Lettre n°47 - **février 2016** - **disponible sur omc.ceis.eu**

« What I find fascinating is that birds can hit the drone in such a way that they don't get injured by the rotors. They seem to be whacking the drone right in the centre so they don't get hit; they have incredible visual acuity and they can probably actually see the rotors. » ***Geoff LeBaron, sur l'utilisation d'aigles par la police londonienne pour intercepter des drones.***

Table des matières

L'ANALYSE PREDICTIVE : NOUVEL ELDORADO DE LA SECURITE INFORMATIQUE ?

Le big-data et l'analyse prédictive

Nous assistons depuis quelques années à l'explosion des données disponibles, que celles-ci proviennent de capteurs utilisés pour collecter les informations climatiques, d'objets connectés, de messages publiés sur les médias sociaux, d'images numériques et de vidéos publiées en ligne, d'enregistrements transactionnels d'achats en ligne, etc. Ce sont ainsi des trillons d'octets de données qui sont produits quotidiennement. Ces volumes massifs de données, appelés big data, constituent, avec un potentiel de 9 milliards d'euros et 130 000 emplois créés ou maintenus en France d'ici à 2020[1], l'un des marchés les plus prometteurs du secteur IT.

Souvent appelée « big data » par amalgame, l'analyse prédictive constitue un ensemble de techniques sous-jacentes au big data visant à récupérer une grande quantité de données de sources différentes, à en extraire des motifs statistiques et à s'en servir pour essayer de prédire le futur (à court, moyen ou long terme). L'analyse prédictive englobe une variété de méthodes et techniques, issues pour la plupart des statistiques, de l'extraction de connaissances à partir de données et de la théorie des jeux[2]. A la différence des modèles purement descriptifs, les modèles prédictifs permettent d'analyser des faits présents et passés pour identifier des « motifs de comportement » et dresser des hypothèses prédictives sur des événements futurs.

L'analyse prédictive peut ainsi avoir pour objectifs :

- De minimiser les comportements déviants avant qu'ils ne se répandent (exemple : fraudes, abus, risques, etc.) ;
- De planifier une opération de maintenance sur un matériel qui semble défectueux ;
- De présenter la meilleure offre pour répondre au besoin du client ;
- …

Elle permet donc, en théorie, de comprendre et d'anticiper les comportements avant qu'ils ne surviennent, afin de mettre en place des pistes d'amélioration ou des actions correctrices.

L'utilisation de l'analyse prédictive

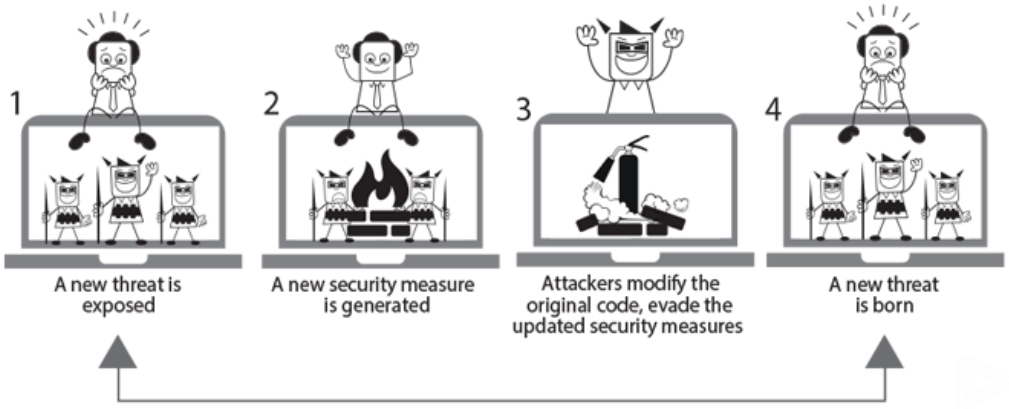
Ces technologies possèdent de nombreuses applications dans des secteurs variés. Les modèles de risque de crédit par exemple, utilisant l'information de chaque demande de prêt pour prédire les risques de perte, ont été conçus et remaniés au fil des ans, à un point tel qu'ils jouent désormais un rôle indispensable en matière de décisions de crédit. Le secteur de la consommation est lui aussi très friand d'analyse prédictive pour pouvoir anticiper l'achat d'un produit ou d'un service, prioriser des cibles et des investissements, analyser des profils de consommation, adapter des offres et des services aux comportements actuels et futurs, optimiser la logistique grâce à la prévision de la demande, etc.[3] L'entreprise israélienne *Salespredict*[4] s'est par exemple donnée pour objectif d'augmenter les ventes de

[1] http://www.economie.gouv.fr/files/files/PDF/Feuille-de-route_big-data151214.pdf
[2] https://fr.wikipedia.org/wiki/Analyse_pr%C3%A9dictive
[3] http://www.docaufutur.fr/2015/09/04/big-data-sailendra-lance-sailstream-un-outil-de-valorisation-des-donnees-et-danalyse-predictive-a-destination-du-marche-bancaire-en-ligne/
[4] http://www.salespredict.com/

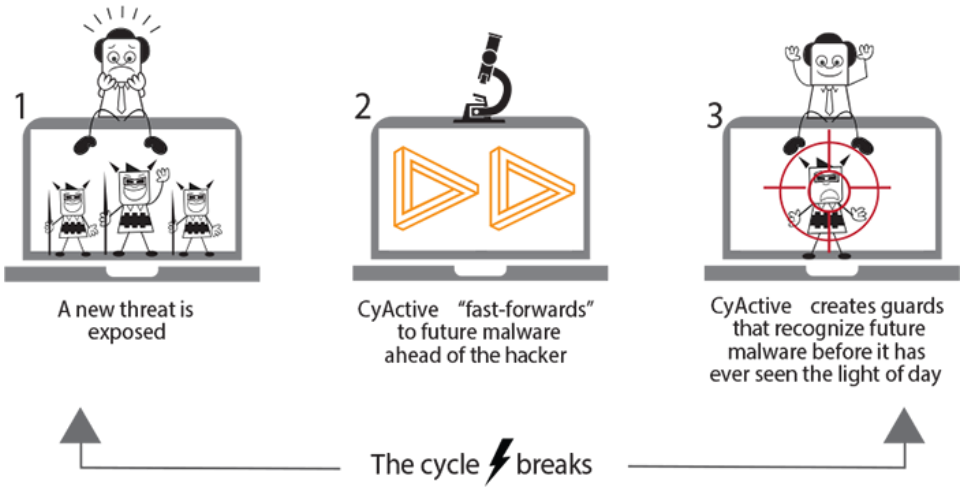
ses clients en s'appuyant sur le big-data et l'analyse prédictive afin d'aider les entreprises à améliorer leur taux de conversion. Sa co-fondatrice, Kira Radinsky, explique que ses prédictions se vérifient avec une probabilité située entre 70 % et 90 %[5].

L'analyse prédictive constitue également un enjeu majeur pour la santé. Confronté à des données multiples, à une complexité croissante en raison des progrès médicaux et technologiques, le médecin de demain devra être assisté d'outils susceptibles, à partir d'un diagnostic et d'une connaissance la plus exhaustive possible de l'état de l'art, de lui proposer des options. C'est là l'objectif du système d'aide à la décision médicale Watson Health d'IBM[6]. Mais l'analyse prédictive peut aussi permettre une meilleure détection, et donc prévention, des épidémies comme celle de choléra qui a sévi à Cuba en 2012 et qui avait été détectée par l'algorithme de Kira Radinsky[7].

Le monde de la sécurité informatique a de son côté commencé à s'intéresser il y a déjà quelques années avec l'émergence des premiers outils d'analyse prédictive dédiés. Ainsi, la start-up israélienne CyActive, créée en 2013, s'est positionnée sur ce domaine avec une technologie censée prédire les futures attaques de malwares grâce à des algorithmes permettant d'analyser et de comprendre les processus de développement de ces logiciels malveillants. Ces algorithmes intelligents ont pour objectif de prévoir en avance les évolutions des malwares afin de pouvoir les détecter. Comme la plupart de ces malwares utilisent le même « noyau » (ce fut le cas pour Flame ou Stuxnet), l'idée est de se baser sur l'analyse de ces noyaux et les données récoltées sur les attaques pour prévoir des évolutions possibles de ces malwares à l'aide d'algorithmes prédictifs. En 2014, les 5 malwares les plus réutilisés ont ainsi été : Snake, Black POS, Gyges, Dragonfly et Zberp. A noter que CyActive a été rachetée en mars 2015 par la société Paypal pour 60 millions de dollars.



[5] http://www.technionfrance.org/docs/kira_radinsky_2014.pdf
[6] http://www.ibm.com/smarterplanet/us/en/think/watson-health/
[7] http://www.israel21c.org/the-israeli-who-can-predict-the-future/



La technologie de CyActive

D'autres technologies d'analyses prédictives apparaissent enfin en matière de gestion et d'analyse des événements sécurité (SIEM). Le big-data et les algorithmes sophistiqués ont permis d'approcher de prédictions de plus en plus correctes et d'identifier les menaces émergentes en analysant des « patterns » d'attaques lors d'analyse en temps réel des journaux d'évènements et du réseau par exemple. Pour cela, la collecte de données au sein du système d'information est primordiale afin de pouvoir récolter le maximum de données : actifs, réseau, attaques subies, fichiers de logs, etc. De nombreuses sociétés émergent sur ce sujet comme SAS (SAS® Cybersecurity[8]), Rapid7 ou bien encore IBM[9].

L'analyse prédictive devrait donc rapidement être une technologie clé en matière de cybersécurité. Mais pour pouvoir mettre en place de façon viable ce type d'outils en interne, il est impératif d'avoir déjà mis en place un écosystème complet de gestion des journaux d'évènements des différents actifs présents au sein du système d'information (collecte, stockage et archivage), ce que de nombreuses entreprises n'ont pas encore fait. Il sera alors possible d'envisager la mise en place d'outils d'analyse prédictive efficace.

[8] http://www.sas.com/en_us/software/fraud-security-intelligence/cybersecurity-solutions.html
[9] http://www.csoonline.com/article/3024407/security/ibm-will-bring-watson-to-security-later-this-year.html

LA CYBERATTAQUE DES RESEAUX ELECTRIQUES EN L'UKRAINE

L'Ukraine et la Russie entretiennent des relations diplomatiques complexes, fruit d'un passé commun parfois douloureux. L'Ukraine est un pays multiculturel, à l'histoire tourmentée. Sa partie ouest a été rattachée à l'Union soviétique en 1939 suite à la signature du pacte germano-soviétique entre Staline et Hitler. Au sud, la Crimée, dont 60 % de la population est russe, n'est devenue une province ukrainienne qu'en 1954, quand le président Khrouchtchev, ukrainien de naissance, l'a « offerte » lors de la célébration du 300ème anniversaire de l'unification de la Russie et de l'Ukraine orientale. L'ouest est majoritairement catholique, l'est est majoritairement russe orthodoxe. L'ouest parle ukrainien, l'est parle essentiellement le russe. En 2014, la crise de la Crimée a donc contribué fortement au raidissement des relations russo-ukrainiennes. Selon les Nations Unies, 6000 personnes ont été tuées d'avril 2014 à mars 2015 dans le Donbass, l'Ukraine orientale, dans un conflit armé encore en cours.[10]

Du point de vue du cyberespace, de nombreuses attaques informatiques ont été réalisées sur le sol ukrainien durant la crise de la Crimée. Par exemple, les forces spéciales russes ont saisi un point d'échange Internet (IXP) et des câbles serveurs. Selon le renseignement ukrainien, une attaque informatique sur la VoIP en provenance de la Crimée aurait ciblé les appareils mobiles des membres de la Rada, le parlement ukrainien. De même, une attaque informatique a eu lieu contre la commission centrale électorale d'Ukraine (*Central Election Commission of Ukraine)* en octobre 2014, dans le cadre des élections parlementaires du pays[11]. Une attaque DDoS a été lancée, ralentissant fortement les systèmes de vote en ligne. De plus, de nombreuses campagnes APT ont été découvertes par le secteur privé en Ukraine et dans les pays de l'OTAN. L'analyse suggère que ces campagnes sont basées en Russie, et utilisent des nouvelles variations de malwares incluant *Turla*, *RedOctober*, *MiniDuke* et *NetTraveler*..

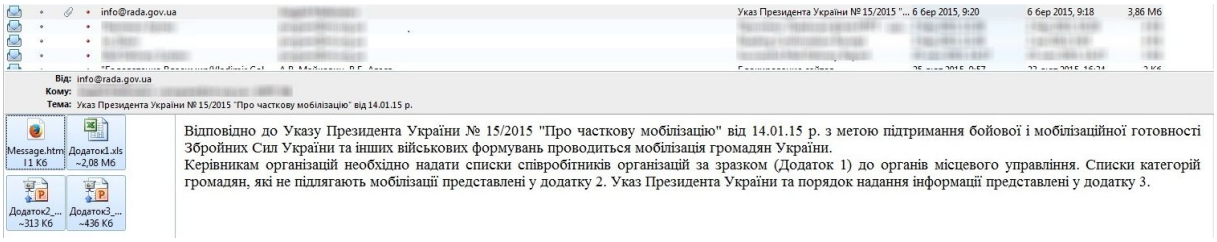
Région d'Ivano-Frankivsk, paralysée suite à l'attaque sur la centrale électrique – Source : Wikipedia

Le 25 décembre 2015, plus de 225 000 personnes autour de la région d'Ivano-Frankivsk ont subi des coupures de courant. Après enquête, il semblerait qu'une série d'attaques informatiques sur trois centrales électriques en Ukraine de l'ouest en ait été l'origine, permettant de paralyser cette partie du territoire, majoritairement hostile à Moscou. Elle fut la première attaque informatique réussie sur un réseau électrique.

[10] https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf
[11] http://www.securityweek.com/hackers-target-ukraines-election-website

Un rapport a été publié le 25 février 2016 par l'ICS-CERT (*Industrial Control Systems Cyber Emergency Response Team*) américain (experts appelés par le gouvernement ukrainien), basé sur les témoignages du personnel IT des organisations ukrainiennes qui ont été directement témoins des évènements (et non sur une analyse forensique). La panne massive qui a frappé Ivano-Frankivsk s'est révélé être une attaque complexe, préparée depuis six mois et coordonnée de telle manière que les différentes attaques informatiques se sont produites à 30 minutes d'intervalle sur chacun des 3 réseaux. Les centres d'appels des centrales électriques ont aussi subi des attaques de type déni de services : ils ont été surchargés d'appels en amont pour les empêcher de réagir rapidement à l'attaque. Dû au nombreux mois de préparation, on peut supposer qu'à l'origine, les pirates n'avaient pas pour objectif premier d'arrêter les centrales électriques en Ukraine, mais l'apparition de la crise de Crimée a accéléré l'opération.

Selon les équipes de l'ICS-CERT, lors de l'attaque, plusieurs individus ont eu accès aux systèmes grâce à des outils de contrôle à distance, soit au niveau du système d'exploitation, soit au niveau des systèmes industriels, le tout via des accès VPN (réseau privé virtuel) dont ils avaient précédemment obtenu les codes d'accès. Le malware BlackEnergy aurait permis de récupérer les identifiants et mots de passe, via des campagnes de phishing contenant des pièces jointes Microsoft Office piégées à destination des employés des centrales électriques (cette information est encore vérifiée par les équipes de l'ICS-CERT).



Email reçu par un employé d'une des 3 centrales électriques
avec une adresse du parlement ukrainien (rada.gov.ua) falsifiée comme expéditeur – Source : Cys-centrum.com[12]

Enfin, le malware KillDisk aurait été utilisé à la fin de l'attaque pour effacer les fichiers compromis et corrompre les secteurs de démarrage des machines ou les firmwares des équipements pour les rendre totalement inopérants.

Bien que les centrales électriques produisent de nouveau, elles continuent de fonctionner de façon limitée actuellement. C'est la première fois que nous voyons une attaque de cette envergue réussir sur un distributeur d'énergie. Selon la société iSight Partners[13], l'APT pourrait avoir été mis en place par le groupe de pirates Sandworm, connus pour avoir de puissants intérêts russes. L'argument principal utilisé pour leur attribution serait l'utilisation du malware Black Energy, qui est une création de ce groupe de pirates.

[12] https://cys-centrum.com/ru/news/uisgcon11_2015
[13] http://www.ibtimes.com/russian-hacking-group-sandworm-targeted-us-knocking-out-power-ukraine-2257194

Les différentes campagnes du groupe Sandworm - Source: iSight Partners[14]

Le ministre de l'énergie ukrainien a mis en place une commission pour enquêter sur cette attaque.[15]

Il est intéressant d'observer que le gouvernement ukrainien, selon les déclarations du DHS américain[16], travaille de façon proche avec les équipes étasuniennes et échangent librement des informations pour prévenir de futures attaques informatiques. On pourrait penser que seules les équipes de l'ICS-CERT sont impliquées dans la résolution du problème, mais d'autres agences américaines sont impliquées :

- *National Cybersecurity and Communications Integration Center* (NCCIC);
- *U.S. Computer Emergency Readiness Team* (US-CERT);
- *Département de l'Energie*;
- *Federal Bureau of Investigation* (FBI);
- La *North American Electric Reliability Corporation* (NERC) qui est chargée de faire appliquer des normes de fiabilité pour les réseaux de transport de l'électricité des États-Unis, du Canada et de certaines Etats du Mexique.

Le 27 janvier 2016, le conseil national de sécurité et de défense ukrainien a adopté sa stratégie de cybersécurité. Selon la déclaration officielle du gouvernement[17], cette dernière a été motivée par l'agression de la Fédération de Russie, la tendance croissante de l'utilisation du cyberespace, les structures militaires spéciales, les terroristes et les criminels. La stratégie de cybersécurité prévoit le développement d'un système de protection du cyberespace national, pour la détection rapide et la neutralisation des menaces, ainsi que la prévention des menaces informatiques, en tenant compte des bonnes pratiques des principaux États membres de l'OTAN et de l'UE. On y voit ainsi une volonté de coopérer sur le sujet de la cyberdéfense avec ses partenaires, afin de pouvoir se protéger de son voisin russe.

Ainsi, l'Ukraine met en place une stratégie lui permettant de se doter de moyens concrets afin de se protéger dans le cyberespace. Un parallèle peut être fait avec l'Estonie, qui a subi en 2007 de nombreuses cyberattaques de la part de la Russie sur ses différents sites (gouvernementaux, médias, banques et opérateurs téléphoniques). Ces attaques informatiques ont marqué les esprits des Estoniens, transformant ce petit Etat balte en quelques années en un des acteurs mondiaux de la cyberdéfense. L'Estonie a même mis en place des programmes de création et renforcement de capacités (*capacity bulding*) pour l'Ukraine sur différents domaines, tel que l'eGouvernement ou encore la cybersécurité[18].

[14] http://www.isightpartners.com/2014/10/cve-2014-4114/
[15] http://www.reuters.com/article/ukraine-crisis-malware-idUSL8N14K12Y20151231
[16] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
[17] http://www.rnbo.gov.ua/en/news/2379.html
[18] http://www.vm.ee/sites/default/files/content-editors/development-cooperation/estonian_aid_to_ukraine_in_2015_0.pdf

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com