New crypto ransomware in town : CryptoFortress

2015-03-04 - Landscape

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

> @kafeine after further verification, it seems CryptoFortress is completely different from TorrentLocker. They only stole the HTML and CSS.
> — Marc-Etienne M.Lévei (@marc_etienne_) March 6, 2015

]
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" :