

Email samples and screenshots in this analysis are from Phishing Pot by Peixoto, licensed under CC BY-NC 4.0. The original sample analysed in this report can be found below:

Phishing Pot: https://github.com/rf-peixoto/phishing_pot

Peixoto: <https://github.com/rf-peixoto>

License: https://github.com/rf-peixoto/phishing_pot/blob/main/LICENSE

Source file: https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-1807.eml

Executive Summary

=====

This report analyzes a phishing email impersonating Dove, sent from unrelated email addresses. The attacker attempts to trick the recipient into clicking a fraudulent link under the pretext of entering a raffle for free products. Indicators of compromise include urgency tactics, grammar issues, failure of SPF authentication, and the use of malicious URLs. Although the phishing page has since been removed, the email demonstrates typical characteristics of credential-harvesting attempts. Defensive actions were taken to block the sender and associated domains to prevent further exposure.

Headers

=====

Date: Mon, 06 Nov 2023 21:43:58 +0100

Subject: Glückwunsch! Jetzt Gewinndaten eintragen 🎉🎊

To: phishing@pot

From: Dove, Dove <news@my.esprit-friends.com>

Reply-To: reply_to@firiri.shop

Return-Path: news@my.esprit-friends.com

Sender IP: 80.96.157.111 (US)

Resolve Host: n4wgdjkjepwozzicwiabrzoku95vbj1qwb.h5ph

Message-ID: <gDTgJcF.65201.535+=phishing@pot@service@newsletter.otto.de>

URLs

=====

hxxps://[t.]co/vlnwg9IYX2 which redirects to:

hxxp://[innovataq[.]com/1013baa9fc394f75000?tr_uuid=20250920-2300-30a1-b6fc-79107f9a89c4&fp=-5

hxxp://[myhealthyliving[.]life/Q1ZDczhkZEEZqL1lyVnVNeGZtOEcxMFptdDFaRHdXV3hha2E1Yjc zdTlIa1Y5bGJNmlueFB2ckRVYWJsc0dFb0lGcjNyM2hSM01oWkdkaFFwR1FLcnc9PQ__

hxxp[:]//myhealthyliving[.]life/TGdSUkdSZ1VsaUJHeXITWHlwTHdPUkpXQVBuK0pwSXA2ZUZ
KTnJPQUY2RIJudmhQUIVPTGdzZENvUIBDa1RuTDhVdEYvdWFPc3Q1NnBJZExZb0IHMXc9P
Q__

Description

=====

It is an email in German claiming to be from Dove. They are holding a raffle for free Dove products due to Black Friday. To participate, they just need to click a button.

There are grammar issues, such as the use of the informal 'du' and the formal 'Ihnen' being used interchangeably, as well as the overuse of certain words that make the email sound clumsy.

The chance to win something is often used by attackers to trick someone into clicking a link.



Artifact Analysis

=====

Sender Analysis:

The email claims to come from Dove, with Dove as the display name, but the email addresses in the From, Reply-To and Return-Path headers are not related to Dove.

The From and Return-Path headers use the my[.]esprit-friends[.]com domain, which has 1 security vendor on VirusTotal claim that it is malicious. That said, the SPF check failed, so the email address may have been spoofed.

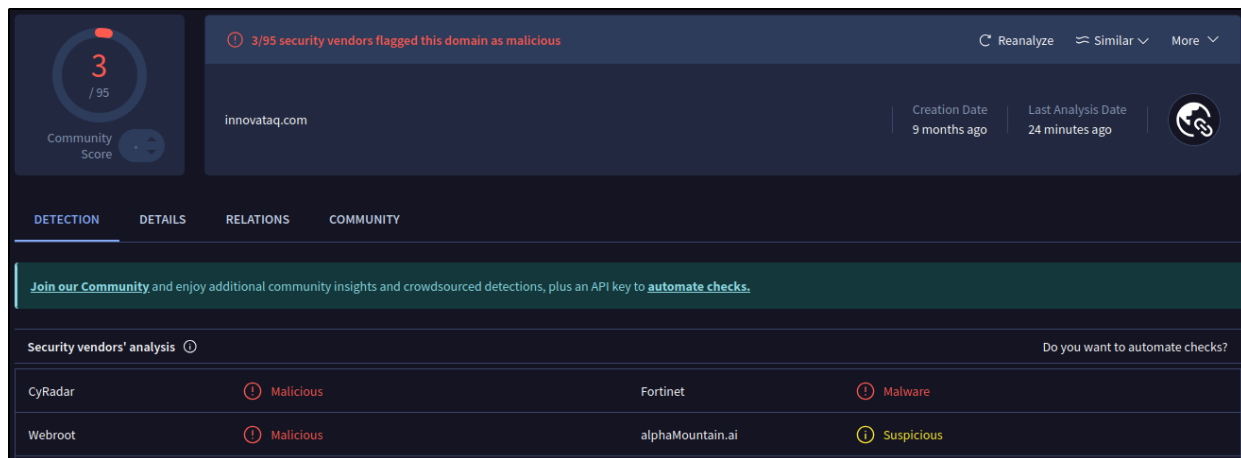
The Reply-To header uses firiri[.]shop, which is a domain that is considered malicious by 10 security vendors on VirusTotal. The sender's IP address also has 1 security vendor on VirusTotal claim that it is malicious. Firiri[.]shop was seen in a previous phishing campaign.

The email message ID mentions service@newsletter[.]otto[.]de which is also not related to Dove, and was seen in a previous report.

SPF check fails, there is no DKIM signature, and no DMARC record. This means that news@my[.]esprit-friends[.]com was not the real sender of the email, and that there is no proof that the email has not been tampered with.

URL Analysis:

hxxps[:]t[.]co/ is a URL shortening service, and the hxxps[:]t[.]co/vlnwg9IYX2 URL redirects to a URL and domain which is considered malicious by 3 security vendors on VirusTotal.



The screenshot shows the VirusTotal interface for the domain **innovataq.com**. At the top, a red banner indicates that 3 out of 95 security vendors flagged this domain as malicious. The domain's creation date is 9 months ago, and the last analysis was performed 24 minutes ago. Below the header, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A green banner encourages joining the community. The 'Security vendors' analysis' section shows the following results:

Vendor	Verdict
CyRadat	Malicious
Fortinet	Malware
Webroot	Malicious
alphaMountain.ai	Suspicious

Innovataq is a legitimate company, but they use the domain innovataq[.]digital

The two URLs on the hxxp[:]myhealthyliving[.]life domain are no longer available. VirusTotal has one security vendor say it is suspicious, without any definitive verdicts. Note that there is a legitimate MyHealthyLiving, but they use the myhealthyliving[.]net domain.

Attachment Analysis:

There were no attachments

Verdict

As the email claims to be from Dove, but the email addresses and URLs all are not only unrelated to Dove, but also unrelated to each other, this is a clear impersonation and spoofing attempt.

To give an overview of all the different domains that were used: my[.]esprit-friends[.]com, firiri[.]shop, myhealthyliving[.]life and innovataq[.]com, none of which mention Dove. A legitimate email would use the dove[.]com domain.

As a result of the analysis, this email has been determined to be malicious.

Defense Actions

After performing a message trace, no other users within the organization received an email from this sender or with a similar subject line.

To prevent the malicious sender from sending any other email to the organization, I have blocked the firiri[.]shop domain on the email gateway.

To ensure users are unable to access these malicious URLs or domains, I have blocked “myhealthyliving[.]life” and “innovataq[.]com” on the EDR and on the Web Proxy.