


Alerte VIRUS « Windigo »

 <p>OPERATION WINDIGO</p> <p>25,000 UNIX servers in total affected 500,000 computers attacked daily</p> <p>eset ENJOY SAFER TECHNOLOGY™</p>	<p>Alerte Virus « Windigo » sur des serveurs Internet</p>
--	---

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 exécutant **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)