Alerte : Des routeurs domestiques attaqués par malvertising via DNSChanger

Alerte : Des routeurs domestiques attaqués par malvertising via DNSChanger

Des routeurs domestiques font l'objet d'une attaque par le biais d'une campagne de publicités malveillantes et via le navigateur Web sur Windows et Android.

Depuis la fin du mois d'octobre, les chercheurs en sécurité de Proofpoint indiquent avoir constaté l'utilisation d'une version améliorée du kit d'exploits DNSChanger dans le cadre de campagnes de publicités malveillantes (du malvertising).
Pour ce retour, DNSChanger – qui avait infecté des millions d'ordinateurs en 2012 – cible des routeurs domestiques et fonctionne la plupart du temps via le navigateur Google Chrome sur Windows et les appareils Android. Toutefois, il s'agit bel et bien d'exploiter des vulnérabilités affectant des routeurs.
Du code JavaScript malveillant permet de révéler une adresse IP locale par le biais d'une requête WebRTC (Web Real-Time Communication) vers un serveur STUN (Session Traversal Utilities for NAT) de Mozilla. WebRTC est un protocole pour la communication en temps réel sur le Web, et STUN est un protocole permettant de découvrir l'adresse IP et le port d'un client ainsi que déterminer des restrictions au niveau du routeur.

Si l'adresse IP est jugée digne d'intérêt, une fausse publicité est affichée. Elle prend la forme d'une image au format PNG. Un code exploit est caché dans les métadonnées et pour rediriger la victime vers une page hôte de DNSChanger.

Proofpoint explique que DNSChanger va une nouvelle fois vérifier l'adresse IP locale de la victime grâce à des requêtes STUN. Puis, le navigateur Google Chrome chargera plusieurs fonctions et une clé de chiffrement AES cachée par stéganographie dans une petite image. La clé sert à dissimuler du trafic et décrypter une liste d'empreintes numériques afin de déterminer si un modèle de routeur est vulnérable.
L'attaque menée dépend du modèle de routeur. Elle est utilisée pour modifier les entrées DNS (Domain Name System ; correspondance entre un nom de domaine et une adresse IP) dans le routeur et tenter de rendre accessibles les ports d'administration depuis des adresses externes. Le chercheur Kafeine de Proofpoint évoque alors une exposition du routeur à d'autres attaques et cite l'exemple des botnets Mirai.
À noter que s'il n'y a pas d'exploits connus, une attaque tentera tout de même sa chance en essayant de tirer parti d'identifiants qui sont ceux par défaut (pas modifiés par l'utilisateur), et toujours pour modifier les paramètres DNS.
Soulignons bien que le navigateur n'est ici pas mis en cause…[lire la suite]

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 de formation, de sensibilisation ou d'audits 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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : DNSChanger attaque des routeurs domestiques via malvertising