

# Ransomware : une menace sans fin ?

Tous les experts s'accordent pour dire que les cybermenaces se sont intensifiées ces derniers mois, avec des demandes de rançons sont de plus en plus nombreuses et des tactiques que l'on pourrait qualifier d'impitoyables.

Personne n'est épargné, des organisations publiques comme les villes de Vincennes et d'Aulnoye-Aymeries il y a quelques semaines aux plus grandes entreprises privées comme [Bouygues Construction](#), CMA-CMG ou encore [Sopra-Steria](#).

Les cybercriminels parviennent en effet à trouver de nouveaux moyens de contourner les défenses des entreprises, grâce à des attaques plus sophistiquées et ciblées. Se défendre contre cette menace en constante évolution n'est certes pas une mince affaire, mais un bon point de départ consiste à comprendre où se situent les points faibles et comment ils sont exploités.

## L'humain reste le maillon faible de la cybersécurité

Il suffit d'un clic sur un lien de phishing pour que le travail soit fait : les défenses du réseau sont violées et le malware est infiltré.

Renforcer ses défenses contre la négligence humaine nécessite non seulement une formation des collaborateurs à la sensibilisation en matière de cybersécurité mais aussi la mise en place d'outils permettant de filtrer les contenus malveillants avant qu'ils ne puissent causer des dommages. Toutefois, la cybersécurité n'étant pas une science exacte, même les plans les mieux conçus doivent être revus et adaptés en permanence pour ne pas se laisser dépasser par le rythme

fou de l'évolution des cybermenaces.

Prenons par exemple, l'augmentation massive du [télétravail](#) pendant la pandémie.

Cette nouvelle « norme » offre aux pirates informatiques un public tout nouveau et une cible facile, peu habituée à se protéger des menaces. Selon le fournisseur de sécurité Kaspersky, ces nouvelles habitudes de travail ont conduit à une montée en flèche des attaques RDP (Remote Desktop Protocol) de Microsoft à l'échelle mondiale.

## **Des cybercriminels bien renseignés**

Les cybercriminels ont tout à fait conscience que chaque secteur d'activité présente des vulnérabilités spécifiques. Ils exploitent ces vulnérabilités en abandonnant les campagnes massives de phishing au profit d'attaques plus ciblées. Certaines, par exemple, se concentrent sur des entreprises individuelles, généralement de grande renommée car elles ont souvent beaucoup à perdre, tandis que d'autres ciblent un secteur spécifique en utilisant des logiciels malveillants adaptés aux technologies utilisées par ce secteur en particulier.

Dans certains cas, ils utilisent les deux, comme lors de la récente attaque de Honda. Le piège dans ce cas était une variante du ransomware Snake, capable à la fois de désactiver les mesures de sauvegarde et de cibler les systèmes de contrôle industriel SCADA utilisés dans la fabrication de véhicules.

Les attaques de ransomware sont en passe de devenir un « business » de plus en plus diversifié. Les victimes sont maintenant menacées de voir leurs données sensibles recueillies lors d'une attaque de chiffrement. Il est également de plus en plus évident que les ransomwares ciblent régulièrement les systèmes de sauvegarde et de récupération après sinistre, ainsi que les données en temps réel. Du moins,

en apparence, car vérifier l'intégrité de ces moyens de défense prend du temps...

## **Suivre le rythme des ransomwares**

Que peut faire une entreprise pour se protéger contre ce qui devient aujourd'hui l'une des principales menaces pour son système informatique ? Il n'existe pas de réponse toute faite ni d'outils simple qui puisse résoudre le problème.

Plus qu'une solution miracle, c'est plutôt une approche méthodologique qu'il faut privilégier : sensibiliser et former davantage les utilisateurs finaux à la sécurité, mettre à jour les outils anti-programmes malveillants sur les postes de travail et l'infrastructure, et s'assurer que les stratégies et les outils de sauvegarde sont suffisamment robustes pour contrer les menaces de ransomware et permettre un retour à la « normale » rapide.

Toutes ces mesures méritent d'être examinées, mais, en tant que dernière ligne de défense, c'est la sauvegarde qui est la plus importante. D'autant plus que l'utilisation des appliances NAS (Network Attached Storage) pour la sauvegarde et l'archivage est très répandue et que, de par leur nature même, elles constituent une cible facile. C'est la partie « réseau » qui met le plus en danger les appareils NAS, les rendant faciles à identifier et, une fois trouvées, faciles à attaquer. Souvent sans que personne ne le sache, jusqu'à ce que les demandes de rançon arrivent dans la boîte de réception.

La première approche consiste à verrouiller le réseau auquel les appareils NAS sont connectés tout en s'assurant que le micrologiciel du NAS est à jour avec tous les derniers correctifs de sécurité. Au-delà, il est intéressant de tirer parti de la double authentification, lorsqu'elle est disponible, et du protocole SSL pour mieux sécuriser l'accès à distance, le cas échéant.

Autres bonnes pratiques : le blocage automatique des adresses IP à la suite d'échecs répétés d'attaques de connexion par « force brute », ainsi que l'utilisation du chiffrement des données et de pare-feu spécifiques au NAS.

En matière de cybersécurité, mieux vaut redoubler de précautions. C'est-à-dire effectuer des sauvegardes fréquentes et régulières du stockage NAS ET stocker ces copies à distance (de préférence hors site) et sans connexion au réseau. C'est la seule façon de s'assurer qu'il existe une version propre et restaurable des données qui ne soit pas obsolète.

Sans oublier, cependant, que cela doit être combiné avec des contrôles d'intégrité réguliers et des analyses de logiciels malveillants pour s'assurer que les données copiées n'ont pas déjà été compromises.

La menace du ransomware cessera-t-elle un jour de planer ? Possible, mais sûrement pour faire place à une menace au moins tout aussi grande. C'est pour cette raison que de nombreuses entreprises cherchent à la désamorcer au niveau du stockage des données, avec les capacités de stockage objets, de versioning, la technologie WORM (Write Once Read Many) et les systèmes de fichiers immuables.

Gartner prévoit que d'ici 2021, environ 80 % des données d'entreprise seront stockées en mode scale-out, contre 30 % aujourd'hui. La fin du ransomware n'étant a priori pas pour demain, il semblerait bien que ce soit ces technologies liées au stockage des données qui permettent de désarmer ce type d'attaque, et de voir un peu de lumière au bout du tunnel !