

Phishing Email Analysis Report

1. Introduction

The objective of this report is to demonstrate my ability to investigate phishing emails using various tools, including PhishTool, Cisco Talos Intelligence, and VirusTotal. This exercise aims to consolidate my knowledge acquired through the TCI learning path on TryHackMe. The phishing email analysed in this report was sourced from the Threat Intelligence Tools room on TryHackMe. Please keep in mind that I am in no way experience at analysing phishing emails and therefore I'm confident my process may be flawed. Therefore, any tips on how to better perform email analysis would be greatly appreciated.

2. Overview of the Phishing Email

The phishing email in question claims to contain a purchase order attached as an Excel file. To analyse this email, I started off by importing it into PhishTool, which provided details insights into the email's structure and content:



Drag and drop an email here

PhishTool can analyse .eml, .msg and .txt message formats.

Choose file

3. PhishTool Analysis

PhishTool extracted critical information from the email headers, including the following:

- **From Address:** 'quickbooks@notification.intuit.com'
- **Display Name:** Customer Service
- **Reply-To Address:** 'quickbooks@notification.intuit.com'
- **Originating IP Address:** 163.176.91.27

From	quickbooks@notification.intuit.com	***
Display name	Customer Service	
To	None	
CC	None	
Timestamp	01:19 am, Oct 14th 2021	
Reply-To	quickbooks@notification.intuit.com	***
Return-Path	None	
Originating IP	163.176.91.27 (Hop 1) ▼	***
rDNS	None	

Please find our purchase order attached to this email.
Thank you for your business - we appreciate it very much.
Sincerely,

Purchase Order Summary -----
Sale #: 5606
Sale Date: 10/13/2021
Total: \$3,431.00

The complete version has been provided as an attachment to this email.

Key Observations:

- The from email address is inconsistent with the display name 'Customer Service'.
- The Reply-To address matches the From address, which is uncommon in phishing attempts where attackers often use different Reply-To addresses to deceive recipients. It is a common tactic to provide a different Reply-to email address whilst spoofing a legitimate from email address. The reason being that a victim might reply to the phishing email believing they are replying to the email address shown in the from header.

4. IP Address Analysis

The originating IP address was further checked against Cisco Talos Intelligence and VirusTotal, revealing no reports of malicious activity:

5. Security Measures

PhishTool revealed that the email lacked essential security/authentication measures such as SPF, DKIM, and DMARC which are all briefly explained below:

- **Sender Policy Framework (SPF)** enables you to identify the mail servers that are allowed to send emails for a given domain. SPF records list all the IP addresses of all the mail servers that are allowed to send emails for a given domain. If a mail server receives an email, it can check it against the SPF record before sending it on to the recipient's inbox. Failure to use SPF records can allow threat actors to spoof your domain and carry out more effective phishing campaigns.
- **DomainKeys Identified Mail (DKIM)** enables domain owners to automatically sign emails from their domain using a digital signature. It works as follows: firstly, a DKIM record stores the domain's public key where mail servers receiving emails from the domain can check this record to obtain the public key. The private key is kept by the sender who signs the email's header with the private key. Lastly, mail servers receiving the email can verify the sender's private key (so their proof of identity) by using the public key.
- **Domain-based Message Authentication Reporting and Conformance (DMARC)** informs a receiving email server what to do once they have checked the SPF and DKIM records. For example, it can be configured to quarantine emails if SPF or DKIM fails, etc. The DMARC policies are stored in DMARC records.

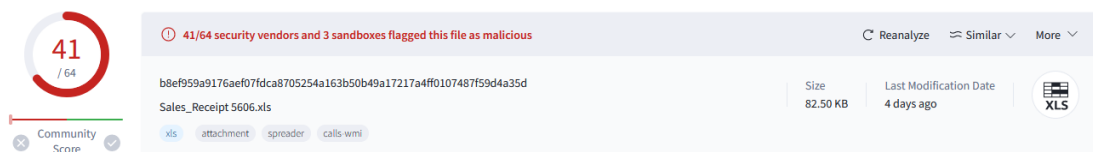
SPF	
Result	None
Originating IP	163.176.91.27 (Hop 1) ▼
rDNS	None
Return-Path domain	None
SPF record	None
DKIM	
Result	None
Verification(s)	0 Signatures
Selector	None
Signing domain	None
Algorithm	None
Verification	None
DMARC	
Result	None
From domain	notification.intuit.com
DMARC record	None

6. Attachment Analysis

The attached Excel file was identified by PhishTool as containing macros, which is a strong indicator of potential malicious activity. The file hashes (MD5, SHA-1, and SHA-256) were used to further analyse the attachment using VirusTotal and Cisco Talos Intelligence.

File Hash Analysis

- **VirusTotal Results:** The attachment was flagged as malicious by multiple antivirus engines/vendors.



- **Talos Intelligence Results:** The file was identified as a Dridex infostealer and trojan, confirming its malicious nature.

The image shows the Cisco Talos Intelligence file reputation page for the same SHA-256 hash. The page is dark-themed and displays the following information:

- FILE REPUTATION:** A biohazard icon and the word 'Malicious' in orange.
- TALOS WEIGHTED FILE REPUTATION SCORE:** 'Score not available.' Below this is a button that says 'Submit a File Reputation Ticket'.
- SHA256:** B8EF959A9176AEF07FDCA8705254A163B50B49A17217A4FF0107487F59D4A35D. A note below states: 'Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.'
- FILE SIZE:** 84480 bytes.
- SAMPLE TYPE:** OLE 2 Compound Document, v3.62, SecID 0x1, 2 FAT sectors, Mini FAT start sector 0x7f, 2 Mini FAT sectors : Microsoft Excel 97-2003 addin.
- CISCO SECURE ENDPOINT DETECTION NAME:** XLS.INV.B8EF959A.CAE.Talos.
- ASSOCIATED DOMAINS FOR THIS HASH:** 'Domains not available.'
- DETECTION ALIASES:** A list of aliases including 'Downloader/XLS.Dridex', 'W97M/Agent.2325811', 'VBA.Dropper-GX [Trj]', 'VB.Trojan.Valyria.5569', 'virus', 'malicious confidence: 100%', 'X97M/Dridex.A.geniEldorado', and 'VBA/Agent.AD55tr'.

A small note at the bottom right says '*Limited to SHA256 lookup'.

7. Indicators of Compromise (IoCs)

- **Malicious Domain:** notifications.inttuit.com
- **File Hashes:**
 - o **MD5:** e63deaea51f7cc2064ff808e11e1ad55
 - o **SHA-1:** 4d58ec4c978988f16468cda2323103ae62b2baea

- **SHA-256:**

b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d

8. Conclusion

This analysis confirms that the email in question is indeed malicious, leveraging social engineering tactics to deceive recipients into downloading malware. By applying a structured analysis process using PhishTool, Cisco Talos Intelligence, and VirusTotal, we can effectively identify phishing threats. This approach can be adapted for future analyses to determine the legitimacy of new email samples.