Johanne Ulloa, Trend Micro : « La v2 du ransomware est déjà là »

Un cauchemar qui devient réalité. Pour Johanne Ulloa, spécialiste en cybersécurité de l'éditeur Trend Micro, le piratage du centre médical presbytérien d'Hollywood, un hôpital américain victime d'un ransomware (un malware de chiffrement qui réclame une rançon pour restaurer les données prises en otage), marque une nouvelle étape dans l'utilisation de cette menace par les cybercriminels. Explications.

Silicon.fr : Pourquoi estimez-vous qu'une étape a été franchie avec le piratage de l'hôpital à Hollywood ?

Johanne Ulloa : Dans ce cas, mais aussi dans celui de certains hôpitaux en Allemagne, il semble que nous n'ayons pas affaire à un ransomware, infectant une organisation via une compromission hasardeuse, consécutive à une campagne massive de spams malicieux par exemple. L'infection ressemble ici plutôt à une opération montée par des cybercriminels bien organisés. Car les assaillants n'auraient pas pu demander une telle somme (le Hollywood Presbyterian Medical Center a reconnu avoir versé 17 000 $ pour débloquer les données) si les données étaient restaurables depuis les sauvegardes de l'organisation. Je pense donc qu'une action préalable a été menée afin de compromettre les sauvegardes ou de les neutraliser. C'est ce que je qualifierais de v2 des attaques par ransomware, dans lesquelles ces malwares ne sont utilisés qu'au cours d'une seconde étape après une première compromission ciblant les sauvegardes.

Êtes-vous surpris de cette évolution de la menace ransomware ?

Non, j'étais même convaincu que cette évolution se produirait. J'ai par contre été surpris que les cybercriminels s'en prennent à un hôpital. Dans ce type d'organisations, l'incapacité à accéder aux données entraîne un risque vital. A Hollywood, des patients ont été évacués, les professionnels de santé ont dû rebasculer sur des opérations manuelles. Mais c'est aussi ce niveau de risque qui donne aux cybercriminels la capacité à demander des rançons importantes.

Comment se préparer à ce type d'attaques ?

Il faut prendre le cas de l'hôpital d'Hollywood, le seul rendu public à ce jour, et étudier comment réduire les risques. L'important lors des infections par ransomware, c'est d'être en mesure de restaurer les données. Il faut donc tester régulièrement le système de restauration et, si possible, effectuer des sauvegardes offline, inaccessibles aux cybercriminels. A défaut, les sauvegardes ne doivent être accessibles qu'en lecture seule. Concernant l'infection par ransomware, comme Locky actuellement au centre d'une vague d'attaques impressionnante, il faut se concentrer sur la phase de première compromission. Comme ces menaces évoluent trop vite pour être détectées par les anti-malware classiques, la piste la plus prometteuse réside dans les outils de sandboxing (ou bacs à sable, permettant d'exécuter du code à l'intérieur d'une enveloppe protégeant le système des contaminations, NDLR).

Les hôpitaux, notamment en France, sont-ils armés pour affronter les nouvelles menaces ?

La cybersécurité des hôpitaux reste un domaine complexe. D'abord parce qu'en plus des environnements IT traditionnels, les équipes doivent gérer des environnements biomédicaux sur lesquels elles n'ont aucune maîtrise. La surface d'exposition est donc très vaste. Par ailleurs, bien que la donnée manipulée dans les hôpitaux soit confidentielle, le corps médical doit pouvoir y accéder très rapidement. Dans ce type d'environnements, il faut renforcer la détection, pour gagner en visibilité sur ce qui se passe sur le réseau. Mais aussi se préparer aux impacts des cyberattaques.

A lire aussi :

Ransomware : les hackers chinois se joignent aux cybercriminels

Le ransomware Locky mute pour multiplier ses victimes en France

Le ransomware KeRanger cadenasse les utilisateurs de Mac