PHISHING EMAIL ANALYSIS

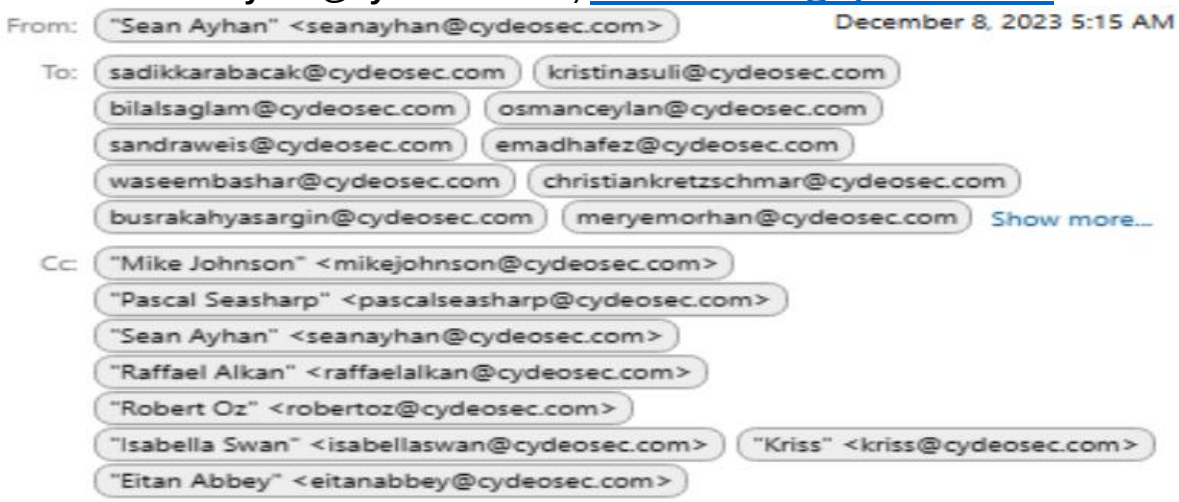
By merkmostafaei

Sender Information:
sean Ayhan seanayhan@cydeosec.com from mail.cydeosec.com ([127.0.0.1])

Receiver Information:

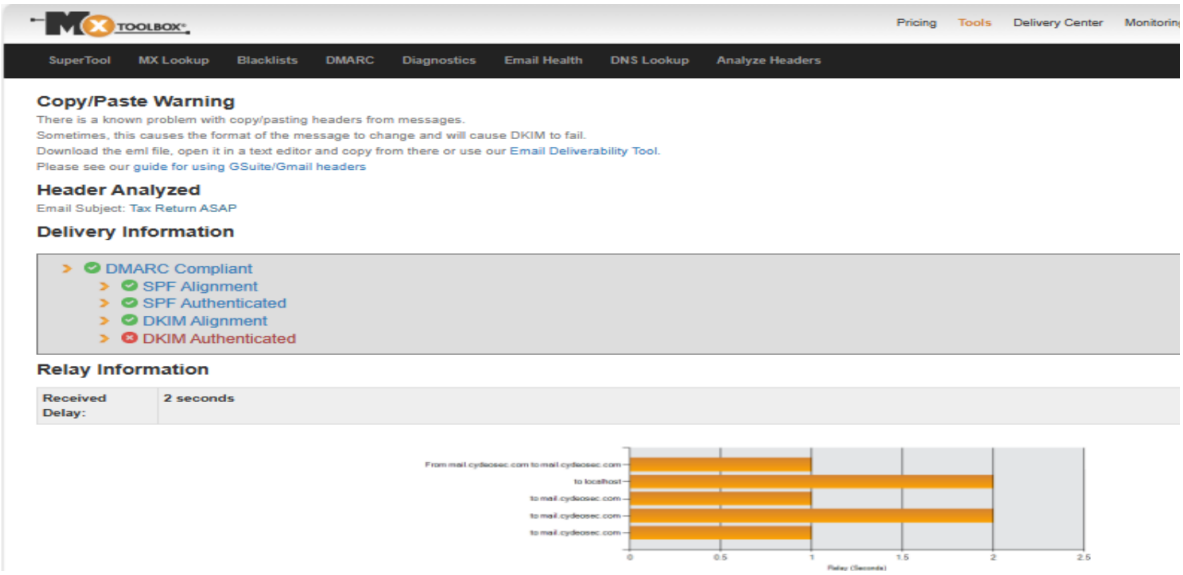
**sadikkarabacak@cydeosec.com, kristinasuli@cydeosec.com,
bilalsaglam@cydeosec.com, osmanceylan@cydeosec.com,
sandraweis@cydeosec.com, emadhafez@cydeosec.com,
waseembashar@cydeosec.com, christiankretzschmar@cydeosec.com,
busrakahyasargin@cydeosec.com, meryemorhan@cydeosec.com,
aseelhussein@cydeosec.com, ibrahimsmajli@cydeosec.com,
hayrunisafakioglu@cydeosec.com, necmedinkera@cydeosec.com,
nitaarapi@cydeosec.com, petramartinavrancic@cydeosec.com,
burakcaliskan@cydeosec.com, surkhaybakirli@cydeosec.com,
halimulatifeilure@cydeosec.com,
talifujiangwusimanjiang@cydeosec.com,
abuduainikailibinuer@cydeosec.com, turansadigli@cydeosec.com,
danuthalau@cydeosec.com, medinmujezini@cydeosec.com,
osimkhonibrokhimov@cydeosec.com, yasinozturk@cydeosec.com,
mohammadrezamostafaei@cydeosec.com,
fazlulhaqueakik@cydeosec.com,
mehmetskaya@cydeosec.com, enesfatichmoustafa@cydeosec.com,
altinrashica@cydeosec.com, omerbicanoglu@cydeosec.com,
mustafaaghamirzayev@cydeosec.com,
hajimuradrazagov@cydeosec.com,
volkancelebi@cydeosec.com, alisirseidi@cydeosec.com,
sabihaturgut@cydeosec.com, bayramsaitmayda@cydeosec.com,
bilalsevinc@cydeosec.com, burakacar@cydeosec.com,
brandisahan@cydeosec.com, oytunazkanar@cydeosec.com,
sumeyrafakioglu@cydeosec.com, akingurcan@cydeosec.com,
taneraydin@cydeosec.com, hannaelizabethjohnson@cydeosec.com,
abrorisaev@cydeosec.com, annieercan@cydeosec.com,
ivanarsic@cydeosec.com, saeedhashmi@cydeosec.com,
mavzunaakhmedova@cydeosec.com,
mohammadibrahimhussein@cydeosec.com,
malgorzataannaniedzwiedz@cydeosec.com,
milicadragutinovic@cydeosec.com, jaimecarlin@cydeosec.com,
samsooralikhail@cydeosec.com, jalalzadran@cydeosec.com,
zanashwan@cydeosec.com, raghdaalqaysi@cydeosec.com,
ivanamanasijevski@cydeosec.com, annavohar@cydeosec.com,**

arslankhakiyev@cydeosec.com, milenamanoleva@cydeosec.com, muhammadzhondavronov@cydeosec.com, zahrakhilwatgar@cydeosec.com, seanestramonte@cydeosec.com, bilalaslan@cydeosec.com, mohamedaminebencaid@cydeosec.com, huseinlizalovic@cydeosec.com, samirlizalovic@cydeosec.com, sabinadzafic@cydeosec.com, bilalzaman@cydeosec.com, jaouadimesmouden@cydeosec.com, niginanovruzova@cydeosec.com, mehtaperguven@cydeosec.com, faruksahin@cydeosec.com, abdellatifsaeed@cydeosec.com, bezhansafah@cydeosec.com, ailiaizaier@cydeosec.com, jeyhunshahmardanov@cydeosec.com, davidberrios@cydeosec.com, zainafzal@cydeosec.com, alexportnoy@cydeosec.com, abdulbasitamin@cydeosec.com, mamurjonismatov@cydeosec.com, talibsuliman@cydeosec.com, rigobertoayala@cydeosec.com, iraklishereshashvili@cydeosec.com, kwestanabdalrahman@cydeosec.com, nihalorhan@cydeosec.com, yahyaselmancanbaz@cydeosec.com, zuhurullahsarwari@cydeosec.com, nemtullahkhalili@cydeosec.com, imankassim@cydeosec.com, ahmadgulbahari@cydeosec.com, yahyaatta@cydeosec.com, moebagheri@cydeosec.com, najibnazari@cydeosec.com, faridabbasov@cydeosec.com, elshatali@cydeosec.com, bilallamharti@cydeosec.com, recepkonus@cydeosec.com, ilyarkasgarli@cydeosec.com, murodjonkhudaykulov@cydeosec.com, burakfehmiozkan@cydeosec.com, israfilyilmaz@cydeosec.com, emingun@cydeosec.com, hamzamayoufi@cydeosec.com, azizullahtahiri@cydeosec.com



Subject Line:
Tax Return ASAP

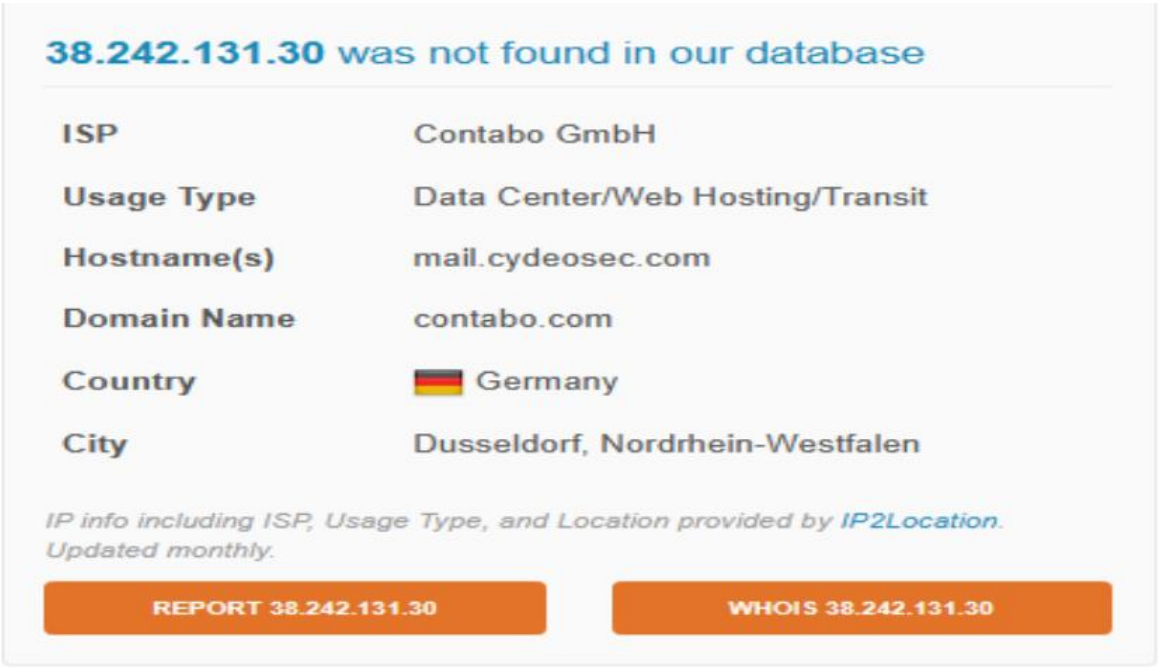
Header Information:
Authentication results. SPF, DKIM, DMARC
SPF alignment
SPF authenticated
DKIM alignment
DKM authenticated faild



sender IP address.: ip : 38.242.131.30

Investigation in abuseipdb:
Hostname(s) mail.cydeosec.com
Domain Name contabo.com
Country Germany

https://www.abuseipdb.com/check/38.242.131.30



investigation in shodan:

OpenPorts
22 25 53 110 143 389 443 465 587 993 995 5222 5269 7071 8143 8443 11211

Investigation in mxtoolbox:

DNS record:

DMARC Record Published
DMARC Record found
Status Ok
DMARC Policy Not Enabled
DMARC Quarantine/Reject policy enabled
Status Ok
DNS Record Published
DNS Record found

https://mxtoolbox.com/SuperTool.aspx?action=mx%3acydeosec.com&run=toolpage

References:
<202187753.781.1670025136233.JavaMail.zimbra@cydeosec.com>Check header

Content and Body:
grammar and spelling errors.seems suspicious.

------=_Part_7026_1639766043.1702041342812
Content-Type: multipart/alternative;
boundary="=_9d0642df-b363-4659-bc5e-1c16f4024281"

--=_9d0642df-b363-4659-bc5e-1c16f4024281
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 7bit

****THIS IS A PHISHING EMAIL EXERCISE. DO NOT DOWNLOAD THE FILE DIRECTLY ON YOUR COMPUTER.****
Follow the instructions which have shown you in the class and analyze it. HAVE FUN!!

Hi There!

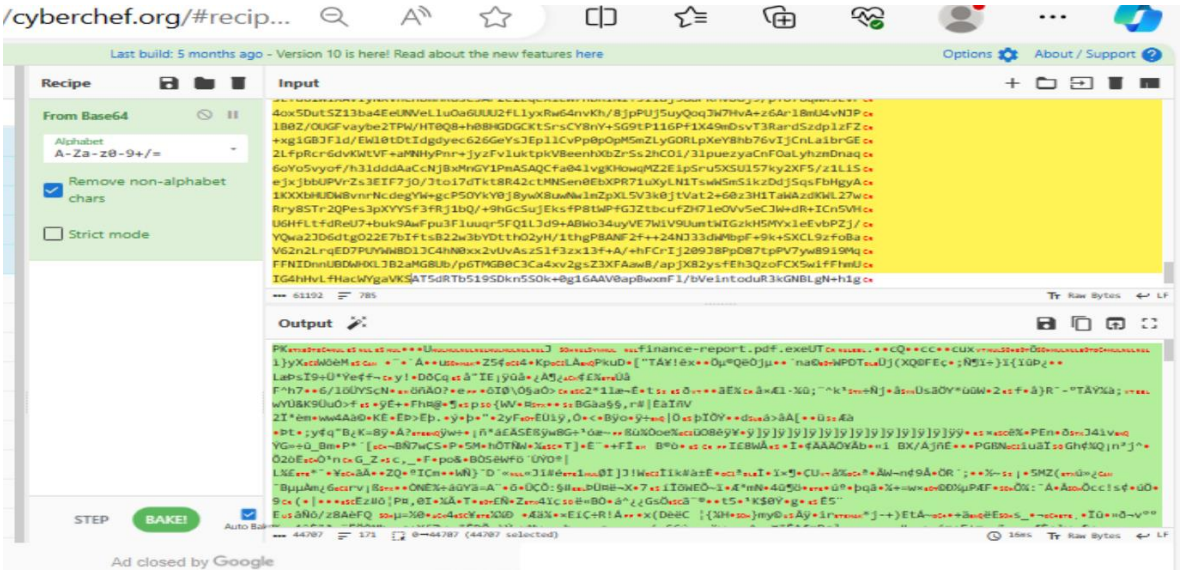
This is Sean from finance department. I started last week and wishing meet with you official!
We are checking employees tax returns. So, may you please check attached file immediately ? You will find receipt for year 2021 and please let me know if you need anything else.

Thank you!

Sean

decode body base 64:

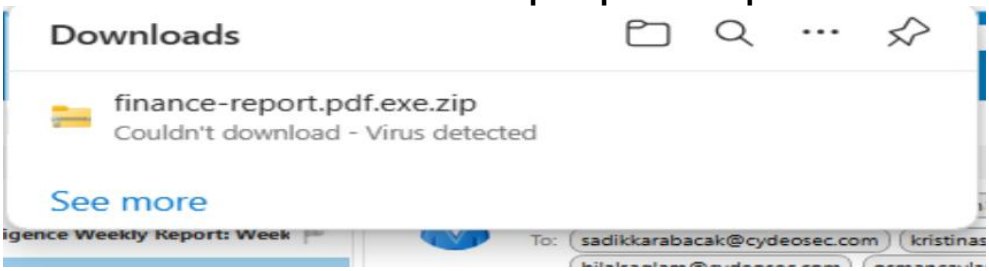
×të• • }½úßŽ¹õ·9{W5éþ4Û• ¼Ô'µéíO*^µìmþf• ÈZ®Ç-ë_ð*'µéíN¶§±÷«w(v)àªê-yÚkŠ{ZnW¡¶i[¡Ü• Šû-*
ÊWÜ7èž ×Úš)rj¸š –¥½ëbq«ž Ë-®'ß¢{l,Þ×jmr%ħ¯M4ÓMŠ÷Zµ©š ®G«pÇ



Links and URLs: (if any)

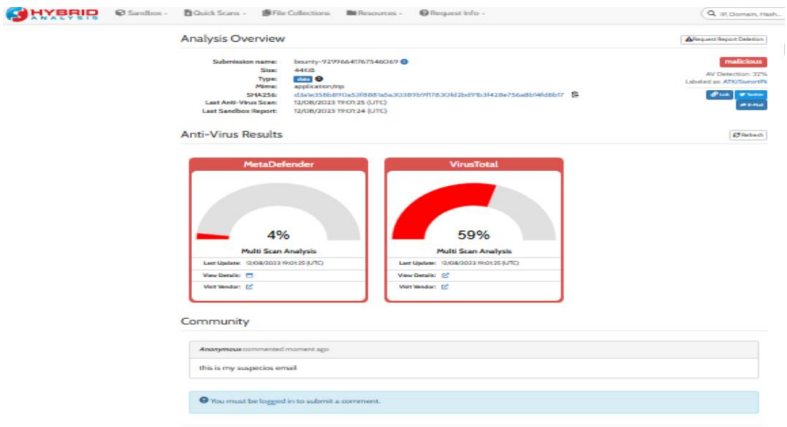
Attachments:(if any)

Filename for Download: finance-report.pdf.exe.zip



Hybrid Analysis investigation:
Submission name:bounty-92996641767546069 malicious
multi meta defender : 4%
virustotal: 59%

HASH sha : d3a1e358b890a53f8881a5a30389b9f17830fd2bd91b3f428e756a8b14fd8b17



on virustotal investigation :
45 security vendors and no sandboxes flagged this file as malicious

Popular threat label : trojan.swrort/deepscan

https://www.virustotal.com/gui/file/d3a1e358b890a53f8881a5a30389b9f17830fd2bd91b3f428e756a8b14fd8b17/detection