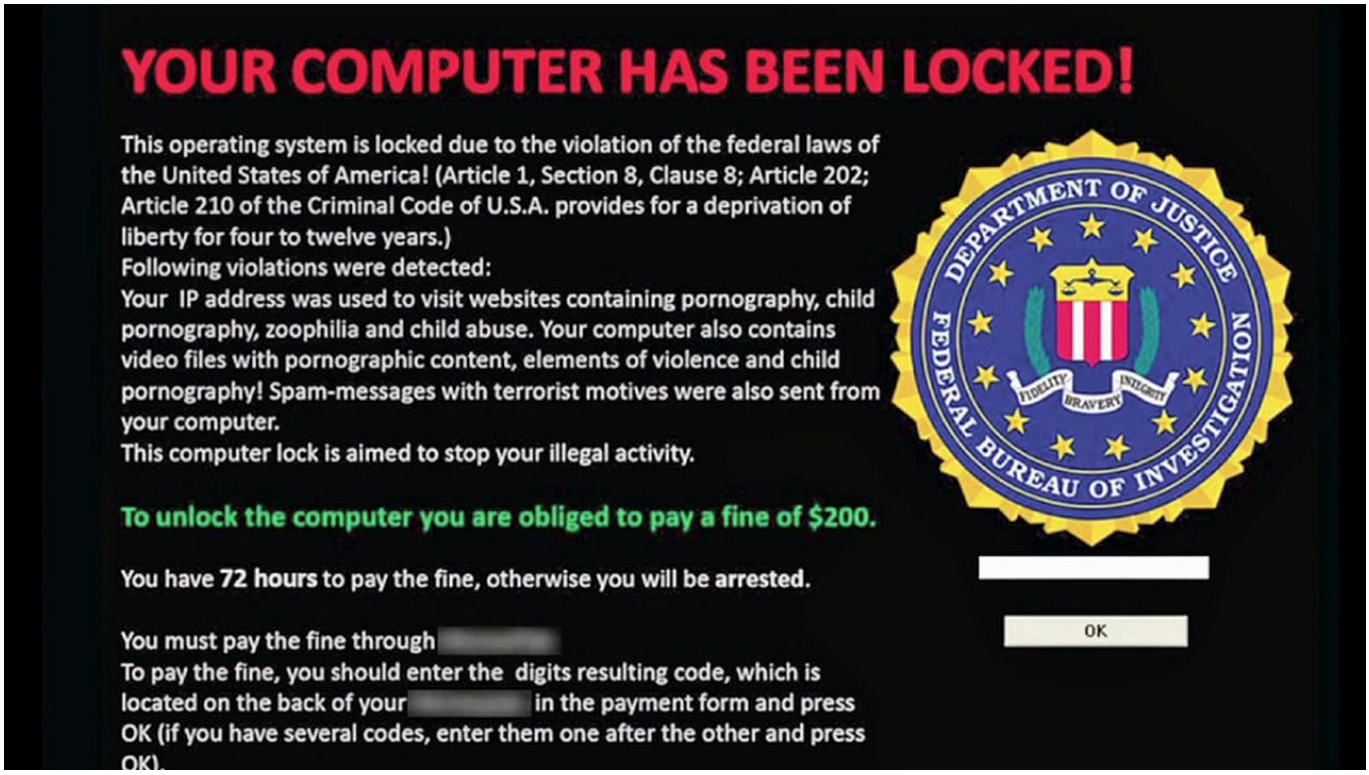
Très à cheval sur la sécurité informatique. Chez NP on essaye d'être alerte quant aux failles de sécurité, proposer des dossiers de sauvegardes des données, de choix de mot de passe, etc.
Aujourd'hui, on discute des ransomware, ces logiciels très vicieux qui bloquent vos appareils.

D'abord il faut connaître la définition du malware: un logiciel malveillant, espion, qui vise précisément à vous nuire. On le nomme couramment virus, bien qu'il existe plusieurs autres types de malware: **vers**, **cheval de Troie**, **spyware**, etc.
En 2017, j'imagine et j'espère que vous avez déjà entendu ces termes-là. Sinon, une bonne recherche sur ~~google~~ votre moteur de recherche préféré, et vous trouverez des articles bien foutus et complets comme celui-ci, ou des guides pour vous aiguiller.

Ransomware

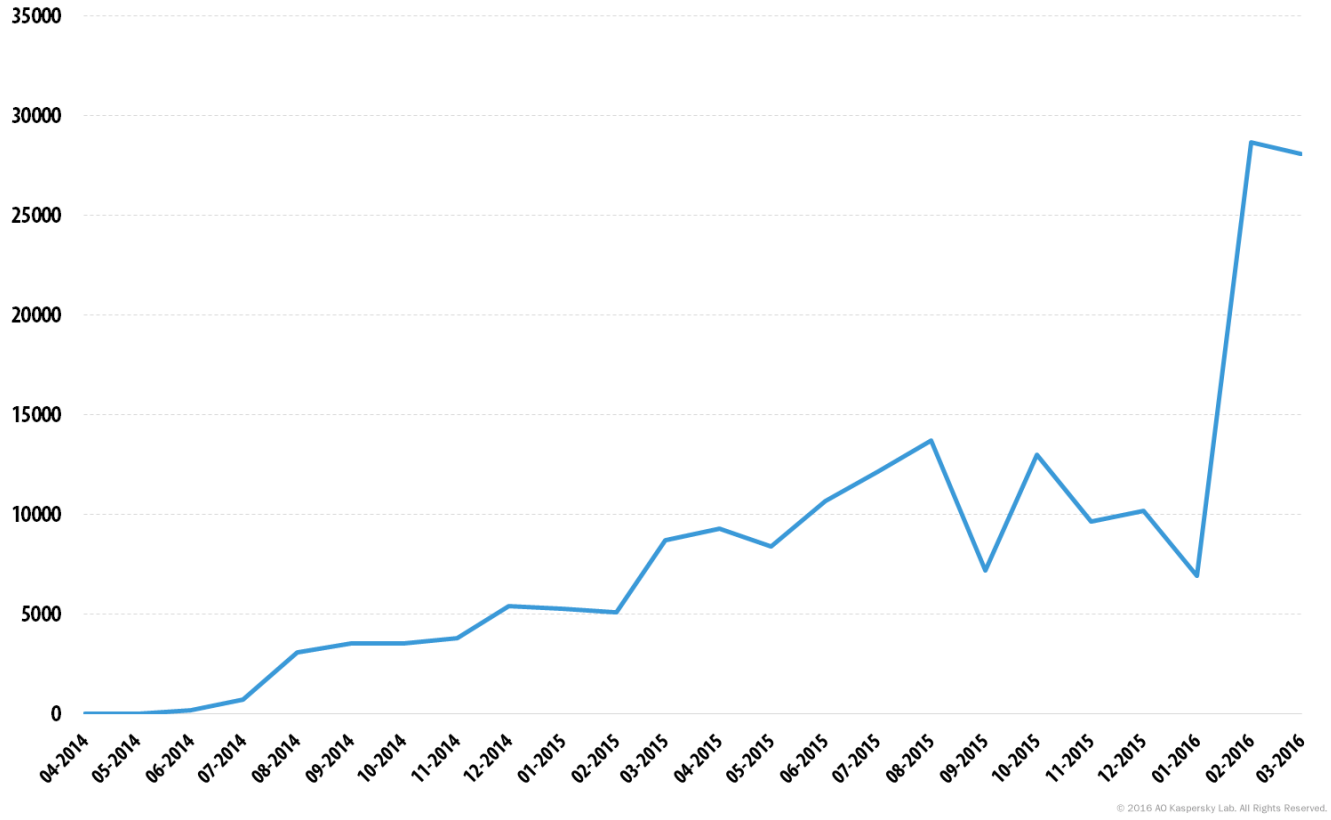
Ransom = rançon.
Le logiciel introduit dans votre ordinateur, 80% des cas, ou votre smartphone, 20% des cas, va crypter votre appareil, un dossier ciblé, ou plusieurs dossiers importants, et vous imposer de payer une **rançon** afin de les débloquer.
La rançon peut-être de quelques euros, pour un particulier, à plusieurs centaines de milliers pour une entreprise. D'ailleurs en 2016 en France, plus d'une entreprise sur deux a été victimes d'un ransomware. **C'est hallucinant !**



Ransomware se faisant passer pour le FBI

Vous arrivez au boulot le matin, votre ordinateur est bloqué, vous avez moins de 24h pour payer, principalement en **bitcoin**, avant que votre ordinateur ne soit totalement effacé. Et cela sans avoir la certitude que tout ne soit débloqué. Un tiers des personnes touchées en

France n'ont jamais vu leurs données débloquées…
C'est aujourd'hui le malware le plus accessible et le plus rentable. Très simples à trouver sur le **darkweb** et à mettre en place, les attaques ont triplé en un an.
En 2014 et 2015, on comptait une poignée de ransomwares, en 2016 plusieurs chaque semaine.



Activité des ransomwares sur Smartphone

En mars 2016, même les utilisateurs de produits **Apple**, appréciés pour leurs sécurités, ont vu apparaître un **ransomware**, **Keranger**.
Après avoir téléchargé un logiciel vérolé, les données sont cryptées petits à petits, et les utilisateurs se sont vu demander d'aller sur un site afin de payer 1 bitcoin (390€) pour décrypter leur contenu.
Évidemment tout le processus est complètement masqué afin de protéger les cyberdélinquants.

Rappel des règles de sécurités

Ca me paraît absurde de répéter ces règles à notre époque, mais :

- Avoir un logiciel antivirus à jour !
- Un firewall
- Des mots de passe réfléchis (chiffres, majuscule, caractères spéciaux, etc.)
- Ne pas cliquer sur des pièces jointes louches
- Tenir son système, ses logiciels à jour
- Être alerte de l'actualité du net
- Télécharger sur des sites louches, non recommandés
- Avoir des sauvegardes

D'une manière générale, être intelligent, responsable, et tourner plusieurs fois ses doigts dans la bouche avant de cliquer.

Que faire si vous êtes ciblés par un ransomware !

- Il est clair qu'on peut être pris de panique, et céder à la tentation de payer. Mais il est important de se reprendre et ne pas céder au **chantage**. Rien ne garantit que vous retrouverez vos données. De plus vous encouragez malgré vous ce type d'attaque.
- Éteindre, débrancher son ordinateur, déconnecter les câbles Ethernet, afin de stopper une éventuelle propagation sur votre réseau pro ou domestique. Je vous conseillerai aussi de débrancher vos disques durs.
- Si vous n'êtes pas à l'aise, mon conseil: contacter un professionnel de l'informatique, dans votre entourage, dans votre ville. Il est préférable de débourser 100€ chez un pro, plutôt que 500€ pour un pirate. Il saura les bonnes choses à faire.
- À l'aise, vous pouvez vous-même désinfecter votre appareil à l'aide de disques proposés pas votre antivirus.
- Demander des conseils sur des forums spécialisés. Il existe des logiciels anti-ransomware.
- Enfin, signaler l'attaque à la gendarmerie ou au commissariat de Police. Dans 100% des cas, ils ne feront rien pour vous techniquement, mais votre plainte aura le mérite de rentrer dans les statistiques et faire évoluer la cyberdéfense en France.