inciter l'ingénieur à télécharger le manuel piégé. Ce faisant, l'ingénieur ouvre involontairement les portes de sa centrale au cheval de Troie. Une fois que le fichier corrompu se trouve à l'intérieur, l'attaque proprement dite peut commencer.

Désynchroniser, surcharger, ralentir

Un programme malveillant qui a réussi à s'introduire dans un réseau de contrôle peut émettre des instructions aux conséquences dévastatrices. En 2007, le Département de la Sécurité intérieure des États-Unis a simulé une cyberattaque au Laboratoire national de l'Idaho. Au cours de cet exercice, nommé *Aurora*, un ingénieur jouant le rôle de pirate s'est frayé un chemin jusque dans un réseau connecté à un générateur de taille moyenne. Comme tous les générateurs, il produit du courant alternatif. L'attaquant a émis une rapide séquence d'instructions marche/arrêt aux disjoncteurs d'un générateur test du Laboratoire, qui ont eu pour effet de le désynchroniser par rapport au courant alternatif du réseau. À « contre-courant » du réseau, le générateur n'a pas résisté longtemps : une vidéo aujourd'hui déclassifiée montre l'énorme machine d'acier tremblant comme si un train l'avait heurtée. Quelques secondes plus tard, la pièce était envahie de fumée.

Les systèmes industriels peuvent aussi tomber en panne quand ils sont poussés au-delà de leurs limites. Des centrifugeuses qui tournent trop vite se désintègrent. Un attaquant pourrait faire en sorte qu'un générateur électrique produise une tension supérieure à ce que les lignes de transport peuvent supporter. La puissance excédentaire serait alors évacuée sous forme de chaleur, entraînant l'affaissement de la ligne, voire sa fusion. Si des lignes affaissées entrent en contact avec quoi que ce soit, cela peut créer un énorme court-circuit. Des relais de protection sont prévus pour empêcher de tels courts-circuits, mais une cyberattaque pourrait également modifier le fonctionnement de ces relais, de façon à infliger des dégâts. En outre, l'attaque pourrait aussi modifier l'information envoyée à la station de contrôle, empêchant les opérateurs de remarquer qu'il y a un problème, comme dans ces films où les cambrioleurs envoient au gardien des images de vidéosurveillance truquées.

Les stations de contrôle elles aussi sont vulnérables aux attaques. Les personnels en salle d'opérations suivent sur écran les données transmises par les postes électriques, puis émettent des instructions pour en modifier les paramètres de contrôle. Une station est souvent responsable du suivi de centaines de postes.

La communication entre les stations de contrôle et les postes électriques utilise des protocoles spécialisés qui peuvent eux-mêmes être vulnérables. Si un intrus parvient à lancer une attaque de l'homme du milieu, il peut insérer un message dans un échange ou corrompre un message existant, voire simplement injecter un message correctement formaté, mais hors contexte, pour induire une défaillance d'un ordinateur à l'une ou l'autre extrémité.

Une autre stratégie est de retarder les messages transitant entre les stations de contrôle et les postes électriques. D'ordinaire, le délai entre la mesure du courant dans un poste et la réaction par la station de contrôle est court (sinon, cela revient à conduire une voiture en regardant là où vous étiez il y a dix secondes !). Le manque de données sur la situation en temps réel du réseau était en partie responsable de l'immense panne de courant qui a frappé l'Amérique du Nord en 2003.

Pour la plupart de ces attaques, nul besoin de logiciel sophistiqué comme *Stuxnet* : la boîte à outils du pirate de base suffit. Par exemple, des pirates prennent fréquemment le contrôle de milliers d'ordinateurs de bureau auxquels ils font faire ce qu'ils veulent, formant un réseau de

Janvier 2003
Le virus informatique *Slammer* contourne de nombreux pare-feu pour infecter le centre de contrôle de la centrale nucléaire de Davis-Besse dans l'Ohio (États-Unis). Le virus se répand à partir de l'ordinateur d'un sous-traitant jusque dans le réseau commercial, d'où il gagne les ordinateurs contrôlant l'exploitation de la centrale, entraînant la panne de multiples systèmes de sécurité. La centrale était à l'époque hors réseau.

Mars 2007
Des agents du gouvernement américain simulent une cyberattaque, nommée *Aurora*, sur un générateur électrique au Laboratoire national de l'Idaho. Le générateur est détruit.

Janvier 2008
Un responsable de la CIA révèle que des pirates informatiques auraient souvent infiltré les services d'électricité hors des États-Unis, avec des tentatives d'extorsion. Dans au moins un cas, les pirates auraient réussi à couper l'alimentation électrique de plusieurs villes, non nommées.

Avril 2009
Selon le *Wall Street Journal*, des cyberespions de Chine, Russie et d'autres pays auraient pénétré le réseau électrique américain et y auraient laissé des logiciels pouvant être utilisés pour le mettre hors service.

Octobre 2010
Des responsables de la sécurité en Iran, en Indonésie et ailleurs signalent la découverte de *Stuxnet*, un virus conçu pour attaquer des systèmes de contrôle industriels fabriqués par *Siemens*, qui commandent les centrifugeuses iraniennes.

2002 2003 2004 2005 2006 2007 2008 2009 2010 2011

Mark Duncan AP Photo, Mark Peterson Redux Pictures, Ebrahim Norouzi AP Photo