Dissection d'une attaque ransomware

C'est un jour comme les autres. Un employé tire un fauteuil jusqu'à son bureau, une tasse de café à la main, il s'apprête à commencer sa journée de travail. Il est encore tôt et son attention n'est pas encore optimale.

Distrait par les allées et venues de ses collègues, il s'efforce néanmoins de prendre connaissance de ses e-mails. Il en repère un qui lui paraît urgent, concernant une facture non réglée, il n'est pourtant pas du genre à oublier un paiement. Il ouvre donc la pièce jointe, soudain sa machine se bloque, et ses données deviennent inaccessibles. Un message lui réclamant de l'argent s'affiche à l'écran, pour récupérer ses données il devra payer sous 24 heures une rançon. Passé ce délai, ses données pourront être effacées définitivement.

Ce type de scénario se produit chaque jour dans une entreprise à travers le monde. Et c'est ce sur quoi misent les cybercriminels pour propager des ransomwares, et infecter les réseaux d'entreprises, dans le but d'extorquer de l'argent. Selon une récente étude de CyberEdge, 55 % des entreprises ont été victimes d'une attaque de ransomware en 2017. En outre, parmi celles qui ont décidé de payer la rançon pour récupérer leurs fichiers, plus de la moitié ont finalement perdu la totalité de leurs données. Les cartes sont donc très nettement dans les mains des maîtres-chanteurs, auxquels, les entreprises ne doivent jamais céder en payant une rançon, car il est très probable qu'une fois la somme encaissée, elles ne revoient toujours pas leurs données.

Par conséquent, que devraient faire les entreprises ? Quelles sont les règles à observer en cas d'attaque ?

Comprendre les motivations des maîtres-chanteurs

Lorsqu'une rançon est demandée, il s'agit généralement d'un montant par machine infectée, ou d'une somme totale, en échange d'une clé de décryptage des fichiers. Comme par exemple : 0,2 bitcoin pour chaque PC touché ou 2,5 bitcoins pour l'ensemble du parc infecté. Les maîtres-chanteurs espèrent donc que leur malware se répandra rapidement dans l'entreprise, afin de maximiser les gains.

C'est pourquoi il importe qu'une fois le PC d'un employé infecté, il faille disposer d'une procédure claire pour alerter rapidement l'équipe de sécurité compétente. Cette dernière décidera alors d'arrêter les systèmes informatiques connectés à la machine infectée. Bien entendu, si cette mesure limite les dégâts, elle paralyse tout de même l'entreprise, avec des postes à l'arrêt pour endiguer l'infection.

Sauvegardes

La mise en place d'un dispositif de sauvegarde efficace est l'une des règles d'or préconisées par les

experts en sécurité, pour se prémunir contre les attaques de type ransomware. Si une entreprise effectue des sauvegardes régulièrement, et ce, tout au long de la journée, les risques de perte de données seront limités au minimum. Attention toutefois, car certaines formes récentes et répandues de ransomwares, hautement élaborées, tels que SamSam, cherchent des informations sauvegardées en ligne et les effacent, afin de maximiser les chances de succès d'une attaque. C'est pourquoi, les entreprises doivent toujours réaliser des copies de sauvegarde physiques et virtuelles de leurs données, pour réduire les dommages en cas d'attaque.

Correctifs et mises à jour

C'est là sans doute l'aspect le plus critique, de tout programme de sécurité en vue de prévenir l'intrusion d'assaillants dans le réseau de l'entreprise. Et c'est d'autant plus vrai pour le ransomware. En effet, les experts en sécurité comme le FBI observent que, lorsqu'une nouvelle version d'un ransomware apparaît, la courbe des hackers l'exploitant grandit immédiatement, ceux-ci cherchant à profiter de logiciels non patchés sur les postes des utilisateurs le plus longtemps possible. Ce fût ainsi le cas avec le ransomware le plus désastreux et le plus médiatisé à ce jour, WannaCry, avec lequel les hackers ont profité de systèmes d'exploitation Windows obsolètes pour propager une infection à travers le monde entier.

La résilience est essentielle

Ainsi, il ne suffit pas pour les entreprises de disposer d'un plan de prévention des attaques. Dans les faits, les chances penchent plutôt en faveur des pirates qui, dans bien des cas, voient leurs intrusions couronnées de succès. Avoir une stratégie prenant en compte le déroulé des événements en cas d'attaque de ransomware, est essentielle pour la résilience de l'entreprise, en particulier dans des secteurs où les informations revêtent une importance critique, capitale, comme en médecine - où elles peuvent être littéralement vitales - dans le commerce, le transport ou la finance.

Pile ou face : telles sont les chances d'une entreprise ciblée par un ransomware. En conséquence, mieux vaut pour elles s'y préparer dès à présent et réduire au minimum un risque d'interruption d'activité et les coûts qui y sont liés, qui pourraient se chiffrer en millions. Anticiper les attaques rendra les entreprises bien plus résilientes et aptes à faire face au pire, le cas échéant.