New crypto ransomware in town : CryptoFortress

2015-03-04 - Landscape

Blitz post.
[This post has been heavily edited to fix my mistake.

]

I was hunting for Gootkit (pushed in a Nuclear Pack instance in France those days) but instead I got a

~~Teerac.A~~ new crypto ransomware.

Nuclear Pack pushing CryptoFortress via CVE-2013-2551 - FR - 2015-03-04
(have no sure explanation for the 444 error on the "undefined" and CVE-2015-0311 call in that pass).

I thought i was facing Teerac.A (aka TorrentLocker) which was showing that design :

Clicking on the "Buy Decryption software" :

The sample I got today is showing a close identity : CryptoFortress

Clicking on the "Buy decryption software"

Samples : Torrent Locker and a fresh CryptoFortress

26f13c4ad8c1ccf81e80a556cf6db0af - 2014-10-25

e6dda3e06fd32fc3670d13098f3e22c9 - 2015-03-04

Read more :

(PDF) TorrentLocker - Ransomware in a country near you - 2014-12 - Marc-Etienne M.Léveillé - Eset

Post Publication Reading :

CryptoFortress - 2015-03-06 - Renaud Tabary - CertLexsi
