Cyberprotect | Nouvelles vagues de rançongiciels : comportement, conseil, solution

Nouvelles vagues de rançongiciels : comportement, conseil, solution

---

Les actes de cybercriminalités se comptent en nombre et de façon récurrente. Beaucoup d'entreprises, d'administrations ou de commerces sont victimes de cyberattaques. Parmi ces attaques nous trouvons des logiciels malveillants comme les rançongiciels. Pour citer l'ANSSI, « c'est une technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de p

Ces rançongiciel sont de plus en plus présents en ce moment et se renouvellent. Actuellement les alertes portent sur le rançongiciel Locky qui se propage via un e-mail de relance qui contient une facture sous le format Word. Ce serait ce même logiciel qui aurait attaqué il y a quelques jours un centre hospitalier américain, perturbant et endommageant considérablement ses activités.
http://www.lefigaro.fr/secteur/high-tech/2016/02/16/32001-20160216ARTFIG00205-un-hopital-americain-paralyse-par-des-pirates-informatiques.php
http://www.lemonde.fr/pixels/article/2016/02/18/un-hopital-americain-paye-une-rancon-a-des-pirates-informatiques_4867296_4408996.html

Malheureusement ce type de logiciel malveillant n'est pas nouveau et s'inspire même de maliciels déjà connus comme le trojan bancaire Dridex. Plusieurs campagnes de prévention avaient été déployées suite à l'identification de ce maliciel par l'ANSSI notamment, mais également par Cyberprotect, service de contrôle et de prévention en continu de la cybersécurité en entreprise :
https://www.cyberprotect.fr/bulletin-dalerte-Cyberprotect-campagne-courriel-malveillant-trojan-bancaire-dridex/

La principale raison d'être et/ou motivation de ces cyberattaques est d'extorquer de l'argent à leur victime, comme ce fut le cas pour cet hôpital américain cité plus haut qui a dû s'acquitter de 17 000 dollars de rançon pour pouvoir rétablir son activité. Et ce n'est qu'une victime parmi d'autres. La propriété intellectuelle de l'entreprise est également visée par ce type d'attaque.

Se pose maintenant la question : comment se prémunir contre ces cyberattaques ?
Une première chose est de ne pas cliquer sur un lien ou d'ouvrir une pièce jointe dont on ne connait pas la provenance. Maintenir le système d'exploitation ainsi que les antivirus à jour est également une bonne pratique. Toutefois, avec le volume de données échangées, il est devenu plus difficile d'éviter ces attaques dont les techniques d'infection se font toujours plus subtiles et discrètes… [Lire la suite]

Réagissez à cet article

Source : *Cyberprotect | Nouvelles vagues de rançongiciels : comportement, conseil, solution*