



Communiqué de presse

Contacts :

Agence

'Just Say It PR' Le Savoir Dire

Sandra Logut

01 44 61 81 84

sandra@just-say-it.com

WatchGuard

Rym Sullivan

06 72 32 85 47

Rym.Sullivan@watchguard.com

Menaces sur les réseaux VoIP selon WatchGuard

Paris, le 11 mai 2009 – WatchGuard Technologies, un acteur mondial spécialiste des solutions de sécurité et de connectivité réseau évolutives, prévient : le vif essor de la technologie VoIP en fait une cible privilégiée pour les hackers.

Des rapports publiés récemment prévoient que près de 75 % des lignes téléphoniques à usage professionnel utiliseront la technologie VoIP (Voice over IP) dans les deux prochaines années. Selon ces mêmes rapports, la moitié des PME et deux tiers de l'ensemble des entreprises vont utiliser des réseaux VoIP. D'ici la fin de cette année, le nombre total d'abonnés VoIP dans le monde (particuliers et commerciaux) devrait atteindre près de 100 millions d'utilisateurs. En raison de son omniprésence, la technologie VoIP devient rapidement un important vecteur de menaces pour les entreprises. Voici les principales menaces pour les réseaux d'entreprise utilisant la VoIP :

- **Déni de service (DoS)** – De manière similaire aux attaques par déni de service sur les réseaux de données, les attaques par DoS sur VoIP exploitent la même tactique, qui consiste à lancer de nombreuses requêtes (par exemple, demandes d'appel et enregistrements) jusqu'au point de défaillance des services VoIP. Ces types d'attaques ciblent souvent des extensions SIP (Session Initiation Protocol) qui finissent par épuiser les ressources des serveurs VoIP, ce qui provoque des signaux d'occupation ou des déconnexions.
- **Spam over Internet Telephony (SPIT)** – Tout comme la majorité du spam classique (courrier électronique), le SPIT peut être généré de manière similaire avec des réseaux de bots visant des millions d'utilisateurs VoIP à partir de systèmes compromis. À l'instar de ceux indésirables, les messages SPIT peuvent ralentir le fonctionnement des systèmes, engorger les boîtes vocales et entraver la productivité des utilisateurs.
- **Détournement de trafic** – Un tel détournement se produit lorsqu'un utilisateur non autorisé obtient accès à un réseau VoIP, en général à l'aide d'un nom d'utilisateur et d'un mot de passe valides, ou parvient à disposer physiquement d'un périphérique VoIP, et lance des appels sortants. Il s'agit souvent d'appels téléphoniques internationaux pour tirer parti des capacités longue distance VoIP.
- **Détournement d'enregistrement** – Il consiste pour un hacker à désactiver l'enregistrement SIP d'un utilisateur connu, et à le remplacer par l'adresse IP du

hacker. Ce dernier peut ainsi intercepter par la suite les appels entrants et les rediriger, les réécouter ou les interrompre à sa guise.

- **Eavesdropping (« Oreille indiscreète »)** – Tout comme les paquets de données, les paquets voix font l'objet d'attaques de type « man-in-the-middle » consistant pour un hacker à usurper l'adresse MAC de deux parties, et à contraindre les paquets VoIP à circuler via le système du hacker. Le hacker peut ainsi reconstituer ensuite les paquets et bel et bien écouter les conversations en temps réel. Ce type d'attaque permet également aux hackers de dérober toute une gamme d'informations sensibles (par exemple, noms d'utilisateurs, mots de passe et données système VoIP).
- **Vol d'adresses électroniques** – Ce type d'attaque se produit lorsqu'un hacker tente de découvrir des adresses VoIP valides en menant des attaques de cassage sur un réseau. Lorsqu'un hacker envoie des milliers d'adresses à un domaine VoIP particulier, la plupart de ces adresses sont retournées comme non valides mais, parmi celles qui ne le sont pas, le hacker peut identifier des adresses VoIP valides. Le pillage de l'annuaire d'un utilisateur VoIP permet au hacker d'obtenir une nouvelle liste d'abonnés VoIP susceptibles de devenir de nouvelles cibles pour d'autres menaces, telles que le SPIT ou des attaques de vishing.
- **Vishing (Voice Phishing)** – Le vishing reproduit des formes classiques du phishing, à savoir des tentatives pour inciter des utilisateurs à divulguer des données personnelles et sensibles (par exemple, noms d'utilisateur, mots de passe et numéros de compte). Ici il s'agit de spam ou de SPIT pour leurrer les utilisateurs afin qu'ils appellent leur banque ou fournisseur de service pour vérifier des informations de compte. Une fois des données utilisateur valides communiquées, le hacker peut les vendre à des tiers ou, dans de nombreux cas, détourner directement des fonds sur des cartes de crédit ou des comptes bancaires.

En raison de ces menaces qui croissent rapidement, WatchGuard recommande aux entreprises utilisant des systèmes VoIP d'examiner leurs périmètre et sécurité VoIP pour s'assurer qu'elles disposent bien des solutions de protection les plus efficaces.

Mots-clés :

Voice over IP, risques de sécurité VoIP, déni de service (DoS) VoIP, SPIT, détournement de trafic, détournement d'enregistrement SIP, eavesdropping, vol d'adresses électroniques, vishing

Citations :

« Tout comme les réseaux de données ont succombé à des menaces pernicieuses, les systèmes VoIP sont confrontés au même péril », déclare Eric Aarrestad, Vice-président en charge du marketing chez WatchGuard Technologies. « Les entreprises poursuivant une phase de convergence des réseaux et d'adoption de la technologie VoIP, quelle que soit leur taille, doivent faire évoluer leur architecture de sécurité pour assurer la protection de leurs clients, utilisateurs et données contre les menaces à l'encontre de la VoIP ».

À propos de WatchGuard Technologies, Inc.

Depuis 1996, WatchGuard® Technologies, Inc. fournit des solutions de sécurité réseau, et permet à des centaines de milliers d'entreprises dans le monde entier de protéger leurs systèmes d'information. La gamme WatchGuard de boîtiers de gestion unifiée des menaces, câblés ou sans fil, et de solutions d'accès à distance VPN SSL permet une sécurité réseau évolutive, un contrôle réseau inégalé ainsi qu'une administration

complète. Les produits WatchGuard sont supportés par le service WatchGuard LiveSecurity® et des programmes innovants en termes de support, maintenance et formation. WatchGuard, dont le siège se trouve à Seattle (États-Unis), possède des bureaux en Amérique du Nord, Europe, sur la région Asie-Pacifique et en Amérique latine. Pour en savoir plus, rendez-vous sur <http://www.watchguard.fr>