

Pi Hediye Var

Cybersecurity Game #18

written by Mert SARICA | 21 February 2020

I am back again with my first Pi Hediye Var Cybersecurity Game of 2020. As in previous games, I will be giving away 2 Raspberry Pi 4s through a raffle among university students who successfully complete this game. I would like to thank Keepnet Labs Turkey Country Director Erdi BALCI, both on my own behalf and on behalf of all game enthusiasts, for being the Pi sponsor of this game.

As for my game, a company executive who has allowed the installation of applications from unknown sources in the settings of a corporate Android phone clicks on the link address in an SMS he receives and downloads the APK file, then runs it. A week later, an alarm comes in from the company's network security system regarding malware traffic and our hero, who is a Corporate SOC employee, gets involved in the situation. The executive, who is aware of the situation, asks for help from our hero to learn which information has been stolen. Our hero, who examines the HTTP traffic that is the subject of the alarm, starts working to decrypt the encrypted data in order to be able to detect the stolen data using the APK file and our story starts here.

To successfully complete the game, you must provide detailed explanations of all answers to the following questions, along with evidence (code snippets, screenshots, etc.). To answer the questions, you must first download the suspicious file that needs to be reviewed from the address

<https://www.dropbox.com/s/t6kakt8jsrsrsqy/ctf18.zip?dl=0>. (zip password: infected)

Instructions & Questions:

1. Analyze the APK file and find the address of the command control center.
2. Find the private key used in encrypting the data in the ws parameter.
3. Decrypt the encrypted data in the ws parameter.

POST / HTTP/1.1

Content-Length: 1118

Content-Type: application/x-www-form-urlencoded

User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Google Nexus 6



YOUR **MIND** IS A WEAPON
KEEP IT LOADED

- JOHN WICK -