N-SECURITY

Artifacts Extracted from Reported Email Investigation Case 1

Business Confidential

Phishing Report

September 09, 2024

Version 1.0

🔒 Confidential

Email Description and Artifacts Collected

This email, originating from an Outlook mailbox and impersonating Amazon with convincing styling, urges the recipient to click a link to reset their password, claiming their account was hacked and used to make a £329.99 purchase. The use of urgency is a common social engineering tactic designed to make the recipient act quickly without considering the situation. The email contains a malicious URL, as the link directs to a non-Amazon domain. This email is classified as malicious / credential harvester.

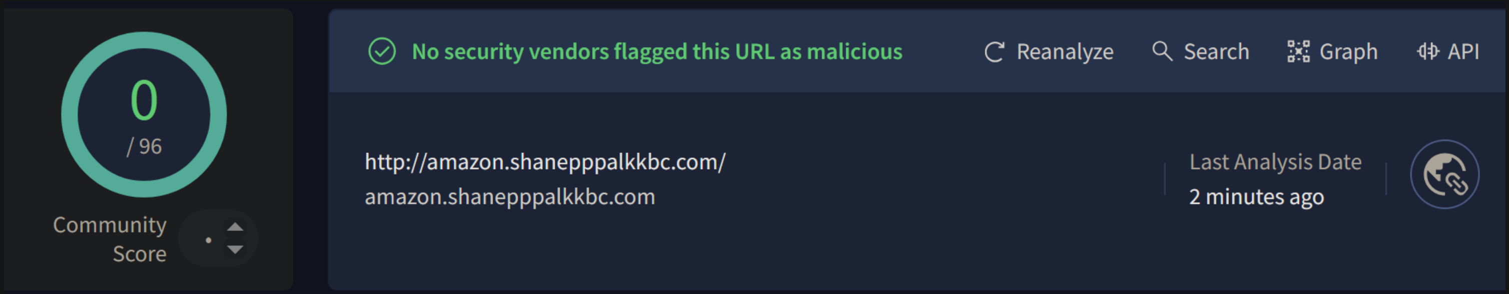
Artifacts	
Email Sender	support@amazon.com
Reply-to Address	no-reply@amazon.co.uk
Subject Line	Suspicious Amazon Order Alert
Date	Thu, 20th October 2023, 9:34:25 -0700
Recipient(s)	jason.s@domain.com
Sending Server IP	40.92.10.10
Reverse DNS	mail-lf1-f91.google.com
URL	hxxp://amazon.shanepppalkkbc[.]com/
File Name(s) + Extension	None
Hash(es)	None

Artifact Analysis

- **URLs**: hxxp://amazon.shanepppalkkbc[.]com/

WHOIS Analysis: A WHOIS search reveals that the domain was registered just 3 days ago, with NameCheap as the registrar. There is no available information about the site owner or domain registrant.

VirusTotal Reputation: A VirusTotal scan of the full URL and root domain indicates no current malicious flags. This is likely due to the domain's recent registration, meaning security engines haven't yet analyzed it.



No security vendors flagged this URL as malicious

http://amazon.shanepppalkkbc.com/
amazon.shanepppalkkbc.com

Last Analysis Date
2 minutes ago

Figure 1: VirusTotal scan result.

URL2PNG Analysis: Using URL2PNG to inspect the link destination, it was found to be hosting a fake Amazon login page designed to steal credentials. The root domain "hxxp://shanepppalkkbc[.]com/" lacks a legitimate homepage, a typical sign of domains used solely for malicious purposes.

Suggested Defensive Measures

[1]	The sending address was successfully spoofing support@amazon.com, however, the sending IP revealed it was a Gmail address, and therefore not from Amazon.
[2]	We are unable to block the sending server IP, as it belongs to Gmail, and would have a negative impact on the business as legitimate emails would be blocked.
[3]	Blocking the sender “support@amazon.com” is also not appropriate, as legitimate emails coming from that address will be blocked.
[4]	I have blocked the subject line on the email gateway, as it is highly unlikely legitimate DHL emails would use it.
[5]	There would be no negative impact to the business, and this action would prevent any more emails in this attack being delivered to employee mailboxes.
[6]	Subject Line Block (Email Gateway) “Suspicious Amazon Order Alert” on 20th October at 12:03 PM by Jane Smith.
[7]	The URL used within the credential harvester is a malicious domain “shanepppalkkbc[.]com” that utilizes a subdomain “amazon” to look more effective when glancing at the link.
[8]	After investigating the domain, it was created purely for malicious purposes, and there is no business justification for employees to visit it, and we can block the entire domain to prevent users from visiting the existing malicious link, or any others that are hosted on the site.
[9]	Domain Block (Web Proxy) “shanepppalkkbc[.]com” on 20th October at 12:03 PM by Jane Smith.

N-SECURITY

Last Page