Wolf Philippe
Institut de Recherche technologique SystemX, Saclay
F-91400
https://www.irt-systemx.fr/
communication [at] irt-systemx.fr

Pièges et obscurité numérique

Résumé.— L'obscurité et la complexité des technologies numériques les prêtent aux pièges, voire les encouragent parfois. Il se crée quotidiennement presque cent mille nouveaux codes ou programmes informatiques malveillants principalement par des techniques de mutations intentionnelles, moins rares mais plus provoquées que les mutations génétiques.
Le vocabulaire emprunte à la biologie (virus), à la mythologie (chevaux de Troie, exploits, machines zombie) et à d'autres domaines de l'activité humaine (portes dérobées, *keylogger*, *ransomware* ou rançongiciel, *wiper* ou essuie-glaces) pour un usage dual à la fois civil (espionnage, cybercriminalité) et militaire (renseignement, cyberguerre) dont il est très difficile de lever les ambiguïtés (qui m'attaque ?, quel dommage ?, comment ?, pourquoi ?).

Mots clés.— Cyberespace, Porte dérobée, virus, Code malveillant, Ver, Cheval de Troie, Espiogiciel, Rançongiciel, Philippe Wolf, *Les Cahiers d'AGORA*

Traps and Digital Darkness

Abstract. — The darkness and complexity of digital technologies lend them to traps, or even sometimes encourage them. They create daily almost one hundred thousand new malicious computer codes or programs mainly by intentional mutation techniques, few but more provoked than genetic mutations.
Vocabulary borrows from biology (viruses, worm), mythology (Trojan horses, exploits, zombie machines) and other areas of human activity (backdoor, keylogger, ransomware, wiper) for a dual use both civilian (espionage, cybercrime) and military (intelligence) of which it is very difficult to remove ambiguities (who attacks me?, damage?, how?, why?).

Key words.— Cyberspace, backdoor, virus, malware, worm, Trojan, spyware, ransomware, Philippe Wolf, *Les Cahiers d'AGORA*

Remarque préliminaire : nous employons volontairement mais sans abus le jargon des informaticiens en donnant une définition des termes essentiels (en encadré).
Ce vocabulaire participe aussi de l'obscurité numérique. La numérisation de nos sociétés va cependant rendre ces termes de plus en plus familiers

Introduction

Piège : Artifice dont on se sert pour tromper quelqu'un et parvenir à ses fins, pour mettre quelqu'un dans une situation sans issue.

L'obscurité et la complexité des technologies numériques les prêtent aux pièges, s'ils ne les encouragent parfois. Ils se créent quotidiennement presque cent mille nouveaux codes ou programmes informatiques malveillants principalement par des techniques de mutations intentionnelles, moins rares mais plus provoquées que les mutations génétiques.

Dans un travail sur le lien entre la cyberguerre et la géographie, nous proposions un nouveau modèle de géographie du cyberespace à sept dimensions en tentant de répondre aux questions suivantes :

« Existe-t-il une géographie du cyberespace et peut-on donner une définition géographique du cyberespace ? Classiquement, ce dernier est défini comme un espace virtuel contenant des sociétés artificielles ; toutefois, dans cette définition, si le terme « espace » ne pose pas de problème, le terme « virtuel » lui est très imprécis car il masque la matérialité des composantes très géographiques de cet espace. Pis ! Il semble même laisser sous-entendre que cet espace est synonyme d'impunité ou d'inefficience ! En réalité, la meilleure définition du cyberespace est moins géographique que sociotechnique : il est plus pertinent en effet de le définir comme un espace d'interaction entre une technologie et un ensemble d'êtres humains et c'est en cela qu'il représente une véritable construction sociotechnique, c'est-à-dire qu'il procède d'une alliance entre, d'une part, les processus communicationnels agissant dans les interactions sociales ainsi que dans les relations interpersonnelles et, d'autre part, les avancées techniques et technologiques[1]*. »*

[1] PERNOT François, WOLF Philippe, Colloque « Guerre et géographie », 6-7 mai 2015, http://rgh.univ-lorraine.fr/articles/view/65/Cyberguerre_et_geographie

Nous y développions, à partir d'un « modèle NSA »[2], une géographie du cyberespace structurée en sept couches ou niveau : le « Niveau des Personnes non connectées » (PNC) ; le « Niveau des Personnes connectées » (PCO) ; le « niveau logique » (LOG ; le « niveau physique » (PHY) ; le « niveau géographique » (GEO) ; le « niveau temps » (TPS) et le « niveau cybersécurité » (CYS).

Couche : Les réseaux ouverts, ancêtres de l'Internet, ont été conçus, dès les années 1970, sous la forme d'une architecture en couches (référence ISO 7498) avec des notions de service, de protocole et d'interface. Notre analyse revisite et étend ces couches dans un modèle plus sociotechnique.

Nous allons revisiter ce modèle (PNC, PCO, LOG, PHY, GEO, TPS, CYS) sous l'angle des chausse-trappes[3] par quelques exemples probants : de l'article fondateur de Ken Thompson en 1984 au piégeage mathématique de l'algorithme Dual_EC_DRBG ; du ver dit Morris de 1988 jusqu'à Stuxnet ; des catalogues et ateliers offensifs secrets de la NSA et de la CIA dévoilés par des fuites récentes[4] au marché semi-ouvert des implants et des cyber-armes. Les possibilités de piégeage en combinant les couches physiques, syntaxiques et sémantiques sont infinies.

Le vocabulaire emprunte à la biologie (virus), à la mythologie (chevaux de Troie, exploits, machines zombie) et à d'autres domaines de l'activité humaine (*trapdoor* ou porte dérobée, *keylogger* ou enregistreur de clavier, *ransomware* ou rançongiciel, *wiper* ou essuie-glaces) pour un usage dual à la fois civil (espionnage, cybercriminalité) et militaire (renseignement, cyberguerre) dont il est très difficile de lever les ambiguïtés (qui m'attaque ?, quel dommage ?, comment ?, pourquoi ?)[5]. Nous finirons cet état des lieux par une exploration des nouvelles pistes de manipulations ouvertes par le devenir des robots et nano

---

[2] Notre matériel primitif était un document révélé par E. Snowden, le modèle en couches retenu par la National Security Agency dans une présentation de son outil de visualisation, d'exploration et d'analyse, en temps-réel, de l'état des réseaux numériques mondiaux intitulé "Treasure Map".

[3] L'image du piège métallique (ou pied de corbeau) n'est pas tout à fait adéquate car la fonction dite active d'un piège informatisé ne se déclenche souvent qu'après une conjonction d'événements conçue par son développeur pour augmenter sa discrétion.

[4] WOLF Philippe, *Snowden, Espionnage et Cyberespace*, « Services », renseignements, « grandes oreilles », de l'Antiquité au XXIe siècle : légendes et réalités, François Pernot et Éric Vial (dir.), les éditions de l'œil/la bibliothèque fantôme, novembre 2017.

[5] WOLF Philippe et VALLÉE, Luc *Cyber-conflits, quelques clés de compréhension*, 2011, https://www.ssi.gouv.fr/uploads/IMG/pdf/Cyber_conflits_quelques_cles_de_comprehension.pdf

robots mus par une intelligence artificielle de plus en plus efficiente, entre transhumanisme et catastrophisme éclairé.

Un cyberespace propice aux pièges

Trois « théorèmes »[6] construisent des caractéristiques du cyberespace favorables au piégeage[7].

Théorème 1 : un fichier numérique se clone parfaitement. Corollaire : toute information n'est pas bonne à numériser.

Une information, dès qu'elle est numérisée peut être dupliquée à l'infini. Sa publication sur Internet lui procure instantanément une diffusion globale et une rémanence qu'il est impossible de mesurer. Ce clonage favorise les fuites d'information organisées ou accidentelles. Dans les fuites de données, il n'y a pas vol mais copie ou emprunt.

Toutes les manipulations sont possibles sur les réseaux numériques ouverts. Le faux (ce qu'on appelle aujourd'hui les *fake news*) y côtoie le vrai sans que le recoupement des sources ne permette par son instantanéité, comme dans le renseignement traditionnel, une véritable qualification de la fiabilité de l'information. Enfin les rumeurs, les « traficotages de listings » (affaire *Clearstream* comme archétype en France) et autres canulars peuplent le cybermonde avec des conséquences parfois démesurées comme des manipulations de cours en bourse (le cours de bourse de Vinci dévisse de 7 milliards d'euros en 7 minutes, le 22 novembre 2016 à 16h06 ; la manipulation est datée avec précision[8]) ou des déstabilisations de cadres d'entreprise ou, plus récemment de pseudo manipulations électorales.

La cryptographie est la seule technique disponible pour protéger l'information en confidentialité et en intégrité. Elle réalise une réduction d'entropie sur les données à protéger grâce à de multiples clés qu'il s'agit de gérer comme les seuls secrets du système d'information. Comme l'affirme un de ses plus brillants spécialistes : « La cryptographie est généralement contournée, pas pénétrée. »[9] On y reviendra.

---

[6] La chaire « Informatique et sciences numériques » du Collège de France marque bien ces fortes filiations entre le cyberespace et les mathématiques.

[7] WOLF Philippe, *Trois théorèmes pour caractériser le cyberespace*, La Jaune et la Rouge, N°640, décembre 2008.

[8] On est ici au degré zéro du piège : un simple faux courriel, technique apprise en cours d'informatique en quelques minutes, mais précédé d'une préparation minutieuse en amont.

[9] SHAMIR Adi, keynote on "Financial Cryptography: Past, Present, and Future", 2016, https://www.lightbluetouchpaper.org/2016/02/22/financial-cryptography-2016/#comment-1456744

Théorème 2 dit de la confiance : « La morale est évidente. Vous ne pouvez pas faire confiance à du code que vous n'avez pas créé entièrement vous-même. (Spécialement du code des entreprises qui emploient des gens comme moi) »[10].

Dans un célèbre article, Ken Thompson, pionnier des systèmes d'exploitation et des logiciels de programmation modernes, piège nativement la fonction d'identification/authentification d'un système d'exploitation en créant une porte dérobée quasiment indétectable. Sa démonstration fait encore régulièrement l'objet de débats passionnés, mais traduit une réalité indéniable.

Porte dérobée (*Backdoor*)[11]

Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive. […]

Pour pouvoir parler d'informatique de confiance, il faut donc en maîtriser les techniques. La politique d'"information dominance"[12] s'accomplit, à travers les géants de l'Internet, dans la maîtrise technologique des pièces logicielles et matérielles constituant les systèmes numériques d'aujourd'hui mais également par la mise en place d'une exploitation commerciale des données personnelles comme modèle économique et aussi d'une hyper-surveillance favorisant les manipulations diplomatiques, sociales et économiques.

La quatrième révolution industrielle du numérique[13] équilibre quelque peu cette domination. L'Europe, quant à elle, existe principalement à travers son marché.

Théorème 3 dit « théorème du virus » : La détection d'un virus est indécidable à la fois par une analyse a priori ou une analyse dynamique.

---

10 THOMPSON Ken, *Reflections on Trusting Trust*, 1984, https://dl.acm.org/citation.cfm?id=358210

11 Pour la définition des termes, voir https://www.ssi.gouv.fr/entreprise/glossaire/

12 Prônée par les États-Unis depuis les travaux fondateurs des années 1990 notamment ceux de Martin C. Libicki.

13 En cours en Chine et plus généralement dans les pays sud-asiatiques.

Un virus est un programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes : réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc. Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB…

Il est parfois polymorphe. Se dit d'un ver ou d'un virus dont le code est chiffré, changeant le code de déchiffrement d'une infection à l'autre, et donc l'apparence et/ou la signature. Il peut donc muter pour se dissimuler comme certains virus humains et s'adapter à la victime.

Ce théorème, exposé en 1984 par Fred Cohen qui a réalisé la première étude *in vivo* sur les virus informatiques au sein de la "National Security Agency", est une variante logique du théorème de Rice qui démontre, en théorie de la calculabilité, que le problème de l'arrêt d'un programme informatique quelconque n'est pas décidable. Au-delà de l'aspect mathématique, il manifeste une double réalité : les pièges informatiques nouveaux contournent régulièrement les barrières installées et la fortune des vendeurs d'antivirus est assurée pour toujours.

Les filtres antitout commercialisés par le marché de la sécurité informatique (antivirus, antispyware, antihameçonnage, anti-rootkits, antispam, etc.) ne sont pas non plus, à l'exemple de la cryptographie, les solutions miracles annoncées. Ils masquent souvent les véritables enjeux d'une vraie politique de sécurité. Ils participent de la « sécurité par l'obscurité » qui n'a jamais démontré ses vertus dans la lutte effective contre la criminalité informatique dont le maître mot reste : « ni vu, ni pris ». La caractéristique principale de développement de la cybercriminalité, c'est la difficulté de l'attribution de l'attaque qui se joue des frontières physiques. L'impunité, sauf pour quelques « second couteaux » est presque totale.

Autres facteurs :

Le choix de ne pas sécuriser l'Internet a été fait en 1991[14] ; il est peu probable que la situation change radicalement dans les prochaines années (sécurisation des cœurs de réseaux ; chiffrement de bout en bout ; durcissement des protocoles de routage, etc.).

[14] Dans l'esprit d'un système ouvert et non centralisé, la mise en place de politiques de sécurité est laissée à l'initiative des sites connectés à l'Internet, voir par exemple https://www.ietf.org/rfc/rfc1244.txt

Mais le meilleur ou le pire selon que l'on se place du côté des défenseurs ou des attaquants est à venir avec de nouvelles technologies toujours plus complexes à maîtriser. Ainsi, le chiffrement homomorphe, dont la faisabilité n'a été démontrée qu'en 2009, permet de faire des calculs sur des données chiffrées. Du côté défensif, le graal de la protection des données personnelles est à portée de calcul ! Du côté offensif, des calculs distribués massifs pourront être organisés dans quelques années sans que quiconque s'en aperçoive.

Une brève histoire des cyber pièges

La société *Trend micro* recense en 2016 près de 700 millions de malware ou codes malveillants car chaque nouvelle souche génère de multiples variantes pour contourner la détection des logiciels anti-tout.

Code malveillant, logiciel malveillant (Malicious software, malware) Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau.

Quelques exemples chronologiques illustrent leurs méfaits et l'évolution des techniques piégeuses.

MORRIS : 1988

Couches concernées : PCO, LOG, TPS, CYS

Le premier virus de l'histoire (ver Morris de 1988) a paralysé l'embryon de ce qui allait devenir l'Internet en s'attaquant à plusieurs failles du service de messagerie. En quelques jours, ce sont plus de 6.000 serveurs qui vont être infectés sur un parc d'environ 60 000 serveurs constituant le premier réseau moderne, soit un taux d'infection de 10 %.

Le courrier non sécurisé reste aujourd'hui, presque 30 ans après, le vecteur privilégié des attaques informatiques, ciblées ou non.

Un ver (ou worm) est un logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis de l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.
Remarques : en dépassant l'étymologie stricte du virus informatique qui est devenu un mot-valise, les deux termes ver et virus sont relativement proches. Un ver est alors un virus qui se propage de manière quasi autonome (sans intervention humaine directe) via le réseau.

Robert Tappan Morris, né en 1965, est le fils de Robert Bob Morris, chercheur aux « Laboratoires Bell » de 1960 à 1986 puis à la « National Security Agency » (NSA) et spécialiste des questions de cryptographie. Le 26 juillet 1989, Robert Tappan Morris sera la première personne jugée selon la loi "Computer Fraud and Abuse Act" de 1986. La justice le condamne à 10 050 dollars d'amende et 400 heures de travaux d'intérêt général. Il est aujourd'hui professeur au Massachusetts Institute of Technology (MIT)[15].

L'absence de coordination lors des attaques du ver poussera l'Agence pour les projets de recherche avancée de défense (DARPA) à fonder le premier centre de coordination "CERT" (*Computer Emergency Response Team*). Le CERT aura alors pour mission de donner aux experts informatiques un point d'entrée unique permettant la coordination des moyens en cas d'urgence[16].

BLASTER : 2003

Couches concernées : PNC, PCO, LOG, GEO, TPS, CYS

Blaster est un ver informatique qui s'est répandu en août 2003 parmi les ordinateurs tournant avec les systèmes d'exploitation Windows XP et Windows 2000. Il provoqua également une instabilité dans tout le reste de la gamme Windows faisant redémarrer le système après avoir affiché le message suivant :

"I just want to say LOVE YOU SAN!!" (Je veux seulement dire que je t'aime SAN) "billy gates why do you make this possible ? Stop making money and fix your software!!" (billy gates pourquoi rends-tu ça possible ? Arrête de te faire de l'argent et corrige ton logiciel !!)"

---

15 Sa page personnelle est ici : https://pdos.csail.mit.edu/~rtm/

16 Le *Forum of Incident Response and Security Teams* coordonne en 2017 plus de 300 CERTs à travers le monde, voir https://www.first.org/

On l'appela aussi Nachi, Lovsan et Lovesan car il contenait ces deux chaînes de caractères au sein de son code (laissées délibérément par son auteur). Aujourd'hui, comme pour les cyclones, on a pris l'habitude de désigner les grandes familles de logiciels malveillants par un nom choisi souvent par les éditeurs des pseudo-vaccins. Cela donne lieu à quelques batailles commerciales souterraines[17].

Blaster a exploité une vulnérabilité de type débordement de mémoire qui était présente dans le service *DCOM RPC* de Windows XP/2000. Il se propageait rapidement vers des adresses Internet générées aléatoirement. Une fois infecté, l'ordinateur s'éteignait après 60 secondes. Le ver était programmé pour commencer une attaque (quatre jours après son apparition) de type *SYN flood* sur le site des mises à jour Windows (windowsupdate.com) ce qui a forcé Microsoft à rediriger le site vers un autre nom de domaine.

Les dommages ont été estimés à plus de 2 milliards de dollars car des centaines de milliers d'ordinateurs ont été infectés. Le virus fut aperçu pour la première fois dans la nature le 11 août. Sa vitesse de propagation augmenta exponentiellement jusqu'à atteindre un pic le 13 août. Seule l'efficacité des filtrages effectués par les fournisseurs d'accès à Internet ainsi que la publicité qu'a entraîné sa rapide propagation ont permis de ralentir celle-ci.

Le 29 août 2003, Jeffrey Lee Parson, un jeune homme de 18 ans, fut arrêté pour avoir créé la variante B du ver Blaster. Il plaida coupable et fut condamné à 18 mois de prison.

Blaster a généré des effets collatéraux. La grande panne électrique du jeudi 14 août 2003 qui avait gravement touché le nord-est de l'Amérique du Nord, avait été expliquée initialement par une conjonction de phénomènes météorologiques mineurs (chute d'arbre). La réalité était plus complexe[18]. Des systèmes automatisés de régulation sous *Windows* avaient été touchés par le ver Blaster. Des erreurs humaines avaient amplifié la crise. Cette information fut dévoilée en partie dans un rapport canadien préliminaire de novembre 2003[19]. Le rapport final officiel mentionne Blaster pour nier son impact sur l'incident[20].

---

[17] Cécile Dehesdin, Qui nomme les virus informatiques?, http://www.slate.fr/story/45985/noms-virus-informatique-duqu

[18] Voir l'analyse de Bruce Schneier, https://www.schneier.com/essays/archives/2003/12/internet_worms_and_c.html

[19] *Interim Report: Causes of the August 14th Blackout in the United States and Canada*, https://certs.lbl.gov/sites/default/files/interim-rpt-aug-14-blkout-03.pdf

[20] *U.S.-Canada Power System Outage Task Force*, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, voir https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

On voit ici une première manifestation des politiques de communications très filtrées autour des effets des logiciels malveillants par craintes d'atteintes aux images et aux réputations.

STUXNET : 2010

Couches concernées : LOG, PHY, GEO, TPS (cinématique lente), CYS

Les vulnérabilités des systèmes industriels connectés étaient flagrantes dès 2005. Il a fallu quelques années pour que le sujet émerge vraiment et bien sûr rien n'est réglé aujourd'hui, où l'on va vers l'usine 4.0 hyper connectée.

« Stuxnet est un ver informatique découvert en 2010 qui aurait été conçu par la NSA en collaboration avec l'unité 8200[21] *pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium. Le programme a été initié sous l'administration Bush et a continué sous l'administration Obama. Il fait partie de l'opération Olympic Games, et ses caractéristiques le classent parmi les APT*[22]*. »*

Les attaques ciblées avancées (ou APT : Advanced Persistant Threat)

Ces attaques principalement menées pour l'espionnage à des fins économiques ou scientifiques utilisent généralement deux modes opératoires connus d'infiltration initiale : l'attaque par point d'eau et l'attaque par hameçonnage ciblé.

La persistance réside dans le mode opératoire qui cherche, pour l'attaquant, à se garder une porte d'entrée dans le système visé.

Spécifique au système Windows, il a été découvert en juin 2010 par VirusBlokAda, société de sécurité informatique basée en Biélorussie. La complexité du ver est très inhabituelle pour un *malware*. Il a été décrit par différents experts comme une cyber arme, conçue pour attaquer une cible industrielle déterminée. C'est le premier ver découvert qui espionne et reprogramme des systèmes industriels. Il cible spécifiquement les systèmes dits SCADA utilisés pour le contrôle commande de procédés industriels produits par la société allemande Siemens. Il

[21] Dans une interview au Spiegel datée du 8 juillet 2013, Edward Snowden affirme : « NSA and Israel co-wrote it. », https://cryptome.org/2013/07/snowden-spiegel-13-0707-en.htm

[22] https://fr.wikipedia.org/wiki/Stuxnet

visait des automates programmables utilisés tant par quelques centrales hydro-électriques ou nucléaires que pour la distribution d'eau potable ou les oléoducs.

Le ver[23] aurait affecté 45 000 systèmes informatiques, dont 30 000 situés en Iran. Il a fait l'objet d'une littérature abondante mais a aussi suscité des développements de pièges ultérieurs s'inspirant de son architecture.

Le catalogue de pièges de la NSA : 2013

Couches concernées : PNC, PCO, LOG, PHY, GEO, TPS, CYS

Un catalogue[24] de 48 pages publié initialement par *Der Spiegel* et Jacob Appelbaum recense un outillage très complet permettant de piéger l'ensemble de la chaîne numérique. La fuite est attribuée initialement à Edward Snowden mais serait le fait d'une seconde source non identifiée[25].

Un exemple significatif concerne une technologie radar portant à quelques kilomètres et permettant de recueillir, probablement au niveau des bâtiments d'ambassades, des informations protégées avec franchissement de l'*air gap* (systèmes non connectés à l'Internet).

Le fonds Snowden dévoile également l'existence du service TAO (Tailored Access Operation) de la National Security Agency, actif depuis 1997 et dédié aux opérations offensives à base de cyber-armes. Doté d'un budget annuel avoisinant le milliard de dollars, il préfigure la militarisation de l'espace numérique qu'on peut dater à la création, le 20 mai 2010, du *United States Cyber Command* (USCYBERCOM) rejoint depuis par l'ensemble des puissances militaires, dont la France avec une montée en puissance dès 2019.

Algorithme piégé : de 2006 à 2014

Couches concernées : PCO, LOG (sous-couche sémantique)[26].

Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) est un algorithme qui a été présenté comme un générateur de nombres pseudo-aléatoires sécurisé utilisant des méthodes de cryptographie à courbe elliptique. Il a été standardisé par les 3

---

23 Analyse assez complète ici : https://www.xmco.fr/actu-secu/XMCO-ActuSecu-27-STUXNET.pdf

24 Disponible ici : https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf

25 Voir https://electrospaces.blogspot.fr/2017/09/are-shadow-brokers-identical-with.html

26 Pour une analyse de la couche sémantique, celle qui s'adresse à l'intelligence humaine, voir https://www.huyghe.fr/actu_1264.htm. Ici, il s'agit de l'abstraction mathématique qui spécifie le code informatique.

organismes NIST (National Institute of Standards and Technology) dès 2006, ANSI (American National Standards Institute) pour les USA et ISO (International Organization for Standardization) avec ses 163 pays membres.

Dès 2007, ses faiblesses ont été connues et publiquement critiquées bien avant que l'algorithme ne devienne une norme internationale. Il ne sera finalement retiré qu'en 2014, huit ans après.

Les mathématiques, elles-mêmes, permettent de confirmer que ce piège ne peut-être fortuit comme l'affirmera le mathématicien Michael Wertheimer[27], directeur à la retraite de la recherche à la NSA : «Avec le recul, la NSA aurait dû cesser de soutenir l'algorithme Dual EC DRBG immédiatement après que les chercheurs de sécurité ont découvert le potentiel d'une trappe. En vérité, je ne pense pas à une meilleure façon de décrire notre échec pour supprimer l'algorithme Dual EC DRBG comme autre chose que regrettable ». Cette confession tardive ne va pas jusqu'à l'aveu.

L'existence du programme Bullrun[28] de la NSA révélée par les fuites Snowden éclaire la stratégie suivie : « Insérer des vulnérabilités dans des systèmes de chiffrement commerciaux, des systèmes informatiques, des réseaux et des périphériques de communication et point de terminaison utilisés par des cibles. […] Influencer les politiques, les normes et les spécifications pour les technologies commerciales à clé publique[29]. »

La NSA avait payé 10 millions de dollars à la société américaine RSA pour implanter le piège dans une bibliothèque appelée BSAFE (acronyme commercial) utilisée pour sécuriser l'Internet. La porte dérobée permettait à la NSA de s'introduire dans les systèmes de communications sécurisés utilisant ce générateur de nombres aléatoires.

Il est envisageable, dans le futur, que des pièges sémantiques puissent exister sans que leur présence puisse être prouvée[30]. Le piège indétectable…

---

27 *The Mathematics Community and the NSA, Notices of the AMS*, Number 2, février 2015, http://www.ams.org/notices/201502/rnoti-p165.pdf

28 https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

29 *Revealed: how US and UK spy agencies defeat internet privacy and security*, 6 septembre 2013, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security Texte original : "Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets. […] Influence policies, standards and specification for commercial public key technologies ».

30 Nous ne développerons pas ici les arguments théoriques permettant de l'envisager, mais de telles pistes sont déjà explorées.

De Wannacry à NotPetya : 2017

Couches concernées : PNC, PCO, LOG, GEO, TPS, CYS

D'autres fuites plus récentes, provenant de sources non identifiées fin 2017[31], et dont la diffusion publique partielle est assurée par le site Wikileaks[32] ont généré, depuis mai 2017, la création de pièges dont la fonction principale n'est plus le chantage ou rançonnage[33] mais la destruction de données numériques.

Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

Ainsi le code malveillant auto-réplicant Wannacry (WannaCrypt, WanaCrypt0r), maquillé en rançongiciel dont il prend les apparences, exploite une faille de sécurité informatique de type 0-day[34] affectant, potentiellement, l'ensemble des systèmes Windows non mis à jour antérieurs à la version 10. Ce rançongiciel se caractérise par sa fréquence d'attaque qui a été d'au moins une tentative par seconde et de 226 800 adresses Internet affectées à son point fort. Des entreprises victimes ont communiqué, dont Renault en France.

0-day : catégorie particulière de codes d'exploitation qui cible des vulnérabilités qui ne sont pas encore publiquement annoncées par l'éditeur, le constructeur ou un chercheur en sécurité puisque la correction n'a été rendue disponible qu'après les premiers dégâts.

Ce logiciel ne semblait pas être développé à l'état de l'art (une hypothèse plausible semblerait alors être une diffusion prématurée ou accidentelle). Un de ses mécanismes particuliers est original. Il s'agit d'une fonction de coupe-circuit (*killswitch*) qui a beaucoup fait s'interroger

---

31 Une source possible est présentée ainsi par Wikipedia : The Shadow Brokers (littéralement « les courtiers de l'ombre ») est un groupe de hackers connu pour avoir dévoilé en 2016 des outils d'espionnages, entre autres, de l'Equation Group, une unité de hackers soupçonnée d'être lié à la National Security Agency (NSA).

32 https://wikileaks.org/vault7/

33 LAURIER Philippe, *Les cyberattaques et leurs préjudices sur les entreprises : quantification et qualification*, 19 septembre 2017, http://www.irt-systemx.fr/wp-content/uploads/2017/10/ISX-IC-Cyber-Risque.pdf

34 La principale faille est un exploit développé par la NSA intitulé EternalBlue et publié par le groupe de pirates *The Shadow Brokers*.

les spécialistes : c'est le non enregistrement d'un domaine sur Internet qui entraînait l'arrêt de la propagation du malware. Ce mécanisme a été supprimé dans des variantes plus récentes.

NotPetya qui doit son nom à la ressemblance avec le code malveillant Petya, découvert initialement en Ukraine en mars 2016, apparait le 27 juin 2017 et touche l'ensemble de la gamme Windows en exploitant une vulnérabilité (encore EternalBlue, code MS17-010 mais aussi EternalRomance) dont le correctif, publié en mars, n'a pas été appliqué dans certains environnements productifs (comme Saint-Gobain, Auchan et la SNCF en France). Il intègre deux outils de piratage volés à la NSA.

Contrairement aux habituels ennemis russes ou chinois, c'est la Corée du Nord[35] qui a été désignée comme source de ce logiciel destructeur.

Un marché légal

Le marché, dit de l'interception légale, développe depuis quelques années, à côté des équipements d'interception traditionnels « cœur de réseau », des outils logiciels et matériels intrusifs et ciblés vers les terminaux des utilisateurs.

La règle de commercialisation générale est celle de la prohibition appliquée aux exportations d'armements[36]. Mais ce marché reste mal ou insuffisamment régulé. Il favorise indirectement la prolifération des armes cybernétiques. On y trouve, pêle-mêle, des outils de dissimulation d'activité et les fameux chevaux de Troie numérique qui renouvellent le mythe à l'âge numérique.

---

[35] Comme l'affirme, par exemple, le Britain's National Cyber Security Centre (NCSC) http://www.bbc.com/news/technology-40297493

[36] Législation française en matière d'outils d'espionnage, https://www.ssi.gouv.fr/publication/legislation-en-matiere-doutils-despionnage/

Outils de dissimulation d'activité (Rootkit). Tout programme ou ensemble de programmes permettant de dissimuler une activité, malveillante ou non, sur une machine. Par extension, tout programme ou ensemble de programmes permettant à une personne malveillante de maintenir un contrôle illégitime du système d'information en y dissimulant ses activités. Par extension, programme ou ensemble de programmes permettant de dissimuler une activité, malveillante ou non, sur une machine. L'activité dissimulée peut être une activité sur le système de fichiers (création, lecture, écriture), une activité réseau, une activité en mémoire. Pour cela, un rootkit peut travailler dans l'environnement de l'utilisateur, sans droits particuliers, ou en profondeur dans le système d'exploitation, nécessitant par conséquent des droits d'exécution élevés.

Les chevaux de Troie permettent le piégeage à distance à presque la vitesse de la lumière. Dans l'histoire des guerres, il s'agit d'une révolution équivalente à celle des drones tueurs et bientôt autonomes qui projettent de la puissance sans projeter de vulnérabilités.

Cheval de Troie (Trojan Horse). Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante.

Pour citer une activité annexe à ce marché des cyber-armes, nous pouvons citer l'entreprise franco-américaine Zerodium fondée en 2015 à la suite de la dissolution de l'entreprise Vupen liée aux incertitudes juridiques pesant sur son activité. Elle pratique « la recherche de vulnérabilités dans les logiciels des principaux éditeurs mondiaux, afin de les revendre ensuite aux agences gouvernementales, comme la NSA, à des fins d'utilisations défensives ou offensives ».

Elle développe une solution dite du « bug bounty »[37] qui récompense jusqu'à la somme de 1 500 000 $[38] la fourniture d'une faille exploitable sur ordiphone.

---

[37] Le *bug bounty* est né en 1995 et connait un succès grandissant, même si l'on peut s'interroger sur son efficacité finale.

[38] Voir https://www.zerodium.com/program.html

Un bug bounty est un programme proposé par de nombreux sites web et développeurs de logiciel qui permet à des personnes de recevoir reconnaissance et compensation après avoir reporté des bugs, surtout ceux concernant des exploits et des vulnérabilités.

Une autre fuite d'information concernant la suite *FinFisher*[39] de produits de surveillance et d'intrusion informatique développée par *Gamma International*, la filiale allemande de *Gamma Group*, fixe le prix en 2014 d'une suite complète autour des 3 millions d'euros. L'efficacité de ces produits nécessite de plus des mises à jour régulières (annuellement autour de 10 % du prix).

Un marché souterrain

S'est développé autour de ce marché légal, un marché plus souterrain, qui contourne des arrangements internationaux et dont quelques fuites permettent d'illustrer l'ampleur.

Hacking Team, entreprise italienne basée à Milan, qui vend des logiciels offensifs servant à l'espionnage a été piratée le 5 juillet 2015. La publication d'un très important volume de données comprenant la messagerie des dirigeants de la société[40], dévoile qu'elle vendait des solutions de surveillance à des dictatures et gouvernements oppressifs[41]. De plus, la méthode de piratage a été décrite par un individu au pseudonyme de "Phineas Phisher"[42]. Il s'agit là d'une caractéristique inhabituelle. La société a été sanctionnée en juillet 2015 par le ministère du commerce italien d'un retrait de licence d'exportation hors de l'UE.

Pour la suite *FinFisher*, une même carte de 32 pays, utilisateurs de la suite, a été publiée[43]. Le logiciel aurait été par ailleurs impliqué dans un scandale d'écoutes illégales ayant secoué la Macédoine en 2015[44].

---

39 Voir https://wikileaks.org/spyfiles4/ et https://wikileaks.org/spyfiles/docs/DREAMLAB-2011-FinFPric-en.pdf

40 Disponibles ici : https://wikileaks.org/hackingteam/emails/

41 Une carte de 21 pays clients a été publiée, voir https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

42 *How Hacking Team got hacked*, 19 avril 2016, https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/

43 Voir https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

44 À l'origine de la crise en Macédoine, une folle histoire d'écoutes illégales, 18 mai 2015, https://tempsreel.nouvelobs.com/rue89/rue89-monde/20150518.RUE9114/a-l-origine-de-la-crise-en-macedoine-une-folle-histoire-d-ecoutes-illegales.html

Un rapport britannique officiel[45] conclut que :

« Gamma International UK Limited n'a pas agi conformément aux dispositions des lignes directrices de l'OCDE […]. L'approche de la compagnie n'était pas conforme aux obligations générales de respect des droits de l'homme […]. »

Ce marché, poussé également par une demande domestique de plus en plus forte[46], va croître de manière forte.

Et demain ?

Nous sommes entrés dans l'ère de l'*Internet of Everything*[47], c'est–à-dire la numérisation de l'ensemble des activités humaines via les réseaux cybernétiques, sociaux et autres. On nous annonce 50 milliards d'objets connectés en 2020 et 1 000 milliards en 2035 soit près de 200 dispositifs électroniques par personne, en considérant que les internautes constitueront plus de la moitié de l'humanité dès 2017. 500 millions d'applications offriront des services à partir de ces capteurs.

Cela ouvre un terrain de jeu immense pour les techniques de piégeage. « L'Internet est un marécage », affirme Louis Pouzin, l'un de ses pionniers français. Il devient dès lors facile d'imaginer des catastrophes numériques, sujet dont s'est déjà emparé le divertissement audiovisuel.

Pour que cet « Internet de toute chose » ne se transforme pas en « Internet du n'importe quoi », il faut pallier le manque de sécurité de certains de ces nouveaux objets individuels, insuffisamment protégés pour des raisons de coûts ou de consommation, en mettant en place des mécanismes de sécurité au niveau des systèmes globaux (véhicules, aéronefs, trains et tramways, implantations industrielles, etc.) qu'ils constitueront. Cela n'exonère pas d'une sécurité minimale les objets connectés « primaires » non embarqués dans un système complexe ou industriel tels qu'une caméra connectée, un cadre-photo, une station météo, une montre, un appareil d'e-santé ou même un drone de loisir, qui peuvent devenir les « couteaux suisses » de la guerre de l'information.

---

[45] Voir https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf

[46] Les sites de vente en ligne prolifèrent à l'étranger comme https://www.thehomesecuritysuperstore.com/spy.asp

[47] Le concept de Internet of Everything a été initialement créé par CISCO en 2013, comme étant « the intelligent connection of people, process, data and things ».

Une autre crainte touche à l'intelligence des robots et des nanorobots. Les transhumanistes et, le plus célèbre et médiatisé d'entre eux, Raymond Kurzweil, le futurologue et directeur de l'ingénierie chez Google, prédit que dans les années 2030 nos cerveaux auront la capacité de se connecter au Nuage informatique. Il annonce ainsi la naissance d'une nouvelle espèce, qui va réinventer l'humanité au cours des 30 prochaines années. « Nous serons plus drôles, plus sexy, et plus doués pour exprimer l'affection ». Selon lui, tout cela sera rendu possible par les nanobots – de minuscules robots faits de brins d'ADN – qui flotteront dans les capillaires de notre cerveau. Il considère l'ouverture de nos cerveaux à des modes de pensée principalement non biologiques comme la prochaine étape de l'évolution humaine, une étape équivalente à la découverte des outils pour nos ancêtres.

Là aussi, le champ d'action du piège va trouver un nouveau terrain que nous ne qualifierons pas de jeu tant les conséquences pourraient être dangereuses si l'on se fie au passé brièvement évoqué dans notre analyse.

Quelques autres définitions d'une typologie ouverte

Le « bestiaire » des cyber pièges est en continuel renouvellement sur des bases cependant bien établies. En voici quelques autres spécimens.

Bombe programmée, bombe logique (Logic bomb)

Logiciel malveillant conçu pour causer des dommages à un système informatique et qui est déclenché lorsque certaines conditions sont réunies.

Remarques : Certains virus contiennent une fonction de bombe logique : déclenchement à date fixe, déclenchement quand une adresse réticulaire (URL) particulière est renseignée dans le navigateur, etc.

Réseaux de machines zombies (Botnet)

Un Botnet, autrement dit un réseau de bots (botnet : contraction de réseau de robots), est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise.

Code d'exploitation (Exploit)

Tout ou partie d'un programme permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes.

Remarques : Les objectifs malveillants consistent souvent en une intrusion, une élévation de privilèges ou un déni de service. L'exploitation peut se faire directement à partir du système ciblé si l'utilisateur malveillant possède un accès physique (« local exploit »), ou à distance s'il s'y connecte (« remote exploit »).

Espiogiciel (spyware)

Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.