Protection contre le rançongiciel WannaCry, une « arme de destruction massive »

Incroyable. Sans précédent. Une arme de destruction massive. C'est ainsi que les experts de la cybersécurité décrivent WannaCry, le rançongiciel qui a déferlé sur des entreprises dans le monde entier. Jusqu'à présent, des centaines de milliers d'ordinateurs dans 150 pays ont été paralysés, depuis des systèmes de santé britanniques à des universités à travers l'Asie. Et la menace n'a pas été circonscrite. De nouvelles variantes de WannaCry sont maintenant détectées, des variantes pour lesquelles il n'existe pas de processus semblable à celui qui a permis d'atténuer les dégâts commis par l'original.

Comment se protéger de la menace WannaCry ?

Résoudre immédiatement la vulnérabilité de Windows

Des acteurs malveillants ont exploité la faille connue de Microsoft, EternalBlue, soulignant l'importance d'installer immédiatement des patchs de sécurité et de mettre à jour les logiciels et systèmes d'exploitation pris en charge.

Ainsi, nous recommandons que les entreprises :

- Continuent à installer les nouveaux patchs de sécurité
- Installent un patch sur les appliances UDP et serveurs RPS Arcserve
- Installent rapidement la mise à jour de sécurité MS17-010 de Microsoft sur leurs systèmes
- Bloquent les anciens protocoles, comme SMBv1, pour se protéger des versions mutantes du logiciel malveillant
- Fassent une mise à jour pour installer une version du système d'exploitation Microsoft prise en charge

Ne pas payer la rançon

Dans le cas de WannaCry, les pirates doivent procéder à un déchiffrement manuel. Étant donnée la recherche intense des personnes responsables, il est fort possible que les rançons versées restent intactes sur les adresses Bitcoin et que les demandes de déchiffrement demeurent sans réponse.

Cela dit, il est possible que les fichiers enregistrés en dehors du Bureau, des Documents ou sur un support amovible puissent être récupérés grâce à l'outil de réparation.

Évaluer sa stratégie de sauvegarde et de reprise d'activité

WannaCry a fait ressortir clairement la nécessité critique de trouver des remèdes aux rançongiciels. Par conséquent, nous recommandons que toutes les entreprises prennent immédiatement des mesures pour s'assurer qu'elles disposent des outils pour procéder à la sauvegarde et à la récupération de leurs données.

- **Étudier le RTO (temps de restauration) et le RPO (point de restauration).** S'assurer que les systèmes critiques sont sauvegardés le plus souvent possible et que la récupération des données correspond aux exigences de l'entreprise.
- **Confirmer la sauvegarde de toutes les sources de données.** Identifier les serveurs ou sources de données qui ne sont pas inclus au plan de protection des données et appliquer le niveau correct de disponibilité des données pour veiller à leur récupération.

- **Accéder au serveur de sauvegarde en tant qu'utilisateur.** Lors de la connexion au serveur sécurisé, s'assurer de se connecter en tant qu'utilisateur et pas en tant qu'administrateur. Ne jamais utiliser un compte d'administrateur pour ouvrir un courriel ou faire des recherches sur le Web.
- **Protéger le protecteur.** S'assurer que les fichiers de sauvegarde sont stockés sur un serveur sécurisé, dont l'accès est limité exclusivement aux utilisateurs qui en ont absolument besoin. Ces fichiers représentent la meilleure chance de réparation. Il faut donc veiller à leur sécurité.
- **La règle 3-2-1.** Enregistrer au moins trois copies différentes des données sur deux supports différents, avec au moins une copie hors site. Il est critique que la stratégie de sauvegarde intègre des redondances et s'appuie sur des options de stockage qui ne sont pas vulnérables aux attaques, comme les bandes, les disques hors ligne et le Cloud.
- **Pratiquer le principe du moindre privilège.** Lors de la configuration des comptes, accorder uniquement le degré de privilèges d'accès strictement nécessaire à chaque rôle.

Récupération réelle après un rançongiciel

« La dernière attaque par un rançongiciel a été incroyablement virulente. Elle a touché 45 serveurs différents, se propageant de manière effrénée. Pour tout dire, les directeurs se sont même installés dans mon bureau pendant un certain temps. »

Avec Arcserve UDP, l'administrateur du réseau informatique a pu récupérer rapidement la sauvegarde de la veille, évitant ainsi une rançon de 30 000 dollars.

Contourner les demandes de rançon avec Arcserve Unified Data Protection

Plus de 48 000 clients dans 150 pays font confiance à Arcserve UDP, solution récompensée, qui procure aux petites équipes IT surchargées les fonctionnalités professionnelles et la facilité dont elles ont besoin.

- Déployez Arcserve sans effort sous la forme d'un logiciel, d'une appliance ou d'une solution sur le Cloud
- Protégez les données physiques et virtuelles, où qu'elles se trouvent : sur site, hors site, hors ligne et sur le Cloud
- Identifiez facilement le RTO (temps de restauration) et le RPO (point de restauration), configurez des tests automatiques et identifiez les machines qui ne sont pas protégées avec les fonctionnalités de restauration garantie (« Assured Recovery »)
- Faites évoluer les fonctions de sauvegarde et de récupération au fur et à mesure de la croissance de l'entreprise, de 1 To à 1Po et au-delà
- Récupérez instantanément les applications critiques avec une solution virtuelle ou Instant Virtual Machine
- Récupérez les données à partir de sauvegardes sur fichiers ou en images ou grâce à des solutions disponibles en permanence

Et tout cela, à partir d'une seule console de gestion, d'une élégante simplicité

Veillez à votre protection

Contactez votre représentant Arcserve ou appelez le + 33 1 82 88 57 87 pour démarrer dès aujourd'hui

Pour plus d'informations à propos d'Arcserve, veuillez consulter le site **arcserve.com**