Phishing Email Analysis Report

1. Basic Information

Analyst Name	Nizar Aderbaz
Date of Analysis	2025-06-19
Email Subject	"*[Binance] Withdraw Successful – 2023-07-30 51 :51 :51(UTC)*"
Sender (From)	Binance <noreply-supportbinancewallet.irs@auswestbc.com.au>
Recipient	*phishing@pot*
Reported By	End user

2. Email Metadata Summary

Message-ID	<01070189a93c67a5-2d72e19a-1525-41c6-92cb-347e9e7f27a5-000000@eu-central-1.amazonses.com>
Return-Path	01070189a93c67a5-2d72e19a-1525-41c6-92cb-347e9e7f27a5-000000@eu-central-1.amazonses.com
Reply-To	None
X-Mailer	PHPMailer 6.1.5
Date Sent	*Sun, 30 Jul 2023 23 :57 :35 +0000*
Received	*from b224-12.smtp-out.eu-central-1.amazonses.com (69.169.224.12) by MW2NAM12FT067.mail.protection.outlook.com (10.13.181.33) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.42 via Frontend Transport ; Sun, 30 Jul 2023 23 :57 :36 +0000*

3. Header Authentication Results

Check	Result	Notes
SPF	PASS	IP is authorized by domain SPF record
DKIM	PASS	Signature verified, message integrity preserved
DMARC	None	No policy found

4. URL & Attachment Analysis

Type	Found	Details
URLs	✓	hxxps[://]shylshom[.]com/ (Phishing, VT : 1/95)
Attachments	✗	None

Note: The embedded URL redirects to a fake login page mimicking a Binance portal.

5. Technical Indicators

IP Address	69.169.224.12 (Known malicious, abuseipdb)
Hosting Country	USA
Domain	auswestbc.com.au (Phishing, VT : 5/94)
Domain Age	2 years
WHOIS Status	Privacy-protected

6. Risk Evaluation

- Phishing Type: Credential Harvesting
- User Impact: High – Targets Binance account credentials
- Delivery Method: Social engineering + fake login page
- Attack Sophistication: Medium To High
- Likelihood of User Click: High – Mimics trusted brand

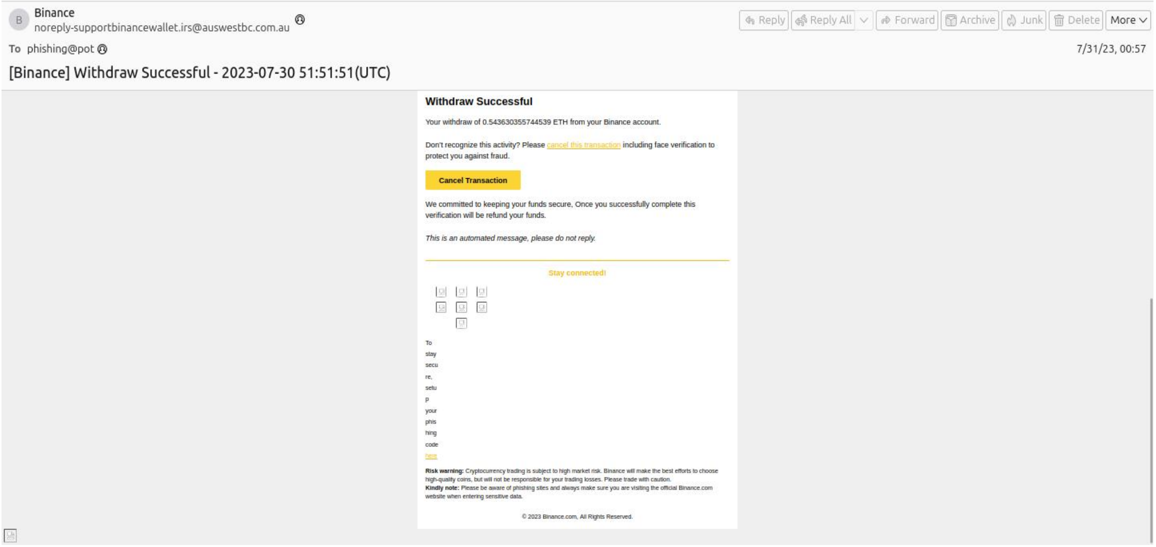
7. Analyst Summary & Recommendation

The email appears to be a phishing attempt using a spoofed sender address to redirect the victim to a fake Binance login page. Although SPF,DKIM checks passed, the sending IP address and the domain are not trusted and do not belong to Binance's official infrastructure. It is recommended :

- Block sending IP and the domain at the firewall and email gateway
- Add URL to phishing blacklist
- Notify affected users and advise password reset
- Submit indicators to threat intelligence systems
- Create detection rules for similar campaigns

8. Attachments

Screenshots of email :



Binance
noreply-supportbinancewallet.irs@auswestbc.com.au

To phishing@pot

7/31/23, 00:57

[Binance] Withdraw Successful - 2023-07-30 51:51:51(UTC)

Withdraw Successful

Your withdraw of 0.543630355744539 ETH from your Binance account.

Don't recognize this activity? Please cancel this transaction including face verification to protect you against fraud.

Cancel Transaction

We committed to keeping your funds secure, Once you successfully complete this verification will be refund your funds.

This is an automated message, please do not reply.

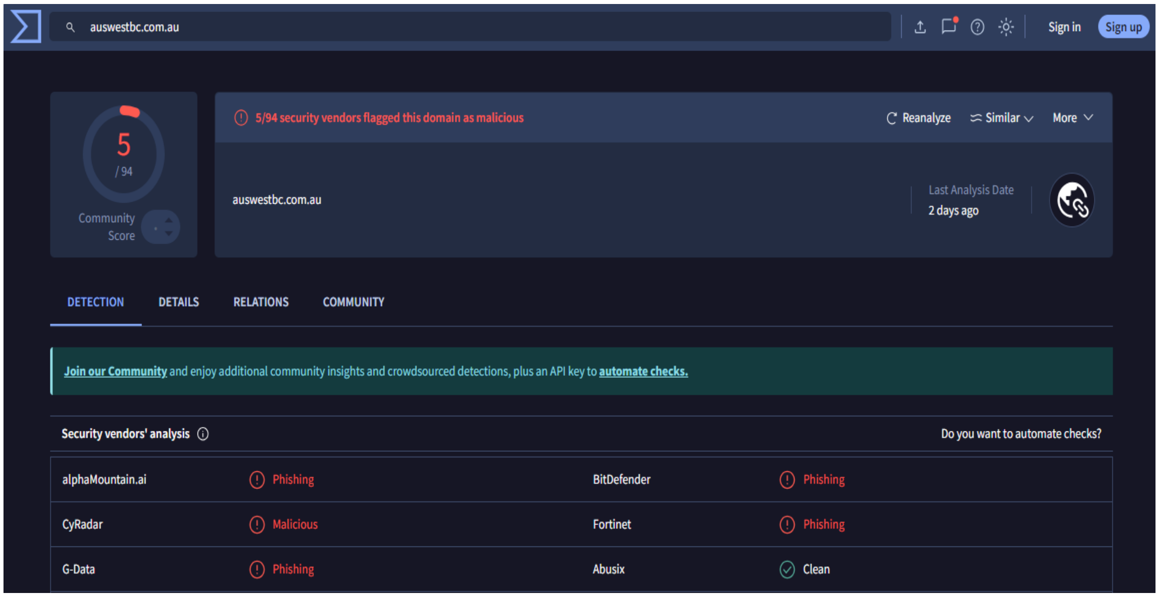
Stay connected!

To stay secu re, setu p your phis hing code here

Risk warning: Cryptocurrency trading is subject to high market risk. Binance will make the best efforts to choose high-quality coins, but will not be responsible for your trading losses. Please trade with caution.
Kindly note: Please be aware of phishing sites and always make sure you are visiting the official Binance.com website when entering sensitive data.

© 2023 Binance.com, All Rights Reserved.

https://www.virustotal.com/gui/domain/auswestbc.com.au



5/94 security vendors flagged this domain as malicious

auswestbc.com.au

Last Analysis Date
2 days ago

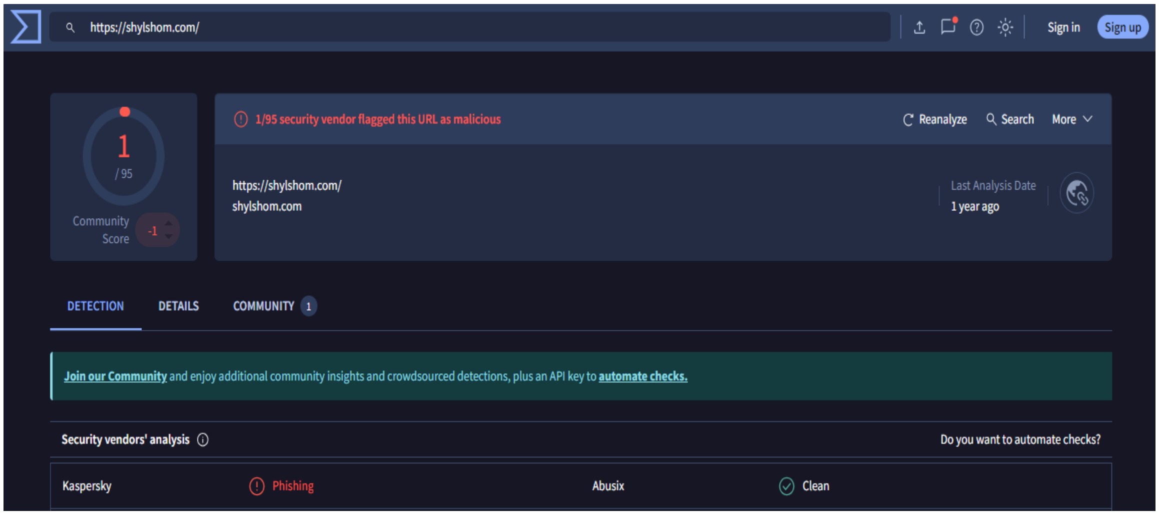
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	BitDefender	Phishing
CyRadar	Malicious	Fortinet	Phishing
G-Data	Phishing	Abusix	Clean

https://www.virustotal.com/gui/url/9de11a58b413c287e1e90aaad58b2fcda434b8cbc3761c54b312556d1493b81a



1/95 security vendor flagged this URL as malicious

https://shylshom.com/
shylshom.com

Last Analysis Date
1 year ago

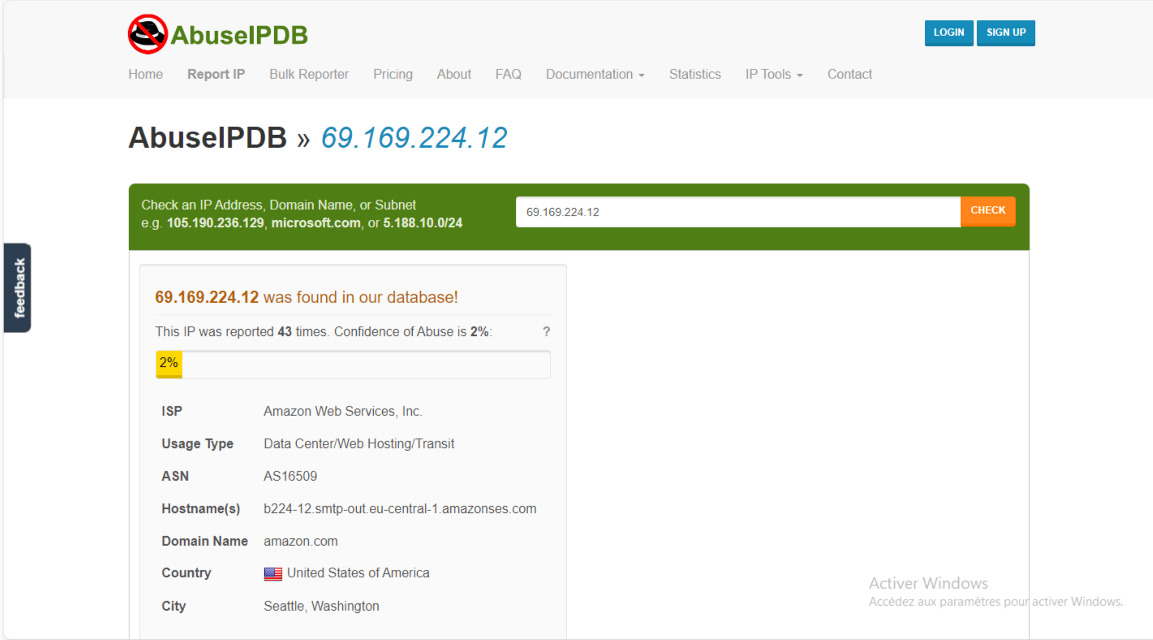
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Kaspersky	Phishing	Abusix	Clean

https://www.abuseipdb.com/check/69.169.224.12



AbuseIPDB » 69.169.224.12

Check an IP Address, Domain Name, or Subnet
e.g. 105.190.236.129, microsoft.com, or 5.188.10.0/24

69.169.224.12

69.169.224.12 was found in our database!

This IP was reported 43 times. Confidence of Abuse is 2%: ?

2%

ISP	Amazon Web Services, Inc.
Usage Type	Data Center/Web Hosting/Transit
ASN	AS16509
Hostname(s)	b224-12.smtp-out.eu-central-1.amazonses.com
Domain Name	amazon.com
Country	United States of America
City	Seattle, Washington