Europol coupe le sifflet au botnet Ramnit

A l'assaut de **Ramnit**. Le 24 février, le centre de lutte contre la cyber-criminalité d'**Europol (EC3)** a coordonné une opération visant à terrasser ce **botnet** qui a infecté 3,2 millions d'ordinateurs dans le monde. Supervisée depuis la Hague, l'intervention a nécessité la collaboration de forces de police de plusieurs pays (Allemagne, Pays-Bas, Royaume-Uni).

Des éditeurs de solutions de sécurité comme Microsoft, Symantec et AnubisNetworks ont également participé à cette offensive anti-malware. De manière plus précise, c'est le J-CAT* (présenté comme une cellule commando anti-cybercriminalité activée sous la tutelle du centre EC3 d'Europol) qui a servi de centre de coordination pour abattre ce botnet. Le CERT-UE (cellule européenne de veille face aux menaces du web) a également été mis à contribution, selon ITespresso.

Débrancher les serveurs de commandes et contrôle

L'objectif de cette opération policière consistait à couper les serveurs de commande et de contrôle qui servent de tableau de bord pour les botnets et à confisquer les 300 domaines Internet exploités par les cybercriminels qui servaient d'appâts pour infecter les ordinateurs des utilisateurs finaux et faciliter la récupération illicite de données confidentielles.

Ramnit ciblait les PC sous Windows. Une fois le système infecté, les pirates étaient en mesure de subtiliser des informations sensibles (comme les codes d'accès à un compte bancaire) et de désactiver les protections antivirus. Les ordinateurs tombant dans le réseau zombie pouvaient également se transformer en vecteurs de propagation de spam.

Le communiqué d'Europol ne précise pas si cette action anti-botnet a donné lieu à des arrestations.

J-CAT pour Joint Cybercrime Action Taskforce