**E-Mail Analizi – 1**

**Sample-1004**

Mailimizin içeriği şu şekilde   
Received: from DS7PR19MB5974.namprd19.prod.outlook.com (::1) by

MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Wed, 26 Jul 2023 16:51:07

+0000

Received: from FR0P281CA0242.DEUP281.PROD.OUTLOOK.COM (2603:10a6:d10:af::12)

by DS7PR19MB5974.namprd19.prod.outlook.com (2603:10b6:8:7f::21) with

Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.6609.33; Wed, 26 Jul

2023 16:51:05 +0000

Received: from VI1EUR04FT036.eop-eur04.prod.protection.outlook.com

(2603:10a6:d10:af:cafe::c4) by FR0P281CA0242.outlook.office365.com

(2603:10a6:d10:af::12) with Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.6631.24 via Frontend

Transport; Wed, 26 Jul 2023 16:51:04 +0000

Authentication-Results: spf=temperror (sender IP is 147.182.193.196)

smtp.mailfrom=ubuntu-s-1vcpu-512mb-10gb-sfo3-01; dkim=none (message not

signed) header.d=none;dmarc=fail action=none

header.from=bradesco.com.br;compauth=fail reason=001

Received-SPF: TempError (protection.outlook.com: error in processing during

lookup of ubuntu-s-1vcpu-512mb-10gb-sfo3-01: DNS Timeout)

Received: from ubuntu-s-1vcpu-512mb-10gb-sfo3-01 (147.182.193.196) by

VI1EUR04FT036.mail.protection.outlook.com (10.152.29.167) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id

15.20.6631.29 via Frontend Transport; Wed, 26 Jul 2023 16:51:02 +0000

X-IncomingTopHeaderMarker:

OriginalChecksum:97C46D1AC621606AEB5B7BF204FF9075B4F86C494C7182BEC2969203950ECBA6;UpperCasedChecksum:62D0C362A8AFABEF2B00A53ED47606FF8241221541C15A52696EC45757E5422C;SizeAsReceived:481;Count:9

Received: by ubuntu-s-1vcpu-512mb-10gb-sfo3-01 (Postfix, from userid 0)

id 6B02D4DDD8; Wed, 26 Jul 2023 12:17:46 +0000 (UTC)

Content-type: text/html; charset=UTF-8

Content-Transfer-Encoding: base64

Subject: Seus pontos Livelo expiram em breve - PROTOCOLO: 57949307.

From: Bradesco <sac@bradesco.com.br>

To: phishing@pot

Message-Id: <20230726121746.6B02D4DDD8@ubuntu-s-1vcpu-512mb-10gb-sfo3-01>

Date: Wed, 26 Jul 2023 12:17:46 +0000 (UTC)

X-IncomingHeaderCount: 9

Return-Path: root@ubuntu-s-1vcpu-512mb-10gb-sfo3-01

X-MS-Exchange-Organization-ExpirationStartTime: 26 Jul 2023 16:51:02.6253

(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:

8f091a1a-57d5-4bd4-88cb-08db8df87f10

X-EOPAttributedMessage: 0

X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0

X-MS-Exchange-Organization-MessageDirectionality: Incoming

X-MS-PublicTrafficType: Email

X-MS-TrafficTypeDiagnostic:

VI1EUR04FT036:EE\_|DS7PR19MB5974:EE\_|MN0PR19MB6312:EE\_

X-MS-Exchange-Organization-AuthSource:

VI1EUR04FT036.eop-eur04.prod.protection.outlook.com

X-MS-Exchange-Organization-AuthAs: Anonymous

X-MS-UserLastLogonTime: 7/26/2023 4:25:12 PM

X-MS-Office365-Filtering-Correlation-Id: 8f091a1a-57d5-4bd4-88cb-08db8df87f10

X-MS-Exchange-EOPDirect: true

X-Sender-IP: 147.182.193.196

X-SID-PRA: SAC@BRADESCO.COM.BR

X-SID-Result: NONE

X-MS-Exchange-Organization-PCL: 2

X-MS-Exchange-Organization-SCL: 7

X-Microsoft-Antispam: BCL:9;

X-MS-Exchange-CrossTenant-OriginalArrivalTime: 26 Jul 2023 16:51:02.4378

(UTC)

X-MS-Exchange-CrossTenant-Network-Message-Id: 8f091a1a-57d5-4bd4-88cb-08db8df87f10

X-MS-Exchange-CrossTenant-Id: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa

X-MS-Exchange-CrossTenant-AuthSource:

VI1EUR04FT036.eop-eur04.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: DS7PR19MB5974

X-MS-Exchange-Transport-EndToEndLatency: 00:00:04.8320948

X-MS-Exchange-Processed-By-BccFoldering: 15.20.6609.030

X-Microsoft-Antispam-Mailbox-Delivery:

abwl:0;wl:1;pcwl:1;kl:0;dwl:0;dkl:0;rwl:0;ucf:0;jmr:0;ex:0;psp:0;auth:0;dest:J;OFR:SpamFilterAuthJ;ENG:(5062000305)(90000117)(91040095)(9050020)(9075021)(9100338)(944500132)(2008001134)(4810010)(4910033)(8820095)(9610025)(9525003)(10145022)(9320005)(9245025);RF:JunkEmail;

X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MjtHRD0yO1NDTD02

X-Microsoft-Antispam-Message-Info:

=?utf-8?B?L3htSDVVT0tuTzhyMDV0M0c4bUE3eUhEWnpIR25STlhoUnVacHhOMXh4LzRF?=

=?utf-8?B?ZkpMSHZxakt5U3I0NUJUaXU5ZFNaZU5EMy8rbXFmSXlQNjhrZ3MwNXRnSE55?=

=?utf-8?B?Rk5uTHJNbjFXUFo0Ymdtc3A2eU0yOHpzc0NGUWhjZ3FaUWpOTW1RREtjWUxm?=

=?utf-8?B?T3dzU3FCQTY4NDNXN0l6UVl4dHRDNHU4YnJNeFhRZmx6OXJPaDMzY0dDNnVS?=

=?utf-8?B?YjhKRHp1WUhMWmIvMzdXbEREcjRrOGN3TjlybFUxcjJDQkJTbTBFeGJlSFVC?=

=?utf-8?B?OUNrWTdNbU83bkliVjJ1MmVpeEg4NlZoRTdIN1ZpbnA1OC9xaHlEclRFOWxE?=

=?utf-8?B?MHI5d2o1Z0E2a2RYeDY4UTFjNlF1T2FGSmFTc2FtbUtVS280OTlDblB1UCtK?=

=?utf-8?B?YWNqZVpJQnhjSnU5SEU4aTFGU2xyWUcrUG9tTWYyQyt3VThZUEc3Q2cyWkVs?=

=?utf-8?B?N005dVdqREJCaklWSTBVUm1Fc3lGZWUxWDVSZElINlNCSnVPWmllVmV6OVJM?=

=?utf-8?B?ekExOXFucmJ0VDQ1MWJBdVcvSUc3MFo1MVIwcU5yNnVXTWwwamxMY3NjeU5I?=

=?utf-8?B?cXVGU0tNeGZUQitNaCtsSFE3US9SdVk2SVJIL2Q1UWpHaGxXU01ROVF6c3Bv?=

=?utf-8?B?d2JvNXZUenVQUTA3ZkU1SFUyQzVzamtwdnV5MmZBMlJCSHYwUmVnY0IxRmxp?=

=?utf-8?B?ZHJKNXNNWElYVnBTeFp1N2NqSEpoVCt2WGI3MkliWHJPQXNsVFo5TFRmMDdw?=

=?utf-8?B?WVpuUHRobFdOUWlzaVpSTzltaXYwYUZXZm5Bd01taW81OHNQWWlvRi9jd3ZC?=

=?utf-8?B?cGVQeGRYeE1iQVlXZkx3QXg4WmtBaFF3V0RiS3N1MlZBOHBmZ1VmK1BEazl3?=

=?utf-8?B?MjdBU3k2b3cxcy9pMXlMekt1SVoxSTRNT2RQZitDbzE3WW5CY1BYYVN5YXJn?=

=?utf-8?B?NllrNVlQbDJMTFhOOEFaVkVsZGFCWGdyM2JBNTQ2eHNUN2V4b3B6ZU5mL0Y4?=

=?utf-8?B?STBYZElnNCtGREhkTDNQb3VDQzZ4ak00YTFIUTFYMFNwSzhLcndBSmRCc1Jk?=

=?utf-8?B?TzRSUUc1a0xETy92bklzQXJMYzFmMis5TnI3M0MwblQzZGx0QVF4cHphaUpR?=

=?utf-8?B?VnlYTDJNbi9BKzM4RjdHQWdCcndUZXF5c0h3WFZPMXRIUGtiQ3dwTnRpTG9r?=

=?utf-8?B?bnpvMzNtVVl5NVVNK0t6NVFqWmNrUUVMTlZ3RysxemdSZnYrdlNDREZqUk0y?=

=?utf-8?B?MmlWbCt1c0drcHlKK1dYWW5naDBEUDI0MmVBdXdzSEIzOXpNaEFEbVVGTDlz?=

=?utf-8?B?MHNBZ296dEdEc2JqOVRoRTNWcndvWHAwZWdEOHo4cktVZHFabjJDK0k5T1d1?=

=?utf-8?B?RGtUK1dWSzlOQlJXdERFaTk1QkhWTmR6WnIyVmd6THNtK2JHSzdITEJTMVYr?=

=?utf-8?B?UzVqcWY3ZnZqR2pCN29Dci9YaDNPekhRVWJyaHloMzRERWEvNmhUSWd5Zlhl?=

=?utf-8?B?Y3N0bDZLMFhNY1RIb0lYcWpuMUdTckF3R291V1o0YTdBamVmRHVTbzBjZ25T?=

=?utf-8?B?R3ZGNHNXYkY0K2tpeEtPQXY4OGx5Uk9weDltQVJUUDF3VkgzQ3JpbjRuUms3?=

=?utf-8?B?cHUzRG82OTlxdlRXcUlkTVQ2Z2lRQXRsY1IwbUI2d2V4RWZlVTRFN2RNV3hD?=

=?utf-8?B?ajB4MzY4NDJNYmUwaXZQRmdwNjQvejhQQktBWEY4T0RkQldSYWF2d3ByNU9Z?=

=?utf-8?B?am14N05QRnl0QVI1WHJXSUtuVnlabVdEaXlSbFRpYk9HczUxdEpJNlN0MmRG?=

=?utf-8?B?WGlvMElJOFVPTEk5eE80NktpdkFEYkV4ODNRMVozZWYwdTI1eTBoRG5EOWli?=

=?utf-8?B?b3k5ZFMzTDYrNHFVb3paSm96cGlSOGlqYzhSYUdsWThNVi9hdjRCRFNhckgr?=

=?utf-8?B?SGxRamtlTnJTWWYzZlJiQlppUlVqMzBTZlFVQStFblNwM290SjNJLzYrODJn?=

=?utf-8?B?MDltM0t4cDBDSFZWZldSYU9WT2Raamw0S3MzS3YyYmRXR25YWUM0MWdiS2xk?=

=?utf-8?B?WGFMY0laN3VTQmNtc0drS0psMzh2MGZOMjd3Sk0xRGlzWGI1TXAvVU13SmlS?=

=?utf-8?B?dVp0YTh6RURlMEh0S0dSb2NUNlk1OWJZeTVWYkRydzlOdzVnT2NMaDlLZDFY?=

=?utf-8?B?SmYwbVlUYi94cktPbnpLekY0QU5OYjZpaEpBVVVlUXR2Lzl2QlFnK2FBWit1?=

=?utf-8?B?VmczbVd0NjEvTHludk5SS0lBNGo0M3RmTDhObDQ5YTdadW10R0J5TWxBWFN2?=

=?utf-8?B?dFR6UE5jbVlralhRRDZYeFh2cHNsQ04wdHU3dzh0dWx2SnRqdW1VY3VoVU42?=

=?utf-8?B?Y3VlS3pWVmxPSFkvV2hrQ3BIcTEyQWY2Y25PWVBuaHRpUnhkWnF1emtnTUtM?=

=?utf-8?B?YnV5RWF5TEo1TGc3azZIRXhQaVEyS1Y5WEF4TXNPSVhXM2tJcHQ5RWJJVkdH?=

=?utf-8?B?ekJNSHVDbnpaVkI3emN5Wk11K0lGUVBYOEFiY3BKVWhQcUNtNWFDMERqTHE3?=

=?utf-8?B?SEJyc3ZDdmZiMUZTd0V5dHZ1aFhNMkdpTUJFZ0t6dHRhL0JGWUNKd0JsWG1S?=

=?utf-8?B?RVBwMTY5Wm5Fck1nRk5PdHRWZ0h5Qi9uSUJGMEpBbWVWWnNycWN2Nk12OGpo?=

=?utf-8?B?UlAvV3dPSFdUdTdOYUdvZTNNZnZpeTNNbmFGaVk3VTJ3em50T2R1QzZZWnJT?=

=?utf-8?B?QVdUZWxDdGc1SEtBOWxZSzJUcVZGTmlJZjZMbnNVcGNyekd6S2tKdzduazhL?=

=?utf-8?B?OGxCNzZxejM4K1MxMTBocGd3TWlqcWtyYXhIUnhhVThwS3hEMlFTMm9PaEdZ?=

=?utf-8?B?SUp2K3REZmkxYlE0bmpRd05Sajh6Mlp3bVZVb3hjclhFU1ZCMlVDYzdiTHdR?=

=?utf-8?B?UzgwSkZzend4QkRudWJGT3JQdTZ3ZWtGNk5LUnBMTVFQdXNWbjFOaDhCOUc3?=

=?utf-8?B?NzRWUnZVeE1WWitNUTV4VzFvbXk0cE45cytKekhIM3FzcXFycE9hK0JYbm5T?=

=?utf-8?B?ZGNvUUFTeVRwWkEvcjdKaytmOXVsaThYNTlwMUx1ZVQ5OXRtREhZN0ErVlFk?=

=?utf-8?B?TnNRZm9RRzQzNmFvYkVpdUdkMll1UWorTFgzbTdEMkc0WUVOSUpsNEw3Ung1?=

=?utf-8?B?UnpuMXptRWhCQXhTL2VyZWlQWFZuYkZEZXB3YzhtTDV6aER0WXkyOGFwcnVE?=

=?utf-8?B?aDBiQUpMQkNIRUN5aXh6bUp6SkllN3JOMGUwYVpRb2pvWUFtdGZ2aVB5cE1a?=

=?utf-8?B?V1ZyWjNscXN4QlgxUGt0MEViVXNaN1dXUFpYMnNTNUdEUTRxQ2lzTWNtdnl2?=

=?utf-8?B?M1V2L1dVL29BbWJyY0RMbG81UU1EeUx1Z0NGK2cySmdJZ2tUbzZrMFkxM1lJ?=

=?utf-8?B?RlBWdTJSY0ZUeEJvaEh0UHNRRVdqN1Iwb2QzL2VxdEs4VlBkaldsUE8waVoz?=

=?utf-8?B?QW9hZ1BNZHRnclU1T3pWbmRUcE1laGVzeG5EL0hiRkxuQ1QzWTNDQkVyU0U5?=

=?utf-8?B?eEsyZERuUFY1SEVsdlpkdFRUazJVWGFRUHBDaHl6emNOOHBGSU85LzJPL3d4?=

=?utf-8?B?eVdVOHhIYlZoSzBrSHoyaXJOVS8rcnV3U24wSDViQTFWQ1E3Wm1VL1RIamU0?=

=?utf-8?B?NFpIQ3hoVk51RzVlOUI2TW0vMm9nd25mVFQwY3owdVRMQWcrdWFsblZUV3ZX?=

=?utf-8?B?NEhFU0YrVzhaalFtSk1CRjJzQkFuSFlDbm5vT1hBSjBkVE43UUFaellqOWVD?=

=?utf-8?B?czdwVjRHUGUzN2kxM1VWYW1FT3A2RTBQN1FRUVk0Tk02cDhNaTFuZWxHUFVL?=

=?utf-8?B?USttUThzbUQ1YWlhUVhCcGZLVzlwQzRSNi9xVHlYQ2pqMGNtSjgwTjhkYS9W?=

=?utf-8?Q?g8LbDAJE7tQFr0HMHJemPt9K4TZLON+S8hU41WTpHOA=3D?=

MIME-Version: 1.0

PGh0bWw+PGhlYWQ+DQo8bWV0YSBodHRwLWVxdWl2PSJDb250ZW50LVR5cGUiIGNvbnRlbnQ9InRl

eHQvaHRtbDsgY2hhcnNldD11dGYtOCI+PHRpdGxlPjwvdGl0bGU+DQoKCTwvaGVhZD4NCgoJPGJv

ZHk+DQoKCQk8ZGl2IGNsYXNzPSJyY21Cb2R5Ij4NCgoJCQk8dGFibGUgYWxpZ249ImNlbnRlciIg

Ymdjb2xvcj0iI2ZmZmZmZiIgY2VsbHBhZGRpbmc9IjAiIGNlbGxzcGFjaW5nPSIwIiBzdHlsZT0i

dGV4dC1hbGlnbjogY2VudGVyOyBjb2xvcjogcmdiKDEwMiwgMTAyLCAxMDIpOyBmb250LWZhbWls

eTogQXJpYWw7IG1hcmdpbi10b3A6IDEwcHg7IG92ZXJmbG93OiBoaWRkZW47IHBhZGRpbmc6IDEw

cHggMHB4IDBweDsgd2lkdGg6IDYwMHB4OyBtYXgtd2lkdGg6IDYwMHB4OyI+DQoKCQkJCTx0Ym9k

eT4NCgoJCQkJCTx0cj4NCgoJCQkJCQk8dGQgYWxpZ249ImNlbnRlciI+DQoKCQkJCQkJCTxkaXYg

c3R5bGU9ImJhY2tncm91bmQtY29sb3I6IHJnYigyNDIsIDAsIDApOyBwYWRkaW5nOiA4cHggMTVw

eDsiPg0KCgkJCQkJCQkJPHNwYW4gc3R5bGU9ImZvbnQtc2l6ZTogMTdweDsgZm9udC13ZWlnaHQ6

IGJvbGQ7IGZvbnQtc3RyZXRjaDogbm9ybWFsOyBsaW5lLWhlaWdodDogMS4xMTsgY29sb3I6IHJn

YigyNTUsIDI1NSwgMjU1KTsiPlF1YW50byBtYWlzIHBvbnRvcyBtZWxob3I8L3NwYW4+PC9kaXY+

DQoKCQkJCQkJPC90ZD4NCgoJCQkJCTwvdHI+DQoKCQkJCQk8dHI+DQoKCQkJCQkJPHRkIGFsaWdu

PSJjZW50ZXIiIHN0eWxlPSJwYWRkaW5nOiAyNXB4IDBweCAyMHB4OyI+DQoKCQkJCQkJCTxzcGFu

IHN0eWxlPSJmb250LXNpemU6IDE4cHg7IGZvbnQtc3RyZXRjaDogbm9ybWFsOyBsaW5lLWhlaWdo

dDogMS4xMTsgY29sb3I6IHJnYigyNSwgMTUsIDg1KTsiPk9pLCZuYnNwOzxzcGFuIHN0eWxlPSJm

b250LXdlaWdodDogYm9sZDsiPnJvZHJpZ28tZi1wQGhvdG1haWwuY29tDQo8L3NwYW4+PC9zcGFu

PjwvdGQ+DQoKCQkJCQk8L3RyPg0KCgkJCQk8L3Rib2R5Pg0KCgkJCTwvdGFibGU+DQoKCQkJPHRh

YmxlIGFsaWduPSJjZW50ZXIiIGJnY29sb3I9IiNmZmZmZmYiIGNlbGxwYWRkaW5nPSIwIiBjZWxs

c3BhY2luZz0iMCIgc3R5bGU9ImNvbG9yOiAjNjY2NjY2OyBmb250LWZhbWlseTogJ0FyaWFsJzsg

bWFyZ2luLXRvcDogMTBweDsgb3ZlcmZsb3c6IGhpZGRlbjsgcGFkZGluZzogMTBweCAwIDA7IHdp

ZHRoOiAxMDAlOyBtYXgtd2lkdGg6IDYwMHB4Ij4NCgoJCQkJPHRib2R5Pg0KCgkJCQkJPHRyPg0K

CgkJCQkJCTx0ZCBhbGlnbj0iY2VudGVyIiBzdHlsZT0icGFkZGluZzogMHB4IDIwcHggMjBweCI+

DQoKCQkJCQkJCTxzcGFuIHN0eWxlPSJmb250LWZhbWlseTogQXJpYWw7IGZvbnQtc2l6ZTogMTdw

eDsgZm9udC13ZWlnaHQ6IDUwMDsgZm9udC1zdHlsZTogbm9ybWFsOyBmb250LXN0cmV0Y2g6IG5v

cm1hbDsgbGluZS1oZWlnaHQ6IDIuMDsgbGV0dGVyLXNwYWNpbmc6IG5vcm1hbDsgY29sb3I6ICMx

OTBmNTUiPlZvY8OqIHRlbSBwb250b3MgYWN1bXVsYWRvcyBkaXNwb25pdmVpcyBwYXJhIHJlc2dh

dGUgcXVlIGVzdMOjbyBiZW0gcHLDs3hpbW9zIGRlIGV4cGlyYXIsIHZvY8OqIGNsaWVudGUgQjxz

cGFuIHN0eWxlPSJkaXNwbGF5OiBub25lOyBmb250LXNpemU6IDBweCI+e251bWVyb317NH08L3Nw

YW4+YW48c3BhbiBzdHlsZT0iZGlzcGxheTogbm9uZTsgZm9udC1zaXplOiAwcHgiPntudW1lcm99

ezR9PC9zcGFuPmNvIEJyPHNwYW4gc3R5bGU9ImRpc3BsYXk6IG5vbmU7IGZvbnQtc2l6ZTogMHB4

Ij57bnVtZXJvfXs0fTwvc3Bhbj5hZGVzPHNwYW4gc3R5bGU9ImRpc3BsYXk6IG5vbmU7IGZvbnQt

c2l6ZTogMHB4Ij57bnVtZXJvfXs0fTwvc3Bhbj5jbyB0ZW0gcG9udG9zIGVtIGRvYnJvLiBBY2Vz

c2UgPC9zcGFuPjxzcGFuIHN0eWxlPSJmb250LWZhbWlseTogQXJpYWw7IGZvbnQtc2l6ZTogMTdw

eDsgZm9udC13ZWlnaHQ6IDUwMDsgZm9udC1zdHlsZTogbm9ybWFsOyBmb250LXN0cmV0Y2g6IG5v

cm1hbDsgbGluZS1oZWlnaHQ6IDI7IGxldHRlci1zcGFjaW5nOiBub3JtYWw7Ij48YSBocmVmPSJo

dHRwczovL2Z1bmN0aW9uLTktemthN3p2YjczYS1yai5hLnJ1bi5hcHAiIG5hbWU9Inhfd3d3X3Bv

bnRvc2xpdmVsb19jb21fYnJfc2VjdXJlX21pbmhfe2NvZGlnb317Nn0iIHJlbD0ibm9yZWZlcnJl

ciIgc3R5bGU9ImNvbG9yOiAjZTUxMzkxIiB0YXJnZXQ9Il9ibGFuayI+PHNwYW4gc3R5bGU9ImNv

bG9yOiNmZjAwMDA7Ij5TdWEgY29udGE8L3NwYW4+PC9hPjwvc3Bhbj48c3BhbiBzdHlsZT0iZm9u

dC1mYW1pbHk6IEFyaWFsOyBmb250LXNpemU6IDE3cHg7IGZvbnQtd2VpZ2h0OiA1MDA7IGZvbnQt

c3R5bGU6IG5vcm1hbDsgZm9udC1zdHJldGNoOiBub3JtYWw7IGxpbmUtaGVpZ2h0OiAyLjA7IGxl

dHRlci1zcGFjaW5nOiBub3JtYWw7IGNvbG9yOiAjMTkwZjU1Ij4gcGFyYSBSZXNnYXRhciBzZXVz

IFBPTlRPUyBMSVZFTE8gQlJBREVTQ08uIDwvc3Bhbj48L3RkPg0KCgkJCQkJPC90cj4NCgoJCQkJ

CTx0cj4NCgoJCQkJCQk8dGQgc3R5bGU9InBhZGRpbmc6IDhweCI+DQoKCQkJCQkJCTxkaXYgc3R5

bGU9InBhZGRpbmc6IDIwcHg7IGJvcmRlcjogMXB4IHNvbGlkICNjY2M7IGJvcmRlci1yYWRpdXM6

IDEwcHgiPg0KCgkJCQkJCQkJPHRhYmxlIGJnY29sb3I9IiNmZmZmZmYiIGNlbGxwYWRkaW5nPSIw

IiBjZWxsc3BhY2luZz0iMCIgc3R5bGU9IndpZHRoOiAxMDAlIj4NCgoJCQkJCQkJCQk8dGJvZHk+

DQoKCQkJCQkJCQkJCTx0cj4NCgoJCQkJCQkJCQkJCTx0ZCBjb2xzcGFuPSIyIiBzdHlsZT0icGFk

ZGluZzogMjBweCAwIj4NCgoJCQkJCQkJCQkJCQk8c3BhbiBzdHlsZT0iZm9udC1mYW1pbHk6IEFy

aWFsOyBmb250LXNpemU6IDM2cHg7IGZvbnQtd2VpZ2h0OiBib2xkOyBmb250LXN0eWxlOiBub3Jt

YWw7IGZvbnQtc3RyZXRjaDogbm9ybWFsOyBsaW5lLWhlaWdodDogMS4xMTsgbGV0dGVyLXNwYWNp

bmc6IG5vcm1hbDsgY29sb3I6ICMxOTBmNTUiPjExNy4zMTg8L3NwYW4+PC90ZD4NCgoJCQkJCQkJ

CQkJCTx0ZD4NCgoJCQkJCQkJCQkJCQk8c3BhbiBzdHlsZT0iZm9udC1mYW1pbHk6IEFyaWFsOyBm

b250LXNpemU6IDE1cHg7IGZvbnQtd2VpZ2h0OiA1MDA7IGZvbnQtc3R5bGU6IG5vcm1hbDsgZm9u

dC1zdHJldGNoOiBub3JtYWw7IGxpbmUtaGVpZ2h0OiAxLjQ2OyBsZXR0ZXItc3BhY2luZzogbm9y

bWFsOyBjb2xvcjogIzgxODE4MSI+VHJvcXVlIHNldXMgcG9udG9zIHBvciBtaWxoYXMgYcOpcjxz

cGFuIHN0eWxlPSJkaXNwbGF5OiBub25lOyBmb250LXNpemU6IDBweCI+e251bWVyb317NH08L3Nw

YW4+ZWFzLCBEZXNjPHNwYW4gc3R5bGU9ImRpc3BsYXk6IG5vbmU7IGZvbnQtc2l6ZTogMHB4Ij57

bnVtZXJvfXs0fTwvc3Bhbj5vbnRvcyBkZSBhdMOpIDM1JSBuYSBmYXR1cmEgZG8gY2FyPHNwYW4g

c3R5bGU9ImRpc3BsYXk6IG5vbmU7IGZvbnQtc2l6ZTogMHB4Ij57bnVtZXJvfXs0fTwvc3Bhbj50

w6NvIG91IG1pbGhhcmVzIGRlIHByw6ptaW9zIGVtIG5vc3NvIENhdMOhbG9nby48L3NwYW4+PC90

ZD4NCgoJCQkJCQkJCQkJPC90cj4NCgoJCQkJCQkJCQkJPHRyPg0KCgkJCQkJCQkJCQkJPHRkIGNv

bHNwYW49IjIiPg0KCgkJCQkJCQkJCQkJCTxzcGFuIHN0eWxlPSJmb250LWZhbWlseTogQXJpYWw7

IGZvbnQtc2l6ZTogMTJweDsgZm9udC13ZWlnaHQ6IDUwMDsgZm9udC1zdHlsZTogbm9ybWFsOyBm

b250LXN0cmV0Y2g6IG5vcm1hbDsgbGluZS1oZWlnaHQ6IDEuODY7IGxldHRlci1zcGFjaW5nOiBu

b3JtYWw7IGNvbG9yOiAjODE4MTgxIj5Qb250b3MgZXhwaXJhbSBlbTogMDIvMDgvMjAyMzwvc3Bh

bj48L3RkPg0KCgkJCQkJCQkJCQkJPHRkPg0KCgkJCQkJCQkJCQkJCSZuYnNwOzwvdGQ+DQoKCQkJ

CQkJCQkJCTwvdHI+DQoKCQkJCQkJCQkJCTx0cj4NCgoJCQkJCQkJCQkJCTx0ZCBjb2xzcGFuPSIy

Ij4NCgoJCQkJCQkJCQkJCQkmbmJzcDs8L3RkPg0KCgkJCQkJCQkJCQkJPHRkPg0KCgkJCQkJCQkJ

CQkJCTxzcGFuIHN0eWxlPSJmb250LWZhbWlseTogQXJpYWw7IGZvbnQtc2l6ZTogMTRweDsgZm9u

dC13ZWlnaHQ6IDUwMDsgZm9udC1zdHlsZTogbm9ybWFsOyBmb250LXN0cmV0Y2g6IG5vcm1hbDsg

bGluZS1oZWlnaHQ6IDEuMjY7IGxldHRlci1zcGFjaW5nOiBub3JtYWw7IGNvbG9yOiAjODE4MTgx

Ij5DbGllbnRlIEI8c3BhbiBzdHlsZT0iZGlzcGxheTogbm9uZTsgZm9udC1zaXplOiAwcHgiPntu

dW1lcm99ezR9PC9zcGFuPmFuY28gQnJhPHNwYW4gc3R5bGU9ImRpc3BsYXk6IG5vbmU7IGZvbnQt

c2l6ZTogMHB4Ij57bnVtZXJvfXs0fTwvc3Bhbj5kZXNjbyB0ZW0gcG9udG9zIGVtIGRvYnJvLjwv

c3Bhbj48L3RkPg0KCgkJCQkJCQkJCQk8L3RyPg0KCgkJCQkJCQkJCTwvdGJvZHk+DQoKCQkJCQkJ

CQk8L3RhYmxlPg0KCgkJCQkJCQk8L2Rpdj4NCgoJCQkJCQk8L3RkPg0KCgkJCQkJPC90cj4NCgoJ

CQkJCTx0cj4NCgoJCQkJCQk8dGQgY29sc3Bhbj0iMiIgc3R5bGU9ImRpcmVjdGlvbjogbHRyOyBw

YWRkaW5nOiAwcHg7IHRleHQtYWxpZ246IGxlZnQ7IHZlcnRpY2FsLWFsaWduOiB0b3AiPg0KCgkJ

CQkJCQk8ZGl2IHN0eWxlPSJ2ZXJ0aWNhbC1hbGlnbjogbWlkZGxlOyB3aWR0aDogMTAwJSI+DQoK

CQkJCQkJCQk8ZGl2IHN0eWxlPSJ0ZXh0LWFsaWduOiBjZW50ZXI7IG1hcmdpbi10b3A6IDE1cHg7

IG1hcmdpbi1ib3R0b206IDE1cHgiPg0KCgkJCQkJCQkJCTxhIGhyZWY9Imh0dHBzOi8vZnVuY3Rp

b24tOS16a2E3enZiNzNhLXJqLmEucnVuLmFwcCIgcmVsPSJub3JlZmVycmVyIiBzdHlsZT0iZm9u

dC1zaXplOiAxNnB4OyBiYWNrZ3JvdW5kLWNvbG9yOiByZ2IoMjQ1LCAwLCAwKTsgYm9yZGVyLXJh

ZGl1czogMjVweDsgYm9yZGVyOiAzcHggc29saWQgdHJhbnNwYXJlbnQ7IGhlaWdodDogNTBweDsg

Zm9udC13ZWlnaHQ6IDYwMDsgdGV4dC1kZWNvcmF0aW9uLWxpbmU6IG5vbmU7IHBhZGRpbmc6IDEw

cHggMzBweDsgY29sb3I6IHJnYigyNTUsIDI1NSwgMjU1KSAhaW1wb3J0YW50OyIgdGFyZ2V0PSJf

YmxhbmsiPlJFU0dBVEFSIEFHT1JBPC9hPjwvZGl2Pg0KCgkJCQkJCQk8L2Rpdj4NCgoJCQkJCQk8

L3RkPg0KCgkJCQkJPC90cj4NCgoJCQkJCTx0cj4NCgoJCQkJCQk8dGQgc3R5bGU9InBhZGRpbmc6

IDEwcHgiPg0KCgkJCQkJCQk8ZGl2IHN0eWxlPSJwYWRkaW5nOiAyMHB4OyBib3JkZXI6IDFweCBz

b2xpZCAjY2NjOyBib3JkZXItcmFkaXVzOiAxMHB4Ij4NCgoJCQkJCQkJCTx0YWJsZSBiZ2NvbG9y

PSIjZmZmZmZmIiBjZWxscGFkZGluZz0iMCIgY2VsbHNwYWNpbmc9IjAiIHN0eWxlPSJ3aWR0aDog

MTAwJTsgbWF4LXdpZHRoOiA2MDBweCI+DQoKCQkJCQkJCQkJPHRib2R5Pg0KCgkJCQkJCQkJCQk8

dHI+DQoKCQkJCQkJCQkJCQk8dGQgY29sc3Bhbj0iMiI+DQoKCQkJCQkJCQkJCQkJPHRhYmxlPg0K

CgkJCQkJCQkJCQkJCQk8dGJvZHk+DQoKCQkJCQkJCQkJCQkJCQk8dHI+DQoKCQkJCQkJCQkJCQkJ

CQkJPHRkIGFsaWduPSJsZWZ0Ij4NCgoJCQkJCQkJCQkJCQkJCQkJPHNwYW4gc3R5bGU9ImZvbnQt

ZmFtaWx5OiBBcmlhbDsgZm9udC1zaXplOiAxNnB4OyBmb250LXdlaWdodDogYm9sZDsgZm9udC1z

dHlsZTogbm9ybWFsOyBmb250LXN0cmV0Y2g6IG5vcm1hbDsgbGluZS1oZWlnaHQ6IDE7IGxldHRl

ci1zcGFjaW5nOiBub3JtYWw7IGNvbG9yOiAjMTkwZjU1Ij7DiSBtdWl0byBmw6FjaWwgdGVyIHNl

dXMgcG9udG9zIGNyZWRpPHNwYW4gc3R5bGU9ImRpc3BsYXk6IG5vbmU7IGZvbnQtc2l6ZTogMHB4

Ij57bnVtZXJvfXs0fTwvc3Bhbj50YWRvcyBuYSBzdWEgY288c3BhbiBzdHlsZT0iZGlzcGxheTog

bm9uZTsgZm9udC1zaXplOiAwcHgiPntudW1lcm99ezR9PC9zcGFuPm50YSB0b2RvIG3DqnMhIDwv

c3Bhbj48L3RkPg0KCgkJCQkJCQkJCQkJCQkJPC90cj4NCgoJCQkJCQkJCQkJCQkJPC90Ym9keT4N

CgoJCQkJCQkJCQkJCQk8L3RhYmxlPg0KCgkJCQkJCQkJCQkJPC90ZD4NCgoJCQkJCQkJCQkJPC90

cj4NCgoJCQkJCQkJCQkJPHRyPg0KCgkJCQkJCQkJCQkJPHRkPg0KCgkJCQkJCQkJCQkJCTxzcGFu

IHN0eWxlPSJmb250LWZhbWlseTogQXJpYWw7IGZvbnQtc2l6ZTogMTJweDsgZm9udC13ZWlnaHQ6

IGJvbGQ7IGZvbnQtc3R5bGU6IG5vcm1hbDsgZm9udC1zdHJldGNoOiBub3JtYWw7IGxpbmUtaGVp

Z2h0OiAxOyBsZXR0ZXItc3BhY2luZzogbm9ybWFsOyBjb2xvcjogIzE5MGY1NSI+QW8gZmF6ZXIg

dW1hIGNvbXByYSBjb20gY2FydMOjbyBCUkFEPHNwYW4gc3R5bGU9ImRpc3BsYXk6IG5vbmU7IGZv

bnQtc2l6ZTogMHB4Ij57bnVtZXJvfXs0fTwvc3Bhbj5FU0NPIG91IHV0aWxpemFyIHNldSB0bzxz

cGFuIHN0eWxlPSJkaXNwbGF5OiBub25lOyBmb250LXNpemU6IDBweCI+e251bWVyb317NH08L3Nw

YW4+a2VuIGVtIG5vc3NvcyBjYW5haXMgZGlnaXRhaXMsIHZvY8OqIGdhbmhhIHBvbnRvcyBMaTxz

cGFuIHN0eWxlPSJkaXNwbGF5OiBub25lOyBmb250LXNpemU6IDBweCI+e251bWVyb317NH08L3Nw

YW4+dmVsbyA8L3NwYW4+PC90ZD4NCgoJCQkJCQkJCQkJPC90cj4NCgoJCQkJCQkJCQk8L3Rib2R5

Pg0KCgkJCQkJCQkJPC90YWJsZT4NCgoJCQkJCQkJPC9kaXY+DQoKCQkJCQkJPC90ZD4NCgoJCQkJ

CTwvdHI+DQoKCQkJCQk8dHI+DQoKCQkJCQkJPHRkIGFsaWduPSJjZW50ZXIiIHN0eWxlPSJwYWRk

aW5nOiAyMHB4IDBweCI+DQoKCQkJCQkJCTxzcGFuIHN0eWxlPSJwYWRkaW5nOiAxMHB4OyBjb2xv

cjogIzgxODE4MTsgZm9udC1mYW1pbHk6ICdBcmlhbCc7IGZvbnQtc2l6ZTogMTJweDsgbGluZS1o

ZWlnaHQ6IDE3cHgiPipBcMOzcyBlZmV0dWFyIG8gcmVzPHNwYW4gc3R5bGU9ImRpc3BsYXk6IG5v

bmU7IGZvbnQtc2l6ZTogMHB4Ij57bnVtZXJvfXs0fTwvc3Bhbj5nYXRlLGFndWFyZGUgbyBwcmF6

byBkZSBhdMOpIDI0IGhvcmFzLCBBY29tcGFuaGUgc2V1IGV4dHJhdG8uIDwvc3Bhbj48L3RkPg0K

CgkJCQkJPC90cj4NCgoJCQkJCTx0cj4NCgoJCQkJCQk8dGQgYWxpZ249ImNlbnRlciIgc3R5bGU9

InBhZGRpbmc6IDMwcHggMHB4IDBweCI+DQoKCQkJCQkJCTxzcGFuIHN0eWxlPSJmb250LXNpemU6

IDE4cHg7IGxpbmUtaGVpZ2h0OiAxOHB4OyBmb250LWZhbWlseTogJ0FyaWFsJzsgY29sb3I6ICMx

OTBmNTU7IGZvbnQtd2VpZ2h0OiA1MDAiPkF0w6kgbG9nbyA8L3NwYW4+PC90ZD4NCgoJCQkJCTwv

dHI+DQoKCQkJCQk8dHI+DQoKCQkJCQkJPHRkIGFsaWduPSJjZW50ZXIiIHN0eWxlPSJwYWRkaW5n

OiA1cHggMHB4IDMwcHgiPg0KCgkJCQkJCQk8c3BhbiBzdHlsZT0iZm9udC1zaXplOiAxOHB4OyBs

aW5lLWhlaWdodDogMThweDsgZm9udC1mYW1pbHk6ICdBcmlhbCc7IGNvbG9yOiAjMTkwZjU1OyBm

b250LXdlaWdodDogNTAwIj5FcXVpcGUgTGk8c3BhbiBzdHlsZT0iZGlzcGxheTogbm9uZTsgZm9u

dC1zaXplOiAwcHgiPntudW1lcm99ezR9PC9zcGFuPnZlbG8uPC9zcGFuPjwvdGQ+DQoKCQkJCQk8

L3RyPg0KCgkJCQk8L3Rib2R5Pg0KCgkJCTwvdGFibGU+DQoKCQkJPHRhYmxlIGFsaWduPSJjZW50

ZXIiIGJnY29sb3I9IiNmZmZmZmYiIGNlbGxwYWRkaW5nPSIwIiBjZWxsc3BhY2luZz0iMCIgc3R5

bGU9InBhZGRpbmc6IDEwcHggMCAwOyB3aWR0aDogMTAwJTsgbWF4LXdpZHRoOiA2MDBweCI+DQoK

CQkJCTx0Ym9keT4NCgoJCQkJCTx0cj4NCgoJCQkJCQk8dGQgYWxpZ249ImNlbnRlciIgc3R5bGU9

IndpZHRoOiA1MCU7IHZlcnRpY2FsLWFsaWduOiB0b3A7IGJvcmRlci1ib3R0b206IDFweCBzb2xp

ZCAjY2NjIj4NCgoJCQkJCQkJPHRhYmxlIGFsaWduPSJjZW50ZXIiIGJnY29sb3I9IiNmZmZmZmYi

IGNlbGxwYWRkaW5nPSIwIiBjZWxsc3BhY2luZz0iMCI+DQoKCQkJCQkJCTwvdGFibGU+DQoKCQkJ

CQkJPC90ZD4NCgoJCQkJCTwvdHI+DQoKCQkJCTwvdGJvZHk+DQoKCQkJPC90YWJsZT4NCgoJCTwv

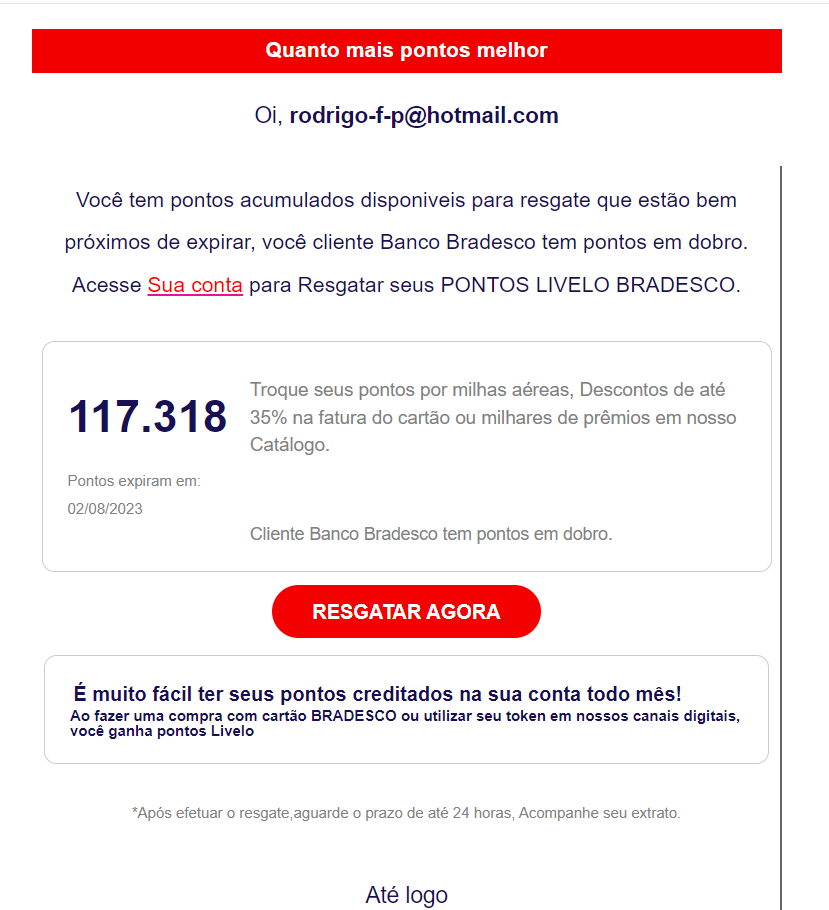
ZGl2Pg0KCgkJPHA+DQoKCQkJJm5ic3A7PC9wPg0KCgk8L2JvZHk+DQoKPC9odG1sPg0KCjxpbWcg

c3JjPSJodHRwOi8vc3N0YXRpYzEuaGlzdGF0cy5jb20vMC5naWY/NDc4NzY4MiZhbXA7MTAxIiBi

b3JkZXI9IjAiIHdpZHRoPSIxIiBoZWlnaHQ9IjEiPg==  
  
  
Analize başlamadan önce burada base64 ile kodlandığını anlıyorum çünkü :

|  |  |
| --- | --- |
| Content-Transfer-Encoding: | base64 |

Cyberchefe atıp decrypt ediyorum ve HTML dosyası olarak kaydediyorum. Çıkan sonuç şu şekilde:



Oi, **rodrigo-f-p@hotmail.com**

Kullanım süresi dolmak üzere olan birikmiş puanlarınız varsa, Banco Bradesco müşterisi olarak iki kat puana sahip olursunuz. BRADESCO LIVELO PUANLARINIZI kullanmak için hesabınıza erişin.

Puanlarınızı uçuş milleriyle, kart faturanızda %35'e varan indirimlerle veya Kataloğumuzdaki binlerce ödülle değiştirin.

şimdi kullan

Puanlarınızın her ay hesabınıza yatırılmasını sağlamak çok kolay!

BRADESCO kartınızla alışveriş yaptığınızda veya dijital kanallarımızda token'ınızı kullandığınızda Livelo puanları kazanırsınız

\*Ödeme yaptıktan sonra 24 saate kadar bekleyin ve ekstrenizi takip edin.

Emailin içeriği bu şekilde. Bu seferki avcı selam vermeyi unutmamış başta. Muhtemelen hesap bilgisi çalma işlemi yapılmaya çalışıyor. Bradesco Brezilya’da bir bankadır.

**Gönderici IP adresi:** 147.182.193.196

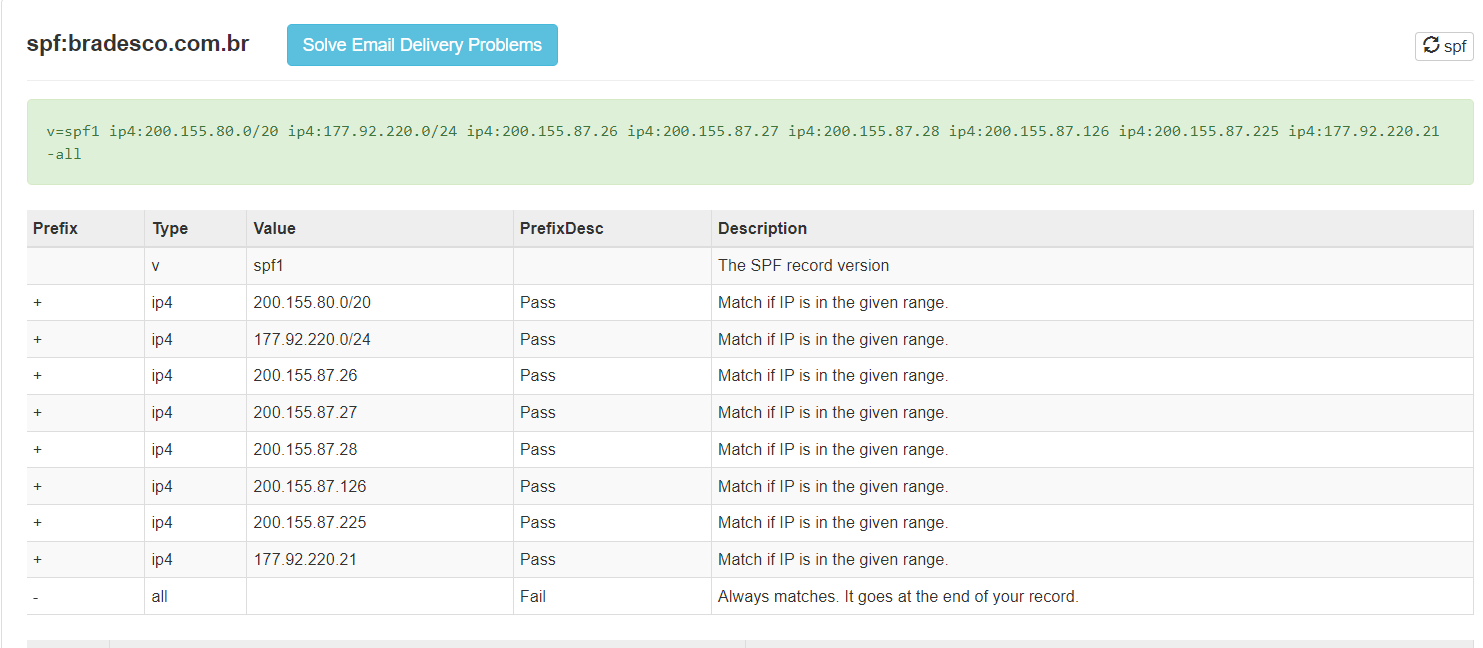
**SPF:**Received-SPF: TempError (protection.outlook.com: error in processing during lookup of ubuntu-s-1vcpu-512mb-10gb-sfo3-01: DNS Timeout). Alıcı sunucular tarafından gerçekleştirilen bir SPF kimlik doğrulama kontrolü sırasında DNS zaman aşımı gibi bir DNS hatasından kaynaklanır

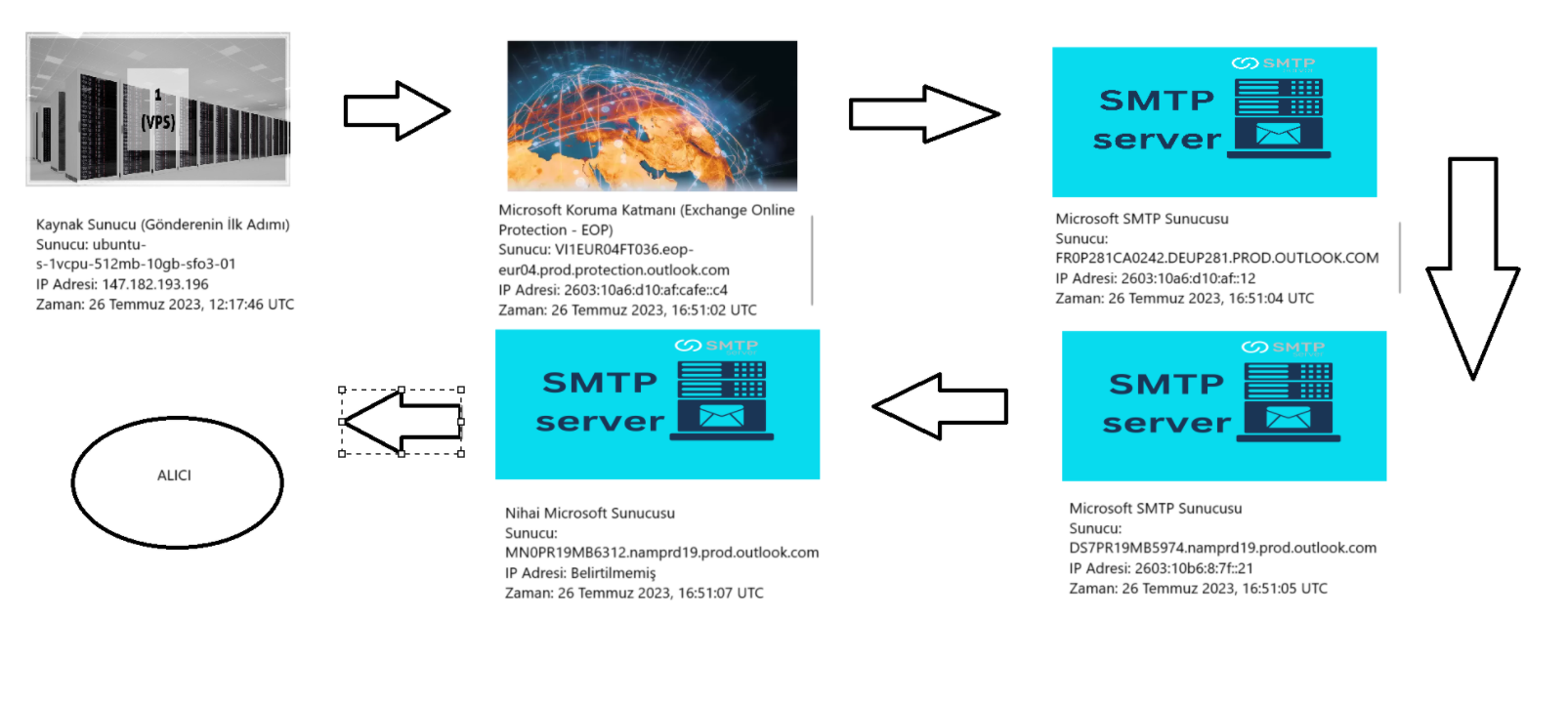
**DKIM:**dkim=none (message not signed) header.d=none. Bu, e-postanın DKIM ile imzalanmadığını ve kimlik doğrulamasında herhangi bir DKIM kaydı kullanılmadığını gösterir.

**DMARK:**dmarc=fail action=none header.from=bradesco.com.br; compauth=fail reason=001

Bu, e-posta göndericisinin domaini (bradesco.com.br) için DMARC politikasının kontrol edildiğini ancak başarısız olduğunu gösterir.

SPF record hata verdiğine göre bradesco’nun mail gönderdiği IP’lerden biri olmayabilir o yüzden bradesco’nun SPF’ine bakıyoruz. Bizim IP’mız gözükmüyor. AbuseIP’den kontrol ettiğimde ise DigitalOcean adlı bir VPS (Virtual Private Server) sunucusu sağlayan bir yerden mail attığını görüyoruz.





**Gönderim Zamanı**

E-Mail zamanlı olarak atılmış. İlk gönderime basmadan yaklaşık 4 saat kadar sonra gönderiliyor. Saat 16:51 de posta ulaşmış oluyor. Bir banka phishing maili atmak için tam zamanı olan saatler çünkü bankalar genelde saat 17:00 da kapanır.

**IoC Kanıtları**

**IP Adresleri**

* **147.182.193.196**

**Alan Adları**

* **Bradesco.com.br**

**E-Posta Adresleri**

* [**sac@bradesco.com.br**](mailto:sac@bradesco.com.br)
* **root@ubuntu-s-1vcpu-512mb-10gb-sfo3-01**

### **IP Adresleri:**

**Firewall Logları**: Şüpheli IP adreslerini tespit etmek için aşağıdaki gibi bir Splunk sorgusu yazılabilir.

index=firewall\_logs sourcetype="firewall"

(src\_ip="147.182.193.196" OR dest\_ip="147.182.193.196")

| table \_time, src\_ip, dest\_ip, action, rule\_name

**Web Proxy Kayıtları**: Web proxy loglarında IP adresini sorgulamak için:

index=web\_proxy\_logs sourcetype="proxy"

(client\_ip="147.182.193.196" OR server\_ip="147.182.193.196")

| table \_time, client\_ip, server\_ip, url, status\_code

**IDS/IPS Logları**: IDS/IPS loglarında şüpheli IP'yi sorgulamak için:

index=ids\_logs sourcetype="snort"   
(src\_ip="147.182.193.196" OR dest\_ip="147.182.193.196")  
| table \_time, src\_ip, dest\_ip, alert\_type, signature

### **2. Alan Adları:**

**DNS Logları**: DNS sorgularında şüpheli alan adı sorgularını tespit etmek için:

* index=dns\_logs sourcetype="dns"   
  query=" **Bradesco.com.br** "   
  | table \_time, query, src\_ip, dest\_ip, record\_type

**Web Proxy Logları**: Proxy loglarında şüpheli domain sorgularını incelemek için:

* index=web\_proxy\_logs sourcetype="proxy"   
  (url=" **Bradesco.com.br** ")  
  | table \_time, client\_ip, server\_ip, url, status\_code

### **3. E-posta Adresleri:**

**Mail Gateway Logları**: E-posta adreslerinde şüpheli gönderenleri tespit etmek için:

* index=mail\_gateway\_logs sourcetype="email"   
  (sender="[**sac@bradesco.com.br**](mailto:sac@bradesco.com.br)" OR [recipient="phishing@target.com](mailto:recipient="phishing@target.com)")  
  | table \_time, sender, recipient, subject, message\_id

**Endpoint Protection Logları**: Endpoint koruma loglarında şüpheli e-posta adreslerine yönelik tespitleri sorgulamak için:

* index=endpoint\_logs sourcetype="endpoint\_security"   
  (email\_sender="[**sac@bradesco.com.br**](mailto:sac@bradesco.com.br)")  
  | table \_time, email\_sender, email\_recipient, threat\_type, action\_taken

### **4. Zaman Bilgisi:**

**SIEM Kural Analizi**: Zaman bilgisi üzerinden, belirli bir zaman diliminde şüpheli etkinlikleri tespit etmek için:

index=siem\_logs sourcetype="siem"   
\_time>=now()-24h   
(src\_ip="147.182.193.196" OR dest\_ip="147.182.193.196")  
| table \_time, src\_ip, dest\_ip, event\_type, rule\_name

### **Şüpheli Davranışlar:**

1. **E-posta Göndereni (**[**sac@bradesco.com.br**](mailto:sac@bradesco.com.br)**):**
   1. **Şüphe Durumu:** Gönderen e-posta adresi ([sac@bradesco.com.br](mailto:sac@bradesco.com.br)), SPF, DKIM ve DMARC doğrulama sonuçlarında başarısızlık göstermiştir. Ayrıca, DMARC kontrolü "fail" olarak işaretlenmiştir. Bu durum, e-posta adresinin sahte olabileceğini veya kimlik doğrulama mekanizmalarının kötüye kullanıldığını gösteriyor.

**Aksiyon:**

* + 1. **E-posta Filtrelemesi:** SIEM veya güvenlik geçidi üzerinde bu e-posta adresini hedef alarak gelen e-postalar için uyarılar oluşturulabilir.

**IP Adresi (147.182.193.196):**

* **Şüphe Durumu:** Bu IP adresi, e-posta gönderiminde kullanılan sunucuya aittir. Ayrıca, DNS sorguları ve diğer log kaynaklarında bu IP'nin şüpheli aktiviteler için daha önce raporlanmış olabileceği göz önünde bulundurulmalıdır.
* **Aksiyon:**
  + **Firewall Engelleme:** Bu IP adresine yönelik firewall üzerinde bir engelleme kuralı ekleyin.
  + **IDS/IPS Analizi:** IDS/IPS sistemleri üzerinden bu IP adresine yönelik olası saldırılar tespit edilebilir ve engellenebilir.
  + **IP Reputasyon Analizi:** Bu IP’nin itibarını kontrol edin ve IP'yi kötü amaçlı olarak raporlanmış IP'ler listesinde sorgulayın.

**Zaman ve Süreklilik (E-posta Gönderim Zamanı: 26 Temmuz 2023, 12:17:46 UTC):**

* **Şüphe Durumu:** Gönderim zamanı, genellikle iş saatleri dışında gerçekleşiyor. Bu tür e-posta aktiviteleri, saldırganların ağ sistemlerine sızmaya çalıştığı veya kritik sistemlere kötü amaçlı yazılım göndermeye çalıştığı saatler olabilir.r.
* **Aksiyon:**
  + **Zaman Tablosu İzleme:** Gelecekteki benzer aktiviteler için zaman tablosu analizleri yapılmalı ve belirli saat dilimlerinde gerçekleşen şüpheli davranışlar izlenmelidir.
  + **Kural Tetikleyici:** SIEM üzerinde, belirli saat dilimlerinde gerçekleştirilen şüpheli e-posta gönderimlerine karşı uyarılar tetiklenmelidir.

**Şüpheli durumlarda bu kullanılabilir:**

index=\* (src\_ip="147.182.193.196" OR domain=" Bradesco.com.br " OR [sender="](mailto:sender="ngcxl@ganmorfan.com)[sac@bradesco.com.br”](mailto:sac@bradesco.com.br))

| stats count by src\_ip, domain, sender