Un ransomware paralyse un hôpital américain

	Un #ransomware paralyse un hôpital américain

La France n’est pas la seule à voir ses infrastructures infectées par les ransomwares. Aux États Unis, le Hollywood Medical Presbyterian Center a été victime d’une attaque similaire à celle relayée dans la presse au ministère des Transports en début d’année.

La France n’est pas la seule à voir ses infrastructures infectées par les ransomwares. Aux États Unis, le Hollywood Medical Presbyterian Center a été victime d’une attaque similaire à celle relayée dans la presse au ministère des Transports en début d’année.

Le système informatique de l’hôpital a été infecté par des cyberattaquants ayant recours à un malware de type ransomware (ou rançongiciel) : celui-ci chiffre les données contenues sur la machine et les rend inaccessibles à l’utilisateur, qui se voit contraint de verser une rançon afin d’espérer récupérer l’accès à ses fichiers. Sans système de sauvegarde fonctionnel, la situation peut rapidement devenir critique et cela semble être le cas de cet hôpital, dont les services administratifs se retrouvent paralysés depuis une semaine comme le relatent les médias locaux.

Si l’attaque n’a pas entièrement bloqué le traitement des patients, mais environ 900 nouveaux entrants ont été redirigés vers d’autres hôpitaux en attendant que le problème soit résolu.

L’attaque n’est, selon les déclarations du directeur de l’établissement, pas directement ciblée contre l’hôpital. Il s’agirait plutôt d’une attaque classique, issue d’un utilisateur peu précautionneux ou d’une politique de sécurité informatique défaillante.

Néanmoins, plusieurs sources expliquent que les cybercriminels exigent le versement de 9000 bitcoins afin de déchiffrer les données retenues par le malware.

Un plan sans accroc?

Et on avoue être un peu surpris : effectivement, les ransomwares sont une menace en pleine expansion et le ministère des Transports a récemment été victime d’une attaque de ce type. En revanche, le succès de ce nouveau type de menace tient à un modèle économique bien rodé. Les auteurs d’attaques par ransomware visent généralement un large panel de cibles et demandent des rançons relativement modérées, afin de s’assurer que les victimes pourront les payer.

9000 bitcoins, même pour un hôpital de grande taille, paraissent être une somme inhabituelle pour une demande de rançon. Cela ne représente pas moins de 3,6 millions de dollars. L’information n’a pas été confirmée par les sources officielles en charge du dossier ou par la communication de l’hôpital, prudence donc avant de tirer des conclusions hâtives. Gageons que si cette information venait à se vérifier, le FBI ne conseillera pas de simplement payer la rançon pour résoudre le problème.

Rançon extravagante ou non, les dégâts sont réels pour l’hôpital : le directeur explique ainsi que les formalités administratives et le renseignement des dossiers médicaux se fait maintenant à la main en attendant que le système informatique soit rétabli… [Lire la suite]

Réagissez à cet article

Source : *Quand un ransomware paralyse un hôpital américain*