Vol de données bancaires : le malware Dridex cible la France

Le botnet Dridex, que les autorités expliquaient avoir démantelé il y a deux semaines, serait toujours actif… et ciblerait en particulier la France. La société américaine, spécialiste de la sécurité des points d'accès, Invincea explique en effet avoir détecté 60 instances du botnet ciblant des utilisateurs français avec le malware Dridex, spécialisé dans le vol de données bancaires. « *Au moins certains de ses serveurs de commande et contrôle ont été remis sur pied* », écrit Invincea. Selon la société, qui explique que ses observations portant sur le retour du botnet remontent au 22 octobre, le malware envoyé par les cybercriminels est **signé avec un certificat émis par l'entreprise de sécurité Comodo**, « *ce qui signifie que les technologies de sécurité qui font confiance aux exécutables signés échoueront à stopper ces attaques* », note Invincea. Ceci concerne notamment les entreprises ayant placé en liste blanche de telles applications.

La menace est confirmée par le CERT-FR, qui a émis une alerte au sujet de Dridex le 23 octobre. « *Depuis la mi-octobre 2015, le CERT-FR constate à l'échelle nationale une vague de pourriels (de type Dridex, NDLR) dont le taux de blocage par les passerelles anti-pourriel est relativement faible* », écrit l'organisme officiel de réponse aux menaces, qui dépend de l'Anssi (Agence Nationale de la Sécurité des Systèmes d'information). Le centre note que ces courriels sont souvent écrits dans un français sans faute.

Radical : désactiver les macros

L'attaque prend en effet la forme d'une campagne de phishing, des mails renfermant des documents Microsoft Office qui semblent renfermer des factures émanant de magasins, d'hôtels ou d'organismes divers (la fourrière de Grenoble, la DGA…). Si l'utilisateur ouvre ces documents, une macro VBScript ou Visual Basic est employée pour assembler le malware PIDARAS.exe, via une technique dite Just-in-Time, qui consiste à construire la souche infectieuse directement sur le poste de la cible, afin d'échapper aux défenses basées sur le monitoring de réseau ou les bacs à sable. Selon le CERT-FR, les téléchargements s'effectuent via le port HTTP « *non standard 8080* », une caractéristique qui « *permet de détecter pour cette variante les postes ayant exécuté la macro* ».

Une fois le malware en place, il communique avec des serveurs basés au Japon, via le port 473. Si Dridex est susceptible d'échapper à la vigilance de certains antivirus, une désactivation de la fonction d'exécution automatique des macros Office permet de lui couper les ailes, rappelle le centre de réponse aux incidents de l'administration française.

Suite à l'arrestation d'individus soupçonnés de liens avec le cybercrime l'été dernier, le FBI américain, en partenariat avec les autorités britanniques, a annoncé mi-octobre le démantèlement des infrastructures de commande et contrôle de Dridex. Repéré en novembre 2014, le malware a infecté des entreprises dans plus de 26 pays, engendrant de **grosses pertes financières** : 10 millions de dollars détournés aux Etats-Unis, 20 millions de livres sterling au Royaume-Uni.

A lire aussi :

Neuf malwares sur 10 échappent aux listes noires
Le malware PoSeidon met les terminaux point de vente en danger
Destover : le malware revient… et il est signé Sony !

crédit photo © GlebStock – Shutterstock