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-5876.eml

Executive Summary
==

This report analyzes a phishing email impersonating Disney, sent from what seems to be a AWS email account. The attacker attempts to trick the recipient into clicking on the image in the email under the pretext of getting very cheap Disneyland tickets. Indicators of compromise include urgency tactics, non-Disney email/URL use, and link obfuscation by embedding a URL inside another URL. The email demonstrates typical characteristics of payment information harvesting attempts. Defensive actions were taken to block the sender and associated domains to prevent further exposure.

Headers
==

Date: Wed, 27 Aug 2025 13:58:50 +0000
Subject: Billet 1 jour / 2 parcs-Disney

To: phishing@pot
From: Disney Libert=?UTF-8?B?w6ktSUQ2NTg=?= <noreply+voppapr@bedis.fomote.com>

Reply-To: None
Return-Path:
01000198ebd2ffa6-672e0ae4-d3d5-400e-8f74-1415b7a69378-000000@amazonses.com

Sender IP: 54.240.9.244
Resolve Host: a9-244.smtp-out.amazonses.com

Message-ID:
<01000198ebd2ffa6-672e0ae4-d3d5-400e-8f74-1415b7a69378-000000@email.amazonses.com>

URLs
==

hxxps[://]s84w7g5c[.]r[.]us-east-1[.]awstrack[.]me/L0/hxxps[://]desniutrf[.]s3[.]us-east-1[.]amazonaws[.]com/Disney/disney[.]html/2/01000198ebd2ffa6-672e0ae4-d3d5-400e-8f74-1415b7a69378-000000/rA2ZY9jqTFuvlJR9J0Bz2cJaecw=441 hxxps[://]pngdesneyrnf[.]s3[.]us-east-1[.]amazonaws[.]com/desneyiro[.]png

Attachments
==
Attachment Name: Li8bnEss.ics
MD5: d41d8cd98f00b204e9800998ecf8427e
SHA1: da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Description
==
The email claims to be from Disney, and offers an exclusive limited deal of 9.99 for 2 tickets to Disneyland Paris.

There are several indicators of urgency, as it says the amount of tickets available at this cheap price is limited.

The visible part of the email only contains an image with text on it, and clicking anywhere on that image will link to a URL.

When you scroll down, there is some unrelated text about an official US government website with a number of links.

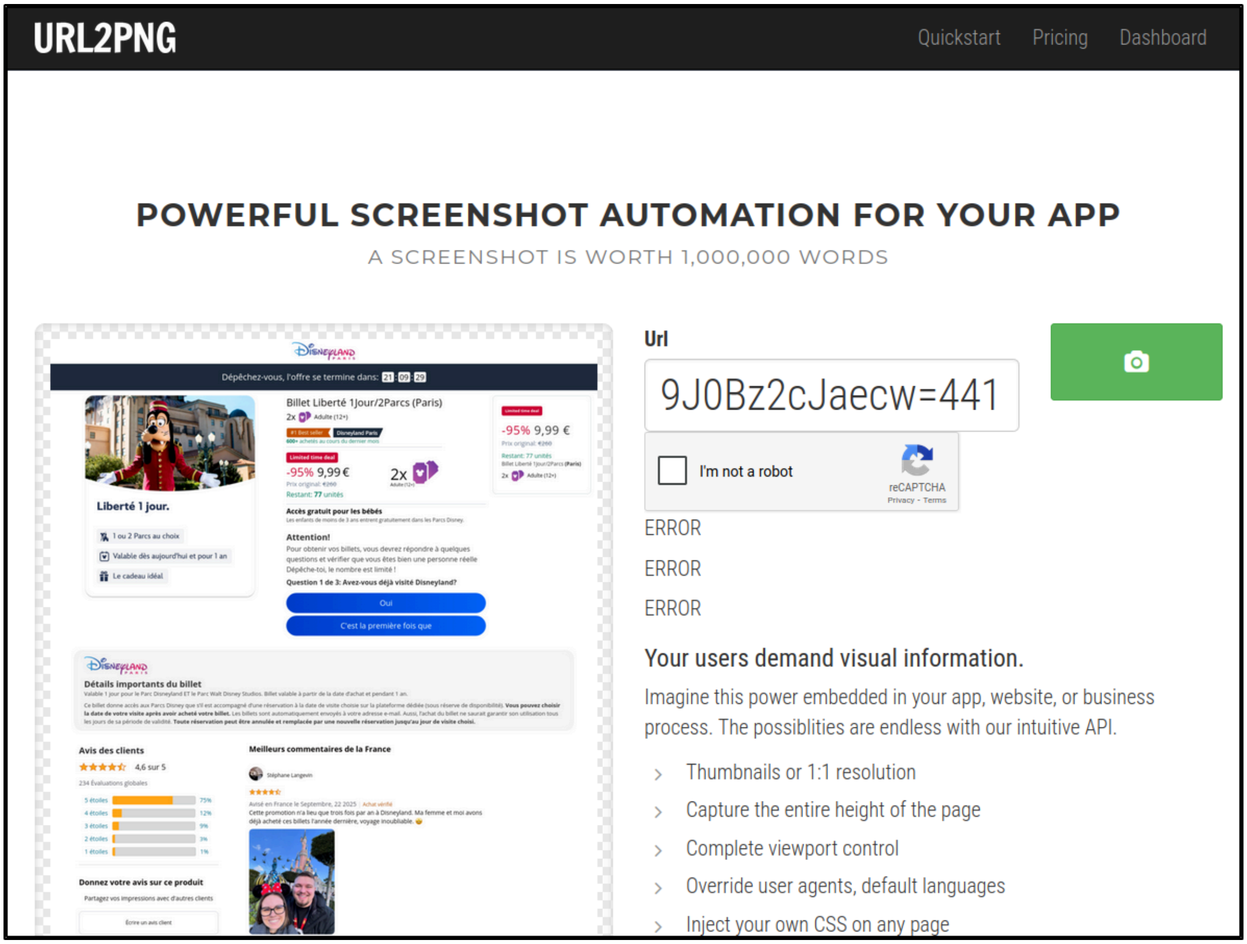
There is also an attachment of 0 bytes.

Artifact Analysis
==
Sender Analysis:
The From email address is not related to Disney. The terms Bedis or Fomote do not seem to be related to any legitimate organizations. The email address is being obfuscated with the display name Disney Liberté.

The Return-Path email address uses the amazonses[.]com domain, which is Amazon Simple Email Service, a cloud based email service from Amazon Web Services (AWS).

URL Analysis:
The first URL is hosted using AWS, which is a legitimate service. However, malicious users do also use that service, and will abuse the trust that AWS has.

Copying the URL that the image links to, you get quite a sophisticated landing page, as shown using URL2PNG. There is a timer for how long the deal lasts and a ‘tickets remaining’ counter to create urgency, as well as reviews to build trust.



POWERFUL SCREENSHOT AUTOMATION FOR YOUR APP

A SCREENSHOT IS WORTH 1,000,000 WORDS

Dépêchez-vous, l'offre se termine dans: 21 : 09 : 29

Billet Liberté 1Jour/2Parcs (Paris)

2x Adulte (12+)

#1 Best seller | Disneyland Paris

600+ achetés au cours du dernier mois

Limited time deal

-95% 9,99 €

Prix original: €260

Restant: 77 unités

2x Adulte (12+)

Limited time deal

-95% 9,99 €

Prix original: €260

Restant: 77 unités

Billet Liberté 1Jour/2Parcs (Paris)

2x Adulte (12+)

Liberté 1 jour.

1 ou 2 Parcs au choix

Valable dès aujourd'hui et pour 1 an

Le cadeau idéal

Accès gratuit pour les bébés

Les enfants de moins de 3 ans entrent gratuitement dans les Parcs Disney.

Attention!

Pour obtenir vos billets, vous devrez répondre à quelques questions et vérifier que vous êtes bien une personne réelle Dépêche-toi, le nombre est limité !

Question 1 de 3: Avez-vous déjà visité Disneyland?

Détails importants du billet

Valable 1 jour pour le Parc Disneyland ET le Parc Walt Disney Studios. Billet valable à partir de la date d'achat et pendant 1 an.

Ce billet donne accès aux Parcs Disney que s'il est accompagné d'une réservation à la date de visite choisie sur la plateforme dédiée (sous réserve de disponibilité). **Vous pouvez choisir la date de votre visite après avoir acheté votre billet.** Les billets sont automatiquement envoyés à votre adresse e-mail. Aussi, l'achat du billet ne saurait garantir son utilisation tous les jours de sa période de validité. **Toute réservation peut être annulée et remplacée par une nouvelle réservation jusqu'au jour de visite choisi.**

Avis des clients

★★★★☆ 4,6 sur 5

234 Évaluations globales

5 étoiles	75%
4 étoiles	12%
3 étoiles	9%
2 étoiles	3%
1 étoiles	1%

Donnez votre avis sur ce produit

Partagez vos impressions avec d'autres clients

Meilleurs commentaires de la France

Stéphane Langevin

★★★★☆

Avisé en France le Septembre, 22 2025 | Achat vérifié

Cette promotion n'a lieu que trois fois par an à Disneyland. Ma femme et moi avons déjà acheté ces billets l'année dernière, voyage inoubliable.

Url

9J0Bz2cJaecw=441

☐ I'm not a robot

ERROR

ERROR

ERROR

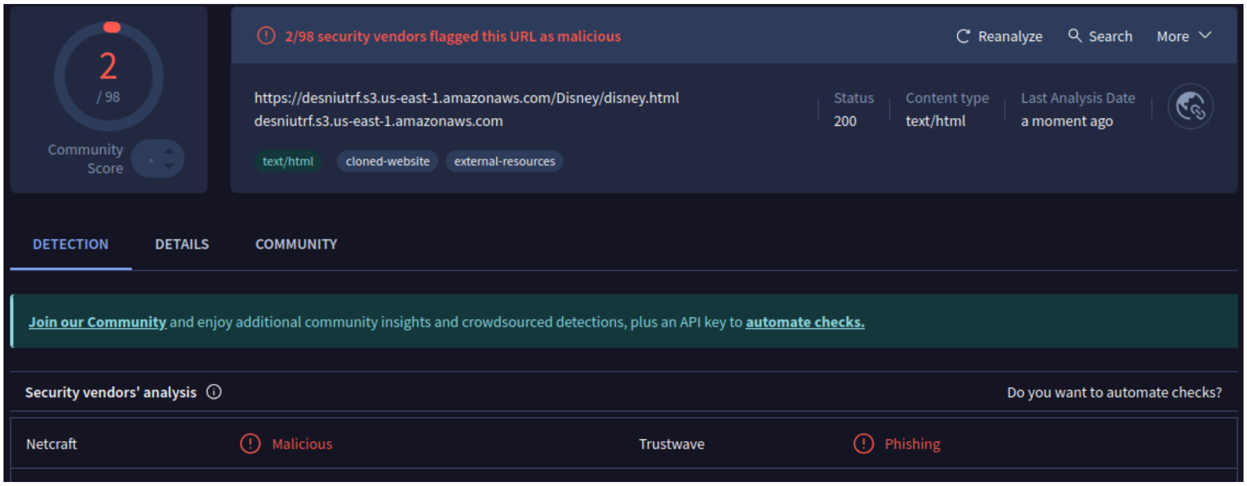
Your users demand visual information.

Imagine this power embedded in your app, website, or business process. The possiblities are endless with our intuitive API.

- Thumbnails or 1:1 resolution
- Capture the entire height of the page
- Complete viewport control
- Override user agents, default languages
- Inject your own CSS on any page

This URL does not have any hits on VirusTotal. But when running the URL in a Hybrid Analysis sandbox, no URLs with the Disney domain can be found. The automatic report deems it suspicious, as one of the domains (boxgift[.]online) is only about a month old. When doing a whois lookup, this can be confirmed. The creation date of the domain is 2025-08-01. Note that boxgift[.]online is offline at the time this report is being written, but was likely used to harvest information such as credit card numbers.

The first URL has embedded within itself another URL:
hxxps[://]desniutrf[.]s3[.]us-east-1[.]amazonaws[.]com/Disney/disney[.]html
This URL has 2 security vendors on VirusTotal say it is malicious.



2 / 98

Community Score

2/98 security vendors flagged this URL as malicious

Reanalyze Search More

https://desniutrf.s3.us-east-1.amazonaws.com/Disney/disney.html
desniutrf.s3.us-east-1.amazonaws.com

Status	Content type	Last Analysis Date
200	text/html	a moment ago

text/html cloned-website external-resources

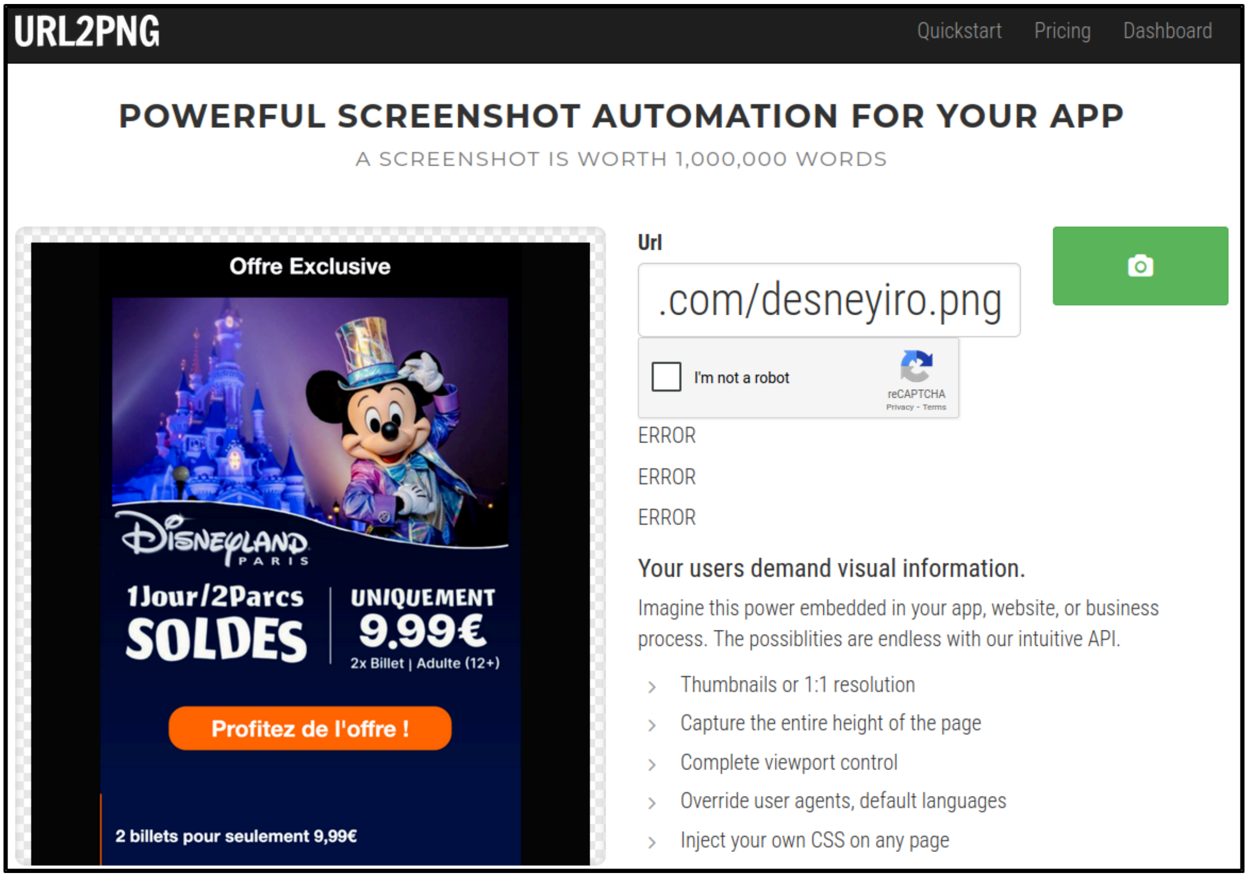
DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

Netcraft	Malicious	Trustwave	Phishing

The second URL has Disney misspelled, seems to link the picture used in the email, and is also hosted on AWS.



URL2PNG — Quickstart Pricing Dashboard

POWERFUL SCREENSHOT AUTOMATION FOR YOUR APP

A SCREENSHOT IS WORTH 1,000,000 WORDS

Offre Exclusive

Disneyland Paris

1Jour/2Parcs SOLDES

UNIQUEMENT 9.99€ 2x Billet | Adulte (12+)

Profitez de l'offre !

2 billets pour seulement 9,99€

Url

.com/desneyiro.png

□ I'm not a robot reCAPTCHA Privacy - Terms

ERROR

ERROR

ERROR

Your users demand visual information.

Imagine this power embedded in your app, website, or business process. The possiblities are endless with our intuitive API.

- Thumbnails or 1:1 resolution
- Capture the entire height of the page
- Complete viewport control
- Override user agents, default languages
- Inject your own CSS on any page

While the picture in itself is benign, it obfuscates the text used in the email, and is ultimately the way that users are tricked into clicking the malicious link.

Attachment Analysis:

The attachment is 0 bytes and does not contain any data. Opening it using Sublime, or using the cat command on the file returns no data.

Verdict
===

Due to the sender not being affiliated with Disney, this is a clear impersonation and spoofing attempt.

Additionally, the URL uses a generic AWS link and is also not related to Disney. A Hybrid Analysis report says that the page is suspicious, as there is a link to a domain that is relatively new and now expired.

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 "01000198ebd2ffa6-672e0ae4-d3d5-400e-8f74-1415b7a69378-000000@amazonses.com" email and the "bedis.fomote.com" email domain on the email gateway.

To ensure users are unable to access these malicious URLs or domains, I have blocked the below URL and domain on the EDR and on the Web Proxy.
hxxps[://]s84w7g5c[.]r[.]us-east-1[.]awstrack[.]me
hxxps[://]desniutrf[.]s3[.]us-east-1[.]amazonaws[.]com
hxxps[://]pngdesneyrnf[.]s3[.]us-east-1[.]amazonaws[.]com