Alerte VIRUS « Windigo »

	Alerte Virus « Windigo » sur des serveurs Internet

Après des mois d'enquête, les experts en sécurité d'ESET viennent de découvrir **une vaste campagne d'attaques cybercriminelles touchant 25 000 serveurs UNIX**, infectant plus de 500 000 ordinateurs chaque jour et ayant généré plus de**35 millions de spams**.

Surnommée « **Windigo** », cette opération cybercriminelle de grande ampleur vise essentiellement les Etats-Unis, l'Allemagne, le Royaume-Uni et la France. Les serveurs à faible niveau de protection (absence d'antivirus ou d'authentification forte) sont principalement visés.

Nous vous recommandons la plus grande vigilance et vous invitons dès maintenant à procéder à une **vérification de l'intégrité de vos serveurs** en éxécutant **la ligne de commande suivante (sur une seule ligne) :**

ssh -G 2>&1 | grep -e illegal -e unknown > /dev/null && echo « System clean » || echo « System infected »

Dans le cas où vos serveurs sont intacts, nous vous recommandons fortement de **considérer la mise en place d'une solution d'authentification forte** afin de protéger vos identifiants administrateur et clés privées.

Dans le cas où votre serveur est infecté, la sécurité de vos

accès et de vos données doit être considérée comme compromise. C'est pourquoi nous vous recommandons de procéder à un formatage et une réinstallation système.

source : WeLiveSecurity.com

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Alerte VIRUS – Recrudescence d'attaques du ransomware Cryptolocker

	Alerte niveau 1 – Recrudescence d'attaques du ransomware Cryptolocker

Alerte niveau 1 – Recrudescence d'attaques du ransomware Cryptolocker

Les caractéristiques de ce malware

- Le plus souvent sous la forme d'un e-mail contenant une pièce jointe malveillante.
- Si la pièce jointe est ouverte, le programme s'installe sur l'ordinateur et chiffre les données.
- Dès lors, le cybercriminel débute son chantage en demandant de verser une rançon.

- D’une valeur moyenne de 700€, elle peut atteindre 4000€ lorsque l’attaque cible un serveur.
- Les serveurs sont la cible préférée des pirates
- Le pirate tente de pénétrer la machine via des accès externes, ouvert sur internet
- Les mots de passe faibles sont facilement découverts par attaques dites « brut force par dictionnaire »
- Le pirate peut ensuite prendre la main sur le serveur, désactiver l’antivirus, et lancer le chiffrement de tous les fichiers de données
- Attention CryptoLocker chiffre également les sauvegardes et lecteurs réseau

Mise en garde, comment se prémunir ?

Voici un rappel des bonnes pratiques élémentaires

- Etre équipé d’un logiciel antivirus performant. ESET permet d’avertir l’utilisateur du danger. Malgré le message d’avertissement, l’utilisateur peut décider d’exécuter le fichier infecté. Il faut donc prendre en compte les messages des antivirus
- Sauvegarder ses données. Le guide édité par l’ANSSI va au-delà de la simple sauvegarde de fichiers et préconise la mise en place de Plan de Reprise d’Activité
- Mettre à jour les logiciels installés sur ses machines et serveurs : navigateur(s), outils Adobe, java, système d’exploitation, antivirus
- Bloquer les fichiers exécutables. Une protection en amont, par exemple sur serveur de messagerie ou passerelle. exemple : ESET Mail Security Exchange
- Répliquer ses sauvegardes locales sur un support externe.
- Appliquer des politiques de restrictions logicielles (PRS). Afin d’empêcher des programmes comme CryptoLocker de s’exécuter dans des répertoires tels que « %AppData% » ou « %LocalAppData% ». (règle qui peut être mise en place via le HIPS d’ESET)

- Utiliser les objets de stratégie de groupe (GPO) pour créer et restreindre les autorisations sur les clés de registre utilisées par CryptoLocker, comme HKCU \ SOFTWARE \ CryptoLocker (et variantes). Si le malware ne peut pas ouvrir et écrire dans ces clés de registre, il sera incapable de chiffrer les fichiers
- Restreindre les autorisations sur les lecteurs réseau partagés pour empêcher les utilisateurs de modifier des fichiers
- Eviter d'utiliser les ports par défaut. Exemple : faille sur le port TSE TCP 3389 (Windows Terminal server)
- Utiliser des mots de passe forts, et mettre en œuvre une authentification multi-facteurs. Outil conseillé : ESET Secure Authentication

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)