Executive Summary

==

This report analyzes a phishing email impersonating ProtonMail, sent from a free Gmail account. The attacker attempts to trick the recipient into clicking a fraudulent link under the pretext of restoring a “Prime” mailbox service, which does not exist. Indicators of compromise include urgency tactics, failure of DKIM authentication, and the use of a malicious Webflow-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: Mon, 24 Jul 2023 09:14:54 -0700
Subject: THE PRIME

To: username@hotmail.com
From: amandastaples353@gmail.com

Reply-To: None
Return-Path: amandastaples353@gmail.com

Sender IP: mail-lj1-f177.google.com
Resolve Host: 209.85.208.177

Message-ID:
<CA+b2QgQh3=9wJxbyTmCq9Sapx9mAuRCCyz31_nvBNrqNL13_pw@mail.gmail.com>

URLs

==

hxxps[://]protonmail-6e3725[.]webflow[.]io/
hxxp[://]skymesh[.]com[.]au/

Description

==
It is an email with just text, no graphics. It claims the Prime version of their mailbox will be replaced by the next day, and to click a link. It is not clear from the email body who the email claims to represent, but the signature mentions ProtonMail.

There are several indications of urgency: The receiver has 1 day to restore their mailbox and avoid the permanent closure of their account.

Artifact Analysis
==
Sender Analysis:
The mail claims to be from Protonmail, but Protonmail does not have a Prime mailbox feature. Additionally, the email came from a Gmail address with a format {firstname}{lastname}{numbers} which is often used by attackers.

DKIM authentication failed.

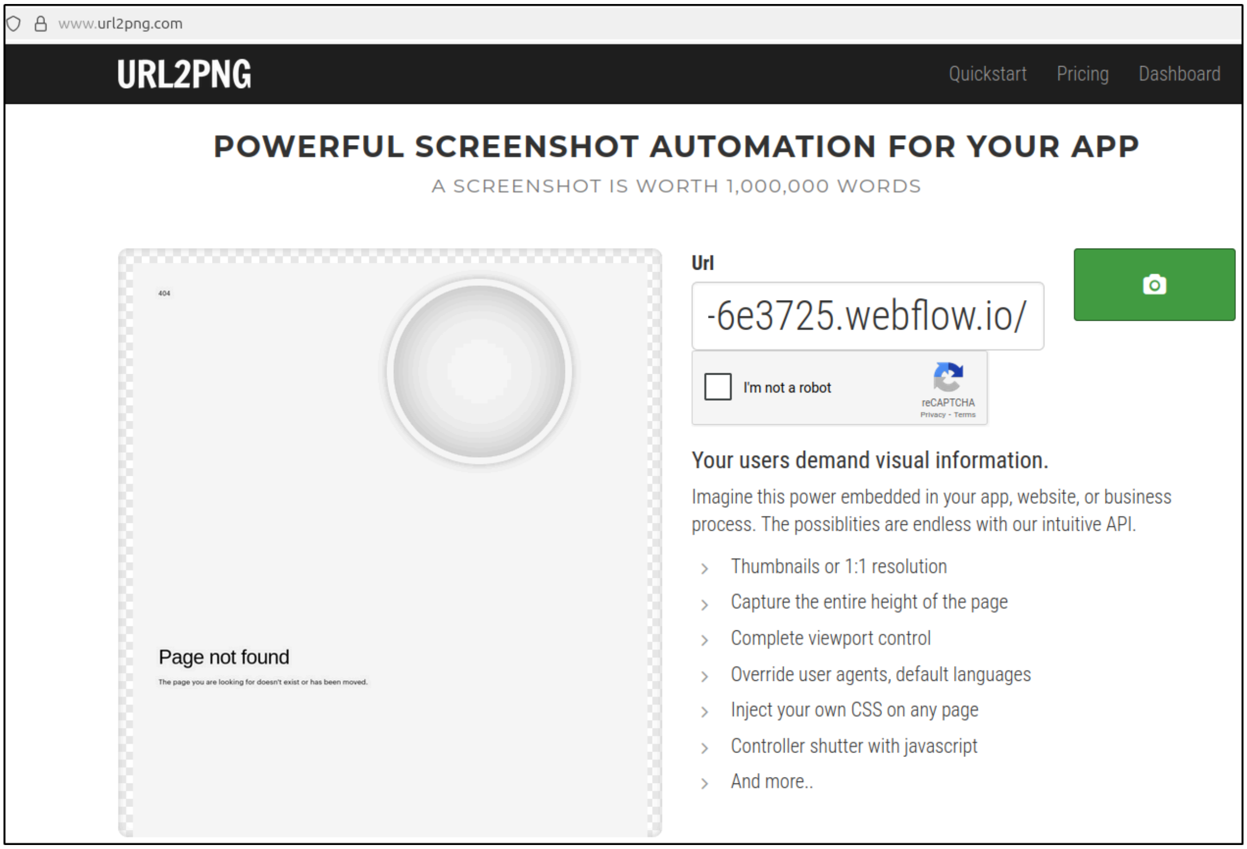
URL Analysis:
hxxps[://]protonmail-6e3725[.]webflow[.]io/ is no longer available and does not give any hits on VirusTotal. This is the link that the email asks to click on with the text being ‘Log-in Restore’ so this was likely a credential harvesting page. Webflow is a legitimate service and must have taken down this page after receiving complaints.

There is another URL: hxxp[://]skymesh[.]com[.]au/. However this seems to not be related to anything, and it is unclear as to why it is there. Skymesh is a legitimate internet provider in Australia, and the link redirects to their homepage https://www.skymesh.net.au/

Verdict
==
Due to the sender being unaffiliated with Protonmail, and the Prime mailbox for Protonmail service not existing, this email is a clear impersonation and spoofing attempt.

The email seems to be a very low effort phish, as there are no logos, and no company is mentioned except for the signature. Legitimate services would usually call an account a {company} account, such as an Indeed account or an Amazon account.

The phishing link has been taken down, as can be seen in the below screenshot:
hxxps[://]protonmail-6e3725[.]webflow[.]io/



POWERFUL SCREENSHOT AUTOMATION FOR YOUR APP

A SCREENSHOT IS WORTH 1,000,000 WORDS

404

Page not found

The page you are looking for doesn't exist or has been moved.

Url: -6e3725.webflow.io/

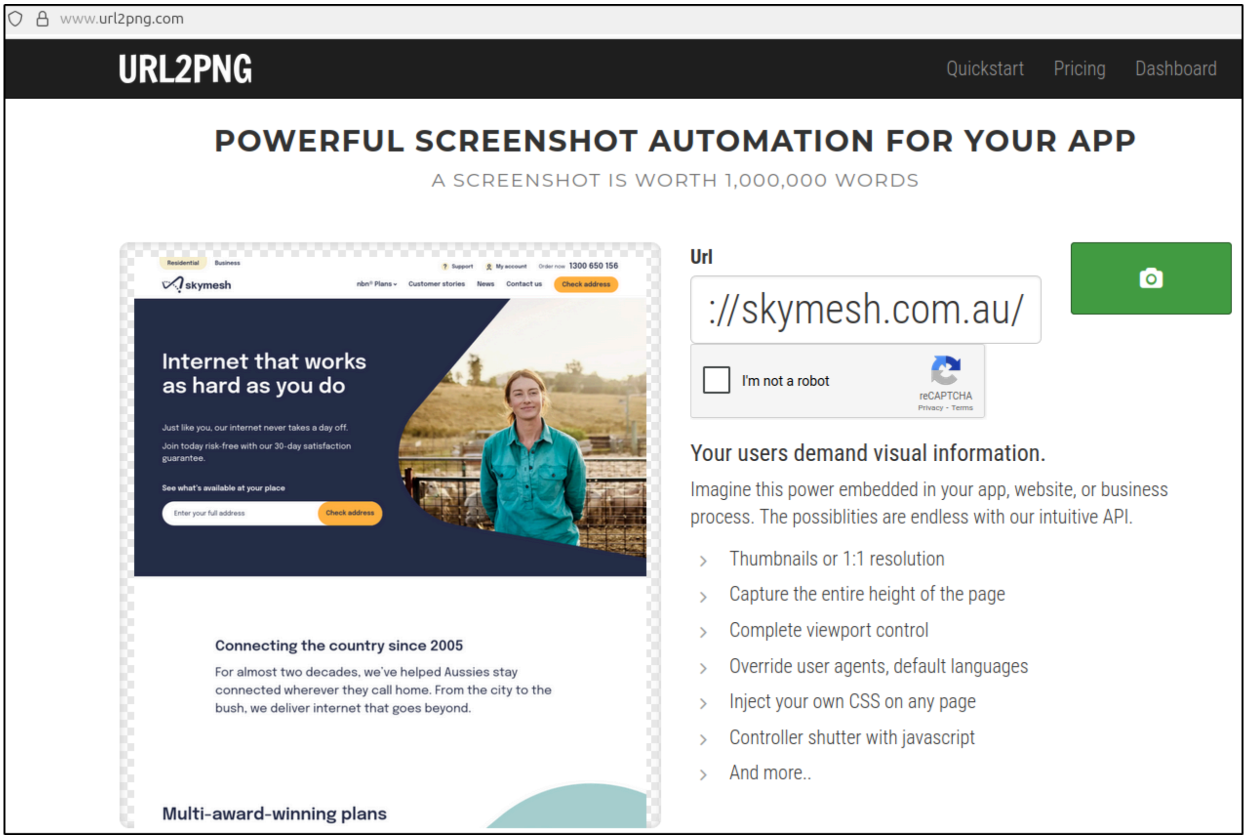
□ I'm not a robot

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
- Controller shutter with javascript
- And more..

And the random Skymesh link seems to be unrelated, and may have been added by accident, or was added to function as a red herring.
http://skymesh[.]com[.]au/



POWERFUL SCREENSHOT AUTOMATION FOR YOUR APP

A SCREENSHOT IS WORTH 1,000,000 WORDS

://skymesh.com.au/

Internet that works as hard as you do

Just like you, our internet never takes a day off.

Join today risk-free with our 30-day satisfaction guarantee.

See what's available at your place

Connecting the country since 2005

For almost two decades, we've helped Aussies stay connected wherever they call home. From the city to the bush, we deliver internet that goes beyond.

Multi-award-winning plans

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
- Controller shutter with javascript
- And more..

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 “amandastaples353[@]gmail[.]com” email on the email gateway. The gmail[.]com domain is legitimate, but this particular user is malicious.

To ensure users are unable to access this malicious URL or domain, I have blocked “hxxps[://]protonmail-6e3725[.]webflow[.]io/” 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.