SECURING MD Maryland INFORMATION SHARING AND ANALYSIS CENTER

POWERED BY ANOMALI

THREAT BULLETIN

TAR20230206-001: [Threat Analysis Report] Exploiting The User: Leveraging Valid Services For Malicious Activity

TLP
White

DESCRIPTION

TLP:CLEAR (TLP v1 WHITE) = Disclosure is not limited.

Summary

The MD-ISAC continues to observe the use of legitimate services/domains to carry out phishing attacks. A legitimate service or domain is any platform, free or purchased, that is associated with a legitimate company/business and is generally used for benign purposes.

Threat actors often take advantage of these services by creating a free or paid account and then posing as a legitimate business entity. These often free or inexpensive accounts allow malicious actors to send emails with legitimate (and possibly whitelisted) domains that will likely pass all network checks (firewall, email security). The fact that these emails often come from a legitimate email address lends further legitimacy to the message, making it more likely for a victim to fall for the scam or attack.

Tactics, Techniques, and Procedures

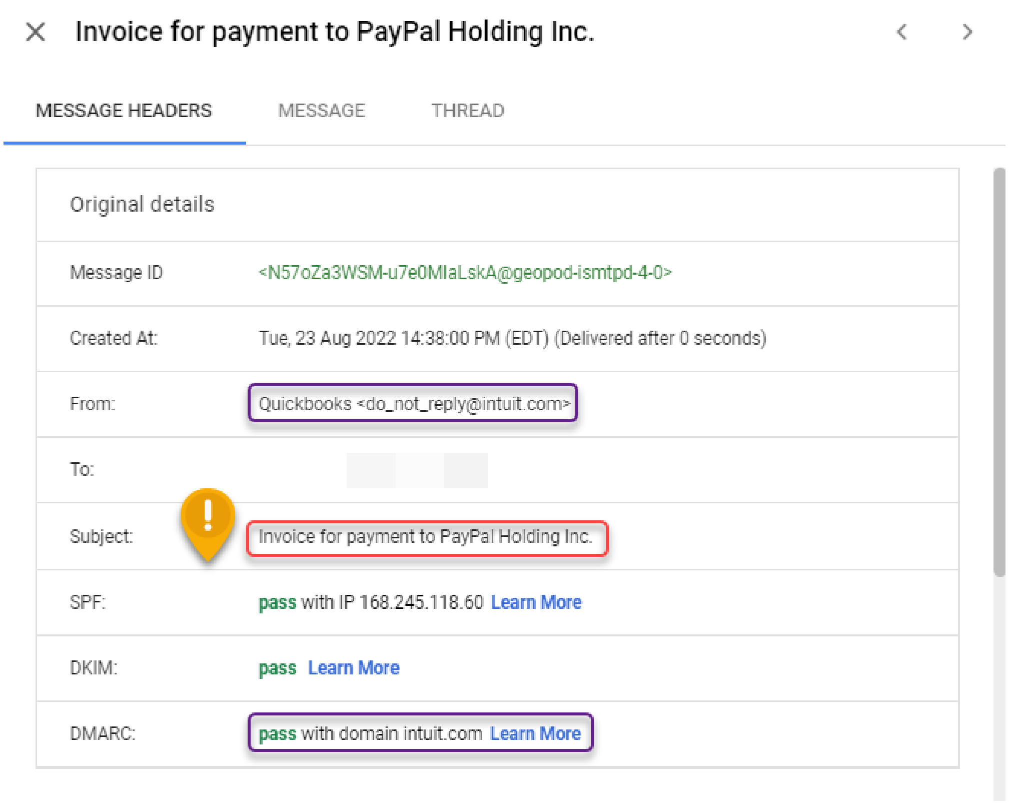
Threat actor creates account → sends message using valid service → victims fall for phish → threat actor operates until account is closed or taken down → threat actor creates new account.

Examples of legitimate services often used with malicious intent include Intuit QuickBooks (and other invoice management apps), Google Drive (and other cloud storage apps), and Herokuapp (and other app development sites).

Analysis

The threat actor creates an account with a legitimate service, in this example, QuickBooks, an “accounting software package developed and marketed by Intuit (Wikipedia).” The scammer then uses that service to send malicious messages, in this case, a falsified invoice, that passes email security checks due to the legitimate nature of the message.

Below are the original details of this message, viewed in the Google Admin portal. As clear from the details outlined in purple, this message was legitimately sent from intuit.com.



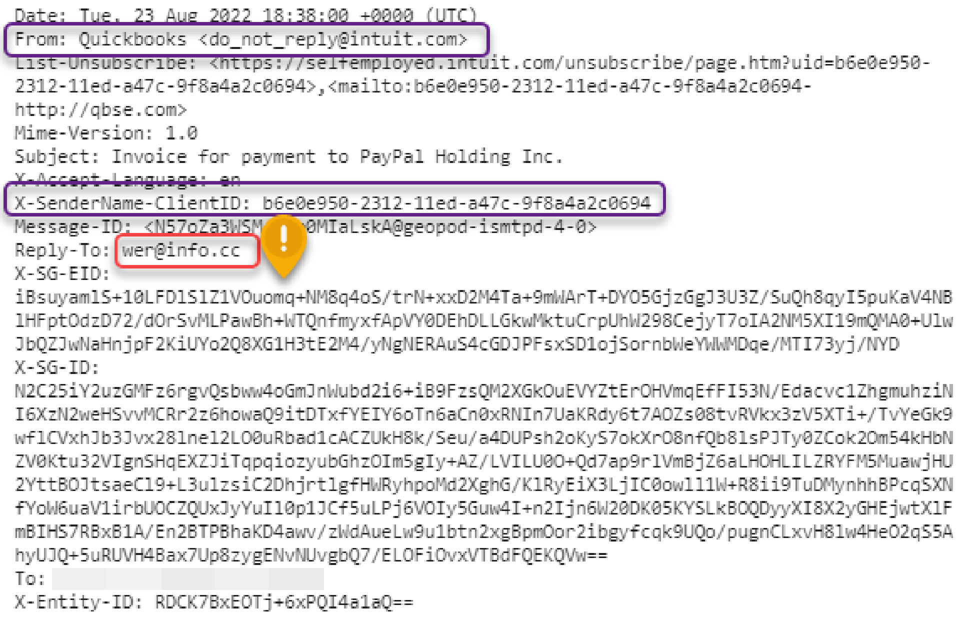
Invoice for payment to PayPal Holding Inc.

Original details

Message ID	<N57oZa3WSM-u7e0MIaLskA@geopod-ismtpd-4-0>
Created At:	Tue, 23 Aug 2022 14:38:00 PM (EDT) (Delivered after 0 seconds)
From:	Quickbooks <do_not_reply@intuit.com>
To:	[redacted]
Subject:	Invoice for payment to PayPal Holding Inc.
SPF:	pass with IP 168.245.118.60 Learn More
DKIM:	pass Learn More
DMARC:	pass with domain intuit.com Learn More

Red Flag(s): PayPal does not use another invoice application, like Intuit QB, to send invoices – PayPal is itself an invoice application.

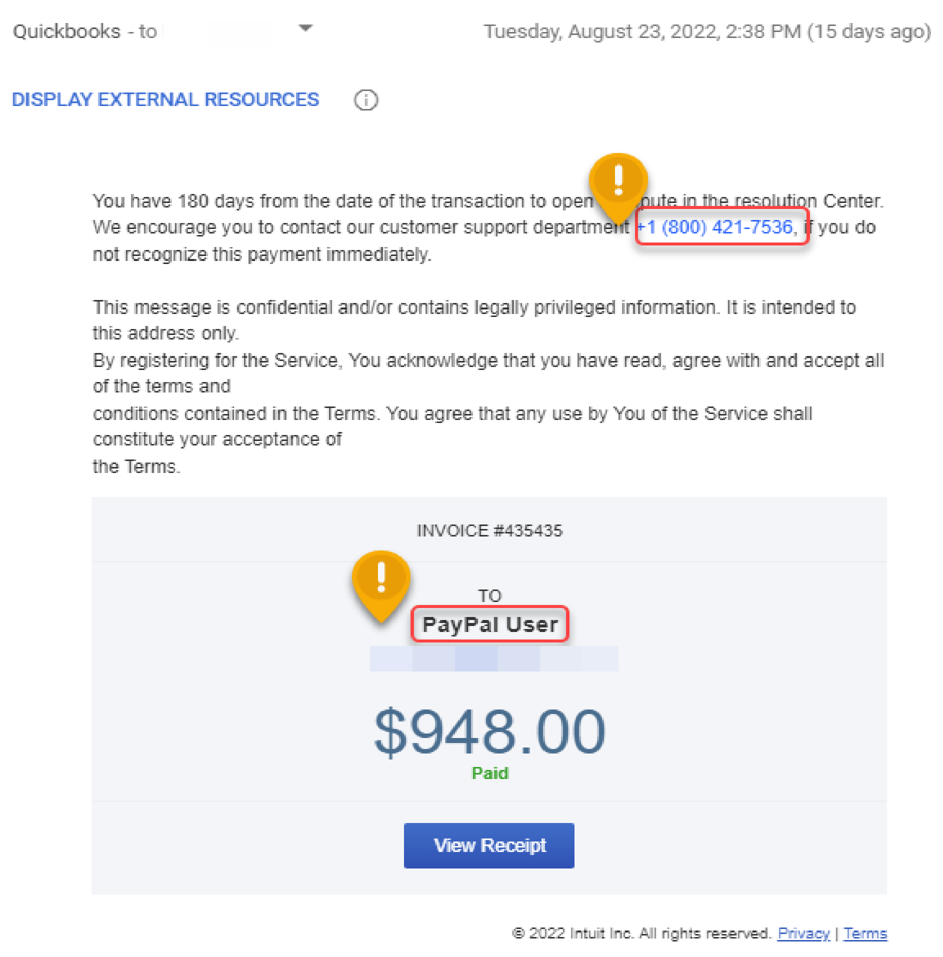
Further analysis of the raw header (below) shows additional proof that this was sent via Intuit QB – and even provides a client ID!



```
Date: Tue, 23 Aug 2022 18:38:00 +0000 (UTC)
From: Quickbooks <do_not_reply@intuit.com>
List-Unsubscribe: <https://selfemployed.intuit.com/unsubscribe/page.htm?uid=b6e0e950-
2312-11ed-a47c-9f8a4a2c0694>,<mailto:b6e0e950-2312-11ed-a47c-9f8a4a2c0694-
http://qbse.com>
Mime-Version: 1.0
Subject: Invoice for payment to PayPal Holding Inc.
X-Accept-Language: en
X-SenderName-ClientID: b6e0e950-2312-11ed-a47c-9f8a4a2c0694
Message-ID: <N57oZa3WSM   0MIaLskA@geopod-ismtpd-4-0>
Reply-To: wer@info.cc
X-SG-EID:
iBsuyam1S+10LFD1S1Z1VOuomq+NM8q4oS/trN+xxD2M4Ta+9mWArT+DYO5GjzGgJ3U3Z/SuQh8qyI5puKaV4NB
1HFptOdzD72/dOrSvMLPawBh+WTQnfmyxfApVY0DEhDLLGkwMktuCrpUhW298CejyT7oIA2NM5XI19mQMA0+U1w
JbQZJwNaHnjpF2KiUYo2Q8XG1H3tE2M4/yNgNERAuS4cGDJPFsxSD1ojSornbWeYWWMDqe/MTI73yj/NYD
X-SG-ID:
N2C25iY2uzGMFz6rgvQsbww4oGmJnWubd2i6+iB9FzsQM2XGkOuEVYZtErOHVmqEfFI53N/Edacvc1ZhgmuhziN
I6XzN2weHSvvMCRr2z6howaQ9itDTxfYEIY6oTn6aCn0xRNIn7UaKRdy6t7AOZs08tvRVkx3zV5XTi+/TvYeGk9
wf1CVxhJb3Jvx28lnel2LO0uRbad1cACZUkH8k/Seu/a4DUPsh2oKyS7okXrO8nfQb8lsPJTy0ZCok2Om54kHbN
ZV0Ktu32VIgnSHqEXZJiTqpqiozyubGhzOIm5gIy+AZ/LVILU0O+Qd7ap9r1VmBjZ6aLHOHLILZRYFM5MuawjHU
2YttBOJtsaeCl9+L3ulzsiC2DhjrtlgfHWRyhpoMd2XghG/K1RyEiX3LjIC0owl11W+R8ii9TuDMynhhBPcqSXN
fYoW6uaV1irbUOCZQUxJyYuI10p1JCf5uLPj6VOIy5Guw4I+n2Ijn6W20DK05KYSLkBOQDyyXI8X2yGHEjwtX1F
mBIHS7RBxB1A/En2BTPBhaKD4awv/zWdAueLw9u1btn2xgBpmOor2ibgyfcqk9UQo/pugnCLxvH81w4HeO2qS5A
hyUJQ+5uRUVH4Bax7Up8zygENvNUvgbQ7/ELOFiOvxVTBdFQEKQVw==
To: [redacted]
X-Entity-ID: RDCK7BxEOTj+6xPQI4a1aQ==
```

Red Flag(s): The reply-to email address is not the account of a reputable business. The email domain info[.]cc is hosted in China and belongs to a site that is used to post information regarding different topics. This is not a likely legitimate sender of a QuickBooks or PayPal invoice to a Maryland user.

The email body looks just like a regular Intuit QB email – that is because it is. All links appear to check out as benign QB links, with a typical payment confirmation and receipt.



Quickbooks - to [redacted]

Tuesday, August 23, 2022, 2:38 PM (15 days ago)

DISPLAY EXTERNAL RESOURCES

You have 180 days from the date of the transaction to open pute in the resolution Center. We encourage you to contact our customer support department +1 (800) 421-7536, if you do not recognize this payment immediately.

This message is confidential and/or contains legally privileged information. It is intended to this address only.
By registering for the Service, You acknowledge that you have read, agree with and accept all of the terms and
conditions contained in the Terms. You agree that any use by You of the Service shall constitute your acceptance of
the Terms.

INVOICE #435435

TO

PayPal User

[redacted]

$948.00

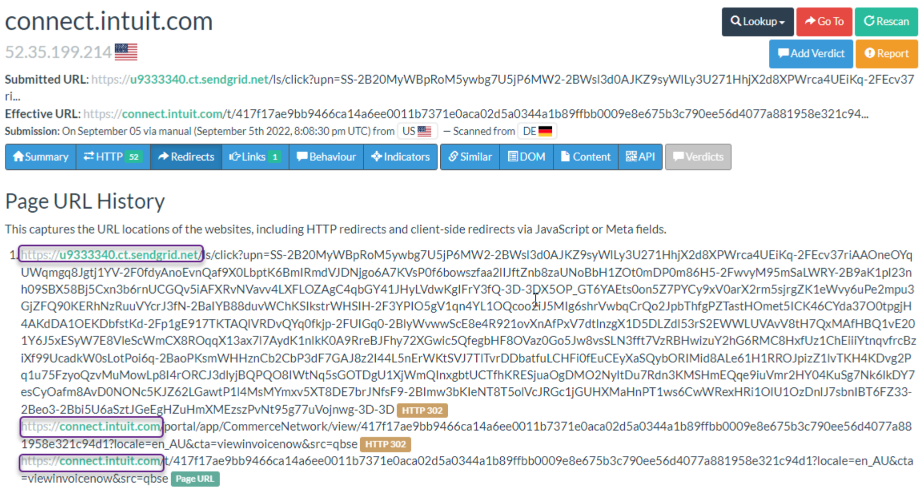
Paid

View Receipt

© 2022 Intuit Inc. All rights reserved. Privacy | Terms

Red Flag(s): The listed phone number for cancellation is 800-421-7536, and the top results for the number on Google are links to verify scams. The real PayPal number, listed on PayPal's website, is 888-221-1161.

What about the actual receipt? The embedded URL is a SendGrid URL, which is a legitimate mailing service. All subsequent redirects are legitimate Intuit domains, as seen below:



connect.intuit.com

52.35.199.214

Submitted URL: https://u9333340.ct.sendgrid.net/ls/click?upn=SS-2B20MyWBpRoM5ywbg7U5jP6MW2-2BWsl3d0AJKZ9syWILy3U271HhjX2d8XPWrca4UEiKq-2FEcv37ri...

Effective URL: https://connect.intuit.com/t/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94...

Submission: On September 05 via manual (September 5th 2022, 8:08:30 pm UTC) from US — Scanned from DE

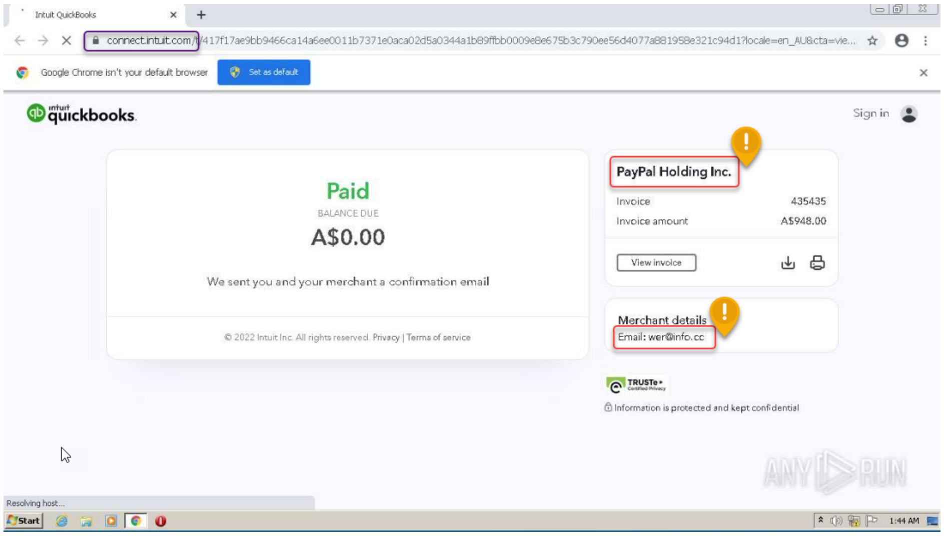
Page URL History

This captures the URL locations of the websites, including HTTP redirects and client-side redirects via JavaScript or Meta fields.

1. https://u9333340.ct.sendgrid.net/ls/click?upn=SS-2B20MyWBpRoM5ywbg7U5jP6MW2-2BWsl3d0AJKZ9syWILy3U271HhjX2d8XPWrca4UEiKq-2FEcv37riAAOneOYqUWqmgq8Jgtj1YV-2F0fdyAnoEvnQaf9X0LbptK6BmIRmdVJDNjgo6A7KVsP0f6bowszfaa2IIJftZnb8zaUNoBbH1ZOt0mDP0m86H5-2FwvyM95mSaLWRY-2B9aK1pl23nh09SBX58Bj5Cxn3b6rnUCGQv5iAFXRvNVavv4LXFLOZAgC4qbGY41JHyLVdwKgIFrY3fQ-3D-3DX5OP_GT6YAEts0on5Z7PYCy9xV0arX2rm5sjrgZK1eWvy6uPe2mpu3GjZFQ90KERhNzRuuVYcrJ3fN-2BaIYB88duvWChKSIkstrWHSIH-2F3YPIO5gV1qn4YL1OQcoo2iJ5MIg6shrVwbqCrQo2JpbThfgPZTastHOmet5ICK46CYda37O0tpgjH4AKdDA1OEKDbfstKd-2Fp1gE917TKTAQIVRDvQYq0fkjp-2FUIGq0-2BlyWvwwScE8e4R921ovXnAfPxV7dtInzgX1D5DLZdl53rS2EWWLUVAvV8tH7QxMAfHBQ1vE201Y6J5xESyW7E8VleScWmCX8ROqqX13ax7l7AydK1nlkK0A9RreBJFhy72XGwic5QfegbHF8OVaz0Go5Jw8vsSLN3fft7VzRBHwizuY2hG6RMC8HxfUz1ChEiiiYtnqvfrcBziXf99UcadkW0sLotPoi6q-2BaoPKsmWHHznCb2CbP3dF7GAJ8z2I44L5nErWKtSVJ7TlTvrDDbatfuLCHFi0fEuCEyXaSQybORIMid8ALe61H1RROJpizZ1lvTKH4KDvg2Pq1u75FzyoQzvMuMowLp8I4rORCJ3dlyjBQPQO8IWtNq5sGOTDgU1XjWmQInxgbtUCTfhKRESjuaOgDMO2NyItDu7Rdn3KMSHmEQqe9iuVmr2HY04KuSg7Nk6lkDY7esCyOafm8AvD0NONc5KJZ62LGawtP1l4MsMYmxv5XT8DE7brJNfsF9-2Blmw3bKIeNT8T5olVcJRGc1jGUHXMaHnPT1ws6CwWRexHRi1OlU1OzDnlJ7sbnIBT6FZ33-2Beo3-2Bbi5U6aSztJGeEgHZuHmXMEzszPvNt95g77uVojnwg-3D-3D HTTP 302
https://connect.intuit.com/portal/app/CommerceNetwork/view/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en_AU&cta=viewinvoicenow&src=qbse HTTP 302
https://connect.intuit.com/t/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en_AU&cta=viewinvoicenow&src=qbse Page URL

The link resolves to a QB page that displays that a balance is all paid up.

Red Flag(s): As mentioned earlier, PayPal does not use QB, nor do they use a Chinese email address with an unfamiliar domain.


Intuit QuickBooks
connect.intuit.com/t/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en_AU&cta=vie...
Google Chrome isn't your default browser
Set as default
intuit quickbooks
Sign in
Resolving host...
Start
1:44 AM
ANY RUN

Paid

BALANCE DUE

A$0.00

We sent you and your merchant a confirmation email

© 2022 Intuit Inc. All rights reserved. Privacy | Terms of service

PayPal Holding Inc.

Invoice	435435
Invoice amount	A$948.00

View invoice

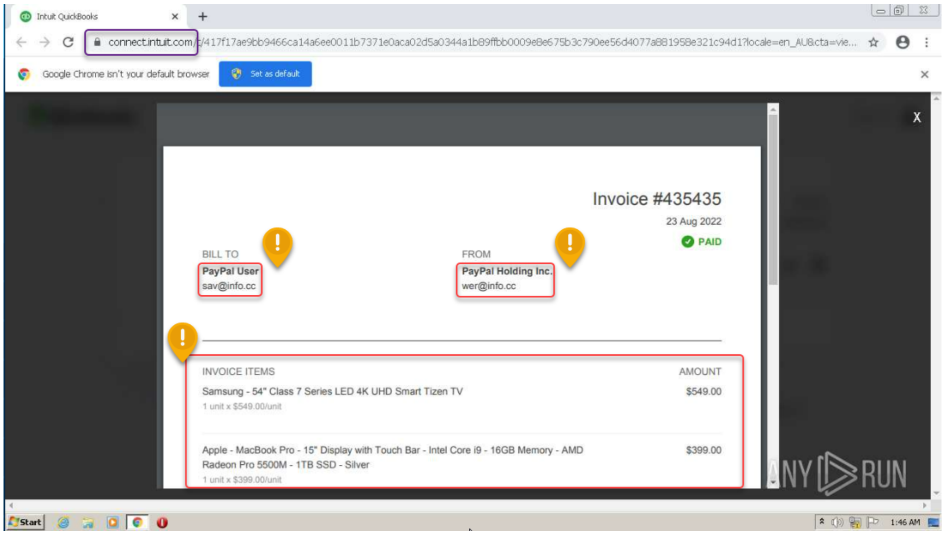
Merchant details

Email: wer@info.cc

TRUSTe Certified Privacy

Information is protected and kept confidential

When clicking the 'view invoice' button above, the user is taken, still without leaving the Intuit domain, to a falsified invoice, pictured below. The same Chinese email address is listed as the "From," and the "To" field is populated by the generic "PayPal user" and a second Chinese email address. The charges, too, are exceedingly high and obviously fake. The phone number listed at the bottom is fake as well and is different than the one listed earlier in the attack.


Intuit QuickBooks
connect.intuit.com/t/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en_AU&cta=vie...
Google Chrome isn't your default browser
Set as default
X
Start
1:46 AM
ANY RUN

Invoice #435435

23 Aug 2022

PAID

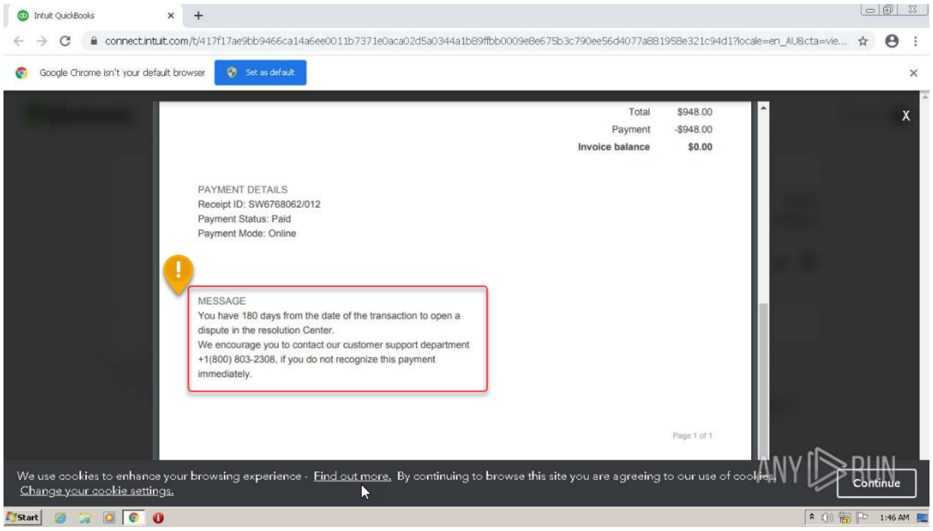
BILL TO

PayPal User
sav@info.cc

FROM

PayPal Holding Inc.
wer@info.cc

INVOICE ITEMS	AMOUNT
Samsung - 54" Class 7 Series LED 4K UHD Smart Tizen TV 1 unit x $549.00/unit	$549.00
Apple - MacBook Pro - 15" Display with Touch Bar - Intel Core i9 - 16GB Memory - AMD Radeon Pro 5500M - 1TB SSD - Silver 1 unit x $399.00/unit	$399.00


Intuit QuickBooks
connect.intuit.com/t/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en_AU&cta=vie...
Google Chrome isn't your default browser
Set as default
Start
1:46 AM
ANY RUN

Total	$948.00
Payment	-$948.00
Invoice balance	**$0.00**

PAYMENT DETAILS
Receipt ID: SW6768062/012
Payment Status: Paid
Payment Mode: Online

MESSAGE
You have 180 days from the date of the transaction to open a dispute in the resolution Center.
We encourage you to contact our customer support department +1(800) 803-2308, if you do not recognize this payment immediately.

Page 1 of 1

We use cookies to enhance your browsing experience - Find out more. By continuing to browse this site you are agreeing to our use of cookies. Change your cookie settings.

Continue

The entire goal of the attack is to initiate contact with the user, causing panic so that they are thinking with less logic. The hacker's goal is to have the user call their fraudulent call center and then extract PII, install malware, or steal funds under the guise of a "refund."

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report activity related to this bulletin to the MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).
- Report any incidents to the MDSOC by filling in this form.

Contact Information

To report suspicious or criminal activity related to information found in this Threat Bulletin, contact the Maryland Security Operations Center at (410) 697-9700 or by email at md-isac@maryland.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. Please state in the report if you are requesting incident response resources or technical assistance related to the incident.

TLP:CLEAR (TLP v1 WHITE) = Disclosure is not limited.

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Recipients may share this information without restriction. Information is subject to standard copyright rules.

For more information about Traffic Light Protocol (TLP) definitions and usage: https://www.cisa.gov/tlp