

Automated Email Analysis with PhishTool

Manual email analysis, while thorough, can be time-consuming in high-volume environments. Automated analysis tools like PhishTool streamline the investigation process by performing many manual checks simultaneously, extracting key indicators, and providing consolidated reports. These tools integrate multiple analysis techniques covered in previous sections - header analysis, authentication checking, URL extraction, and attachment scanning - into a single platform with automated threat intelligence lookups.

PhishTool

While there is an enterprise edition of Phishtool, there also is a free tool. Note that this will need an account, so you would need to sign up with an email address, even for the free version.

When you upload an eml file to PhishTool, it displays the email for you with options for Rendered, HTML and Source. On the left, it provides Header information, with a number of alerts if anything suspicious is found. In the below screenshot it gives alerts for the Reply-To and Return-Path being different to the From: header. There also is an Alert about the DMARC check failing under the Authentication tab.

The screenshot displays the PhishTool web interface. At the top, there's a navigation bar with links for Dashboard, Uploads, In-tray, Notifications, My Account, and an Upgrade button. Below the navigation bar, a message states: "Your Bank Account has been blocked due to unusual activities". The main content area is divided into two sections. On the left, under the "Details" tab, there's a table of email headers:

Header	Value
From	alerts@chase.com
Display name	None
Sender	None
To	bob.sanders@corhalitech.com
Cc	None
In-Reply-To	None
Timestamp	2024-05-01T20:04:05Z
Reply-To	kellyellin426@proton.me
Message-ID	<i7g9MMh5NtErtaOzQZEp3D-i-u3FWwdo0wY5mhD8Q1v1vw1yeLj-jMWPAn-HP3FugK sucesWSub00Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>
Return-Path	kellyellin426@proton.me
Originating IP	185.70.40.140 (Received-SPF)
rDNS	185-70-40-140.protonmail.ch

On the right, under the "Rendered" tab, there's a preview of the email body. It features the Chase logo and a message from Chase Online Service stating: "Dear Customer, Due to unusual activities on your account, we placed a temporary suspension until you verify your account. What You Need To Do In Order To Restore Your Account. To verify your account, Click on 'Reactivate Your Account' below and complete the steps to verify recent account activity." Below the message is a button labeled "Reactivate Your Account".

Additionally, it extracts URLs, Attachments, Transmissions and X-headers. The Transmissions tab shows the Received-chain.

It is even possible to get automatic VirusTotal results for the URLs and attachments if you configure your PhishTool account with a VirusTotal API key.

Your Bank Account has been blocked due to unusual acti...

Details

Authentication

URLs

Attachments

Transmission

X-headers

Filters (0)

URL

https://dsgo.to/CQECQECnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQCnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQCQECnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQ

Domain

dsgo.to

VirusTotal

0 / 97

Once you have made a conclusion, you can click on Resolve in the upper right, and fill in whether the email was safe or malicious under Disposition, as well as add Flagged artifacts and Classification codes.

Resolve

Resolution

Disposition ▼

Malicious

Flagged artifacts ▼

⊗ Reply-To email address

kellyellin426@proton.me

⊗ Return-Path email address

kellyellin426@proton.me

⊗ Message URL

https://dsgo.to/CQECQECnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQCQECnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQ

Classification codes ▼

⊗ CRED_HARV

Credential harvesting

⊗ SPOOF

Spooing

Notes

Enter notes here...

Resolve

We can take a look at another eml file, this time one with an attachment. This is the same email examined in the Attachment Analysis section.

Uploads > FW: Due Invoice Payment - protonmail.com - Wire Transfer Document ✓ Resolve ...

FW: Due Invoice Payment - protonmail.com - Wire Transf...

Details Authentication URLs Attachments Transmission X-headers Rendered HTML Source

From	Paol.Reggiani@moss.it	...
Display name	Paolo Reggiani	
Sender	None	
To	wp@protonmail.com	
Cc	None	
In-Reply-To	None	
Timestamp	2020-01-14T08:06:05Z	
Reply-To	None	
Message-ID	<20200114000605.14F3983143C82AAA@moss.it>	
Return-Path	Paol.Reggiani@moss.it	...
Originating IP	213.227.154.65 (Hop 1) ▼	...
rDNS	None	

Good Morning,

Please find the attached transfer slip from our bank and confirm receipt of the payment to your account.

Following the trail mail below, our client requested from us to remit payment to your account for business you did with them.

Based on my telephonic conversation with your colleague, kindly reconfirm that your bank details on the wire slip is correct.

I await your kind reply and feedback.

Received with thanks.

Regards,

Dejahnea

The alerts show that there is an issue with Authentication (both SPF and DMARC failed) and an alert for an Attachment:

Details Authentication URLs Attachments Transmission X-headers

! (1) quotation.iso ...

File name	quotation.iso
File size	112.00 KB
File type	None
MD5	6aef1d7f88e8aa450a0c604b4caee5ba
SHA-1	3fe45f8cd20cd7c63e55e3918dac1d3a0d7fb05a
SHA-256	75fdb848eac332b4ca7d88f497e7ba7ebbb9a798d825b28cf1f87b9d7149e87f
VirusTotal	39 / 62

Just like was determined in the Attachment Analysis section, quotation.iso was deemed malicious by PhishTool.

While not all organizations use this particular tool, it is clear that PhishTool, and other tools like this save a lot of time.

Summary

PhishTool demonstrates how automated email analysis platforms can significantly reduce investigation time while maintaining analysis quality. The tool performs comprehensive checks including header analysis, authentication verification, URL and attachment extraction, and automatic VirusTotal integration through API keys. It provides structured reporting with

disposition tracking and artifact flagging, making it suitable for organizational incident response workflows. While automation tools are valuable for efficiency and consistency, they complement rather than replace manual analysis skills, as complex threats may require deeper investigation beyond automated capabilities.