ANALYZING A MALICIOUS MALICIOUS EMAIL

This cheat sheet explains what to look for in your determination of whether or not an email is malicious. Analysis should always be completed on a virtual machine in an isolated environment.

General Approach to Email Analysis

1. Identify sender's email address.
   - *From* field in header. Caution, may be spoofed.
2. Identify reply-to email address.
   - *Reply-To* field in header. Reply-to should typically match From field.
3. Hops should correlate to the domain of the sender's email address.
4. Identify IP address of sender
   - X-Originating-IP: Sender's IP.
   - Client-IP: IP of server/client/machine where email originated.
   - Received: Contains IP of servers that received/sent message.
5. Analyze all suspicious URLs.
   - Search https://virustotal[.]com for reference to URLs.
6. Analyze all attachments.
   - Search https://virustotal[.]com for hash:
     - Windows: certutil –hashfile [filename] MD5
     - Linux: md5sum [filename]
   - Manual analysis: PeePDF, oledump, ClamAV, pdfextract
7. If email is found to be malicious, proceed with remediation/documentation/reporting steps.

Email Headers

IMPORTANT! Headers can be easily spoofed. Trust only items in Received lines.

`From`	Indicates who an email came from
`Subject`	The subject of the message is contained here.
`Date`	Displays the date and time the email was written.
`To`	Indicates to whom the email was addressed.
`Return-Path`	Indicates the email address to which a reply or bounced message should be delivered.
`Reply-To`	Indicates the email address to which a reply or bounced message should be delivered.
`Envelope-To`	The email address to whom the email was sent.
`Delivery Date`	The date and time the email was received by an email service/client.
`Received`	Together, the received lines form a list of all servers an email traversed to reach its destination. Read from bottom to top.
`Message-id`	Unique string of characters assigned to an email by the mail system. Easily spoofed.
`X-Spam-Status`	Spam score set by service/client.
`X-Spam-Level`	Spam score set by service/client.
`X-Originating-IP`	IP address of sender.

Helpful Sites

Do not upload sensitive information to any third party tool/website!

- https://virustotal[.]com
- https://urlscan[.]io
- https://phishtank[.]com
- https://hybrid-analysis[.]com
- https://pulsedive[.]com/
- https://authentic8[.]com
- https://url2png[.]com
- https://ipvoid[.]com
- https://any[.]run
- https://toolbox[.]google[.]com/apps/messageheader/analyzer
- https://mailheaderanalyzer[.]herokuapp[.]com

Malicious Attachment Analysis

Use the following tools to identify potentially malicious behavior in common email attachments. Analysis is assumed to be completed using REMnux.

1. Upload hash of pdf to VirusTotal
   - # peepdf.py –c [file.pdf]
2. Identify potentially malicious format tags: /JS, /Java, /AA, /OpenAction, /URI
   - # pdfid.py [file.pdf]
3. Locate JavaScript within PDF.
   - # pdf-parser –search=JavaScript [file.pdf]
4. Identify macros embedded within Office Doc.
   - # oledump - i [filename]
5. Perform ClamAV scan of attachment.
   - # freshclam
   - # clamscan [file.pdf]

Brad D
August 2019

Collecting Email Headers

Certain steps must be followed in order to obtain the headers for a particular email. These steps will depend on the email client or web application being used.

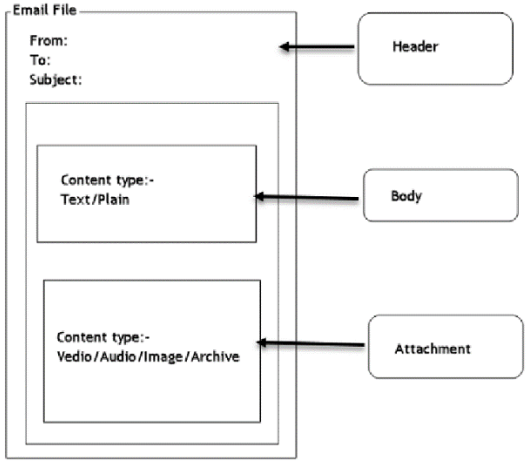
Outlook Client
1. File
2. Properties
3. Internet headers
Outlook Web App/Office 365
1. Click … at top right of message
2. View Message Details
Gmail
1. Click ⋮ at top right of message
2. Show original
Yahoo
1. Click More options
2. View Raw Message
Perform ClamAV scan of attachment.
freshclam
clamscan [file.pdf]

Reporting Malicious Sites

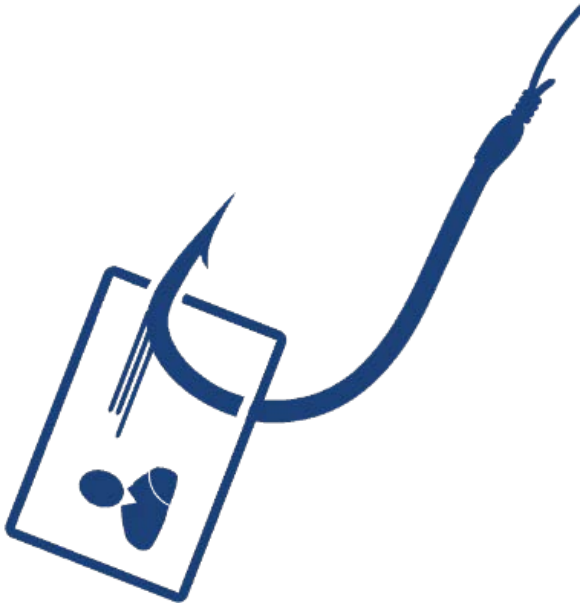
To protect others, malicious URLs may be reported to the following organizations.

Google	https://goo[.]gl/#reportspam
	https://www[.]google[.]com/safebrowsing/report_phish/
Microsoft	https://www[.]microsoft[.]com/en-us/wdsi/support/report-unsafe-site
	phish@office365.microsoft.com
Bit.ly	abuse@bitly.com
Dropbox	abuse@dropbox.com
US-CERT	Phishing-report@us-cert.gov

Email Structure



Analyzing a Malicious Email



Brad D
August 2019