Depuis le vendredi 12 mai 2017, une cyberattaque par rançongiciel d'une ampleur sans précédent frappe la planète entière, France comprise.

Rien que dans hexagone on dénombre plus de 20 000 victimes (PME, grandes entreprises, hôpitaux, etc…) . La plus emblématique est l'usine Renault de Douai dont la production a été stoppée pratiquement une journée. Imaginez le cout phénoménal d'une telle problématique. Ça se chiffre en million d'euros ! Hélas le bilan risque de s'alourdir. Après le week-end combien d'ordinateurs vont s'allumer aujourd'hui ?!

WannaCry qu'est-ce que c'est ?

Un rançongiciel. Comme son nom l'indique, c'est une rançon 2.0. Si vous voulez récupérer vos données va falloir casquer. Grosso modo un « virus » qui va crypter tout le contenu de votre ordinateur, et de tout ce qui y est connecté et contient des données (y compris un réseau). Une page va s'afficher et vous donner la marche a suivre pour payer la rançon (en Bitcoin – cette monnaie virtuelle convertible en cash classique) .

Malheureusement, comme dans tous les cas de rançons de la vie physique, les chances de récupérer son bien est proche de zéro. En effet donné un « code » de déblocage tuerait la poule aux œufs d'or.

Particularité : là où un rançongiciel s'active en ouvrant une pièce jointe d'un mail celui là utilise une faille réseau Windows (le port 445 pour les connaisseurs). Elle a été corrigée par Microsoft en mars, mais de nombreux utilisateurs n'ont pas installé la mise à jour pour tout un tas de raisons (genre trop cool cette vidéo youtube, je ferais ça demain…ou jamais) et sont donc vulnérables. Une fois Wannacry installé, il se répand à travers le réseau local, ce qui explique comment des établissements entiers comme des hôpitaux sont devenus inopérants ce week-end.

Anecdote amusante, cette faille a été utilisée la première fois par le NSA qui l'exploitait dans le cadre de ses opérations de surveillance électronique sous le nom de code « EternalBlue » révélé en avril 2017 par un groupe de Hacker (The shadow brokers).

A quoi ça ressemble ? – la petite vidéo du site Zataz qui en fait la démo

Comment s'en prémunir ?

Pour minimiser les risques, il faut travailler en amont :

- Effectuez des sauvegardes régulières et multiples (ainsi en cas de chiffrement du disque dur, une restauration des données sera possible)
- Mettez impérativement à jour vos systèmes d'exploitation et vos applications.
- Installez un anti-virus sur chaque poste de travail, mais également sur le serveur de messagerie e-mail de l'entreprise.

- Mettez à jour régulièrement vos antivirus
- N'ouvrez pas les mails dont l'identité de l'expéditeur est incertaine ou inconnue. Attention les pirates peuvent imiter les adresses de correspondants habituels : La-Poste » au lieu de « LaPoste »
- Sensibiliser tous vos proches à ce type de risque mais aussi à tous ce qui a trait à la sécurité informatique.

Si vous avez été infecté :

- Déconnectez immédiatement le poste infecté du réseau et effectuez une restauration complète du système (on voit l'importance de ce qui est dit plus haut).
- Dans le cas où la pièce jointe aurait été ouverte, isolez immédiatement l'ordinateur compromis en le déconnectant du réseau (arrêt du WiFi, câble Ethernet débranché). L'objectif est de bloquer la poursuite du chiffrement et la destruction des dossiers partagés.
- Prenez en photo les écrans ou réaliser des copies d'écran (mail frauduleux et ses pièces jointes) et notez l'ensemble des actions réalisées.
- Contactez rapidement une société de maintenance informatique ou un ami geek (un vrai, pas juste celui qui sait mettre la clé Usb dans le bon sens).
- Communiquez immédiatement sur l'attaque auprès de l'ensemble des utilisateurs de votre ordinateur mais aussi à vos contacts afin qu'ils appliquent les mesures préventives.
- Et enfin, déposez plainte auprès du service de police ou de gendarmerie territorialement compétent.

NB : Les ordinateurs les plus fragiles et d'ailleurs cible principale de Wannacry sont les machines sous Windos XP (soit encore 13% des machines en service en France.

Microsoft qui a pourtant cessé la maintenance de cet OS a quand même réactivé un correctif qui réduit la vulnérabilité et publie un tuto pour se prémunir. C'est par ici.

Qui est à l'origine de l'attaque et quel est son mobile ?

A vrai dire on n'en sait rien, mais ce qui est étonnant c 'est que la page de rançon est en Français au lieu de l'anglais habituellement utilisé, ce qui en soit est suffisamment rare pour être significatif. Faut il relier cette attaque au groupe de hacker évoqué plus haut ? Pas évident… je pense que l'avenir nous donnera quelques clés.

Si vous voulez en savoir plus sur les rançongiciel (s) :

http://stopransomware.fr
https://forum.malekal.com/
https://korben.info/wannacry-bien-pleurez.html

Voilà, vous en savez un peu plus sur le monstre qui écume la toile.

N'oubliez pas de mettre à jour votre windows, vos antivirus et restez vigilants. La matrice est un monde formidable, mais l'agent Smith n'est jamais loin….