Internet : les dangers du Â« RAM scraping Â» comment l'Ã©viter.?

Internet

PostÃ© par : JPilo
PubliÃ©e le : 14/2/2014 13:00:00

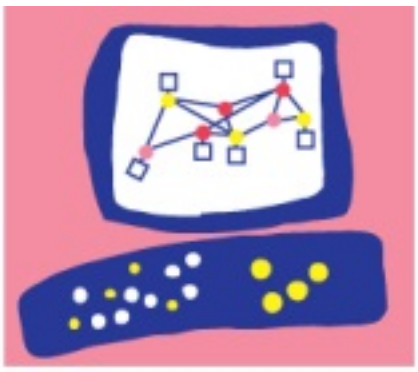
La technique de Â« RAM scraping Â» (collecte de donnÃ©es stockÃ©es en RAM) est Ã l'origine d'un des plus importants vols de donnÃ©es au monde. Comment fonctionne-t-elle et comment les entreprises peuvent-elle s'en protÃ©ger ? Par Thierry Karsenti, Directeur Technique Europe - Check Point Software Technologies

Lorsque nous avons publiÃ© en dÃ©cembre dernier nos prÃ©visions en matiÃ¨re de sÃ©curitÃ© pour 2014, nous indiquions que Â« les campagnes de logiciels malveillants ciblÃ©es ... visant Ã dÃ©rober de l'argent ou de la propriÃ©tÃ© intellectuelle Â» seraient l'une des trois principales menaces pour les entreprises au cours de l'annÃ©e. Nous ne nous attendions certainement pas Ã ce que cette prÃ©diction se rÃ©alise aussi rapidement, ni Ã une telle ampleur.

On estime que les failles de sÃ©curitÃ© des grandes enseignes amÃ©ricaines Target et Neiman Marcus ont permis de dÃ©rober les donnÃ©es personnelles et les donnÃ©es des cartes bancaires de prÃ¨s de 110 millions de clients.

Les enquÃªtes menÃ©es sur ces attaques ont rÃ©vÃ©lÃ© que les caisses enregistreuses des magasins ont Ã©tÃ© infectÃ©es par des outils de Â« RAM scraping Â», qui ont ainsi permis aux agresseurs d'intercepter des donnÃ©es bancaires et autres donnÃ©es personnelles. MÃªme si le Â« RAM scraping Â» n'est pas une nouvelle technique (elle a Ã©tÃ© signalÃ©e pour la premiÃ¨re fois en 2008 par le Centre des technologies de l'information de l'UniversitÃ© de Princeton), son utilisation dans le cadre de ces attaques rÃ©centes soulÃ¨ve des questions sur la sÃ©curitÃ© des transactions par carte bancaire, et de la norme PCI-DSS qui est sensÃ©e protÃ©ger les terminaux de point de vente et les donnÃ©es des cartes bancaires des clients durant leur transfert.

La norme PCI-DSS renforce la sÃ©curitÃ© des transactions jusqu'au stockage des donnÃ©es client sur les systÃ¨mes des marchands, mais elle n'est cependant pas invulnÃ©rable. Au cours d'une transaction, les donnÃ©es de la carte bancaire d'un client, y compris le nom du titulaire de la carte, le numÃ©ro de la carte, sa date d'expiration et son code de sÃ©curitÃ© Ã trois chiffres, sont disponibles en texte brut pendant une trÃ¨s courte pÃ©riode de temps, parce que les systÃ¨mes de traitement des paiements ont besoin de donnÃ©es non chiffrÃ©es. C'est cette fenÃªtre d'opportunitÃ© que les outils de Â« RAM scraping Â» exploitent.



Check Point®
SOFTWARE TECHNOLOGIES LTD.

Une fenÃªtre Ã©troite

Les donnÃ©es de la carte lues par le terminal de point de vente sont temporairement stockÃ©es en mÃ©moire vive durant le processus d'autorisation de la carte et le traitement de la transaction, avant d'Ãªtre chiffrÃ©es. De mÃªme, les donnÃ©es d'une transaction client traitÃ©es par un serveur de back-end sont temporairement dÃ©chiffrÃ©es en mÃ©moire.

Â

Les donnÃ©es sont accessibles pendant une fraction de seconde uniquement, suffisamment longtemps cependant pour l'outil de Â« RAM scraping Â» qui s'active chaque fois qu'une transaction se produit et recherche des numÃ©ros de carte bancaire en RAM lorsque de nouvelles donnÃ©es y sont chargÃ©es.

Les donnÃ©es sont ensuite silencieusement enregistrÃ©es dans un fichier texte, puis transmises aux agresseurs lorsqu'un nombre prÃ©dÃ©terminÃ© d'enregistrements est collectÃ©. Les criminels n'ont ainsi pas besoin de dÃ©chiffrer les donnÃ©es des clients.

On ne sait pas encore prÃ©cisÃ©ment quelles variantes de logiciel malveillant ont Ã©tÃ© utilisÃ©es pour ces attaques, ni comment elles ont Ã©tÃ© introduites dans les systÃ¨mes.

Cependant, dÃ©but janvier 2014, l'organisme US-CERT a Ã©mis une alerte concernant les logiciels malveillants de Â« RAM scraping Â» ciblant les systÃ¨mes de point de vente, en nommant les types de logiciels malveillants actuellement capables de parcourir les zones mÃ©moire utilisÃ©es par les processus spÃ©cifiques des logiciels de point de vente pour trouver les donnÃ©es des cartes bancaires.

Vecteurs d'infection

Comment les criminels ont-ils Ã©tÃ© en mesure d'injecter les outils de Â« RAM scraping Â» dans les systÃ¨mes de point de vente de ces grandes enseignes ? Leurs systÃ¨mes et leurs terminaux de point de vente Ã©tant connectÃ©s par rÃ©seau, l'infection initiale a probablement Ã©tÃ© introduite par des mÃ©thodes classiques : soit par un lien ou une piÃ¨ce jointe malveillante dans un email qui a Ã©tÃ© ouvert par un employÃ© sur le rÃ©seau de l'entreprise, ou par l'exploitation des faiblesses des identifiants de connexion des logiciels d'accÃ¨s Ã distance.

Une fois parvenus dans le rÃ©seau d'entreprise, les agresseurs ont pu transfÃ©rer leurs logiciels malveillants sur le rÃ©seau et les terminaux de point de vente. Les rÃ©seaux de point de vente n'Ã©tant pas isolÃ©s des autres rÃ©seaux d'entreprise, cela les rend vulnÃ©rables.

Protection des points de vente

En termes de protection contre de futures attaques de Â« RAM scraping Â» ou d'autres attaques visant les systÃ¨mes de point de vente, l'organisme US-CERT recommande six meilleures pratiques aux propriÃ©taires et aux exploitants de ces systÃ¨mes :

â¢ L'utilisation de mots de passe sur les systÃ¨mes de point de vente, diffÃ©rents de ceux dÃ©finis dans la configuration par dÃ©faut
â¢ La mise Ã jour des applications logicielles de point de vente, exactement de mÃªme que les logiciels d'entreprise doivent Ãªtre mis Ã jour pour corriger les vulnÃ©rabilitÃ©s
â¢ L'installation d'un pare-feu pour protÃ©ger les systÃ¨mes de point de vente et les isoler des autres rÃ©seaux

â¢ L'utilisation d'un logiciel antivirus maintenu Ã jour
â¢ La restriction de l'accÃ¨s Ã Internet depuis les ordinateurs ou les terminaux de point de vente

pour empÃªcher l'exposition accidentelle Ã des menaces
â¢ La dÃ©sactivation de l'accÃ¨s Ã distance aux systÃ¨mes de point de vente

Les entreprises doivent Ã©galement envisager des contre-mesures supplÃ©mentaires pour ajouter une couche de protection contre les infections de logiciels malveillants, qui sont le point de dÃ©part le plus frÃ©quent des attaques. Il est relativement facile pour les criminels d'ajuster leur code malveillant pour contourner les mÃ©canismes de dÃ©tection des antivirus reposant sur des signatures, ce qui laisse les entreprises vulnÃ©rables. Une technologie de sÃ©curitÃ© telle que l'Ã©mulation ThreatCloud de Check Point permet d'identifier et d'isoler les fichiers malveillants avant qu'ils ne pÃ©nÃ¨trent dans un rÃ©seau, afin d'Ã©viter les infections accidentelles.

En conclusion, le Â« RAM scraping Â» est une menace qui pourrait cibler non seulement le secteur de la distribution, mais Ã©galement tout secteur d'activitÃ© nÃ©cessitant le traitement des cartes bancaires des clients, que ce soit l'hÃ´tellerie, la restauration, ou encore la finance et l'assurance. Les entreprises qui utilisent rÃ©guliÃ¨rement des terminaux de point de vente devraient examiner attentivement leur vulnÃ©rabilitÃ© Ã de telles attaquesâ¦