Les terminaux de paiement cibles des pirates chasseurs de failles

Les terminaux de paiement cibles des pirates chasseurs de failles

Avant le passage à des cartes à puce plus sécurisées, les cybercriminels sont à l'affût de failles dans les anciens systèmes de paiement aux États-Unis, pour continuer à voler des identifiants et des mots de passe. Vu les revenus qu'ils peuvent encore en tirer, l'enjeu reste assurément très attractif.

Selon FireEye, les cybercriminels redoublent d'efforts pour voler les informations des cartes de paiement sur les terminaux des détaillants américains avant la mise en place de nouveaux systèmes de défense.

L'an dernier, plus d'une douzaine de logiciels malveillants différents ciblant les TPV utilisés par de nombreux détaillants pour le traitement des paiements électroniques ont été découverts. Ces dernières années, les pirates ont réussi à pénétrer plusieurs fois dans ces systèmes, ciblant faiblesses ou vulnérabilités des logiciels afin d'extraire les informations qu'ils peuvent revendre sur le marché noir.

Depuis le mois d'octobre dernier, les détaillants endossent la responsabilité des transactions frauduleuses quand les paiements ne sont pas réalisés avec des cartes EMV. Celles-ci ont été dotées d'une puce électronique et bénéficient de meilleures sécurités pour protéger les données inscrites sur la puce. D'importants revendeurs qui ont été victimes de ces usurpations ces dernières années, comme le distributeur américain Target, ont amélioré leurs systèmes. Mais le coût et les retards de livraison des nouveaux systèmes certifiés ont ralenti la transition, laissant encore une marge d'action pour les cybercriminels. Au City Target sur Bush Street à San Francisco la semaine dernière, un achat de moins de 10$ effectué avec une carte à puce française n'a donné lieu à aucune vérification : ni code, ni signature et encore moins d'ID.

Des terminaux toujours très vulnérables aux Etats-Unis

Hier, un chercheur senior de FireEye spécialisé dans l'intelligence et les menaces, Nat Villeneuve, a écrit que plus d'une douzaine de logiciels malveillants de familles différentes ciblant les systèmes TP avaient été découverts l'an dernier. « Aux États-Unis, les criminels sont très actifs et cherchent par tous les moyens à infecter rapidement les systèmes de paiement avant que les détaillants américains n'achèvent la transition vers des systèmes plus sécurisés », a prévenu le chercheur. En réponse, les émetteurs de cartes et les banques ont amélioré leur capacité à identifier et à bloquer les transactions potentiellement frauduleuses. Mais la fraude reste suffisamment lucrative pour inciter les criminels à y consacrer encore beaucoup de ressources.

Nat Villeneuve parle d'un nouveau type de malware appelé POS Treasurehunt, qui vole les données des cartes de paiement à partir de la mémoire d'un ordinateur. « Le mode opératoire classique consiste à implanter Treasurehunt sur un système de TP, soit en utilisant des identifiants déjà volés, soit par force brute, c'est-à-dire en testant des séries de mots de passe courants pour accéder à des systèmes de paiement mal sécurisés », a-t-il écrit. Jusqu'ici, le champ d'action de Treasurehunt a été limité, signe que ses auteurs l'ont déployé sélectivement. Une chaîne de code du malware indique qu'il a été développé par un groupe dénommé Bears Inc. « Bears Inc. est très actif sur un forum dédié à la cybercriminalité souterraine liée à la fraude aux cartes de crédit », écrit le chercheur. « Sur ce forum, Bears Inc. a mis en vente des informations de carte de paiement volées ». Une autre chaîne de code comporte le message suivant : « Bonjour à Xylitol and Co ». Xylitol est le surnom d'un chercheur en malware bien connu, basé en France, qui anime un blog technique très suivi.

Une activité très rentable

Le piratage des TPV est toujours rentable pour les cybercriminels. On trouve facilement des forums de « carding » sur lesquels il est possible d'acheter des identifiants de carte de paiement. Le tarif de ces informations varie en fonction de la date limite d'utilisation de la carte et de la date où les données ont été volées. Les revenus tirés par les cybercriminels semblent tellement intéressants que les prix de ces informations ont même baissé.

Réagissez à cet article

Source : *Les pirates cherchent activement des failles dans les terminaux de paiement – Le Monde Informatique*