Pi Hediyem Var Cybersecurity Game #17

written by Mert SARICA | 26 July 2019

After a long hiatus, I'm back with the first Pi Hediyem Var (I Have Pi Gift) game of 2019. Just like in previous games, I will be giving away 3 Raspberry Pi 4 devices through a draw among university students who successfully complete this game. I would like to express my gratitude to Erdinç BALCI, the Country Manager of Keepnet Labs Turkey, who is the Pi sponsor for this game, both on my behalf and on behalf of all gamers.

Regarding the game, one of your organization's employees realizes that after entering their credit card information on a deal website they visited to get a service, they were redirected to a different website. Suspicion arises that their credit card information may have been stolen, and the employee seeks your assistance to shed light on this matter. Our hero, who has been reading news about cyberattacks on websites using the Magento e-commerce platform lately and is part of the Corporate SOCIAL MEDIA (SOME) team, visits this website from their virtual system to begin analyzing web traffic for suspicious code detection, and our story begins here.

To successfully complete the game, you need to answer all of the following questions in detail, along with evidence (code snippets, screenshots, etc.). To answer the questions, you must first download the suspicious file that needs to be examined from the following link: https://www.dropbox.com/s/yyfretoo11hopq8/ctf17.zip?dl=0. You can analyze the file using the Fiddler tool. (zip password: infected)

Instructions & Questions:

1. Find the files containing malicious code.
2. Decode at least a 50-character hidden string (strings) from the code. (Using ready-made deobfuscator programs is prohibited.)
3. Based on the previous step, identify which web address the malicious code sent the stolen information to.
4. Based on your analysis, state at least 5 pieces of information that the malicious code could steal from the customer.
5. Based on the information obtained from code analysis, make an educated guess about which hacking group may have developed the malicious code.

For those who haven’t won a Raspberry Pi before and wish to participate in the draw or want to be included in the list of those who have successfully completed the game, they must send the detailed solution path, their name, surname, age, and contact information to me or my email address with evidence (code, screenshots, etc.) by Saturday, July 27th at 20:00.

A blog post containing the solution path of the game will be published in the coming days, and the lucky winner will be announced on this page and my Twitter account.

Note: While solving this game, please remember that you are dealing with malicious software and conducting code analysis. I strongly recommend working with an isolated and up-to-date virtual system software (such as VMware, VirtualBox, etc.).

Good Luck


NO PAIN
THE ITALIAN STALLION
ROCKY IV