Veille Techno : Cyberattaques – Cheval de Troie ResolverRAT

ResolverRAT est un cheval de Troie à distance détecté par Morphisec Threat Labs. Il se propage principalement via des mails de phishing déguisés en notifications légales ou de violations de droits d'auteur, incitant les employés à cliquer sur des liens malveillants. Une fois installé, le malware s'intègre discrètement dans les systèmes Windows, se copiant dans des dossiers clés tels que « Program Files » ou « LocalAppData ». Il exfiltre ensuite les données sensibles en fragmentant les fichiers de plus de 1 Mo en petits morceaux de 16 Ko, rendant ainsi le trafic difficile à détecter.

Cette campagne de cyberattaques vise spécifiquement les entreprises du secteur de la santé et de la pharmacie à l'échelle mondiale. Les chercheurs ont observé des mails de phishing en plusieurs langues, dont l'italien, le tchèque, l'hindi, le turc et le portugais, indiquant une opération coordonnée à portée internationale.

Cette attaque souligne la nécessité pour les organisations du secteur santé/pharma de renforcer leurs défenses. Concrètement, cela passe par la formation du personnel contre le phishing, l'installation de filtres anti-phishing et d'outils de détection avancée (EDR), l'application du principe du moindre privilège pour limiter les accès, la mise en place de sauvegardes sécurisées et testées, ainsi que l'usage de l'authentification multifacteur (MFA). Ces mesures permettent de réduire fortement les risques d'intrusion et de protéger la confidentialité des données médicales.

Sources :

https://www.01net.com/actualites/cyberattaque-mondiale-virus-resolverrat-prend-assaut-secteur-sante-pharmacie.html

https://www.generation-nt.com/actualites/cyberattaque-sante-pharmacie-virus-malware-resolverrat-2057162