How To Extract & Decrypt Qbot Configs Across Variants

Published: 2021-12-11 · Archived: 2026-04-05 15:43:03 UTC

Follow me on Twitter for RE tips and resources: _/ agdcservices_ View our malware analysis products to aid in your RE efforts (Ghidra / python scripts, tools, and individual analysis results) https://github.com/agdcservices Qbot is a common banking malware that calls out to dozens of domains which need to be blocked. These networking IOCs are stored in an encrypted configuration resource file within the malware. This video will show you how to extract and decrypt the networking configuration so you can quickly identify all the IOCs with minimal effort and 100% accuracy. You will use several techniques shown in previous videos in order to accomplish that goal. Download the malware samples at https://malshare.com to review in your own analysis lab: Sample 1: bfcc44f774aa4363939aedbf6d19bffe8861a9922fbdf2dc15e8a34580638f9c Sample 2: da05722fd87989e188845773fce82c382b40d18e48130afa1f985cac6f63ca0f #ReverseEngineering #MalwareAnalysis #SRE #RE #Ghidra #QBot #Quakbot #Malware #Crypto #RC4

Source: https://www.youtube.com/watch?v=M22c1JgpG-U