Maati, Oussama

Mail analysis report

Email 1:

What is the email's timestamp?

Mon, 20 Mar 2023 08:57:04 -0700

Who is the email from?

“service@paypal.be”

What is his email address?

service@paypal.be

What email address will receive a reply to this email?

service@paypal.be

What brand was this email tailored to impersonate?

PayPal

What is the originating IP? Defang the IP address.

66[.]211[.]170[.]87

What do you think will be a domain of interest? Defang the domain.

Hxxps[://]www[.]paypal[.]com[/]signin

What is the shortened URL? Defang the URL.

[@] paypal[.]com

Do you think this is a phishing email?

No, I don’t this this is a phishing email, because the website redirect to a true PayPal website (without clicking on it), and there is not a possible way that it is a domain name “theft”. Also, the sender is only service@paypal.be so there is no other senders or hidden one.

Email 2:

What is the email's timestamp?

Mon, 12 Dec 2022 03:56:38

Who is the email from?

“no reply”

What is his email address?

stainless@midnightmagicevents.com

What email address will receive a reply to this email?

stainless@midnightmagicevents.com

What brand was this email tailored to impersonate?

Trust Wallet

What is the originating IP? Defang the IP address.

66[.]211[.]170[.]87

What do you think will be a domain of interest? Defang the domain.

hxxps[://]climovil[.]com[=/]

What is the shortened URL? Defang the URL.

Climovil [.]com

Do you think this is a phishing email?

Yes, because without clicking we can see that the Trust wallet link goes to “climovil.com” and that is a site used to host website so anyone can buy server to host his website there. Trust wallet would use his own server for that.

Email 3:

What is the email's timestamp?

Sun, 26 Mar 2023 13:31:56

Who is the email from?

Tinder

What is his email address?

gq@80-78-255-128.cloudvps.regruhosting.ru

What email address will receive a reply to this email?

gq@80-78-255-128.cloudvps.regruhosting.ru

What brand was this email tailored to impersonate?

Tinder

What is the originating IP? Defang the IP address.

80[.]78[.]255[.]128

What do you think will be a domain of interest? Defang the domain.

Hxxp[://]blog[.]xulingxueyuan[.]cn[/]contradictedqm[.]php?uxm_campaign=xpdjuresn

What is the shortened URL? Defang the URL.

Hxxp[://]blog[.]xulingxueyuan[.]cn

Do you think this is a phishing email?

Yes this is a fishing mail, because first the mail is not from tinder, and also the link don’t redirect to tinder website or app.

Email 4:

What is the email's timestamp?

Fri, 3 Mar 2023 03:44:03 -0800 (PST)

Who is the email from?

Dr. Dan Miller

What is his email address?

babakingsouthmichael@gmail.com

What email address will receive a reply to this email?

imorourafiatou0@gmail.com

What brand was this email tailored to impersonate?

United Nations Special Representative for Disaster Risk Reduction

What is the originating IP? Defang the IP address.

209[.]85[.]220[.]41

What do you think will be a domain of interest? Defang the domain.

babakingsouxhmichael[@]gmail[.]com

What is the shortened URL? Defang the URL.

google[.]com

Do you think this is a phishing email?

Yes, because there is no proof, he is a doctor, or part of the UNSRDRR, and mostly because no one will give me money for free, for just giving your information the scammer want to steal information to use them or impersonate them.

Email 5:

What is the email's timestamp?

27 Aug, 2022 9:42:09 AM

Who is the email from?

Ariana

What is his email address?

newsmail@app9l.serenitepure.fr

What email address will receive a reply to this email?

Ariana news@aichakandisha.com

What brand was this email tailored to impersonate?

WhatsApp

What is the originating IP? Defang the IP address.

51[.]83[.]34[.]109

What do you think will be a domain of interest? Defang the domain.

Hxxp[://]secure-netcloud[.]com/?a=71&c=76&s1=dadaa&amp

What is the shortened URL? Defang the URL.

Hxxp[://]secure-netcloud[.]com

Do you think this is a phishing email?

Yes, because WhatsApp never send mail, never claim to be a concurrence to Tinder and the emails are not coming from WhatsApp. But mostly all the link goes to secure netcloud that is probably another website that host website so probably scammers make a online server to get information with those links.