du réseau électrique, puisque ce système n'est pas directement connecté à Internet. Mais depuis, *Stuxnet* a démontré que les réseaux sans connexion permanente vers l'extérieur sont eux aussi vulnérables. Les virus peuvent par exemple se propager physiquement *via* des clefs USB utilisées par des employés. Même la plus petite porte dérobée peut servir d'entrée pour un cambrioleur entreprenant.

Prenons le cas d'un poste électrique. De tels postes reçoivent des courants à haute tension venant d'une ou plusieurs centrales, les synchronisent, abaissent la tension et les répartissent entre de multiples lignes pour la distribution locale. En cas de panne sur une de ces lignes, un disjoncteur coupe le courant. Toute l'électricité envoyée dans cette ligne est alors répartie entre les autres lignes. Si les lignes de distribution sont proches de leur limite de capacité, une attaque qui coupe la moitié des lignes et maintient les autres ouvertes a toutes les chances de surcharger ces dernières.

Des portes d'entrée multiples

Ces disjoncteurs sont encore aujourd'hui équipés de modems auxquels les techniciens peuvent se connecter. Or il n'est pas difficile de trouver ces numéros. Les pirates ont inventé depuis longtemps des programmes pour composer tous les numéros de téléphone d'un central téléphonique et repérer ceux auxquels un modem répond. Quand cela est combiné à une faible protection, comme des mots de passe bien connus ou pas de mot de passe du tout, un attaquant peut utiliser ces modems pour s'introduire dans le réseau d'un poste électrique. De là, il pourrait configurer les disjoncteurs de façon à ce qu'ils passent outre une situation dangereuse, au lieu d'ouvrir le circuit.

Les nouveaux systèmes ne sont pas plus sûrs. De plus en plus, les dispositifs déployés dans les postes électriques communiquent entre eux par ondes radio à faible puissance. Celles-ci ne s'arrêtent cependant pas aux murs du poste électrique. Un pirate peut s'introduire dans le réseau en se cachant dans les parages avec son ordinateur. Les réseaux Wi-Fi cryptés sont plus sûrs, mais un attaquant compétent peut quand même casser le cryptage avec des logiciels faciles à se procurer. De là, il pourrait lancer une « attaque de l'homme du milieu » qui fait transiter par son ordinateur toutes les communications entre deux ordinateurs légitimes, ou faire accepter son ordinateur comme légitime. Il serait alors en mesure d'envoyer des messages de contrôle frauduleux qui perturberaient le fonctionnement des disjoncteurs.

Une fois qu'un virus s'est introduit dans un réseau, sa première consigne est en général de se répandre le plus possible. Là encore, *Stuxnet* illustre des stratégies bien connues. Il a tiré profit d'un mécanisme du système d'exploitation *Windows*, qui lit et exécute un fichier nommé autoexec.bat à chaque fois qu'un utilisateur s'identifie pour localiser des pilotes de périphériques, lancer un antivirus, ou d'autres fonctions de base. Mais le système suppose que tout fichier ayant le bon nom est un code fiable. Il suffit ainsi de modifier le fichier autoexec.bat pour qu'il exécute le code malveillant.

Les attaquants peuvent aussi exploiter la structure du marché de l'électricité. Dans le cadre de la dérégulation, l'électricité est produite, transportée et distribuée par des compagnies concurrentes, dans le cadre de contrats qui portent sur diverses échéances, obtenus dans des enchères en ligne. La branche commerciale d'une compagnie doit recevoir en permanence des informations en temps réel de sa branche d'exploitation afin de faire des transactions intéressantes ; inversement, la branche exploitation doit savoir combien d'électricité elle doit produire pour répondre aux commandes de la branche commerciale. C'est là que se trouve le talon d'Achille. Un pirate pourrait pénétrer dans le réseau commercial, y dénicher des noms d'utilisateurs et des mots de passe, et utiliser ces identifiants pour accéder au réseau d'exploitation.

D'autres attaques pourraient se répandre en exploitant des scripts cachés dans des fichiers. On trouve des scripts partout (les fichiers PDF, par exemple, contiennent souvent des scripts qui gèrent l'affichage), mais ils représentent aussi un danger potentiel. Une entreprise de sécurité informatique estimait récemment que plus de 60 pour cent des attaques ciblées utilisent des scripts enfouis dans des fichiers PDF. Le simple fait de lire un fichier corrompu peut laisser entrer un attaquant dans votre ordinateur.

Imaginons qu'un attaquant pénètre dans un premier temps sur le site Web d'un fournisseur de logiciels et remplace un manuel en ligne par un faux manuel corrompu semblable au premier. Le cyberattaquant envoie alors à un ingénieur de la centrale électrique un message, qui va

ATTAQUES INFORMATIQUES, DÉGÂTS PHYSIQUES

À mesure que l'on relie les machines industrielles au réseau Internet, le potentiel de nuisance des pirates augmente. Les attaques recensées ces dix dernières années montrent que le réseau électrique n'est pas le seul point faible : tout ce qui comporte un circuit intégré peut être pris pour cible.

La centrale nucléaire de Davis-Besse (Ohio, États-Unis).

Avril 2000
Un ancien employé mécontent d'une entreprise de traitement de l'eau vole des composants radio et les utilise pour envoyer de fausses instructions aux équipements des égouts du Queensland, en Australie. Plus de 750 000 litres d'eaux usées sont déversées dans les parcs et les rivières du secteur.

2000 2001

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