Club de la sécurité de l'information français

Panorama de la cybercriminalité année 2016

Paris, 11 janvier 2017

Evénement organisé avec le soutien de nos sponsors

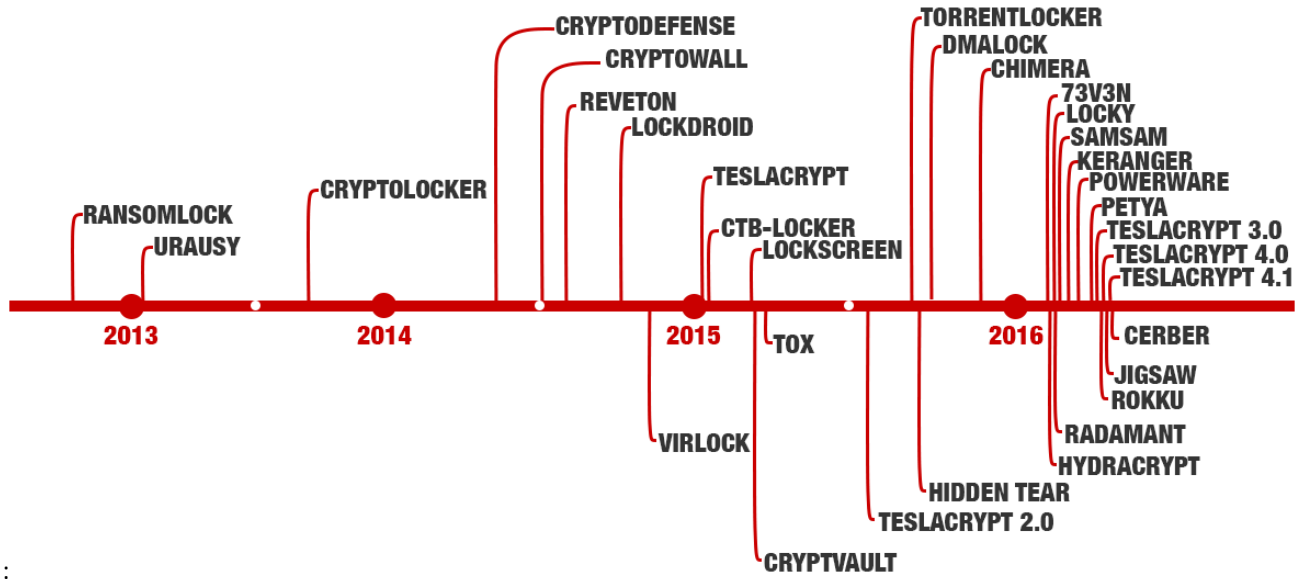
Club de la sécurité de l'information français

Rançongiciels : le changement de dimension

Colonel Éric FREYSSINET
Conseiller – DMIS/C – Ministère de l'intérieur

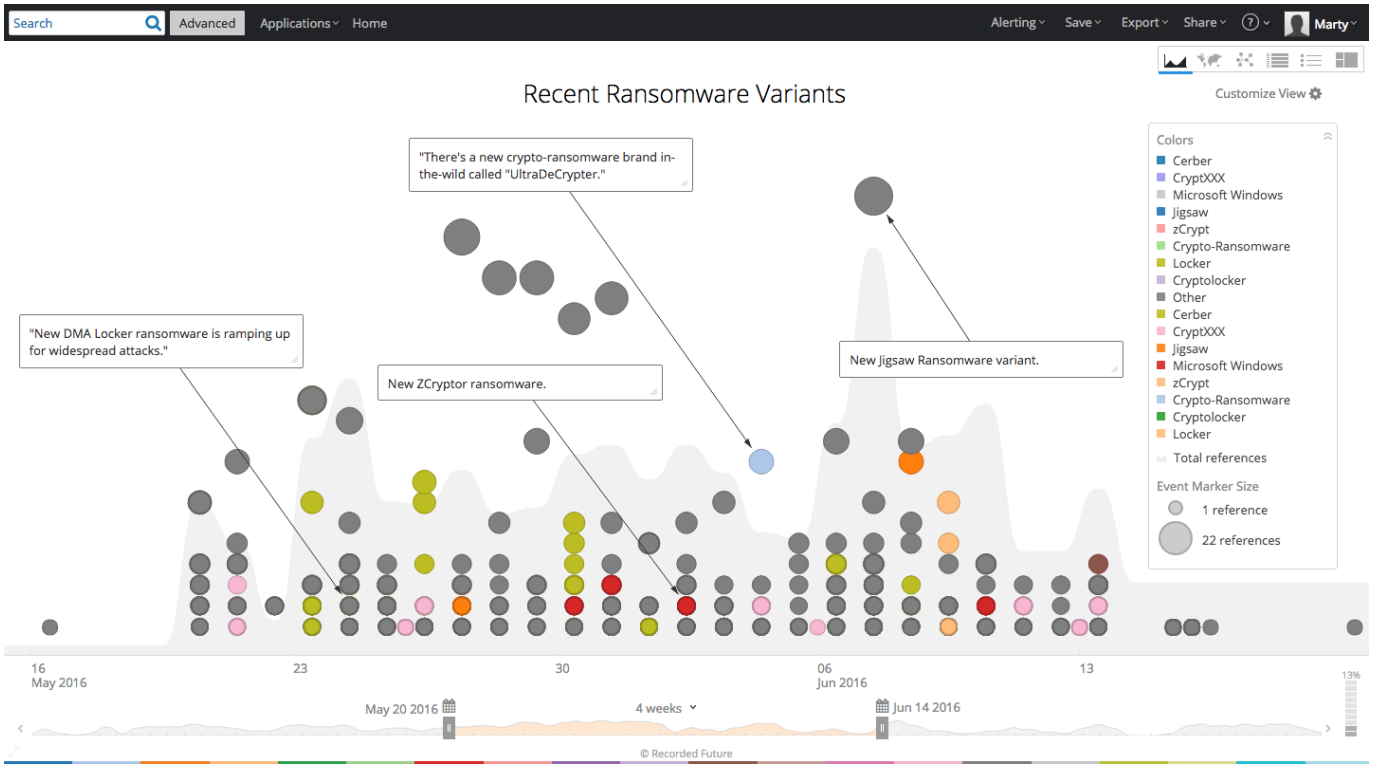
Explosion en 2015 et 2016 des rançongiciels

Et plus particulièrement des rançongiciels chiffrants <u>les cryptolockers et plein de variantes</u>
(ici jusqu'en Avril 2016)



Source :
https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain

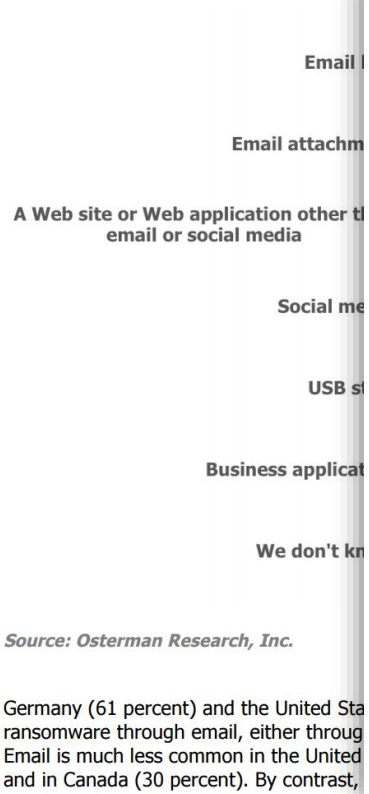
Explosion en 2015 et 2016 des rançongiciels



Source : Visualisation https://www.recordedfuture.com/all-source-ransomware-analysis/

Comment on l'attrape?

- Le courrier électronique comme premier mode de propagation (Aux USA, des variations selon les pays)



Locky, un «ransomware» très actif en France

L'AFP a été la cible d'une autre tentative de piratage ce samedi 19, quand près de 400 boîtes mail ont reçu un message infecté, de nouveau, par le ransomware Locky. Là encore, l'attaque n'a pas eu de conséquence: l'antivirus de l'agence a reconnu la signature de ce logiciel et a été en mesure de le bloquer immédiatement.

Il y a quelques semaines, ce même ransomware a commencé à cibler les clients de Free. Certains d'entre eux ont reçu un mail contenant une fausse facture au format PDF: télécharger ce fichier installe Locky qui bloque et crypte les ordinateurs Windows. En janvier, le site du ministère des Transports était lui aussi la cible d'un «ransomware» similaire. Locky a également paralysé un hôpital américain pendant une semaine en chiffrant les données de 900 patients. La semaine dernière, des sites de médias anglo-saxons, à très forte audience, ont également propagé un programme de ce type, à leur insu, à travers leurs espaces publicitaires.

Combien est-ce que cela rapporte ?

- Plus de la moitié des victimes finissent par payer

Près d'un milliard de dollars de revenus aux USA? (FBI 04)

Source : http://www-03.ibm.com/press/us/en/pressrelease/51230.wss

Rappel: l'extorsion ne demande pas toujours des moyens complexes

- Menace de DDoS transmise par simple courriel

04/18/2016 11:20 pm — Armada Collective

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
http://lmgtfy.com/?q=Armada+Collective

Most importantly, we have launched largest DDoS in Swiss history and one of the largest DDoS attacks ever. Search for "ProtonMail DDoS"

All your servers will be DDoS-ed starting Monday (April 25) if you don't pay protection fee - exactly 10.08 Bitcoins
1Fz53XCH6aa18sEBL8BXf2fFFNCto3Pu2

If you don't pay by Monday, attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

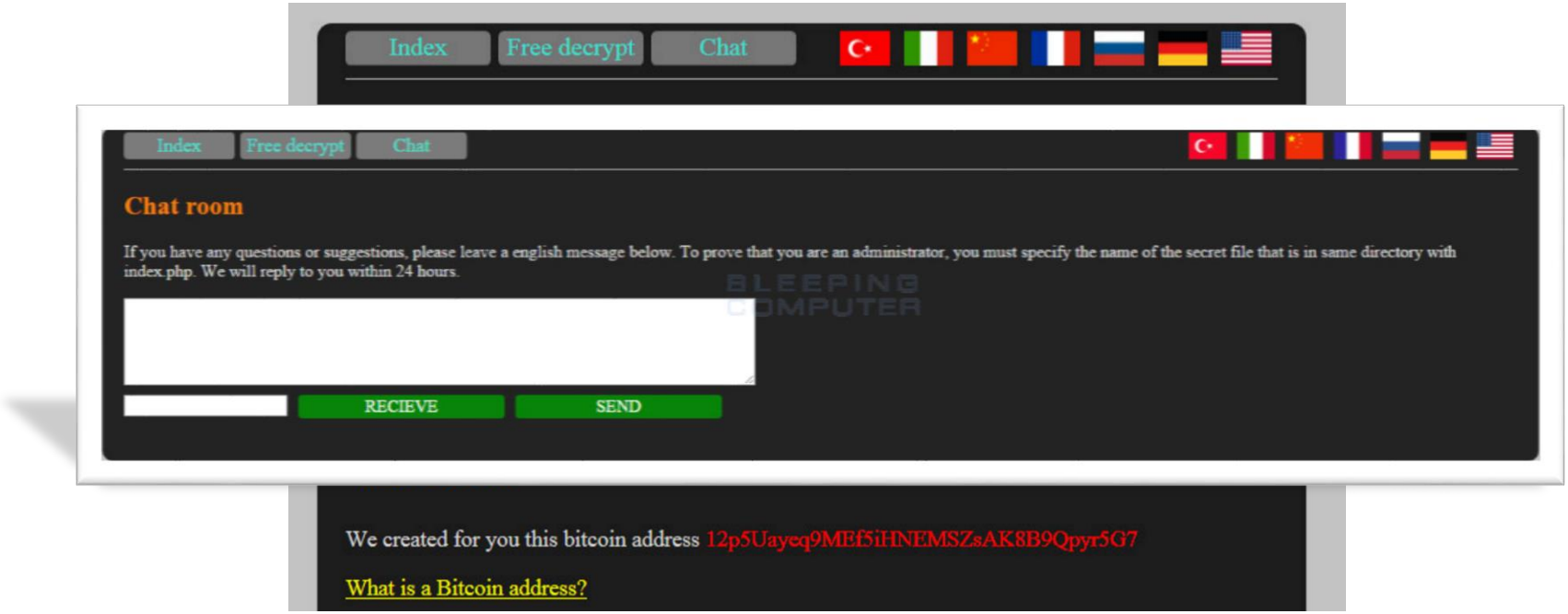
This is not a joke.
Our attacks are extremely powerful - peak over 1 Tbps per second.

Do not reply, we will not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated.

Source :
http://thehackernews.com/2016/04/ddos-extortionist-ransom.html

CTBLocker/Critroni > Sites Web (02/2016)

- Simple fichier index.php et chiffrement AES-256



Source :
https://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/

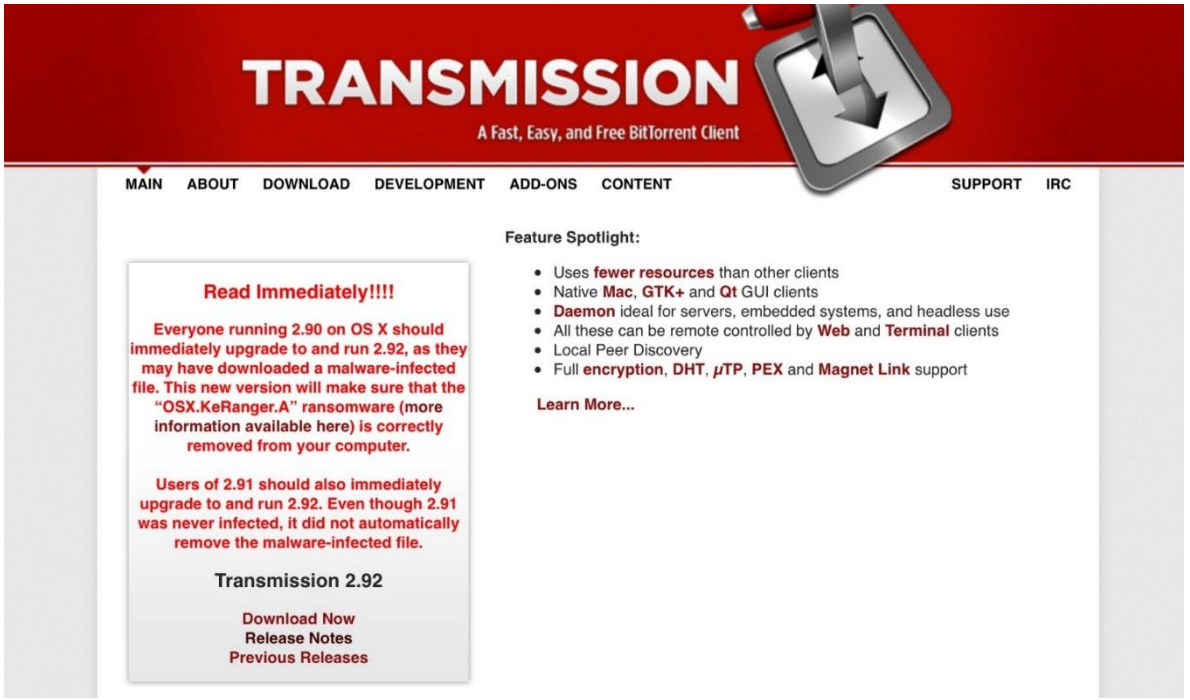
Petya: il chiffre des disques entiers (03/2016)

D'abord il fait croire à une vérification de disque

Source :
https://www.gdata.fr/news/2016/03/28521-petya-le-nouveau-ransomware-qui-chiffre-l-ensemble-du-disque

KeRanger: MacOS X aussi victimes! (03/2016)

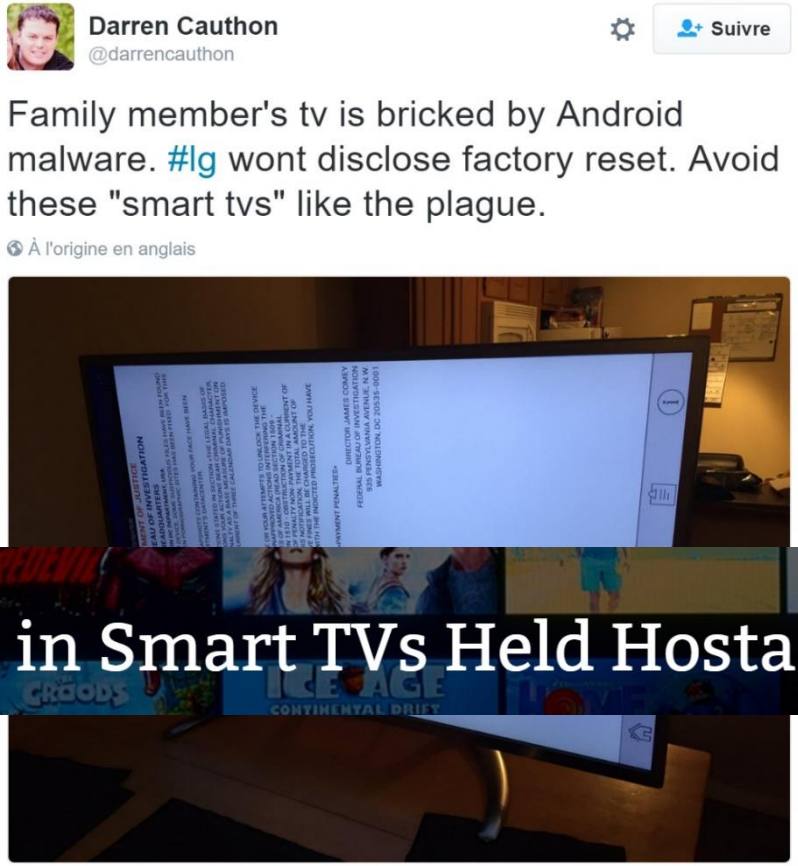
- Infection en téléchargeant un logiciel Bittorrent



Source :
http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

Les téléviseurs ne sont plus à l'abri (06/2016)

- Flocker sur Android TV… (Ne s'active pas dans pays ex URSS…)

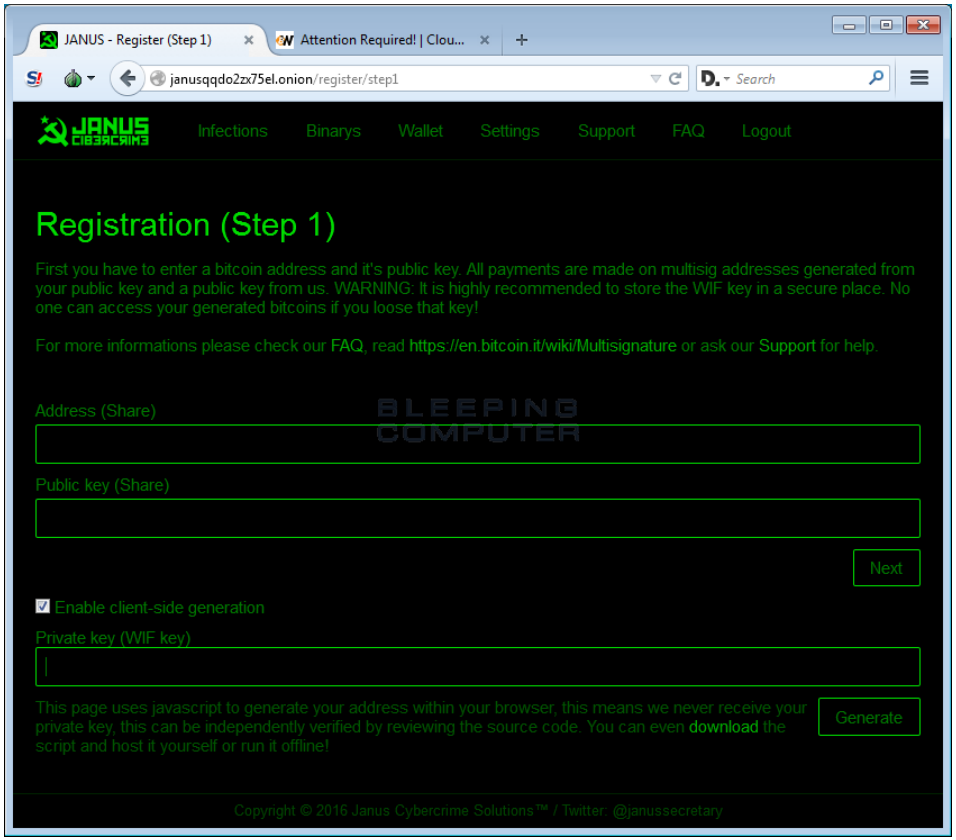


Source : http://www.infosecurity-magazine.com/news/japan-sees-a-spike-in-smart-tvs/

Petya/Mischa : Ransomware as a service (07/2016)

- Les retours pour l'affilié dépendent des revenus générés (de 25% à 85%)

Cible principalement l'Allemagne



Source : https://www.bleepingcomputer.com/news/security/petya-and-mischa-ransomware-affiliate-system-publicly-released/

Popcorn Time (12/2016): Chacun pour soi !

Source : https://www.bl… security/new-s… ransomware-ge… key/

Et ça continue début 2017…

- Avec des cibles de plus en plus variées

KillDisk now targeting Linux: Demands $250K ransom, but can't decrypt

Ransomware : 10.000 bases MongoDB touchées par l'épidémie

Sécurité : *Des chercheurs alertaient récemment sur une campagne de piratage s'attaquant aux bases de données MongoDB mal sécurisées afin d'exiger des rançons. Le bilan s'alourdit.*

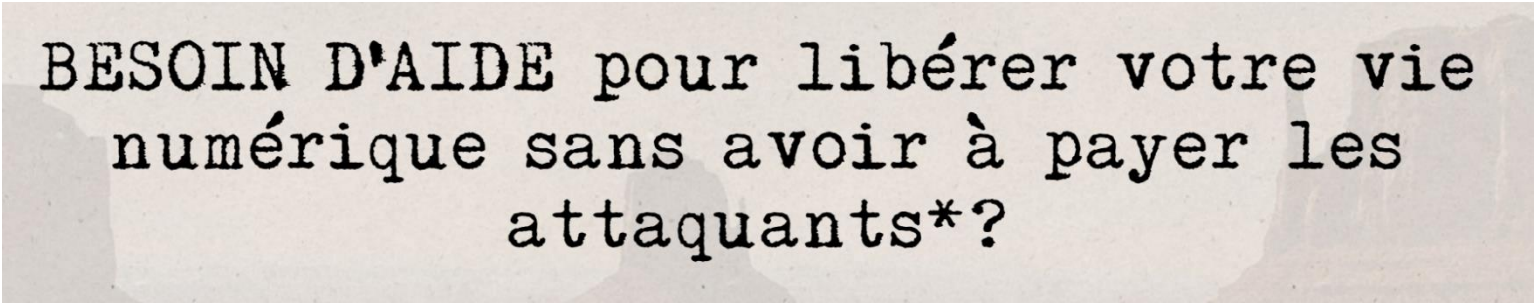
Latest #Mongodb ransack looks like ~27K servers compromised from 12K this morning.. Numbers and info https://t.co/wLF96DLUBQ with @0xDUDE

— Niall Merrigan (@nmerrigan) January 8, 2017

Source :
http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/
http://www.zdnet.fr/actualites/ransomware-10000-bases-mongodb-touchees-par-l-epidemie-39846846.htm

No More Ransom
Agissons contre les rançongiciels!

- Les outils de déchiffrement
- Conseils pour se protéger
- Et réagir !
  - Diagnostiquer
  - Déchiffrer
  - Déposer plainte

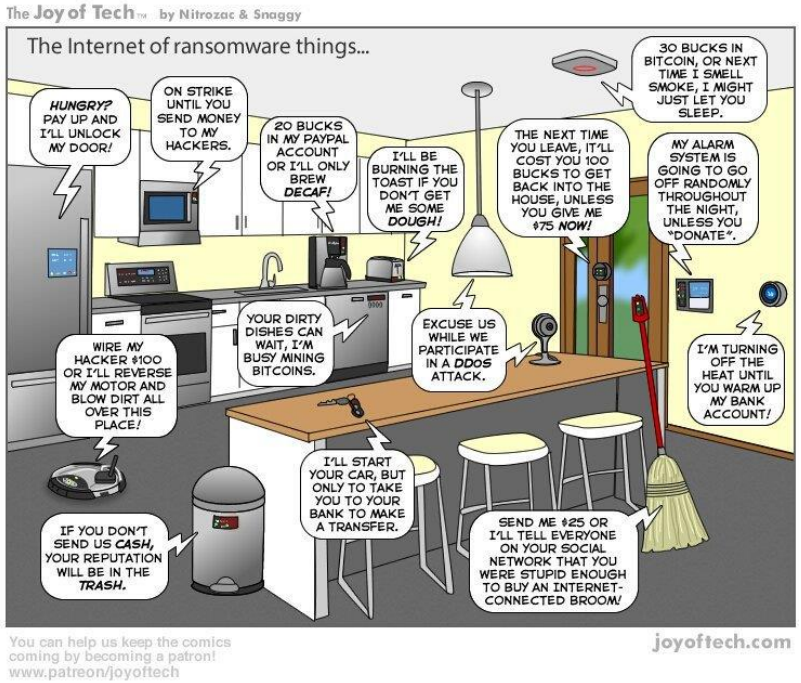


Source :
https://www.nomoreransom.org/fr/index.html

Les conseils

Que nous réserve 2017 ?

- Toujours aussi nombreux, plus difficiles à détecter, les entreprises ciblées….
- Les objets connectés personnels et industriels seront ciblés



Source : joyoftech.com

Sujet 1 – Les rançongiciels 1/5

- Explosion des rançongiciels
  https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain
  https://www.recordedfuture.com/all-source-ransomware-analysis/
- Comment on l'attrape
  https://www.malwarebytes.com/pdf/white-papers/UnderstandingTheDepthOfRansomwareIntheUS.pdf
  http://www.lefigaro.fr/secteur/high-tech/2016/03/21/32001-20160321ARTFIG00183-l-afp-victime-de-deux-tentatives-de-piratage-au-rancongiciel.php
  www.lemonde.fr/pixels/article/2016/11/28/les-transports-en-commun-de-san-francisco-victimes-d-un-piratage_5039627_4408996.html

Sujet 1 – Les rançongiciels 2/5

- Combien ça rapporte
  http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X
  http://www-03.ibm.com/press/us/en/pressrelease/51230.wss
- Extorsion simple
  http://thehackernews.com/2016/04/ddos-extortionist-ransom.html
- Critroni
  https://threatpost.com/ctb-lockercritroni-finds-new-legs-targeting-websites/116457/
  https://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/

Sujet 1 – Les rançongiciels 3/5

- Petya
  https://www.gdata.fr/news/2016/03/28521-petya-le-nouveau-ransomware-qui-chiffre-l-ensemble-du-disque
- KeRanger
  http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/
- Smart TVs
  http://www.infosecurity-magazine.com/news/japan-sees-a-spike-in-smart-tvs/
  http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/
  https://twitter.com/darrencauthon/status/813096722989809665
  https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv/
- Koolova
  http://www.cnetfrance.fr/news/koolova-le-ransomware-qui-veut-vous-sensibiliser-a-la-securite-39846772.htm

Sujet 1 – Les rançongiciels 4/5

- Ransomware as a service
  https://www.bleepingcomputer.com/news/security/petya-and-mischa-ransomware-affiliate-system-publicly-released/
- Popcorn Time (infecter ses amis)
  https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/
- Koolova
  http://www.cnetfrance.fr/news/koolova-le-ransomware-qui-veut-vous-sensibiliser-a-la-securite-39846772.htm
- Nouveautés 2017
  http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/
  http://www.zdnet.fr/actualites/ransomware-10000-bases-mongodb-touchees-par-l-epidemie-39846846.htm

Sujet 1 – Les rançongiciels 5/5

- NoMoreRansom
  https://www.nomoreransom.org/fr/index.html
- Prédictions pour 2017
  http://www.darkreading.com/vulnerabilities---threats/what-to-watch-for-with-ransomware-2017-edition/
  https://techcrunch.com/2016/10/02/what-makes-iot-ransomware-a-different-and-more-dangerous-threat/