

# Project 5 Phishing Report

## Email Description

The email is a promotional leaflet for discounted “miracle weight loss” bottle without exercises. This is a real phishing email that I regularly receive in my personal mail box.

## Email Artifacts

**Sending Address :** Breaking News FRI <[hongmon033@gmail.com](mailto:hongmon033@gmail.com)>

**Subject Line :** Re: hoamiadasfhkja, YES... No\_Exercise No\_Diet\_

**Recipients :** [ixxx@xxxxxxxx.com](mailto:ixxx@xxxxxxxx.com) —> my mail box

**Sending Server IP :** 209.85.128.171

**Reverse DNS :** mail-ywl-f171.google.com

**Reply-To :** None

**Date and Time :** Sun, 16 Jul 2023 11:18:31 +0000

## Web Artifacts

**Full URL (sanitized):** [hxxps://link.scsend.net/AeU7?](https://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff)

[recipient\\_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!](https://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff)

[XOI8n9moA!d=14283\\_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!](https://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff)

[498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!](https://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff)

[0g6lgUJEhiGTYmQYxdM4xQMgyff](https://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff)

**Root Domain:** [hxxps://link.scsend.net](https://link.scsend.net)

**Effective Root Domain :** [hxxp://launchpad.adsolary.com/cl!XOI8n9moA!](https://launchpad.adsolary.com/cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL)

[d=14283\\_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!](https://launchpad.adsolary.com/cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL)

[o=4589!ln9AsyDUKYJL](https://launchpad.adsolary.com/cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL)

## Investigation

**WHOIS :** Scanning the effective root, domain tool have found as the register url [AdSoLary.com](https://www.whois.com/whois/AdSoLary.com) created 51 days with an IP : 109.94.208.5

**URL2SCAN.IO :** Scanning the full URL showed another effective url : <http://launchpad.adsolary.com>. Rescanning the new URL showed that creation of this url was 51 days ago. This website contacted 3 IPs in 3 countries across 3 domains to perform 16 HTTP transactions. The main IP is the matched [AdSoLary.com](https://www.whois.com/whois/AdSoLary.com) IP: 109.94.208.5, located in London, United Kingdom and belongs to RETN-AS, GB.

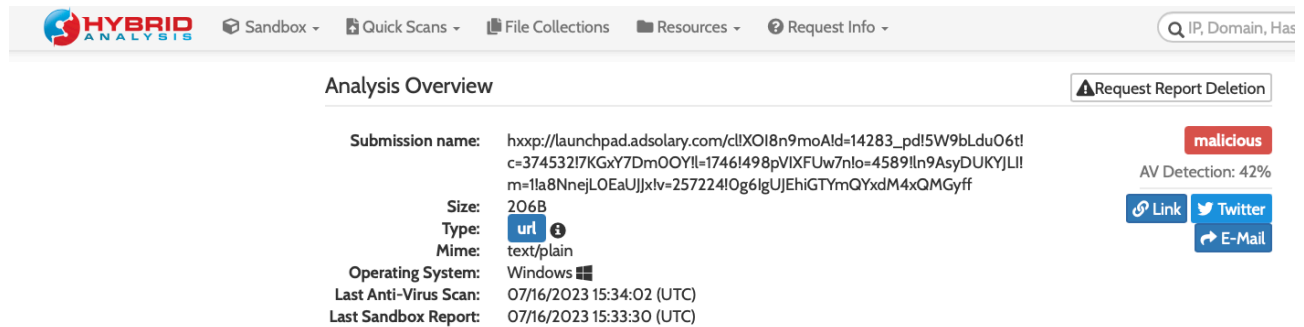
**VirusTotal :** Scanning the Full URL, I have noticed it only scanning part of the URL : [hxxps://link.scsend.net/AeU7?](https://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff)

[recipient\\_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#](https://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff) but not the rest of the URL (I WANDER WHY) [cl!XOI8n9moA!d=14283\\_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff](https://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJL!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff)

Scanning <http://launchpad.adsolary.com/> did not show any security flags.  
Scanning <http://adsolary.com/> also did not show any security flags.

**URL2PNG** : Out of the 3 URLs, on <http://adsolary.com/> has a web page.

**HYBRID ANALYSIS** : HYBRID ANALYSIS did not show threat to all URL except this URL : [http://launchpad.adsolary.com/cl!XOI8n9moA!d=14283\\_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!!=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJLI!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTymQYxdM4xQMgyff](http://launchpad.adsolary.com/cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!!=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJLI!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTymQYxdM4xQMgyff) has shown an 94% from ScamAdviser confirming my gut as Malicious.



The screenshot shows the Hybrid Analysis web interface. At the top, there's a navigation bar with 'Sandbox', 'Quick Scans', 'File Collections', 'Resources', and 'Request Info'. A search bar on the right says 'Q IP, Domain, Has'. Below this is the 'Analysis Overview' section. It displays the submission name as the long URL, size as 206B, type as 'url', and mime as 'text/plain'. The operating system is 'Windows'. The last anti-virus scan and sandbox report are both dated 07/16/2023. On the right, a red 'malicious' badge is shown, along with 'AV Detection: 42%' and social media links for Link, Twitter, and E-Mail.

## Defensive measure

[1] The sending IP revealed it was actually from a Gmail address. [2]

Therefore ,blocking the sending server would have a negative impact as legitimate emails would be blocked.

**[ActionTaken]** - Block for the sending address “honmon033@gmail.com“ by Idriss JAMA on the 16 July 2023.

[4] The URLs was purely recently create for Phishing/Malicious activities purpose although NOT flagged by VirusTotal. But the half scanned url Scanning was suspicious to me. There are 2 URLs <http://launchpad.adsolary.com/AdSoLary.com> who shares the same IP Address, was created 51 days ago and located in London,UK.

[5] Therefore, there is no justification for users (My Family) to visit it, and we can block the entire domain to prevent employees from visiting .

**[ActionTaken]** - Block for the domain(web proxy):

- <http://link.scent.net>
- [http://link.scsend.net/AeU7?recipient\\_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283\\_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!!=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJLI!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTymQYxdM4xQMgyff](http://link.scsend.net/AeU7?recipient_id=14cTNqpFVPgVUO0T9RrdVKbuSz36b39dt0vcIDQqIIQG4#cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!!=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJLI!m=!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTymQYxdM4xQMgyff)
- <http://launchpad.adsolary.com/>

- [hxxp://launchpad.adsolary.com/cl!XOI8n9moA!d=14283\\_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJLI!m=1!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff](http://launchpad.adsolary.com/cl!XOI8n9moA!d=14283_pd!5W9bLdu06t!c=374532!7KGxY7Dm0OY!l=1746!498pVIXFUw7n!o=4589!ln9AsyDUKYJLI!m=1!a8NnejL0EaUJjx!v=257224!0g6lgUJEhiGTYmQYxdM4xQMgyff)
- <http://adsolary.com/>

### **The investigating analyst**

- The headline “Breaking News” from the sender raises Suspicious to me, the Subject line suggests this email was forwarded.
- These 2 URLs <http://launchpad.adsolary.com/AdSoLary.com> shares the same IP Address, was created 51 days ago and located in London,UK.
- To prevent any further malicious emails from this sender, the address has been blocked.
- All URLs has been also blocked because of the result HYBRIS ANALYSIS classify as Malicious.
- The domain associated with the URLs was intentionally created for malicious purposes, and there is no valid reason to revisit it.
- As a precautionary measure, the sender and the URLs were blocked by Idriss Jama on July 16, 2023.