CryptoFortress mimics TorrentLocker but is a different ransomware

welivesecurity.com/2015/03/09/cryptofortress-mimics-torrentlocker-different-ransomware/

March 9, 2015

ESET assess the differences between CryptoFortress and TorrentLocker: two very different strains of ransomware.

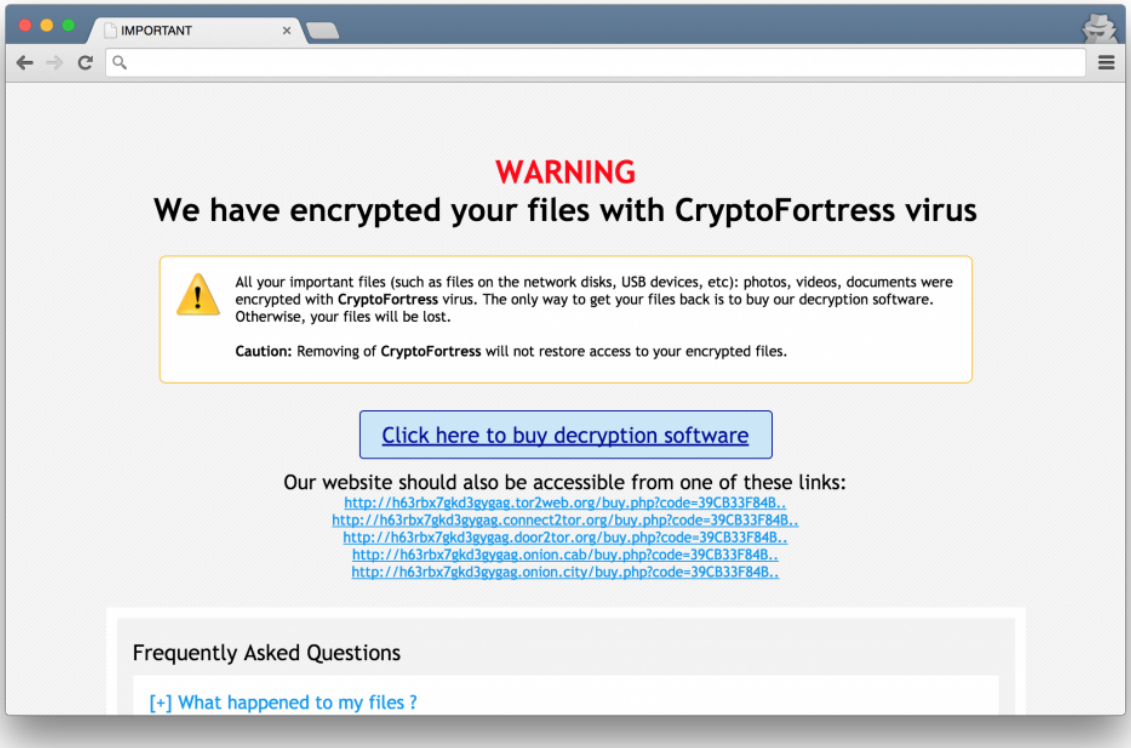
9 Mar 2015 - 05:25PM

ESET assess the differences between CryptoFortress and TorrentLocker: two very different strains of ransomware.

Last week, Kafeine published a blog post about a ransomware being distributed by the Nuclear Pack exploit kit. This ransomware identify itself as “CryptoFortress”, but the ransom message and payment page both looks like an already known ransomware: TorrentLocker.

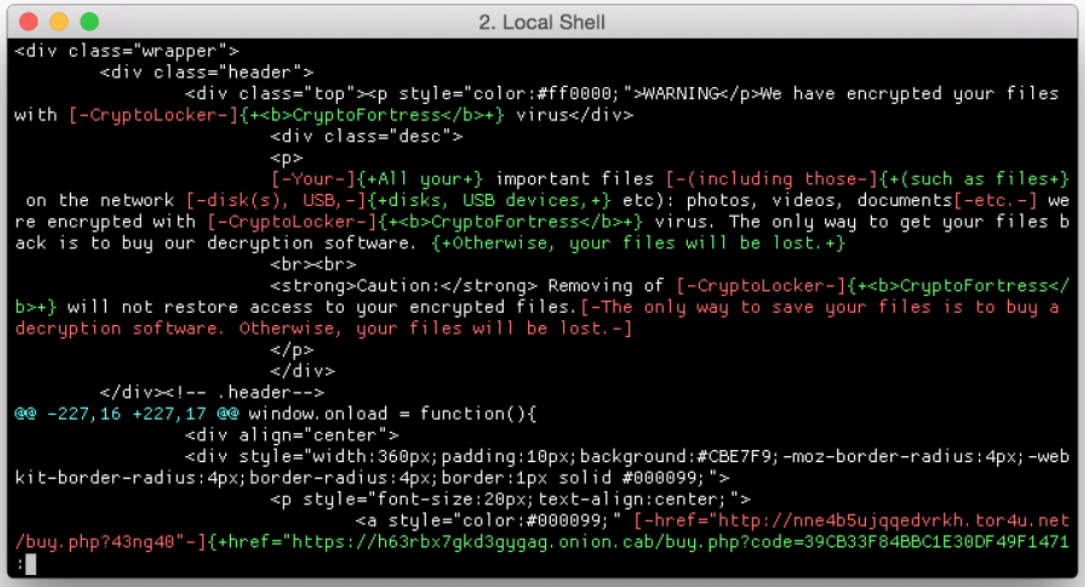
After further analysis, ESET researchers found out is the two threats are in fact very different. **It appears the group behind CryptoFortress has stolen the HTML templates with its CSS.** The malware code and the scheme are actually very different. Here is a table summering the similarities and differences:

	TorrentLocker	CryptoFortress
Propagation	Spam	Exploit kit
File encryption	AES-256 CBC	AES-256 ECB
Hardcoded C&C server	Yes	No
Ransom page location	Fetched from C&C server	Included in malware
Payment page location	Onion-routed (but same server as the hardcoded C&C)	Onion-routed
AES key encryption	RSA-1024	RSA-1024
Cryptographic library	LibTomCrypt	Microsoft CryptoAPI
Encrypted portion of files	2 Mb at beginning of file	First 50% of the file, up to 5 Mb
Payment	Bitcoin (variable amount)	1.0 Bitcoin



CryptoFortress ransom page

TorrentLocker ransom page



Differences in the HTML pages

Last Friday, Renaud Tabary from Lexsi published a complete analysis of the new ransomware. ESET researchers have independently analyzed the CryptoFortress samples before Lexsi released the details. The technical details described in the article matches our findings.

ESET Telemetry also shows TorrentLocker campaign is still propagating via spam messages. Both campaign are now running in parallel.

References

CryptoFortress: Teerac.A (aka TorrentLocker) got a new identity, http://malware.dontneedcoffee.com/2015/03/cryptofortress-teeraca-aka.html

CryptoFortress, http://www.lexsi-leblog.com/cert-en/cryptofortress.html

Sample analyzed

SHA-1 sum	ESET Detection name
d7085e1d96c34d6d1e3119202ab7edc95fd6f304	Win32/Kryptik.DAPB

CryptoFortress public key

```
1 -----BEGIN PUBLIC KEY-----
2 MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmeXVlPGxKoOyvZgLUoyDdzPEH
3 8D6gKlAdZVKmbv2RTjjTAcyOY/40zloPX+iJupuvwO1B/yXlsHZD8y0x/jv7v6ML
4 jHxetmZxUjqv9gLQJE8mJBbU/h0qwc9R7LQwcMapLxvv9O6aMa3Bimjp7bP7WY/9
5 fXgr1m/wA6Tz/kxF+wIDAQAB
6 -----END PUBLIC KEY-----
```

9 Mar 2015 - 05:25PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion