Case #9833 - Phishing email example Possible Phishing EW1b8rMzxWDnH8ST

Assignees

Description

Overall Classification: MALICIOUS

Analysis results for this email can be found below

Email reported by: reporter@yourcompany.com.
Subject: Fwd: Suspicious Email

Sender Analysis Results:

Email Address	From Headers	Overall Verdict	Response Actions
sender@gmail.com	Sender name sender@gmail.com	Not Malicious	Not Malicious

Email Analysis Results:

Email Address	Overall Verdict	Response Actions
tinesdemos@gmail.com	Not Malicious	Not Malicious
anotheremail@gmail.com	Not Malicious	Not Malicious
report-phishing@yourcompany.xyz	Not Malicious	Not Malicious

Email Domain Analysis Results:

Email Domain	Overall Verdict	Response Actions
yourcompany.com	Not Malicious	Not Malicious
yourcompany.xyz	Not Malicious	Not Malicious
gmail.com	Malicious	Add Domain to Known Good Resource

IP Headers Analysis Results:

IP	Overall Verdict
209.85.208.50	Not Malicious

URL Analysis Results:

URL	Overall Verdict	Response Actions
hxxps?//prontomedwork[.]com[.]br/wp-content/themes/prontomed/login[.]php	Malicious	View Screenshot of URL

Attachment Results: 0 Attachments Analyzed.
No Results Found

Body

-------- Original Message -------- SUBJECT:Suspicious Link DATE:2021-06-22 14:10 FROM:anotheremail@gmail.com TO:sender@gmail.com http://prontomedwork.com.br/wp-content/themes/prontomed/login.php

Headers

"Return-Path": "<reporter@yourcompany.com>", "Received": "from xxx.google.com", "Date": "Mon, 18 Sep 2023 14:47:50 -0700", "From": "Sender name <sender@gmail.com>", "To": "sender@gmail.com", "Message-ID": "<xxxx@mail.gmail.com>", "In-Reply-To": "<xxxx@mail.gmail.com>", "References": "<xxx@mail.gmail.com> <xxx@mail.gmail.com>", "Subject": "Fwd: Suspicious Email", "Mime-Version": "1.0", "Content-Type": "multipart/alternative; boundary=\"xxx\"", "Received-SPF": "pass", "Authentication-Results": "xxxx", "X-SES-RECEIPT": "xxx", "X-SES-DKIM-SIGNATURE": "xxx", "DKIM-Signature": "xxx", "X-Google-DKIM-Signature": "xxx", "X-Gm-Message-State": "xxx", "X-Google-Smtp-Source": "xxx", "X-Received": "xxx" }

Details

Open/Closed	Open
Status	Open
Priority	Medium
Tags	
Opened	2025-03-25 04:00:06 UTC
Resolved	

Records

Threat Intel

Record: 7820849

Story name	Phishing Use Case
Timestamp	2025-03-25 04:00:37
IOC	aadams@rondo.arsenal.xyz
Threat Level	none
Threat Score	Suspicious
Vendor	EmailRep
SNOW ID	

Record: 7820846

Story name	Phishing Use Case
Timestamp	2025-03-25 04:00:34
IOC	hxxp://apoolcondo[.]com/images/doc[.]exe

Threat Level	
Threat Score	
Vendor	Recorded Future
SNOW ID	

Record: 7820848

Story name	Phishing Use Case
Timestamp	2025-03-25 04:00:36
IOC	ocook@candle.radical.me
Threat Level	none
Threat Score	Suspicious
Vendor	EmailRep
SNOW ID	

Record: 7820850

Story name	Phishing Use Case
Timestamp	2025-03-25 04:00:38
IOC	AF7C84017DA35B83C5FFBF1EB1921B93@amadeus.diana.ril
Threat Level	none
Threat Score	Suspicious
Vendor	EmailRep
SNOW ID	

Actions

2025-03-25 04:00:06 UTC	Tines	created	9833
2025-03-25 04:00:06 UTC	Tines	sub_status_updated	Open
2025-03-25 04:00:06 UTC	Tines	severity_updated	Medium
2025-03-25 04:00:39 UTC	Record Lookup	record_result_set_added	Phishing Use Case,2025-03-25 04:00:34,hxxp://apoolcondo[.]com/images/doc[.]exe,,,Recorded Future,
2025-03-25 04:00:41 UTC	Record Lookup	record_result_set_added	Phishing Use Case,2025-03-25 04:00:36,ocook@candle.radical.me,none,Suspicious ,EmailRep,

2025-03-25 04:00:42 UTC	Record Lookup	record_result_set_added	Phishing Use Case,2025-03-25 04:00:37,aadams@rondo.arsenal.xyz,none,Suspicious ,EmailRep,
2025-03-25 04:00:43 UTC	Record Lookup	record_result_set_added	Phishing Use Case,2025-03-25 04:00:38,AF7C84017DA35B83C5FFBF1EB1921B93@amadeus.diana.ril,none,Suspicious ,EmailRep,
2025-03-25 13:01:51 UTC	Tines	sla_warning	response
2025-03-25 13:01:51 UTC	Tines	sla_warning	resolution
2025-03-25 16:01:53 UTC	Tines	sla_exceeded	response
2025-03-25 16:01:53 UTC	Tines	sla_exceeded	resolution

Fields