Faille DNS : rectifications et précisions de la part de Mr Moro Israël

Cet entretien a provoqué un torrent de commentaires, notamment de la communauté Linux qui a très mal apprécié (c'est un euphémisme) les propos de Mr Israël.

Nous en convenons : certains propos ont été mal compris par notre journaliste, d'autres ont manqué de précisions, notamment sur la définition des fichiers host et des mises à jour automatique (étaient évoquées les appliances et les routeurs et pas les PC des particuliers qui évidemment sont mis à jour simplement sous Windows ET sous Linux).

Nous avons repris contact avec Mr Israël qui nous livre les précisions suivantes La rédaction

---

« Ce fichier (host) retrace toutes les adresses IP consultées, ***quelqu'un qui s'y introduirait aurait alors accès à une multitude de données »***

Plutôt : **«** Ce fichier fait le lien entre une adresse IP et un nom de serveur, par exemple *« 145.23.55.12 www.bnp.fr »* **quelqu'un qui s'y introduirait avec une fausse adresse détournerait alors le trafic du vrai site bancaire sur son faux site, sans que l'utilisateur s'en rende compte ou puisse l'empêcher… »**

« Ce type de problème est pour l'instant maîtrisé sous Windows, mais Linux et surtout Ubuntu n'ont, à mon sens, aucune maîtrise réelle sur ce type de dangers. »

Ce type de problème est -pour l'instant- maîtrisé, par le fait que l'utilisateur ne doit plus être administrateur de son poste en entreprise, mais les administrateurs des systèmes UNIX ou Windows ont la fâcheuse habitude de se connecter en root ou admin, et le danger reste toujours possible d'un exploit qui permettrait de modifier fichier «hosts » par élévation de privilèges. Dans des versions « grand public » comme Ubuntu ou Windows, les utilisateurs et les PME/TPE n'ont aucune compétence réelle sur ce type de dangers, et dépendent complètement de la sécurité de leur fournisseur Internet, ou de leur routeur d'accès ou du serveur interne de l'entreprise qui contiennent un système DNS de relais.

« Cette faille est connue depuis 1974, date à laquelle j'attribue l'invention d'Internet. »

« Cette faille est d'autant plus grave qu'elle est structurelle, et remonte à la structure même du protocole au moment de l'invention d'Internet, à savoir le *Domain Name* relié à une adresse IP, clé de toute consultation d'un site sur Internet comme un site web. »

« A la loupe, on se rend compte qu'il s'agit de failles liées à l'OS. Le moment critique se situe au moment de la séquence de questionnement. Je m'explique : si vous lancez une requête DNS à partir, par exemple, du port 53 UDP, la réponse que vous allez obtenir n'est pas du tout due au hasard. Il faut savoir que ce que l'on appelle le dialogue du port est prévisible et peut être calculé. Ce qui nous fait comprendre qu'à ***partir de là, hé bien, tout est possible… »***

Plutôt : **«** A la loupe, on se rend compte qu'il s'agit d'un type de faille structurelle. Le moment critique se situe au moment de la séquence de dialogue entre le client et le serveur DNS. Je m'explique : si votre navigateur lance une requête DNS du port 53 UDP, la réponse que vous allez obtenir n'est pas suffisamment due au hasard. Il faut savoir que ce que –contrairement aux recommandations qui ont été faites sous forme de RFC pour rendre imprévisible le numéro de port de la séquence de réponse, beaucoup de programmeurs, par facilité ou par « copier-coller » d'autres programmes ont crée des systèmes où le port n'est pas si aléatoire que ça et peut dans certains cas être calculé, voilà le cœur de la faille actuelle. Ce qui nous fait comprendre qu'à **partir de là, hé bien, tout est possible… Comme par exemple de détourner tout le trafic de tous les internautes de leur vraie banque à un faux site, et ainsi de vider la plupart des comptes en banque de la planète, provoquant une gigantesque crise économique, le fameux « big one »**

*Mais que fait-on pour Linux, combien de temps va durer cette faille ? Il faut bien savoir qu'il y a quelques mois,**on a frôlé le » Big One », le jour où tous les comptes ont été remis à zéro**. Il faut continuer la sensibilisation des entreprises et encourager les patchs. Pas seulement sous Windows mais pour Unix, Linux, et toutes les appliances de type routeurs, firewalls, serveurs de mails…*

Plutôt : « Alors qu'un système automatique de patches existe pour Windows et pour Linux, combien de temps va durer la vulnérabilité dans les entreprises où l'on trouve de nombreux systèmes non patchés depuis leur mise en œuvre ? Il faut bien savoir qu'il y a quelques mois, **on a déjà frôlé le » Big One », par déni de service distribué, alors que 5 des 13 principaux serveurs DNS de la planète ont été bloqués par une inondation massive de paquets, ou bien lors de la découverte d'une faille dans le protocole SSL**. Il faut donc continuer la sensibilisation des entreprises et encourager les patches. Pas seulement sous Windows mais pour Unix, Linux, et toutes les « appliances » de type routeurs, firewalls, serveurs de mails… C'est à ce prix que la sécurité réelle sera rétablie, car cette fois ce n'est pas uniquement Windows qui est classiquement visé, mais le fondement même d'Internet à travers le protocole DNS, donc toute machine et appareil connecté à Internet quel que soit son système.

*« quant aux grands groupes ils sont obligés de prendre des risques énormes car il faut avouer que dans de nombreux cas, leur politique est… de ne rien faire. Le DNS est une chose trop » instable » pour qu'on la laisse sans protection. Il faudrait une sorte de*SecureDNS *qui permettrait un cryptage des données »*

Plutôt : « quant aux grands groupes ils prennent actuellement des risques énormes car il faut avouer que dans de nombreux cas, leur politique actuelle concernant les patches autres que Windows est… de ne rien faire. Le DNS est une chose trop au centre d'Internet pour qu'on le laisse sans protection, ou avec des patches manuels, ce qui nous ferait régresser d'une bonne dizaine d'années par rapport aux patches automatisés. Il faudrait donc une sorte de *SecureDNS* qui permettrait un cryptage des données échangées et un véritable séquencement aléatoire du dialogue. Ce système *DNSSEC* a été publié pour le principal système de DNS le « BIND » de l'ISC, mais est loin d'être répandu car il entraine des conséquences de performances et de fonctionnement notables. Enfin, au moment où la France va se doter d'une agence de sécurité des systèmes d'information, **il faudrait créer une équipe dédiée dans cette agence qui pourrait donner l'alerte, et le status « vert-jaune-rouge »** pour les entreprises et les particuliers vis-à-vis du risque internet, comme dans d'autres pays comparables, **mais cette fois en Français**, car toute l'information dont j'ai fait état provient de sites Américains…