Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients



Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements....[Lire la suite]



- 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.



Contactez-nous

Réagissez à cet article





- 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.



Contactez-nous

Réagissez à cet article





- 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.



Contactez-nous

Réagissez à cet article





- 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.



Contactez-nous

Réagissez à cet article





- 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.



Contactez-nous

Réagissez à cet article

10 points à connaître sur l'attaques DDoS des Étatsunis



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

 $: \ https://www.lenetexpert.fr/formations-cybercriminal ite-protection-des-donnees-personnelles\\$



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.



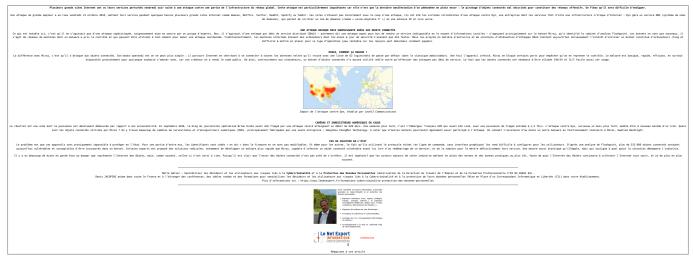
Contactez-nous

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

Pourquoi les objets connectés sont un danger pour l'Internet ?





Original de l'article mis en page : Le retour des botnets ou pourquoi les objets connectés sont un danger pour l'Internet

Quelques détails sur la cyberattaque massive dont ont été victime les états unis



Ouelques détails sur la cyberattaque massive dont ont été victime les états unis Pendant plusieurs heures, une vaste attaque informatique a paralysé de nombreux sites internet outre-Atlantique, vendredi 21 octobre.

En se réveillant vendredi 21 octobre, plusieurs millions d'Américains ont la désagréable surprise de se voir refuser l'accès à leurs sites préférés. Pendant de longues heures, impossible en effet de se connecter à **Twitter**, **Spotify**, **Amazon ou eBay**. Mais aussi à des grands médias, tels que le **New York Times**, **CNN**, **le Boston Globe**, **le Financial Times** ou encore le célèbre quotidien anglais **The Guardian**. En cause : une **cyberattaque massive** menée en plusieurs vagues qui a fortement perturbé le fonctionnement d'internet outre-Atlantique.

Le fait que tous ces sites mondialement connus soient hors d'accès ne révèle toutefois que la partie émergée de l'iceberg. En effet, les pirates s'en sont pris en réalité à la société Dyn, dont la notoriété auprès du grand public est beaucoup plus faible. Le rôle de la firme est de rediriger les flux internet vers les hébergeurs et traduit en quelque sorte des noms de sites en adresse IP. À 22h17, Dyn a indiqué que l'incident était résolu.



Le département de la sécurité intérieure (DHS) ainsi que le FBI ont annoncé dans la foulée **l'ouverture d'une enquête** « sur toutes les causes potentielles » de ce gigantesque piratage à l'envergure inédite. Des investigations qui s'annoncent de longue haleine, tant cette attaque se déplaçant de la côte est vers l'ouest du pays semble sophistiquée. « C'est une attaque très élaborée. À chaque fois que nous la neutralisons, ils s'adaptent », a expliqué Kyle Owen, un responsable de Dyn, cité sur le site spécialisé Techcrunch.

Qui est à l'origine de l'attaque ?

Pour l'heure, l'identité et l'origine des auteurs demeurent inconnues. Mais l'ampleur du piratage éveille les soupçons. « Quand je vois une telle attaque, je me dis que c'est un État qui est derrière », a estimé Eric o'Neill, chargé de la stratégie pour la société de sécurité informatique Carbon Black et ex-chargé de la lutte contre l'espionnage au FBI. Les regards se tournent inévitablement vers des pays comme la Russie ou la Chine, qui pourraient avoir intérêt à déstabiliser le géant américain, alors que les élections approchent.

Mais d'autres hypothèses circulent. Le site Wikileaks, qui a publié des milliers d'emails du directeur de campagne de la candidate démocrate à la présidentielle Hillary Clinton, a cru déceler dans cette attaque une marque de soutien à son fondateur Julian Assange, réfugié dans l'ambassade d'Équateur à Londres et dont l'accès à internet a été récemment coupé. « Julian Assange est toujours en vie et Wikileaks continue de publier. Nous demandons à nos soutiens d'arrêter de bloquer l'internet américain. Vous avez été entendus », a tweeté le site.

Comment les pirates ont-ils procédé ?

La technique utilisée vendredi pour plonger le web américain dans le chaos est dite de déni de service distribué (DDoS). Cette dernière consiste à rendre un serveur indisponible en le surchargeant de requêtes. Elle est souvent menée à partir d'un réseau de machines zombies – des « botnets » – elles mêmes piratées et utilisées à l'insu de leurs propriétaires. En l'occurrence, les pirates ont hacké des objets connectés, tels que des smartphones, machines à café, des téléviseurs ou des

« Ces attaques, en particulier avec l'essor d'objets connectés non sécurisés, vont continuer à harceler nos organisations. Malheureusement, ce que nous voyons n'est que le début en termes de 'botnets' à grande échelle et de dommages disproportionnés », prédit Ben Johnson, ex-hacker pour l'agence américaine de renseignement NSA et cofondateur de Carbon Black.

Quelles peuvent être les conséquences ?

La société Dyn était préparée à ce type d'attaque et a pu résoudre le problème dans des délais relativement brefs. Mais les conséquences pourraient être bien plus graves dans les secteurs de la finance, du transport ou de l'énergie, bien moins préparés, selon Eric o'Neill. Quelle qu'en soit l'origine, l'attaque a en effet mis en lumière les dangers posés par l'utilisation croissante des objets connectés, qui peuvent être utilisés à l'insu de leurs propriétaires pour bloquer l'accès à un site.[lire la suite]

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



spécialisé en cybercriminalité et en protection des

- Expertises techniques (virus, espions, piratages fraudes, arnaques Internet...) et judiciaire
- (investigations telephones, 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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Trois questions pour comprendre la cyberattaque massive

La Métropole de Lyon touchée par un virus informatique



La Métropole de Lyon touchée par un virus informatique Les services du Grand Lyon sont touchés depuis jeudi, en fin d'après-midi, par un virus informatique. Un mail reçu, comportant un fichier Excel, serait à l'origine du problème.Il est demandé aux usagers d'être vigilants et de ne pas ouvrir de mails suspects.Le nettoyage est en cours et tout devrait être rétabli dans la journée.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées 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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Lyon | La Métropole touchée par un virus informatique

OVH attaqué par des réseaux

d'objets connectés

```
in range(1, 1000):

ck()

ct socket, sys, os

""][Remote DDoS Attack"

""injecting " + sys.argv

cttack():

socket.socket(socket.AF IN
```

C'est un record dont il se serait sans doute passé. La semaine dernière, le fondateur d'OVH Octave Klaba expliquait sur son compte Twitter que l'hébergeur roubaisien était victime d'une série d'attaques en déni de service (DDoS) d'une ampleur inédite.

Ces attaques, qui consistent à submerger un service Web de demandes pour le mettre hors service, sont monnaie courante sur la Toile. Dans une étude portant sur la période avril 2015-mai 2016 , la société Imperva notait une multiplication par deux du nombre d'attaques DDoS par rapport à l'année précédente (à 445 attaques par semaine chez ses clients).

Mais c'est surtout la puissance de feu déployée récemment qui surprend. Mesurée en Gigabits par seconde (Gbps) quand elle se concentre sur la couche réseau, l'attaque la plus forte enregistrée par Imperva atteignait 470 Gbps mi-2016. Depuis, ce record ne cesse de tomber.

Cet été, les organisateurs des Jeux olympiques de Rio remportaient la médaille d'or de l'attaque DDoS avec des pics à 540 Gbps. La semaine dernière, c'était au tour du blog du spécialiste de la sécurité informatique Brian Krebs de subir « la plus grande attaque DDoS qu'Internet ait jamais vu », à 665 Gbps. Presque simultanément, OVH lui ravissait la couronne, encaissant des pics à plus de 1.000 Gbps.

Des botnets extrêmement efficaces

Pour mener des raids aussi violents, les cybercriminels s'appuient désormais non plus seulement sur des ordinateurs corrompus pour relayer leurs attaques (un « botnet », dans le jargon), mais sur des millions d'objets connectés — caméras IP, enregistreurs vidéo, routeurs…

Selon Octave Klaba, le botnet qui s'est attaqué à OVH comprenait ainsi pas moins de 145.607 caméras et enregistreurs numériques . Si les premiers botnets d'objets connectés (téléviseurs, réfrigérateurs...) ont été détectés dès 2014 , ils sont devenus extrêmement efficaces...[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées 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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : OVH : ces cyberattaques dopées par des réseaux d'objets connectés, High tech