Ransomware : trois cyber criminels sur quatre prêts à négocier la rançon

	Trois cyber criminels sur quatre prêts à négocier la rançon

Les auteurs de ransomware (logiciels rançonneurs) ne sont pas complètement fermés au dialogue.

Ces conclusions se basent sur une récente expérience détaillée dans le rapport F-Secure Evaluating the Customer Journey of Crypto-Ransomware and the Paradox Behind It (« Évaluation de l'expérience utilisateurs des victimes de logiciels rançonneurs, récit d'un paradoxe »). Cette étude a pour but d'évaluer « l'expérience utilisateur » de cinq logiciels rançonneurs actuels, dès lors que s'affiche le message réclamant la rançon. Elle retrace les différentes interactions ayant lieu avec les pirates.
Plusieurs conclusions émergent de ce rapport. Tout d'abord, les interfaces utilisateur de logiciels rançonneurs les plus professionnelles ne sont pas nécessairement celles qui offrent le « suivi » le plus adapté.
Les pirates utilisant ransomware sont souvent disposés à négocier le prix de la rançon. Pour trois des quatre logiciels rançonneurs, ils se sont montrés prêts à négocier : la rançon a été revue à la baisse, de 29% en moyenne. Les dates limites, quant à elles, ne sont pas nécessairement gravées dans le marbre. 100% des groupes contactés ont accordé un report de la date limite. L'un des groupes a déclaré qu'une entreprise avait fait appel à lui pour hacker une autre entreprise.
Le rapport souligne également le paradoxe des logiciels rançonneurs : « *D'un côté, les auteurs sont des criminels sans scrupules, mais de l'autre, ils doivent établir un degré relatif de confiance avec la victime et être prêts à offrir certains niveaux de « services » pour que cette dernière effectue finalement le paiement* ». Les groupes utilisant des ransomware fonctionnent sur le modèle des entreprises : ils possèdent un site internet, une FAQ (Frequently Asked Questions – Foire aux questions), des « essais gratuits » pour le déchiffrement de fichiers et même un chat d'assistance.
« *Nous lisons chaque jour des histoires au sujet de logiciels rançonneurs… Dernièrement, le mot 'épidémie' a été employé pour faire état de l'ampleur des attaques* », explique Sean Sullivan, Security Advisor chez F-Secure. « *Nous avons voulu proposer une approche différente face à ces attaques en masse, et également rappeler aux particuliers et aux entreprises ce qu'il est possible de faire pour se protéger de ce type de menaces. Avant même d'être victime d'une attaque, il faut adopter plusieurs réflexes-clés : la mise à jour des logiciels, l'utilisation d'un bon logiciel de cyber protection, la vigilance face aux e-mails suspects et surtout, des sauvegardes régulières* ».
Article original de itrmanager

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Ransomware : trois cyber criminels sur quatre prêts à négocier la rançon