Pi Hediyem Var Cybersecurity Game #19

written by Mert SARICA | 12 March 2021

I am back with my first Pi Hediyem Var Cybersecurity Game of 2021, after a year break. As with previous games, I will be giving away 1 Raspberry Pi 4 and 2 Raspberry Pi 3s through a lottery among university students who successfully complete this game. I would like to thank Erdinç BALCI, the Country Manager of Keepnet Labs Turkey, who is the Pi 4 sponsor of this game, both on my behalf and on behalf of all game enthusiasts.

As for my game, our hero, who has been working on cyber security incident response for a long time, closely follows cyber attacks carried out by advanced persistent threat (APT) groups and acquires knowledge about new tactics, techniques, and procedures used by these groups by analyzing technical reports.

One day, a PowerShell/Agent.QX security alarm is triggered on the proxy server of the institution where our hero works, for the EPUWBt3.png file that passed through the web traffic created by an employee. Not long after, a PowerShell/Injector.D alarm is triggered on the antivirus software installed on the same user's operating system for the 8ROnVhd.png file.

The hero, who remembers what he heard in the 6th episode of APTv, thinking that the alarms may be from a targeted cyber attack, starts working to solve what's happening. To successfully complete the game, you must provide detailed explanations, including evidence (code snippets, screenshots, etc.) for all the questions below. To answer the questions, you will first need to download and examine the suspicious file from the address https://www.dropbox.com/s/syn4l1c6r35vsl4/ctf19.zip?dl=0. (zip password: infected)

Instructions & Questions:

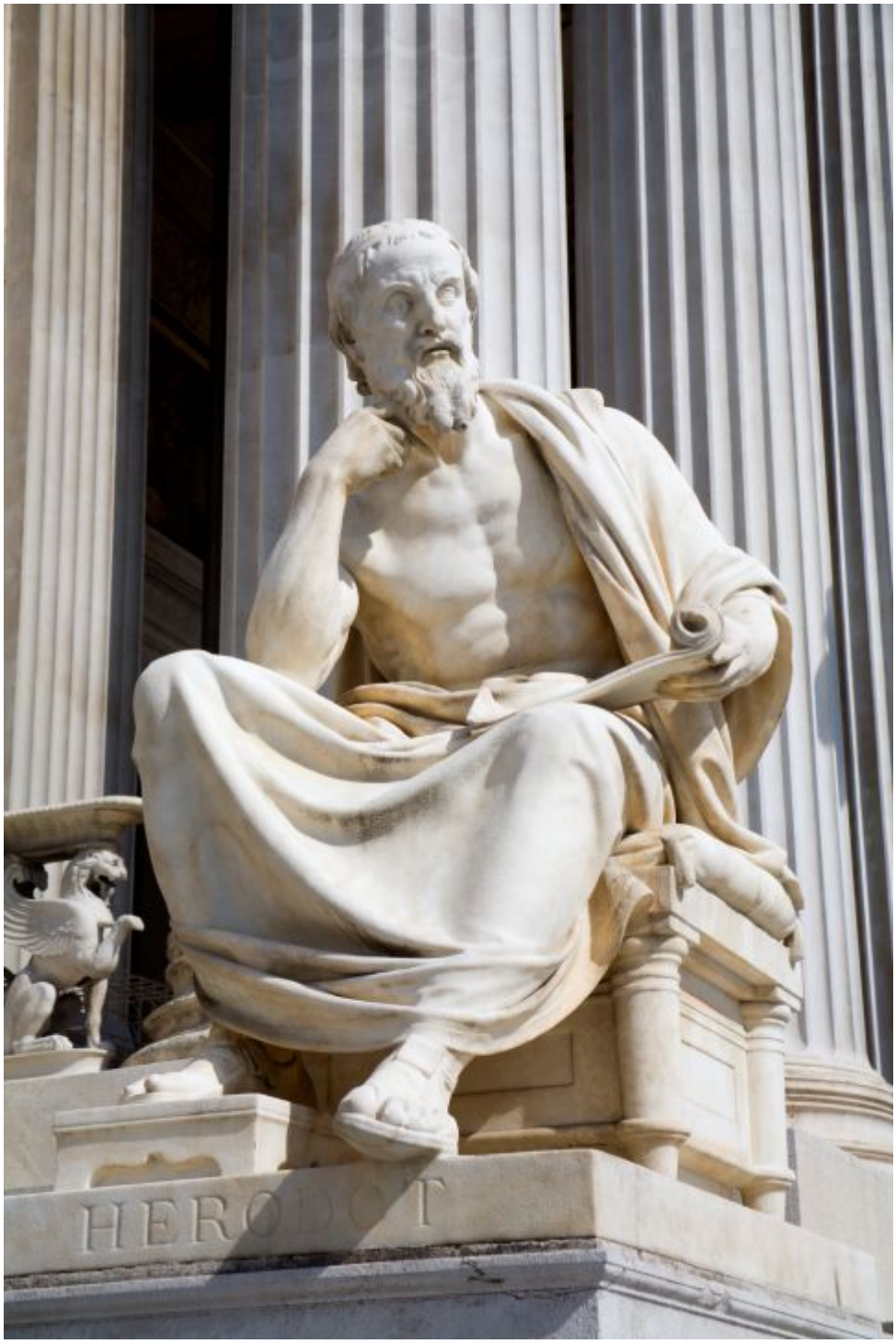
1. Analyze the EPUWBt3.png file and find the malicious code, the tool used to create the code, and the command and control center's address.
2. Based on the information obtained during the analysis of the EPUWBt3.png file, prepare a script that reveals the malicious code in the 8ROnVhd.png file.

Those who have not won a Raspberry Pi before and want to participate in the lottery or want their name to be listed among those who successfully completed the game, must send their detailed solution path, name, surname, and evidence (code, screenshots, etc.) via the contact form or my e-mail address by 21:00 on Sunday, March 14th.

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

Note: When solving this game, remember that you are analyzing malicious software. I strongly recommend that you work with an isolated and up-to-date virtual system software (vmware, virtualbox, etc.)

Good Luck



Herodotus tells how Demeratus, a Greek at the Persian court, warned Sparta of an imminent invasion by Xerxes: he removed the wax from a writing tablet, wrote his message on the wood underneath and then covered the message with wax. The tablet looked exactly like a blank one (it almost fooled the recipient as well as the customs men).