Instagram détourné pour espionner des membres de gouvernements

	Instagram détourné pour espionner des membres de gouvernements

Turla, le groupe de cyberespionnage qui cible des représentants de gouvernements et des diplomates, lance une nouvelle attaque en se servant d'Instagram®. En février 2017, Forcepoint® a publié une liste de sites Internet récemment compromis.

Les cybercriminels utilisent **la technique d'attaque de trou d'eau**, qui vise à rediriger les victimes ayant cliqué sur un site compromis vers leurs serveurs C&C. Les chercheurs ESET® ont repéré **une extension de Firefox® qui utilise une URL bit.ly pour renvoyer vers les serveurs C&C. Le chemin de l'URL est diffusé via des commentaires d'une publication Instagram.** Dans l'échantillon analysé par ESET, l'un des commentaires s'affiche sur une photo du compte officiel de Britney Spears.

© https://www.instagram.com/p/BO8gU41A45g/

Pour obtenir l'URL bit.ly, l'extension scrute les commentaires de chaque photo et pour chaque commentaire en calcule un hash. Si la valeur de hash correspond à un code de déclenchement, l'extension exécute une opération pour convertir le commentaire en URL.

« L'utilisation par Turla des réseaux sociaux pour récupérer les adresses C&C ne facilite pas la tâche aux chercheurs en cybersécurité. Il est difficile de distinguer le trafic malveillant du trafic légitime sur les réseaux sociaux, » explique Jean-Ian Boutin, Senior Malware Researcher chez ESET. Par ailleurs, c**ette technique offre plus de souplesse aux pirates :** « comme l'information nécessaire pour obtenir l'URL du serveur C&C n'est autre qu'un commentaire sur les réseaux sociaux, **le cybercriminel a la possibilité de le modifier ou de l'effacer** à tout moment, » poursuit Jean-Ian Boutin.

Pour éviter d'être infecté par une attaque de trou d'eau de ce type, les chercheurs ESET recommandent de :

• mettre à jour les navigateurs et les plugins des navigateurs
• éviter de télécharger ou d'installer des extensions venant de sources non vérifiées
• utiliser une solution de sécurité (à jour) capable de détecter les sites Internet compromis

Seuls 17 clics ont été enregistrés sur ce lien en février lorsque le commentaire a été posté. Le nombre étant relativement faible, ESET suppose qu'il s'agit d'un test pour une attaque de plus grande envergure.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *ESET*