Suspicious Email

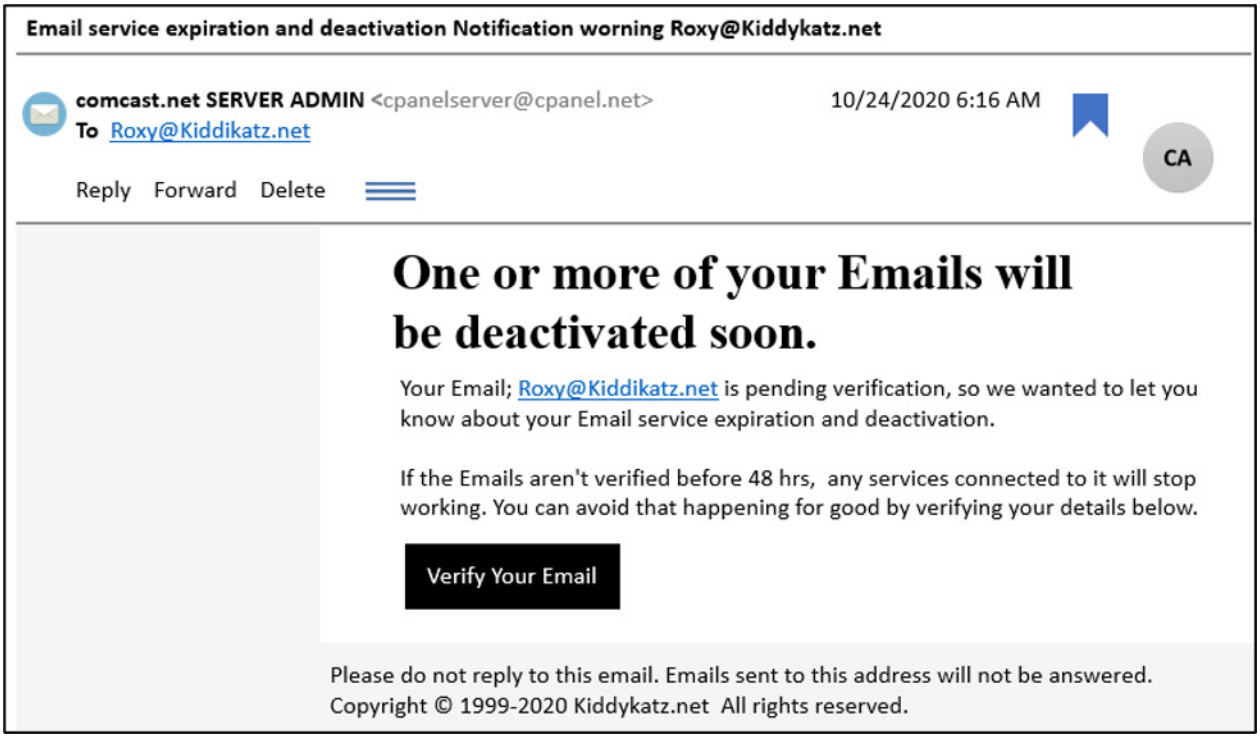
In this challenge, we'll do a forensic exercise on a suspicious email to learn more information on where the email originated and to see how email providers detect possible spam and phishing emails.

1. Examining the email

Question 1

Take a look at the following image, then:

- Tell me a couple of ways this email looks *legitimate*.
- Tell me a couple of ways this email looks *suspicious*.



The hyperlink for **Verify Your Email** is as follows:

```
https://firebasestorage.googleapis.com/v0/b/XXXXXXXXXX?alt=media&token=851844a5-9b3c-449d-b31e-00d57238a4e8#Roxy@Kiddikatz.net
```

Email Header

The email header tells the story about the journey the email took from sender to receiver. This header has been modified to include Roxy@Kiddikatz for the email address.

Important note:

If you don't know how to find an email header visit:
https://mxtoolbox.com/Public/Content/EmailHeaders/

Take a look at the email header:

START EMAIL HEADER

Return-Path: <cpanelserver@cpanel.net>

Delivered-To: Roxy@Kiddikatz.net

Received: from dovdir4-asa-02o.email.Kiddikatz ([96.114.154.195])

by dovback4-asa-02o.email.Kiddikatz with LMTP

id iI0bBuH+k1/kcgAA1Vbeiw

(envelope-from <cpanelserver@cpanel.net>)

for <Roxy@Kiddikatz>; Sat, 24 Oct 2020 10:16:01 +0000

Received: from dovpxy-asc-13o.email.Kiddikatz ([96.114.154.195])

by dovdir4-asa-02o.email.Kiddikatz with LMTP

id uKDkA+H+k1/wLgAApBwMGg

(envelope-from <cpanelserver@cpanel.net>)

for <Roxy@Kiddikatz>; Sat, 24 Oct 2020 10:16:01 +0000

Received: from reszmta-po-01v.sys.Kiddikatz ([96.114.154.195])

by dovpxy-asc-13o.email.Kiddikatz with LMTP

id 8EcmAeH+k1/DXgAAKsibjw

(envelope-from <cpanelserver@cpanel.net>)

for <Roxy@Kiddikatz>; Sat, 24 Oct 2020 10:16:01 +0000

Received: from resimta-po-21v.sys.Kiddikatz ([96.114.154.149])

by reszmta-po-03v.sys.Kiddikatz with ESMTP

id WGadkLSgbxSFOWGaekA6i1; Sat, 24 Oct 2020 10:16:00 +0000

Received: from yogarafi.de ([144.76.72.196])

by resimta-po-21v.sys.Kiddikatz with ESMTP

id WGabkOpIji6AfWGadk3Lzc; Sat, 24 Oct 2020 10:16:00 +0000

X-CAA-SPAM: F00001

X-Meowkatz-VAAS: NOTE: Verification and Authentication Agents (*VAAs*).

ggruggvucftvghtrhhoucdtuddrgedujedrkedvgddvjecutefuodetggdotefrodftvfcurfhrohhfihhlvgemu
cevohhmtggrshhtqdftvghsihenuceurghilhhouhhtmecufedtudenucgoufhushhpvggtthffohhmrghinh
culdegledmnegorfhhihhshhhinhhgqdetgeduhedqtdelucdlfedttddmnecujfgurhephffvufffkfggtgfgsehhqhe
ftddttddtnecuhfhrohhmpedftghomhgtrghsthdrnhgvthcuuffgtfgggfftucetfffokffpfdeotghprghnvghlshgvrh
hvvghrsegtphgrnhgvlhdrnhgvtheqnecuggftrfgrthhtvghrnhepjeeijefgjeekgffhudejiefffeettdehhedtkefhud
efudfhhfefjeelfeejteejnecuffhomhgrihhnpehgohgurgguugihrdgtohhmpdhgohhoghhlvggrphhishdrtghom
henucfkphepudeggedrjeeirdejvddrudeliedpudektddrvddugedrvdefledrudegnecuvehluhhsthgvrhfuihiivg
eptdenucfrrghrrghmpehhvghlohephihoghgrrhgrfhhirdguvgdpihhnvghtpedugeegrdejiedrjedvrdduleeipdh
mrghilhhfrhhomheptghprghnvghlshgvrhhv

X-Meowkatz-VMeta: sc=349.00;st=phishing

X-Meowkatz-Message-Heuristics: IPv6:N;TLS=1;SPF=2;DMARC=F

Received: by yogarafi.de (Postfix, from userid 1001)

id 3A3D514C1A97; Sat, 24 Oct 2020 10:26:31 +0200 (CEST)

Received: from cpanel.net (unknown [180.214.239.14])

by yogarafi.de (Postfix) with ESMTPA id 2E88C14C1A7E

for <Roxy@Kiddikatz>; Sat, 24 Oct 2020 10:26:27 +0200 (CEST)

From: “Kiddikatz SERVER ADMIN”<cpanelserver@cpanel.net>

To: Roxy@Kiddikatz

Subject: Email service expiration and deactivation Notification worning Roxy@Kiddikatz

Date: 24 Oct 2020 01:26:28 -0700

Message-ID: <20201024012627.6E1B2AB836AF8BD7@cpanel.net>

MIME-Version: 1.0

Content-Type: text/html

Content-Transfer-Encoding: quoted-printable

END EMAIL HEADER

2. Diving into the header

Go to mxtoolbox, where I have uploaded the email header.

https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=09bf5bab-8678-4e44-91ad-2d1d3c7e6aa0

Take a look at the details.

Important note:

To read more on dmarc visit https://dmarc.org/

Scroll down where you will see **yogarafi.de 144.76.72.196** is on a blacklist.

Question 2

What does it mean when an IP address is on a blacklist?

Scroll down where you will see SPF failed for IP - 96.114.154.195.

This means a test to verify that the IP address is included in the Sender Policy Framework. In this case, the specified IP address is not included in the SPF record.

3. Verifying IP blacklists

Go to https://mxtoolbox.com/SuperTool.aspx?action=blacklist%3a144.76.72.196&run=toolpage

to verify the IP address is on a blacklist.

Then visit https://anti-hacker-alliance.com/index.php?ip=144.76.72.196&searching=yes where we can see more information on the IP address: **144.76.72.196**.

Question 3

What country is this IP address located?

More Reading

Visit this site where we can see the email is a phishing email:

https://brendinghat.com/2020/10/24/brendinghat-com-server-admin-email-service-expiration-and-deactivation-notification/

This article shares information about the prevalence of hackers using Google Firebase Storage:

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/phishing-in-a-bucket-utilizing-google-firebase-storage/