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-1366.eml

Executive Summary
==========
This report analyzes a phishing email impersonating Stayfriends, sent from a spoofed email. The attacker attempts to trick the recipient into clicking a fraudulent link under the pretext of a romantic encounter. Indicators of compromise include grammar issues, failure of DKIM authentication, and the use of a malicious self-hosted URL. 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: Sat, 23 Sep 2023 09:02:18 +0200
Subject: Nachricht für dich!

To: phishing@pot
From: service@stayfriends[.]de

Reply-To: None
Return-Path: return@audiogold[.]co[.]uk

Sender IP: 45.89.54.13
Resolve Host: 2lur[.]audiogold[.]co[.]uk

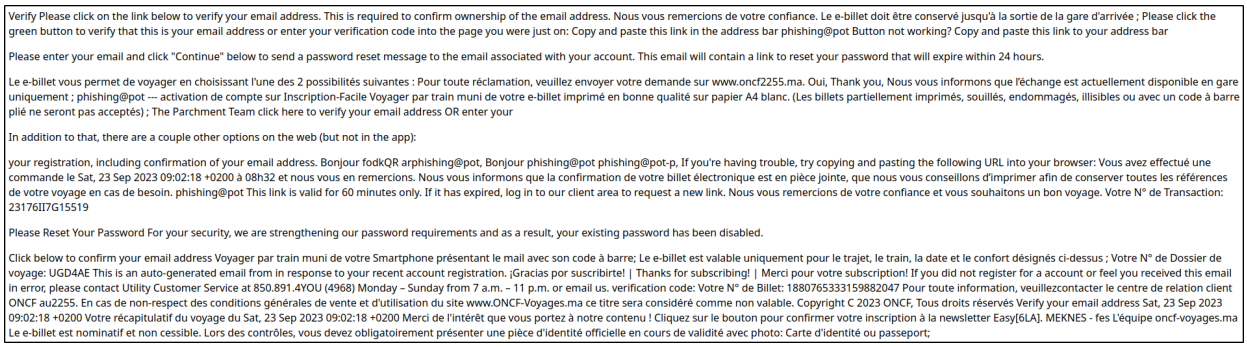
Message-ID:
<976b3f3e-43d0-41ed-962b-843b78676caa@BN8NAM11FT078.eop-nam11.prod.protection.outlook.com>

URLs
==========
hxxp[://]easilett[.]com/cl/221_md/31/20/1/23/2459859
hxxp[://]easilett[.]com/oop/221_md/31/20/1/23/2459859

Description
==========
It is an email in German saying that to entice the recipient with the promise of a personal or romantic interaction, specifically implying openness to an “adventurous” encounter. This type of lure is a common social engineering tactic that seeks to exploit human curiosity and sexual attraction in order to increase the likelihood of link clicks. Such approaches are typical of spam and phishing campaigns targeting individuals rather than organizations.

The politeness levels are not consistent, using both the informal dich and formal sich. The names of two women are used. Michelle sent the message, but there is also another name mentioned: Laura, and it is unclear why.

The email appears completely different when viewed in simple HTML, where it asks users to copy and paste a URL to verify their email address in English and French.


Verify Please click on the link below to verify your email address. This is required to confirm ownership of the email address. Nous vous remercions de votre confiance. Le e-billet doit être conservé jusqu'à la sortie de la gare d'arrivée ; Please click the green button to verify that this is your email address or enter your verification code into the page you were just on: Copy and paste this link in the address bar phishing@pot Button not working? Copy and paste this link to your address bar

Please enter your email and click "Continue" below to send a password reset message to the email associated with your account. This email will contain a link to reset your password that will expire within 24 hours.

Le e-billet vous permet de voyager en choisissant l'une des 2 possibilités suivantes : Pour toute réclamation, veuillez envoyer votre demande sur www.oncf2255.ma. Oui, Thank you, Nous vous informons que l'échange est actuellement disponible en gare uniquement ; phishing@pot --- activation de compte sur Inscription-Facile Voyager par train muni de votre e-billet imprimé en bonne qualité sur papier A4 blanc. (Les billets partiellement imprimés, souillés, endommagés, illisibles ou avec un code à barre plié ne seront pas acceptés) ; The Parchment Team click here to verify your email address OR enter your

In addition to that, there are a couple other options on the web (but not in the app):

your registration, including confirmation of your email address. Bonjour fodkQR arphishing@pot, Bonjour phishing@pot phishing@pot-p, If you're having trouble, try copying and pasting the following URL into your browser: Vous avez effectué une commande le Sat, 23 Sep 2023 09:02:18 +0200 à 08h32 et nous vous en remercions. Nous vous informons que la confirmation de votre billet électronique est en pièce jointe, que nous vous conseillons d'imprimer afin de conserver toutes les références de votre voyage en cas de besoin. phishing@pot This link is valid for 60 minutes only. If it has expired, log in to our client area to request a new link. Nous vous remercions de votre confiance et vous souhaitons un bon voyage. Votre N° de Transaction: 23176II7G15519

Please Reset Your Password For your security, we are strengthening our password requirements and as a result, your existing password has been disabled.

Click below to confirm your email address Voyager par train muni de votre Smartphone présentant le mail avec son code à barre; Le e-billet est valable uniquement pour le trajet, le train, la date et le confort désignés ci-dessus ; Votre N° de Dossier de voyage: UGD4AE This is an auto-generated email from in response to your recent account registration. ¡Gracias por suscribirte! | Thanks for subscribing! | Merci pour votre subscription! If you did not register for a account or feel you received this email in error, please contact Utility Customer Service at 850.891.4YOU (4968) Monday – Sunday from 7 a.m. – 11 p.m. or email us. verification code: Votre N° de Billet: 1880765333159882047 Pour toute information, veuillezcontacter le centre de relation client ONCF au2255. En cas de non-respect des conditions générales de vente et d'utilisation du site www.ONCF-Voyages.ma ce titre sera considéré comme non valable. Copyright C 2023 ONCF, Tous droits réservés Verify your email address Sat, 23 Sep 2023 09:02:18 +0200 Votre récapitulatif du voyage du Sat, 23 Sep 2023 09:02:18 +0200 Merci de l'intérêt que vous portez à notre contenu ! Cliquez sur le bouton pour confirmer votre inscription à la newsletter Easy[6LA]. MEKNES - fes L'équipe oncf-voyages.ma Le e-billet est nominatif et non cessible. Lors des contrôles, vous devez obligatoirement présenter une pièce d'identité officielle en cours de validité avec photo: Carte d'identité ou passeport;

Artifact Analysis
==========
Sender Analysis:
Although the email claims to be from Stayfriends, the email in the Return-Path header uses an Audiogold domain, which is a second hand Hi fi retailer in the UK, inconsistent with the Stayfriends branding. Additionally, the display name in the From field says Fgehen69 instead of Stay Friends or something similar.

SPF, DKIM and DMARC checks all fail.

URL Analysis:
The URL that the user is supposed to click on is not affiliated with Stayfriends. The hxxp[://]easilett[.]com domain is no longer available and has no hits on VirusTotal. Easilett is a legitimate company, but they do not seem to have a website.

While the domain is no longer available, it likely was used to harvest credentials by impersonating a Stayfriends login page.

Verdict

==========

As there are various domain mis-matches with the Return-To and clickable URLs, this is a spoofing attempt. There are also language mistakes, which a legitimate service would not make. A legitimate email would also not have hidden text in two different languages about a completely different subject from the main email body.

The From: email address can easily be spoofed. The Return-Path and Received headers both indicated that the email came from audiogold[.]co[.]uk, which is a legitimate domain. However, as SPF, DKIM and DMARC checks failed, the attacker likely spoofed the domain rather than sending through the organization's actual mail infrastructure.

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 "Fgehen69 " display name on the email gateway. service@stayfriends[.]de is the legitimate email that Stayfriends uses, but they would not use such a display name for themselves.

To ensure users are unable to access this malicious URL or domain, I have blocked the "easilett[.]com" domain on the EDR and on the Web Proxy. While the website seems to have been removed, it is unlikely that a legitimate service will use that domain in the future, as the company Easilett was incorporated in 2012, and has not created a website in all this time.