Se protéger d'une pandémie numérique

Valérie Viet Triem Tong, Jean-Louis Lanet

Se protéger d'une pandémie numérique

Valérie Viet Triem TongJean-Louis Lanet dans trimestriel 576
daté janvier-mars 2024 - 1542 mots

Si les virus numériques présentent des points communs avec leurs homologues biologiques, ils diffèrent en particulier par leur vitesse de propagation bien plus élevée. Ainsi, il est illusoire de vouloir bloquer une pandémie avec un vaccin numérique comme une mise à jour d'antivirus. C'est pourquoi il est nécessaire de prévoir des mécanismes génériques dans les antivirus et, surtout, pour l'utilisateur, d'adopter une prophylaxie numérique. Cette dernière passe par de bonnes pratiques dans les usages quotidiens.

Le terme « virus » appliqué à l'informatique remonte à 1983, lorsque l'Américain Frederick Cohen, alors étudiant, crée l'un des premiers codes malveillants : il définit un virus comme un programme informatique ayant la capacité de s'installer puis de s'exécuter sur une machine, avant de se propager dans un réseau par l'intermédiaire des machines voisines. C'est son enseignant, Leonard Adleman - connu pour avoir introduit le système cryptographique RSA, avec Ronald Rivest et Adi Shamir - qui, par analogie avec la biologie, propose le terme « virus » **(1)**. La similitude est en effet frappante : à l'instar de son pendant biologique, un virus informatique est un programme indésirable qui va infecter un « hôte » et cherchera ensuite à se propager vers les machines voisines de ce dernier.

Généralement, un virus informatique est très résilient et furtif, apte à s'assurer que la cible visée présente un intérêt pour son objectif. Il peut chercher à altérer le fonctionnement du système ou de l'information stockée, voire à l'exfiltrer. Parfois, il tente aussi de prendre le contrôle des ressources de la machine, comme sa capacité de stockage de données et sa puissance de calcul.

L'analogie peut être poussée plus loin : ainsi, on parle de cycle de vie d'un virus informatique, avec des phases d'infection, d'incubation, de propagation et d'activation. Durant la phase d'infection, le virus est encore hors de l'hôte, et il cherche à exploiter une vulnérabilité pour le compromettre. Cette faille est la porte d'entrée du virus dans la machine. Au cours de la phase d'incubation, le virus peut s'assurer de sa résilience sur l'hôte par des réplications de son propre code, des modifications de la séquence de démarrage, la recherche de la présence d'outils d'analyse. Une fois répliqué, le virus se propage vers d'autres machines hôtes. Cette diffusion peut s'effectuer par le biais d'un support matériel (DVD, clé USB), par un site Internet infecté, ou encore l'envoi d'une pièce jointe dans un email. Elle se fait aussi sur les autres éléments du réseau de manière à contaminer le plus d'appareils possible, généralisant ainsi l'infection. La dernière étape est l'activation de la charge malveillante, dont le déclenchement peut dépendre de la survenue de divers événements comme la réception d'un message, une date précise, la frappe sur le clavier de certains caractères, un appel système, l'écoulement d'un laps de temps ou encore une combinaison d'événements.

La comparaison entre les deux sortes de virus a toutefois ses limites. L'informatique est une science jeune, de sorte que les virus numériques n'existent que depuis peu. À l'inverse, les biologiques sont apparus il y a des milliards d'années. La connaissance du code d'un virus informatique permet de développer rapidement une solution de remédiation, alors qu'un vaccin biologique peut être très long à développer, voire impossible. De plus, un virus informatique n'est pas capable d'évolution, seulement de mutations préprogrammées qui ne modifient que l'apparence de son code, contrairement au virus biologique dont la charge virale peut évoluer.

La dernière différence, qui rend la protection difficile, est liée à la vitesse de propagation de l'infection. La pandémie de

Covid-19 a mis plusieurs mois à devenir un phénomène mondial. À l'inverse, une infection informatique peut se généraliser en quelques heures, rendant le ciblage des mécanismes de protection impossible : la défense contre les virus numériques doit être de nature générique.

L'un des premiers virus à s'être propagé hors des laboratoires a été écrit en 1982 par un adolescent de 15 ans. Baptisé *Elk Cloner,* il infectait les ordinateurs Apple II. Son vecteur de transmission était des disquettes, utilisées à l'époque pour stocker et transmettre les données. Le virus se propageait à travers des copies de disquettes transmises de proche en proche.

En raison du faible nombre d'équipements et de la lenteur des moyens de transmission, les virus informatiques sont restés sous le radar pendant de nombreuses années. À la fin des années 1990, 2 % seulement de la population mondiale avait accès à Internet avec un ordinateur. Il fallait utiliser un modem qui transmet les données avec un débit très faible par rapport à ce que l'on connaît aujourd'hui. L'accroissement de la capacité des réseaux a radicalement changé la donne, marquant un tournant dans la capacité de propagation des virus.

« I LOVE YOU » OU LA PREMIÈRE PANDÉMIE NUMÉRIQUE

En 2000, le virus « I Love You » utilisait le réseau Internet comme moyen de dissémination, exploitant les contacts email pour se propager. L'utilisateur recevait un message ayant pour objet « Iloveyou », accompagné d'une pièce jointe. Tenté de cliquer sur le fichier joint « Love-Letter-For-You.txt.vbs », il déclenchait l'envoi du même email à tous ses contacts et voyait dans le même temps une partie de ses documents numériques détruits. « I Love You » infectait les ordinateurs capables d'interpréter les programmes écrits en langage VBScript, majoritairement sous Windows. Il fut l'initiateur de l'ingénierie sociale par l'utilisation d'un mail au titre accrocheur. Cette combinaison d'une propagation par Internet et d'une incitation à cliquer fut redoutablement efficace : on estime qu'à l'époque, « I Love You » a infecté 10 % des ordinateurs connectés dans le monde (environ 2,5 millions de machines). La propagation était incontrôlable tant que les ordinateurs n'étaient pas dotés d'antivirus capables de détecter le virus et de prévenir son exécution. Cette première pandémie numérique a coûté, selon les sources, entre 5 et 15 milliards de dollars.

Par la suite, des milliers de virus informatiques de toute nature ont vu le jour. Certains sont de type *ransomware,* un logiciel d'extorsion qui prend en otage les données personnelles ou bloque l'ordinateur en échange d'une rançon. Par principe, les virus exploitent les failles des logiciels et des machines qu'ils infectent. En 2017, le *ransomware* Wannacry avait utilisé comme porte d'entrée sur son hôte une vulnérabilité découverte peu auparavant dans le protocole de communication *Server Message Block* (SMB). Ce dernier, qui permettait le partage de ressources entre deux ordinateurs, était très populaire sur Windows. Hélas, plus le virus exploite une faille existant dans un protocole ou un service largement utilisé, plus il est susceptible de se propager rapidement. La diffusion de Wannacry fut en effet fulgurante : en quelques heures seulement, il s'est répandu à 300 000 machines dans plus de 150 pays **(2)**. L'attaque a été stoppée grâce à l'activation d'un *kill switch*, un dispositif d'arrêt d'urgence découvert dans son code. Le virus a ensuite été éradiqué lorsque la vulnérabilité qui constituait sa porte d'entrée a été réparée et que toutes les instances de son code ont été effacées.

La propagation de tels virus est incontrôlable, de sorte qu'ils peuvent se retourner contre leurs créateurs, puisque ces derniers utilisent eux aussi des services hébergés sur des ordinateurs connectés à Internet. Ainsi, la présence d'un *kill switch* dans Wannacry suggère l'idée que les concepteurs du virus avaient mis en place cette ultime mesure afin de se protéger eux-mêmes.

Les développeurs, qui ne manquent pas d'imagination, conçoivent désormais des logiciels malveillants contrôlables à distance, dotés de fonctions de commande et de contrôle permettant leur pilotage. L'ensemble des machines infectées par un même virus devient alors un seul réseau décentralisé de machines dites « zombies » que l'on appelle un *botnet* - ou réseau de robots. Il est difficile d'estimer sa taille, d'autant plus que celui-ci peut être composé d'objets connectés comme des caméras de surveillance ou des réfrigérateurs, souvent peu protégés **(3)**. De tels réseaux de machines sont ensuite activables à distance, permettant de lancer des campagnes d'attaques d'envergure.

À la différence d'un virus biologique, un virus numérique est écrit par un groupe d'êtres humains. Si les premiers virus relevaient plutôt du défi technique ou de la « petite malveillance », les actuels servent maintenant des revendications plus politiques ou financières. En 2023, le logiciel espion Pegasus est utilisé pour surveiller des journalistes, avocats, dissidents politiques et militants des droits humains. Les gains financiers sont aussi des moteurs de développement des logiciels malveillants. Ainsi, certains *botnets* sont aujourd'hui employés par des cybercriminels pour générer de faux clics ou de faux avis sur des services en ligne dans le but d'engendrer des bénéfices pour les opérateurs.

DES PROGRAMMES TOUJOURS PLUS NOMBREUX ET SUBTILS

Chaque année, des dizaines de millions de nouveaux logiciels malveillants sont détectés. Certes, les antivirus sont de plus en plus puissants, mais les programmes qu'ils combattent sont toujours plus nombreux et subtils. La partie contre les virus informatiques est-elle pour autant perdue ? Non, à condition d'adopter des gestes prophylactiques. Pas question de masque FFP2 ici, mais de bonnes pratiques. Par exemple, il convient d'utiliser des mots de passe robustes et différents pour chaque site, et les changer régulièrement. Il faut aussi garder les logiciels sur votre ordinateur, téléphone ou tablette à jour (utiliser les dernières versions, et faire les mises à jour préconisées à partir des sites officiels des éditeurs). Parmi les autres mesures recommandées, la désactivation de l'ouverture automatique de documents. Enfin, il faut rester très prudent avec la messagerie électronique et les réseaux sociaux.

À l'heure de la généralisation d'Internet, sur ordinateur, téléphone - plus de 8 milliards de portables offrant un accès au réseau sont désormais utilisés -, tablettes, montres, réfrigérateurs, ces mesures peuvent sembler relever du simple bon sens, mais elles constituent une protection raisonnable. Les compagnies d'assurances estiment que, dans les années à venir, les risques cyber et ceux liés au changement climatique seront les plus coûteux à couvrir, appelant les pouvoirs publics à en assumer leur part **(4)**.

Image d'ouverture : Des employés de l'Agence coréenne de l'Internet et de la sécurité à Séoul, en Corée du Sud, surveillent des tableaux électroniques décrivant la transmission du logiciel malveillant (ransomware) Wannacry, le 15 mai 2017.

Crédit image : YUN DONG / JIN / AP / SIPA

(1) https://www.wired.com/2009/11/1110fred-cohen-first-computer-virus/

(2) https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

(3) M. Abu Rajab et al., HotBots'07 : Proceedings of the First Workshop on Hot Topics in Understanding Botnets, 2007.

(4) https://www.genevaassociation.org/publication/cyber/cyber-risk-accumulation-fully-tackling-insurability-challenge

8

MILLIARDS
DE TÉLÉPHONES PORTABLES

ayant un accès à Internet sont utilisés dans le monde.

VALÉRIE VIET TRIEM TONG

INFORMATICIENNE, RENNES

Professeur en informatique à CentraleSupélec, campus de Rennes, elle mène des recherches sur les attaques contre les systèmes informatiques.

JEAN-LOUIS LANET

INFORMATICIEN, RENNES

Ancien directeur de recherche au centre INRIA de l'université de Rennes, il est spécialiste des systèmes de sécurité embarqués.