EMAIL ANALYSIS REPORT

Analysis URL	https://app.phishtool.com/analysis/68f8c272370b6cd6b3e675d7
Email subject	CLIENTE PRIME - BRADESCO LIVELO: Seu cartÃ£o tem 92.990 pontos LIVELO expirando hoje!

RESOLUTION

Resolved by	madhavgarg679 (madhavgarg679@gmail.com)
Resolved on	2025-10-22T12:15:08Z
Disposition	Malicious

CLASSIFICATION CODES

COMPRO_SEND The sender is legitimate; however, an attacker has gained control of the sender’s mailbox and has used it to send a phishing email to the target.

AUTO ANALYSIS

1 Malcious indicators

Inconsistent Return-Path domain

The 'Return-Path' domain **ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06** is inconsistent with the 'From' domain **atendimento.com.br**.

DETAILS

From	banco.bradesco@atendimento.com.br
Display name	BANCO DO BRADESCO LIVELO
Sender	*None*
To	phishing@pot
CC	*None*
In-Reply-To	*None*
Timestamp	Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
Reply-To	*None*
Message-ID	<20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>
Return-Path	root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
Originating IP	137.184.34.4 (Hop 2)
rDNS	*None*

AUTHENTICATION

SPF

Result	***NONE***
Originating IP	137.184.34.4 (Hop 2)
rDNS	*None*
Return-Path domain	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
SPF record	*None*

DKIM

Result	***NONE***
Verification(s)	0 Signatures

DMARC

Result	***NONE***
From domain	atendimento.com.br
DMARC record	*None*

URLS

URL	https://blog1seguimentmydomaine2bra.me/
VirusTotal	0/98

TRANSMISSION

HOP 1

Timestamp	Tue, 19 Sep 2023 18:35:49 +0000
Received by	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 ((Postfix, from userid 0)id 39DEA3F725)

```
by ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (Postfix, from userid 0)id 39DEA3F725; Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
```

HOP 2

Timestamp	Tue, 19 Sep 2023 18:36:44 +0000
Received from	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 ((137.184.34.4))
Received by	BN8NAM11FT066.mail.protection.outlook.com ((10.13.177.138))
Via	Frontend Transport
With	Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))
ID	15.20.6813.19

```
from ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (137.184.34.4) by BN8NAM11FT066.mail.protection.outlook.com (10.13.177.138) with Microsoft SMTP Server
```

HOP 3

Timestamp	Tue, 19 Sep 2023 18:36:45 +0000
Received from	BN8NAM11FT066.eop-nam11.prod.protection.outlook.com ((2603:10b6:408:e6:cafe::23))
Received by	BN0PR03CA0023.outlook.office365.com ((2603:10b6:408:e6::28))
Via	Frontend Transport
With	Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))
ID	15.20.6792.28

```
from BN8NAM11FT066.eop-nam11.prod.protection.outlook.com (2603:10b6:408:e6:cafe::23) by BN0PR03CA0023.outlook.office365.com (2603:10b6:408:e6::28
```

HOP 4

Timestamp	Tue, 19 Sep 2023 18:36:45 +0000
Received from	BN0PR03CA0023.namprd03.prod.outlook.com ((2603:10b6:408:e6::28))
Received by	SA3PR19MB7370.namprd19.prod.outlook.com ((2603:10b6:806:317::17))
With	Microsoft SMTP Server ((version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384))
ID	15.20.6792.27

```
from BN0PR03CA0023.namprd03.prod.outlook.com (2603:10b6:408:e6::28) by SA3PR19MB7370.namprd19.prod.outlook.com (2603:10b6:806:317::17) with Micros
```

HOP 5

Timestamp	Tue, 19 Sep 2023 18:36:46 +0000
Received from	SA3PR19MB7370.namprd19.prod.outlook.com ((::1))
Received by	MN0PR19MB6312.namprd19.prod.outlook.com
With	HTTPS

```
from SA3PR19MB7370.namprd19.prod.outlook.com (::1) by MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 19 Sep 2023 18:36:46 +0000
```

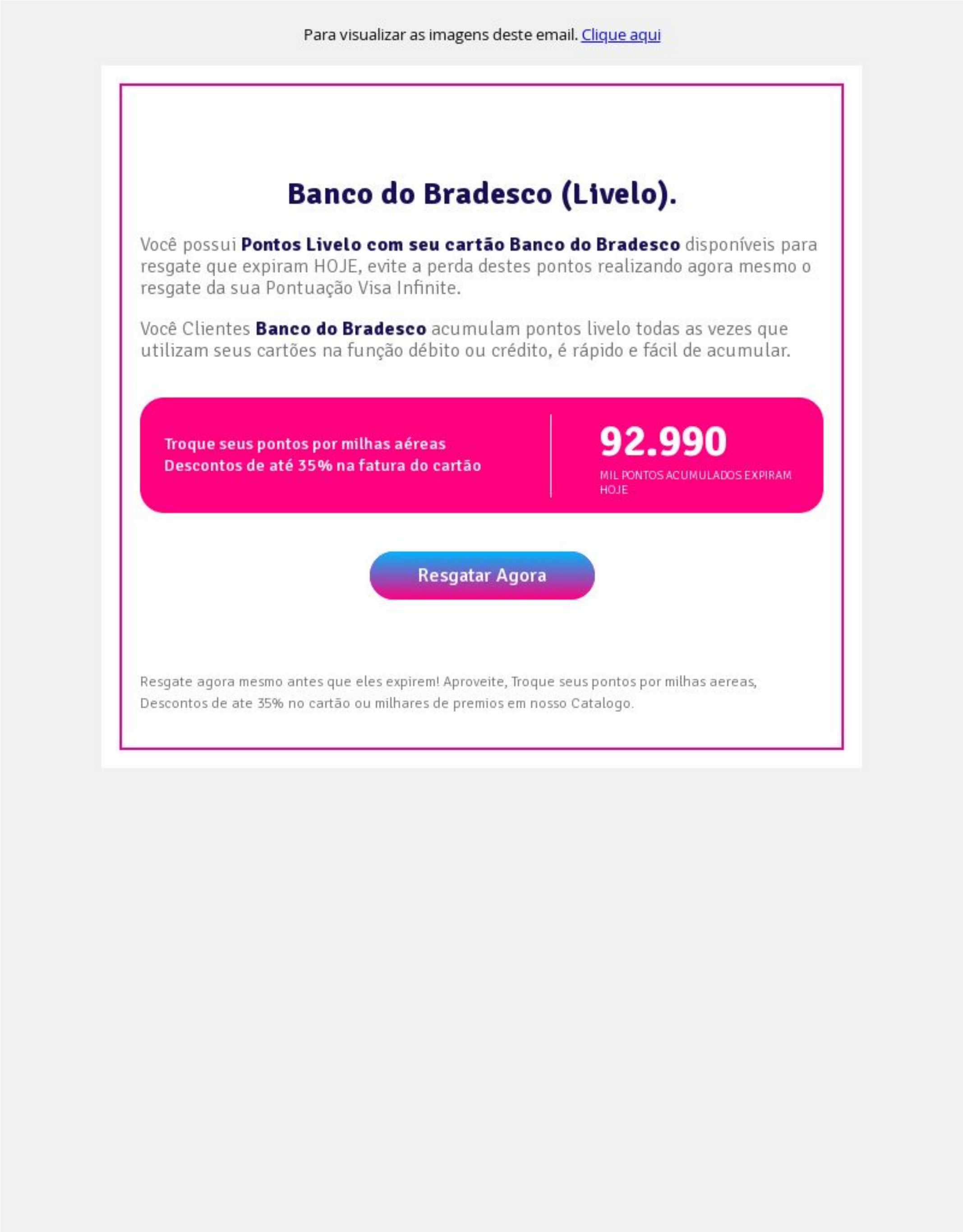
RECIPIENT MAILBOX

Timestamp	Tue, 19 Sep 2023 18:35:49 +0000 (UTC)

X-HEADERS

x-incomingtopheadermarker	OriginalChecksum:3B61F64750F88C5569DF38A496B2374685F23D8BC662A6A19B6823B2F6745D54;UpperCasedChecksum:62071BC7A7CF5B0844A7B406B0E9EFCDAA2CB94988E687CF8C56555AD4B52D30;SizeAsReceived:544;Count:9
x-incomingheadercount	9
x-ms-exchange-organization-expirationstarttime	19 Sep 2023 18:36:44.2236 (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	b9106deb-bd54-4815-e5c9-08dbb93f5fab
x-eopattributedmessage	0
x-eoptenantattributedmessage	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
x-ms-exchange-organization-messagedirectionality	Incoming
x-ms-publictraffictype	Email
x-ms-traffictypediagnostic	BN8NAM11FT066:EE_|SA3PR19MB7370:EE_|MN0PR19MB6312:EE_
x-ms-exchange-organization-authsource	BN8NAM11FT066.eop-nam11.prod.protection.outlook.com
x-ms-exchange-organization-authas	Anonymous
x-ms-userlastlogontime	9/19/2023 6:25:15 PM
x-ms-office365-filtering-correlation-id	b9106deb-bd54-4815-e5c9-08dbb93f5fab
x-ms-exchange-eopdirect	true
x-sender-ip	137.184.34.4
x-sid-pra	BANCO.BRADESCO@ATENDIMENTO.COM.BR
x-sid-result	NONE
x-ms-exchange-organization-pcl	2
x-ms-exchange-organization-scl	5
x-microsoft-antispam	BCL:9;
x-ms-exchange-crosstenant-originalarrivaltime	19 Sep 2023 18:36:44.1298 (UTC)
x-ms-exchange-crosstenant-network-message-id	b9106deb-bd54-4815-e5c9-08dbb93f5fab
x-ms-exchange-crosstenant-id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
x-ms-exchange-crosstenant-authsource	BN8NAM11FT066.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	SA3PR19MB7370
x-ms-exchange-transport-endtoendlatency	00:00:02.6179349
x-ms-exchange-processed-by-bccfoldering	15.20.6792.025
x-microsoft-antispam-mailbox-delivery	wl:1;pcwl:1;ucf:0;jmr:0;ex:0;psp:0;auth:0;dest:I;OFR:TrustedSenderList;ENG:(5062000305)(920221119095)(90000117)(920221120095)(91040095)(9050020)(9075021)(9100341)(944500132)(2008001134)(4810010)(4910033)(9610028)(9560006)(10180021)(9439006)(9310011)(9220031)(120001);
x-message-info	qZelhIiYnPlgo3oeAkqKQrb/Je8fpvpPmRGjYwLej8PYXc5p/l16IG5I8gDUPoij+JWSvja0BAMLtkgrOcbx5zEN7V98T2UZUZs4k8BX/DcDfI7QJ0t2aouiqx4ENvkR1M3sDKP/XN09+50x9Rxi6onUtDV4eqq36VUi2qAa0zCzkJwjdl3Y9DzNE1OkaWjrHAizeUyMZ/UtK/Pz9zhA2A==
x-message-delivery	Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtHRD0yO1NDTD0tMQ==
x-microsoft-antispam-message-info	A9WDUZMTanasU4dmPSHTRQDkA4rh8seW3cdQ9awmUCMgdmU4TrvQOpYAKmyEEeTrlugn8j983BLEV3eoVVA75Vi+GiI5YIArG7oAcIyq26SkfpqpokfNsA0/30OlLIYh6HXDAeoDMBxHn30zgHdQgh44V7E4cRGr9q8dLQ4U8PGGTQLYg50SC79Kla8rbdNJMaXxiDJrrcJ1z/BeQQB+Dit+OI78ZgadIrD28l10GjfS5Ri6NGzhxMSrB9bHRbeOIp7c2DkcmJ4HZGQUqRx5UnkVGt+rrI+yVEd83aGnQl0pQt+bO5diP8HlWnrGkd4/gzGwWSZ7wR00t3k5yn1o4pzVb/KkcPUTPGHVk+aBqJHIqdDmSMXdEHfqkbHjxjaVufSozOANeFFr/WIYeJBqxOA1oretAr7MRpqYeHl2zQjoZ0QK4aUUHlLHX8SCuCUwVXPAYARZ7ehIgpvrEcqHB3v8iH98idTMNMaAnkPycmUwT2Oa+4TWvtLLrxGgiuQHKRnDI/CNpXk87PO7oj8dt3KNQ9zdqhkPguxYxBXS2T0NJwDVjeTimJJfzhdiQPd1h2ULYR6fZ5JuD4HbdHOHwDrQ+VA2DLs0YnEowS+TDpK+Q19PZXhcDzWbjDWKC6KoCly2BDxfFZiWACrT4r4ZCSExfV9ZNCkt9+g3qTdUfm+yVMdzqaBUKoF0NXE8s37xrKcLIR5xxozjn8VFfVz/ykAO4a5C1R7boM4WkzjjtUNRdc1lqjAMuiWtP1yxbtEGc1Y6ocVgJ56fCN+E7j3DjCL85fhLo0Uisy5I4DfshNBMrb4cG0qxluGrm54GnbBKz2+h2tjjxO1T6VxtWwEx734hUYaTehqCIVd9esCMRh6EIB+h3yBEMqMibgeVmunNeTz0OTVrPlUeMGZPjP2Ju0e3VBhvW4sUmKH8Yp+jLV+QB63VYMdZmxgTw61gWIHuUeBr5w2Z1y6gMH/8xX/Fm2oSYo/gpD5/j+0whrdtAleRL4AKqGheJPdmJJkcmvrYy83Tzs9pXLGC67d+Uk33ZHsLSYqTTYFkzbPPmr696cX337IvP/L0BB70NxDMz3S2XkazqLDdTERyWO8b03bFI6ZTEhaz+J5gGv+CxrQXljbUGMHoadtW0O9rmeMLJ2zT3dgpUWO75PyudRZcEKNnS55Kb3vn0TFW8ZHAhQD55vpEfvQkbGlKm9liRJ/v/3vL4H+4wPr2HwnWnMEZLaw4ZB7nrJSsa7aYfQWstI90LrUb+Y23mo/zXyTxisERzMbXogysUqw+QLSTzfdGXYG7TgTVv7HehGpmo/yVVNaxvPtBIZk3xU7t9VdYMomn0cWeVKSa5hW40hm74NRe3SnO5j2G5Z2FTP4hNeUzivl132R11hzjcSZMTwHDa/mH6FMfOYP3Ba5xxrtCEDLdWRMcEXbxViPyJc7W9eYPUOoobVkrzRHZiErGB3teaKDKKDd2j3b5KkrSHLa+WaYSqDUfwTm0Q405yH4WASCtjqLYUmvqs2LUnapA4HBj8zZEB4q1yPrPNoUaPZHJ7h+bgYq67+uVhz7Jlcsn/8fp750cQUA6DtGWGDfbrlMKscV1iOPAGgzinwkLiOg9LwtTbqnqNiscux4RgIDHPpef5JcnTNyxjMFQ/3htymlYdCV4bo6XFsmqG9kxbweipkP7TyQcOCHqkDwRmTwFekquWIbly88wSVWy7ucfOUsOVP7ft25t/lX6/UPZ7XL59l2p/92LDGtvwhE3eF+9PjgSc3Jxh37dzLkcXCyANBWg1Pbk/RYECWdVIcLAYR75ECIj16y5a/iRs2l4IHGNBnWessjnEYj3lHjFxBM/amYWkCs6PkAW7S2RwOSig1gCqsKR8rHyA/LR5qjdfCG7rlHd2rKeKwNnVfiBf7e/F6AgksjxbVPWD6MoCy2HKpXGotO2+YmcVwTx5SLpEmbBUwLh1ZWdWKg6K40bfrreI17Om/2I5YsQvajOQh4LxpjU3ZzzKDl94zDc8WyPKMzbmTska14Rfyz/20CztdptNubn+CMuUeezqC/Cm0NY14Zz1hcZhWN9XT6AlVcwbc3dNoEh07Bm9c29BImiVs074GXQhKS89yF9wCwh6A2n3KP5qghQB+5BXzXWYQjHSuHLbbf2Aykr6KUggjkESlgT8imYdzvF++3VYCZgVaj1uyhKsXuylbVFq6GcDjw9LYC5RoqrsEXQCHwSqXDCHKfDsPeB4teJsEcPIVUDNiQxWOp5VXQ98wJgWzc/ZMD/Bi/T/fWy9PcxTDrk/DP5G2RG60RJre67BtnsAKpAf+DhkQT041hdDHCo9X5/40KUCBI60HTbo3S252o3tMlzG3bePqDYti4Lcsjw6Fh70h7Us0mwmaljJ7wT9hyxkoy3DOV6WegpGQrAxmu48Qv+Ewni85jh13/6toBfvNFIe8LKPJSWFMOofrDYR9w50DRCnhB/jAJbX3IF5oU45xPbBCKgLobc7kovAV9sSOKUIqKwJhbbEYq1q0OtA+2rNRIlVoNofliELUgqU0dtLOvHd1MrhRiLykB27zX254Yf3XZvjj+gbKU7uQERoTxmX4s26MJrDNGDD3CAkRWj+PbRRlcXjOmTWgIVgydoqT97SPTgEorEq3krKPfE4A==

MESSAGE RENDER



Para visualizar as imagens deste email. Clique aqui

Banco do Bradesco (Livelo).

Você possui **Pontos Livelo com seu cartão Banco do Bradesco** disponíveis para resgate que expiram HOJE, evite a perda destes pontos realizando agora mesmo o resgate da sua Pontuação Visa Infinite.

Você Clientes **Banco do Bradesco** acumulam pontos livelo todas as vezes que utilizam seus cartões na função débito ou crédito, é rápido e fácil de acumular.

Troque seus pontos por milhas aéreas
Descontos de até 35% na fatura do cartão

92.990
MIL PONTOS ACUMULADOS EXPIRAM HOJE

Resgate agora mesmo antes que eles expirem! Aproveite, Troque seus pontos por milhas aereas, Descontos de ate 35% no cartão ou milhares de premios em nosso Catalogo.

FLAGGED ARTIFACTS

From domain	atendimento.com.br
Return-Path email address	root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
Originating IP Address	137.184.34.4
Message URL	https://blog1seguimentmydomaine2bra.me/

OPEN SOURCE INTELLIGENCE

DNS - ATENDIMENTO.COM.BR

WHOIS - ATENDIMENTO.COM.BR

Name servers	ns822.hostgator.com.br ns823.hostgator.com.br

IPWHOIS - 137.184.34.4

Network Name	DIGITALOCEAN-137-184-0-0
Organisation name	DigitalOcean, LLC (DO-13)
CIDR	137.184.0.0/16
Registration date	2019-11-13
Updated date	2025-03-03

DNS - BLOG1SEGUIMENTMYDOMAINE2BRA.ME

WHOIS - BLOG1SEGUIMENTMYDOMAINE2BRA.ME

AUDIT LOG

2025-10-22T12:15:08Z	Resolved as "Malicious" by madhavgarg679@gmail.com
2025-10-22T11:39:30Z	Manually uploaded by madhavgarg679@gmail.com