ALERTE À LA SÉCURITÉ DE VISA

13 novembre 2015

MISE À JOUR – CYBERCRIMINELS CIBLANT LES INTÉGRATEURS DE POINT DE VENTE

Distribution : Revendeurs de produits à valeur ajoutée au PDV, fournisseurs de services aux marchands, fournisseurs, acquéreurs, marchands au point de vente
Qui devrait lire ceci : Responsables de la sécurité de l'information et leur personnel, fournisseurs de services de soutien informatique

Mise à jour : novembre 2015

En octobre 2015, Visa Inc. a été informée de nombreuses nouvelles infections liées à des programmes malveillants affectant divers secteurs d'entreprises partout en Amérique du Nord, notamment :

- **Concessionnaires automobiles**
- **Cabinets dentaires**
- **Terrains de golf**
- **Stations-service**
- **Prêteurs hypothécaires**
- **Restaurants**

En outre, au moins une chaîne de restaurants dans le sud des États-Unis et un intégrateur non inscrit au programme de revendeurs et d'intégrateurs autorisés sont au nombre des victimes de cette infection. Selon les renseignements examinés par Visa Inc., les infections ont commencé à se manifester au mois d'août 2015, et elles semblent avoir augmenté de manière vertigineuse à la mi-octobre 2015. Windows XP et Windows 7 (32 octets et 64 octets) sont les principaux systèmes d'exploitation touchés et des comptes d'utilisateur offrant divers privilèges, notamment celui d'« administrateur » semble avoir été compromis. Visa Inc. travaille activement avec leurs partenaires avec leurs partenaires de l'écosystème afin d'identifier correctement les victimes et de les aviser.

Sommaire du mois de juin 2015

Afin de promouvoir la sécurité et l'intégrité du système de paiements, Visa prépare périodiquement des documents sur la sécurité des données des titulaires de carte et la protection de l'industrie des paiements. Afin de garantir que nous soyons toujours préparés à contrer les nouvelles vulnérabilités informatiques émergentes en matière de cybersécurité, nous vous invitons à consulter l'alerte à la sécurité qui suit.

Visa a constaté une forte hausse des activités d'accès malveillant à distance associées à un accès non autorisé aux points de vente (PDV) des marchands par des intégrateurs au point de vente. Les intégrateurs au point de vente sont des entreprises qui revendent, installent, configurent et voient à l'entretien du logiciel et du matériel au point de vente pour divers types de marchands. Ils procurent souvent un soutien informatique et des services d'entretien par l'entremise de connexions réseau à distance qui, pour la plupart, sont établies par l'intermédiaire de tiers fournisseurs d'accès à distance à partir d'un ordinateur. Lorsqu'elles sont adéquatement sécurisées, ces connexions posent peu de risque pour les marchands. Dernièrement, toutefois, les cybercriminels ont profité de contrôles de

sécurité inadéquats pour accéder aux systèmes au PDV et aux données de cartes de paiement d'un nombre important de marchands.

Depuis au moins janvier 2013 et aussi récemment qu'en mai 2015, LogMeIn s'est servi des médias sociaux et d'autres forums publics pour renseigner ses clients sur des arnaques par hameçonnage connues liées aux attaques de logiciels malveillants. Voir facebook.com/logmein, logmein.com, blog.logmein.com et community.logmein.com pour en savoir plus.

En outre, une récente série d'événements de données de compte compromises ont été retracés à un courriel d'hameçonnage frauduleux de LogMeIn, ce qui est venu compromettre les renseignements de l'utilisateur à l'intégrateur du PDV. Des exemples de courriels frauduleux publiés par LogMeIn figurent ci-dessous. Une fois les renseignements volés, l'attaquant pénètre dans le réseau de l'intégrateur au PDV pour accéder à la clientèle des marchands de l'intégrateur, infectant ainsi les systèmes aux points de vente des marchands au moyen du logiciel malveillant de « RAM scraping » conçu pour récupérer les données de suivi des cartes de paiement.

Campagnes orchestrées pour attaquer les systèmes d'accès à distance

Un certain nombre de solutions d'accès à distance sont couramment utilisées pour fournir une gestion et un soutien à distance aux détaillants (p. ex., LogMeIn, PCAnywhere, VNC et Microsoft Remote Desktop). Utilisées correctement, les applications de gestion à distance sont une façon efficace et rentable de fournir un soutien technique auprès de nombreux marchands. Toutefois, si elles sont exploitées, ces applications exposent potentiellement les données de carte de paiement et autres renseignements sensibles à des cybercriminels. Les applications d'accès à distance, si elles sont déployées de manière non sécurisée, servent d'intermédiaire en permettant aux cybercriminels d'ouvrir une session, d'installer des portes dérobées avec l'installation de logiciels malveillants, souvent avec la possibilité d'enregistrer les frappes, de capturer des éléments audio et vidéo de l'ordinateur concerné et de voler des données de suivi liées aux cartes de paiement. Le risque de compromission des données augmente lorsque les applications d'accès à distance sont configurées d'une façon non conforme à la PCI DSS (Payment Card Industry Data Security Standard).

Au cours des derniers mois, des campagnes d'hameçonnage ont été lancées, mettant l'accent sur les courriels LogMeIn frauduleux conçus pour dérober des identifiants de connexion qui, à leur tour, fournissent aux agresseurs un accès aux réseaux des marchands par l'intermédiaire de ces intégrateurs au PDV. Les courriels renferment souvent un lien malveillant ou un document annexé comportant une charge malveillante. Exemples réels de courriels récemment envoyés aux intégrateurs au PDV pour tenter d'implanter des logiciels malveillants ou de voler des mots de passe et noms d'utilisateur LogMeIn :

Une analyse des fichiers en pièces jointes de ces courriels a révélé que le programme malveillant tente de se connecter à un serveur situé à l'étranger, de télécharger un autre virus, de désactiver des applications antivirus et d'installer des enregistreurs de frappe afin de pouvoir voler les identifiants de connexion, d'injecter un code personnalisé dans des pages web et d'établir la connexion d'accès à distance par « porte dérobée » à des systèmes infectés. L'infection subséquente des systèmes mène alors au vol des données des cartes de paiement par l'entremise d'un virus de récupération des données appelé « RAM scraper » capable d'analyser la mémoire des cartes de paiement.

Virus « FindPOS »

La gamme la plus courante de programmes malveillants au PDV fixés à ces attaques a plusieurs noms, y compris celui de « FindPOS ». Voici deux sites qui expliquent le comportement de ce logiciel malveillant :
http://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/
http://blogs.cisco.com/security/talos/poseidon
Les deux sites contiennent de nombreux indicateurs utiles de compromis. Les intégrateurs au PDV ou leurs partenaires devraient examiner attentivement ces indicateurs dans le cadre de leurs pratiques générales sur la sécurité de l'information.

Mesures d'atténuation

Visa encourage fortement les fournisseurs de traitement, les fournisseurs au point de vente, les revendeurs et les intégrateurs à partager cette alerte avec leurs marchands. Veuillez noter que cette menace est très active et que les acteurs malveillants sont diligemment à la recherche d'autres intégrateurs au point de vente vulnérables aux attaques. Visa mène actuellement une enquête auprès des nombreux intégrateurs où la sécurité a été compromise à l'origine par le service d'accès à distance LogMeIn. Les marchands dont les systèmes au point de vente utilisent les services de LogMeIn de façon continue sont particulièrement à risque. Les marchands devraient examiner immédiatement leur environnement de traitement des paiements afin de déterminer si LogMeIn est déployé dans leurs systèmes de façon conforme.

Les pratiques de sécurité suivantes aideront à atténuer cette menace ainsi que d'autres risques de récupération des données de carte de paiement :

- Utilisez toujours l'authentification à deux facteurs pour l'accès à distance. L'authentification à deux facteurs peut être quelque chose que vous *avez* (un dispositif) ainsi que quelque chose que vous *connaissez* (un mot de passe).
- Assurez-vous que les règles de pare-feu adéquates sont en place, permettant l'accès à distance uniquement à partir des adresses IP connues.
- Si la connectivité à distance doit être utilisée, veillez à l'activer uniquement au besoin. Communiquez avec votre fournisseur ou intégrateur au point de vente afin de prendre les mesures immédiates nécessaires pour désactiver l'accès à distance lorsque vous ne vous en servez pas.
- Restreignez l'accès uniquement au fournisseur de service et seulement au cours d'une période donnée.
- Communiquez avec votre fournisseur de soutien ou au point de vente pour vérifier si un nom d'utilisateur et un mot de passe uniques existent pour chacune de vos applications de gestion à distance.
- Servez-vous de la dernière version d'applications de gestion à distance afin de garantir que les derniers correctifs de sécurité ont été appliqués avant le déploiement.
- Activez la connexion aux applications de gestion à distance et examinez les journaux régulièrement afin de déceler tout signe d'activités inconnues.
- N'utilisez pas de valeur par défaut ou des mots de passe qui se devinent facilement.
- Utilisez uniquement les demandes d'accès à distance qui offrent des contrôles de sécurité renforcés.

- Prévoyez ne plus utiliser des systèmes d'exploitation désuets ou qui ne sont pas pris en charge comme Windows XP.

Voici des exemples de vulnérabilités de l'accès à distance qui permettent à des attaquants d'accéder aux environnements des marchands au PDV. Veuillez noter que la plupart de ces exemples sont des violations de la norme PCI DSS.

- **Services d'accès à distance utilisés en permanence et offerts sur Internet.** Un attaquant n'a qu'à effectuer une analyse du port dans l'espace d'une adresse IP du marchand pour détecter des cibles potentielles. Des applications d'accès à distance en usage continu sont particulièrement à risque d'une attaque.
- **Authentification unifactorielle.** Les accès à distance peuvent être vulnérables à des attaques par force brute et de découverte d'un mot de passe**,** particulièrement lorsque l'authentification nécessite uniquement un nom d'utilisateur et un mot de passe.
- **Applications et systèmes désuets ou non protégés.** Les anciennes versions logicielles de systèmes d'exploitation et d'applications sont reconnues pour être vulnérables aux attaques et sont facilement exploitables pour obtenir un accès non autorisé.
- **Utilisation de mots de passe par défaut ou d'aucun mot de passe.** L'utilisation de mots de passe et de paramètres par défaut pour accéder aux éléments du système d'accès augmentera les possibilités de compromission. Les nouveaux dispositifs et logiciels sont habituellement livrés avec des paramètres par défaut. Ces paramètres par défaut doivent être modifiés avant le début du déploiement, car ils peuvent être facilement devinés et les renseignements de ces paramètres sont facilement accessibles sur Internet.
- **Utilisation de noms d'utilisateurs et de mots de passe communs.** Il arrive souvent qu'un fournisseur de services se serve d'un mot de passe et d'un nom d'utilisateur communs pour plusieurs succursales d'un client afin de faciliter les visites de service.
- **Pare-feu mal configurés.** Dans certains cas, le système au point de vente se sert d'une adresse IP publique directement accessible par Internet.

Programme de revendeurs et d'intégrateurs autorisés PCI

Le programme de revendeurs et d'intégrateurs autorisés PCI offre une formation et des pratiques exemplaires afin de garantir une installation sécuritaire des systèmes de paiement chez les marchands. Le programme identifie et encourage les intégrateurs et les revendeurs autorisés à installer leurs applications PA-DSS validées de manière à faciliter la conformité à la norme PCI DSS.

Un revendeur et un intégrateur autorisés PCI bénéficient des avantages suivants :

- Obtiennent une certification reconnue (valable pendant trois ans)
- Figurent dans la liste des experts mondiaux d'intégrateurs et de revendeurs autorisés des marchands
- Reçoivent une formation spécialisée des experts en matière de conformité à la PCI SSC sur les directives de mise en oeuvre et d'entretien des applications de paiement
- Reçoivent des crédits CPE
- À compter du 1er juin 2015, Visa ajoutera des intégrateurs et des revendeurs autorisés à son registre mondial de fournisseurs de services

Pour obtenir plus d'information et pour présenter une demande, veuillez visiter le www.pcisecuritystandards.org/training, appeler le +1 781 876-6231 ou envoyer vos questions par courriel à qir@pcisecuritystandards.org .