

Eml file of email

Source : https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-1030.eml

Headers

Date: Wed, 02 Aug 2023 20:45:14 +0000

Subject: 3rd attempt: You Are Our July Winner Ultimate Nonstick Cookware

To: phishing@pot

From: noreply@costco.com

Return-Path: 7gzye41@oqmhwr.net

Sender IP: 89.144.10.219

Resolve Host: 89-144-10-219.altunhost.com

URLs

hxxps[://]i[.]imgur[.]com/r3tErDX[.]png

http://thebandalisty[.]com/rd/u40160ctlWW22448528lFms49413vFR67002TmWk2845

http://thebandalisty[.]com/rd/c40160pGvPy22448528YPxp49413HPa67002PzOZ2845

Description

This email is claiming to be from “Costco Wholesale Corporation” that the recipient has gotten a reward.

It claims that recipient has been chosen to receive brand new ultimate Nonstick Cookware as a reward.

There are several indication of persuading a recipient through impersonation, along with urgency as it claims the reward offer expire on “August 9, 2023” if not grab the reward by then.

Artifact Analysis

Sender Analysis:

Although claiming to be from Costco Wholesale Corporation, the Return Path header indicate that this email originated form the altunhost.com mail server and also utilized qmhwr.net, neither of them are affiliated with Costco.

If we take a closer look on a email subject, there is a indication of grammatical error in the subject line. I.e(**3rd attempt**)

URL Analysis:

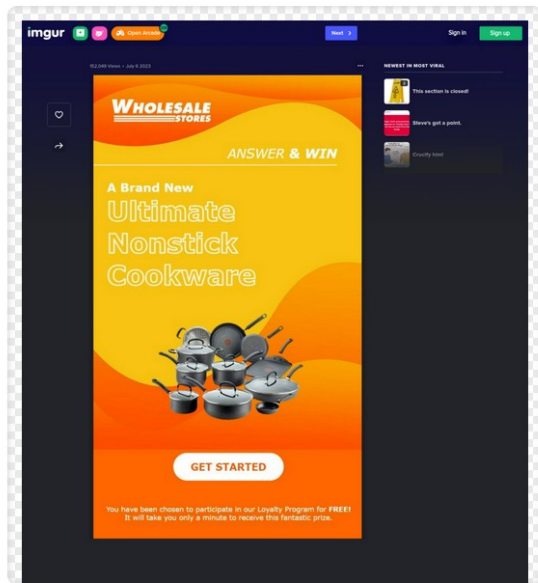
After performing a URL reputation check using URL2PNG and VirusTotal, the URL within the call to action button of this email was found to be malicious, as it redirects to a phishing website. It appears to be hosting a credential capture page, then when submitted, will log and steal the credentials of any victims

Verdict

Due to the original sender being unaffiliated with Amazon, this email is clear impersonation and spoofing attempt.

Additionally, after analyzing the URL contained in the email's call to action, it was flagged on URL2PNG and Virustotal to be malicious.

URL2PNG



http://thebandalisy.com/rd/u40160ctHW2244528Fms43413vFR67002TmWk2845

4 / 97
Community Score

4/97 security vendors flagged this URL as malicious

http://thebandalisy.com/rd/u40160ctHW2244528Fms43413vFR67002TmWk2845
thebandalisy.com
Last Analysis Date
2 months ago

DETECTION DETAILS COMMUNITY

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

Security vendors' analysis

Security vendor	Result	Security vendor	Result
BitDefender	Phishing	Fortinet	Phishing
G-Dat	Phishing	Sophos	Phishing
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BlockList	Clean	Blueliv	Clean

Do you want to automate checks?

https://imgur.com/v3EtDX.png

1 / 97
Community Score

1/97 security vendor flagged this URL as malicious

https://imgur.com/v3EtDX.png
imgur.com
Status
200
Content type
text/html
Last Analysis Date
2 months ago

DETECTION DETAILS COMMUNITY

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

Security vendors' analysis

Security vendor	Result	Security vendor	Result
Phishing Database	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BitDefender	Clean
BlockList	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean

Do you want to automate checks?

Defense Actions

=====

After performing a message trace, no other users within the organization received an email from this sender or with this subject line.

Due to the malicious nature of the domain, I have blocked any incoming emails that contains **"hebandalisty[.]com"** and **"i[.]imgur[.]com"** on the email gateway.

To ensure users are unable to access this malicious URL or domain, I have blocked **"hebandalisty[.]com"** and **"i[.]imgur[.]com"** on the EDR (Endpoint Detection and Response) and on the web Proxy.