La source du ver « Witty » est-elle identifiée ?

Trois universitaires américains ont, cette semaine, relancé l'histoire de « Witty » : ils déclarent avoir identifié la source du »

malware » après plusieurs mois d'enquête et d'analyses. L'originalité de ce ver a poussé Abhishek Kumar, Vern Paxson et Nicholas Weaver à l'étudier dans les moindres détails. Leur rapport vient d'être publié. **Une course contre la montre ?** Le 8 Mars 2004, eEye Security découvre une vulnérabilité triviale de type « *stack overflow*» affectant plusieurs produits de la société ISS. Dans la foulée, eEye avertit l'éditeur. Le 9 Mars un correctif est disponible pour l'ensemble des clients ISS. Le 18 Mars, eEye annonce alors publiquement sa découverte. Dans la soirée du 19 Mars 2004, le ver « Witty » apparaît sur la Toile. C'est ce « delta » minime entre l'annonce officielle de la vulnérabilité et la mise en circulation du ver qui interloque bon nombre d'experts. En effet, n'aurait-il fallu que 48 heures au créateur de « Witty » pour développer ce ver particulièrement sophistiqué et destructeur ? **Des hypothèses à foison** Le pirate aurait pu découvrir la vulnérabilité avant que la société eEye ne la rende publique ou même la mette en évidence. Dans ce cas, pourquoi avoir attendu ce moment précis pour libérer le ver ? Pourquoi lâcher la bête alors qu'un correctif vient juste d'être développé et distribué aux clients ISS ? Le pirate aurait également pu utiliser des méthodes de « *reverse engineering* » sur le correctif publié par ISS le 9 Mars. Ce qui lui aurait laissé près de 10 jours pour développer le ver. Plausible. Mais encore une fois, pourquoi lancer l'attaque alors qu'un correctif est disponible ? D'autant plus que la charge active du ver a pour unique vocation la destruction de données et témoigne d'une réelle volonté de nuire au plus grand nombre. Nous pourrions également imaginer que le pirate aurait eu accès, d'une manière ou d'une autre, aux systèmes informatiques de ISS ou d'eEye. Il se serait alors emparé des informations concernant la vulnérabilité découverte le 8 Mars et aurait développé tranquillement sa bestiole. **L'oeuvre d'un inconditionnel opportuniste?** Autre hypothèse, l'assaillant pourrait être un inconditionnel opportuniste qui parierait sur le fait qu'une telle vulnérabilité puisse être découverte et aisément exploitée. Il développerait alors un véritable 'framework' (ensemble de briques logicielles) permettant de construire le ver en un temps record puis de le lâcher dans la nature. Dans ce cas, pourquoi utiliser une charge active aussi radicale et ravageuse ? En utilisant un «*payload*» différent, il aurait pu tirer plus de profits d'un nombre incalculable de machines sous ses ordres. Bref, les motivations de l'auteur du ver « Witty » restent encore obscures, bien que l'intention de nuire soit manifeste. Cependant, sur un plan purement technique, on commence à voir plus clair dans le mode opératoire de l'attaque. **Originaire d'Europe…** L'étude réalisée par les trois universitaires aurait permis de remonter à la source du ver. Il s'agirait d'une machine « piratée » et localisée en Europe. L'adresse IP incriminée aurait été transmise aux autorités compétentes. Cette machine aurait fait office de « rampe de lancement » pour le '*malware*'. Un programme spécifique ainsi qu'une liste pré-établie de machines potentiellement vulnérables y furent déposés. De là est parti « Witty », il aurait fait 12.000 victimes. La première serait le système d'information d'une base de l'armée américaine. D'après le rapport, c'est bien cette cible que voulait atteindre en priorité l'auteur du ver. A l'heure d'aujourd'hui, la cellule X-Force d'ISS ne souhaite pas commenter le rapport. Toutefois, selon elle, les arguments de ce dernier ne seraient que pures spéculations. Le

ver « Witty », lui, existe bel et bien. (*) **pour Vulnerabilite.com**