BTLO: PHISHING ANALYSIS 2

Prepared by:

Joel Mas Martínez
Spain

Spain, 23/05/2024
Version 1.0

RIGHTS OF USE

Summary

1. Documentary control

VERSION	DATE	AUTHOR	APRUEBA
1.0	23/05/2024	Joel Mas Martínez	-

2. Objectives and Scope

Objectives and Scope of the Forensic Analysis

Jaksponz S.L. has contacted and hired me to conduct an analysis of a phishing attack they recently experienced. They provided full access to the affected computer to investigate the attacker's objective, what they achieved, and how they successfully executed the attack.

Attack Description

The attacker executed the attack by impersonating the well-known company Amazon, sending the recipient, in this case, Saint, a message stating that his account had been blocked. This attack took place on July 14, 2021, at 01:40:32 am.

The message sent by the attacker contained a button that said "Review Account," which redirected to a page displaying the message "the page you are trying to access cannot be loaded."

Techniques Used

The attacker encoded the message body with Base64 to prevent easy decryption. Using the Cyberchef tool from GitHub, the message was successfully decoded.

The URL to retrieve the company's logo in the email is the following: https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13ed/1500584238342-OX2L298XVSKF8AO6I3SV/amazon-logo?format=750w&amp;content-type=image%2Fpng

Possible Errors by the Attacker

Due to a possible error by the attacker, the Base64 encoded message contains a Facebook link with the ID amir.boyka.7.

3. Criteria for classification of vulnerabilities

The following table shows the risk classification criteria used to categorise the vulnerabilities detected.

Risk	Descripción
🟥🟥🟥🟥🟥	An attacker could take **full control over the host**, e.g. read and write access to the file system, execution of arbitrary commands, etc…
🟥🟥🟥🟥⬜	Ease of gaining full control over the host or leaking sensitive information that can help commit an intrusion. For example, **read access to files on disk.**
🟥🟥🟥⬜⬜	**Access to sensitive information** hosted on the host, including security parameters, or access to specific sites of the file system, directory navigation, disclosure of local configurations, or systems. Mail subjects that accept relay.
🟥🟥⬜⬜⬜	**Collection of sensitive host information**, such as specific versions of installed software. This information will help an attacker to perform targeted attacks on services on the host.
🟥⬜⬜⬜⬜	**Possibility** of collecting general host information, such as open ports, running services, etc. This information will be useful in finding other vulnerabilities.

4. Executive Summary

Jaksponz S.L. has fallen victim to a phishing attack. This report outlines how the attack was carried out, the methods used by the attacker, and the key information discovered during the investigation. To understand the whole content, I've downloaded the mail information. I've also used a special tool to decode and understand the message content named CyberChef.

Attack Description

The attacker meant to steal Saint's identity and his Amazon account asswell, impersonating Amazon and sending a false message to him claiming that his account had been blocked and he had to click a link to recover it. Luckly the attacked was mitigated just at the time and he couldn't go any further. This message was sent on July 14, 2021, at 01:40 am. The message contained a "Review Account" button, which redirected to an error page.

Methods Used

1. **Message Encoding**: The attacker encoded the message to make it difficult to read at first glance.
2. **Amazon Logo Link**: The email included a link to display the Amazon logo, making it appear more legitimate. This link is not directly related to the attack but helps make the email more convincing.

Key Information Discovered

During the investigation, we found a Facebook link in the encoded message that may be related to the attacker. Such mistakes provide valuable clues about the attacker's identity.

5. Vulnerability Summary

Below is the list of the detected vulnerabilities, ordered from the most critical to the least:

Affected Hosts	Vulnerabilities	Risk
Windows	test	🟥⬜⬜⬜⬜

6. Legend: vulnerability table

Below is an example table with the nomenclature used in all the reports, to facilitate understanding of each of the detailed fields.

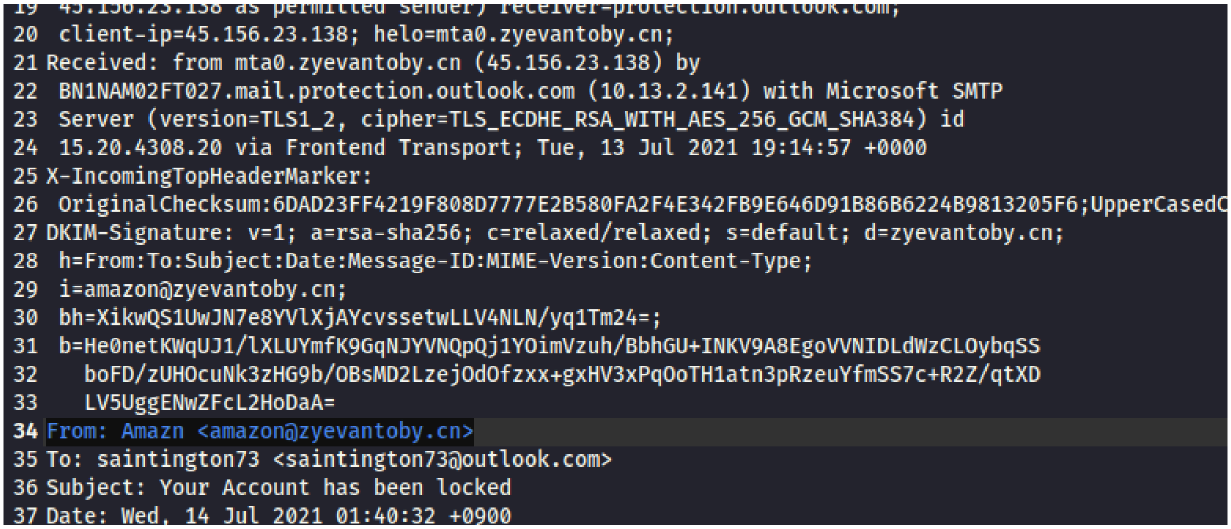
Title			
Data and identity theft			
Code	CA1-R2L3-OS	**Risk**	🟥⬜⬜⬜⬜
Affected hosts		**Ports**	No ports affected
Windows			
Vulnerability details			
The attacker has tried to take advantage of an employee's misinformation to steal their Amazon account and possibly their identity, all through a Phishing attack on their Outlook email.			
Remediations			
The recommended remedies to prevent this type of attack are to thoroughly review the contents of the email and read the domain behind the name, for example amazon@domain.com , and compare them with the original Amazon domains. If something doesn't match, do not click the link under any circumstances.			

7. Vulnerabilities: table of vulnerabilities

Title			
Data and identity theft			
Code	CA1-R2L3-OS	**Risk**	🟥□□□□
Affected hosts		**Port**	No ports affected
Windows			
Vulnerability details			

In the mail info we can find the next information:

Attacker mail:

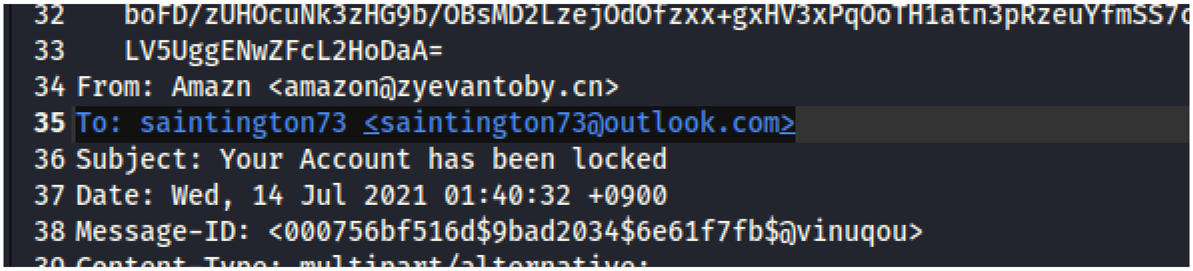


```
19  45.156.23.138 as permitted sender) receiver=protection.outlook.com;
20  client-ip=45.156.23.138; helo=mta0.zyevantoby.cn;
21 Received: from mta0.zyevantoby.cn (45.156.23.138) by
22  BN1NAM02FT027.mail.protection.outlook.com (10.13.2.141) with Microsoft SMTP
23  Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
24  15.20.4308.20 via Frontend Transport; Tue, 13 Jul 2021 19:14:57 +0000
25 X-IncomingTopHeaderMarker:
26  OriginalChecksum:6DAD23FF4219F808D7777E2B580FA2F4E342FB9E646D91B86B6224B9813205F6;UpperCasedC
27 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=default; d=zyevantoby.cn;
28  h=From:To:Subject:Date:Message-ID:MIME-Version:Content-Type;
29  i=amazon@zyevantoby.cn;
30  bh=XikwQS1UwJN7e8YVlXjAYcvssetwLLV4NLN/yq1Tm24=;
31  b=He0netKWqUJ1/lXLUYmfK9GqNJYVNQpQj1YOimVzuh/BbhGU+INKV9A8EgoVVNIDLdWzCLOybqSS
32    boFD/zUHOcuNk3zHG9b/OBsMD2LzejOdOfzxx+gxHV3xPqOoTH1atn3pRzeuYfmSS7c+R2Z/qtXD
33    LV5UggENwZFcL2HoDaA=
34 From: Amazn <amazon@zyevantoby.cn>
35 To: saintington73 <saintington73@outlook.com>
36 Subject: Your Account has been locked
37 Date: Wed, 14 Jul 2021 01:40:32 +0900
```

As we can see in the picture, at lane 34, it appears the mail sender is pretending to be Amazon.

From: Amazn <amazon@zyevantoby.cn>

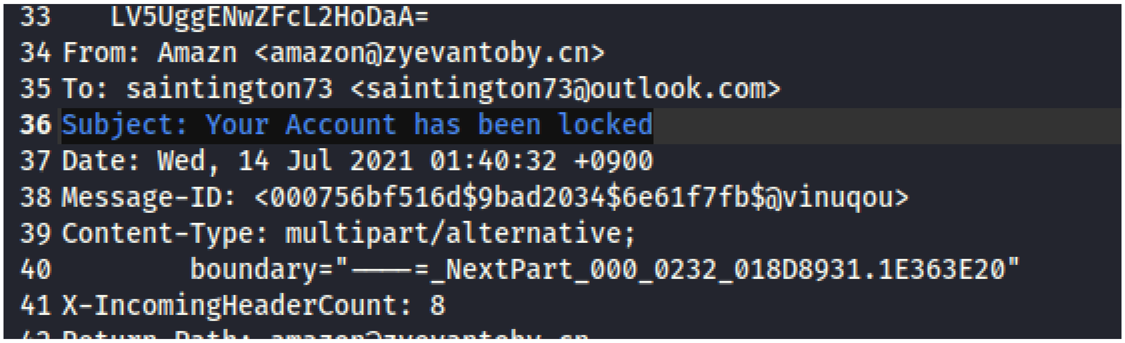
Destinatary mail:



```
32    boFD/zUHOcuNk3zHG9b/OBsMD2LzejOdOfzxx+gxHV3xPqOoTH1atn3pRzeuYfmSS7c
33    LV5UggENwZFcL2HoDaA=
34 From: Amazn <amazon@zyevantoby.cn>
35 To: saintington73 <saintington73@outlook.com>
36 Subject: Your Account has been locked
37 Date: Wed, 14 Jul 2021 01:40:32 +0900
38 Message-ID: <000756bf516d$9bad2034$6e61f7fb$@vinuqou>
39 Content-Type: multipart/alternative;
```

To: saintington73 <saintington73@outlook.com>

Mail subject:

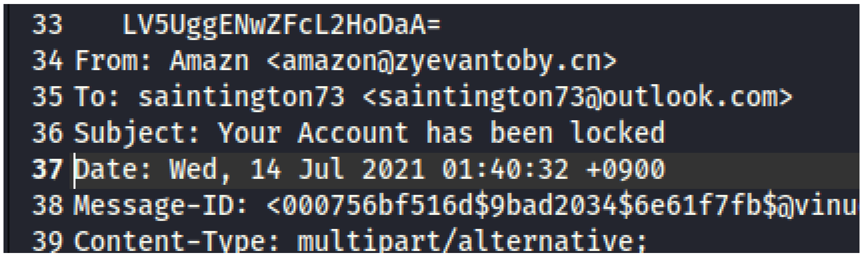


```
33    LV5UggENwZFcL2HoDaA=
34 From: Amazn <amazon@zyevantoby.cn>
35 To: saintington73 <saintington73@outlook.com>
36 Subject: Your Account has been locked
37 Date: Wed, 14 Jul 2021 01:40:32 +0900
38 Message-ID: <000756bf516d$9bad2034$6e61f7fb$@vinuqou>
39 Content-Type: multipart/alternative;
40         boundary="----=_NextPart_000_0232_018D8931.1E363E20"
41 X-IncomingHeaderCount: 8
42 Return-Path: amazon@zyevantoby.cn
```

As we can see in the image, at lane 36 it appears the mail subject.

Subject: You Account has been locked

Date and hour:

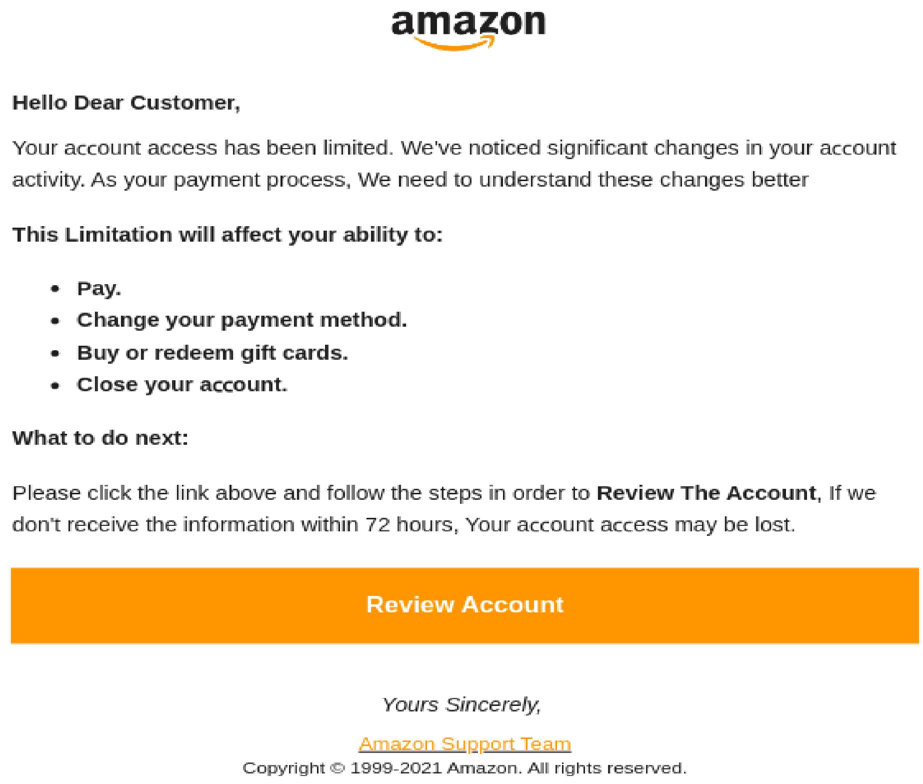


```
33    LV5UggENwZFcL2HoDaA=
34 From: Amazn <amazon@zyevantoby.cn>
35 To: saintington73 <saintington73@outlook.com>
36 Subject: Your Account has been locked
37 Date: Wed, 14 Jul 2021 01:40:32 +0900
38 Message-ID: <000756bf516d$9bad2034$6e61f7fb$@vinu
39 Content-Type: multipart/alternative;
```

As we can see, at lane 37 it appears the date and hour when the hackers sent the email.

Date: Wed, 14 Jul 2021 01:40:32 +0900

Analysing the html code, we can get the mail view:



amazon

Hello Dear Customer,

Your account access has been limited. We've noticed significant changes in your account activity. As your payment process, We need to understand these changes better

This Limitation will affect your ability to:

- **Pay.**
- **Change your payment method.**
- **Buy or redeem gift cards.**
- **Close your account.**

What to do next:

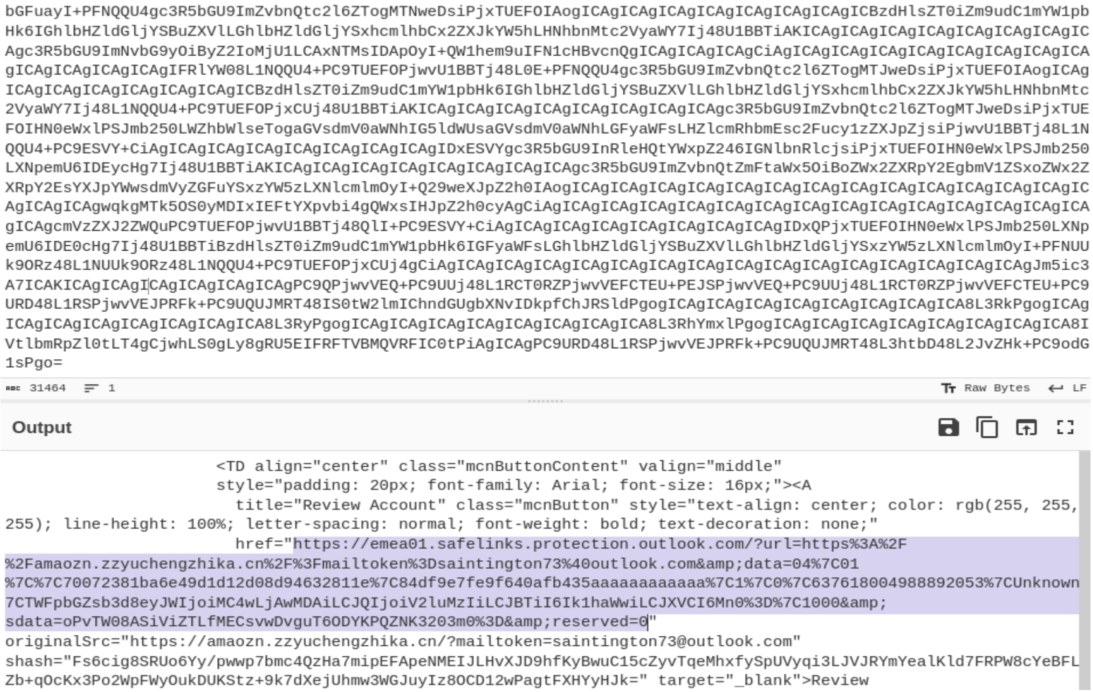
Please click the link above and follow the steps in order to **Review The Account**, If we don't receive the information within 72 hours, Your account access may be lost.

Review Account

Yours Sincerely,

Amazon Support Team
Copyright © 1999-2021 Amazon. All rights reserved.

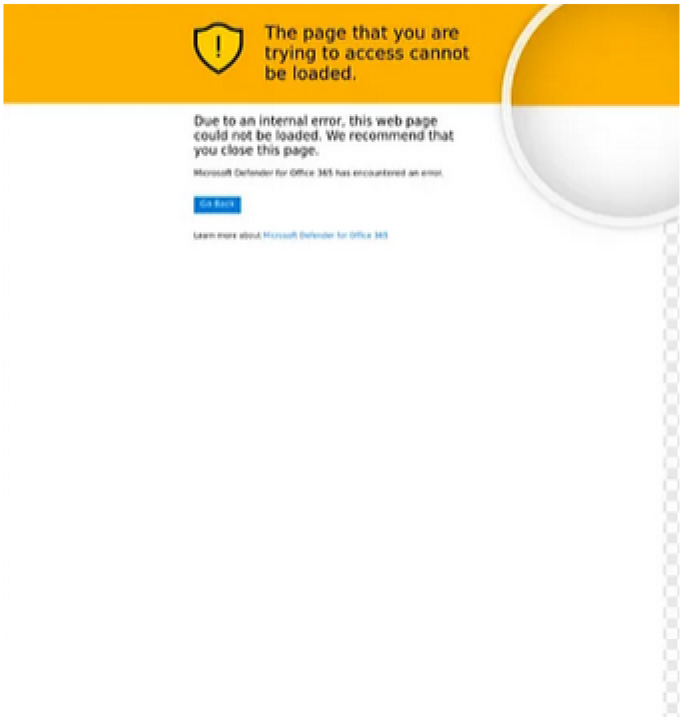
Decrypting the message on CyberChef, we can find the malicious URL:



```
bGFuayI+PFNQQU4gc3R5bGU9ImZvbnQtc2l6ZTogMTNweDsiPjxTUEFOIAogICAgICAgICAgICAgICAgICAgICAgICBzdHlsZT0iZm9udC1mYW1pb
Hk6IGhlbHZldGljYSBuZXVlLGhlbHZldGljYSxhcmlhbCx2ZXJkYW5hLHNhbnMtc2VyaWY7Ij48U1BBTiAKICAgICAgICAgICAgICAgICAgICAgIC
Agc3R5bGU9ImNvbG9yOiByZ2IoMjU1LCAxNTMsIDApOyI+QW1hem9uIFN1cHBvcnQgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICA
gICAgICAgICAgICAgIFRlYW08L1NQQU4+PC9TUEFOPjwvU1BBTj48L0E+PFNQQU4gc3R5bGU9ImZvbnQtc2l6ZTogMTJweDsiPjxTUEFOIAogICAg
ICAgICAgICAgICAgICAgICBzdHlsZT0iZm9udC1mYW1pbHk6IGhlbHZldGljYSBuZXVlLGhlbHZldGljYSxhcmlhbCx2ZXJkYW5hLHNhbnMtc
2VyaWY7Ij48L1NQQU4+PC9TUEFOPjxCUj48U1BBTiAKICAgICAgICAgICAgICAgICAgICAgICAgc3R5bGU9ImZvbnQtc2l6ZTogMTJweDsiPjxTUE
FOIHN0eWxlPSJmb250LWZhbWlseTogaGVsdmV0aWNhIG5ldWUsaGVsdmV0aWNhLGFyaWFsLHZlcmRhbmEsc2Fucy1zZXJpZjsiPjwvU1BBTj48L1N
QQU4+PC9ESVY+CiAgICAgICAgICAgICAgICAgICAgIDxESVYgc3R5bGU9InRleHQtYWxpZ246IGNlbnRlcjsiPjxTUEFOIHN0eWxlPSJmb250
LXNpemU6IDEycHg7Ij48U1BBTiAKICAgICAgICAgICAgICAgICAgICAgICAgc3R5bGU9ImZvbnQtZmFtaWx5OiBoZWx2ZXRpY2EgbmV1ZSxoZWx2Z
XRpY2EsYXJpYWwsdmVyZGFuYSxzYW5zLXNlcmlmOyI+Q29weXJpZ2h0IAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
AgICAgICAgwqkgMTk5OS0yMDIxIEFtYXpvbi4gQWxsIHJpZ2h0cyAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICA
gICAgcmVzZXJ2ZWQuPC9TUEFOPjwvU1BBTj48QlI+PC9ESVY+CiAgICAgICAgICAgICAgICAgICAgIDxQPjxTUEFOIHN0eWxlPSJmb250LXNp
emU6IDE0cHg7Ij48U1BBTiBzdHlsZT0iZm9udC1mYW1pbHk6IGFyaWFsLGhlbHZldGljYSBuZXVlLGhlbHZldGljYSxzYW5zLXNlcmlmOyI+PFNUU
k9ORz48L1NUUk9ORz48L1NQQU4+PC9TUEFOPjxCUj4gCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgJm5ic3
A7ICAKICAgICAgICAgICAgICAgICAgPC9QPjwvVEQ+PC9UUj48L1RCT0RZPjwvVEFCTEU+PEJSPjwvVEQ+PC9UUj48L1RCT0RZPjwvVEFCTEU+PC9
URD48L1RSPjwvVEJPRFk+PC9UQUJMRT48IS0tW2lmIChndGUgbXNvIDkpfChJRSldPgogICAgICAgICAgICAgICAgICAgICAgICAgICA8L3RkPgogICAg
ICAgICAgICAgICAgICAgICAgICA8L3RyPgogICAgICAgICAgICAgICAgICAgICAgICA8L3RhYmxlPgogICAgICAgICAgICAgICAgICAgICAgICA8I
VtlbmRpZl0tLT4gCjwhLS0gLy8gRU5EIFRFRFTVBMQVRFIC0tPiAgICAgPC9URD48L1RSPjwvVEJPRFk+PC9UQUJMRT48L3htbD48L2JvZHk+PC9odG
1sPgo=
```

```
                      <TD align="center" class="mcnButtonContent" valign="middle"
                      style="padding: 20px; font-family: Arial; font-size: 16px;"><A
                        title="Review Account" class="mcnButton" style="text-align: center; color: rgb(255, 255,
255); line-height: 100%; letter-spacing: normal; font-weight: bold; text-decoration: none;"
                        href="https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F
%2Famaozn.zzyuchengzhika.cn%2F%3Fmailtoken%3Dsaintington73%40outlook.com&amp;data=04%7C01
%7C%7C70072381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown
7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&amp;
sdata=oPvTW08ASiViZTLfMECsvwDvguT6ODYKPQZNK3203m0%3D&amp;reserved=0"
originalSrc="https://amaozn.zzyuchengzhika.cn/?mailtoken=saintington73@outlook.com"
shash="Fs6cig8SRUo6Yy/pwwp7bmc4QzHa7mipEFApeNMEIJLHvXJD9hfKyBwuC15cZyvTqeMhxfySpUVyqi3LJVJRYmYealKld7FRPW8cYeBFL
Zb+qOcKx3Po2WpFWyOukDUKStz+9k7dXejUhmw3WGJuyIz8OCD12wPagtFXHYyHJk=" target="_blank">Review
```

Scanned malicious url on the URL2PNG page:



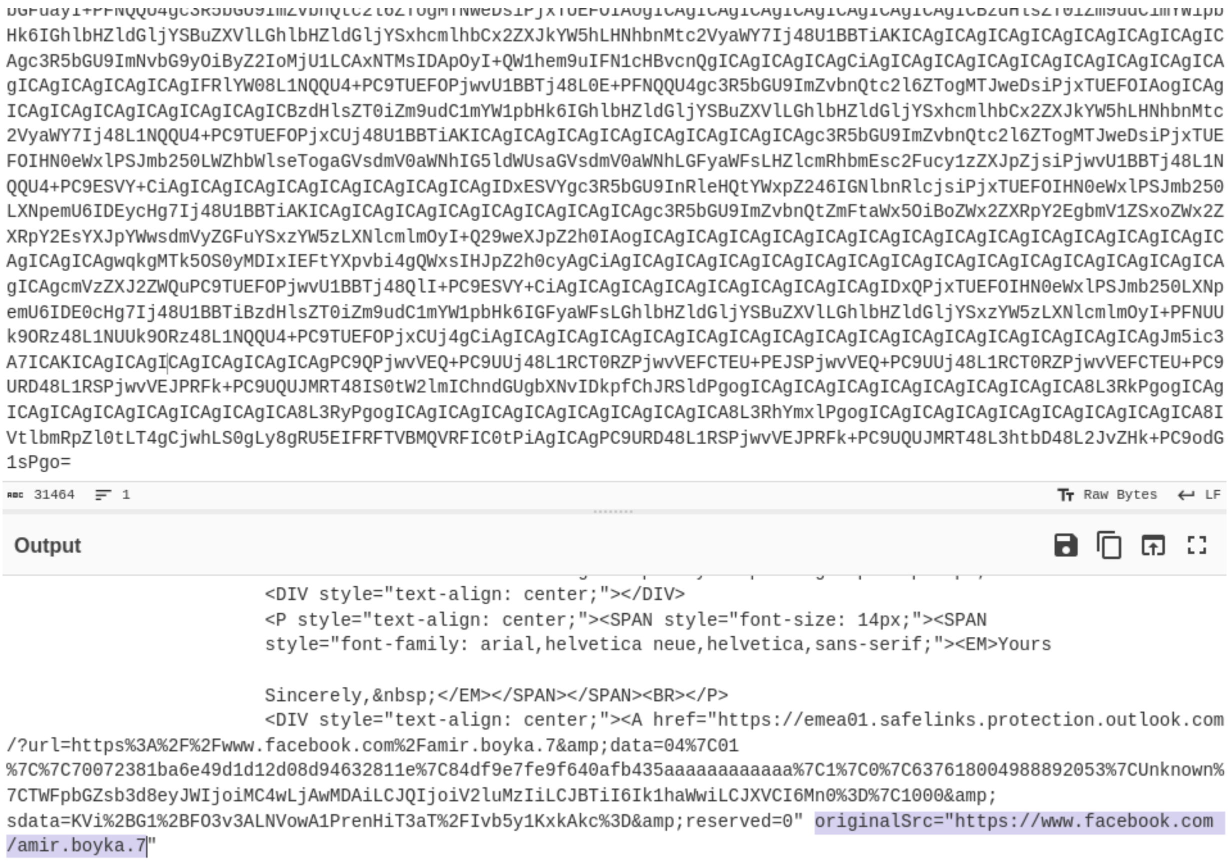
The page that you are trying to access cannot be loaded.

Due to an internal error, this web page could not be loaded. We recommend that you close this page.

Microsoft Defender for Office 365 has encountered an error.

Learn more about Microsoft Defender for Office 365

Facebook account found decrypting the mail body with Base64 on CyberChef:

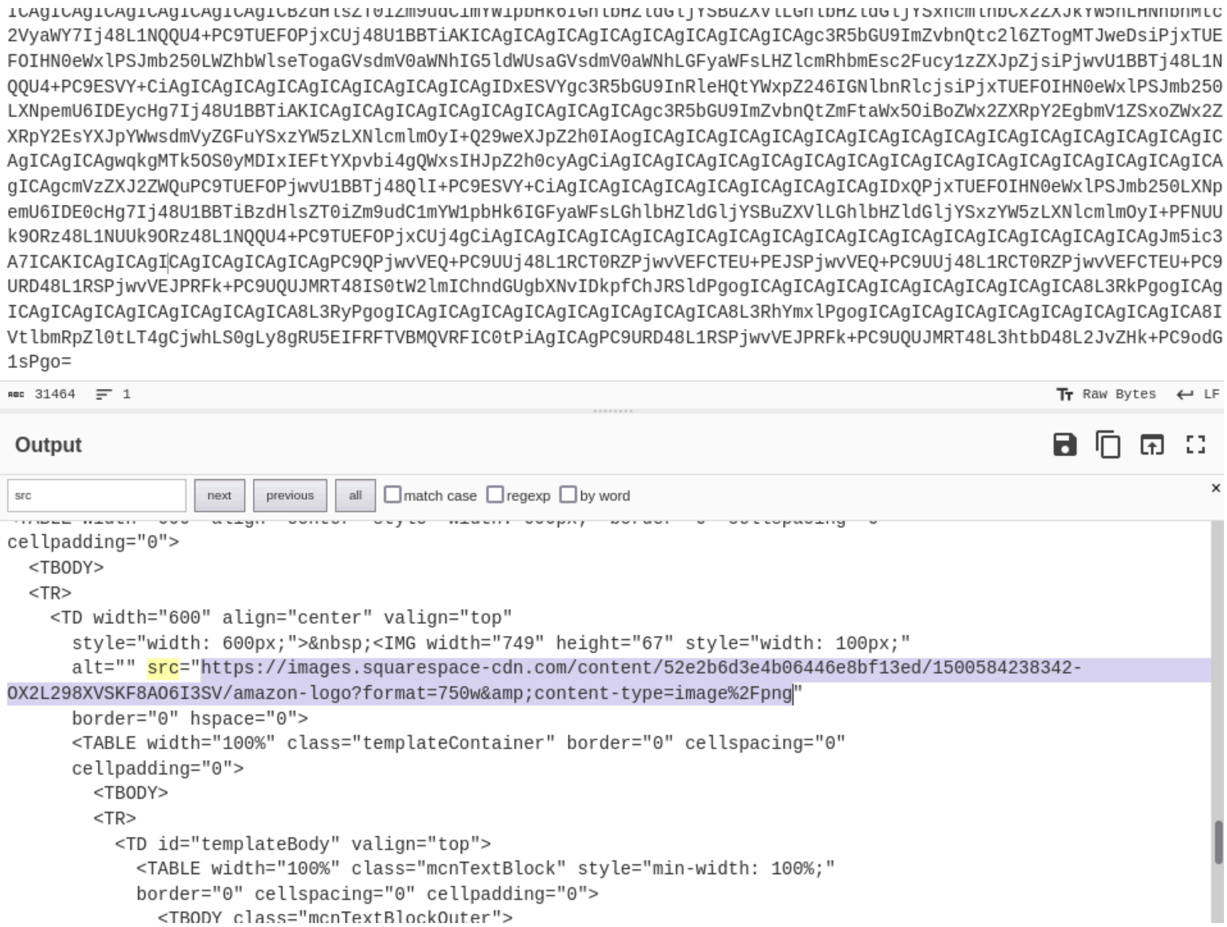


```
bGFuayI+PFNQQU4gc3R5bGU9ImZvbnQtc2l6ZTogMTNweDsiPjxTUEFOIAogICAgICAgICAgICAgICAgICAgICAgICBzdHlsZT0iZm9udC1mYW1pb
Hk6IGhlbHZldGljYSBuZXVlLGhlbHZldGljYSxhcmlhbCx2ZXJkYW5hLHNhbnMtc2VyaWY7Ij48U1BBTiAKICAgICAgICAgICAgICAgICAgICAgIC
Agc3R5bGU9ImNvbG9yOiByZ2IoMjU1LCAxNTMsIDApOyI+QW1hem9uIFN1cHBvcnQgICAgICAgICAgCiAgICAgICAgICAgICAgICAgICAgICAgICA
gICAgICAgICAgICAgIFRlYW08L1NQQU4+PC9TUEFOPjwvU1BBTj48L0E+PFNQQU4gc3R5bGU9ImZvbnQtc2l6ZTogMTJweDsiPjxTUEFOIAogICAg
ICAgICAgICAgICAgICAgICAgICBzdHlsZT0iZm9udC1mYW1pbHk6IGhlbHZldGljYSBuZXVlLGhlbHZldGljYSxhcmlhbCx2ZXJkYW5hLHNhbnMtc
2VyaWY7Ij48L1NQQU4+PC9TUEFOPjxCUj48U1BBTiAKICAgICAgICAgICAgICAgICAgICAgICAgc3R5bGU9ImZvbnQtc2l6ZTogMTJweDsiPjxTUE
FOIHN0eWxlPSJmb250LWZhbWlseTogaGVsdmV0aWNhIG5ldWUsaGVsdmV0aWNhLGFyaWFsLHZlcmRhbmEsc2Fucy1zZXJpZjsiPjwvU1BBTj48L1N
QQU4+PC9ESVY+CiAgICAgICAgICAgICAgICAgICAgICAgIDxESVYgc3R5bGU9InRleHQtYWxpZ246IGNlbnRlcjsiPjxTUEFOIHN0eWxlPSJmb250
LXNpemU6IDEycHg7Ij48U1BBTiAKICAgICAgICAgICAgICAgICAgICAgICAgc3R5bGU9ImZvbnQtZmFtaWx5OiBoZWx2ZXRpY2EgbmV1ZSxoZWx2Z
XRpY2EsYXJpYWwsdmVyZGFuYSxzYW5zLXNlcmlmOyI+Q29weXJpZ2h0IAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
AgICAgICAgwqkgMTk5OS0yMDIxIEFtYXpvbi4gQWxsIHJpZ2h0cyAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICA
gICAgcmVzZXJ2ZWQuPC9TUEFOPjwvU1BBTj48QlI+PC9ESVY+CiAgICAgICAgICAgICAgICAgICAgIDxQPjxTUEFOIHN0eWxlPSJmb250LXNp
emU6IDE0cHg7Ij48U1BBTiBzdHlsZT0iZm9udC1mYW1pbHk6IGFyaWFsLGhlbHZldGljYSBuZXVlLGhlbHZldGljYSxzYW5zLXNlcmlmOyI+PFNUU
k9ORz48L1NUUk9ORz48L1NQQU4+PC9TUEFOPjxCUj4gCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgJm5ic3
A7ICAKICAgICAgICAgICAgICAgICAgPC9QPjwvVEQ+PC9UUj48L1RCT0RZPjwvVEFCTEU+PEJSPjwvVEQ+PC9UUj48L1RCT0RZPjwvVEFCTEU+PC9
URD48L1RSPjwvVEJPRFk+PC9UQUJMRT48IS0tW2lmIChndGUgbXNvIDkpfChJRSldPgogICAgICAgICAgICAgICAgICAgICA8L3RkPgogICAg
ICAgICAgICAgICAgICAgICA8L3RyPgogICAgICAgICAgICAgICAgICAgICA8L3RhYmxlPgogICAgICAgICAgICAgICAgICAgICA8I
VtlbmRpZl0tLT4gCjwhLS0gLy8gRU5EIFRFTVBMQVRFIC0tPiAgICAgPC9URD48L1RSPjwvVEJPRFk+PC9UQUJMRT48L3htbD48L2JvZHk+PC9odG
1sPgo=
```

```
                         <DIV style="text-align: center;"></DIV>
                         <P style="text-align: center;"><SPAN style="font-size: 14px;"><SPAN
                         style="font-family: arial,helvetica neue,helvetica,sans-serif;"><EM>Yours

                         Sincerely,&nbsp;</EM></SPAN></SPAN><BR></P>
                         <DIV style="text-align: center;"><A href="https://emea01.safelinks.protection.outlook.com
/?url=https%3A%2F%2Fwww.facebook.com%2Famir.boyka.7&amp;data=04%7C01
%7C%7C70072381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown%
7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&amp;
sdata=KVi%2BG1%2BFO3v3ALNVowA1PrenHiT3aT%2FIvb5y1KxkAkc%3D&amp;reserved=0" originalSrc="https://www.facebook.com
/amir.boyka.7"
```

And that's what they try to imitate, found on CyberChef as well:



```
ICAgICAgICAgICAgICAgICBzdHlsZT0iZm9udC1mYW1pbHk6IGhlbHZldGljYSBuZXVlLGhlbHZldGljYSxhcmlhbCx2ZXJkYW5hLHNhbnMtc
2VyaWY7Ij48L1NQQU4+PC9TUEFOPjxCUj48U1BBTiAKICAgICAgICAgICAgICAgICAgICAgICAgc3R5bGU9ImZvbnQtc2l6ZTogMTJweDsiPjxTUE
FOIHN0eWxlPSJmb250LWZhbWlseTogaGVsdmV0aWNhIG5ldWUsaGVsdmV0aWNhLGFyaWFsLHZlcmRhbmEsc2Fucy1zZXJpZjsiPjwvU1BBTj48L1N
QQU4+PC9ESVY+CiAgICAgICAgICAgICAgICAgICAgICAgIDxESVYgc3R5bGU9InRleHQtYWxpZ246IGNlbnRlcjsiPjxTUEFOIHN0eWxlPSJmb250
LXNpemU6IDEycHg7Ij48U1BBTiAKICAgICAgICAgICAgICAgICAgICAgICAgc3R5bGU9ImZvbnQtZmFtaWx5OiBoZWx2ZXRpY2EgbmV1ZSxoZWx2Z
XRpY2EsYXJpYWwsdmVyZGFuYSxzYW5zLXNlcmlmOyI+Q29weXJpZ2h0IAogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
AgICAgICAgwqkgMTk5OS0yMDIxIEFtYXpvbi4gQWxsIHJpZ2h0cyAgCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICA
gICAgcmVzZXJ2ZWQuPC9TUEFOPjwvU1BBTj48QlI+PC9ESVY+CiAgICAgICAgICAgICAgICAgICAgICAgIDxQPjxTUEFOIHN0eWxlPSJmb250LXNp
emU6IDE0cHg7Ij48U1BBTiBzdHlsZT0iZm9udC1mYW1pbHk6IGFyaWFsLGhlbHZldGljYSBuZXVlLGhlbHZldGljYSxzYW5zLXNlcmlmOyI+PFNUU
k9ORz48L1NUUk9ORz48L1NQQU4+PC9TUEFOPjxCUj4gCiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgJm5ic3
A7ICAKICAgICAgICAgICAgICAgICAgPC9QPjwvVEQ+PC9UUj48L1RCT0RZPjwvVEFCTEU+PEJSPjwvVEQ+PC9UUj48L1RCT0RZPjwvVEFCTEU+PC9
URD48L1RSPjwvVEJPRFk+PC9UQUJMRT48IS0tW2lmIChndGUgbXNvIDkpfChJRSldPgogICAgICAgICAgICAgICAgICAgICA8L3RkPgogICAg
ICAgICAgICAgICAgICAgICA8L3RyPgogICAgICAgICAgICAgICAgICA8L3RhYmxlPgogICAgICAgICAgICAgICAgICAgICA8I
VtlbmRpZl0tLT4gCjwhLS0gLy8gRU5EIFRFTVBMQVRFIC0tPiAgICAgPC9URD48L1RSPjwvVEJPRFk+PC9UQUJMRT48L3htbD48L2JvZHk+PC9odG
1sPgo=
```

RBC 31464 ☰ 1 Tт Raw Bytes ↵ LF

Output

```
<TABLE width="600" align="center" style="width: 600px;" border="0" cellspacing="0"
cellpadding="0">
  <TBODY>
  <TR>
    <TD width="600" align="center" valign="top"
      style="width: 600px;">&nbsp;<IMG width="749" height="67" style="width: 100px;"
      alt="" src="https://images.squarespace-cdn.com/content/52e2b6d3e4b06446e8bf13ed/1500584238342-
OX2L298XVSKF8AO6I3SV/amazon-logo?format=750w&amp;content-type=image%2Fpng"
      border="0" hspace="0">
      <TABLE width="100%" class="templateContainer" border="0" cellspacing="0"
      cellpadding="0">
        <TBODY>
        <TR>
          <TD id="templateBody" valign="top">
            <TABLE width="100%" class="mcnTextBlock" style="min-width: 100%;"
            border="0" cellspacing="0" cellpadding="0">
              <TBODY class="mcnTextBlockOuter">
```

Copying the link on internet it appears amazon png image:

Remediations

The recommended remedies to prevent this type of attack are to thoroughly review the contents of the email and read the domain behind the name, for example amazon@domain.com , and compare them with the original Amazon domains. If something doesn't match, do not click the link under any circumstances.

8. Conclusions

The document provides a detailed analysis of a phishing attempt aimed at impersonating Amazon to steal sensitive information from the recipient. The attack exploits common social engineering tactics, such as creating a sense of urgency with the subject line "Your Account has been locked" and using a deceptive sender email address.

To mitigate the risk of phishing attacks, it is crucial to combine user education with robust security practices. By thoroughly verifying email domains and scrutinising email content, individuals and organisations can better protect themselves against data and identity theft. Furthermore, leveraging cybersecurity tools can aid in the detection and analysis of such threats, enhancing overall email security.