

SecureDoc_Scanner Image Analysis Report

Detailed analysis of the provided image

[*] Starting RTF Analysis...

[*] Performing detection of the malicious code patterns...

| Pattern | Description | Count |
|----------|--|-------|
| \objdata | This pattern identifies embedded binary data objects in RTF documents. | 3 |

[*] Keywords for this sample: ['embedding']

[*] Performing embedded exploit/script detection...

[*] Looking for embedded binary sections...

[*] Looks like we found possible exploit between brackets. Attempting to identify and extract

[*] Data saved as: securedoc_extracted_exploit-0.bin

[*] Checking URL values...

| URL Values |
|---|
| http://account-complaint-support-10048677845.netlify.app/ |
| https://products.office.com/en-us/word |
| http://phishing.site |
| http://payload.site |
| http://driveby.site |
| http://malicious.site');</script>\\htmltag\ |
| http://malicious.site |

[*] Performing YARA rule matching...

There is no rules matched for /home/kali/Testing Files/file2.rtf

[*] RTF Analysis Completed.