

Contents

Synopsis	2
First message: The IM chat message within booking.com App (iOS)	2
Second message: The phishing mail (including the header)	3
The scammer webpage	5
This page has 3 stages	7
REMITLY bank support contacted:	11
Analysis	13
Any.run analysis	13
Manual analysis.....	13
VirusTotal.....	14
Cyotek Website Downloader.....	15
GPT Analysis on mail header	15
Whois & nslookup & dig.....	17
Cloudflare Abuse report filed in	25
Traceroute & MTR	30
GPT Analysis on whois, traceroute, dig.....	33
Browser Developer Mode F12	35
Attachments	37
Wireshark packet capture	37
Bank statement	38
Website download	38
TLS certificate is valid	39
Any.run files.....	39

Synopsis

We've made a reservation in booking.com to stay at 'Vital Hotel Rhein Main Therme Wellness Resort & SPA'. Within the booking.com platform we've received a suspicious message from that Hotel in English (the Hotel is usually chatting in German). The message primes us into believing that we need to complete the purchase process outside of the booking.com platform by trusting the mail instructions from the upcoming mail. Indeed a few moments later an email from vitalhotel.rheinmain@gmail.com landed in Maria's iCloud Junk folder. She clicked on the misleading link and landed on the credentials harvesting scam site where she introduced her credit card data. After checking the bank report she realized the money went to RIMITLY, not Booking.com.

Victim: maria.musterfrau@icloud.com

Platform: [Booking.com](https://www.booking.com)

Phishing mail: received from vitalhotel.rheinmain@gmail.com

Credentials harvesting site: <https://bookingconfilm-id5735.com/gozmteavt>

Online bank which received the money: [RIMITLY](https://www.rimitly.com)

First message: The IM chat message within booking.com App (iOS)

~~~~~ IM Message ~~~~~

Hello  
Your reservation at Vital Hotel Rhein Main Therme Wellness Resort & SPA  
requires immediate processing. Please contact us at the e-mail address below to resolve the issue. Otherwise  
we will be forced to cancel your reservation.  
The e-mail address where you can reach us is:  
[vitalhotel.rheinmain@gmail.com](mailto:vitalhotel.rheinmain@gmail.com)  
Duplicate in one message :  
Booking number  
Name of the person for whom the booking is made.  
Thank you for your understanding.  
With kind regards

~~~~~ IM Message ~~~~~

Shortly after this message, we've received a phishing mail on maria.musterfrau@icloud.com offering us a link to finish the payment. It was directed to the Junk folder. Unfortunately, my wife clicked on the link and

landed on the scammers site, entering her MasterCard credentials. We've realized the mistake after we've processed the payment on that site.

Second message: The phishing mail (including the header)

PSHISHING MAIL

~~~~~ HEADER ~~~~~

Junk  
Vital Hotel Rhein Main Therme Wellness Resort  
Yesterday at 6:22 PM  
To:  
Maria Musterfrau  
Return-path: <vitalhotel.rheinmain@gmail.com>  
Original-recipient: rfc822;maria.musterfrau@icloud.com  
Received: from p00-icloudmta-smtpin-us-central-1n-20-percent-0 by p139-mailgateway-smtp-cf79bf76b-lb9hr (mailgateway 2429B41) with SMTP id aad5a8ff-096d-46b0-bb0d-4577975e42fd for <maria.musterfrau@icloud.com>; Wed, 11 Dec 2024 17:22:30 GMT  
X-Apple-MoveToFolder: Junk  
X-Apple-Action: JUNK/Junk  
X-Apple-UUID: aad5a8ff-096d-46b0-bb0d-4577975e42fd  
Received: from mail-pjl-f68.google.com (mail-pjl-f68.google.com [209.85.216.68]) by p00-icloudmta-smtpin-us-central-1n-20-percent-0.p00-icloudmta-smtpin-vip.icloud-mail-production.svc.kube.us-central-1n.k8s.cloud.apple.com (Postfix) with ESMTPS id 50D26C0014F for <maria.musterfrau@icloud.com>; Wed, 11 Dec 2024 17:22:26 +0000 (UTC)  
X-ICL-Info:  
GAtbQlYDBVFFTVJHTAQEUUVUKE0oQVV8PERgKG1hDXxJIS1ZOVggDTEdIUFlOCBYHEUQQHgXRWgoaDQMbVkJJeBxwXCxYRXnYFGBgPG1ZTWQ9VHwJKH1lXCx1XBRgVEEQBSAoJGRFRGAACFQcZEV52C  
xYVCQIchLUNGfKOEhrFkCw8UEApaCFoHTxNPXlkfX1kFGRxIFBddFhIBC1saGv1aTwUTV1oeBg5MEhYJEBRVGAeAFeyTHA1RDxQQClkbX1tCGBACSkRzdyYBTysfL2JiDTEQKS5AVwBRMwErHkEDTx  
U2PAEAIVNCMiUSHzg1CHADozYrJgpjDzM1FAceFB5RDxQQClkbX1tc  
X-ICL-Score: 4.33304404423  
X-Spam-Flag: yes  
X-Suspected-Spam: true  
Authentication-Results: bimi.icloud.com; bimi=skipped reason="insufficient dmarc"  
X-ARC-Info: policy=fail; arc=none  
Authentication-Results: arc.icloud.com; arc=none  
Authentication-Results: dmarc.icloud.com; dmarc=pass header.from=gmail.com  
X-DMARC-Policy: v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@google.com  
X-DMARC-Info: pass=pass; dmarc-policy=none; s=r1; d=r1; pdomain=gmail.com  
Authentication-Results: dkim-verifier.icloud.com; dkim=pass (2048-bit key) header.d=gmail.com header.i=@gmail.com header.b=dCdsDCy+  
Authentication-Results: spf.icloud.com; spf=pass (spf.icloud.com: domain of vitalhotel.rheinmain@gmail.com designates 209.85.216.68 as permitted sender) smtp.mailfrom=vitalhotel.rheinmain@gmail.com  
Received-SPF: pass (spf.icloud.com: domain of vitalhotel.rheinmain@gmail.com designates 209.85.216.68 as permitted sender) receiver=spf.icloud.com; client-ip=209.85.216.68; helo=mail-pjl-f68.google.com; envelope-from=vitalhotel.rheinmain@gmail.com  
Received: by mail-pjl-f68.google.com with SMTP id 98e67ed59eld1-2ee8aa26415so6244829a91.1 for <maria.musterfrau@icloud.com>; Wed, 11 Dec 2024 09:22:25 -0800 (PST)  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20230601; t=1733937745; x=1734542545; darn=icloud.com; h=to:subject:message-id:date:from:in-reply-to:references:mime-version :from:to:cc:subject:date:message-id:reply-to; bh=xNoBEqsGOENRN1+FFh0GuHmPFY1sPimU+dMwuHdZWWU=; b=dCdsDCy+MM19bWwANV8rV+qJQYn3vErdwgXaW3ME0SBP88t+Z8Xt5X2+Ht4yjbZE/m 9eK/H+teeMR2GG/gvMZFlGU/TvXq4gHcqD++Dd2UEXlvLC745iEqnEx0+9P32fQodfYi PLbhJ5T8jQAM9SmIJe16ikVlmicykL9Khm6ldd7jMRbQwAy+sE5q/8U8OhxRbzIH2ikg HJyA86KxJh+n2FwbmexNeGCFVhJtG5aIjYKohBW2rndDYFqtXZ011252f6T71nw2vv09 BDrSD0o9X2MQNjRfAF9mDDiQoHjPoPpUXUefi9qurb1EpCDAPiGqt4aExYnmXKmlvLIpI VSEw==

X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20230601; t=1733937745; x=1734542545; h=to:subject:message-id:date:from:in-reply-to:references:mime-version :x-gm-message-state:from:to:cc:subject:date:message-id:reply-to;  
bh=xNoBEqsGOENRn1+FFh0GuHmPFY1sPimU+dMwuHdZWWU=; b=YkYZYeIM3xoITxpk4rv9wQkBI4+0vogxDf6dZwoXlv/mlQFiLPsDDgw3qD+MbBYUsa  
XYn5Jm2JMoF/yovsvGU9bbgFJyu7DMo5C6HYOTlw1C01TFFpKMCY/pGOg+fwj277CsCL HT8RnWgm1VDwbWYbrfAfIaoqMm+9jGRTrinexK48sK7kJ42D+ioYab5SmwvDYRqvDkJP  
aomWgt7vv40nLg+OwsRjXfdtfl4N1/VnsUrK85aifWFhY71wiJwwWns7tyL+1wLUP8Zx fQ/W2MhK3VpIcZQMv6GwLmdQSit/UPsAK0fvTnJbOjwTJmAcUbd9cZMuwt3NQrhU/BnF 6g5A==  
X-Gm-Message-State: AOJu0YzZZSariT2N/ODocURv0AImqeMOSmtXPe50C4PLjwZzEQUULJ/ak  
FCmTheY8JYfZCY3Kn1Aa790LyC2Kr0S9TU7jot+nMqVOIaUEOA2/tY82Bm4tVMtR6SI5etR5sZ3 N22D+oEf/GiXh9t7Xs8iW+Rbl/91VZGHkPB1WRmEZ  
X-Gm-Gg: ASbGnctxVHIWrTFjXzF2f6W1WfBLHPGhKRgA68+XgHxmQQFGgUiiGtwsOAJL/13y/KY o8DPVf6dhG03wbEIDID5bonEsnirQCZ7naoQ=  
X-Google-Smtp-Source: AGHT+IHpg5yI7MWXXf/xlnYmQCL8GBEUodtKB9MiKEgXghLpUN15lQDMjrRbIVB9gO6woZMRMeowWxtHNQQs910PEcs=  
X-Received: by 2002:a17:90b:4d11:b0:2ee:8c98:a965 with SMTP id 98e67ed59e1d1-2f139327bdemr1012267a91.34.1733937745066; Wed, 11 Dec 2024 09:22:25 -  
0800 (PST)  
MIME-Version: 1.0  
References: <146DE55B-1E47-4B7B-AED5-672A6E60F900@icloud.com>  
In-Reply-To: <146DE55B-1E47-4B7B-AED5-672A6E60F900@icloud.com>  
From: Vital Hotel Rhein Main Therme Wellness Resort <vitalhotel.rheinmain@gmail.com>  
Date: Wed, 11 Dec 2024 17:22:08 +0000  
Message-ID: <CADt6MhWRTtoDiOY8g63FxmI93ywCEGwYctPPkyOs8FaNOMQrS9Q@mail.gmail.com>  
Subject: Re: Reservation  
To: Maria Musterfrau <maria.musterfrau@icloud.com>  
Content-Type: multipart/alternative; boundary="0000000000005b83c8062901d7e3"  
X-MANTSH: 1TFkXBxsZGhIRC1lEF2AYSX5uZkRpWXP5EQpZTRdgX0RBEQpfWRcbHx4RC19NF2R FRE8RC1lJFxf0fcrsGGx8adwYYHgYaBhoGGB8GnEaEBp3BhoGGgYZGgYaBhoGGB8GnEaEBp3BhoRC  
lleF2xseREKQ04XdUN1WV1PcGt7fGxtWntsfxJzR3JDE3NkeFNge2dtch4RC1hcFxxEGgQfGgU bHQbGxsEGx8fBBsdHBAhHhofGhEKX1kXT0AYHV8RCk1cFx8bEQpMWhdo2t7axEKTEYXaGtrY  
klrEQpDWhcYGHMEeh8EGBscBBwSEQpCXhcbEQpCXbcbEQpEThcbEQpCSxdjU2NrexNYfhpfxHE KQkkXYlNja3sTWH4aX14RCkJFF2xAU25GeQEBE3pOEQpCThdjU2NrexNYfhpfxHEKQkwXaR1ZY  
EZbWnxYZ2kRCkJsf2J9bnlLXWzhGhJcEQpCQBdhGnNTWH5AX0heYBEKQlqXb2JwWlscG2BmBRo RClpYfXkRCnBoF2tkQxlftEXsQh9BEBORCnBoF2FraG4TeV9mfVBjEBORCnBoF2FzBW5OGx1CW  
mJjEBORCnBoF3p9GXJ7GR4dHn9tEBORCnBoF2hAU01QGW5LBVByEBORCnBoF2dNYGJOe3xpBWw BEBORCnBoF2JoenIfAX5bZ35mEBORCnBoF21wRnt+TxxzyQVvEBORCnB/F3pcYgFfHlNFYftkE  
AceHxEKcF8XYXhET34aQUZyGlsQGhEKcH0XaxlPbBxwEmYzB4QGhEKcH8XYFJyYGIbcmTYn0 QGhEKcF8XYkVGYWfGyYhpdeWgQGhEKcH0XZWJaThJdTwdvS1IQGhEKcH0XZWJaThJdTwdvS1IQG  
hEKcGwXZF9taG0ebmt+WxwQGhEKcEwXalwaH0JQaXpJREkQGhEKbX4XGhEKWE0XSxE=  
X-Authority-Info: v=2.4 cv=MtUA6Hae c=1 sm=1 tr=0 ts=6759ca53 cx=c\_pps a=Onalrd0PjN/cLj0D0vGj8g==:117 a=RZcAm9yDv7YA:10 a=x7bEGLp0ZPQA:10  
a=k2oT3Wp\_mxAA:10 a=95EFz5htlIgA:10 a=micXuVJiAAAA:8 a=Hi-V8OWyAAAA:8 a=v3ZZPjhaAAAA:8 a=pGLkceISAAAA:8 a=I6hsuPh6Q1a2wA7lZscA:9 a=QEXdDO2ut3YA:10  
a=Ouk6sila6Q0A:10 a=FY7la5fBVHcAbFA31foA:9 a=vrATzbkfjnJDMmff:21 a=lqcHg5cX4UMA:10 a=cpfl\_drxbwQA:10 a=FgCO9eFurDiPTMNWewVh:22  
X-Proofpoint-ORIG-GUID: \_i\_sweZAQVFGpQFU8YmXi9YNRYJ9MGX4  
X-Proofpoint-GUID: \_i\_sweZAQVFGpQFU8YmXi9YNRYJ9MGX4  
Re: Reservation  
~~~~~ HEADER ~~~~~

From: Vital Hotel Rhein Main Therme Wellness Resort <vitalhotel.rheinmain@gmail.com>
Date: 11 December 2024 at 18:22:30 CET
To: Maria Musterfrau <maria.musterfrau@icloud.com>
Subject: Re: Reservation

Dear guest

We regret to inform you that your credit card has not passed the security check performed by the reservation system and has been marked as invalid. As a result, your reservation may be canceled.

To prevent this from happening, you will need to complete a short card verification process. Follow this link to start the procedure.

<https://booking.com/confirmed-reservation-guest/4964741737>

Please note that after entering your data do not leave the page for 5 minutes, our payment system is overloaded and delays may occur, also after processing your card in some situations you will need to call your bank to authorize the transaction, also check your mobile app regularly and confirm the transactions you have received after entering your bank card details.

IMPORTANT! IF THE PAYMENT HAS ALREADY BEEN DEBITED EARLIER. JUST GO THROUGH THE TRANSACTION AGAIN, THE MONEY WILL NOT BE CHARGED AGAIN!

In accordance with our booking policy, if this process is not completed within the next 12 hours, your booking will unfortunately be canceled.

We apologize for any inconvenience and thank you in advance for promptly resolving this issue

PSHISHING MAIL

The scammer webpage

Clicking on that hyperlink we get redirected to: <https://bookingconfilm-id5735.com/gozmteavt> , the credentials harvesting site.

Booking.com | Official site | The X

https://bookingconfirm-id5735.com/gozmteavt

Booking.com

1 Your selection

2 Your details

3 Final step

Your booking details

Check-in | Check-out

21.12.2024 | 23.12.2024

Your price summary

Price

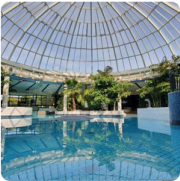
EUR 483.3

How much will it cost to cancel?

Free cancellation at any time!

Limited supply for your dates:

10 hotels like this are already unavailable on our site



Vital Hotel Rhein Main Therme Wellness Resort & SPA

Niederhofheimer Str. 67 65719 Hofheim am Taunus Germany

Great location

Your price summary

Price

EUR 483.3

Enter your details

Almost done! Just fill in the * required info

Are you travelling for work?

☐ Yes ☐ No

First name *

Last name *

Email *

Confirmation email goes to this address

Country/region *

-- Select country/region --

Telephone (mobile number preferred) *

+93

Needed by the property to validate your booking

Are you travelling for work? (optional)

☐ Yes ☒ No

Special requests

Special requests cannot be guaranteed – but the prop make a special request after your booking is complete

Support

We will resend the PUSH notification, please wait until we receive it, and then confirm the code by entering it in the corresponding window.

Verification error. PUSH code rejected. We will resend the PUSH notification, please wait until we receive it, and then confirm the code by entering it in the corresponding window.

Hi. I have done the card verification and the money has been paid

Dear guest there was just an erroneous debit from your card you need to confirm the still swollen notification in order for the funds to be returned to you.

I have not received any notification

The money has been charged from my account but there is no other notification

Enter a message...

This page has 3 stages

Stage 1 - Filling the personal information

bookingconfilm-id5735.com/gozmtaevt

Booking.com

1 Your selection 2 Your details 3 Final step

Your booking details

Check-in 21.12.2024 Check-out 23.12.2024

Your price summary

Price EUR 483.3

How much will it cost to cancel?

Free cancellation at any time!

Limited supply for your dates:

10 hotels like this are already unavailable on our site

Vital Hotel Rhein Main Therme Wellness Resort & SPA

Niederhofheimer Str. 67 65719 Hofheim am Taunus Germany
Great location

Your price summary

Price EUR 483.3

Enter your details

Almost done! Just fill in the * required info

Are you travelling for work?

☐ Yes ☐ No

First name * **Last name ***

Email *

Confirmation email goes to this address

Country/region *

-- Select country/region --

Telephone (mobile number preferred) *

Needed by the property to validate your booking

Are you travelling for work? (optional)

☐ Yes ☒ No

Special requests

Special requests cannot be guaranteed – but the prop make a special request after your booking is complete

Please write your requests in English or French. (opt

Support

code by entering it in the corresponding window.

Verification error. PUSH code rejected. We will resend the PUSH notification, please wait until we receive it, and then confirm the code by entering it in the corresponding window.

Hi. I have done the card verification and the money has been payed

Dear guest there was just an erroneous debit from your card you need to confirm the still swollen notification in order for the funds to be returned to you.

I have not received any notification

The money has been charged from my account but there is no other notification

Enter a message...

Network

Filter 10000 ms 20000 ms 30000 ms 40000 ms 50000 ms 60000 ms 70000 ms 80000 ms 90000 ms 100000 ms 110000 ms 120000 ms 130000 ms 140000 ms

Headers

General

Request URL: https://bookingconfilm-id5735.com/ajax/payment_card_status.php
Request Method: POST
Status Code: 200 OK
Remote Address: [2606:4700:3030:6815:1001]:443
Referrer Policy: strict-origin-when-cross-origin

Response Headers

Alt-Svc: h3="443"; ma=86400
Cache-Control: no-store, no-cache, must-revalidate
CF-Cache-Status: DYNAMIC
CF-Ray: 8f0f70d8be7618df-FRA
Content-Encoding: zstd
Content-Type: text/html; charset=UTF-8
Date: Thu, 12 Dec 2024 17:30:10 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Pragma: no-cache
Report-To: {"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport/v4? s=E2M63wNlod2q2z8Hh4mkGx2%28xPwzJ5DkoeGazG%28Rvgikm1z0fJEN7W O%2FdZUGgC45sSOy%2FJ9W7pRuhJEe4m9QAL%2FuvCM012N3kL1%2FgMC dECsxg5OBpmOgKV41Q/UZ/VMW7gsXjDUZUQ6I4NHammcc7R3them"}],"group p":"cf-nel","max_age":604800}
Server: cloudflare

Request Headers

:authority: bookingconfilm-id5735.com
:method: POST
:path: /ajax/payment_card_status.php
:scheme: https
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Content-Length: 14
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie: PHPSESSID=6vmccctuljrcmrcl0km9jn9hd1
Origin: https://bookingconfilm-id5735.com
Priority: u=1,i
Referer: https://bookingconfilm-id5735.com/gozmtaevt
Sec-Ch-Ua: "Brave";v="131", "Chromium";v="131", "Not A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Sec-Gpc: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
X-Requested-With: XMLHttpRequest

95 requests | 70.4 kB transferred

Console Issues

Group by kind Include third-party cookie issues

A form field element should have an id or name attribute.

Stage 2 – Entering the credit card information

Booking.com



| OUTLET | AMOUNT |
|-------------|-----------|
| BOOKING.COM | 483.3 EUR |

| | |
|------|------------|
| Date | 2024-12-12 |
|------|------------|

| | |
|-------------|-------------|
| Card number | **** * 1111 |
|-------------|-------------|



Please do not close the link, your card is being verified, we will let you know what to do in the support chat.

Copyright © booking.com

Support

We will resend the PUSH notification, please wait until we receive it, and then confirm the code by entering it in the corresponding window.

Verification error. PUSH code rejected.
We will resend the PUSH notification, please wait until we receive it, and then confirm the code by entering it in the corresponding window.

Hi. I have done the card verification and the money has been payed

Dear guest there was just an erroneous debit from your card you need to confirm the still swollen notification in order for the funds to be returned to you.

I have not received any notification

The money has been charged from my account but there is no other notification

Enter a message...



Bank statement reveals where the money went -> REMITLY

| | | |
|--|------------------|-------------|
| Vorläufiger Kontoauszug | | ̄N26 |
| 12.12.2024 bis 12.12.2024 | | |
| Beschreibung | Verbuchungsdatum | Betrag |
| Asiapalast Musterstadt
Mastercard • Bars & Restaurants
Wertstellung 11.12.2024 | 12.12.2024 | -67,30€ |
| SumUp *einfachschoen
Mastercard • Shopping
Wertstellung 12.12.2024 | 12.12.2024 | -19,99€ |
| REMITLY
Mastercard • Investitionen
Wertstellung 12.12.2024 | 12.12.2024 | -483,99€ |

REMITLY bank support contacted:

Chinthalapati (12/12/2024, 6:24:10 PM): Hi Maria! My name is Chinthalapati. How can I help you today? Keep in mind this chat may be recorded.

Chinthalapati (12/12/2024, 6:24:19 PM): Thank you for contacting Remitly! My name is Rajiv . How may I help you?

Maria (12/12/2024, 6:25:38 PM): Hi, I've received a phishing mail and I clicked the link which transferred me to this scam site:

<https://bookingconfilm-id5735.com/gozmteavt>

And I've introduced my credit card infos, transferring them 483.99 Euro.

My bank is N26 from Germany and in my report I see that the target who received my money is using an account at REMITLY

Chinthalapati (12/12/2024, 6:27:13 PM): I understood your concern

Maria (12/12/2024, 6:28:36 PM): what can we do? I already reported this scam with my bank N26

Chinthalapati (12/12/2024, 6:29:13 PM): May I know you have any account in remitly

Maria (12/12/2024, 6:30:32 PM): no

Maria (12/12/2024, 6:30:41 PM): I only have my N26 account

Maria (12/12/2024, 6:30:49 PM): the criminal has a REMITLY account

Chinthalapati (12/12/2024, 6:30:50 PM): Thank you for confirming

Chinthalapati (12/12/2024, 6:31:11 PM): I'm transferring you to compliance team

Lerry (12/12/2024, 6:32:25 PM): Thank you for contacting Remitly. My name is Larry from the customer protection team, how can I help you?

Maria (12/12/2024, 6:32:49 PM): Hi, I've received a phishing mail and I clicked the link which transferred me to this scam site:

<https://bookingconfilm-id5735.com/gozmteavt>

And I've introduced my credit card infos, transferring them 483.99 Euro.

My bank is N26 from Germany and in my report I see that the target who received my money is using an account at REMITLY

Lerry (12/12/2024, 6:32:57 PM): OPK

Lerry (12/12/2024, 6:32:59 PM): OK

Lerry (12/12/2024, 6:33:59 PM): Thank you very much for the information, in this case I notice that we have to do A VERIFICATION and it is necessary to confirm with you some details to complete it.

Lerry (12/12/2024, 6:34:02 PM): We are an online financial institution and must comply with banking regulations to ensure the security of your account. To achieve this we have to go through a verification process in which we require some information from your side

Lerry (12/12/2024, 6:34:05 PM): There are certain procedures that cannot be attended by chat or WhatsApp. I am verifying and you have a pending review with us that must be performed by phone.

Maria (12/12/2024, 6:35:21 PM): I'm at N26 Bank in Germany

Lerry (12/12/2024, 6:35:25 PM): Ok

Maria (12/12/2024, 6:35:44 PM): ok

Lerry (12/12/2024, 6:35:48 PM): so you can call us at the phone number
Maria (12/12/2024, 6:35:53 PM): we can talk over the phone as well
Lerry (12/12/2024, 6:36:00 PM): yes
Lerry (12/12/2024, 6:36:08 PM): +49 - 800 - 723 - 6193
Lerry (12/12/2024, 6:36:14 PM): this is the number
Maria (12/12/2024, 6:36:30 PM): ok, mine is

+49 160 *****

Lerry (12/12/2024, 6:36:32 PM): Thank you for trusting Remitly. If you need additional assistance, we recommend checking out Remitly.com/help where you can read frequently asked questions. Our team is available in English and Spanish 24/7.

Analysis

Any.run analysis

Report

<https://any.run/report/46456c191869b32ad3f070b9fc9599639ce8abea5e030a943dea773516824909/88f580a5-6723-43d2-b28d-e967b4481515#General>

Full report

<https://app.any.run/tasks/88f580a5-6723-43d2-b28d-e967b4481515>

Includes:

- HTTP Requests
- Connections
- DNS Requests
- Threats
- PCAP packet capture
- IOC
- ATT&CK (MITRE)

Manual analysis

The scammer site which stole our credit card data: <https://bookingconfilm-id5735.com/gozmteavt>, resolved to 104.21.64.1.

I've tried to gather as much information as possible about this scammer. See below outputs:

Virustotal

<https://bookingconfilm-id5735.com/gozmteavt>

<https://www.virustotal.com/gui/url/46456c191869b32ad3f070b9fc9599639ce8abea5e030a943dea773516824909>

It's detected as being a Phishing site:

https://bookingconfilm-id5735.com/gozmteavt

Sign inSign up

1

/ 96

Community Score

1/96 security vendor flagged this URL as malicious

Reanalyze

Search

Graph

API

https://bookingconfilm-id5735.com/gozmteavt

bookingconfilm-id5735.com

Status

200

Content type

text/html; charset=UTF-8

Last Analysis Date

23 hours ago

text/html

iframes

DETECTION

DETAILS

COMMUNITY

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

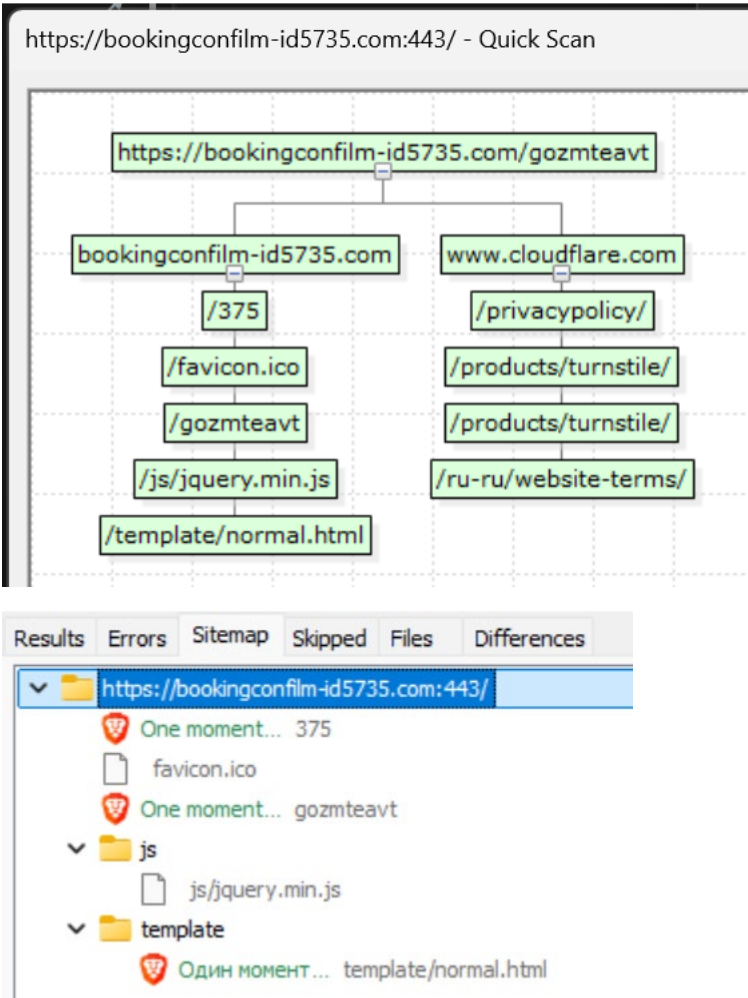
Security vendors' analysis ⓘ

Do you want to automate checks?

| | | | |
|-----------|----------|----------|-------|
| Trustwave | Phishing | Fortinet | Spam |
| Abusix | Clean | Acronis | Clean |

I've downloaded that website as much as I could.

Cyotek Website Downloader
Sitemap:



GPT Analysis on mail header

Key Insights from the Headers

1. From Field

From: Vital Hotel Rhein Main Therme Wellness Resort <vitalhotel.rheinmain@gmail.com>

- **vitalhotel.rheinmain@gmail.com** is the sender's address. While it appears legitimate, Gmail accounts are frequently used in phishing attacks as they are easy to create and spoof.

2. Received Field

Received: from mail-pj1-f68.google.com (mail-pj1-f68.google.com [209.85.216.68])

- **mail-pj1-f68.google.com** is a Gmail server.
- The IP address **209.85.216.68** belongs to Google, indicating that the email was sent via Gmail servers.
- This suggests the email was sent from a legitimate Gmail account, possibly compromised or newly created by the attacker.

3. SPF, DKIM, and DMARC Authentication

• **SPF (Sender Policy Framework):**

Received-SPF: pass

- The SPF check passed, meaning Gmail is an authorized sender for this domain.

• **DKIM (DomainKeys Identified Mail):**

DKIM-Signature: v=1; a=rsa-sha256; d=gmail.com; s=20230601

- The DKIM signature passed, verifying that the email has not been altered in transit and was indeed sent from Gmail.

• **DMARC (Domain-based Message Authentication, Reporting, and Conformance):**

Authentication-Results: dmarc=pass header.from=gmail.com

- The DMARC policy passed, further supporting that the email originated from Gmail.

4. Message ID

Message-ID: <CADt6MhWRTToDiOY8g63FxFMi93yWCEgwYctPPkyOs8FaNOMQrS9Q@mail.gmail.com>

- The message ID is unique to the email and generated by Gmail.
- This can be used to report the email to Gmail for abuse investigation.

5. X-Apple-MoveToFolder and X-Spam Flags

X-Apple-MoveToFolder: Junk

X-Spam-Flag: yes

X-Suspected-Spam: true

- Indicates that Apple Mail flagged this email as spam and moved it to the Junk folder.
- Suggests the email exhibits characteristics of spam or phishing.

6. Authentication and Proofpoint Details

Authentication-Results: bimi.icloud.com; bimi=skipped reason="insufficient dmarc"

- The **Brand Indicators for Message Identification (BIMI)** check was skipped due to insufficient DMARC settings, which is common for phishing emails.

X-Proofpoint-GUID: _i_sweZAQVFGpQFU8YmXi9YNRyJ9MGX4

- Indicates Proofpoint scanned the email and flagged it as spam/phishing.

Analysis of the Headers

- **Legitimacy:** The email successfully passes SPF, DKIM, and DMARC checks, indicating that it was sent via Gmail and not spoofed. This suggests the attacker either:
 1. Compromised a legitimate Gmail account.
 2. Created a new Gmail account for phishing purposes.
- **Spam Indicators:** Apple Mail and Proofpoint identified the email as spam based on its content and behavior, despite the authentication checks passing.
- **Phishing Attempt:**
 - The sender address **vitalhotel.rheinmain@gmail.com** impersonates a legitimate hotel.
 - The email body contains a malicious link (<https://bookingconfilm-id5735.com/gozmteavt>).

Next Steps

1. Report the Phishing Email

- Report the email to Gmail:
 - Forward it as an attachment to abuse@gmail.com.
- Report the phishing site:
 - Use [Google Safe Browsing](#).
 - Submit it to [PhishTank](#) and [APWG](#).

2. Trace the Phishing Link

- Use tools like:
 - [URLScan.io](#) or [VirusTotal](#) to analyze the link.

3. Block the Domain and Sender

- Add **bookingconfilm-id5735.com** and **vitalhotel.rheinmain@gmail.com** to blocklists for your email system or security tools.

4. Educate Users

- Warn potential victims about this phishing campaign and advise them to avoid clicking on similar links.

Whois & nslookup & dig

```
└─(kali@Legion)-[~]
└─$ whois bookingconfilm-id5735.com
Domain Name: BOOKINGCONFILM-ID5735.COM
Registry Domain ID: 2941403776_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.webnic.cc
```

Registrar URL: <https://www.webnic.cc>
Updated Date: 2024-12-11T15:43:36Z
Creation Date: 2024-12-11T15:27:27Z
Registry Expiry Date: 2025-12-11T15:27:27Z
Registrar: Web Commerce Communications Limited dba WebNic.cc
Registrar IANA ID: 460
Registrar Abuse Contact Email: compliance_abuse@webnic.cc
Registrar Abuse Contact Phone: +60.189836788
Domain Status: ok <https://icann.org/epp#ok>
Name Server: BRIT.NS.CLOUDFLARE.COM
Name Server: COBY.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
>>> Last update of whois database: 2024-12-11T20:38:16Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

...snip...

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Domain Name: **BOOKINGCONFILM-ID5735.COM**
Registry Domain ID:
Registrar WHOIS Server: whois.webnic.cc
Registrar URL: <http://www.webnic.cc>
Updated Date: 2024-12-11T15:27:26Z
Creation Date: 2024-12-11T15:27:27Z
Expiration Date: 2025-12-11T15:27:27Z
Registrar: WEBCC
Registrar IANA ID: 460
Registrar Abuse Contact Email: compliance_abuse@webnic.cc
Registrar Abuse Contact Phone: +60.389966799
Domain Status: ok <https://icann.org/epp#ok>
Registry Registrant ID: Not Available From Registry
Registrant Name: John Deecon
Registrant Organization: TrafficDomains INC
Registrant Street: Zablocie 2
Registrant City: Poznan

Registrant State/Province: Poznan
Registrant Postal Code: 57000
Registrant Country: PL
Registrant Phone: +603.6454578
Registrant Phone Ext:
Registrant Fax: +0.0
Registrant Fax Ext:
Registrant Email: abuse@lreg.club
Registry Admin ID: Not Available From Registry
Admin Name: John Deecon
Admin Organization: TrafficDomains INC
Admin Street: Zablocie 2
Admin City: Poznan
Admin State/Province: Poznan
Admin Postal Code: 57000
Admin Country: PL
Admin Phone: +603.6454578
Admin Phone Ext:
Admin Fax: +0.0
Admin Fax Ext:
Admin Email: abuse@lreg.club
Registry Tech ID: Not Available From Registry
Tech Name: John Deecon
Tech Organization: TrafficDomains INC
Tech Street: Zablocie 2
Tech City: Poznan
Tech State/Province: Poznan
Tech Postal Code: 57000
Tech Country: PL
Tech Phone: +603.6454578
Tech Phone Ext:
Tech Fax: +0.0
Tech Fax Ext:
Tech Email: abuse@lreg.club
Name Server: BRIT.NS.CLOUDFLARE.COM
Name Server: COBY.NS.CLOUDFLARE.COM
DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: <https://www.icann.org/wicf>
>>> Last update of WHOIS database: 2024-12-11T20:38:27Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

The Data in Web Commerce Communications Limited ("WEBCC")'s WHOIS database is provided by WEBCC for information purposes, and to assist in obtaining information about or related to a domain name registration record. WEBCC does not guarantee its accuracy. By submitting a WHOIS query, you agree that you will use this Data only for lawful purposes and that, under no circumstances will you use this Data to:

- (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (spam).
- (2) enable high volume, automated, electronic processes that apply to WEBCC (or its systems).

The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of WEBCC. WEBCC reserves the right to terminate your access to the WEBCC WHOIS database in its sole discretion, including without limitation, for excessive querying of the WHOIS database or for failure to otherwise abide by this policy. WEBCC reserves the right to modify these terms at any time.

```
└─(kali@Legion)-[~]
```

```
└─$ nslookup bookingconfilm-id5735.com
```

```
Server:          10.255.255.254
Address:         10.255.255.254#53
```

Non-authoritative answer:

```
Name:   bookingconfilm-id5735.com
Address: 104.21.64.1
Name:   bookingconfilm-id5735.com
Address: 104.21.96.1
Name:   bookingconfilm-id5735.com
Address: 104.21.80.1
Name:   bookingconfilm-id5735.com
Address: 104.21.32.1
Name:   bookingconfilm-id5735.com
Address: 104.21.16.1
Name:   bookingconfilm-id5735.com
```

Address: 104.21.112.1
Name: bookingconfilm-id5735.com
Address: 104.21.48.1
Name: bookingconfilm-id5735.com
Address: 2606:4700:3030::6815:1001
Name: bookingconfilm-id5735.com
Address: 2606:4700:3030::6815:4001
Name: bookingconfilm-id5735.com
Address: 2606:4700:3030::6815:2001
Name: bookingconfilm-id5735.com
Address: 2606:4700:3030::6815:5001
Name: bookingconfilm-id5735.com
Address: 2606:4700:3030::6815:7001
Name: bookingconfilm-id5735.com
Address: 2606:4700:3030::6815:6001
Name: bookingconfilm-id5735.com
Address: 2606:4700:3030::6815:3001

PS C:\Users\lucia> dig bookingconfilm-id5735.com

```
; <<>> DiG 9.16.28 <<>> bookingconfilm-id5735.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57970
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bookingconfilm-id5735.com.      IN      A

;; ANSWER SECTION:
bookingconfilm-id5735.com. 223 IN      A      104.21.112.1
bookingconfilm-id5735.com. 223 IN      A      104.21.96.1
bookingconfilm-id5735.com. 223 IN      A      104.21.16.1
bookingconfilm-id5735.com. 223 IN      A      104.21.48.1
bookingconfilm-id5735.com. 223 IN      A      104.21.32.1
bookingconfilm-id5735.com. 223 IN      A      104.21.64.1
bookingconfilm-id5735.com. 223 IN      A      104.21.80.1
```

```
;; Query time: 0 msec
;; SERVER: 127.0.2.2#53(127.0.2.2)
;; WHEN: Thu Dec 12 19:11:14 W. Europe Standard Time 2024
;; MSG SIZE rcvd: 166
```

```
PS C:\Users\lucia>
```

```
(kali㉿Legion)-[~]
└─$
lucian@Legion:/mnt/c/Users/lucia$ traceroute 104.21.64.1
traceroute to 104.21.64.1 (104.21.64.1), 64 hops max
 1  172.30.80.1  0.388ms  0.167ms  0.145ms
 2  192.168.1.1  0.667ms  0.520ms  0.586ms
 3  192.168.0.1  2.097ms  2.415ms  2.320ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * 92.214.120.17 68.298ms 24.495ms
10 92.214.120.19 18.128ms 92.214.120.18 21.782ms 17.544ms
11 92.214.120.18 30.130ms 145.254.2.195 22.914ms *
12 145.254.2.179 72.003ms 162.158.84.8 34.071ms 20.089ms
13 162.158.84.8 23.039ms 162.158.84.161 31.476ms 19.391ms
14 162.158.84.135 20.463ms 104.21.64.1 19.795ms 16.345ms
```

```
(kali㉿Legion)-[~]
└─$
whois 104.21.64.1

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
```

#

NetRange: 104.16.0.0 - 104.31.255.255
CIDR: 104.16.0.0/12
NetName: CLOUDFLARENET
NetHandle: NET-104-16-0-0-1
Parent: NET104 (NET-104-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS13335
Organization: Cloudflare, Inc. (CLOUD14)
RegDate: 2014-03-28
Updated: 2024-09-04
Comment: All Cloudflare abuse reporting can be done via <https://www.cloudflare.com/abuse>
Comment: Geofeed: <https://api.cloudflare.com/local-ip-ranges.csv>
Ref: <https://rdap.arin.net/registry/ip/104.16.0.0>

OrgName: Cloudflare, Inc.
OrgId: CLOUD14
Address: 101 Townsend Street
City: San Francisco
StateProv: CA
PostalCode: 94107
Country: US
RegDate: 2010-07-09
Updated: 2024-11-25
Ref: <https://rdap.arin.net/registry/entity/CLOUD14>

OrgNOCHandle: CLOUD146-ARIN
OrgNOCName: Cloudflare-NOC
OrgNOCPhone: +1-650-319-8930
OrgNOCEmail: noc@cloudflare.com
OrgNOCRef: <https://rdap.arin.net/registry/entity/CLOUD146-ARIN>

OrgTechHandle: ADMIN2521-ARIN
OrgTechName: Admin
OrgTechPhone: +1-650-319-8930
OrgTechEmail: rir@cloudflare.com
OrgTechRef: <https://rdap.arin.net/registry/entity/ADMIN2521-ARIN>

OrgAbuseHandle: ABUSE2916-ARIN

OrgAbuseName: Abuse
OrgAbusePhone: +1-650-319-8930
OrgAbuseEmail: abuse@cloudflare.com
OrgAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE2916-ARIN>

OrgRoutingHandle: CLOUD146-ARIN
OrgRoutingName: Cloudflare-NOC
OrgRoutingPhone: +1-650-319-8930
OrgRoutingEmail: noc@cloudflare.com
OrgRoutingRef: <https://rdap.arin.net/registry/entity/CLOUD146-ARIN>

RTechHandle: ADMIN2521-ARIN
RTechName: Admin
RTechPhone: +1-650-319-8930
RTechEmail: rir@cloudflare.com
RTechRef: <https://rdap.arin.net/registry/entity/ADMIN2521-ARIN>

RAbuseHandle: ABUSE2916-ARIN
RAbuseName: Abuse
RAbusePhone: +1-650-319-8930
RAbuseEmail: abuse@cloudflare.com
RAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE2916-ARIN>

RNOCHandle: NOC11962-ARIN
RNOCName: NOC
RNOCPHONE: +1-650-319-8930
RNOCEmail: noc@cloudflare.com
RNOCRef: <https://rdap.arin.net/registry/entity/NOC11962-ARIN>

ARIN WHOIS data and services are subject to the Terms of Use
available at: <https://www.arin.net/resources/registry/whois/tou/>

If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/

Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

Cloudflare Abuse report filed in

~~~~~ Mail 1 ~~~~~

[3d3168735073a65f] Cloudflare: Abuse report confirmation

This email is to confirm that your abuse report to Cloudflare has been received and will be processed shortly.

This may be the only response you receive regarding your report. Due to the large volume of reports we receive, it is not possible for us to send a personal response to every report.

Please be aware Cloudflare offers network service solutions including pass-through security services, a content distribution network (CDN) and domain registrar services. Due to the pass-through nature of our services, our IP addresses appear in WHOIS and DNS records for websites using Cloudflare. Cloudflare is not generally a website hosting provider, and we cannot remove material from the Internet that is hosted by others.

To respond to this issue, please reply to abusereply@cloudflare.com.

Regards,  
Cloudflare Trust & Safety

~~~~~ Mail 2 ~~~~~

[3d3168735073a65f]: Cloudflare has responded to your phishing report

Cloudflare received your phishing report regarding: bookingconfilm-id5735.com

Please be aware Cloudflare offers network service solutions including pass-through security services, a content distribution network (CDN) and registrar services. Due to the pass-through nature of our services, our IP addresses appear in WHOIS and DNS records for websites using Cloudflare. Cloudflare cannot remove material from the Internet that is hosted by others.

Accepted URL(s) on bookingconfilm-id5735.com:
hxxps://bookingconfilm-id5735[.]com/gozmteavt

Hosting Provider:

Karina Rashkovska

Abuse Contact:

karina-rashkovska@ukr.net

We have notified our customer of your report.

We have forwarded your report on to the responsible hosting provider.

You may also direct your report to:

1. The provider where bookingconfilm-id5735.com is hosted (provided above); 2. The owner listed in the WHOIS record for bookingconfilm-id5735.com and/or; 3. The contact listed on the bookingconfilm-id5735.com site.

Note: A lookup of the IP for a Cloudflare customer website will show Cloudflare IPs because we are a pass-through network. The actual website is still hosted at the hosting provider indicated above. If the hosting provider has any questions, please have the hosting provider contact us directly regarding this site. Due to attempted abuse of our complaint reporting process, we will only provide the IP of bookingconfilm-id5735.com to the responsible hosting provider if they contact us directly at abusereply@cloudflare.com.

To respond to this issue, please reply to abusereply@cloudflare.com.

Regards,

Cloudflare Trust & Safety

Host:

<https://whois.ipip.net/AS215789>

<https://whois.ipip.net/AS215789/147.45.47.0/24>

% Abuse contact for '147.45.47.0 - 147.45.47.255' is 'karina-rashkovska@ukr.net'

inetnum: 147.45.47.0 - 147.45.47.255

netname: S147_45_47_0

country: BZ (Belize)

org: ORG-KR98-RIPE

admin-c: NA8574-RIPE

tech-c: NA8574-RIPE

status: SUB-ALLOCATED PA

mnt-by: karina-rashkovska-mnt

created: 2024-01-26T10:28:06Z

last-modified: 2024-01-26T16:15:41Z

source: RIPE

organisation: ORG-KR98-RIPE
org-name: Karina Rashkovska
country: UA
org-type: OTHER
address: street Tsentralna building 17 Vysoke 53200, Dnipropetrovska UA
abuse-c: AM51356-RIPE
mnt-ref: karina-rashkovska-mnt
mnt-by: karina-rashkovska-mnt
created: 2023-12-30T14:18:19Z
last-modified: 2024-01-07T09:48:06Z
source: RIPE # Filtered

role: NOC
address: Ukraine
address: area Dnipropetrovska
address: district Nikopolskyi
address: village Vysoke
address: street Tsentralna, building 17
nic-hdl: NA8574-RIPE
mnt-by: karina-rashkovska-mnt
created: 2023-12-25T11:38:45Z
last-modified: 2023-12-25T11:42:43Z
source: RIPE # Filtered

Details

The IP block is registered in Belize (**BZ**) but managed by an organization in Ukraine (**UA**). This occurs due to sub-allocation of IPs across countries. Belize may serve as the jurisdiction for registration, while Ukraine is the operational location. This setup can be legitimate but may also indicate attempts to obscure ownership or geographic location, often seen in spam or abuse cases. Further checks like traceroute or abuse database lookup can help confirm its purpose.

The presence of two countries, BZ (Belize) and UA (Ukraine), in this WHOIS data is due to the following:

1. IP Allocation Country (BZ):

The "country: BZ" field in the inetnum object refers to the geographical or administrative location of the IP address block allocation. In this case, the IP range (147.45.47.0 - 147.45.47.255) is administratively registered under Belize (BZ). This doesn't necessarily mean the IP address is physically used in Belize; it reflects where the IP block was allocated or registered within databases such as RIPE.

2. Organization Country (UA):

The "country: UA" field in the organisation object specifies the country where the organization (in this case, Karina Rashkovska) is based. The organization is located in Ukraine (UA), with its address in Dnipropetrovska Oblast. This indicates that the organization in Ukraine is managing or sub-allocating the IP range registered in Belize.

Why This Happens:

This situation arises because organizations or individuals can sub-allocate IP ranges they own to others in different countries. IP addresses are often sold, leased, or sub-allocated across borders. In this case, the IP block is officially registered in Belize but is managed by an organization or individual based in Ukraine.

Suspicious Patterns:

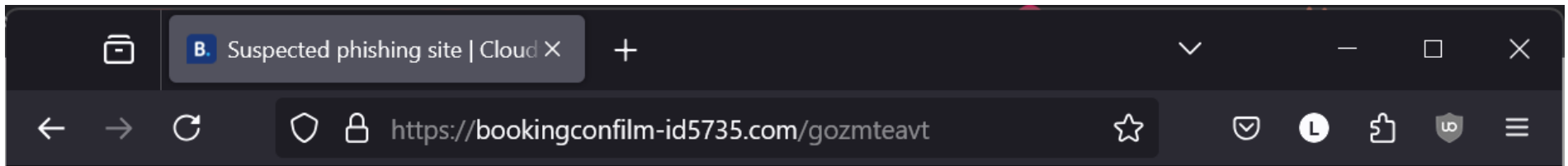
1. Belize and Ukraine combination: Belize is sometimes used as a jurisdiction for hosting anonymous services or circumventing certain regulations, while Ukraine might be the operational base.
2. Abuse contact in Ukraine: The abuse contact email and organization name are Ukrainian, suggesting the IP range is actively managed from there.

What This Could Indicate:

1. Legitimate sub-allocation: The IP block may have been legally allocated to someone in Ukraine who is operating under Belize's registration.
2. Potential proxy use: Belize may be used as a proxy jurisdiction for privacy, hosting, or other less-regulated purposes while the operations are carried out in Ukraine.
3. Possible abuse or misuse: The setup could indicate a potential attempt to obscure true ownership or geographic location, which is common in cases of spam, malicious hosting, or cyber activities.

Further Investigation:

1. Run a traceroute to the IP (147.45.47.0) to determine its actual physical location.
2. Check abuse databases (e.g., Spamhaus, AbuseIPDB) for any reported activities associated with this range.
3. Contact the listed abuse contact (karina-rashkovska@ukr.net) if necessary, for clarification or to report concerns.



Warning

Suspected Phishing

This website has been reported for potential phishing.

Phishing is when a site attempts to steal sensitive information by falsely presenting as a safe source.

[Learn More](#)

[Ignore & Proceed](#)

| WinMTR statistics | | | | | | | | | |
|--|---|-----|------|------|------|------|------|------|----|
| Host | - | % | Sent | Recv | Best | Avrg | Wrst | Last | |
| 192.168.1.1 | - | 1 | 131 | 130 | 0 | 0 | 3 | 0 | |
| 192.168.0.1 | - | 0 | 134 | 134 | 1 | 1 | 5 | 2 | |
| No response from host | - | 100 | 27 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 27 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 27 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 27 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 27 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 27 | 0 | 0 | 0 | 0 | 0 | |
| ipservice-092-214-120-017.092.214.pools.vodafone-ip.de | - | 0 | 0 | 134 | 134 | 14 | 54 | 167 | 21 |
| ipservice-092-214-120-016.092.214.pools.vodafone-ip.de | - | 0 | 135 | 135 | 14 | 51 | 167 | 14 | |
| 145.254.2.179 | - | 39 | 52 | 32 | 0 | 55 | 178 | 25 | |
| 162.158.84.8 | - | 0 | 134 | 134 | 16 | 58 | 173 | 16 | |
| 162.158.84.53 | - | 0 | 134 | 134 | 14 | 46 | 159 | 24 | |
| 104.21.64.1 | - | 1 | 131 | 130 | 0 | 57 | 198 | 114 | |

WinMTR v0.92 GPL V2 by Appnor MSP - Fully Managed Hosting & Cloud Provider

```
$ mtr -rwzb 104.21.64.1
Start: 2024-12-15T00:47:29+0100
HOST: Legion
1. AS??? 172.30.80.1
2. AS??? 192.168.1.1
3. AS??? 192.168.0.1
4. AS??? ???
5. AS??? ???
6. AS??? ???
7. AS??? ???
8. AS??? ???
9. AS??? ???
10. AS3209 ipservice-092-214-120-019.092.214.pools.vodafone-ip.de (92.214.120.19)
11. AS3209 ipservice-092-214-120-018.092.214.pools.vodafone-ip.de (92.214.120.18)
12. AS3209 145.254.2.195
13. AS13335 162.158.84.8
14. AS13335 162.158.84.145
15. AS13335 104.21.64.1
```

| | Loss% | Snt | Last | Avg | Best | Wrst | StDev |
|---|-------|-----|------|------|------|------|-------|
| 1. AS??? 172.30.80.1 | 0.0% | 10 | 0.3 | 0.3 | 0.2 | 0.5 | 0.1 |
| 2. AS??? 192.168.1.1 | 30.0% | 10 | 0.7 | 0.8 | 0.6 | 1.0 | 0.2 |
| 3. AS??? 192.168.0.1 | 30.0% | 10 | 1.7 | 1.6 | 1.4 | 1.7 | 0.2 |
| 4. AS??? ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 5. AS??? ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 6. AS??? ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 7. AS??? ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 8. AS??? ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 9. AS??? ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 10. AS3209 ipservice-092-214-120-019.092.214.pools.vodafone-ip.de (92.214.120.19) | 0.0% | 10 | 19.6 | 18.3 | 15.5 | 25.5 | 3.0 |
| 11. AS3209 ipservice-092-214-120-018.092.214.pools.vodafone-ip.de (92.214.120.18) | 0.0% | 10 | 17.0 | 17.3 | 11.5 | 21.3 | 2.8 |
| 12. AS3209 145.254.2.195 | 40.0% | 10 | 17.6 | 17.4 | 16.6 | 18.7 | 0.8 |
| 13. AS13335 162.158.84.8 | 0.0% | 10 | 19.7 | 28.0 | 16.4 | 59.6 | 13.1 |
| 14. AS13335 162.158.84.145 | 0.0% | 10 | 16.6 | 20.3 | 13.8 | 35.2 | 5.9 |
| 15. AS13335 104.21.64.1 | | | | | | | |

147.45.47.0

```
$ tcptraceroute 147.45.47.0 80
Selected device eth0, address 172.30.92.170, port 54113 for outgoing packets
Tracing the path to 147.45.47.0 on TCP port 80 (http), 30 hops max
1 172.30.80.1 0.284 ms 0.287 ms 0.249 ms
2 192.168.1.1 0.656 ms * 0.746 ms
3 192.168.0.1 2.026 ms 2.339 ms *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 ipservice-092-214-120-016.092.214.pools.vodafone-ip.de (92.214.120.16) 18.086 ms 12.939 ms 17.886 ms
12 145.254.2.179 21.695 ms 12.999 ms 19.967 ms
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
```

28 * * *
29 * * *
30 * * *

Destination not reached

| WinMTR statistics | | | | | | | | | |
|--|---|-----|------|------|------|------|------|------|----|
| Host | - | % | Sent | Recv | Best | Avrg | Wrst | Last | |
| 192.168.1.1 | - | 1 | 545 | 543 | 0 | 0 | 3 | 0 | |
| 192.168.0.1 | - | 1 | 542 | 539 | 1 | 1 | 16 | 1 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| ipservice-092-214-120-019.092.214.pools.vodafone-ip.de | - | | 0 | 553 | 553 | 11 | 20 | 50 | 19 |
| ipservice-092-214-120-018.092.214.pools.vodafone-ip.de | - | | 0 | 553 | 553 | 11 | 22 | 52 | 21 |
| 145.254.2.195 | - | 25 | 285 | 216 | 11 | 21 | 49 | 18 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |
| No response from host | - | 100 | 112 | 0 | 0 | 0 | 0 | 0 | |

WinMTR v0.92 GPL V2 by Appnor MSP - Fully Managed Hosting & Cloud Provider

\$ mtr -rwzb 147.45.47.0

Start: 2024-12-15T00:43:40+0100

| HOST: Legion | | Loss% | Snt | Last | Avg | Best | Wrst | StDev |
|--------------|-------|-------------|-------|------|-----|------|------|-------|
| 1. | AS??? | 172.30.80.1 | 0.0% | 10 | 0.4 | 0.3 | 0.3 | 0.1 |
| 2. | AS??? | 192.168.1.1 | 0.0% | 10 | 0.9 | 1.1 | 0.6 | 0.4 |
| 3. | AS??? | 192.168.0.1 | 0.0% | 10 | 1.4 | 1.9 | 1.4 | 0.4 |
| 4. | AS??? | ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 |
| 5. | AS??? | ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 |
| 6. | AS??? | ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 |
| 7. | AS??? | ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 |
| 8. | AS??? | ??? | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 |

| | | | | | | | | | |
|------------|--|-------|-------|------|------|------|------|-----|-----|
| 9. AS??? | ??? | | 100.0 | 10 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 10. AS3209 | ipservice-092-214-120-019.092.214.pools.vodafone-ip.de (92.214.120.19) | 0.0% | 10 | 17.8 | 18.4 | 15.6 | 22.6 | 1.9 | |
| 11. AS3209 | ipservice-092-214-120-018.092.214.pools.vodafone-ip.de (92.214.120.18) | 0.0% | 10 | 17.8 | 18.3 | 12.5 | 20.5 | 2.5 | |
| 12. AS3209 | 145.254.2.195 | 60.0% | 10 | 19.6 | 17.6 | 14.9 | 19.6 | 2.1 | |
| 13. AS??? | ??? | | | | | | | | |

GPT Analysis on whois, traceroute, dig

The information you have retrieved provides key insights about the phishing domain **bookingconfilm-id5735.com**. Here's how to interpret and act on it:

Key Findings

1. WHOIS Information:

- **Registrar:** Web Commerce Communications Limited dba WebNic.cc (common for suspicious or fraudulent registrations).
- **Creation Date:** 11th December 2024 (extremely recent, a common indicator of a phishing domain).
- **Registrant:** Listed as "John Deecon" from "TrafficDomains INC," likely fake.
- **DNS Servers:** Hosted on Cloudflare (common for obfuscating true server locations).

2. DNS Resolution:

- **Multiple IPs resolved:**
 - IPv4: 104.21.x.x
 - IPv6: 2606:4700:3030::xxxx
- All belong to Cloudflare, suggesting the attacker uses Cloudflare to mask the actual origin server and distribute traffic.

Steps to Investigate Further

1. Analyze the IPs

- The resolved IPs (e.g., 104.21.64.1) are part of Cloudflare's infrastructure.
- Since Cloudflare is a content delivery network (CDN) and proxy, the actual server hosting the phishing site is hidden.

2. Use Cloudflare's Abuse Reporting

- Cloudflare may assist in taking down phishing domains.
- Report the abuse at: [Cloudflare Abuse Form](#).
 - Provide:
 - Domain: bookingconfilm-id5735.com.
 - Evidence of phishing (e.g., email with links and screenshots).

3. Extract Subdomain Information

- Check for subdomains of the phishing site using tools like:

- [Censys](#).
 - [Shodan](#).
- Example query for Shodan:
hostname:"bookingconfilm-id5735.com"
- 4. Investigate Linked Domains**
 - Look for other domains registered with similar patterns (e.g., TrafficDomains INC or WebNic).
 - Use tools like:
 - [ViewDNS.info Reverse Whois](#).
 - [SecurityTrails](#).
- 5. Analyze Domain's History**
 - Use tools to check historical data and domain changes:
 - [URLScan.io](#).
 - [VirusTotal](#).
- 6. Contact the Registrar**
 - Notify **WebNic.cc** of the phishing domain:
 - Abuse contact: compliance_abuse@webnic.cc.
 - Provide evidence of phishing, including email headers and the fraudulent website link.
- 7. Report the Domain to Authorities**
 - **Phishing Databases:**
 - [PhishTank](#).
 - [Anti-Phishing Working Group \(APWG\)](#).
 - **Local CERT/CSIRT:**
 - Report the domain to your country's Computer Emergency Response Team.
- 8. Inspect Website Behavior in a Sandbox**
 - Use tools to analyze the phishing site without interacting directly:
 - [Any.run](#) (interactive sandbox).
 - [Hybrid Analysis](#).
 - Analyze the behavior of <https://bookingconfilm-id5735.com/gozmteavt>.

Precautionary Notes

- 1. Do Not Visit the Website Directly:**
 - Accessing phishing sites directly risks malware infections or further phishing.
 - Use sandboxes or analysis tools.
- 2. Secure Affected Users:**
 - If someone entered details on the site, advise them to:
 - Cancel associated cards or accounts.
 - Monitor financial transactions.
- 3. Raise Awareness:**
 - Share findings with affected users and organizations to prevent further damage.

Browser Developer Mode F12

Request URL:

https://bookingconfilm-id5735.com/ajax/payment_card_status.php

Request Method:

POST

Status Code:

200 OK

Remote Address:

[2606:4700:3030::6815:1001]:443

Referrer Policy:

strict-origin-when-cross-origin

alt-svc:

h3=":443"; ma=86400

cache-control:

no-store, no-cache, must-revalidate

cf-cache-status:

DYNAMIC

cf-ray:

8f0f70d8be7618df-FRA

content-encoding:

zstd

content-type:

text/html; charset=UTF-8

date:

Thu, 12 Dec 2024 17:30:10 GMT

expires:

Thu, 19 Nov 1981 08:52:00 GMT

nel:

{"success_fraction":0,"report_to":"cf-nel","max_age":604800}

pragma:

no-cache

report-to:

{"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=E2Mf63vNJod2q2zx8HfHmkX2%2BxPPwZJ5DkoeGzxG%2BRvgikmlz0FjEN7WO%2FdvZtUGgC4j5sSOy%2FJ9W7pRuhJEe4m9QAL%2FuvCM012N3kLL%2FgMCdECsxxg5OBpmOgKV4TQ7UZrVMW7gsXjD UZUQ6I4NHAmcc7R3them"}],"group":"cf-nel","max_age":604800}

server:
cloudflare
:authority:
bookingconfilm-id5735.com
:method:
POST
:path:
/ajax/payment_card_status.php
:scheme:
https
accept:
application/json, text/javascript, */*; q=0.01
accept-encoding:
gzip, deflate, br, zstd
accept-language:
en-US,en;q=0.9
content-length:
14
content-type:
application/x-www-form-urlencoded; charset=UTF-8
cookie:
PHPSESSID=6vmccctuljrcmrcl0km9jn9hd1
origin:
https://bookingconfilm-id5735.com
priority:
u=1, i
referrer:
https://bookingconfilm-id5735.com/gozmteavt
sec-ch-ua:
"Brave";v="131", "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile:
?0
sec-ch-ua-platform:
"Windows"
sec-fetch-dest:
empty
sec-fetch-mode:
cors
sec-fetch-site:
same-origin

```
sec-gpc:
1
user-agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
x-requested-with:
XMLHttpRequest
```

Attachments

[booking-phishing-files.zip](#)

Wireshark packet capture

tcpdump-booking-104.21.80.1.bookingconfilm-id5735.com.pcapng



tcpdump-booking-10
4.21.80.1.bookingconf

Target: [104.21.80.1](#)
ip.addr == 104.21.80.1
All 3 stages: Personal details + Credit card + Checkout

tcpdump-booking-104.21.80.1.bookingconfilm-id5735.com.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 104.21.80.1

| No. | Time | Source | Destination | Protocol | Length | TCP Segm Info |
|-----|--------------|----------------|----------------|----------|--------|---|
| 51 | 57.692747447 | 192.168.100.14 | 104.21.80.1 | TCP | 74 | 0 37700 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2202915991 TSecr=0 WS=12 |
| 52 | 57.717012567 | 104.21.80.1 | 192.168.100.14 | TCP | 74 | 0 443 → 37700 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM TSval=1956264878 TSecr=2202915991 |
| 53 | 57.717058535 | 192.168.100.14 | 104.21.80.1 | TCP | 66 | 0 37700 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2202916015 TSecr=1956264878 |
| 54 | 57.717978650 | 192.168.100.14 | 104.21.80.1 | TLSv1.3 | 583 | 517 Client Hello (SNI=bookingconfilm-id5735.com) |
| 55 | 57.748593838 | 104.21.80.1 | 192.168.100.14 | TCP | 66 | 0 443 → 37700 [ACK] Seq=1 Ack=518 Win=73728 Len=0 TSval=1956264913 TSecr=2202916016 |
| 56 | 57.753376609 | 104.21.80.1 | 192.168.100.14 | TLSv1.3 | 3212 | 3146 Server Hello, Change Cipher Spec, Application Data |
| 57 | 57.753419707 | 192.168.100.14 | 104.21.80.1 | TCP | 66 | 0 37700 → 443 [ACK] Seq=518 Ack=3147 Win=31872 Len=0 TSval=2202916051 TSecr=1956264918 |
| 58 | 57.758425105 | 192.168.100.14 | 104.21.80.1 | TLSv1.3 | 130 | 64 Change Cipher Spec, Application Data |
| 59 | 57.758616171 | 192.168.100.14 | 104.21.80.1 | TLSv1.3 | 236 | 170 Application Data |
| 60 | 57.758793366 | 192.168.100.14 | 104.21.80.1 | TLSv1.3 | 398 | 332 Application Data |
| 61 | 57.779521472 | 104.21.80.1 | 192.168.100.14 | TLSv1.3 | 578 | 512 Application Data, Application Data |
| 62 | 57.779866303 | 192.168.100.14 | 104.21.80.1 | TLSv1.3 | 97 | 31 Application Data |
| 63 | 57.789777532 | 104.21.80.1 | 192.168.100.14 | TCP | 66 | 0 443 → 37700 [ACK] Seq=3659 Ack=1084 Win=73728 Len=0 TSval=1956264954 TSecr=2202916057 |
| 64 | 57.789777712 | 104.21.80.1 | 192.168.100.14 | TLSv1.3 | 97 | 31 Application Data |
| 65 | 57.831653977 | 192.168.100.14 | 104.21.80.1 | TCP | 66 | 0 37700 → 443 [ACK] Seq=1115 Ack=3690 Win=31872 Len=0 TSval=2202916130 TSecr=1956264954 |

▶ Frame 51: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: Microsoft_00:0a:ce (00:15:5d:00:0a:ce), Dst: Microsoft_00:0a:c6 (00:15:5d:00:0a:c6)
 ▶ Internet Protocol Version 4, Src: 192.168.100.14, Dst: 104.21.80.1
 ▶ Transmission Control Protocol, Src Port: 37700, Dst Port: 443, Seq: 0, Len: 0

Bank statement



balance-statement-M
aria-Musterfrau-2024

REMITLY
Mastercard • Investitionen
Wertstellung 12.12.2024

12.12.2024

-483,99€

Website download



site-download-gozmteavt1733990623058-step1.zip



site-download-gozmteavt1733990623058-step2-confirm.zip

TLS certificate is valid



TLS

bookingconfilm-id57:

Any.run files



any.run-report.pdf



any.run-packet-capture.pcap