

Phishing Email Analysis Report

1. Summary

This report provides a detailed analysis of a suspected phishing email with the subject 'Re: Congratulations! Order Verification - AirPods'. The email attempts to impersonate Walmart and lure the user with a fake reward to click on a malicious link.

Subject: Re: Congratulations! Order Verification - AirPods

To: (phishing@pot)

From: AirPods Unlocked

From Address: ksbda@intersho.com

Date: 06/11/2022, 23:49:48

[Final Notice Coming for a AirPods Reward](#)

Walmart 








ANSWER
&WIN
A Brand New

2. Email Metadata

[Uploads](#) > [Re: Congratulations! Order Verification - AirPods](#)

Re: Congratulations! Order Verification - AirPods

 [Details](#) [Authentication](#) [URLs](#) [Attachments](#) [Transmission](#) [X-headers](#)

 From	 ksbda@intersho.com	...
Display name	AirPods Unlocked	
Sender	None	
To	phishing@pot	
Cc	None	
In-Reply-To	DM4PR19MB6317A7801126BBD236418D0EB3389@intersho.com	
Timestamp	2022-11-06T23:49:48Z	
 Reply-To	 newsletter@intersho.com	...
Message-ID	<2ca04292-69a9-4604-b558-3d302edd5f91@MW2NAM12FT070.eop-nam12.prod.protection.outlook.com>	
 Return-Path	 weyly@pjhpe.com	...
Originating IP	 103.167.154.165 (Hop 1) ▼	...
rDNS	None	

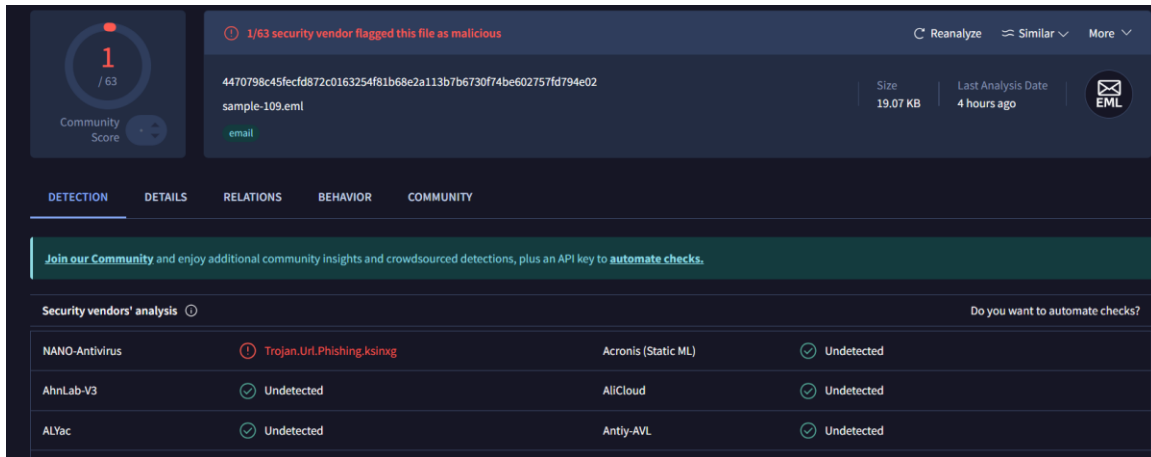
-
- Subject: Re: Congratulations! Order Verification - AirPods
 - From: AirPods Unlocked <ksbda@intersho.com>
 - To: phishing@pot
 - Date: 2022-11-06T23:49:48Z
 - Reply-To: newsletter@intersho.com
 - Return-Path: weyly@pjhpe.com
 - IP: 103.167.154.165 (No rDNS)

3. Key Phishing Indicators

- Spoofed Sender Email:
 - Domain `intersho.com` has no SPF, DMARC, or MX records
 - Trust score: 0/100, Spoofable: True
- Header Discrepancies:
 - Return-path domain and sender domain mismatch
 - No reverse DNS for originating IP
- Suspicious Links and Attachments:
 - Link text: 'Final Notice Coming for a AirPods Reward'
 - Likely phishing URL behind legitimate branding (Walmart)
- Urgency or Manipulative Language:
 - Terms like 'Final Notice' and 'Congratulations'
- Brand Impersonation:
 - Walmart logo used without permission or verification
- Spelling or Grammar Errors:
 - 'a AirPods Reward' is grammatically incorrect

4. VirusTotal Scan Result

- File: sample-109.eml
- Detection: 1/63 vendors flagged as malicious
- Detection Name: Trojan.Url.Phishing.ksinxg (by NANO-Antivirus)



The image shows a VirusTotal scan result for a file named 'sample-109.eml'. The file is 19.07 KB and was analyzed 4 hours ago. The scan shows that 1 out of 63 security vendors flagged the file as malicious. The detection name is 'Trojan.Url.Phishing.ksinxg' by NANO-Antivirus. Other vendors like AhnLab-V3, ALYac, Acronis (Static ML), AllCloud, and Antiy-AVL all reported the file as 'Undetected'. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. A banner encourages joining the community for more insights and an API key to automate checks.

Security vendors' analysis				Do you want to automate checks?
NANO-Antivirus	🚫 Trojan.Url.Phishing.ksinxg	Acronis (Static ML)	✅ Undetected	
AhnLab-V3	✅ Undetected	AllCloud	✅ Undetected	
ALYac	✅ Undetected	Antiy-AVL	✅ Undetected	

5. Email Reputation Check

Detailed analysis of the sender domain shows multiple red flags.

Report Summary	
Email Address	Ksbda@intersho.com
Should Block	True
Trust Score	0 / 100
Valid Format	True
Username	Ksbda
Role Address	False
Suspicious Username	False
Dirty Words Username	False
Domain	Intersho.com

6. Conclusion & Recommendations

Based on the collected evidence and analysis, this email is confirmed to be a phishing attempt. The spoofed sender, deceptive content, and malicious intent are clear indicators.

- Do NOT click on any links or respond to the email.
- Block and report the domain `intersho.com`.
- Submit the email to anti-phishing services (e.g., VirusTotal, PhishTank).
- Educate users on phishing indicators and email hygiene.