Attention ! Le Cloud est espionné

	Attention ! Le Cloud est espionné

Les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Si vous n'êtes pas propriétaire du hardware, vous n'êtes pas propriétaire des données, selon une étude de Bitdefender.

L'éditeur de solutions de sécurité informatique affirme que les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Les révélations de l'affaire Snowden sur les capacités d'interception des données de la part de la NSA et de ses agences partenaires ont incité les propriétaires d'infrastructures et les fournisseurs de services, ainsi que les utilisateurs, à s'assurer que leurs données sont échangées sans encourir de risque de confidentialité et qu'elles sont stockées sous forme chiffrée. Régulièrement, les chercheurs s'attaquent à des protocoles très utilisés ou à leur mode de mise en œuvre. Des failles sont ainsi découvertes de manière récurrente et corrigées à plus ou moins brèves échéances, comme dans le cas de vulnérabilités bien connues telles que Heartbleed ou Logjam, qui ont entraîné le déploiement massif de correctifs à une échelle jusque-là inédite.
Mais les entreprises, et par conséquent, leurs clients, sont-elles vraiment protégées une fois que ces failles sont corrigées ? Existe-t-il des méthodes dissimulées et plus ou moins légales que les organismes d'État et certaines grandes entreprises bien informées seraient susceptibles d'utiliser pour passer outre les protocoles TLS / SSL, censés protéger les échanges d'informations ? Bref, espionnage dans le Cloud possible ?
Le 26 mai 2016, lors de la Conférence HITB à Amsterdam, Radu Caragea, Chercheur en sécurité des Bitdefender Labs, a démontré lors d'un POC (preuve de concept), que la communication protégée peut être déchiffrée en temps réel, en utilisant une technique qui ne laisse pratiquement aucune empreinte et qui reste invisible pour presque tout le monde, sauf peut-être pour des auditeurs de sécurité particulièrement vigilants.

Espionnage dans le cloud : Quelles conséquences pour votre sécurité ?
Cette attaque permet à un fournisseur de services cloud mal intentionné (ou sur lequel on a fait pression pour qu'il donne des accès à des agences gouvernementales) de récupérer les clés TLS utilisées pour chiffrer chaque session de communication entre votre serveur virtualisé et vos clients (même si vous utilisez Perfect Forward Secrecy !). Si vous êtes un DSI et que votre entreprise externalise son infrastructure de virtualisation auprès d'un prestataire de service, considérez que toutes les informations circulant entre vous et vos utilisateurs ont pu être déchiffrées et lues pendant une durée indéterminée.
Il est impossible de savoir dans quelle mesure vos communications ont pu être compromises et pendant combien de temps, puisque cette technique ne laisse aucune trace anormale derrière elle. Les banques et les entreprises qui gèrent des dossiers de propriété intellectuelle ou des informations personnelles, ainsi que les institutions gouvernementales sont les secteurs susceptibles d'être particulièrement touchés par cette faille.

Espionnage dans le Cloud : Premières découvertes
Cette nouvelle technique, surnommée TeLeScope, a été développée par l'éditeur dans le cadre de ses recherches et permet à un tiers d'écouter les communications chiffrées avec le protocole TLS, entre l'utilisateur final et une instance virtualisée d'un serveur. Cette technique n'est opérationnelle qu'avec les environnements virtualisés fonctionnant au-dessus de l'hyperviseur. Ces infrastructures sont extrêmement répandues et sont proposées par les géants de l'industrie tels qu'Amazon, Google, Microsoft ou DigitalOcean, pour ne citer qu'eux. Si la plupart des experts de l'industrie s'accordent pour dire que la virtualisation est l'avenir, aussi bien en termes de stockage, que de déplacement et de traitement de gros volumes de données, ce type de solutions fait déjà partie du quotidien de nombreuses entreprises.
Plutôt que d'exploiter une faille dans le protocole TLS, cette nouvelle technique d'attaque repose sur l'extraction des clés TLS au niveau de l'hyperviseur par une inspection intelligente de la mémoire. Même si l'accès aux ressources virtuelles de la VM est une pratique déjà connue (accéder au disque dur de la machine, par exemple), le déchiffrement en temps réel du trafic TLS, sans mettre en pause la machine virtuelle de manière flagrante et visible, n'avait jamais été réalisé jusqu'alors.
La découverte de ce vecteur d'attaque a été possible en recherchant un moyen de surveiller des activités malveillantes depuis le réseau de honeypots de l'éditeur, sans altérer la machine et sans que les pirates puissent comprendre qu'ils sont surveillés. Un administrateur réseau ayant accès à l'hyperviseur d'un serveur hôte pourrait surveiller, exfiltrer et monétiser toutes les informations circulant depuis et vers le client : adresses e-mail, transactions bancaires, conversations, documents professionnels confidentiels, photos personnelles et autres données privées.

Espionnage dans le Cloud : Comment cela fonctionne-t-il ?
Normalement, la récupération des clés à partir de la mémoire d'une machine virtuelle nécessiterait de mettre en pause la VM et de décharger le contenu de sa mémoire sur un fichier. Ces deux processus sont intrusifs et visibles par le propriétaire de la VM (de plus ils enfreignent le SLA – Service Level Agreement). L'approche des chercheurs repose sur les mécanismes de Live Migration, disponibles au sein des hyperviseurs modernes, qui nous permettent de réduire le nombre de pages nécessaire pour le vidage de la mémoire de l'ensemble de la RAM, à celles modifiées lors de l'établissement d'une liaison TLS.
« ***Au lieu de mettre la machine en pause (ce qui entraînerait une latence notable) et de réaliser un vidage complet de la mémoire, nous avons développé une technique de différentiel de la mémoire qui utilise des fonctions de base déjà présentes dans les technologies de l'hyperviseur,*** » explique Radu Caragea. « ***Ensuite, bien que cela permette de réduire le volume de vidage mémoire de giga-octets à méga-octets, le temps nécessaire pour écrire une telle quantité de données sur un espace de stockage reste non négligeable (de l'ordre de quelques millisecondes) et c'est pourquoi nous montrons comment 'déguiser ' le processus pour le faire passer pour une latence du réseau, sans qu'il soit nécessaire de stopper la machine.*** »

Atténuation des risques
L'attaque TeLeScope n'exploite pas de faille lors de l'implémentation du protocole TLS et ne tente pas de contourner le niveau de chiffrement de l'implémentation TLS via des attaques par repli (downgrade attacks). Au lieu de cela, elle exploite une caractéristique de l'hyperviseur pour exfiltrer les clés utilisées par le protocole pour chiffrer la session. Notre POC révèle un écart fondamental qui ne peut être corrigé ou atténué sans réécrire les bibliothèques de cryptographie qui sont déjà en cours d'utilisation. La seule solution à ce jour est, en premier lieu, de bloquer l'accès à l'hyperviseur – en exécutant votre propre hardware à l'intérieur de votre propre infrastructure.
Article original de Damien BANCAL

Réagissez à cet article

Original de l’article mis en page : ZATAZ Espionnage dans le Cloud – ZATAZ