Backoff écume les lignes de caisses : plus de 1 000 entreprises US touchées

Plus de 1 000 entreprises, de toutes tailles, ont été victimes du malware Backoff et toutes n'en ont probablement pas conscience, selon une **alerte du ministère de l'Intérieur des Etats-Unis** (Department of Homeland Security) publiée vendredi dernier. Apparu en octobre 2013, Backoff se distingue par sa capacité à aller **piocher dans la mémoire des terminaux de points de vente** pour y récupérer les données bancaires de cartes de crédit ou de débit. Des millions de clients des commerces infectés sont concernés, leurs données sont déjà ou seront probablement revendues au marché noir.

Rappelons que Backoff est déployé après une **première attaque ciblant**, elle, **des accès distants à des systèmes**, via des solutions comme Microsoft's Remote Desktop, Apple Remote Desktop, Chrome Remote Desktop, Splashtop 2, Pulseway et LogMeIn Join.Me. Une fois repérés, ces accès distants sont attaqués par force brute (l'assaillant tente d'entrer en essayant un maximum de couples login / mots de passe). Si les hackers parviennent à se ménager un accès par ce biais, ils déploient ensuite leur malware ciblant les terminaux point de vente et plus spécifiquement leur mémoire vive où les données des pistes magnétiques des cartes de débit ou de crédit américaines sont décryptées afin d'autoriser les transactions. Ces données sont ensuite exfiltrées discrètement.

Indétectable par les antivirus… jusqu'à tout récemment

Si le malware a semé derrière lui **quelques affaires très médiatisées** – on lui attribue le piratage de la chaîne de supermarchés Target, suivis par celui de SuperValu puis des magasins UPS tout récemment -, c'est bien à une **vague d'intrusions très importante** que doit faire face le Department of Homeland Security (DHS), qui parle d'interventions des services secrets auprès « *de nombreuses entreprises réparties à travers les Etats-Unis* ». Dans son alerte publiée en fin de semaine dernière, le DHS explique que **7 fournisseurs de systèmes de terminaux point de vente ont confirmé** que « *plusieurs de leurs clients ont été touchés* » par Backoff.

La première alerte concernant Backoff remonte au mois de juillet, le DHS expliquant alors que le malware échappait à la vigilance de la plupart des antivirus. Une lacune aujourd'hui comblée, les éditeurs ayant mis à jour leur solution tout récemment. Le DHS explique en effet que **les antivirus détectent le malware depuis ce mois d'août**. Lors du premier bulletin de fin juillet, les autorités américaines expliquaient que les éditeurs d'antivirus s'apprêtaient à mettre à jour leurs solutions pour assurer la détection des différentes variantes de Backoff. Il est donc probable que le bilan diffusé vendredi dernier par le DHS – un premier état des lieux pour le moins inquiétant – résulte de cette montée de version des antivirus.

Rappelons que le piratage de la chaîne de magasins **Target** a 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.

Pour limiter la fraude, Visa, Mastercard et consorts envisagent de remplacer **progressivement les pistes magnétiques des cartes utilisées aux US par des puces**. La migration est estimée à **8 milliards de dollars** et pourrait faire le bonheur des industriels français de la carte à puce (Gemalto, Oberthur et Morpho qui, tous trois, font partie du Top 5 mondial).

A lire aussi :

Sécurité de l'information : les entreprises dépensent toujours plus