PAR
GILLES FAVIER
DG D'ENCELIS, STRATÉGIE ET GOUVERNANCE SÉCURITÉ

Programmes malveillants, logiciels espions, états et cybercriminels

Depuis la fin des années 90 nous avons été les témoins privilégiés de l'ascension et de l'organisation mondiale du secteur du numérique. Nous avons parallèlement assisté à une professionnalisation du secteur de la cybercriminalité, investi par les acteurs de l'économie traditionnelle aujourd'hui reconvertis : « *hacktivists* », mafia, contrebandiers et états. Ils se livrent une guerre d'un nouveau genre, sans champ de bataille ni frontières, sans adversaires, feutrée et sans victimes collatérales car toute victime y est utile.

Les motivations des cybercriminels ont évolué avec les capacités technologiques et l'élargissement du potentiel de nuisance. Le début des années 1990 est la période des balbutiements, les « virus » sans réelles fonctions (Win.Vir_1_4) de cette époque relèvent plus de la curiosité intellectuelle des experts que de la malveillance. Ils ont peu à peu muté pour devenir de véritables boîtes à outils (*Fanny & Stuxnet*) à l'instar des logiciels des principaux éditeurs du marché.

Aujourd'hui, ces « *malware* » les plus sophistiqués sont dotés de toutes les fonctionnalités attendues pour un espionnage discret et efficace de leur cible : enregistrement des frappes claviers, capture d'écran, enregistrement audio et vidéo, envoi de fichiers, exécution de commandes et prise de contrôle à distance sans oublier l'effacement sécurisé des traces et, pour certains, le moyen de s'intégrer au *firmware* des disques durs (*Fanny & Grayfish*). Pilotés à distance depuis des centres de contrôle (C&C), leurs auteurs ont alors les mains libres pour vendre des services ou mener à bien leurs desseins. Ces programmes malveillants s'appuient le plus souvent sur des failles de sécurité parfois non corrigées par les éditeurs (zéro-day) et pour lesquelles aucun système de sécurité du marché n'est en mesure de réagir efficacement.

Si nous en sommes là, c'est précisément pour des raisons économiques

Dès 1991 le DoD (*Department of Defense*) a mis en évidence qu'il ne serait pas économiquement viable pour les éditeurs de développer des logiciels sécurisés. Ce constat, toujours valable aujourd'hui, offre un avenir prometteur tant à ceux qui exploitent les failles qu'aux sociétés de sécurité. En effet, dans leur course pour la maîtrise du marché (*lock-in*), les éditeurs développent les fonctionnalités nécessaires aux utilisateurs finaux et relaient la sécurité au rang d'amélioration. Les nouveaux logiciels introduiront donc systématiquement de nouvelles vulnérabilités même s'ils corrigent les anciennes. Pour preuve, les versions les plus sécurisées de Linux sont encore basées sur des noyaux anciens et embarquent peu de fonctionnalités de base. Le temps manque aux équipes, souvent bénévoles, pour contrôler, corriger et valider le niveau de sécurité.

Ce qui est surprenant dans cette course entre les pirates et les éditeurs de logiciels de sécurité est que les méthodes employées par les premiers sont les

> ***Les nouveaux logiciels introduiront systématiquement de nouvelles vulnérabilités même s'ils corrigent les anciennes***

mêmes qu'il y a 5000 ans. Sun Tzu (*L'art de la guerre*) et plus récemment Kevin Mitnick dans *The art of deception* expliquent pages après pages la nécessité de connaître son adversaire afin d'exploiter ses faiblesses. La tromperie est employée dans toutes les attaques visant aussi bien les organisations que le grand public et se matérialise très simplement au travers d'une clef USB offerte, d'emails ciblés ou plus récemment d'applications mobiles à télécharger. In fine, le seul changement depuis Sun Tzu tient dans la technicité des attaques.

Les trois clefs du succès d'une action d'envergure discrète et bénéfique pour son commanditaire sont : le temps, le talent et l'argent

Les états et les organisations criminelles développent leurs propres programmes espions (bien plus performants que ceux en vente sur les réseaux parallèles) : *Pawn Storm* (soupçons Russe), *Stuxnet & Flame* (soupçons NSA), *Casper* (soupçons Français) pour collecter des informations et déstabiliser leurs cibles. Ces dernières sont très variées : industrie, recherche, nucléaire, ministères, lobbies… Les organisations criminelles, qu'elles soient soutenues ou non par des états, développent aussi des trésors d'ingéniosité et disposent d'une capacité de nuisance phénoménale : *Guardian of Peace* (*Sony Pictures Entertainment*), Cabarnak (100 banques victimes) sont responsables de pertes évaluées en milliards de dollars, sans parler des impacts sur la réputation. Que se passera-t-il quand ces logiciels se retourneront indifféremment contre leurs auteurs ou une nouvelle cible choisie par un pirate informatique ou un « *hacktivist* » talentueux ?

Sachant que, d'une part la fraude (Cabarnak) et l'espionnage peuvent rester invisibles pendant des années : c'est le cas de l'organisation « Equation » soupçonnée d'agir pour le gouvernement américain depuis près de vingt ans et qui n'a été démasquée qu'en 2015 par la *Global Research & Analysis Team* de Kaspersky, d'autre part les attaques ou les logiciels qui font l'objet de publication représentent uniquement la partie visible de l'iceberg, on peut légitimement s'interroger sur l'envergure réelle de ces agissements et les stratégies à mettre en place pour nous en protéger.

Les entreprises, prises individuellement, plieront nécessairement dans le rapport de force, tant technique que financier, qui les oppose aux organisations désireuses de les déstabiliser.

Plusieurs stratégies émergent pour faire face à ces nouveaux risques tout en maintenant l'outil informatique comme un des moteurs de la production de valeur :

- La prise en compte du facteur humain : victime ou acteur d'une malveillance, l'individu reste le principal vecteur de propagation des attaques informatiques citées (biais de confirmation, illusion positive) ;
- l'identification précise des valeurs et périmètres qui doivent être protégés (Comex, R&D…) afin de déployer des moyens de protection adaptés et à des coûts raisonnables ;
- l'adaptation, la technicité des attaques a évolué, l'entreprise désormais attaquée en son sein doit revoir sa stratégie. Le modèle du bastion imprenable est désormais dépassé, nous sommes aujourd'hui dans un aéroport où de multiples acteurs interagissent, les contrôles de sécurité doivent être réalisés en permanence et à tous les niveaux ;
- la mutualisation des efforts dans la collaboration non seulement inter-entreprises mais aussi avec leurs fournisseurs de solutions de sécurité. Plusieurs initiatives sont d'ores et déjà à l'œuvre en France : cloud souverain, Cigref…

Une révolution est plus que souhaitable dans la définition des stratégies de sécurité. Celles-ci doivent être pilotées en fonction des effets attendus et des risques à couvrir et non plus seulement par les coûts. En matière de protection contre les risques, tout est une question de méthode, de capacité et de volonté. ●