Virus : que se passe-t-il avec Zotob and co ?

Il aura fallu moins d'une semaine pour que la faille révélée par Microsoft sur l'environnement Plug-and-Play de Windows soit exploitée par les 'hackers'. Au '

Patch Tuesday' de Microsoft, mardi 9 août, a succédé, dès mercredi 10 août, la publication – par un russe anonyme sous le pseudo '*Houseofdabus*' – du code d'exploitation de la faille sur les machines sous Windows 2000. Le ver Zotob.A est apparu le dimanche 14 août. Silicon.fr a publié l'information le 15 août (Alerte au ver Zotob.A). Pas d'exploit particulier hormis la rapidité de réaction, un inconnu a incorporé le code d'exploitation dans un '*bot*', un ver qui se répand automatiquement. Sven Jaschan avait fait de même avec Sasser ! Le mercredi 17 août, une nouvelle menace commençait à faire parler d'elle, IRCbot, conçue sur le même modèle que Zotob. Une menace plus grande encore que son prédécesseur, puisque McAfee affirmait que IRCbot « *bat tous les records de propagation*« . Le 17 août, Trend Micro annonçait que six vers exploitant la même faille sur le Plug-and-Play de Windows 2000 étaient actifs : Zobot.C, Zobot.D, RBOT.CBQ, RBOT.CBR, SDBOT.BZH et DrugeBot.A. Depuis, une vague de vers est venue menacer les systèmes **Windows 2000**, sans que l'on sache bien si la menace a l'envergure qu'on lui attribue, ou s'il ne s'agit pas plutôt du réveil des éditeurs et de la presse après les vacances. **Une origine commune, une menace cumulée** Point commun entre toutes ces attaques virales: elles exploitent **la même faille sur Windows**, révélée par l'éditeur lors de ses dernières mises à jour, l'alerte MS05-039 du 9 août qui révélait **la vulnérabilité Plug-and-Play de Windows 2000**. Les hackers se sont précipités sur la faille et ont lancé leurs vers. Facile, on leur a généreusement fourni le code ! Ce type de ver, autonome, se répand en scannant les machines via le port 445/TCP. Lorsqu'une victime est identifiée, ce ver utilise le code d'exploitation afin de télécharger le dossier principal du virus via FTP. Il met alors en place un serveur FTP sur la machine infectée et commence à scanner à partir de celle-ci afin de trouver d'autres victimes et se répandre. Les hackers se sont, semble-t-il, donné le mot et le code de '*Houseofdabus*' s'est retrouvé dupliqué, soit directement dans des souches virales, Zotob, IRCbot, Bozori, soit sur des variantes de ces derniers, qui se multiplient et amplifient la menace, très **concentrée sur les grandes organisations implantées aux Etats-Unis**. On a du mal à imaginer Zotob et confrères en menace planétaire, car le ver ne s'attaque qu'aux systèmes Windows 2000. Certes, celui-ci est encore présent sur de nombreux postes. En particulier, et cette information a participé à la médiatisation de l'attaque, chez les géants américains des médias ABC, CNN, The Associated Press et The New York Times (qui révèlent l'ampleur de l'obsolescence de leur parc informatique). Mais aussi DaimlerChrysler, Kraft Foods, UPS, General Electric Caterpillar ou le Congrès des Etats-Unis. Selon F-Secure, l'infection trouve très probablement son origine dans les **ordinateurs portables contaminés** qui se connectent ensuite au réseau de l'entreprise, à l'intérieur du périmètre du 'firewall'. Sans vouloir polémiquer, le seul enseignement que nous révèle l'information, c'est que ces sites de médias, d'industries et d'administrations sont bien mal protégés, et plutôt en retard pour la mise à jour de leurs protections ! En effet, rappelons-le, la faille ne permet d'infecter que les machines fonctionnant sous Windows 2000 et non protégées par un firewall. Au discours sur la gravité des attaques, nous pourrions objecter la gravité de l'absence de défense à jour ! **Le danger est réel, mais probablement surévalué** Le danger est cependant réel pour les contaminés. Pour McAfee, ces vers sont capables de lancer des attaques par déni de service (DoS), mais leur plus grand danger provient de leur capacité à agir sans intervention

humaine. Pour l'éditeur d'antivirus Kaspersky, le danger provient de leur capacité à prendre le contrôle du poste infecté pour expédier du 'spam', des 'malwares', dérober des données personnelles, ou de nouveau des attaques par 'DoS'. Un vrai zombie ! L'ampleur de la menace prendrait en partie sa source dans la multiplication des variantes, un phénomène aggravé par le manque de coordination des éditeurs de solutions de protection virale. Lorsque par exemple Trend Micro annonce 6 'bots' (vers qui se propagent via un réseau d'ordinateurs 'zombies'), qu'il évoque Zotob.C et Zotob.D, sont-ce les mêmes vers que Zotob.A ou Zotob.B, ou sont-ce des vers différents ? De même, RBOT.CBQ n'est-il pas IRCBot, ne se propagent-ils pas tous deux sur le canal IRC ? Dernière menace en date, **Bozori**. Ce ver est un ennemi de Zotob, qui lorsqu'il s'installe élimine les infections provenant de ses concurrents. Tout aussi menaçant sous des allures d'ange exterminateur, il prend le contrôle des postes compromis. **De la paranoïa médiatique à la réalité, une menace en cache une autre?** Concrètement, en faisant le cumul des attaques confirmées par les laboratoires des éditeurs de solutions antivirus, 11 vers exploitant la faille de Windows 2000 ont été déclarés jusqu'à ce jour, vendredi 19 au matin. Et précisément, la menace est réduite, car elle ne vise que des systèmes Windows 2000, anciens et qui tendent à se raréfier. Il y a en revanche un véritable danger qui émerge de cette vague médiatique? Les hackers ne cherchent plus les failles, ils se contentent désormais d'attendre qu'on leur indique le chemin. Là est le véritable danger de l'affaire Zotob, moins d'efforts mais plus de volumes et plus rapidement pour envahir la planète. Et dernière nouvelle: on vient de repérer un Esbot.A, même modèle que ses concurrents, même menace sur des vieux postes Windows 2000. Il n'y a que la couleur de la carrosserie qui change, à l'intérieur, c'est tout pareil ! **Des solutions gratuites pour se protéger**

Tout d'abord, bien évidemment, mettre à jour Windows. **Plus de 90% des vers et virus peuvent être tenus en échec en maintenant son système à jour !** Le bulletin de sécurité MS-039 est disponible sur le site de Microsoft. A télécharger sur le site de Microsoft TechNet. Microsoft qui propose pour les postes qui craignent d'être infectés, un outil de nettoyage des '*malware*' pour éradiquer Zotob, mais aussi d'autres menaces comme Blaster, Sasser ou MyDoom. A télécharger sur le site de Microsoft Security. Panda Software, qui qualifie l'alerte virale des vers Zotob et IRCBot de niveau orange, propose des applications gratuites PQRMOVE, qui détectent et éliminent définitivement toutes les variantes de Zotob, IRCBot et KD. A télécharger sur le site de Panda Software. Trend Micro propose son service de recherche de virus HouseCall. En accès sur le site HouseCall.