Phishing Email

Project 2

Artifacts Manual

From :App Store <customerid272717-15@pusingsendiriaku.info>
Recipient :ixxxx@hxxxxxxxxxx.com
Reply-to : undisclosed-recipient
Date and Time: Mon, 28 May 2018 01:01:01 +0700
Subject Line : Re : [Order-Confirmed] Thanks for buying on App Store at May, 27 2018 #271628 [CONFIRMATION]
Recipient(s): ixxxxx@xxxxx.com
Sending IP: 74.125.82.67
rDNS Host:
Suspected Link URL : hxxp://ykm.de/YWVmMT
Attachment: Invoice_Receipt_2837193894655273.pdf

Email Description

The email appears to be a phishing attempt impersonating Apple Store. The body of the email is empty, but it contains a PDF attachment. The subject line suggests that it is regarding a purchase made the previous day and asking for confirmation of payment . It then prompts the recipient to click on a link if I believe I did not authorize the payment.

URL Analysis :

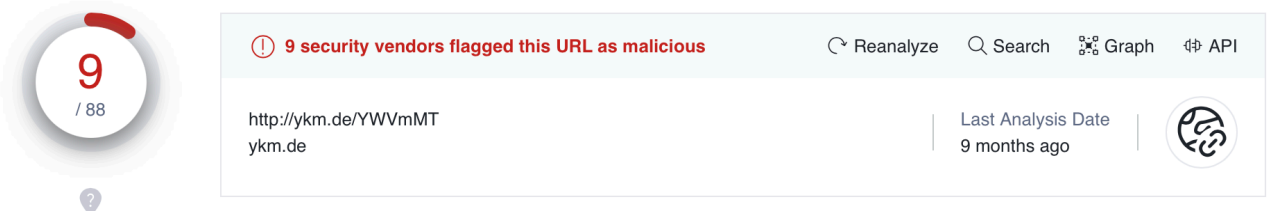
WHOIS : Registrar Status: Active connection, Last Updated: August 19, 2020. Tech Contact: Not available. IP Address: 188.40.79.62 hosted on a dedicated server in Germany (Bayern, Gunzenhausen) by Hetzner Online GmbH. Warning: Incomplete Record from Whois server.

URLSCAN.IO: —> http://ykm.de/
The main IP, 188.40.79.62, is located in Germany and belongs to HETZNER-AS. The TLS certificate for the website was issued by R3 on July 3rd, 2023, and is valid for 3 months. It has no classification verdict in Google Safe Browsing, and the current DNS A record is 188.40.79.62, associated with HETZNER-AS in Germany.

URLSCAN.IO: —> hxxp://ykm.de/YWVmMT
The scanning of the complete URL did not show any results or findings.

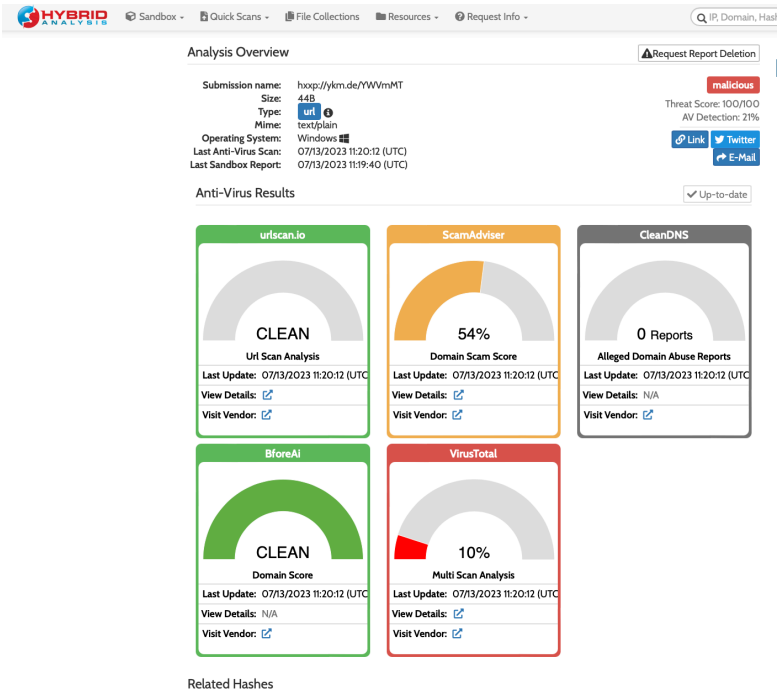
URL2PNG : —> hxxp://ykm.de/YWVmMT
The scanning of the complete URL did not ALSO show any results or findings.

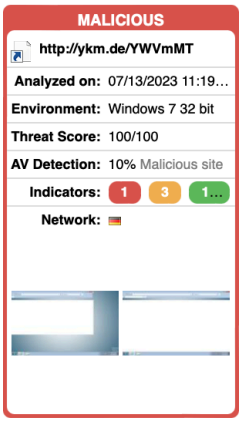
VirusTotal :
VirusTotal has provided notable findings indicating that 9 security vendors have classified this URL as malicious and phishing.

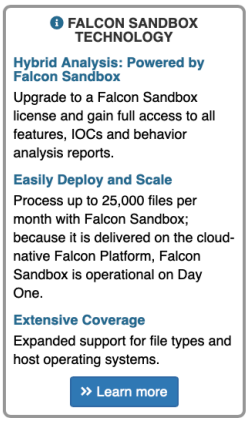


HYBRID ANALYSIS:

HYBRID ANALYSIS shown a significant report of a threat score of 100/100 and AV Detection of 21%.





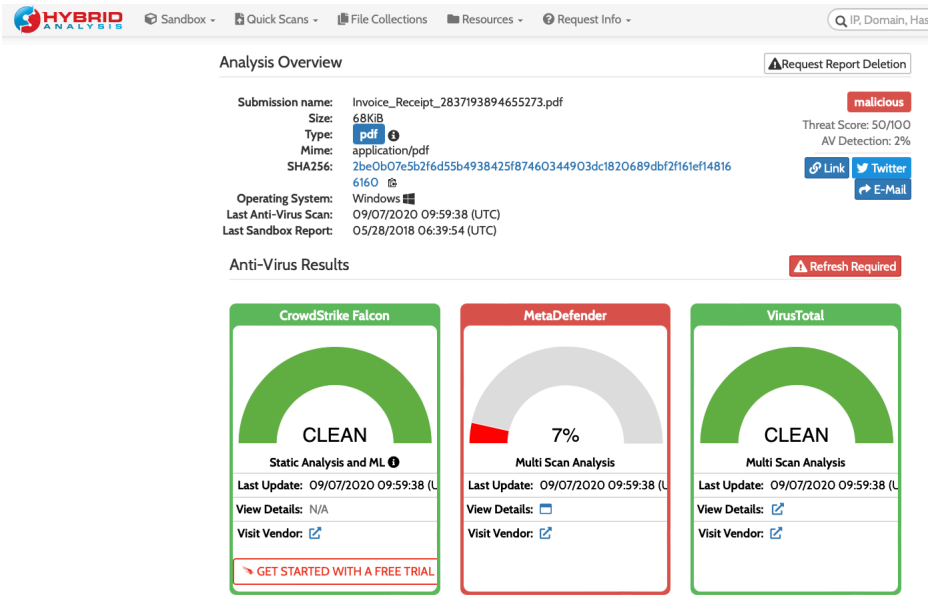


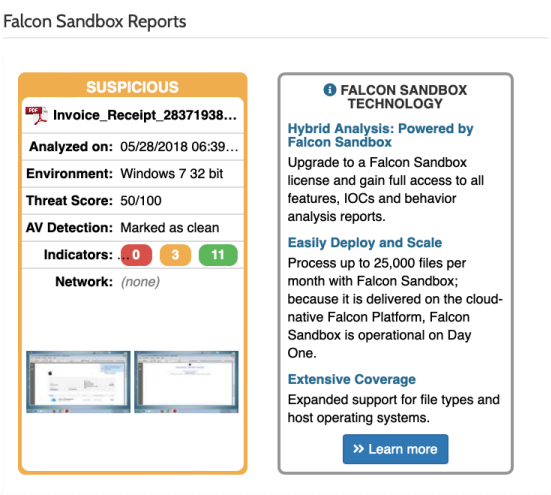
File Analysis :

Submission name: Invoice_Receipt_2837193894655273.pdf
Size : 68KiB
Type: pdf
SHA256: 2be0b07e5b2f6d55b4938425f87460344903dc1820689dbf2f161ef148166160

HYBRID ANALYSIS:

HYBRID ANALYSIS has shown significant results about the attached file to categorise as "Malicious" with 50/100 score.





Defensive measures taken

[1] The sending email address DO NOT come from https://www.apple.com/uk/.
[2] Blocking the sender domain "customerid272717-15@pusingsendiriaku.info" would stop more malicious emails being delivered to me.

- ***[Action Taken]*** Sending Address Block (Email Gateway)
"***customerid272717-15@pusingsendiriaku.info***" on 13 July at 15:28 PM by I. Jama.

[3] The URL "hxxp://ykm.de/YWVmMT**"** used within the email was created recently for purely malicious purposes, and there is no business justification for me to visit it, and I am blocking the URL to prevent others users (My family) from clicking unattentionnly.

- ***[Action Taken]*** *The malicious url link is blocked:*
  - hxxp://ykm.de/YWVmMT (Web Proxy) on 13 July at 15:28 PM by Idriss Jama.

The investigating analyst

- The email appears to be weird looking, the presence of a "Reply-to: " address pointing to a "undisclosed-recipient" raises suspicion.
- To prevent any further malicious emails from the sending email, It has been blocked.
- The persuading hidden URL is potentially Malicious, with 9 vendors flagging it as such.
- The domain associated with the URL was intentionally created for malicious purposes, and there is no valid reason to revisit it.
- As a precautionary measure, the sender and the URL were blocked by Idriss Jama on July 13, 2023.