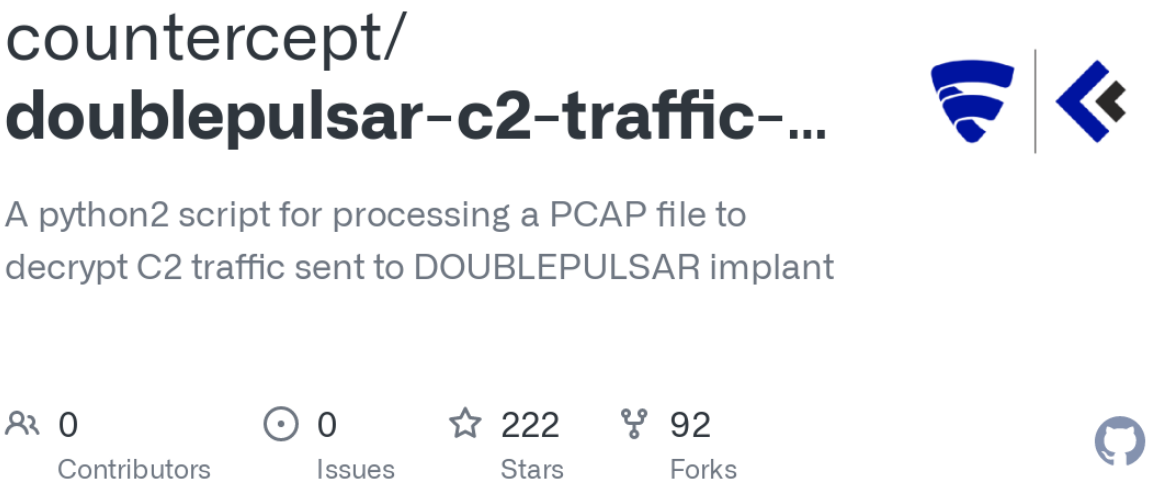
countercept/doublepulsar-c2-traffic-decryptor: A python2 script for processing a PCAP file to decrypt C2 traffic sent to DOUBLEPULSAR implant

github.com/countercept/doublepulsar-c2-traffic-decryptor

countercept



Author: Luke Jennings (luke.jennings@countercept.com - @jukelennings)

Company: Countercept (@countercept)

Website: https://countercept.com

A python2 script for decrypting the C2 traffic used by the DOUBLEPULSAR SMB implant from a PCAP file. The encryption used is a simple 4-byte XOR, which you can often see being displayed in the command output from the FUZZBUNCH toolset. This makes use of the fact that a set of four contiguous zeros are present in the SESSION_SETUP parameters in the first non-ping packet, which reveals the XOR key directly and this is used to decrypt all of the traffic.

This is an early release and relies on finding certain specific components in the network packets and has been tested with the DLL injection functionality. For best results, supply a PCAP file that has only one command within the traffic.

For testing purposes, a PCAP file is contained within this repository that was captured using the DLL injection command to inject the standard windows DLL wininet.dll into a running calc.exe process on the target machine. The decrypted output from running this script is also

present in the repository and contains 4885 bytes of shellcode followed by a byte-for-byte copy of wininet.dll

This script has a dependency on the python-pcapng library. Example usage below:

root@kali:~# pip install python-pcapng

root@kali:~# python decrypt_doublepulsar_traffic.py --pcapng inject-dll-wininet-into-calc.pcapng --output decrypted_data.bin