Parc d'Activités Schweitzer
26 rue du bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

NDR

NETWORK PROTECTION & REPONSE

COMMENT SE PROTEGER EFFICACEMENT CONTRE LA NOUVELLE GENERATION DE CYBER-ATTAQUES ?

❖ Cinq ans après wannacry, ce que nous avons appris sur les ransomwares

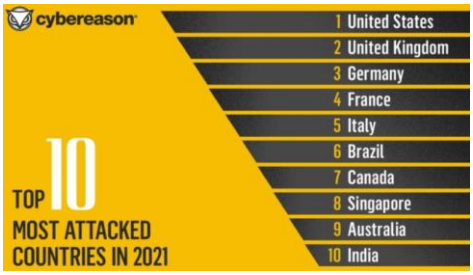
Le 12 Mai 2017 le logiciel malveillant Wannacry se déployait sur la moitié des ordinateurs du monde.

Wannacry exploitait une vulnérabilité de Windows et 230.000 victimes ont découvert leurs données chiffrées.

Ce fut la 1ere et l'une des plus grandes cybers attaques de tous les temps.

Cette attaque a mis en évidence la nécessité de mesures de sécurité plus proactives, démontrant l'insuffisance de simples pare-feu pour assurer la protection des systèmes.

<u>Des ransomwares aux RansomOps</u>



Cinq ans après Wannacry, les entreprises ont acquis une nouvelle conscience de la sécurité informatique.

Entre-temps, toutefois, les ransomwares ont également évolué et le niveau de menace n'a cessé de croître.

Plutôt que de ransomware, il serait préférable aujourd'hui de parler de RansomOps. Les menaces actuelles reposent principalement sur **des tactiques modernes et interactives mises en œuvre par des <u>opérateurs humains</u>**, qui ont remplacé l'approche automatique et programmée d'une attaque via des vers informatiques comme l'était Wannacry.

Cette distinction est importante car elle affecte la manière dont les entreprises doivent se défendre. On ne se défend pas contre des humains comme on se défend contre des algorithmes

Avec les générations précédentes de ransomware, le délai entre l'infection et l'activité malveillante exécutée par le logiciel cible était court et le chemin de l'attaque était assez prévisible, car engendré par des « Robots ».

Les groupes de cybercriminels modernes, quant à eux, ont tendance à se tapir dans les systèmes informatiques pendant le temps qu'il faut pour s'approprier les droits d'accès administrateur du S.I., des sauvegardes (même externalisées) de la messagerie, des serveurs dans le cloud etc.. .

La préparation de l'attaque est méthodique et celle-ci n'est lancée que quand les agresseurs sont certains que l'entreprise n'a plus de solution de secours et ne pourra pas avoir d'autre option que payer la rançon.

Lorsque l'attaque est lancée (chiffrement, exfiltration ou destruction des données), toutes les barrières sont tombées et il est très souvent trop tard pour agir.

De la prévention à la détection

Compte tenu de la stratégie actuelle des cybercriminels, un système de protection moderne doit se concentrer sur la phase précédant le lancement de l'attaque.

Lorsque les attaquants ont réussi à pénétrer le système d'information, ils vont, dans un 1er temps, découvrir le réseau, installer des logiciels de détection de frappe, lancer des applications spécifiques, naviguer dans les dossiers, exfiltrer les données issues de leurs outils, etc… .

C'est à ce moment que les pirates sont vulnérables et peuvent être détectés car ils vont se manifester par des comportements inhabituels sur le réseau. Nos nouvelles solutions de détection basées sur l'I.A. et la surveillance humaine vont détecter ses comportements inhabituels et caractéristiques d'une attaque en cours de préparation.

Il est alors encore possible d'empêcher l'attaque fatale.

Analogie

On pourrait, afin de vulgariser le processus, comparer cette nouvelle façon de procéder à l'attaque d'un château fort au moyen âge.

Les fortifications, peuvent être comparées aux antivirus, antimalwares et autres mots de passe d'identification.

Le pont-Levis et la porte fortifiée, sont comparables aux Firewalls et proxy.

Imaginons qu'au lieu d'assiéger le château, les attaquants s'infiltrent à l'intérieur du château fort à l'instar d'espions, qu'ils accèdent au système d'ouverture de la porte fortifiée et puissent actionner le pont-levis. Qu'ils inhibent les archers présents sur les fortifications et déploient les échelles. Enfin qu'ils rendent inopérant l'accès au stock d'armes de l'enceinte.

Lorsque l'attaque est lancée simultanément, de l'intérieur et de l'extérieur, il est trop tard et les fortifications sont inutiles.

Il est donc stratégique que, malgré les fortifications et les sécurités de protection contre les attaques externes, une équipe de surveillance interne s'assure qu'aucun espion n'est réussi à pénétrer la fortification et ne prépare l'attaque fatale.

VOUS SOUHAITEZ EN SAVOIR PLUS SUR NOS SOLUTIONS DE PROTECTION NDR (NETWORK PROTECTION & REPONSES) CONSULTEZ-NOUS.
NOTRE EXPERT EN CYBER SECURITE EST A VOTRE DISPOSITION POUR EVALUER, CONSEILLER, FORMER ET TESTER VOS VULNERABILITES TECHNIQUES ET HUMAINES.

Parc d'activité Schweitzer
26 rue du Bois Fossé - BP 147
85301 CHALLANS Cedex

Tél. : 02 51 49 31 31
Email : contact@espace-technologie.com
Web : www.espace-technologie.com

Organisme de formation n° 52850059385 - SAS au capital de 38 500 € - Siret : 38979357100024 - APE : 4741Z - RCS La Roche sur Yon B389793571