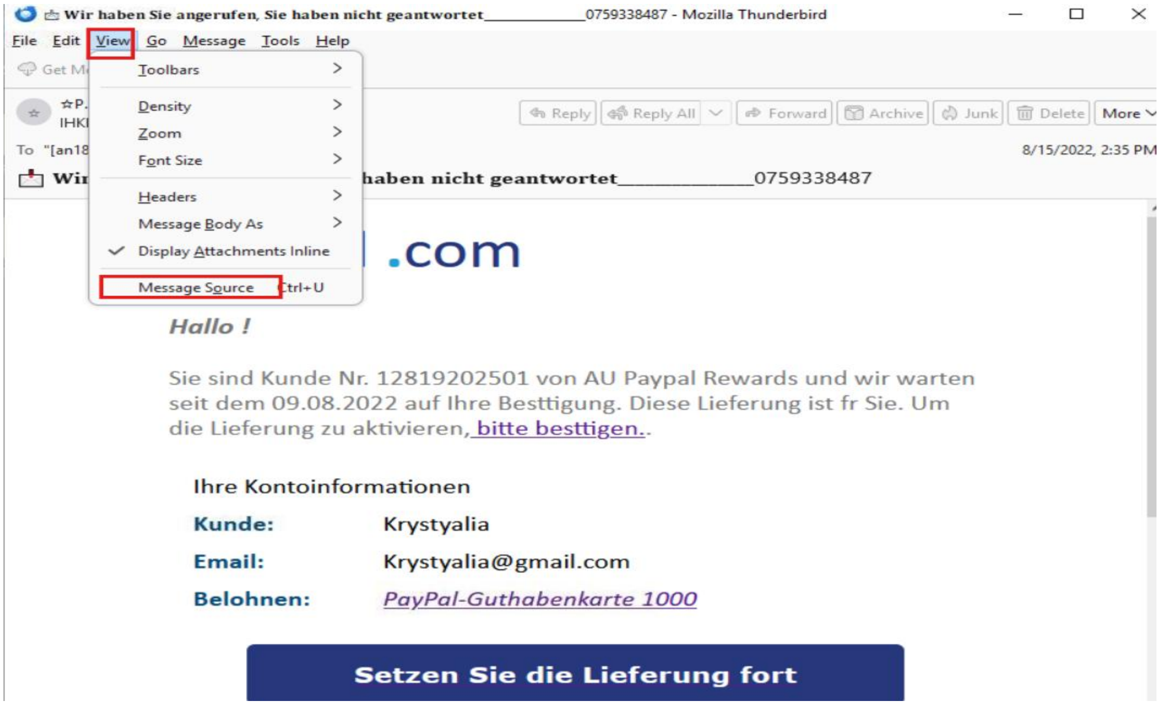
Phishing Email Writeup [LetsDefend]

Your email address has been leaked and you receive an email from Paypal in German. Try to analyze the suspicious email.

File location: C:\Users\LetsDefend\Desktop\Files\PhishingChallenge.zip Password: infected

| Start Investigation:

Q1: What is the return path of the email?



Hallo !

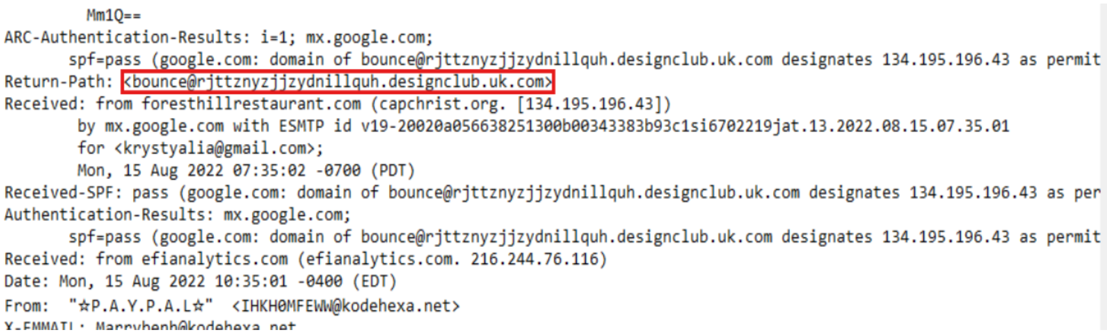
Sie sind Kunde Nr. 12819202501 von AU Paypal Rewards und wir warten seit dem 09.08.2022 auf Ihre Besttigung. Diese Lieferung ist fr Sie. Um die Lieferung zu aktivieren, bitte besttigen..

Ihre Kontoinformationen

Kunde:	Krystyalia
Email:	Krystyalia@gmail.com
Belohnen:	*PayPal-Guthabenkarte 1000*

Setzen Sie die Lieferung fort

At the beginning of the analysis, I wanted to know more details, so I went to View --> Message Source.

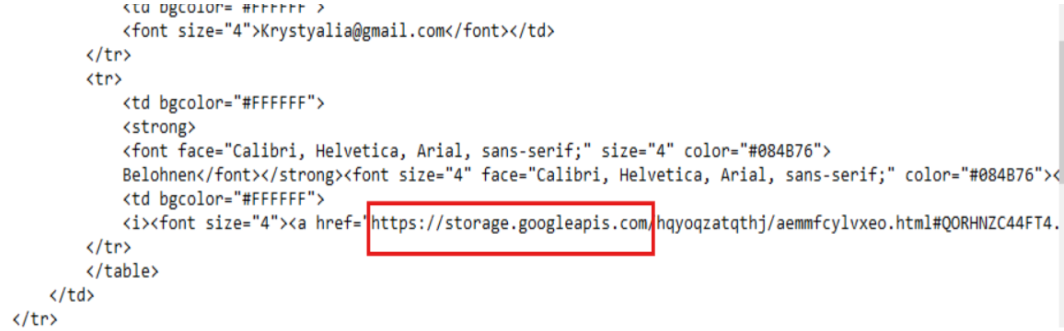


```
         Mm1Q==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: domain of bounce@rjttznyzjjzydnillquh.designclub.uk.com designates 134.195.196.43 as permit
Return-Path: <bounce@rjttznyzjjzydnillquh.designclub.uk.com>
Received: from foresthillrestaurant.com (capchrist.org. [134.195.196.43])
        by mx.google.com with ESMTP id v19-20020a056638251300b00343383b93c1si6702219jat.13.2022.08.15.07.35.01
        for <krystyalia@gmail.com>;
        Mon, 15 Aug 2022 07:35:02 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce@rjttznyzjjzydnillquh.designclub.uk.com designates 134.195.196.43 as per
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of bounce@rjttznyzjjzydnillquh.designclub.uk.com designates 134.195.196.43 as permit
Received: from efianalytics.com (efianalytics.com. 216.244.76.116)
Date: Mon, 15 Aug 2022 10:35:01 -0400 (EDT)
From:  "☆P.A.Y.P.A.L☆"  <IHKH0MFEWW@kodehexa.net>
X-EMMAIL: Marryhenh@kodehexa.net
```

Then I searched for the return path to find the email.

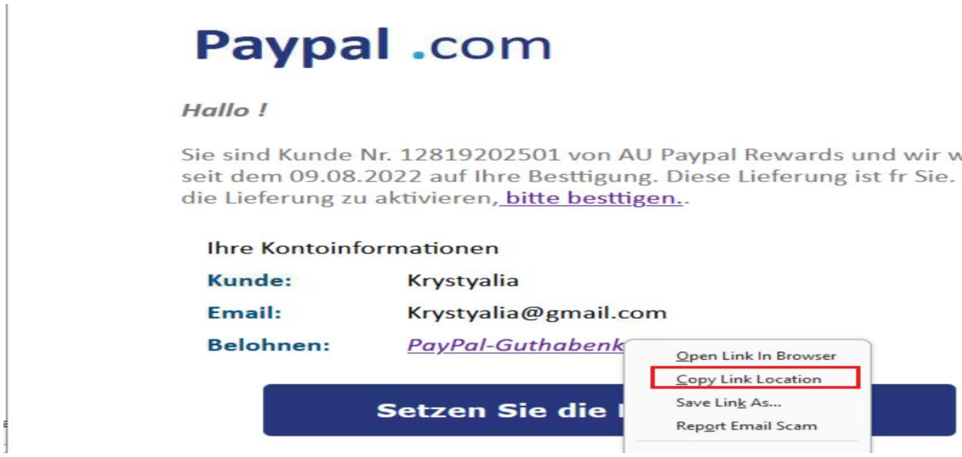
Answer: bounce@rjttznyzjjzydnillquh.designclub.uk.com**.**

Q2: What is the domain name of the url in this mail?



```
            <td bgcolor="#FFFFFF">
            <font size="4">Krystyalia@gmail.com</font></td>
        </tr>
        <tr>
            <td bgcolor="#FFFFFF">
            <strong>
            <font face="Calibri, Helvetica, Arial, sans-serif;" size="4" color="#084B76">
            Belohnen</font></strong><font size="4" face="Calibri, Helvetica, Arial, sans-serif;" color="#084B76"><
            <td bgcolor="#FFFFFF">
            <i><font size="4"><a href='https://storage.googleapis.com/hqyoqzatqthj/aemmfcylvxeo.html#QORHNZC44FT4.
        </tr>
        </table>
    </td>
</tr>
```

By scrolling down, I got the URL. And there's another way to find it.



Hallo !

Sie sind Kunde Nr. 12819202501 von AU Paypal Rewards und wir warten seit dem 09.08.2022 auf Ihre Besttigung. Diese Lieferung ist fr Sie. Um die Lieferung zu aktivieren, bitte besttigen..

Ihre Kontoinformationen

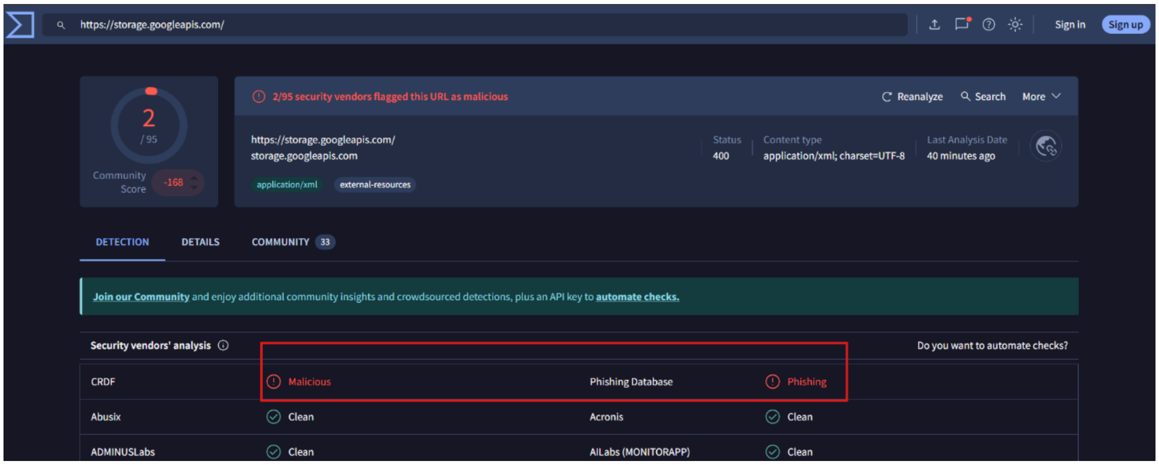
Kunde: Krystyalia
Email: Krystyalia@gmail.com
Belohnen: *PayPal-Guthabenk*

After clicking on Copy Link Location, this website appears. https://storage.googleapis.com/hqyoqzatqthj/aemmfcylvxeo.html#QORHNZC44FT4.QORHNZC44FT4?dYCTywccxr3jcxxrmcdcKBdmc5D6qfcJVcbbb4M

Answer: storage.googleapis.com.

Q3: Is the domain mentioned in the previous question suspicious?

To know whether the domain was suspicious or not, I just searched on Virustotal.



2 / 95

Community Score -168

2/95 security vendors flagged this URL as malicious

https://storage.googleapis.com/
storage.googleapis.com

application/xml external-resources

Status 400

Content type application/xml; charset=UTF-8

Last Analysis Date 40 minutes ago

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

Security vendors' analysis

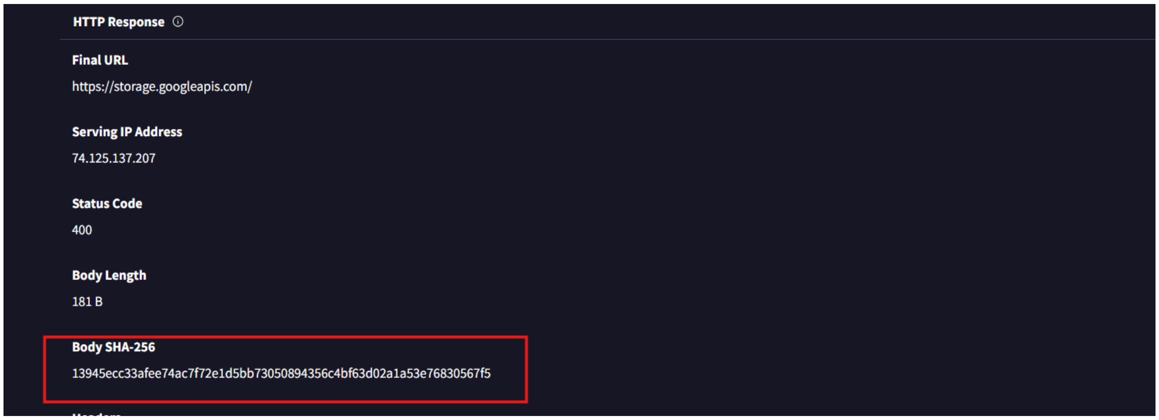
Do you want to automate checks?

CRDF	Malicious	Phishing Database	Phishing
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean

Anwer: So, the answer is Yes.

Q4: What is the body SHA-256 of the domain?

Based on our research for the previous question in Virustotal, I went to Details to see the hash.



HTTP Response

Final URL
https://storage.googleapis.com/

Serving IP Address
74.125.137.207

Status Code
400

Body Length
181 B

Body SHA-256
13945ecc33afee74ac7f72e1d5bb73050894356c4bf63d02a1a53e76830567f5

Anwer: 13945ecc33afee74ac7f72e1d5bb73050894356c4bf63d02a1a53e76830567f5.

Q5: Is this email a phishing email?

After all these investigations, yes, this is a phishing email.