MA BAKER

[Publish Date]

European Cyber Security Challenge 2018
London, United Kingdom

1. Initial Write-Up

Description:

One of your clients has been the victim of a ransomware attack. From the preliminary testing performed by your team, the ransomware targets only docx files on linux systems. Your client has shared with you an archive with some of the files they would like to recover.

Task:

See if you can recover any of the files.

Proof:

The flag located in any of the unencrypted docx files.

2. Challenge specifications

- Category: Crypto, Binary

3. Tools needed

Description:

Tools needed for the solution of the challenge:

- General Linux tools

4. Artefacts hashing

FILES	MD5	SHA256
ransome.tar.gz	6731852e5c3dd5114406ed08a445bb1e	54048d813daa79351674a4401dd92db5b85df70489169777939f6e476af8c605

ECSC 2018_Ma Baker.pdf	c29c1981f34fad91b217ef2c44360d6c	d9ef64d541916dfa052d3a04272a1514aa3dcb6ebd7ac9fc9678269156fafa46

5. Walkthrough (writeup)

Flag: ECSC{1dddeeac14b2e5755723baa7cf2c0363}

Overview:

1. The analysts can either perform a dynamic or static analysis of the binary;

2. There is a small anti-debugging obstacle (ptrace can be called only once). A simple solution would be to NOP the check;

3. The binary uses srand() to generate a random 256 byte key. The key is used to XOR all the docx files in the current directory. The weakness of the key, which makes it recoverable, is that the seed used is derived from the current process id modulo 255.

4. A brute-force attack would require someone to generate a maximum of 255 keys to recover the files.