Pi Hediyem Var Cybersecurity Game #18

written by Mert SARICA | 21 February 2020

I am back again with my first Pi Hediyem 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 Erdinç 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

```
Build/OPR6.170623.017)
Host: xxxxxxxxxxxxxxx
Accept-Encoding: gzip
Connection: keep-alive

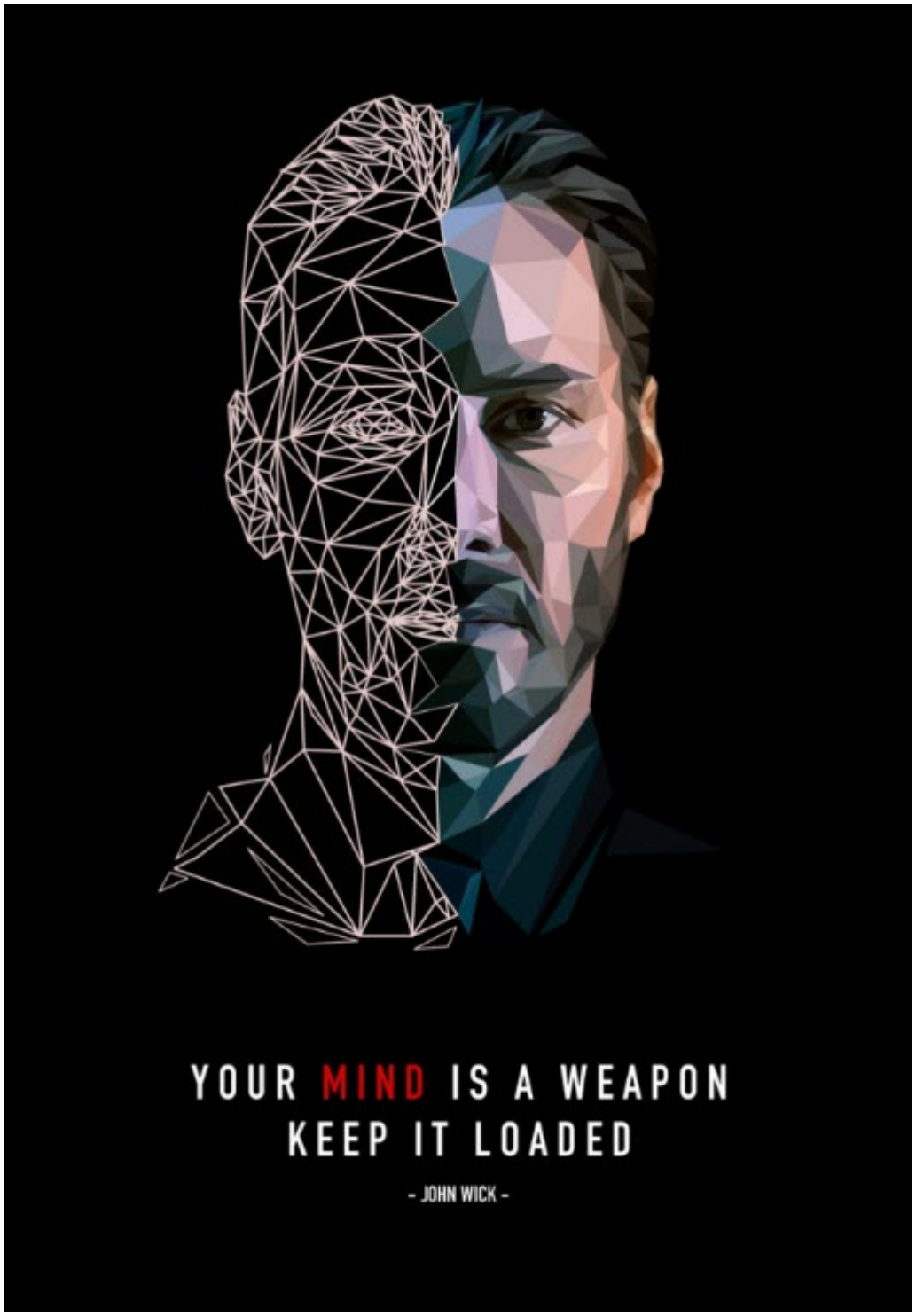
sti=006&q=saved_data_attacker&zip=q7&ws=ODYyMmYzNDRiMThjZDU3MzM3YWNmZmUw
MWNiZDZlNzk4NjdiZjA1MGY5NmY0NzIyYjJkMTBhYWM1MzhhNWQ2Nzc3MzRiMDgyMzgxZjI1
NTQ2ZGFkZTg4ODBhYjZkOWQwOWFiY2Y0NjU1MTJlM2JmMjllNDAwN2E4MDVkMWQwZjQxMWEw
MDY4ZWIyOTlhMGY4YWY3NDk4NWIxNmM5NDEyMjNmOTAyMzNhNGRhMDQ4MGM1YWUzN2NiYzVh
MzNhZTI1NzRjMTg4ODlmNGYwYThhMGRkMzYxYTk3OGNhOGU0NDI5YTI2Y2VjYzhiYzZlMWE2
OWRiMWI4ZDViMWM0Yjc5YjcyNjQ4NTZlNGJjNWZkYjhhZDY1MWVlMDBlYzM3MTM2NTk3ZTQz
ZDhiM2JmNWY2YjBkYzdkMDUxYWRmMjZiOTgzMTU3ZjZiMDhhNjE4ZTY2NDdhMzIyOTg3ODI1
ZmM2ZGNhMGU3MGM3OTMxZWE1ZWQwMzdhZDJlZjBlYjQ1ODdkNTc3ZDg2YTg0NzdiYWUyNWI4
OTAxZTQ2NzAxNDVhNjM1MTQ0ZjFiZmE0NWU2ZjlhYWZmMmY0N2MyY2ZjNGU5MWU5ZDk3OWY5
MDE5M2MzNzc2YmRmOTY4NWQ3NjhjOTIxMjk3OWVkYTUyYmJiNjkwZGYwMTIyODUxNzM5Mjc3
ODgxYTcyMmMzMDUwNjA2YTM0OGQ1NDUwMzg1ODk5NTlkOWVlZmY0ZDViNTYwMGZmOTllYjkz
ZjE3ODFiYmI0OTUyYzM3ZjQzYzA0NjUxYWFjNjMxMjU1OGNkMzUwYWY5NTMyYTRlMjM2NmE2
ZmYxMGU4M2QzZjc1MDk5NWE5MzVhZjVjODQwYjRiZjAwMGEwZWQ1YmQ0N2Y2ZGIzYWYxYTlj
NzFhYWRmZDE3M2U2NWU3MjY5NDQ0NzUzOWI1ZjhlYjEzOTZhNzJjN2U4N2ZhYjc1MDgzYzM2
NWFiZWRhOTQwODM5MmYzZTJkZjY2NDAyYWMwZmEyZjgxYTQ2NzVhM2JiYWNlODRjODAxNzlk
ZTdiNWViMDFmODgxNDkyOWZk
```

For those who have not previously won a Raspberry Pi and wish to participate in the drawing, or those who wish to have their name written on the list of those who successfully completed the game, they must send the detailed solution path, name, surname, age and evidence (code, screenshot, etc.) through the contact form or my email address by Sunday, February 23, at 9:00 PM. If no one correctly solves it, an additional time will be given.

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

Note: Remember that when solving this game, you are analyzing potentially malicious file, so I strongly recommend that you work with a virtual system software (vmware, virtualbox, etc.) that is isolated and has up-to-date patches.

Good luck!


YOUR MIND IS A WEAPON
KEEP IT LOADED
- JOHN WICK -