La chimie, cible des cyberattaques ?

© Can Stock Photo/welcomia.

Nous avons tous été piratés par un virus ou un « cheval de Troie » qui a infecté notre ordinateur malgré nos antivirus et pare-feux de Microsoft ou Kaspersky… Cela nous a mis en fureur et demandé un plus ou moins grand nombre de nettoyages et de mises en quarantaine, mais sans trop de dégâts à notre niveau de particulier. D'une toute autre dimension sont les cyberattaques qui visent de grands serveurs, des plateformes informatiques, des banques, des administrations et des industries.

Ces attaques peuvent pirater des données, saturer un réseau, arrêter ou détourner un procédé ou une production, ce qui est particulièrement dangereux s'il s'agit d'une plateforme chimique. Les logiciels malveillants ou « malware » sont de plusieurs types :
- vol de données ou secrets de fabrications, qui s'assimile à l'espionnage industriel ;
- blocage de toutes les données par cryptage inaccessible à l'entreprise concernée, sauf si elle verse une rançon pour les débloquer – souvent en bitcoins, monnaie difficile à tracer – : ce sont les « rançongiciels » ;
- intrusion dans les logiciels des protocoles utilisés par l'industrie pour le contrôle des procédés de fabrication en vue de les perturber, qui s'assimile au sabotage.

Quelques exemples : en 2016, le cheval de Troie « BlackEnergy » s'est infiltré dans le réseau d'une centrale d'énergie ukrainienne et s'est propagé de poste en poste jusqu'à la salle de commande pour bloquer la production électrique alors que le conflit avec la Russie battait son plein. Il a rappelé l'attaque par déni de service (DoS, pour « denial of service ») de même type fin 2015, qui avait rendu indisponibles toutes les ressources et services qu'une entreprise ou un site doit exploiter sans interruption et qui avait bloqué la distribution électrique dans une grande partie de l'Ukraine.
Le virus WannaCry et ses dérivés NotPetya ou Petwrap ont sévi en Europe en 2017. Ils se sont engouffrés dans une faille du système d'exploitation Windows de Microsoft ; c'était à nouveau un « rançongiciel » qui bloquait toutes les données. Environ 29 000 serveurs ont été touchés en Europe, et plus de deux millions dans le monde.
En juin 2017, l'entreprise Saint-Gobain a été victime du virus NotPetya *via* sa filiale ukrainienne infectée par un logiciel de l'administration fiscale auquel les entreprises du pays doivent se connecter. Tous les systèmes de commande, de fabrication et de facturation ont été bloqués ainsi que les réseaux de distribution, y compris pour ses filiales en Europe. Il a fallu quatre jours pour gérer la crise et dix pour que l'activité reprenne totalement.
Encore plus récemment, le cabinet américain FireEye spécialisé dans la cyberprotection a publié un rapport suite à l'attaque en décembre 2017 d'un nouveau virus, « Triton », visant une raffinerie, probablement en Arabie saoudite. Ce virus a pu accéder à un poste de commande qui gérait toute une série de capteurs assurant le déroulement de plusieurs procédés pétrochimiques. Le virus a tenté de les reprogrammer en faisant croire que tout fonctionnait normalement et en même temps d'initier un incident critique qui aurait provoqué d'importants dégâts sur le site industriel. Heureusement, semble-t-il, une faille dans l'algorithme de la cyberattaque a déclenché la procédure d'arrêt. Toujours d'après FireEye, cette attaque très sophistiquée a nécessité des moyens importants et l'agence soupçonne un groupe de pirates russes, TEMP.Veles, qui a utilisé une adresse IP enregistrée auprès de l'Institut Central de Recherche Scientifique de Chimie et Mécanique (ICRSM) de Moscou. Est-ce une initiative de quelques personnes agissant sans l'aval de l'Institut ? De fortes présomptions situent le groupe en Russie, avec sans doute l'accord de l'État russe. Le cabinet publie d'ailleurs un *Guide pratique sur les groupes de cyberattaques* où l'on trouve un joli nombre d'« APT » (« advanced persistent threat »), pirates agissant généralement pour le compte d'un État qui finance ses activités, d'origines diverses : huit en Chine, deux en Russie, deux en Iran et d'autres en Corée du Nord et Vietnam, qui suivent assez bien l'actualité des tensions économicopolitiques [1].

D'après l'entreprise de sécurité informatique française Sentryo, l'industrie chimique constitue une cible de choix dans un climat géopolitique qui peut devenir tendu avec des produits chimiques très sensibles et parce qu'elle constitue un maillon indispensable pour d'autres industries. Cette situation préoccupante l'a fait placer en tête des seize secteurs critiques de la « Presidential Policy Directive on Critical Infrastructure

Security and Resilience » aux États-Unis, comme nécessitant un renforcement de leur protection face aux cybermenaces.
Le problème a reçu un coup de projecteur médiatique à l'occasion du « Forum de la paix » le 11 novembre, avec un appel de Paris visant à éviter une cyberguerre mondiale. En effet, malgré les avertissements de plusieurs ONG, des fondateurs d'Internet et de nombreuses sociétés de sécurité informatique, les blocs opposant les États-Unis et leurs alliés à la Russie et à la Chine ont bloqué en 2017 les discussions du groupe spécialisé de l'ONU sur les normes internationales du cyberespace. La course aux armements numériques est loin d'être enrayée. En octobre dernier, la ministre néerlandaise de la Défense estimait que les Pays-Bas se trouvaient en guerre informatique avec la Russie et assurait avoir expulsé quatre agents russes qui préparaient une cyberattaque contre l'Organisation pour l'interdiction des armes chimiques (OIAC) à La Haye. Ce qui fait dire aux experts de la Défense que « *la problématique de la prolifération des cyber-armes est du même niveau que celle des armes nucléaires, chimiques et bactériologiques* », d'où l'appel de Paris, en espérant qu'il ait plus de succès que le précédent !

Comment se prémunir ?

Le déclenchement d'une cyberattaque a souvent un acte humain à son origine : insertion d'un périphérique, ouverture d'une pièce jointe, clé USB infectée… Aussi la sécurité informatique demande à l'industriel de mettre en place une stratégie de cybersécurité :
- Se soumettre à un audit par un service externe spécialisé qui identifie les risques et la hiérarchie des droits d'accès des salariés et des sous-traitants.
- Protéger à chaque niveau, et Dieu sait qu'ils se multiplient dans une industrie 4.0 où tous les réseaux de production, logistique, commerciaux, transports, sont interconnectés, avec des pare-feux, des codes d'accès et des mots de passe.
- Passer un contrat avec un centre opérationnel de sécurité qui va utiliser de plus en plus les moyens de l'intelligence artificielle pour surveiller automatiquement tout comportement anormal sur le réseau, l'identifier et lancer une parade protectrice.
De nombreuses sociétés ou jeunes et moins jeunes entreprises se sont lancées dans ce nouveau job de cybersécurité que les assurances des sites vont bientôt exiger. Citons FireEye aux États-Unis, Sentryo bien implanté en Europe, ITrust à Toulouse et surtout Orange Cyberdefense en France, qui traitent des milliards d'évènements par jour pour les centaines d'entreprises clientes. L'État français, à travers l'Agence nationale de sécurité des systèmes d'information (ANSSI), a détecté une augmentation des attaques depuis 2015 et à travers le groupe de travail sécurité Intelligence artificielle, les acteurs de la sécurité numérique se mobilisent pour ce secteur prioritaire.

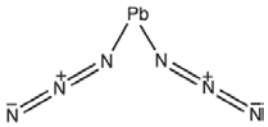
En recherche, l'Institut des sciences de l'information et de leurs interactions (INS2I) au CNRS et l'Institut national de recherche en informatique et en automatique (Inria) sont en pointe sur la recherche d'algorithmes et ont réalisé la cartographie académique en cybersécurité. Si on peut, comme pour les grandes entreprises internationales, avoir une protection de qualité, il n'en est pas de même pour les petites entreprises et aussi pour chaque université. Pour l'instant à la Société Chimique de France et à *L'Actualité Chimique*, nos archives et nos sites n'ont pas encore fait l'objet d'une attaque ciblée, et pourtant, que de beaux secrets (bien) gardés !

Jean-Claude Bernier
Novembre 2018

[1] www.fireeye.fr/current-threats/apt-groups.html

Erratum

Deux erreurs se sont glissées dans la dernière chronique, « La chimie et les chimistes de la Grande Guerre », dans l'encadré de la page 8 sur les « molécules belliqueuses » :
- le TNT est un dérivé du toluène (et non du phénol) ;
- la formule du trinitrorésorcinate de plomb a remplacé celle de l'azoture de plomb ; la bonne est :



Merci aux lecteurs fidèles et attentifs !