Vaste attaque contre les réseaux britanniques

« Nous n'avons jamais vu de pareilles séries d'attaques à une telle échelle industrielle », s'alarme Roger Cummings, directeur du NISCC, le Centre britannique de coordination de la sécurité de l'infrastructure nationale cité par le *Financial Times*. Depuis plusieurs heures, les réseaux informatiques vitaux du Royaume-Uni (gouvernement, institutions, banques et groupes privés) font l'objet de graves attaques virales ciblées via Internet et les courriers électroniques. On ne connaît pas encore les dégâts causés par ces assauts. 300 sites clés auraient été attaqués. *« Le but des auteurs est de récupérer des informations ayant une valeur commerciale ou économique »*, explique le NISCC. Les attaques auraient pour origine l'Asie du Sud-Est et se font sous la forme de virus dits chevaux de Troie, diffusés sous la forme de fichiers joints, de liens joints à des courriels ou automatiquement téléchargés sur Internet lors de l'ouverture de messages électroniques. Les environnements Microsoft sont les plus touchés (exploitation de failles connues et corrigées), prévient le NISCC. Ces 'malwares' automatiques, qui ne nécessitent pas pour être activés d'être exécutés à partir d'un fichier joint, sont aujourd'hui monnaie courante. Contrairement à la plupart des attaques en masse de courriers non sollicités ou « pourriels », qui s'en prennent régulièrement aux réseaux de la planète, les courriers infectés sont très « piégeants », soigneusement personnalisés pour inciter les destinataires à les ouvrir, met en garde le NICSS. Une description qui ressemble furieusement au profil du dernier Mytob. Les nouvelles versions de ce ver se révèlent plus insidieuses, et exploitent la technique de base du 'phishing': le message dispose d'un lien hypertexte pointant vers le code malicieux. Cliquer sur ce lien ne renvoie pas vers le nom de domaine indiqué mais sur un autre site Web, et provoque le téléchargement d'une copie du ver. Le courriel associé aux nouvelles versions du ver prend l'apparence d'un message légitime expédié par la direction informatique ou par un fournisseur d'accès. **L'attaque avait été pressentie** Pour parfaire la tromperie en apportant une dose supplémentaire de crédibilité, le courriel fait même référence au nom de domaine du destinataire et à son adresse complète. En mars dernier, l'ex-patron des services de renseignement s'inquiétait de la possibilité d'une cyber-attaque à grande échelle contre les infrastructures du pays. Intervenu lors d'une réunion rassemblant des experts de la sécurité informatique et des chefs d'entreprises, Sir David Omand a expliqué que la conjonction d'une compétence informatique de plus en plus pointue observée chez les terroristes connus et de la dépendance du pays à certains réseaux laissait peu de doute à un éventuel assaut cyber-terroriste. Selon l'ex-patron du Government Communications Headquarters (GCHQ), les cibles de telles attaques ne seraient pas les réseaux militaires et gouvernementaux, mais plutôt les infrastructures critiques gérées par les civils : les marchés financiers, les services d'urgence, les réseaux de production… Il semble avoir vu juste. Le rapport d'alerte du NISCC: https://www.niscc.gov.uk/niscc/docs/ttea.pdf