27 juin 2017

APPEL À LA VIGILANCE

PETYA OPTIMISE PAR WANNACRY : PETWRAP

Contexte

Un rançongiciel utilisant le même mode de propagation de Wanacry est apparu aujourd'hui.
Il se propagerait par le port 445 (SMB) en utilisant la même faille EternalBlue.
Pour informations, il utiliserait un certificat Microsoft (joint).

IOC

- *FileHash-SHA256* : 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
- *FileHash-SHA1* : 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
- *FileHash-SHA256* : 64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b
- *FileHash-MD5* : 71b6a493388e7d0b40c83ce903bc6b04
- *FilePath* : dllhost.dat
- *Email de paiement*: wowsmith123456@posteo.net
- *Wallet BTC* : 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
  qui a reçu (à 16h15 0,88 BTC soit environ 1900€)

Echantillons :

https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100
https://virustotal.com/en/file/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745/analysis/

Effet

Comme son ancêtre Petya, PetraWrap chiffre les données et efface le MBR, empêchant la machine infectée de redémarrer.

Propagation

La France et l'Ukraine seraient touchées.