Google se penche sur le phishing 2.0

Les serveurs DNS « Open Recursive » ou « Ouverts et récursifs » peuvent être utilisés par les cybercriminels pour rediriger les internautes vers des sites de phishing ou d'hameçonnage, expliquent des chercheurs de Google et de l'institut de technologie de Georgie.

Ces derniers, doivent d'ailleurs publier une étude sur ce sujet d'ici le mois de février. Les serveurs DNS dits « Open recursive » qui d'une certaine façon fonctionnent en boucle, sont utilisés pour indiquer aux ordinateurs comment se retrouver sur le réseau Internet.

Pour cela, ils procèdent de la façon suivante, ils traduisent une URL classique par exemple celle du site yahoo.com en une adresse IP numérique…

Seulement les criminels de la Toile commencent à utiliser ces serveurs avec de nouvelles méthodes de phishing. Selon les chercheurs à l'origine de cette découverte, il existe 17 millions de serveurs Open Recursive, et dans la plupart des cas ces serveurs fonctionnent bien.

Malheureusement, contrairement aux autres serveurs DNS, les systèmes « open-recursive » peuvent répondre à une requête de DNS lookup depuis n'importe quel poste connecté à la Toile. Une fonctionnalité très intéressante du point de vue des hackers.

Pour l'institut technologique de Georgie, **0.4% des serveurs DNS open-recursive, soit 68.000 machines,** fonctionnent déjà de façon malveillante. Et 2% de ces mêmes serveurs génèrent des erreurs.

Comment l'attaque fonctionne-t-elle au niveau de l'utilisateur ? Dans les faits, une victime va visiter un site Web infecté par un code malveillant ou ouvrir une pièce jointe à un email.

Une fois le poste cible infecté, les attaquants vont simplement modifier une clé du registre de l'utilisateur pour indiquer au poste cible comment se rendre automatiquement sur le serveur des criminels où toutes les informations DNS de l'utilisateur sont collectées.

Si l'antivirus de l'utilisateur ne détecte rien, alors le hacker peut prendre le contrôle total du poste. Pour de nombreux experts en sécurité, il s'agit de l'attaque ultime de phishing, et elle a été baptisée le Phishing 2.0. Et comme elle se déroule au niveau du DNS, les solutions traditionnelles sont inefficaces.