Quelques jours suffisent à hacker une faille sur Windows? ce jour ?

Etonnante et inquiétante expérience qui se déroule sous nos yeux ! En trois étapes, nous assistons à la naissance d'une famille de vers ou virus, sans que nous sachions encore ce qui en résultera. Rappelons les faits?

Samedi 14 février, le site français K-Otik consacré à la sécurité publie le code d'une faille sur la librairie ASN.1 de Microsoft Windows, qui '*pourrait*' permettre de créer une attaque par déni de service en forçant le '*reboot*' de l'ordinateur. **Une faille sur Windows ASN.1 Library** ASN (*Abstract Syntax Notation*) est un standard international pour afficher différents types de données binaires, comme des chaînes de caractères ou des chiffres. ASN.1 Library est exploité dans de nombreuses applications Windows. ASN.1 cible un protocole d'authentification de Windows, *NT LAN Manager V2* (NTLMV2) qui permet à des postes distants de se connecter sur un réseau. Ce dernier est présent par défaut sur de nombreux postes en environnement Windows. **L'information circule sur les forums** Dès sa publication, l'information est relayée par de nombreuses communautés, et le code de la faille, toujours en ligne au moment où nous publions cet article, a sans doute dû circuler aussi rapidement. Les experts, dans un premier temps, minimisent le risque, car à la différence du code de *Distributed component object model* (DCOM) qui a permis le développement du ver Blaster, LAN.1 ne permettrait pas d'exécuter du code, ni d'accéder à des fichiers sur les machines vulnérables. De plus, la nature de la vulnérabilité de ASN.1 rendrait son exploitation autrement plus difficile que celle de DCOM, car une éventuelle attaque ne disposerait d'aucun contrôle à travers la mémoire de l'ordinateur. **Le week-end pour exploiter le code** Seulement voilà, dès **lundi 16 février**, la société iDefense, qui scanne en permanence les forums à la recherche d'informations, voit passer des messages inquiétants sur des développements en cours d'un programme capable d'exploiter la vulnérabilité de ASN.1. Malgré l'avis des experts, et d'ailleurs avant même la publication de leur avis, une information circulerait sur la technique permettant à un hacker de prendre le contrôle d'un poste distant. **En attendant les premières attaques?…** Ce **mercredi 18 février**, les premiers retours sur des attaques exploitant la faille de ASN.1 sous Windows seraient attendus dans la journée. En principe, le risque est quasiment nul sur les postes à jour sur les patchs de Microsoft Windows (la faille a été signalée voici déjà plusieurs mois) et toute attaque devrait être bloquée par un *firewall*. Mais le risque demeure, surtout chez les particuliers disposant d'une connexion haut débit, mais qui ne sont pas à jour et peu au fait de la sécurisation de leur ordinateur. A suivre dans les heures et jours à venir?