

Des noms de domaines détournés pour mieux vous infecter



Efficacité et transparence chez le registrar Gandi. L'entreprise, via un partenaire, a du faire face au détournement de 751 noms de domaines. Mission de ce hijacking, diffuser des codes malveillants par l'intermédiaire des noms de domaine ainsi pris en main par le pirate.

Vendredi 7 juillet, un incident de type hijacking est survenu chez un partenaire technique du fournisseur de noms de domaine Gandi. Un partenaire qui gère 31 extensions. Suite à une connexion non autorisée chez ce partenaire, l'attaquant a utilisé des identifiants Gandi pour se connecter à cette interface. Le pirate informatique a pu détourner 751 noms de domaines et renvoyé les visiteurs sur un espace numérique, basé au Gabon, ayant pour mission de lancer des tentatives d'infiltration dans les ordinateurs des visiteurs. Le but étant de lancer des exploits via des navigateurs web (IE, Chrome, Firefox, ...) non mis à jour. Le pirate a utilisé Rig Exploit Kit et Neutrino Bot lors de son opération...[lire la suite]

Commentaire de Denis JACOPINI :


Mélange probablement de phishing (pour obtenir les identifiants du prestataire), d'attaque en point d'eau (qui consiste à prendre le contrôle et de piéger un espace de confiance à fort trafic) et d'attaque par exploitation de faille (le code malveillant permettra d'infiltrer les navigateurs qui n'ont pas été mis à jour). Malheureusement un grand classique très répandu dans les structures où le personnel n'est pas sensibilisé.

Suivez nos
formation <https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles/>

Notre métier : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec le RGPD (règlement Européen relatif 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 : *ZATAZ Hijacking : 751 noms de domaines détournés chez Gandi – ZATAZ*