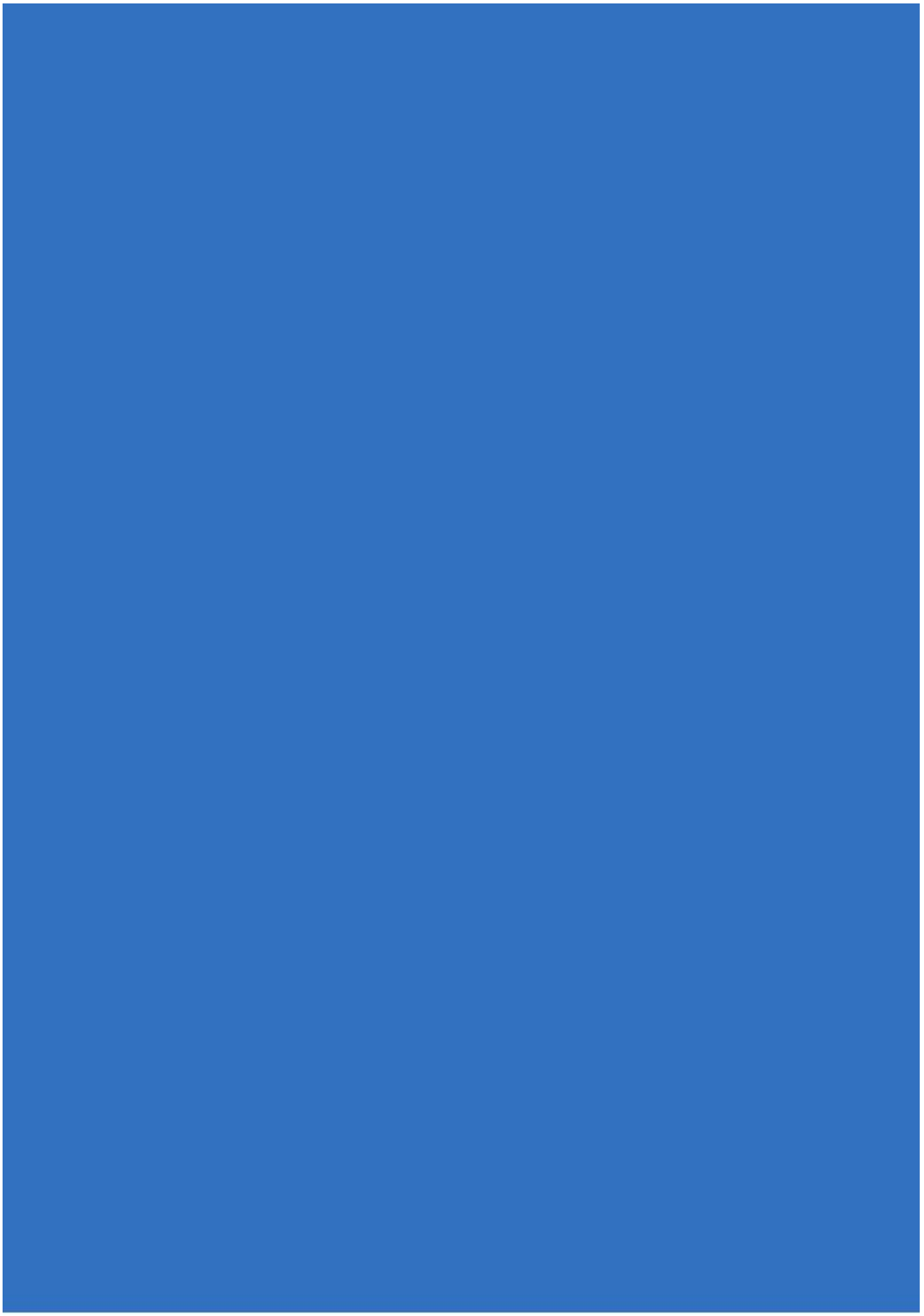
X-HEADERS

x-incomingtopheadermarker	OriginalChecksum:AE6B18BB87B6E8849F685FDD8BC92B678F04AF3C85AAEC058D3CD15E5F0F0DD5;UpperCasedChecksum:D6AA996F3E50465C02956D1E9B9169A73DC0B6ADF88D2C0C76625DE1A93BE9BD;SizeAsReceived:2468;Count:15
x-sg-eid	PJTXchHg3/msS3AKIQ4IujsfPQG5HBgLBPuDGhVEO0yfBVzbZerITote1iD/K5lSIWmD6TBJDLrjP6z+KJU5hEcpj7MgYHzeFNfAq/fJO+HBfC5TRw5MccyO6n5XphxB038b0pRFycHxaMU0yG7/qcibc9audQkvD0ABqzB9DySLj26+kvr4zBiht2qdhwK3xVqwqiit/A9sb1vpb3/ljvSJmgVEcGw1GS4tHkM7dVEYlMqQys91fnx62JbV2W9R

x-sg-id	N2C25iY2uzGMFz6rgvQsb8raWjw0ZPf1VmjsCkspi/Kg6ychMtueaf6Ck44Mttgf5Rjjw6BS7a8I9rdJtuUIVQ02LNoTeLwsO75p5/KnYXfFfEo0epVkYGbw3TvfsrHhu2k0LeaTBrre9C9nqHydJUtqo0zFkQ9IL9kA+BcJ2WQFqIHVGXwQQVCVa24BJTaO9R6o2E7+Hscu2Ub5BbHFfVNeL5g5uwquoJQHAcWZXCzOQU3UYtiR0zR26cc7EOsjCinarnZbjEu6M6dRHA4iY99fRNTXoGQzsgXkTOQipZm7hWYJU/jpOUNBkrxj7Ksrs5fp2Kc+lzOmlxKWVXR/oQfUsO5YZWQS7vLMqiYyI4Wuu19KkNvk42ezUVTTxYYveMhVQqyx0IsdDzw8gI04hR2IXATZkBiBtfCu/yAT1GSmGk2N8Edh4I9YPNtqy6/I7Hx3mBxFdneW54INyvVsdSSp6X4k2YihVcCV7Yc8QZM=
x-entity-id	mdPEYpC/ruADmyyF+Dr3Qg==
x-incomingheadercount	15
x-ms-exchange-organization-expirationstarttime	03 Oct 2023 23:47:35.8545 (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	89718940-b62f-4291-6b23-08dbc46b1eb1
x-eopattributedmessage	0
x-eoptenantattributedmessage	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
x-ms-exchange-organization-messagedirectionality	Incoming
x-ms-publictraffictype	Email
x-ms-traffictypediagnostic	CO1NAM11FT080:EE_|PH7PR19MB6657:EE_|MN0PR19MB6312:EE_
x-ms-exchange-organization-authsource	CO1NAM11FT080.eop-nam11.prod.protection.outlook.com
x-ms-exchange-organization-authas	Anonymous
x-ms-userlastlogontime	10/3/2023 10:56:25 PM
x-ms-office365-filtering-correlation-id	89718940-b62f-4291-6b23-08dbc46b1eb1
x-ms-exchange-eopdirect	true
x-sender-ip	149.72.240.56
x-sid-pra	CLAUDIA@ITPRO.NET.BR
x-sid-result	PASS
x-ms-exchange-organization-pcl	2
x-ms-exchange-organization-scl	5
x-microsoft-antispam	BCL:0;
x-ms-exchange-crosstenant-originalarrivaltime	03 Oct 2023 23:47:35.3389 (UTC)
x-ms-exchange-crosstenant-network-message-id	89718940-b62f-4291-6b23-08dbc46b1eb1
x-ms-exchange-crosstenant-id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
x-ms-exchange-crosstenant-authsource	CO1NAM11FT080.eop-nam11.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	PH7PR19MB6657
x-ms-exchange-transport-endtoendlatency	00:00:02.9607338
x-ms-exchange-processed-by-bccfoldering	15.20.6813.014
x-microsoft-antispam-mailbox-delivery	ucf:0;jmr:0;ex:0;auth:1;dest:J;OFR:SpamFilterAuthJ;ENG:(5062000305)(920221119095)(90000117)(920221120095)(90005022)(91005020)(91035115)(9050020)(9100341)(944500132)(2008001134)(2008121020)(4810010)(4910033)(9710001)(9555003)(10175021)(9320005)(9245025)(120001);RF:JunkEmail;
x-message-info	6hMotsjLow9yPHoe0Cp3K2KkvdzhS2QAiZV2HP+hE3mDjOQ0pn4FpDXlbQGc7c/VZGZ17pw5ETWOmsq1jM7XmuRcHl2LWO+CVYxaLC9FVaKeMBpVUspN4cqunVXy7KpcuEAf2UT4pWQGi8oLG30syBu0q8B8gUh2zgrq/Wo4yNaX+0CkS6+YEsS0BrAErLiTxUunq2OugC0IjUnIazDOeQ==
x-message-delivery	Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MjtHRD0yO1NDTD02
x-microsoft-antispam-message-info	WxxLDvX70efynVClNwXNdsyFoP2ySaIZ3Yfs4vfj0O8dcGULyTXB2PG3O35Ywo/jVd4qxyEg7koj9ZSCQt24zzWnln/jeU96HWGTFPGGmscmnySPs+7xFnetZg/iI6Tf1POpmhXzd9Uwlh04x5LAdMd6lECDf/PbLRiypelwyB3Gy16bxS7xPnJorj+t74dJ/nSbTRfhjHchQAxusQ515liKGzRhIsWI0ysE8ls4jaZGqZCu+F/iP5yZn/8/W+r/zBMkk57YmDbe3AX2sPeQzsV6HuGMeiS0+vtLIUrupsaHaQ2vPIzIlfIDwOnvWVJ/ipqcjNmN7DRfRT8xEABuyTKydbApR+uTxVudv0ZKz5epnZ7wXz+rp6UUQK6Yea/n1Um33GOe+cKYCkPyNTBBAiRCx4eJy+2BKq75PxnuaNtkBfL/ui8vdHO00VmUgAvF777KL9FW1QN0WNNc7K2U3wZf3t5wOSt5KKbdbTT7V/dqMGCx3BmyychLKT0fMb9nvnqvNIXQzVPKUxD+PW9564gKfz6QN0GLJzVID8R6Xt/mcAaJmHzOhfBm+ne1wmM1Y+877fajAaMZK5B1W3Sh3zYMCAJc4dLZS3QaAiOak3H5iyCs/6eBHx88vZaFEhmjxgeWgW5YmNXJq1MGvtyID2pNcrRSKNxuXUFkt1mldfP8M7tvTDXX2wIxvdT7DK9YjitQoVRkDbY9qAP42UgMnnvWW1UTLPU9qNjq87B2/Y9st7tcKzk0Zk/BYF0nEBS+DPmAdO9gRQiH1n95WzBDIGvgTjfb73wkgjwuI855BXtlWeo5xrdCdlufnIDkR9X/6Jrq4uyvnQcw3xNfiQmAW0bCKvvWQExUshZvP+CRZcsb2uTkuedpJRBXZfaYmFpWBXZDi/heoaIuP79oW4uSi4fL9dtZ9bAuStIUvedtv/UmQKhiAjNf9hhTNgUivn7s12U8F1ghNO59jxbZYwzSYuc8UVtzKoCTcsajiIYgFBUq0S17ryhpvuQ15hUURtcObzHz8AS9siYOkvqpV8ULcZcvGIOCzVTmsdHUii1CKp7o/LokmEa+R2J1qV3MLvj+c9WSpVTj3nM8olCG8/mEtTr3hWSHht12rEc60uB5A9JbAC0kUUqRmW8d/XtoV+bDqd40+IKvw7oqGZr4jR20mkn5tIDztL6WbPk+MrNYjrB/m87xiCxjghfUrHSoZeeh/5cltBAqx5CcCsq+zHmU0H7s10k8Q1guMrKpFHHY5KdYPl2YD5DHFduWhLA9L0Kj7jPBThcJfznlhLQ4uCPVaVqAPgk/3AxhBWVAapmrzKVmNCQHDSnVO01xbvNpjCxCJ2wJiYtk+c2ABBQ/Y3i32RefgcMdcJHUk8QpgkWTjbnVFJiofu/S6KLE6PYqs0jo4rFgxclRSbKYdfsnYl2C37n1R7d6rwEamXXTBG3dN+KfaYeCrYcVQ4zn9L+IuJm8RcWDTJ/eq8h4l2W73EPUAWonAMAn1vsfhEXl3+Yq3VC2Fs/oBux2NbQAPzdHMI8RusviRZjaUcTM+jqikaqxuMU/2M4h0qfQPjrHef/KsB5BiqPhW9sCibssWYkQBrXxqnUO4vC7/O7Dij1SI4LlTipsFwiZ/ktAmkM4zfQUUKfcSDW9H3DbP7ILK9+KHs1jS7IoDP+poyxJBJUDYU2mSApmZKXfM9DO8X9QLXBDcX8xYI46SShnouHPRydpIzs3+4s5Xc72fM8JmJTNZPTuPEfN/hslAcL1sDye77rzGAn4rDgizfEppsLABwzd7FT+oV6JfHt4vRTmM60m6n8dR1YMABYlsOD3HI8ysI0xWwESGZtArUYGEDSI0mFda77tU3iWU1tt8Na894IeH+zfbGBXewdvqdlPxW98qZ88A3eZn29ka7HI/KF01SU1XHYRwQpFAhEOSevuV+EakjesT2HqaAyvZizz37vAsbGNXGmCi+i0pGlfm/nk9+hMShl/

MESSAGE RENDER





Enviado por **IT PRO**
Rua Henrique Monteiro 79 - Pinheiros São Paulo - SP
Se deseja não receber mais mensagens como esta, clique aqui.
Visualizar como página web

MESSAGE PLAINTEXT

Verify Your Wallet

Our system shows that your wallet has not yet been verified. The verification process can be done easily via the button below.

All unverified wallets will be suspended on Wednesday 4 Oct, 2023.

Sorry for any inconveniences caused, please keep in mind that our intention is to keep our customers sate and happy.

Thank you for understanding.

Verify your wallet [https://t.rdsv1.net/ls/click?upn=QJHDLu6c7joILAshEaWRB90ZvG3MeB7stfqQoNfEMaoKnttIpVYuRKEo8ASi9sTkYTGqKsbrHulqBqCo6R83H-2BMPpTZ-2FPFQPHNxCWnvt06OfPqj6vFBieRdLd63IeEdddn-2BtNZ15bfQjlTLRr2eDqnuV-2BpwBQ9ZHfBRMwYi5ADY-3D5pdi_Ee7nT2ZQdJ749eAGxVv-2FHN3XNBqa48KbYVWhgkx4gPmq9lJRJyAOpJGecmhmqQ-2BOzEdxpPZTG3-2FcbtSAK-2BaUclKhX3UXigAovFtamcPLixidlDIa9dezstz6DOOZsPHpelYCac1FQPgsvVUSZ0w6dS2L5Idr282b2EFYRQJJsGe1vbi7ptE4MqirpmltcQah43s-2BHvwh5IvmVRP-2FHUgrXo5kOW39-2BayhRLSI3vJxMWy3tZvn-2BYJZ3CLiwjSEDblXyvlyOt9-2BjQAzVEVQ-2FkiOVieZmwidMbDKsMWYmJ5uGhHB-2FXgtDgecz6UlzvkA0I7-2FD-2BgZ6StBCBMzARh-2FmeYTGt49pPRR2zjL2YDZwP3z-2FOmPw-2BcTqQ3fbQnHxooO-2FsFZPsul1fyi0vwtBEOVQJl2Hv1nQ4AtlYiJnis5gBiAZnTLy0EcwXvMPfUVjUQMh-2B8wMG3Rl1mbOuD8vAkSIBVFkRmXKNRmfyapSxfbwDDC310leXSC-2FPkhx0EjfK3EWFfndccYwu2Ul2-2FtcfQUcvS9pY-2Feg9vHB44mEU8bMs-2Fw7Nzz0S7D7gj4Pu4JEIDA3jw4-2BQdujgqqjhYpGxh6XyNuF13GSmyvVZ79kU4EoRtOBdcb6OMUbZADdiI8LYNpr50gU5qOsAaz27C-2BhwPh2dmNw-3D-3D]

Thank you for being a part of us!

FLAGGED ARTIFACTS

From email address	claudia@itpro.net.br
Return-Path email address	bounces+14043109-f56e-phishing@pot=hotmail.com@alavancandominhacarreira.itpro.net.br
Return-Path domain	pot=hotmail.com

OPEN SOURCE INTELLIGENCE

DNS - ITPRO.NET.BR

A 187.45.193.168

MX 20 mx.b.locaweb.com.br
10 mx.core.locaweb.com.br
20 mx.jk.locaweb.com.br
20 mx.a.locaweb.com.br

TXT v=spf1 include:_spf.locaweb.com.br -all

SOA ns1.locaweb.com.br. hostmaster.locaweb.com.br. 2022031001 3600 600 1209600 3600

NS ns1.locaweb.com.br
ns2.locaweb.com.br
ns3.locaweb.com.br

WHOIS - ITPRO.NET.BR

Name servers ns1.locaweb.com.br
ns2.locaweb.com.br
ns3.locaweb.com.br

AUDIT LOG

2025-10-22T12:29:55Z Resolved as "Malicious" by madhavgarg679@gmail.com

2025-10-22T12:27:01Z Manually uploaded by madhavgarg679@gmail.com