Attaques informatiques : défaillance humaine, technique et… politique

Description

L'été 2017 a été marqué par des attaques informatiques d'une ampleur sans précédent. La meilleure défense reste la garantie de sécurité qui devrait être assurée aux entreprises et aux citoyens.

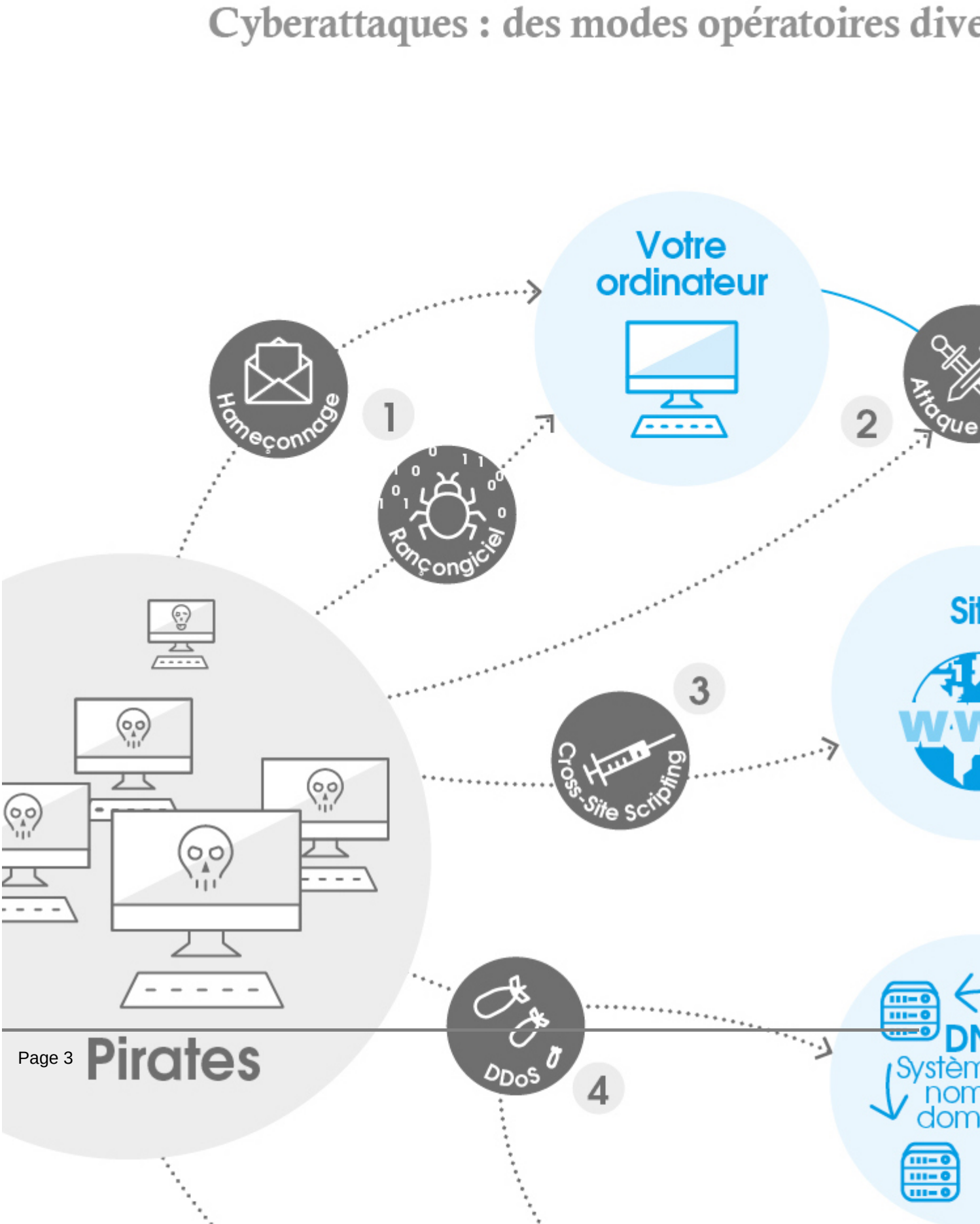
L'opérateur de télécommunications Telefónica, le National Health Service au Royaume-Uni, le ministère de l'intérieur ainsi que l'opérateur de télécommunications Megafon en Russie, le transporteur FedEx aux États-Unis, des usines du constructeur automobile Renault, dont la production, en France, a dû être stoppée : au total, plus de 200 000 systèmes informatiques dans 150 pays ont été victimes d'une attaque fulgurante par le rançongiciel WannaCry (voir *La rem* n°41, p.54) dans la nuit du 11 au 12 mai 2017. Quatre grands groupes auraient été infectés sur le territoire français. *« Nous menons des opérations contre environ 200 cyberattaques par an mais nous n'avions encore jamais rien vu de tel »* a déclaré Rob Wainwright, directeur d'Europol, l'Office européen de police.

Quelques jours plus tard, un nouveau logiciel malveillant baptisé Adylkuzz affecte plusieurs centaines de milliers d'ordinateurs répartis dans le monde entier, afin de pirater la *blockchain* de la monnaie virtuelle Monero : *« du jamais vu à cette échelle »* selon les spécialistes. Déclenchée le 27 juin 2017 à partir de l'Ukraine où elle a bloqué de nombreuses entreprises et administrations, Petya (la mise à jour de ce virus porte le nom de Petrwap), nouvelle cyberattaque par rançongiciel à l'envergure planétaire, se propage en Russie, affectant notamment le site web du groupe pétrolier Rosneft et le groupe de sidérurgie Evraz, avant de toucher les groupes Saint-Gobain et SNCF en France, Nivea en Allemagne, l'entreprise pharmaceutique Merck aux États-Unis, le transporteur danois Maersk, le géant mondial de la publicité WPP ou encore le cabinet d'avocats international DLA Piper.

Le point commun entre ces trois attaques informatiques s'appelle Eternal Blue : un « exploit » dans le langage des experts en sécurité informatique, c'est-à-dire un programme exploitant une faille de sécurité. Cet outil a été conçu par l'agence de renseignement américaine NSA pour espionner les communications, à partir d'un défaut de sécurité logé dans d'anciennes versions du système d'exploitation Windows. Le 14 avril 2017, un groupe de pirates baptisé The Shadow Brokers rend publique l'existence d'Eternal Blue. Microsoft avait déjà procédé, en mars 2017, à une mise à jour, applicable aux seuls ordinateurs récents. Le rançongiciel WannaCry a pu ainsi être propagé sur des milliers d'ordinateurs équipés soit d'anciennes versions de Windows, pour lesquelles Microsoft ne fournit plus de mise à jour, soit de plus récentes n'ayant pas encore été corrigées. À la suite de cette première attaque, le groupe américain a néanmoins proposé un correctif spécialement pour les anciennes versions, solution que les entreprises concernées n'ont pas toutes eu le temps d'installer avant l'arrivée de Petya.

Dans un premier temps, l'enquête sur l'origine du rançongiciel WannaCry fait porter les soupçons sur un groupe de pirates nommé Lazarus, auteur présumé de l'attaque informatique dont fut victime Sony Pictures en 2014 (voir *La rem* n°33, p.81) et supposément piloté par la Corée du Nord, comme l'a indiqué le FBI. Des experts en sécurité informatique auraient repéré des ressemblances entre une ancienne version de WannaCry et des logiciels développés par Lazarus. Selon les informations rapportées par le magazine américain *Wired*, WannaCry a également servi à extorquer des données confidentielles avant de les détruire et pourrait être d'origine russe. Même revirement concernant Petya, que la société spécialisée en sécurité informatique Kaspersky Lab a finalement rebaptisé NotPetya, après avoir découvert qu'il s'agissait en fait d'un logiciel destructeur de données (*wiper*) masqué sous l'apparence d'un rançongiciel, diagnostic partagé par de nombreux experts. Pointant des similitudes avec le virus Black Energy, déjà utilisé contre son réseau électrique en décembre 2015, l'Ukraine dénonce une action de la Russie, pays pourtant lui aussi victime de ce piratage. *« Petya a probablement été lancé par un acteur étatique ou un acteur non étatique agissant avec le soutien ou l'approbation d'un État. L'opération est trop complexe pour avoir été préparée par des pirates indépendants à des fins d'entraînement,* explique le Centre d'excellence de cyberdéfense coopérative de l'Otan. *Des cybercriminels ne sont pas derrière Petya, étant donné que la méthode de collecte de la rançon était si mal conçue qu'elle n'aurait même pas couvert le coût de l'opération. »*

En septembre 2017, l'enquête menée sur la propagation, un mois plus tôt, d'un logiciel malveillant *via* la mise à jour du programme CCleaner, servant à nettoyer un PC, commercialisé sous la marque Piriform, propriété de l'éditeur tchèque d'antivirus Avast, a démontré que cette attaque informatique en cachait en réalité une autre visant expressément les systèmes informatiques des fleurons de la high-tech mondiale comme Google, Samsung, Sony, Epson, Akamai, Microsoft et Cisco. Ce piratage, dissimulé derrière un logiciel malveillant ordinaire et servant à extorquer des informations confidentielles, s'apparente à une opération d'espionnage industriel, selon Cisco. Moins de la moitié des groupes ciblés par cette attaque ont effectivement été piratés, tandis que la diffusion du premier logiciel malveillant attaché à CCleaner a infecté quelques centaines entreprises. En l'occurrence, le stratagème des pirates est le même que celui employé dans l'attaque Petya/NotPetya pour laquelle les enquêteurs ont conclu que le vecteur de propagation du logiciel malveillant était la mise à jour d'un programme de comptabilité appelé M.E.Doc, utilisé par la grande majorité des entreprises ukrainiennes, démontrant que la cible visée était bien l'Ukraine, ainsi que les groupes étrangers ayant établi des relations commerciales avec ce pays.


Cyberattaques : des modes opératoires dive
Votre ordinateur
Hameçonnage
1
Rançongiciel
2
Attaque
3
Cross-Site Scripting
DDoS
4
Pirates
Page 3

Graphisme DC

Les révélations d'attaques informatiques se multiplient, sans compter celles qui restent confidentielles. Ont été rendus publics entre août et septembre 2017 : la demande de rançon de plusieurs millions d'euros adressée à la chaîne américaine HBO, à laquelle les pirates « Mr Smith » auraient dérobé 1,5 téraoctet de données, dont certains scripts de la série Game of Thrones ; le piratage de la base de données EDGAR de la Commission des opérations en Bourse américaine (SEC), comportant les informations légales concernant les entreprises cotées ; le vol des bases de données de l'une des plus importantes agences d'évaluation de crédit américaines, Equifax, comportant les informations personnelles de 145 millions d'Américains, 700 000 Britanniques et près de 100 000 Canadiens ; l'accès par piratage à quatre mois d'échanges de courriers électroniques entre les 244 000 employés de Deloitte, société d'audit et de conseil (y compris en sécurité informatique) et ses clients, bon nombre de grands groupes cotés en Bourse.

Certaines de ces attaques informatiques s'apparentent à une « cyberguerre froide », comme l'affaire des centaines de faux comptes Facebook activés depuis la Russie propageant des messages publicitaires de campagne afin d'influer sur l'élection présidentielle américaine ou bien encore comme celle du piratage de l'agence de presse qatarie, dont une fausse dépêche a enflammé les relations entre les pays du Golfe en mai 2017.

Face à ces événements, le problème majeur reste la difficulté à identifier avec certitude le commanditaire de ces actions, tandis que l'internet amplifie la puissance de *« l'arme douce »* qu'est la manipulation de l'information. Dans un contexte de fortes suspicions à l'égard du Kremlin, le gouvernement américain a d'ailleurs donné trois mois, à compter de septembre 2017, à ses ministères et ses agences fédérales pour désinstaller les logiciels anti-virus de l'éditeur russe Kaspersky Lab, comptant parmi les géants mondiaux de la cybersécurité. *« Il est tout à fait possible de monter une attaque pour que 98 % des traces digitales qu'elle va laisser désignent quelqu'un d'autre*, a expliqué Sandro Gaycken, directeur du Digital Society Institute de Berlin, lors de la Conference on Cyber Conflict (CyCon) organisée par le Centre d'excellence en cyberdéfense de l'Otan à Tallinn en juin 2017. *Des criminels ont tout intérêt à se faire passer pour des États, des États ont tout intérêt à se faire passer pour des criminels. Il est assez facile de faire croire que votre attaque vient de la Corée du Nord. »*

Néanmoins, la question cruciale reste la parade à trouver à ce nouveau type de conflit planétaire. Les experts présents à la conférence CyCon ont rappelé avec insistance qu'*« une chaîne n'est jamais aussi solide que son maillon le plus faible »*. Un lien hypertexte, une pièce jointe, une clé USB, infectés et utilisés par mégarde, ou encore un mot de passe trop simple constituent l'élément déclencheur de la plupart des piratages. Si la faille provient souvent d'une erreur humaine, il n'en reste pas moins que les consignes de sécurité prodiguées aux entreprises et aux citoyens constituent une solution illusoire. *« Demander aux particuliers de sécuriser leur ordinateur revient à leur demander d'installer un bouclier antimissile dans leur jardin. Cela ne fonctionne pas »*, écrit Ko Colijn, expert néerlandais en sécurité et défense, dans les colonnes du quotidien *NRC Handelsblad* du 15 mai 2017, alors que WannaCry avait touché les Pays-Bas.

Dans les entreprises, l'inventaire du parc informatique n'est pas toujours une priorité et l'installation des mises à jour nécessite du temps, et même l'arrêt de la production dans les usines comme ce fut le cas pour Renault en mai dernier. *« Nous devons faire plus attention aux mises à jour de sécurité*, reconnaît Jose-Vincente de los Mozos Obispo, directeur des fabrications du groupe automobile. *Chez nous mais aussi chez les fournisseurs. Il n'y avait pas que notre système qui était concerné… »*

La balle peut également être renvoyée dans le camp des éditeurs de logiciels qui, contrairement aux industriels d'autres secteurs comme l'automobile, ne sont jamais poursuivis pour défaut de fabrication. *« Les fournisseurs de logiciels transfèrent tous les risques associés à leurs produits à l'utilisateur par les accords de licence, que les tribunaux considèrent en général comme un contrat exécutoire »*, explique Jane Chong, spécialiste des questions juridiques en matière de sécurité nationale à la Hoover Institution. Pour certains spécialistes, il est temps d'établir des normes de sécurité imposables aux éditeurs de logiciels. *« La solution va être de réglementer. Il faut qu'on change les priorités tout de suite,* insiste Bruce Schneier, directeur de la technologie à IBM Resilient. *On a choisi de faire rapide et pas cher. Attendez que ça arrive à votre voiture, votre réfrigérateur, aux systèmes électroniques d'un avion ou à votre serrure connectée, et que vous ne puissiez plus rentrer chez vous »*.

Au moment de l'attaque WannaCry, le lanceur d'alerte Edward Snowden a de son côté vivement critiqué, *via* Twitter, la NSA qui *« a laissé cette faille de sécurité exister pendant plus de cinq ans »*, au bénéfice de son activité de surveillance au lieu de la dénoncer afin que les éditeurs de logiciels puissent y remédier. De son côté, le groupe Microsoft a dénoncé la logique des États en matière de sécurité informatique. *« Le stockage de vulnérabilités par les gouvernements est un problème,* écrit Brad Smith, son directeur juridique, sur un blog du groupe. *À plusieurs reprises, des failles dans les mains de gouvernements ont été publiées, causant de gros dégâts »*, et de qualifier la cyberattaque WannaCry de *« lien troublant entre les deux plus grandes menaces pour la cybersécurité : le crime organisé et les États »*. Pour l'ONG Openrightsgroup, la NSA et le GCHQ, son allié britannique, *« portent une part importante de la responsabilité »*.

« Il y a une prise de conscience que l'Europe doit accélérer la cadence. Nous nous sommes engagés à revoir d'ici à septembre notre stratégie de cybersécurité, qui date de 2013 », a déclaré Julian King, commissaire européen chargé de la sécurité, à l'occasion de sa rencontre avec le ministre français de l'intérieur fin juin 2017. Ainsi, parmi les mesures annoncées par la Commission européenne en septembre 2017, il y a la transformation de l'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en Agence de la cybersécurité dont la mission sera axée sur la préparation et la réponse aux cyberattaques ; l'harmonisation de la procédure de certification garantissant que les biens et les services vulnérables répondent aux exigences minimales de sécurité et la préparation d'un plan de réaction rapide des 28 en cas d'attaque. Et le commissaire européen d'ajouter : *« Si l'on veut aider les citoyens et toutes les entités concernées à être plus responsables, il faut impliquer aussi les géants du Net. »*

Sources :

- « WannaCry ravive le débat sur les failles de sécurité », Martin Untersinger, *Le Monde*, 17 mai 2017.

- « Piratages informatiques : le maillon faible humain », Michel Moutot, AFP, tv5monde.com, 1er juin 2017.
- « Europe : la lutte contre la cybercriminalité et les incitations au terrorisme s'intensifie », Catherine Chatignoux, *Les Echos*, 27 juin 2017.
- « Les mystères de la cyberattaque géante de Petya », Damien Leloup avec Benoît Vitkine (à Kiev), *Le Monde*, 29 juin 2017.
- « Renault, un mois et demi après WannaCry », Julien Dupont-Calbo, *Les Echos*, 29 juin 2017.
- « Les mystères de « Petya « , faux rançongiciel mais vrai virus destructeur », Martin Untersinger, *Le Monde*, 4 juillet 2017.
- « Virus « Petya » : de nouveaux éléments éclairent le mécanisme de diffusion du logiciel », *Le Monde* , 6 juillet 2017.
- « L'Etat doit protéger les citoyens », Ko Colijn, *NRC Handelsblad*, 15 mai 2017 in *Courrier internationa*l, n° 1392 du 6 au 12 juillet 2017.
- « Aux éditeurs de logiciels d'agir ! », Jack Detsch, *The Christian Science Monitor*, 15 mai 2017 in *Courrier international*, n° 1392 du 6 au 12 juillet 2017.
- « Les hackers de « Game of Thrones » réclament une rançon à HBO », Maelle Lafond, *Les Echos*, 9 août 2017.
- « Sur Facebook, des centaines de faux comptes ont cherché à influencer l'élection américaine », *Le Monde*, AFP et AP, LeMonde.fr, 7 septembre 2017.
- « L'éditeur de logiciels russe Kaspersky banni des ordinateurs fédéraux américains », Martin Untersinger, *Le Monde*, 14 septembre 2017.
- « Etats-Unis : le gendarme de la Bourse victime de pirates informatiques en 2016 », AFP, tv5monde.com, 21 septembre 2017.
- « Piratage de CCleaner : la piste de l'espionnage économique ciblé », Martin Untersinger, *Le Monde*, 22 septembre 2017.
- « La firme d'audit et de conseil Deloitte victime d'un piratage », Martin Untersinger, *Le Monde*, 27 septembre 2017.
- « Equifax : près de 700 000 Britanniques affectés par le piratage », AFP, tv5monde.com, 11 octobre 2017.

Categorie

1. Infographies
2. Usages

date créée
16 novembre 2017
Auteur
francoise