Phishing Emails 3

* Introduction
* What information should we collect?
  + Pertinent information to check
    - 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
  + No answer needed
* Email header analysis
  + A few tools
    - Google admin toolbox, Message Header Analyzer (Azure), mailheader.org
  + What is the official site name of the bank that capitai-one.com tried to resemble?
    - Capitalone.com
* Email body analysis
  + How do you manually get the location of a hyperlink?
    - Copy Link Location
* Malware Sandbox
  + No answer needed
* PhishTool
  + <https://www.phishtool.com/>
  + Look at the Strings output. What is the name of the exe file?
    - #454326\_PDF.exe
* Phishing Case 1
  + What brand was this email tailored to impersonate?
    - Netflix
  + What is the From email address?
    - JGQ47wazXe1xYVBrkeDg-JOg7ODDQwWdR@JOg7ODDQwWdR-yVkCaBkTNp.gogolecloud.com
  + What is the originating IP? Defang the IP address.
    - [209[.]85[.]167[.]226]
  + From what you can gather, what do you think will be a domain of interest? Defang the domain
    - Etekno[.]xyz
  + What is the shortened URL? Defang the URL.
    - hxxps[://]t[.]co/yuxfZm8KPg?amp=1
* Phishing Case 2
  + Link: <https://app.any.run/tasks/8bfd4c58-ec0d-4371-bfeb-52a334b69f59>
  + What does AnyRun classify this email as?
    - suspicious activity
  + What is the name of the PDF file?
    - Payment-updateid.pdf
  + What is the SHA 256 hash for the PDF file?
    - cc6f1a04b10bcb168aeec8d870b97bd7c20fc161e8310b5bce1af8ed420e2c24
  + What two IP addresses are classified as malicious? Defang the IP addresses
    - 2[.]16[.]107[.]83, 2[.]16[.]107[.]24
  + What windows process was flagged as Potentially Bad Traffic?
    - Svchost.exe
* Phishing Case 3
  + What is this analysis classified as?
    - Malicious activity
  + What is the name of the Excel file?
    - CBJ200620039539.xlsx
  + What is the SHA 256 hash for the file?

# **5F94A66E0CE78D17AFC2DD27FC17B44B3FFC13AC5F42D3AD6A5DCFB36715F3EB**

* + What domains are listed as malicious? Defang the URLs & submit answers in alphabetical order
    - biz9holdings[.]com
    - findresults[.]site
    - ww38[.]findresults[.]site
  + What IP addresses are listed as malicious? Defang the IP addresses & submit answers from lowest to highest
  + What vulnerability does this malicious attachment attempt to exploit?
    - CVE-2017-11882
* Conclusion
  + Tools
    - <https://mxtoolbox.com/>
    - <https://phishtank.com/?>
    - <https://www.spamhaus.org/>