Communiqué de presse

Worm SQL Saphhire : Security Keepers détecte et notifie l'attaque en première mondiale

Acteur incontournable du marché de la sécurité, les solutions Security Keepers en place chez les clients ont protégé ceux-ci et ont permis, parallèlement de détecter et diagnostiquer cette attaque. La notification transmise par Security Keepers au CERT a été la plus précoce en ce matin du 25 janvier 2003.
L'attaque débutée, selon nos information à 05H29:42 UTC a été diagnostiquée, par notre Security Center à 05H35 UTC et les procédures de réponse ont été mises en place immédiatement dans le Security Center, centre de sécurité et de supervision distante 24/7 de Security Keepers.

Paris, le 25 janvier 2003 : Il s'agit d'une des attaques les plus lourdes qu'ait connu Internet, sinon la plus lourde. Elle repose sur la propagation massive d'un vers utilisant une vulnérabilité des serveur MS-SQL assez ancienne (voir advisory CERT CA-2003-04 de Juillet).
Ce vers se diffuse aux machines vulnérables (MS-SQL server non patché) par un mode de diffusion aléatoire lourd, reposant sur des tentatives de connections sur le port UDP 1344. Le mode de scanning des adresses faisant appel à une résolution DNS, la surcharge de ces requêtes a engendré une saturation du réseau mondial, aboutissant à la panne par saturation (déni de service : DDOS) de plusieurs des treize K-Root serveurs mondiaux.

"Les tentatives de propagation de ce vers ont toutes été bloquées chez nos clients et ceux-ci ont été ainsi protégés à un premier niveau. Dans un second temps, notre stratégie a été de sauvegarder les bandes passantes des accès Internet de ces clients en agissant sur les réponses à ce trafic. Cette stratégie a été efficace et a permis de diminuer les charges constatées chez nos clients d'un facteur dix.
Par la suite, nous avons collaboré avec des opérateurs hébergeant certains de nos clients en leur apportant des informations techniques sur cette attaque afin de les aider à protéger les réseaux encore fonctionnels ou de favoriser la remise en route des réseaux en panne." explique François Raisky, Président du Directoire de Security Keepers.

La réponse à ces attaques mise en place par Security Keepers, montre la nécessité absolue d'une réponse dynamique à ce type de problèmes.
La sécurité des réseaux repose en effet sur la capacité de réponse aux attaques et non pas uniquement sur une protection statique, non adaptative.

"Ce type d'attaque voit sa fréquence augmenter depuis deux ans. Les conséquences majeures de ces attaques et le manque à gagner générer par ces paralysies partielles de certaines entreprises confirme notre approche dynamique et réactive des problèmes.
La réactivité de nos équipes tient à la coopération entre un système de diagnostic automatisé, temps réel par intelligence artificielle des attaques et une équipe spécialisée en sécurité des réseaux présente 24h sur 24 dans notre centre.
Les réponses à ce type d'attaques se doivent d'être adaptatives et ne saurait reposer uniquement sur des équipements de sécurité statiques, le réseau Internet étant aujourd'hui trop complexe et trop critique pour pouvoir être géré en mode automatisé." poursuit François Raisky.

Les clients de Security Keepers bénéficient de cette approche depuis plusieurs années et ce service tout compris permet d'approcher la protection des réseaux comme un service à coût constant avec une efficacité précise.

A propos de Security Keepers

Security Keepers est un acteur incontournable dans le domaine de la sécurité informatique. Fort de son capital humain expérimenté dans les réseaux et les systèmes en environnement Linux, il propose une approche originale et transversale des besoins de l'entreprise utilisatrice. Security Keepers inclut l'ensemble des aspects concernés (matériel, logiciel et services) du point de vue de l'entreprise dans les solutions qu'elle propose.

Née du constat que les entreprises étaient à la recherche de solutions de protection efficaces pour leur réseau tout en ne possédant pas en interne les moyens de répondre efficacement à cette problématique, Security Keepers a été créée début 1999 par François Raisky, ancien DSI d'un groupe international.

Son actionnariat privée et son indépendance totale sont les garants d'une impartialité complète mise au service des clients.

Plusieurs années de Recherche & Développement ont permis de concevoir, développer et mettre au point le produit EverProtect qui réunit des technologies de pointes et innovantes.

Les solutions EverProtect sont déjà commercialisées auprès d'une trentaine de clients comme le Groupe Carrefour-Promodés, le Groupe Picard Surgelés, Union-SDA – Beghin-Say,, HPC – Groupe Crédit Agricole, Groupe ACES (aéronautique).

Security Keepers

François Raisky
Président Directeur Général
Tel. : 01 47 70 38 84 – Fax : 01 47 70 08 50 – e-mail : francois.raisky@securitykeepers.com

Georges Bell
Directeur Général
Tel. : 01 47 70 08 01 – Fax : 01 47 70 08 50 – e-mail : georges.bell@securitykeepers.com