Vonnas Multimédia Services
8 Place des Marronniers 01540 Vonnas
04.74.50.24.83
contact@vmsvonnas.fr
www.vmsvonnas.fr

La sauvegarde de données externalisée, seule protection efficace contre les attaques au Ransomware et cryptolocker

54 %, voici le pourcentage d'entreprises françaises attaquées en 2021, **+255 % d'attaques par ransomwares** pour un cout médian s'élevant à 50 000€. Les auteurs de ces méfaits ont amélioré leur ciblage. Ils ne cherchent plus à toucher des grosses structures avec de fortes rançons à la clé, mais préfèrent multiplier les attaques vers des cibles plus petites et plus fragiles : les PME et TPE.

Les caractéristiques de ce malware sont :

- Pour initier l'attaque, un fichier ou un lien vérolé est envoyé sous la forme d'un **email.** À noter que les **clés USB ou disques durs externes** peuvent aussi véhiculer ce virus**.** Si le fichier vérolé est ouvert, le programme s'installe sur l'ordinateur et **crypte alors toutes les données, rendant impossible l'utilisation ou la consultation de ces fichiers.**

- Dès lors, **le cybercriminel débute** son chantage en demandant de **verser une rançon**. D'une valeur moyenne comprise entre 1000 et 4000€ au départ (en fonction du nombre de postes infectés), ce montant va doubler chaque jour et peut rapidement atteindre des sommes folles**.**

- **Les serveurs Windows** sont la cible préférée des pirates

- **Il n'y a pas de solution de protection 100% efficace.** Une machine protégée par un antivirus récent et à jour peut quand même être infectée par cette attaque.

- **Attention,** un cryptolocker crypte également les lecteurs réseau mais aussi **les sauvegardes classiques sur disque dur externe ou NAS, rendant alors impossible la restauration.**

Point important : Une fois l'attaque déclenchée il est alors quasiment impossible de décrypter les fichiers par ses propres moyens, et hormis le paiement de la rançon avec un résultat aléatoire, **seule la solution de restauration complète du système et des données reste efficace.**

Mise en garde, comment se prémunir ?

➢ **Mettre à jour les logiciels installés sur ses machines et serveurs :** navigateur(s), outils Adobe, java, système d'exploitation, antivirus…

➢ **Ne pas ouvrir des fichiers attachés**, en particulier des fichiers .doc ou .zip, provenant d'une **source inconnue**

➢ Être équipé d'un logiciel antivirus performant, même si la protection n'est pas **fiable à 100%**

➢ **Sauvegarder ses données.** La préconisation des experts en informatique est de réaliser une sauvegarde de ses données **quotidiennement** (à minima) et d'effectuer régulièrement des **tests de restauration.**

Consciente des enjeux, l'entreprise VMS s'est rapprochée d'un acteur majeur de la sauvegarde externalisée, la société Beemo. Contrairement aux autres solutions de sauvegarde, les solutions Beemo sont parfaitement hermétiques aux attaques en raison de l'invisibilité de leurs boîtiers sur le réseau.

C'est pour toutes ces raisons que Vonnas Multimédia Services vous informe qu'elle ne pourra vous garantir techniquement la récupération de vos données que si vous avez mis en place une solution Beemo pour la gestion de vos sauvegardes. Dans le cas contraire, nous ne pouvons pas vous assurer la restauration de vos fichiers en cas d'attaque de ce type.

Nous insistons sur le fait que seule la mise en place d'une politique préventive efficace de sauvegarde de vos données permet de contrer efficacement ce type de virus. Nos équipes restent bien entendu à votre disposition pour toute demande d'information complémentaire.

N'hésitez pas à nous contacter **pour demander une étude gratuite.**

Vous remerciant pour votre vigilance.

Cordialement,

Toute l'équipe Vonnas Multimédia Services