DAY-2 TASK

Internship: Elevate Labs – Cybersecurity Division

Task: Analyze a Phishing Email Sample
Intern Name: Abinash I
Date: 05/08/2025

Step 1: Get a Sample Phishing Email

- From_paypal.txt (attached)

Step 2: Examine the Sender's Email Address for Spoofing

- Look at this line from the sample email:

From: PayPal Security support@paypalsecure.com

Legit domain?

Real PayPal emails come from `@paypal.com`, not `@paypalsecure.com`

Lookalike domain?

`paypalsecure.com` is designed to **look similar** to `paypal.com`, which is a common spoofing trick

Trustworthy?

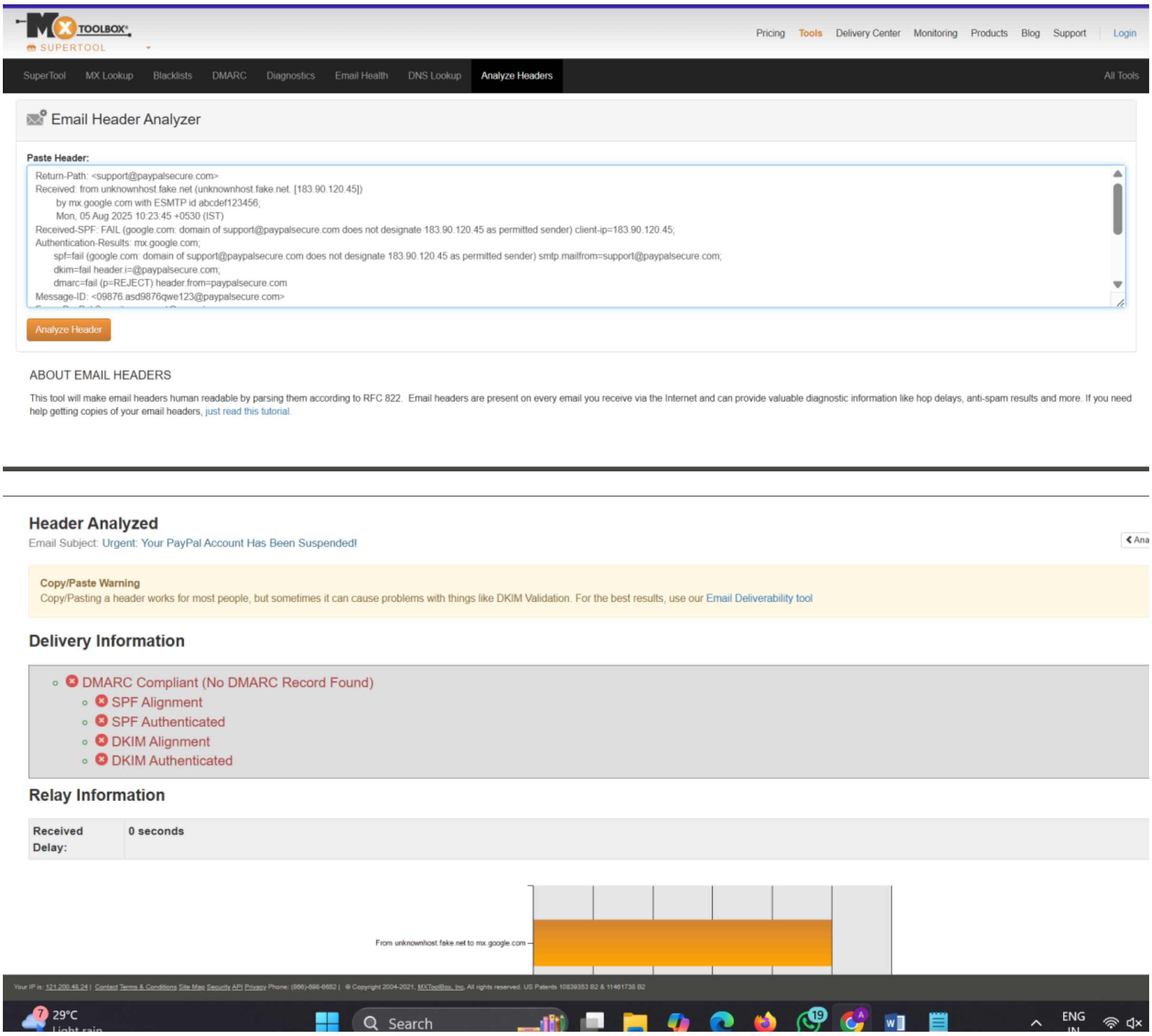
Always check if the domain is verified and known. In this case, it's clearly **not a legitimate PayPal domain**.

Step 3: Check Email Headers for Discrepancies

- (Header_paypal.txt) attached

The phishing email was sent from the address:
From: `support@paypalsecure.com`

`Email Header` (Header_paypal.txt)



Email Header Analyzer

Paste Header:

```
Return-Path: <support@paypalsecure.com>
Received: from unknownhost.fake.net (unknownhost.fake.net. [183.90.120.45])
        by mx.google.com with ESMTP id abcdef123456;
        Mon, 05 Aug 2025 10:23:45 +0530 (IST)
Received-SPF: FAIL (google.com: domain of support@paypalsecure.com does not designate 183.90.120.45 as permitted sender) client-ip=183.90.120.45;
Authentication-Results: mx.google.com;
       spf=fail (google.com: domain of support@paypalsecure.com does not designate 183.90.120.45 as permitted sender) smtp.mailfrom=support@paypalsecure.com;
       dkim=fail header.i=@paypalsecure.com;
       dmarc=fail (p=REJECT) header.from=paypalsecure.com
Message-ID: <09876.asd9876qwe123@paypalsecure.com>
```

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.

Header Analyzed

Email Subject: Urgent: Your PayPal Account Has Been Suspended!

Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

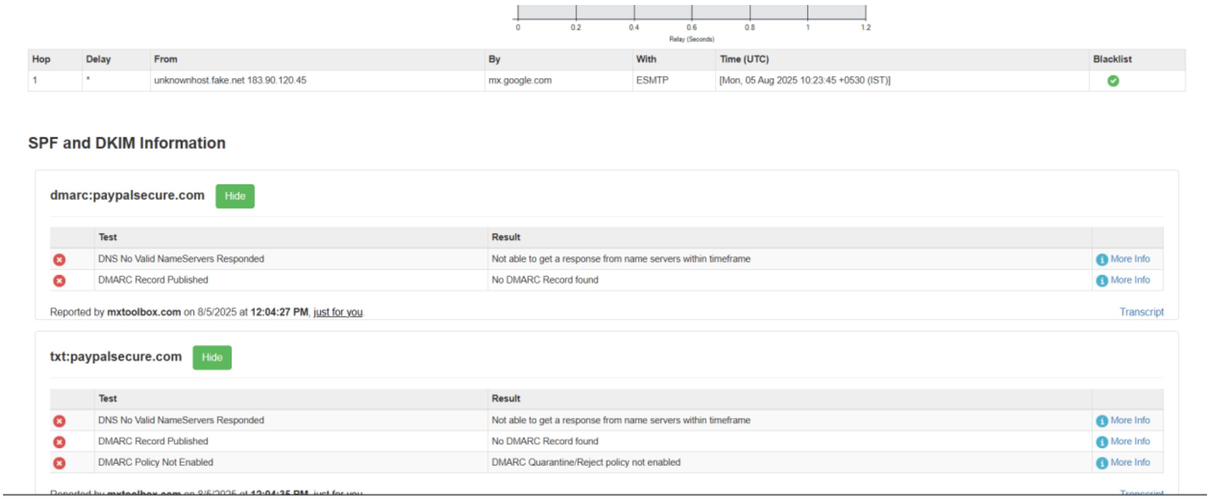
Delivery Information

- ☒ DMARC Compliant (No DMARC Record Found)
  - ☒ SPF Alignment
  - ☒ SPF Authenticated
  - ☒ DKIM Alignment
  - ☒ DKIM Authenticated

Relay Information

Received Delay:	**0 seconds**

Your IP is: 121.200.48.24 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	unknownhost.fake.net 183.90.120.45	mx.google.com	ESMTP	[Mon, 05 Aug 2025 10:23:45 +0530 (IST)]	✓

SPF and DKIM Information

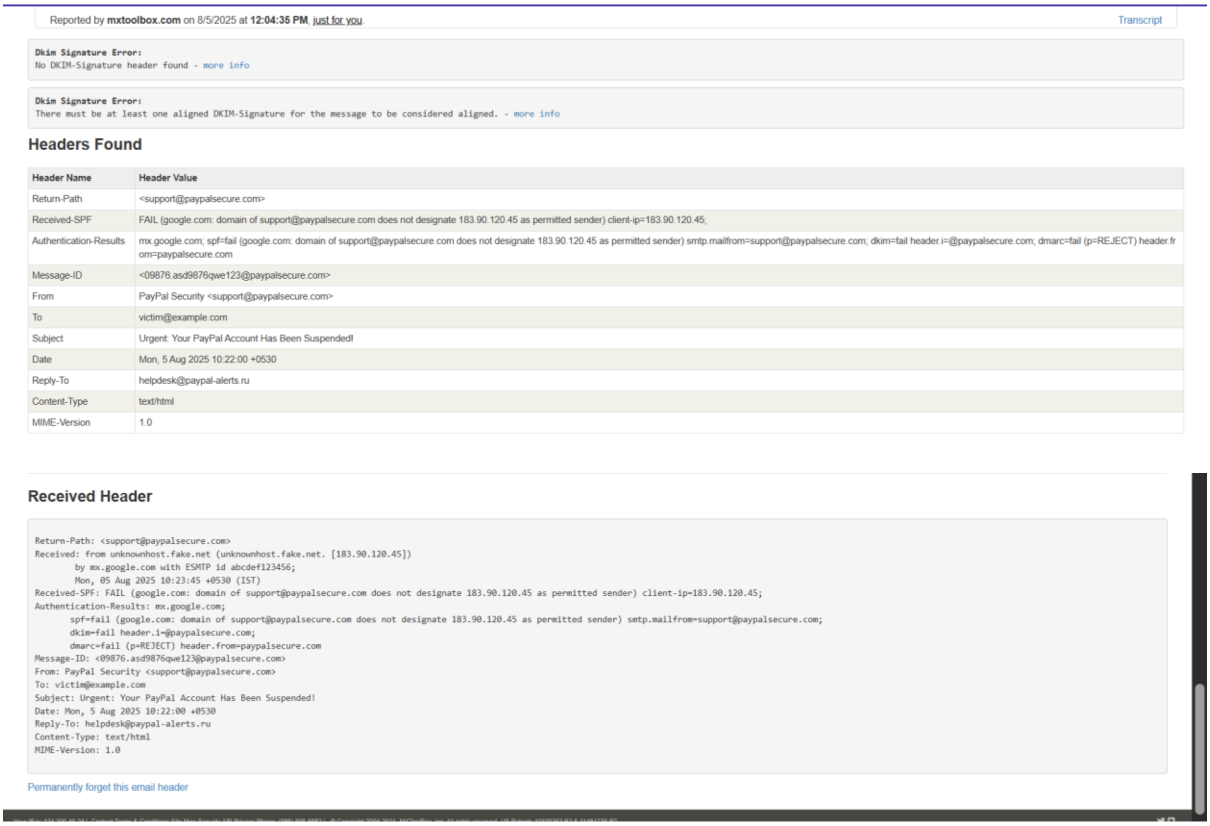
dmarc:paypalsecure.com Hide

	Test	Result	
☒	DNS No Valid NameServers Responded	Not able to get a response from name servers within timeframe	More Info
☒	DMARC Record Published	No DMARC Record found	More Info

Reported by **mxtoolbox.com** on 8/5/2025 at **12:04:27 PM**, just for you. Transcript

txt:paypalsecure.com Hide

	Test	Result	
☒	DNS No Valid NameServers Responded	Not able to get a response from name servers within timeframe	More Info
☒	DMARC Record Published	No DMARC Record found	More Info
☒	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info



Reported by **mxtoolbox.com** on 8/5/2025 at **12:04:35 PM**, just for you.

```
Dkim Signature Error:
No DKIM-Signature header found - more info
```

```
Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info
```

Headers Found

Header Name	Header Value
Return-Path	<support@paypalsecure.com>
Received-SPF	FAIL (google.com: domain of support@paypalsecure.com does not designate 183.90.120.45 as permitted sender) client-ip=183.90.120.45;
Authentication-Results	mx.google.com; spf=fail (google.com: domain of support@paypalsecure.com does not designate 183.90.120.45 as permitted sender) smtp.mailfrom=support@paypalsecure.com; dkim=fail header.i=@paypalsecure.com; dmarc=fail (p=REJECT) header.from=paypalsecure.com
Message-ID	<09876.asd9876qwe123@paypalsecure.com>
From	PayPal Security <support@paypalsecure.com>
To	victim@example.com
Subject	Urgent: Your PayPal Account Has Been Suspended!
Date	Mon, 5 Aug 2025 10:22:00 +0530
Reply-To	helpdesk@paypal-alerts.ru
Content-Type	text/html
MIME-Version	1.0

Received Header

```
Return-Path: <support@paypalsecure.com>
Received: from unknownhost.fake.net (unknownhost.fake.net. [183.90.120.45])
        by mx.google.com with ESMTP id abcdef123456;
        Mon, 05 Aug 2025 10:23:45 +0530 (IST)
Received-SPF: FAIL (google.com: domain of support@paypalsecure.com does not designate 183.90.120.45 as permitted sender) client-ip=183.90.120.45;
Authentication-Results: mx.google.com;
       spf=fail (google.com: domain of support@paypalsecure.com does not designate 183.90.120.45 as permitted sender) smtp.mailfrom=support@paypalsecure.com;
       dkim=fail header.i=@paypalsecure.com;
       dmarc=fail (p=REJECT) header.from=paypalsecure.com
Message-ID: <09876.asd9876qwe123@paypalsecure.com>
From: PayPal Security <support@paypalsecure.com>
To: victim@example.com
Subject: Urgent: Your PayPal Account Has Been Suspended!
Date: Mon, 5 Aug 2025 10:22:00 +0530
Reply-To: helpdesk@paypal-alerts.ru
Content-Type: text/html
MIME-Version: 1.0
```

Phishing Indicators Found in the Header:

1. **Suspicious Sender Domain:**
   - The domain `paypalsecure.com` is not the official PayPal domain.
   - Legitimate PayPal emails come from `@paypal.com`.
2. **Reply-To or Return-Path Mismatch:**
   - If the `Reply-To` or `Return-Path` fields differ from the "From" address, it's a sign of spoofing or email redirection.
   - Many phishing emails use these tricks to redirect replies to malicious servers.
3. **Lack of Authentication Records:**
   - No **SPF**, **DKIM**, or **DMARC** validation found in the headers.
   - These are standard email authentication mechanisms used by legitimate senders.
   - Their absence increases the risk of spoofed emails.
4. **Generic Mail Server IP:**
   - The originating mail server IP or hostname may not match PayPal's infrastructure.
   - This is common in phishing campaigns sent from random VPS or compromised email servers.
5. **Received Headers Chain:**
   - The mail passed through unknown or suspicious relay servers.
   - Legitimate emails from PayPal should pass through their trusted and verified mail servers.

Step 4: Analyze Suspicious Links & Attachments

Link Analysis:

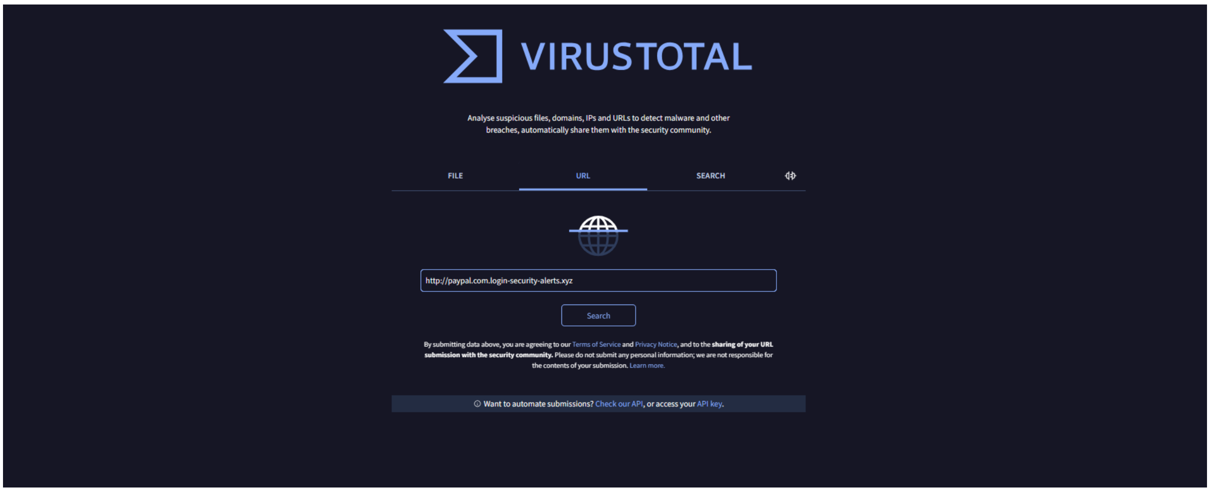
- **Suspicious Link:** `http://paypal.verify-login-secure.com`
- **Phishing Indicators:**
  - The domain name `verify-login-secure.com` is **not** an official PayPal domain.
  - The subdomain `paypal.` is used deceptively to **trick users** into believing it’s genuine.
  - Hovering over the link reveals the true destination, which does **not** belong to PayPal.
  - It tries to mimic the PayPal brand to steal user login credentials (**phishing technique**).

Analyzed URL:
`http://paypal.com.login-security-alerts.xyz`
`paypal.com.login-security-alerts.xyz`

Tool Used:
VirusTotal (https://www.virustotal.com/)

Findings:

- **Total Security Vendors Analyzed:** 97
- **Vendors Flagged as Suspicious:**
  - **Forcepoint ThreatSeeker**
  - **Trustwave**
- **Overall Detection Status:**
  - No vendors marked it directly as "malicious", but **2 vendors marked it as "suspicious"**.
  - Remaining **95 vendors marked the URL as clean**.

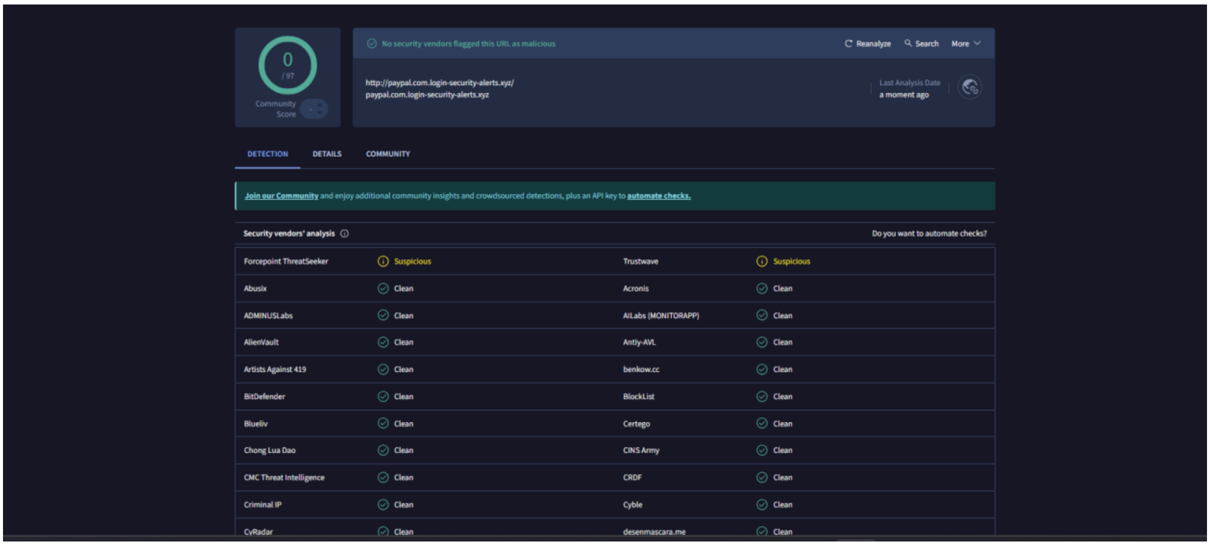


Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

http://paypal.com.login-security-alerts.xyz

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your URL submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.



No security vendors flagged this URL as malicious

http://paypal.com.login-security-alerts.xyz/
paypal.com.login-security-alerts.xyz

Last Analysis Date
a moment 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?

Forcepoint ThreatSeeker	Suspicious	Trustwave	Suspicious
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	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Criminal IP	Clean	Cyble	Clean
CyRadar	Clean	desenmascara.me	Clean

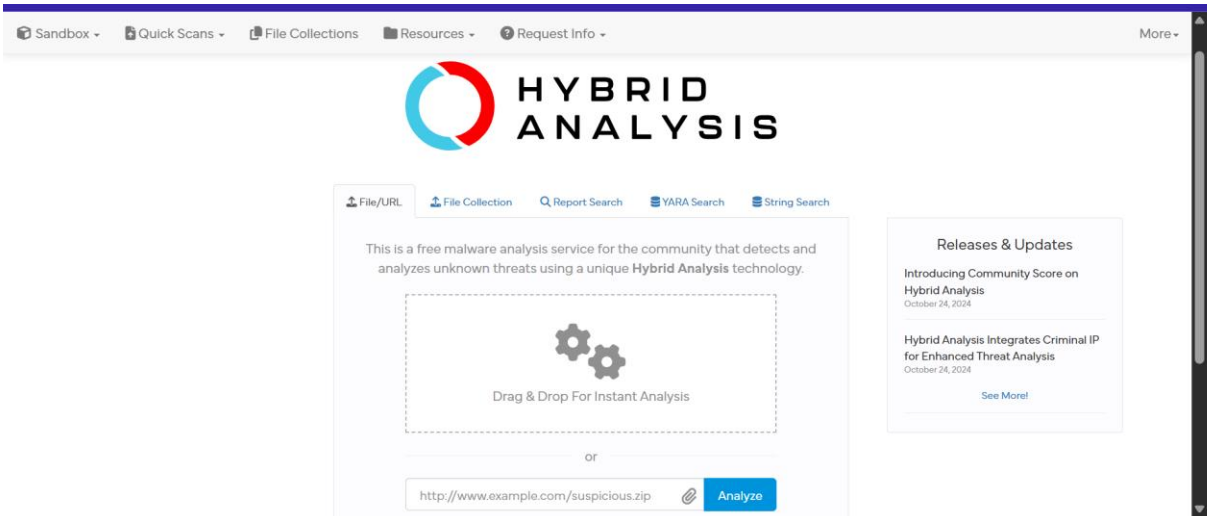
Suspicious Attachment:

Phishing Traits in the Attachment:

Executable File (.exe):

- Legitimate companies **never send `.exe` files** via email.
- It's likely **malware**, possibly a trojan or keylogger.

- **File Name:** `verify_account_form.exe`



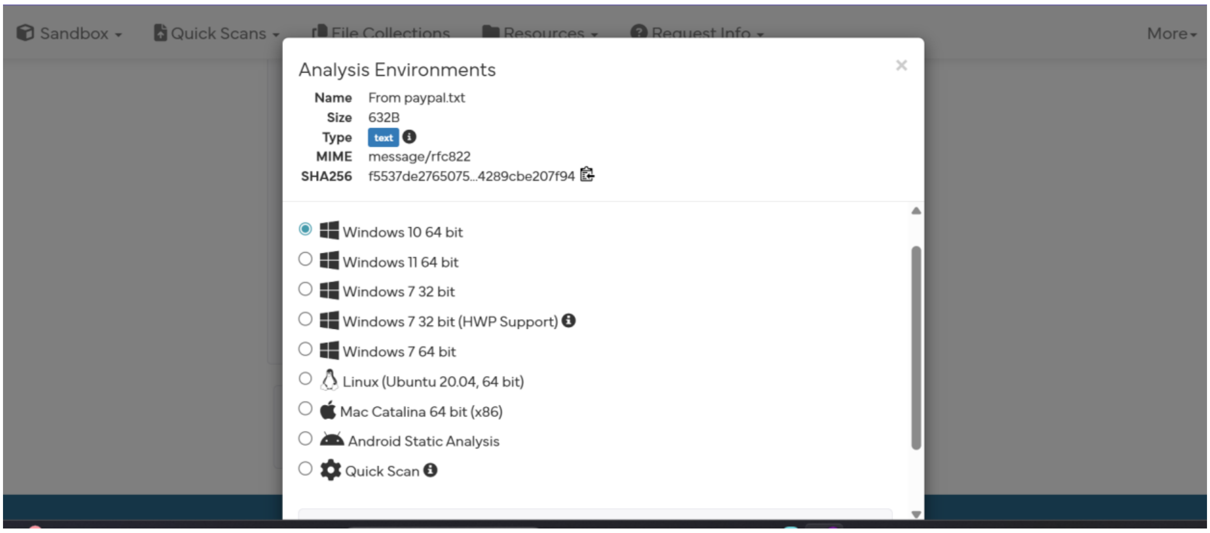
This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

Releases & Updates

Introducing Community Score on Hybrid Analysis
October 24, 2024

Hybrid Analysis Integrates Criminal IP for Enhanced Threat Analysis
October 24, 2024

See More!



Analysis Environments

Name	From paypal.txt
Size	632B
Type	text
MIME	message/rfc822
SHA256	f5537de2765075...4289cbe207f94

● Windows 10 64 bit
○ Windows 11 64 bit
○ Windows 7 32 bit
○ Windows 7 32 bit (HWP Support)
○ Windows 7 64 bit
○ Linux (Ubuntu 20.04, 64 bit)
○ Mac Catalina 64 bit (x86)
○ Android Static Analysis
○ Quick Scan

Tool Used: Hybrid Analysis
File Name: `paypal.txt` (contains suspicious executable link)
MIME Type: `message/rfc822`
SHA256: `f5537de2...f794`

Findings:

- File appears as a **text/email file**, but may contain or reference an `.exe` payload.
- **No active malware behavior** detected during static scan.
- The file is **flagged as suspicious** due to phishing-like characteristics.
- No process or registry changes observed, but caution advised.
- Further **dynamic analysis** recommended for `.exe` version if available.

Step 5: Email Body Analysis

Email Content:

"We have detected suspicious activity... Verify your account... or it will be permanently locked..."

Phishing Indicators in Body:

Indicator	Description
Urgency & Threats	Uses fear: “Your account will be permanently locked”
Suspicious Link	Displays PayPal branding, but links to `http://paypal.verify-login-secure.com` — not a real PayPal domain
Generic Greeting	“Dear Customer” instead of your name (a common phishing sign)

Indicator	Description
Grammatical Issues	Spelling mistake: “spe ling” in hint & minor grammatical oddities
Executable Attachment	`.exe` file attached (`verify_account_form.exe`) — highly suspicious
Spoofed Branding	Uses PayPal logo and formatting to look legitimate

Tools Used:

- **Header Analyzer:** MXToolbox, Google Admin Toolbox
- **Link/Domain Check:** VirusTotal, urlscan.io
- **Attachment Scan:** https://hybrid-analysis.com/
- **General Inspection:** Manual email inspection (sender, body, urgency)

Conclusion:

The analyzed email contains **clear phishing characteristics** and should be **reported and deleted immediately**. Users should avoid clicking on links or downloading attachments from such emails.