Malicious Document Analysis BY P3NGU1N

Static Malicious Document Analysis

🎯 What is the MD5 value of the "/root/Desktop/QuestionFiles/PO-465514-180820.doc" file?

ANSWER: d7e6921bfd008f707ba52dee374ff3db

🎯 What is the file type of the "/root/Desktop/QuestionFiles/PO-465514-180820.doc" file?

ANSWER: doc

More Details About Document File Analysis 2

🎯 **Note:**

Before starting, install the oletools: "sudo -H pip install -U oletools"

Does the file "/root/Desktop/QuestionFiles/PO-465514-180820.doc" contain a VBA macro?

Answer Format: Y/N

ANSWER: Y

🎯 Some malicious activity occurs when the document file "/root/Desktop/QuestionFiles/PO-465514-180820.doc" is opened. What is the macro keyword that enables this?

ANSWER: document_open

🎯 Who is the author of the file "/root/Desktop/QuestionFiles/PO-465514-180820.doc"?

ANSWER: alexandre riviere

🎯 What is the last saved time of the "/root/Desktop/QuestionFiles/PO-465514-180820.doc" file?

ANSWER: 2020-08-18 08:19:00

🎯 The malicious file "/root/Desktop/QuestionFiles/Siparis_17.xls" is trying to download files from an address. From which domain is it trying to download the file?

ANSWER: hocoso.mobi

🎯 How many IOCs are in the "/root/Desktop/QuestionFiles/Siparis_17.xls" file according to the Olevba tool?

ANSWER: 2

Analysis with Sandboxes

🎯 The file "/root/Desktop/QuestionFiles/PO-465514-180820.doc" is trying to make a request to a domain ending with ".kz". What is this domain?

ANSWER: www.msbc.kz

🎯 With which Windows tool are the connection requests made? (File: /root/Desktop/QuestionFiles/PO-465514-180820.doc)

ANSWER: powershell.exe

🎯 How many addresses does the file send DNS requests to? (File: /root/Desktop/QuestionFiles/PO-465514-180820.doc)

ANSWER: 5

🎯 The "/root/Desktop/QuestionFiles/Siparis_17.xls" malware document is trying to download a file. With what name does he want to save the file it is trying to download to the device?

ANSWER: 6LeGwKmrm.jar