ARL South Cyber Rapid Innovation Group Presents:

Cybersecurity Awareness Workshop Series
WannaCry – UBER Exercise

Developed by Adriana Escobar Del La Torre & Ana Garcia Ramirez
Advised by Dr. Jaime Acosta and Dr. Salamah Salamah

Activity – Find the service that WannaCry uses to spread and observe the behavior of the malware when the process is stopped.

1. In IDA Pro, after the conditional jump, look in the part of the code that continues the encryption (i.e., follow the ***call***)
2. Find the name of a service being executed by the malware.
    a. What is the name of the service that the malware is using to spread?

    _____
3. Close the current remote desktop session and re-open the *WannaCryA* file on your desktop.
4. Click on the Windows button and search for services.
5. Open Windows Services and search for the service found in step 3.
6. Stop the service.
7. Use Wireshark to observe the network traffic.
8. Describe what the service is doing.

This concludes the uber challenge.