

Task-2: What information should we collect?

Below is a checklist of the pertinent information an analyst (you) is to collect from the email header:

- Sender email address
- Sender IP address
- Reverse lookup of the sender IP address
- Email subject line
- Recipient email address (this information might be in the CC/BCC field)
- Reply-to email address (if any)
- Date/time

Below is a checklist of the artifacts an analyst (you) needs to collect from the email body:

- Any URL links (if an URL shortener service was used, then we'll need to obtain the real URL link)
- The name of the attachment
- The hash value of the attachment (hash type MD5 or SHA256, preferably the latter)

Task-3: Email header Analysis

- Message Header: <https://toolbox.googleapps.com/apps/messageheader/analyzeheader>
- Message Header Analyzer: <https://mha.azurewebsites.net/>
- Mail Header Analysis: mailheader.org
- IPinfo.io: <https://ipinfo.io/>
- URLScan.io: <https://urlscan.io/>

urlscan.io is a free service to scan and analyse websites. When a URL is submitted to urlscan.io, an automated process will browse to the URL like a regular user and record the activity that this page navigation creates. This includes the domains and IPs contacted, the resources (JavaScript, CSS, etc) requested from those domains, as well as additional information about the page itself. urlscan.io will take a screenshot of the page, record the DOM content, JavaScript global variables, cookies created by the page, and a myriad of other observations. If the site is targeting the users one of the more than 400 brands tracked by urlscan.io, it will be highlighted as potentially malicious in the scan results".

- Talos Reputation Center: <https://talosintelligence.com/reputation>

Task-4: Email Body Analysis

- URL Extractor: <https://www.convertcsv.com/url-extractor.html>
- Talos File Reputation: https://talosintelligence.com/talos_file_reputation

The Cisco Talos Intelligence Group maintains a reputation disposition on billions of files. This reputation system is fed into the AMP, FirePower, ClamAV, and Open-Source Snort product lines. The tool below allows you to do casual lookups against the Talos File Reputation system. This system limits you to one lookup at a time, and is limited to only hash matching. This lookup does not reflect the full capabilities of the Advanced Malware Protection (AMP) system".

- VirusTotal: <https://www.virustotal.com/gui/>

"Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community."

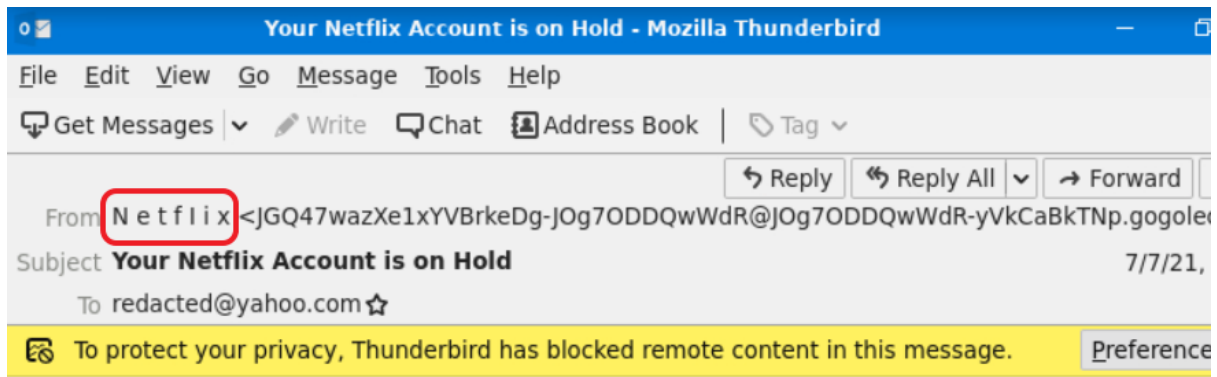
Task-5: Malware Sandbox

- Any.Run: <https://app.any.run/>
- Hybrid Analysis: <https://www.hybrid-analysis.com/>
- <https://www.joesecurity.org/>

Joe Sandbox empowers analysts with a large spectrum of product features. Among them: Live Interaction, URL Analysis & AI based Phishing Detection, Yara and Sigma rules support, MITRE ATT&CK matrix, AI based malware detection, Mail Monitor, Threat Hunting & Intelligence, Automated User Behavior, Dynamic VBA/JS/JAR instrumentation, Execution Graphs, Localized Internet Anonymization and many more".

Task-7: Phishing Case 1

a) What brand was this email tailored to impersonate?



Your account is on hold



Please Update Your Payment Details

Hi redacted@yahoo.com,

We're having some trouble with your current billing

b) What is the From email address?

From Netflix <JGQ47wazXe1xYVBrkeDg-JOg7ODDQwWdR@JOg7ODDQwWdR-yVkJCaBkTnp.gogolecloud.com>
Subject: Your Netflix Account is on Hold 7/7/21, 2:14 AM

c) What is the originating IP? Defang the IP address.

Return-Path: <postmaster@etekno.xyz>
X-Originating-Ip: [209.85.167.226]
Received-SPF: none (domain of etekno.xyz does not designate permitted sender host)

Input + [

209.85.167.226

abc 14 1

Output [

209[.]85[.]167[.]226

d) From what you can gather, what do you think will be a domain of interest? Defang the domain.

Input + [

etekno.xyz

abc 10 1

Output [

etekno[.]xyz

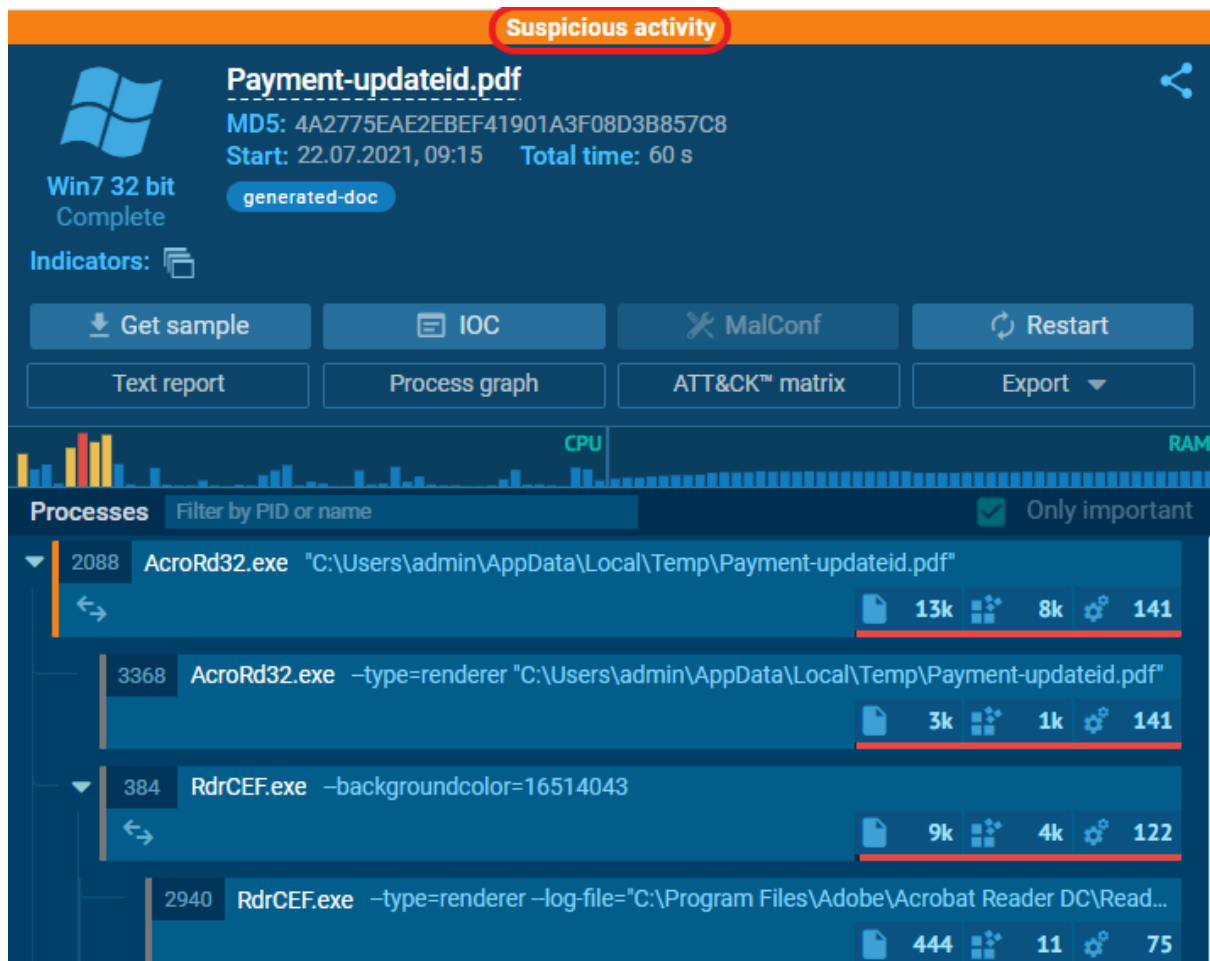
e) What is the shortened URL? Defang the URL.

`http://t.teckbe.com/p/?j3=E0owFcEwFH16EOAyFcoUFVTVEchwFH1UFOo6MjL6EbTT`

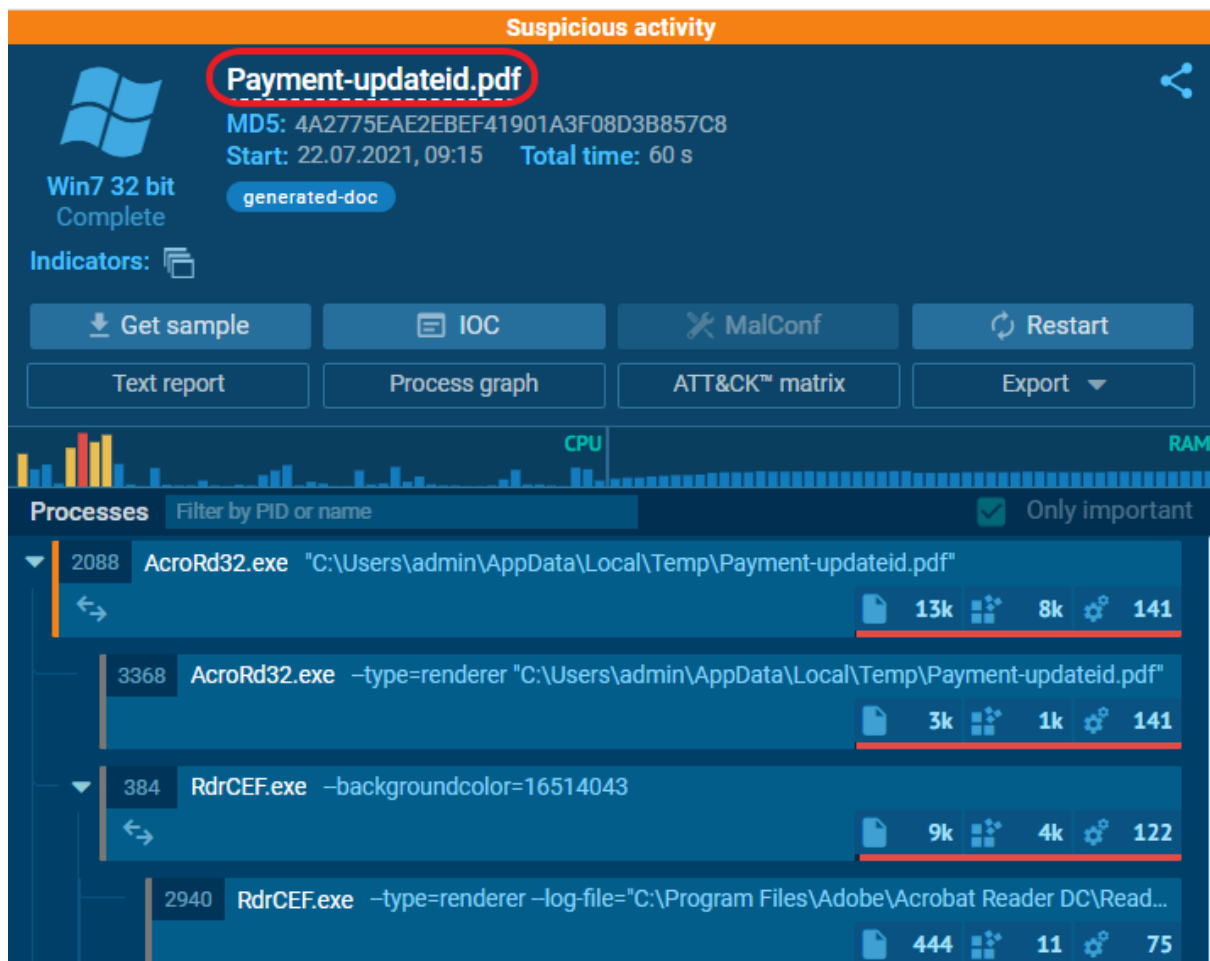


Task-8: Phishing Case 2

a) What does AnyRun classify this email as?



b) What is the name of the PDF file?



c) What is the SHA 256 hash for the PDF file?

General Info

File name:	Payment-updateid.pdf
Full analysis:	https://app.any.run/tasks/8bfd4c58-ec0d-4371-bfeb-52a334b69f59
Verdict:	Suspicious activity
Analysis date:	July 22, 2021 at 09:15:38
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	generated-doc
Indicators:	
MIME:	application/pdf
File info:	PDF document, version 1.7
MD5:	4A2775EAE2EBEF41901A3F08D3B857C8
SHA1:	8B3439F5EA2F20C6BE329C4C6B8EAA9CC439233B
SHA256:	CC6F1A04B10BCB168AEEC8D870B97BD7C20FC161E8310B5BCE1AF8ED420E2C24
SSDEEP:	3072:eiilNpcqF7c/DTmHbARHwHfScBb/jKPNsxcQ0XLN40/yU:piTpcqF7IPmHbGHwHfSEg2xcVXLNP/h

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted. **ANY.RUN** does not guarantee maliciousness or safety of the content.

d) What two IP addresses are classified as malicious? Defang the IP addresses.
(answer: IP_ADDR,IP_ADDR)

PID	Process	IP	Domain	ASN	CN	Reputation
2088	AcroRd32.exe	2.16.107.24.443	acroipm2.adobe.com	Akamai International B.V.	-	malicious
1776	svchost.exe	2.16.107.83.443	ardownload3.adobe.com	Akamai International B.V.	-	malicious


e) What Windows process was flagged as Potentially Bad Traffic?

1776	svchost.exe	Potentially Bad Traffic	ET INFO TLS Handshake Failure
------	-------------	-------------------------	-------------------------------

Task-9: Phishing Case 3

a) What is this analysis classified as?





Malicious activity

**CBJ200620039539.xlsx**

MD5: F7F4EC2A0ADC9CC33CDBC7D548A6BEF9
Start: 22.07.2021, 10:35 Total time: 60 s

trojan exploit CVE-2017-11882

Win7 32 bit
Complete

Indicators:    

Get sample

IOC

MalConf

Restart

Text report

Process graph

ATT&CK™ matrix

Export ▼

CPU

RAM

Processes

Filter by PID or name

☒ Only important

1016 EXCEL.EXE /dde

1068 COM EQNEDT32.EXE -Embedding

1328 ntvdn.exe -i1

1k 1k 79

645 403 69

305 12 25

b) What is the name of the Excel file?

General Info

✓ Add for printing

File name: CBJ200620039539.xlsx
Full analysis: <https://app.any.run/tasks/82d8adc9-38a0-4f0e-a160-48a5e09a6e83>
Verdict: Malicious activity
Analysis date: July 22, 2021 at 10:35:05
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags: trojan exploit CVE-2017-11882
Indicators: * ☠ 📄 📋
MIME: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
File info: Microsoft Excel 2007+
MD5: F7F4EC2A0ADC9CC33CDBC7D548A6BEF9
SHA1: D460315F92AA3DCA63617431883834ED94C09F45
SHA256: 5F94A66E0CE78D17AFC2DD27FC17B44B3FFC13AC5F42D3AD6A5DCFB36715F3EB
SSDEEP: 384:jhzRpm16A+fEAgjnP5O5ykBmx4ml/NhQqhKZLOU2pukVnF5:NzsAMpE5TsWGHhKZ+

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Activat
Go to S...

c) What is the SHA 256 hash for the file?

MD5: F7F4EC2A0ADC9CC33CDBC7D548A6BEF9
SHA1: D460315F92AA3DCA63617431883834ED94C09F45
SHA256: 5F94A66E0CE78D17AFC2DD27FC17B44B3FFC13AC5F42D3AD6A5DCFB36715F3EB
SSDEEP: 384:jhzRpm16A+fEAgjnP5O5ykBmx4ml/NhQqhKZLOU2pukVnF5:NzsAMpE5TsWGHhKZ+

d) What domains are listed as malicious? Defang the URLs & submit answers in alphabetical order.

DNS requests

Domain	IP	Reputation
biz9holdings.com	204.11.56.48	malicious
findresults.site	103.224.182.251	malicious
ww38.findresults.site	75.2.11.242	malicious

e) What IP addresses are listed as malicious? Defang the IP addresses & submit answers from lowest to highest.

DNS requests

Domain	IP	Reputation
biz9holdings.com	204.11.56.48	malicious
findresults.site	103.224.182.251	malicious
ww38.findresults.site	75.2.11.242	malicious

f) What vulnerability does this malicious attachment attempt to exploit?

Tags: trojan exploit CVE-2017-11882
Indicators: * ☠ 📄 📋