Questions/réponses sur les attaques portées au système des noms de domaine

(Source : annonce de l'ICANN du 22 février 2019)

Q : Pourquoi l'ICANN publie-t-elle des déclarations maintenant ?
R : Après avoir pris connaissance des attaques, via des rapports de médias ou de professionnels de la sécurité, il était important que l'ICANN prenne des mesures visant à s'assurer que la communauté de l'ICANN et le public dans son ensemble soient également informés de la situation. Cela relève de notre mission consistant à garantir la sécurité et la stabilité du système des noms de domaine (DNS).

Q : De quel type d'attaque s'agit-il ?
R : Les rapports publics révèlent une tendance : les attaques multidimensionnelles utilisant différentes méthodologies. Certaines de ces attaques visent le DNS. Elles ont recours à des modifications non autorisées de la structure de délégation des noms de domaine, remplaçant les adresses de certains serveurs par des adresses de machines contrôlées par les attaquants. Ce type d'attaque spécifique, qui cible le DNS, est uniquement possible lorsque les extensions de sécurité du système des noms de domaine (DNSSEC) ne sont pas utilisées.

Q : Qui se trouve derrière ces attaques ?
R : Selon les rapports, les opinions divergent quant à la question de savoir qui se trouve derrière les attaques, et il est souvent difficile de déterminer avec précision l'entité à l'origine de ces attaques.

Q : Les organismes chargés de l'application de la loi mènent-ils des enquêtes sur les attaques ?
R : Les rapports publics indiquent que les organismes chargés de l'application de la loi et les services de sécurité nationaux de différents pays enquêtent sur les attaques. La société civile (ingénieurs du DNS, experts en cybersécurité et autres) travaille également activement à l'identification des types d'attaques utilisés. Elle aide en outre les organisations affectées par ces attaques à renforcer leurs systèmes.

Q : L'ICANN a-t-elle été victime de piratage ?
R : Rien n'indique que les systèmes de l'ICANN ont été piratés. Nous avons effectué un examen des systèmes par mesure de prudence.

Q : Des serveurs racine ont-ils été piratés ?
R : Rien n'indique qu'un des serveurs racine du DNS a été piraté. L'ICANN a contacté le Comité consultatif du système des serveurs racine (RSSAC) afin de lui demander de consulter les opérateurs de serveurs racine pour qu'ils confirment qu'il n'y a aucun signe de piratage. Jusqu'à présent, aucun opérateur de serveur racine ne nous a informés d'un piratage.

Q : Quelle est la gravité du risque ? Combien de noms de domaine ne présentent aucune garantie de sécurité ?
R : Une partie des attaques se servent des mots de passe qui ont été piratés. Il est impossible de savoir combien d'autres mots de passe ont pu être piratés. De ce fait, nous encourageons une nouvelle fois toutes les parties de l'écosystème du DNS à

utiliser des mots de passe complexes, de les changer souvent, de ne pas utiliser les mêmes mots de passe sur plusieurs sites, et d'utiliser l'authentification multifactorielle dès que possible.

Q : Les attaques se poursuivent-elles ? Quand ont-elles commencé ? Quand ont-elles pris fin ?
R : Bien que nous n'ayons pas connaissance des attaques en cours, nous estimons qu'il existe un risque constant. Nous encourageons l'ensemble des organisations à améliorer leur sécurité en ligne, notamment via la mise en œuvre des extensions de sécurité du système des noms de domaine (DNSSEC), si cela n'a pas déjà été fait. Elles devraient également veiller à ce que leurs identifiants pour la gestion des noms de domaine sont sécurisés et effectuer un examen de leurs systèmes afin de détecter d'éventuels signes de piratage, falsification, etc. Les rapports publiés suggèrent que l'ensemble d'attaques actuel remonte à 2017.

Q : L'ICANN recommande-t-elle de prendre des mesures spécifiques ?
R : Oui. Le 15 février 2019, l'ICANN a proposé la liste de contrôle suivante, bien qu'elle ne comprenne pas toutes les mesures susceptibles d'être mises en œuvre afin de garantir une sécurité maximale :

- S'assurer que les correctifs de sécurité ont été révisés et appliqués
- Passer en revue les fichiers journaux afin de détecter des accès non autorisés aux systèmes, notamment des accès administrateur
- Réviser les contrôles internes de l'accès administrateur (« racine »)
- Vérifier l'intégrité de tous les enregistrements DNS ainsi que l'historique de modifications de ces enregistrements
- Imposer l'utilisation de mots de passe suffisamment complexes, notamment en termes de longueur
- Veiller à ce que les mots de passe ne sont pas partagés avec d'autres utilisateurs
- Veiller à ce que les mots de passe ne sont jamais stockés ou transmis en texte clair
- Imposer régulièrement des changements de mots de passe
- Mettre en œuvre une politique de verrouillage du mot de passe
- S'assurer que les enregistrements de la zone du DNS sont signés DNSSEC et que vos résolveurs du DNS procèdent à la validation des DNSSEC
- Idéalement, s'assurer de l'activation de l'authentification multifactorielle dans tous les systèmes, notamment pour l'accès administrateur
- Idéalement, veiller à ce que le domaine de sa boîte de réception dispose d'une politique DMARC avec SPF et/ou DKIM et que les politiques fournies par d'autres domaines sont respectées sur le système de votre boîte de réception

Q : La mise en œuvre des DNSSEC protège-t-elle les utilisateurs finaux ?
R : Oui. La mise en œuvre des DNSSEC protégera les utilisateurs contre des types d'attaques spécifiques. Certains des systèmes qui ont été utilisés afin de préparer les attaques ont eu recours à des noms de domaine qui étaient protégés par des DNSSEC, et les propriétaires de ces zones ont confirmé que leur utilisation des DNSSEC avait permis d'atténuer les effets des attaques.