Study Methodology

100 malicious document samples were collated, studied and broadly categorized into 4 main groups:

1. Original Malicious Documents from Malware Bazaar
2. Slightly Altered Malicious Documents from Malware Bazaar, such as changes in metadata and file formats
3. Malicious Documents modified using attack tools that have existed for many years
4. Basic Macro-enabled Documents that execute programs on user devices

These document samples were sent through a third party email provider (ProtonMail) to each of the email provider (Gmail, Outlook, Yahoo, AOL, and Apple iCloud Mail). The main outcome was whether the email was delivered successfully to the user, which implied that they were susceptible to the attacks embedded in the documents.

Summary of Results

This table summarizes the outcome of sending 7 of the 100 malicious samples to the various email providers. If an email was undelivered, it is a sign that malware was detected when the email was being processed by the server.

Document Category	Document Type	Email Provider				
		Gmail	Outlook	iCloud	Yahoo	AOL
A	Malicious .pptx file detected by 40 Virus Scanners	✗ Mail Undelivered	✗ Mail Undelivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered
A	Malicious .xls file detected by 35 Virus Scanners	✗ Mail Undelivered	✗ Mail Undelivered	✗ Mail Undelivered	✓ Mail Delivered	✓ Mail Delivered
B	Modified Malicious .xlsx with Metadata Changed	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered
C	Modified Malicious .doc that has been Purged	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered
C	Simple .docx with Macros Executing "Calc.exe"	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered
D	Simple .xlsx with Macros Executing WannaCry User Interface "ui.exe"	✗ Mail Delivered with Warning Included	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered
B	Simple .xlsx with Macros Executing WannaCry User Interface "ui.exe" Renamed as PDF	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered	✓ Mail Delivered

If the email was delivered, the user was able to interact with the attachment and download it to their system. Leaving them vulnerable to attack. Hence, the times email providers protected the users were the times when the mail was undelivered.

Details of Sample Files Used in Study

This document provides an overview of the files used in the study focused on testing how various email providers handle malicious file samples. For more details, please refer this blog.

Unmodified Malware Samples

1. Malicious .pptx document

- *Hash*: 061e17f3b2fd4a4dce1bf4f8a31198273f1abc47c32456d06fd5997ea4363578
- *Source*: Malware Bazaar
- *Analysis*: This file employs obfuscation and executes commands to manipulate and execute files on the system without user consent. It attempts to disguise its actions with a misleading error message, indicating an attempt to compromise the system.
- In this blog you can find:
    - Demonstration Video using this document *"1. Malicious (Unmodified) pptx Demo.mp4"*

2. Malicious .xls document

- *Hash*: a1d323166349f499aa796148c0120f89d3a0946abdf74f0dc045c5641b2ab2d3
- *Source*: Malware Bazaar
- Analysis: Recognized by 35 security vendors and sandboxes as containing a trojan downloader, this Excel file is clearly identified as malicious and poses a significant threat.
- In this blog you can find:
    - Demonstration Video using this document *"2. Malicious (Unmodified) xls Demo.mp4"*

Mildly Modified Samples

3. Malicious .doc document

- *Hash*: 77b45d70062e2d27973484bfa11f3dc838a579d53d0989ba630bf109316d4684
- *Source*: Malware Bazaar
- *Description*: Contains macros that perform suspicious functions, such as file manipulation and displaying splash screens. The malicious document has been purged (modified) with OfficePurge to potentially evade antivirus detection. When user opens the document on their computer, the harmful macros still executes as designed. This demonstrates an attempt to disguise the harmful nature of the file.
- In this blog you can find:
    - Demonstration Video using this document *"3. Malicious (Modified) doc Demo.mp4"*

4. Malicious .xlsx document

- *Hash*: af843dee2be7f8aac802500b3ea1c848e36cd936073250be0dfad58e842e75ee
- *Source*: Malware Bazaar
- *Description*: The malicious excel document contains trojan. In the modified version, the excel contents are exactly the same, but the metadata – name of creater, name of author, time of created and time of last modification has been modified. This changes the hash of the file, making it hard to detect by scanners.
- In this blog you can find:
    - Demonstration Video using this document *"4. Malicious (Modified) xlsx Demo.mp4"*

Created Malicious Samples

5. Simple .docx with Macros executing "Calc.exe"

- This word document has a macros code that uses the shell command to call "calc.exe" – in windows, this refers to the Calculator app.

6. Simple .xlsx with Macros executing WannaCry User Interface "ui.exe"

- This Excel document has a macros code that uses the shell command to call a "ui.exe" hosted on another site that pulls the user interface of the famous WannaCry Ransomware.

7. Simple .xlsx with Macros executing WannaCry User Interface "ui.exe" Renamed to PDF

- The same file as (6) but with file type renamed to PDF