Dangerous Phishing Campaign for Harvesting Credentials using an HTML Attachment

perception-point.io/dangerous-phishing-campaign-for-harvesting-credentials-using-an-html-attachment/

June 20, 2021

Overview.

Attackers are becoming more sophisticated in their phishing techniques, and brand impersonation attempts are looking more and more genuine. Recently, Perception Point's platform intercepted a dangerous phishing campaign that would easily fool many users, as it looks quite authentic.

In this post, we will present the attack and how Perception Point's engines prevented it.

In this attack, we see legitimate-looking emails, spoofing the target company using name only or full address, using a legitimate-looking payload in the form of an HTML attachment (the term payload, in this context, refers to any attack containing a file or a URL).

The HTML attachment embodies a well-made login page, spoofing the real brand login page, and once you type in your password, you're redirected to the actual phished brand's URL, and simultaneously your credentials are sent to the attacker.

The Mail.

In this phishing attack, the attacker tries to impersonate the targeted brand using the following assets in the email:

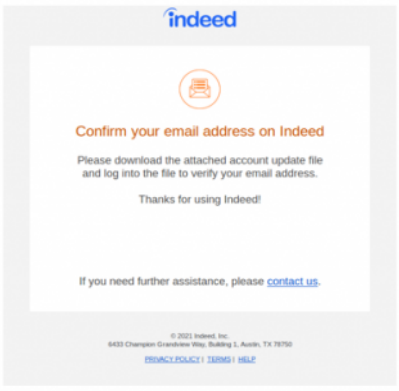
- Brand logo
- Brand signature
- Brand email body design
- Using the brand's color pallet and language

To add credibility, the attacker takes advantage of typical messages that are sent by the brand and mimics those messages.

In the following examples, you can see the attacker's original emails, where he uses the brand's language and typical messages that the receiver would expect, based on past interaction with known websites such as CMA CGM, Coinbase, and Indeed:

An incoming shipment notification for CMA CGM

An unusual sign-in activity alert from coinbase

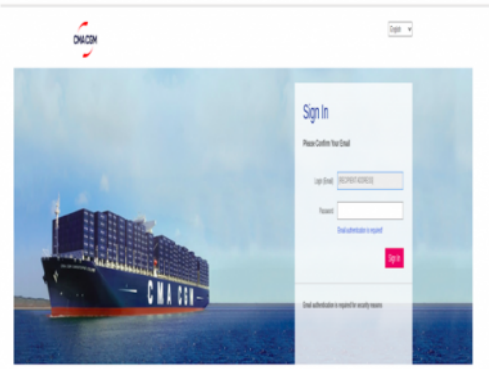


Account details update request from indeed

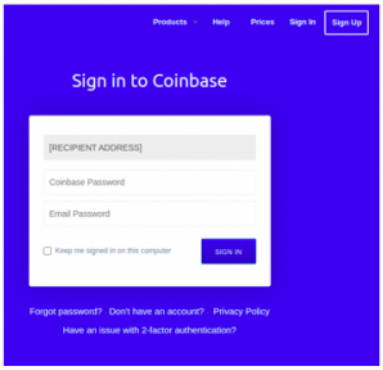
The Payload.

To complete the disguise, the attacker uses an HTML file containing a well-faked brand login page which upon credential submission actually redirects you to the real brand login page, making it look like it really belongs to the brand – all the while sending the submitted credentials to the attacker.

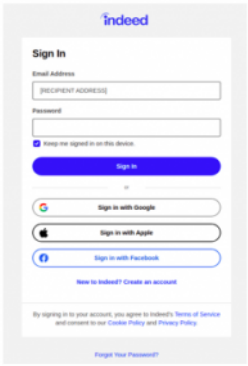
The sign-in page completely spoofs the real brands. Here are our 3 examples from CMA CGM, Coinbase, and Indeed:



CMA CGM HTML Sign in page



Coinbase HTML Sign in page



indeed HTML Sign in page

The credentials are sent to a different WordPress domain which was hacked by the same attacker or bought by him (we saw in another article how attackers use compromised WordPress sites to host phishing)

How did we prevent this attack?

Perception Point's email threat protection prevents advanced anti-phishing algorithms. The system leverages image-recognition algorithms for the purpose of identifying brand impersonation sites, as well as machine learning and other technologies to detect spoofing of names, domains, and brands, to prevent any attack – even if highly disguised.

Perception Point takes an active ("dynamic") approach, rendering the HTML page on several browsers, to ensure "zero-day" phishing attacks are intercepted well before reaching the end-user's email box as opposed to other solutions that only use reputation and static engines.

For more information about our anti-phishing capabilities, we welcome you to check this link.

Recommendations.

Awareness and education of users could have helped to prevent this attack. It is important to educate users on the fact that an HTML attachment would never be sent by a legitimate business, and they should never submit any personal information through such attachment.

Also, rather than clicking a link through an email to submit any requested information, it is good best practice for users to actively surf to the website, in order to complete any transaction that they were requested to complete in the email. And the final recommendation is of course to use an advanced security solution with dynamic analysis, to catch these kinds of attacks and others that have managed to evade users for any kind of reason.

IOCs.

- Subject: CMA-CGM Receipt for [RECIPIENT ADDRESS] / Indeed account update for [RECIPIENT ADDRESS] / Unusual sign-in activity

- From: Coinbase <no-reply@coinbase.com> / Indeed <employers-noreply@indeed.com> / CMA-CGM <it@fmx00.freemail.hu>
- Email server IP: 170.0.100.2 for all attacks