PDF Document Analysis (AgentTesla)

Question: Locate the sample in the directory "C:\Tools\Maldoc\PDF\Demo\Samples\WikiLoader". Perform analysis of the objects within the sample. What is the value of /URI in object 7? Answer format is a URL.

Answer: https://infplaute.com/international-commercial

So, you RDP to the target, and then use the peepdf.exe with the path. After you write object 7 and get the answer.

PDF XObject Analysis (Quakbot)

Question: Investigate the PDF sample located at "C:\Tools\MalDoc\PDF\Demo\Samples\RedLineStealer\Price_Quote.pdf". Figure out the URI embedded in the document. Type the name of the file hosted at that remote URL. Answer format is "_.bat"

Answer: Price_Quote.bat

Analysis of Malicious Office Files

Question: Run olevba.py with -a option on the file "C:\Tools\MalDoc\Office\Demo\Samples\QuasarRAT\QuasarRAT.docx". This will show a list of suspicious keywords. Figure out the keyword that downloads files from the Internet. Type the keyword as your answer. Answer Format is m********.*******

Answer: microsoft.xmlhttp

You RDP to the target and run this command: python C:\Tools\MalDoc\Office\Tools\oletools\ olevba.py -a C:\Tools\MalDoc\Office\Demo\Samples\QuasarRAT\QuasarRAT.docx

You analyze the result and see that the file mentioned above is the one that download things.

Office Document - VBA Macro Analysis

Question: Use olemeta.py to analyse the document properties. Find out who is the author of this document, and type the name of author as your answer.

Answer: Mohammed Alkuwari

Connect to RDP into the target run this command python C:\tools\maldoc\office\tools\oletools\oleid.py

C:\Tools\MalDoc\Office\Demo\Samples\Havoc\3dfddb91261f5565596e3f014f9c495a.doc there it shows the author.

Obfuscated VBA Macro Analysis

Question: When you extract VBA Macro code of this sample using olevba.py, there is a call to MsgBox. What is the content of this MsgBox function? Type it as your answer.

Answer: Open this Transaction Recipt Again!

Connect to the target through RDP, run this command: python C:\Tools\MalDoc\Office\Tools\oletools\olevba.py C:\Tools\MalDoc\Office\Demo\Samples\QuasarRAT\QuasarRAT.docx

You go down and get the answer.

Analysis of External Relationships

Question: Locate the sample "C:\Tools\MalDoc\Office\Demo\Samples\SnakeKeylogger\PO026037.docx" and investigate relationships with external links. Type the external link as your answer. Answer format is an HTTP URL.

Answer: http://gurl.pro/u8-drp

Connect to the target with RDP and run the oleobj to get the link with the specific docx. This command: python C:\Tools\MalDoc\Office\Tools\oletools\oleobj.py C:\Tools\MalDoc\Office\Demo\Samples\SnakeKeylogger\PO026037.docx