10 points à connaître sur l’attaques DDoS des États-unis

	10 points à connaître sur l’attaques DDoS des États-unis

Le vendredi 21 Octobre, une série d'attaques par déni de service (DDoS) a provoqué une importante perturbation de l'accès aux sites Internet aux États-Unis. Les attaques ont ciblé les serveurs DNS (qui livrent les informations aux bonnes adresses), rendant de nombreux sites inaccessibles pendant plusieurs heures. Parmi eux figurent des sites permettant d'effectuer des achats en ligne, des réseaux sociaux, et d'écouter de la musique.

10 points à connaître sur l'attaque DDoS

ESET dresse un bilan des 10 points à retenir sur cette attaque. En voici un extrait, la version détaillée étant disponible sur WeLiveSecurity (version anglaise).

1. Les attaques ont ciblé la société Dyn, un important fournisseur de serveur DNS utilisé par de grands groupes comme Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast, et le réseau Playstation.
2. Les attaquants ont piraté des milliers d'appareils connectés mal-protégés tels que les routeurs domestiques et les caméras de surveillance, pour former un réseau botnet.
3. L'attaque a été facilitée par la négligence des utilisateurs qui n'ont pas changé le mot de passe par défaut de leurs appareils.
4. L'exploitation d'appareils numériques par un code malveillant peut perturber l'activité économique d'un pays : il est probable que plusieurs millions de dollars de vente ligne soient perdus.
5. De nombreuses personnes malveillantes sont prêtes à nuire à l'activité économique d'un pays au moyen d'un code malveillant, et ce pour de multiples raisons.
6. L'information et l'éducation des utilisateurs sont primordiales.
7. La réduction du nombre d'appareils connectés vulnérables est un objectif réalisable et auquel les entreprises peuvent contribuer. Voici d'ailleurs 4 mesures recommandées par l'US CERT :

• Remplacer tous les mots de passe par défaut par des mots de passe forts ;
• Mettre à jour les objets connectés ;
• Désactiver l'UPnP (universal plug and play) des routeurs sauf en cas d'absolue nécessité ;
• Acheter des objets connectés auprès d'entreprises certifiant de fournir des dispositifs sécurisés.

1. Le code malveillant infectant les routeurs n'est pas nouveau et a déjà été repéré en mai 2015 par les équipe ESET.
2. Les nouvelles générations d'attaques DDos amplifient leur portée dans le fait qu'elles s'appuient sur de nombreux objets connectés.
3. Cette dernière attaque nous montre à quel point un pays peut être vulnérable en cas d'attaque de son système d'informations.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : ESET livre les 10 points à connaître sur l’attaque DDoS – Global Security Mag Online