Virus : Kama Sutra a fait beaucoup de bruit pour rien…

Contacté, le Club de la sécurité des systèmes d'information français (Clusif) estime qu'il ne s'est rien passé, et que

« certains concepteurs et éditeurs de logiciels de sécurité ont joué la carte de l'alarmisme ». Le club indique même non sans humour avoir reçu un mail d'une société lui expliquant *« nous présentons une exécution massive de ce ver. Plusieurs centaines de milliers sont touchées et il va faire des ravages en France »* une information erronée qui a pour unique objectif de faire paniquer l'internaute mal informé. Malgré cela, le Clusif ne veut pas jeter l'opprobre sur les éditeurs car il existe tout de même des sociétés qui ne profitent pas des sujets porteurs pour vanter leurs produits. Pour François Paget, membre actif du Club et membre fondateur du groupe AVERT (AntiVirus Emergency Response Team) au sein de McAfee : *« Le virus vérifiant le jour actuel toutes les 30 minutes, l'ensemble des machines déjà infectées d'un pays (pour peu qu'elles soient à peu près à l'heure) aurait dû subir l'attaque entre 0h et 0h30 (heure locale), ou encore entre 8h et 10h (heure locale) si leurs propriétaires ne les ont allumées qu'en arrivant sur leur lieu de travail. En Inde, dans l'un des pays qui semblait être le plus touché, il est déjà 14h30 (il est 9h à Paris lorsque j'écris cette note) et on annonce à cette heure qu'une seule entreprise aurait été touchée dans le pays? »* Chez F-Secure, qui a, il faut bien le reconnaître, surfé sur ce sujet porteur pour vanter le niveau de sécurité de ses outils et encourager le chaland à s'équiper a publié des rapports particulièrement inquiétants, on reconnaît aujourd'hui qu'il ne s'est pas passé grand-chose. Interrogé par nos soins, Eugenio Correnti, Directeur Technique pour F-Secure a déclaré : *« Il est difficile pour nous d'établir un chiffre mais je pense que le phénomène va surtout toucher les particuliers. Environ 300.000 ordinateurs sont infectés, mais on n'a pas de données plus précises concernant son activation . Des estimations à ce propos devraient être publiées en début de semaine prochaine. »* D'après Eugenio Correnti, il faut souligner que la prévention a bien marché, ainsi, il évoque le fait que : *« La mairie de Milan a éteint 10.000 machines et serveurs pour éviter que le virus ne s'active le 3 février. L'opérateur IP européen, Easynet qui est partenaire de F-Secure a prévenu ses usagers par l'intermédiaire du Web »*. Pour Sophos, l'état de lieux est plus clair, interrogé à propos de sa base client , Michel Lanastéze, responsable marketing de Sophos a déclaré : *« Nous n'avons pas été surpris. Aucun rapport de fichiers perdus n'a été signalé dans le monde. Ce qui veut dire que la protection que nous avons publié dès le 16 janvier fonctionne. Enfin nous n'avons pas encore constaté l'existence de variantes, et il faut noter que ce virus peut s'activer encore le trois des prochains mois ». « Il n'y a pas eu de suppression massive de fichiers cette nuit en Asie, il n'y a donc aucune chance que le virus fasse des dégâts importants aujourd'hui en Europe »*, a estimé de son côté Damase Tricart, chef de produits chez Symantec France. Symantec considère que ce virus représente des risques *« modérés »*, le classant au 2e échelon d'une échelle en comptant 5, a souligné M. Tricart. Enfin, il est intéressant de préciser que le virus ne s'active qu'une demi-heure après le démarrage de l'ordinateur, ce qui laisse un petit délai de réaction pour les utilisateurs craignant une attaque et ne disposant pas de solutions anti-virus. Pour conclure, pendant que ce sujet monopolisait l'attention des internautes, des menaces plus discrètes se préparent. Ainsi hier nous annoncions une nouvelle attaque de type phishing touchant les clients français du Crédit Lyonnais. Le fait que des mafias russes ont mis au point de nouvelles techniques de contrôle de Botnet, et que selon le Clusif, *« ces dernières heures, 2 nouvelles variantes de Bagle*

viennent d'être distribuées selon la technique habituelle du spam », présentent un risque plus important.