Un gros botnet détourne des requêtes de recherche

Un gros botnet détourne des requêtes de recherche

Depuis septembre 2014, un botnet a pu compter près d'un million de zombies pour faire gonfler des revenus publicitaires de cybercriminels.

Actif depuis mi-septembre 2014, un botnet est parvenu à prendre le contrôle de près d'un million d'ordinateurs dans le monde. L'agent infectieux est un malware intégré dans un fichier d'installation modifié de type MSI pour Windows.
Botnet-Redirector.Paco-carte-BitdefenderCes fichiers corrompus sont associés à des programmes tels que WinRAR, YouTube Downloader, Connectify, Start8 et KMSPico. Après installation sur la machine prise pour cible, le nuisible dénommé Redirector.Paco s'appuie sur un fichier PAC (Proxy auto-config) pour rediriger des requêtes de recherches sur Google, Bing ou Yahoo.
Au gré de quelques modifications dans la base de registre, le trafic sera redirigé vers des publicités contextuelles permettant de générer des revenus ici frauduleux grâce au programme AdSense pour les recherches de Google.
Les opérateurs du botnet détournent les recherches vers un autre moteur de recherche personnalisé spécifiquement conçu qui affiche ses propres résultats, et détournent par la même occasion des revenus publicitaires… [Lire la suite]
Article de Jérôme GARAY

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

Source : *Un gros botnet détourne des requêtes de recherche*