Devolutions

La multiplication des rançongiciels : La situation actuelle et comment protéger votre entreprise

LE TITRE DE LA BÊTE LA PLUS EFFRAYANTE DU PAYSAGE DES CYBERMENACES REVIENT DÉSORMAIS AUX RANÇONGICIELS

Ce n'est pas un logiciel malveillant. Ce n'est pas un logiciel espion. Ce ne sont pas non plus des chevaux de Troie. Il ne s'agit même pas d'une attaque par déni de service distribué (de l'anglais distributed denial of service ou DDoS). Non, selon les experts, le titre de la bête la plus effrayante du paysage des cybermenaces revient désormais aux rançongiciels.

Qu'est-ce qu'un rançongiciel?

Un rançongiciel est un type de logiciel que les pirates utilisent pour entraver l'accès des victimes à leurs propres données. Si les victimes ne se plient pas aux exigences financières dans un délai déterminé, leurs données seront définitivement supprimées (c'est du moins la menace qui fait froid dans le dos). Dans certains cas, les pirates menacent également d'exploiter et de divulguer les informations personnelles de la victime sur le Web profond.

La somme d'argent exigée par les pirates fluctue. Fait intéressant, certains pirates semblent avoir un sens basique de l'économie, puisqu'ils insistent pour obtenir des paiements moins importants de la part des particuliers que des entreprises. Cette démarche n'est pas guidée par un sentiment d'empathie. Elle est motivée par l'aspect pratique. Les pirates sont conscients que les entreprises ont de plus grandes poches. De ce fait, une victime individuelle peut être contrainte à payer quelques centaines de dollars (par le biais d'une cryptomonnaie comme le Bitcoin qui ne peut être tracée), alors qu'une organisation peut être amenée à verser des dizaines, voire des centaines de milliers de dollars.

Des recherches récentes ont démontré que la rançon moyenne payée a progressé jusqu'à 170 704 dollars par incident (tous les chiffres sont en dollars américains). Pour couronner le tout, seulement 8 % des victimes qui paient une rançon récupèrent 100 % de leurs données. Dans ce cas, pourquoi les victimes devraient-elles se plier aux exigences des pirates? Simplement en raison du fait que le prix de la restauration d'une attaque par rançongiciel - y compris les enquêtes, les interruptions de service, les commandes perdues, les coûts opérationnels et d'autres facteurs - a explosé, passant de 761 106 dollars en 2020 à 1,85 million de dollars en 2021. En fait, la plupart des victimes « font le calcul » et estiment qu'il est financièrement intéressant de payer moins aux pirates et de récupérer une partie ou la totalité de leurs données plutôt que de payer davantage en frais de remédiation et ne rien obtenir.

Comment fonctionne un rançongiciel

Bien que les pirates soient de plus en plus sophistiqués, les principes de base des rançongiciels sont assez simples : une fois que le logiciel malveillant est téléchargé sur un terminal ou un réseau, il chiffre les données et ajoute une extension aux fichiers, ce qui les rend inaccessibles. Les pirates ont recours à plusieurs méthodes pour déployer les rançongiciels, à savoir :

- Intégrés dans des macros (par exemple, des fichiers Word)
- Pièces jointes de courriers électroniques non sollicités
- Ingénierie sociale
- Placement de publicité malveillante

- Lecteurs USB amovibles
- Messages lors d'un clavardage
- Vulnérabilités des modules d'extension du navigateur (de l'anglais drive-by attacks).

Statistiques sur les rançongiciels

Nous avons présenté auparavant des statistiques alarmantes sur les rançongiciels. Hélas, avec l'aide de PurpleSec, de nouveaux chiffres effrayants s'ajoutent à la discussion :

- En 2021, une entreprise est victime d'une attaque par rançongiciel une fois toutes les 11 secondes.
- Les coûts mondiaux des rançongiciels devraient atteindre 20 milliards de dollars d'ici la fin de 2021.
- 20 % des victimes de rançongiciel sont des PME.
- 85 % des MSP estiment que les rançongiciels constituent une menace courante pour les PME.
- 50 % des professionnels de la sécurité de l'information sondés ne considèrent pas que leur entreprise est prête à faire face à une attaque par rançongiciel.
- Types de rançongiciels plus répandus : CryptoLocker (66 %), WannaCry (49 %), CryptoWall (34 %), Locky (24 %), Petya (17 %), CryptXXX (14 %), notPetya (12 %).
- Systèmes d'exploitation les plus couramment visés par les rançongiciels : Windows (85%), macOS (7%), Android (5%), iOS (3%)

Attaques notables

Vous trouverez ci-dessous quelques-unes des plus importantes attaques de rançongiciels ainsi que les rançons correspondantes en 2020 et 2021 :

- ACER (50 millions de dollars)
- JBS Foods (11 millions de dollars)
- CWT Global(4,5 millions de dollars)
- Colonial Pipeline (4,4 millions de dollars)
- Brentagg (4,4 millions de dollars)
- L'Université de Californie à San Francisco (1,14 million de dollars)

Et tout récemment, le 2 juillet 2021, des pirates ont attaqué Kaseya IT et ont exigé que l'entreprise de logiciels de gestion verse la somme faramineuse de 70 millions de dollars, sans quoi les données de l'entreprise, ainsi que celles de centaines de ses clients, seront effacées ou diffusées sur le Web profond.

Comment protéger votre entreprise

Il est impossible d'éliminer à 100 % le risque d'une attaque par rançongiciel. Tant qu'il y aura de l'informatique, il y aura des pirates.

Toutefois, il existe des méthodes efficaces que les entreprises devraient - ou franchement, compte tenu des conséquences potentielles, elles doivent - adopter pour réduire leur exposition et leur vulnérabilité. Le Center for Internet Security (CIS) recommande 15 actions :

1- Développez un plan complet de réponse aux incidents, qui identifie clairement ce qu'il faut faire - et qui doit le faire - en cas d'attaque par rançongiciel.

2- Mettez en place un système de sauvegarde qui prend en charge plusieurs itérations ou données archivées dans le cas où une copie de la sauvegarde contiendrait des fichiers infectés ou chiffrés. Les sauvegardes doivent de plus être régulièrement vérifiées pour s'assurer de l'intégrité des données et de la disponibilité opérationnelle.

3- Déployez des logiciels antivirus et antipourriel, et ajoutez une bannière/signature d'avertissement sur tous les courriels qui rappelle aux utilisateurs les dangers de cliquer sur les liens et d'ouvrir les pièces jointes.

4- Si cela est possible, désactivez les macros de script et exigez des utilisateurs qu'ils affichent les fichiers transmis par courrier électronique plutôt que de les ouvrir. L'intégration de logiciels malveillants dans des macros Word/Excel est un vecteur courant d'attaques par rançongiciel.

5- Maintenez tous les appareils, logiciels, matériels et applications (y compris les environnements infonuagiques) à jour et corrigés, de préférence par le biais d'un système centralisé de gestion des correctifs.

6- Utilisez la liste blanche des applications et les politiques de restriction des logiciels pour empêcher l'exécution des programmes dans les emplacements courants des rançongiciels (par exemple, les dossiers temporaires).

7- Utilisez un serveur proxy pour l'accès à Internet.

8- Utilisez un logiciel de blocage des publicités.

9- Limitez l'accès aux vecteurs courants de rançongiciels, notamment les sites de réseaux sociaux et les comptes de messagerie personnels.

10- Appliquer le principe du moindre privilège (POLP).

11- Mettre en place une segmentation du réseau ainsi qu'une architecture « zéro confiance ».

12- Évaluer et surveiller les tiers ayant accès au réseau, et s'assurer qu'ils appliquent avec diligence les meilleures pratiques en matière de cybersécurité.

13- Participer à des programmes et organisations de partage d'informations sur la cybersécurité (par exemple, MS-ISAC et InfraGard).

14- Fournir aux utilisateurs finaux une formation continue en cybersécurité sur des sujets comme l'ingénierie sociale et l'hameçonnage.

15- Mettez sur pied un plan de signalement qui indique aux utilisateurs finaux comment et quand signaler toute activité insolite ou suspecte.

Faire face à une attaque

Le CIS donne également quelques conseils sur la façon de réagir dans le cas d'une attaque par rançongiciel :

- Déconnectez immédiatement le système infecté du réseau.
- Déterminez si les données affectées nécessitent des mesures d'atténuation ou des exigences de déclaration supplémentaires (par exemple, les informations des dossiers de santé électroniques protégées).
- Voyez si un décrypteur tel que No More Ransom ! peut vous aider.
- Restaurez les fichiers au moyen de sauvegardes effectuées régulièrement.
- Signalez l'attaque à l'autorité compétente en fonction du pays et de la juridiction. Les entreprises américaines doivent communiquer avec le MS-ISAC, le FBI ou l'Internet Crime Complaint Center (IC3).

Le mot de la fin

Les entreprises (notamment les PME) ne peuvent pas se contenter d'une attitude passive et attentiste lorsqu'il est question de se protéger contre les rançongiciels, car les coûts et les conséquences d'une attaque peuvent être catastrophiques. Elles doivent être proactives et renforcer leur profil de cybersécurité maintenant. En adoptant toutes les recommandations énumérées ci-dessus, les entreprises contribueront considérablement à éviter d'être victimes de rançongiciel et d'autres cybermenaces.