Comment lutter contre WannaCry ? / G.Litzistorf – 30 mai 2017

Plus de 200 000 ordinateurs ont été infectés par un « rançongiciel » qui réclame 300 francs à ses victimes (Le Temps du 15 mai 2017)

A) Analyse du mode opératoire

12 mai 2017 Le ransomware WannaCry (aussi connu sous les noms Wanna Cry, WannaCrypt et WanaCrypt0r 2.0) bloque plus de 200 000 PC depuis ce vendredi 12 mai. Les ordinateurs affectés par le virus affichent un message indiquant à l'utilisateur que ses données ont été ~~cryptées~~ chiffrées et qu'elles peuvent être récupérées (=déchiffrées) en l'échange d'une somme d'argent à verser en bitcoins.

Source = http://www.blogdumoderateur.com/cyberattaque-ransomware-wannacry/

Consulter au besoin cet excellent rapport http://www.tdeig.ch/security/Manoubi_RPS.pdf pour comprendre le mode opératoire de ce type de malware qui chiffre vos fichiers puis vous demande une rançon

14 mars 2017 Microsoft (MS) publie un correctif (de plus) pour les systèmes Windows 7, 8 et 10
Il s'agit de Security Update for Microsoft Windows SMB Server (4013389)
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Selon MS :
Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerabilities could gain the ability to execute code on the target server.
To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server.
The security update addresses the vulnerabilities by correcting how SMBv1 handles these specially crafted requests.

La faille (=bug) est présente dans le code qui gère le très vieux protocole SMBv1
Le hacker sachant l'exploiter peut exécuter son code à distanc

Une société a développé du code pour la NSA et se l'est fait voler par le groupe Shadow Brokers qui l'a publié → https://github.com/adamcaudill/EquationGroupLeak

Selon Talos appartenant à Cisco
http://blog.talosintelligence.com/2017/05/wannacry.html
WannaCry utilise le module ETERNALBLUE et la porte dérobée DOUBLEPULSAR
https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit/

Le mécanisme d'infection utilise les ports SMB traditionnels = 445 et 139

Pour celui qui veut en savoir plus :
http://gelit.ch/Secu/41_Malware.pdf
http://gelit.ch/Secu/42_Lab_Malware.pdf

B) Défense du poste de travail

Mesures préventives (valables pour toutes les versions de Windows)

1) Désactiver le serveur de fichier
   Dans Control Panel\Network and Internet\Network Connections
   ☐ File and Printer Sharing for Microsoft Networks
2) Utiliser un modem routeur (ADSL) qui bloque toutes les requêtes en provenance d'internet
3) Séparer vos données du système d'exploitation en créant une partition D:
4) Faire régulièrement une sauvegarde de D: sur un disque USB externe qui n'est connecté que le temps de la sauvegarde (éviter les services Cloud gratuit … car ils ont tous été hackés)
5) Tester – tester – tester

Mesures correctives (inutiles si les mesures préventives ont été respectées)
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Défense du serveur de fichiers

1) Utiliser une version Linux comme CentOS et le package Samba
2) Identifier les principaux risques
   Où sont les postes client ? … dans l'intranet, sur internet, …
3) Gérer correctement les authentifications
4) Gérer correctement les droits en lecture – écriture
5) Faire des sauvegardes
6) Tester – tester – tester

La **sécurité** du poste de travail, d'un serveur de fichiers et des complexes systèmes d'information **repose** sur la notion de **confiance :**

- Avez-vous confiance dans le firewall (pare-feu) qui protège votre intranet ?
- Avez-vous confiance dans le système d'exploitation de votre ordinateur ou smartphone ?
- Pensez-vous que tous les sites sur internet sont dignes de confiance ?
- Pensez-vous que tous les mails reçus qui vous promettent des millions sont sérieux ?

Il est plus économique d'éviter de surfer sur des sites douteux ou d'effacer un mail douteux que de construire des défenses logicielles complexes, donc chères, que le hacker se fera un plaisir de contourner … avec l'aide parfois de la NSA

Au niveau technique, il convient de mettre en place des mesures **préventives** réfléchies qui permettent souvent un bon niveau de défense.
Ne pas compter sur les mises à jour et les antivirus qui arrivent très souvent après la tempête pour se concentrer sur **une défense en profondeur de type white list**

La très grande majorité des problèmes informatiques est due à une ou des erreurs humaines !

Nous sommes le maillon faible qui a oublié de faire une sauvegarde, mal configuré des droits, oublié de désactiver un service, … mal programmé une application … oublié de fermer la porte à clé

Chacun le fait au quotidien pour éviter vol, incendie ou accident