OpÃ©ration Tovar : les internautes britanniques ont deux semaines pour rÃ©agir
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 5/6/2014 13:00:00

Le National Crime Agency (NCA) britannique vient de lancer une alerte et encourage fortement les internautes du Royaume-Uni Ã protÃ©ger et mettre Ã jour leurs ordinateurs au cours des deux prochaines semaines, suite au dÃ©mantÃ¨lement d'un puissant rÃ©seau de cybercriminels dans le cadre de l'OpÃ©ration Tovar menÃ©e conjointement par le FBI, Europol et le NCA.

Le groupe de hackers est en effet soupÃ§onnÃ© d'avoir infectÃ© prÃ¨s d'un million d'ordinateurs dans le monde grÃ¢ce au virus Cryptolocker et au botnet Gameover Zeus (ou GOZeuS).

Le virus Cryptolocker aurait dÃ©jÃ infectÃ© plus de 234 000 machines ; sa technique consiste Ã empÃªcher les utilisateurs d'accÃ©der Ã leur ordinateur, puis Ã encrypter les donnÃ©es de faÃ§on Ã rÃ©clamer une rançon. GOZeuS est, quant Ã lui, destinÃ© Ã dÃ©rober des identifiants et donnÃ©es bancaires, notamment via la technique du phishing.

Olivier MÃ©lis, Country Manager France chez CyberArk a fait les commentaires suivants :

Â« *Les Botnets infectent gÃ©nÃ©ralement leurs victimes de maniÃ¨re opportuniste plutÃ´t que via des attaques ciblÃ©es. Le plus souvent, la finalitÃ© est de prendre le contrÃ´le des machines afin de perpÃ©trer des attaques par dÃ©ni de service (DoS), via des redirections de communications command and control (C&C) et pour rassembler des informations personnelles d'identifications (PII) et codes d'accÃ¨s de haute importance.*

Â

Bien qu'elles concernent principalement les individus, ces attaques opportunistes sont Ã©galement en mesure d'atteindre les rÃ©seaux d'entreprises afin de dÃ©tourner les codes d'accÃ¨s, que ce soit Ã travers l'infection d'une machine au sein du rÃ©seau ou les identifiants VPN. Les hackers peuvent ainsi viser les utilisateurs individuels mais Ã©galement les organisations qui leur permettent de faire des bÃ©nÃ©fices financiers plus intÃ©ressants.

Le plus ennuyeux dans ce type d'attaques est le succÃ¨s que rencontrent les hackers lors du dÃ©tournement de comptes Ã privilÃ¨ges, tels que les comptes d'administrateurs ou ceux d'opÃ©rateurs de systÃ¨mes de contrÃ´le industriels. C'est pourquoi les organisations ne peuvent plus se contenter de sÃ©curiser les informations d'identification sensibles par de simples pÃ©rimÃ¨tres de sÃ©curitÃ© ou outils traditionnels.

Il est essentiel de surveiller et de contrÃ´ler ces comptes puissants pour limiter au maximum la menace d'une attaque sur une organisation. Les entreprises auraient raison de penser que leur rÃ©seau est dÃ©jÃ potentiellement compromis et de se concentrer sur la sÃ©curisation de l'accÃ¨s Ã leurs ressources les plus vitales.

De son cÃ´tÃ©, le NCA a lancÃ© le compte Ã rebours, laissant deux semaines aux britanniques pour protÃ©ger leurs ordinateurs. Il faut toutefois rappeler que cette attaque a Ã©tÃ© perpÃ©trÃ©e au niveau mondial et qu'aucune organisation d'aucun pays n'est Ã l'abri aujourd'hui. Â»