Les sites de e-commerce attaqués par le keylogger Magecart

Des dizaines, voire des centaines peut-être plus, de sites e-commerces sont peut-être infectés par Magecart, un programme qui surveille les saisies du clavier. Plus précisément, le malware affecterait les applications de panier électronique, c'est-à-dire la phase de validation et de paiement de la commande proprement dite. Magecart permet potentiellement de récupérer les informations de paiement par carte bancaire (nom, numéro de carte, date d'expiration, cryptogramme virtuel…) saisies lors d'un achat en ligne. C'est du moins ce que rapporte RiskIQ.

A la manière d'un homme-du-milieu

Selon cette société spécialisée dans la gestion des menaces, la campagne d'infection des sites de commerce en ligne a commencé en mars dernier. Elle affecte particulièrement les sites exploitant les plates-formes Magento Commerce, Powerfront CMS et OpenCart. La société de sécurité Sucuri s'en était d'ailleurs fait l'écho en juin dernier. Les fournisseurs de services de paiement Braintree et VeriSign sont également visés par la menace que RiskIQ a donc baptisée «Magecart». Ce dernier fonctionne à la manière d'un logiciel espion, ou keylogger, sur un poste client, mais au niveau d'un serveur web cette fois.

Les chercheurs ne donnent pas de précision sur le mode opératoire des pirates pour installer leur logiciel espion sur les sites victimes. Ils profitent sans doute de vulnérabilités serveurs non corrigées ou – plus inquiétant – de failles zero day (sans correctif). Mais l'installation d'un simple script web suffirait aux attaquants pour activer leur keylogger. Schématiquement, une fois en place dans la page de paiement en ligne, le Javascript permet d'envoyer les contenus des formulaires de commande vers un domaine contrôlé par les pirates et extérieur au site légitime. *« Fondamentalement, ce Javascript agit comme un homme-du-milieu entre l'utilisateur et le processus de paiement à chaque fois qu'une information de carte de crédit est fournie*, explique Sucuri de son côté. *Il permet le traitement original par la plate-forme, mais en même temps, il transmet les données à un domaine malveillant. »* Bref, pour l'internaute mais aussi pour le e-commerçant, les transactions semblent se dérouler sans accroc. Visiblement, le chiffrement de la connexion en HTTPS s'avère inefficace pour protéger les données qu'elle véhicule. Signalons que les pirates utilisent eux mêmes un mode chiffré pour récupérer les données.

Un périmètre d'infections assez large

RiskIQ a identifié une poignée de sites victimes de Magecart, dont ceux du libraire britannique Faber & Faber, du magasin de vêtements de sport Everlast Worldwide, du marchand australien Guess, ou encore du fournisseur d'articles de mode Rebecca Minkoff. La société parle de *« nombreux »* sites de e-commerce victimes des Javascipts malveillants, sans pour autant indiquer un chiffre précis. Mais la popularité des plates-formes de paiement ciblées laisse penser que le périmètre des infections pourrait être assez large.

RiskIQ et Sucuri recommandent aux gestionnaires de sites de e-commerce de toujours tenir à jour leurs plates-formes de panier électronique, de respecter les règles élémentaires de sécurité d'accès aux serveurs (à commencer par la modification régulière des mots de passe), de faire appel à un intégrateur pour s'assurer de la bonne implémentation du module de paiement, etc. Les utilisateurs, eux, peuvent essayer de se protéger en installant des extensions de listes blanches et d'analyse de code à l'image de NoScript pour Firefox, qui prévient l'exécution de scripts douteux. L'usage d'autres formes de paiement, comme les portes-monnaies électroniques à la Paypal (à condition que les identifiants soit pré-saisis) ou les systèmes d'eCarte bancaire (un numéro de carte virtuel et unique à la transaction), devraient aussi les protéger d'une capture de leurs informations de paiement.

Lire également

Les montres connectées à l'écoute de vos claviers
Vol de données bancaires : le malware Dridex cible la France
Que se passe-t-il après un vol de données ?