Piratage des lignes de caisse : le bilan de Backoff s'alourdit encore

Selon Kaspersky Labs, le bilan de Backoff, ce **malware qui cible les lignes de caisse** pour exfiltrer des données bancaires, sera encore plus lourd que les 1 000 entreprises touchées, première estimation donnée la semaine dernière par le ministère de l'Intérieur américain. Pour livrer cette estimation très noire, les chercheurs se fient **au trafic reçu par deux serveurs de commande et contrôle** sur lesquels ils sont parvenus à prendre la main. En seulement deux jours, plus de 100 systèmes infectés – provenant de 85 adresses IP distinctes localisées essentiellement aux Etats-Unis et au Canada – ont tenté d'établir une connexion avec ces serveurs. Parmi les victimes, figurent une grande chaîne de restaurants mexicains aux Etats-Unis, un spécialiste de la logistique nord-américain, une chaîne de magasins d'alcools aux Etats-Unis…

C'est l'ampleur de cette moisson qui inquiète les chercheurs. « *Les serveurs détournés (sinkhole) couvrent moins de 5 % des canaux de contrôle et commandes et ces deux domaines ne s'appliquent, qui plus est, qu'à certaines versions de Backoff conçues au premier trimestre de cette année* », expliquent-ils.

Une sécurité bien laxiste

Chez Computerworld, Roel Schouwenberg, un chercheur travaillant chez Kaspersky, précise même que la plupart des systèmes infectés l'ont été par une **variante du malware datant d'octobre 2013**. Les entreprises en question étaient donc victimes de Backoff depuis de longs mois, et ne semblaient pas en avoir conscience, reprend le chercheur pour qui cette affaire illustre la faiblesse des mesures de protection mises en place autour des terminaux point de vente. Car, si le malware est resté longtemps indétectable des outils standards, il **génère des transferts de données et des connexions** qui auraient dû donner l'alerte. « *Pourquoi un terminal de point de vente en Alabama aurait-il besoin de se connecter à un serveur en Russie ?* », ironise Roel Schouwenberg.

Rappelons que Backoff cible les terminaux point de vente et utilise une faiblesse de sécurité du processus d'autorisation des paiements par carte bancaire à piste magnétique pour extorquer un maximum d'informations. De grands distributeurs aux Etats-Unis, comme **les chaînes de magasins Target ou SuperValu**, ont été victimes de cette faille. Le piratage de la chaîne de magasins Target a ainsi abouti au vol de dizaines de millions de numéros de cartes bancaires et entraîné les départs du Pdg et de la DSI. Côté SuperValu, 180 magasins ont été victimes d'une fuite de données. 51 magasins **UPS** ont eux aussi subi les assauts de Backoff.

La première alerte concernant ce malware remonte au mois de juillet, le ministère de l'Intérieur américain (Department of Homeland Security, DHS) expliquant alors que Backoff échappait à la vigilance de la plupart des antivirus. Une lacune aujourd'hui comblée, les éditeurs ayant mis à jour leur solution tout récemment, selon la dernière alerte du DHS datant de fin août.

A lire aussi :

Sécurité de l'information : les entreprises dépensent toujours plus