

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.

< >

MESSAGE HEADERS

MESSAGE

THREAD

Original details	
Message ID	<N57oZa3WSM-u7e0MlaLskA@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:	
Subject:	Invoice for payment to PayPal Holding Inc.
SPF:	pass with IP 168.245.118.60 <a href="#">Learn More</a>
DKIM:	pass <a href="#">Learn More</a>
DMARC:	pass with domain intuit.com <a href="#">Learn More</a>

**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-u7e0MlaLskA@geopod-ismtpd-4-0>  
Reply-To: wer@info.cc  
X-SG-EID: iBsuyam1S+10LFD1S1Z1VUomq+NM8q4oS/trN+xxD2M4Ta+9mWArT+DY05GjzGgJ3U3Z/SuQh8qyI5puKaV4NB1HFptOdZD72/dOrSvMLPawBh+WtQnfmYxfApVY0DEhDLGkwMktuCrpUhw298CeJyT7oIA2NM5XI19mQMA0+UlwJbQZJwNaHjpf2KiUYo2Q8XG1H3tE2M4/yNgNERAuS4cGDJPFsXSD1oJSoRnbWeyWMDqe/MTI73yj/NYD  
X-SG-ID: N2C25iY2uzGMFz6rngvQsbw4oGmJnWubd2i6+iB9FzsQM2XGkOuEVYZtErOHVmqEfiI53N/Edacvc1ZhgmuhziNI6XzN2weHSvvMCRr2z6howaQ9itDTxfYIEY6oTn6aCn0xRNIn7UaKRdy6t7A0Zs08tvRVKx3zV5XTi+/TvYeGk9wf1CVxhJb3Jvx281ne12L00uRbad1cACZUKH8k/Seu/a4DUPsh2oKyS7okXr08nfQb81sPJTy0ZCok20m54kHbNZV0Ktu32VIgnSHqEXZJiTpqqiozyubGhzOIIm5gIy+AZ/LVILU00+Qd7ap9r1VmBjZ6aLH0HLILZRYFM5MuawjHU2YttB0JtsaeC19+L3u1zsiC2Dhjrt1gfHWRyhpomd2XghG/K1RyEiX3LjIC0ow111W+R8ii9TuDMynhhBPcqSXNfYom6uaV1irbUOCZQUxJyYuII0p1JCf5uLPj6VOIy5Guw4I+n2Ijn6W20DK05KYSLkBOQDyyXI8X2yGHEjwX1FmBIHS7R8xB1A/En28TPBhaKD4awv/zldAueLw9u1btn2xgBpmOor2ibgyfcqk9UQo/pugnCLxvH81w4He02qS5AhyUJQ+5uRUVH4Bax7Up8zygENvNUvgbQ7/EL0FI0vXVTBdFQEKQVW==  
To:   
X-Entity-ID: RDCK78xEOTj+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.

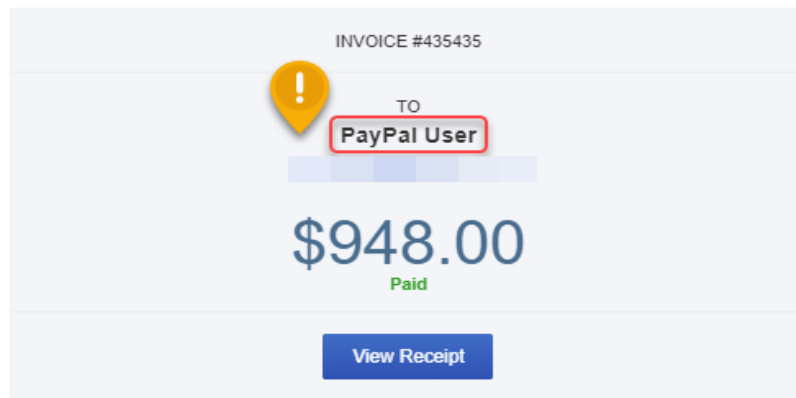
## DISPLAY EXTERNAL RESOURCES



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 at **+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.



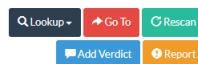
© 2022 Intuit Inc. All rights reserved. [Privacy](#) | [Terms](#)

**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-2B20MyWBpRoM5ywb7U5JP6MW2-2BWsl3d0AJKZ9syWily3U271HhjX2d8XPWrc4UEIKq-2FEcv37rIAAOneOYqri...>

Effective URL: [https://connect.intuit.com/t/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en\\_AU&cta=viewinvoicenow&src=qbse](https://connect.intuit.com/t/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en_AU&cta=viewinvoicenow&src=qbse)

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



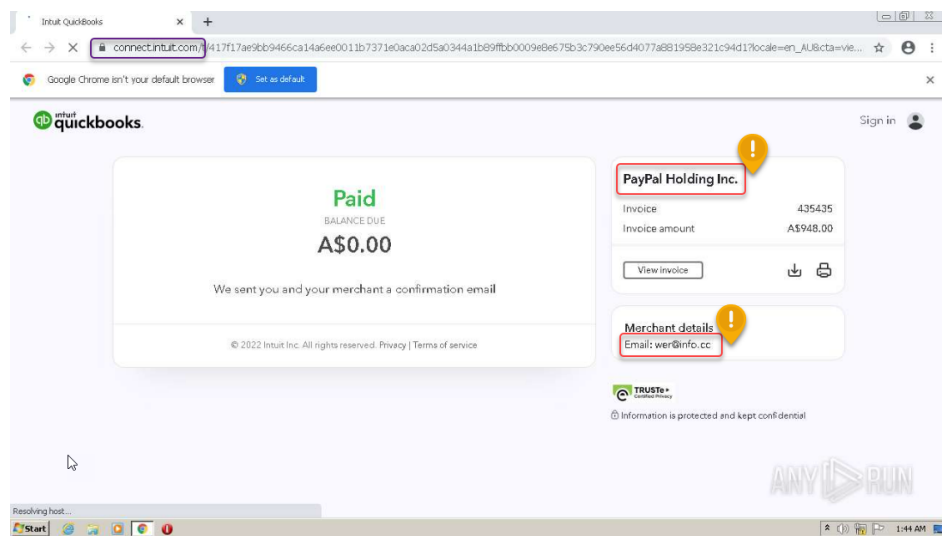
## Page URL History

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

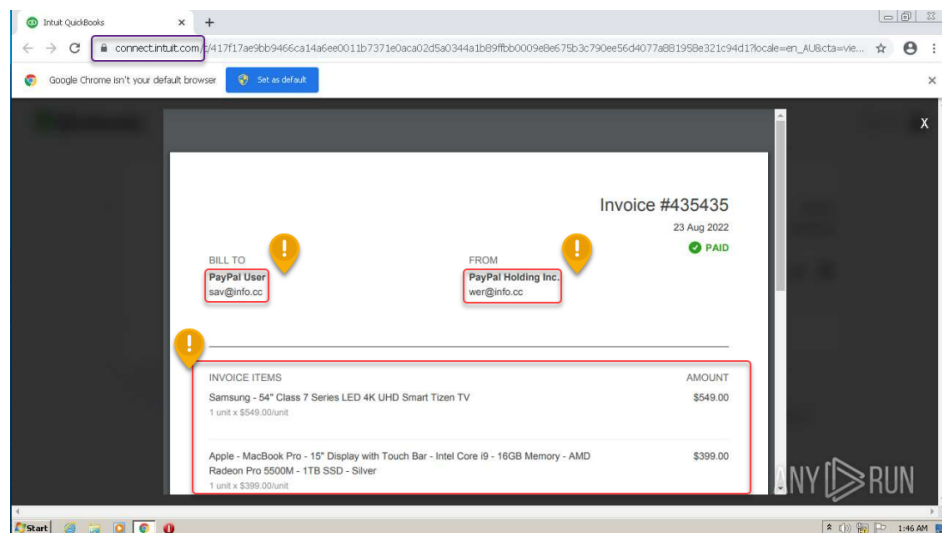
1. <https://u9333340.ct.sendgrid.net/ls/click?upn=SS-2B20MyWBpRoM5ywb7U5JP6MW2-2BWsl3d0AJKZ9syWily3U271HhjX2d8XPWrc4UEIKq-2FEcv37rIAAOneOYqri...>  
UWmqg8Jgtj1YV-2F0dyAnoEvnQaf9X0LbptK6BmlRmdVJDNJgo6A7KVp0f6bowszfaa2lJftZnb8zaUNoBbH1Z0t0mDP0m86H5-2FvvyM95mSaLWRY-2B9aK1pl23n  
h09SBX58BJ5Cxn3b6rnUCQGv5IAFXRvNvav4LXFLOZAgC4qbGY41JHylVdwKglFRY3fQ-3D-3DX5OP\_GT6YAEts0on5Z7PYCY9xV0arX2rm5sjrgZK1eWvy6uPe2mpu3  
GjZFQ90KERhNzRuuVYcrJ3N-2BaLYB88duvWChKSlkstrWHSIH-2F3YPI05gV1qn4YL1OQcoo8iJ5Mlg6shrVwbqCrQe2JpbThfgPZTastHomet5ICK46CYda3700tpgJH  
4AKdDA1OEKDfbstKd-2Fp1gE917TKTAQIVRDvQYq0fKjp-2FUIGq0-2BlyWwwwScE8e4R921ovXnAfPxV7dtlnzgX1D5DLZdl53rS2EWWLUVAvV8H7QxMAfHBQ1vE20  
1Y6J5xESyW7EBVleSWMcX8ROqqX13ax717Aydk1nlkK0A9RreBJFhy72XGwic5QfegbHF80Vaz0Go5Jw8vsSLN3ft7VzRBHwizuY2hG6RMC8BxfUz1ChEliYtnqvfrBz  
IXf99UcadKW0sLotPoi6j-2BaOPKsmWHHzCb2CbP3dF7GAJ8z2144L5nErWktSVJ7TITvrDDbatfuLCHfIOEuCEyXaSqybORIMid8ALe61H1RROJplz21vTKH4KdVg2P  
q1u75FzoQzvMuMowlp8l4rORCJ3dljyBQPQO8IWtNq5sGOTDgU1XWmQlnxgbtUCTfhKRESJuaGDMO2NyttDu7Rdn3KMSHmEQqe9luVmr2HY04KuSg7Nk6lkDY7  
esCyOafm8AvDONONc5KJZ62LgawtP14MsMymxv5XT8DE7brJNfSf9-2Blmw3bKleNT8T5oIVcJRGc1JGUHXMhHnPT1ws6CwWRexHR10IU10zDnIJ7sbnlBT6FZ33-  
2Beo3-2Bbl5U6a5ztJGeEgH2uHmXMEzszPvNt95g77V0jnwg-3D-3D [HTTP 302](#)  
[https://connect.intuit.com/portal/app/CommerceNetwork/view/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en\\_AU&cta=viewinvoicenow&src=qbse](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](https://connect.intuit.com/t/417f17ae9bb9466ca14a6ee0011b7371e0aca02d5a0344a1b89ffbb0009e8e675b3c790ee56d4077a881958e321c94d1?locale=en_AU&cta=viewinvoicenow&src=qbse) [Page URL](#)

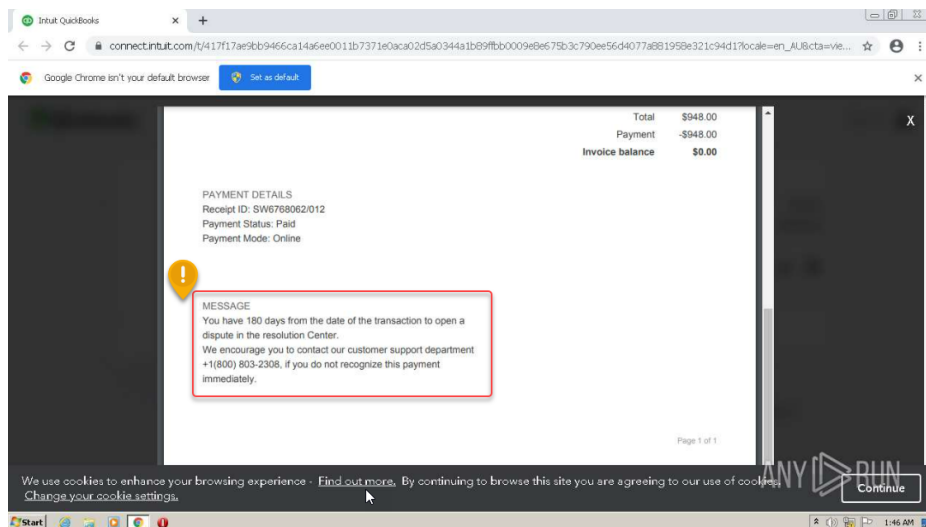
The link resolves to a QB page that displays that a balance is all paid up.

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



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.





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>