2017 : l'année du ransomware et des objets connectés piratés ?

Les cybercriminels ont eu fort à faire en 2016, année qu'ils ont passée à exploiter d'anciennes vulnérabilités, mais aussi à développer de nouvelles techniques.

En 2017, cette tendance devrait se poursuivre à un rythme d'autant plus accéléré que le nombre d'ordinateurs, de laptops, de smartphones et autres appareils connectés à internet va exploser. En outre, plus les utilisateurs seront conscients des menaces et apprendront à les contrer, plus les criminels renforceront la sophistication des technologies, leurs stratégies et leurs méthodes.

À la maison ou au travail, nous vivons dans un monde de plus en plus connecté, et le nombre de dangers susceptibles de nous affecter ne cesse d'augmenter. De par l'explosion des appareils mobiles personnels, l'adoption massive des applications cloud et l'impact croissant de llsquo;Internet des objets, les menaces informatiques se présentent aujourd'hui sous d'innombrables formes.

L'année du "Ransomware pour les nuls"

2016 est indéniablement l'année du ransomware, mais devrait bien vite être dépassée par 2017 tant le déploiement de ces attaques a récemment gagné en simplicité. Ce type de logiciel malveillant chiffre les données personnelles des utilisateurs et ne les rend accessibles que contre rançon. Plus de 150 nouvelles formes de ransomwares ont été détectées en 2016, uniquement pour Windows ! Ce nombre est appelé à s'envoler en 2017, au vu des nombreux programmes ransomwares open-source disponibles sur GitHub et sur les forums de piratage. Ces logiciels sont disponibles gratuitement et exploitables par toute personne ayant les notions de base pour adapter le code existant.

Si un pirate en herbe n'a pas les capacités nécessaires pour créer son propre malware à partir d'un code libre, il peut désormais faire appel très facilement à un "sous-traitant". En effet, Il existe déjà un modèle de RaaS (Ransomware as a Service), capable de générer de façon automatique des programmes exécutables par n'importe quel utilisateur lambda, comme Petya par exemple. En bref, créer ou acheter son propre ransomware n'ayant jamais été aussi facile, ce type d'attaque n'est donc pas prêt de disparaitre et devrait nous donner encore plus de fil à retordre en 2017.

L'expansion du ransomware "Spread or Pay"

L'une des tendances émergentes consiste à obliger les victimes à répandre le ransomware si elles ne peuvent pas payer pour récupérer leurs données. Fini le temps où il fallait choisir entre verser un montant défini par les hackers ou perdre ses données ; l'utilisateur a désormais le choix : infecter d'autres personnes ou débourser des sommes d'argent importantes.

Les personnes déjà impactées ont ainsi l'espoir de récupérer leurs fichiers personnels si elles contribuent activement à la propagation du ransomware. Cette pratique peut se révéler

particulièrement lucrative dans le cas d'un utilisateur contraint par exemple d'infecter le réseau entier de son entreprise. Les hackers sont d'ailleurs davantage tentés de pirater des petites et moyennes organisations plutôt que des particuliers.

Divulgation des données personnelles via "Doxing"

Les ransomwares sont aujourd'hui monnaie courante, tout comme les suppressions de fichiers si la victime refuse de payer la rançon dans le délai imposé. Il est toutefois possible de minimiser ces risques en déployant une protection efficace contre les malwares, en filtrant correctement ses emails et en effectuant régulièrement des sauvegardes hors ligne. Cette dernière méthode permettra de restaurer les données si le système de protection n'a pu éviter l'attaque.

Mais que faire si les cybercriminels ont téléchargé une copie des précieuses données, tels que les emails privés, les photos, ou encore des ordres de paiement, et menacent de publier ces fichiers en ligne si la victime s'abstient de verser la somme ? Cette technique est appelée doxing. À ce jour, aucun ransomware reposant entièrement sur ce principe n'a encore été recensé. Cependant, au vu de l'évolution constante des stratégies et méthodes utilisées par les hackers, ce type d'extorsion pourrait devenir une réalité en 2017.

De plus en plus d'objets connectés pris en otage en 2017

Avec l'avènement de la maison connectée et la croissance accélérée des villes et lieux de travail intelligents, tous les appareils connectés comme les véhicules, les routeurs ou box Wifi, les écrans vidéo et même les thermostats, sont devenus plus vulnérables que jamais.

En 2016, de nombreux botnets - des réseaux de robots informatiques - ont été créés à partir d'appareils insoupçonnés et ancrés dans notre quotidien : caméras IP, consoles de jeu, téléviseurs, ou encore interphones pour bébé. En exploitant les identifiants de connexion par défaut de ces terminaux et d'autres failles bien connues, des personnes malintentionnées arrivent à pirater ces objets en vue de réclamer des Bitcoins, de répandre des spams ou de perpétrer des attaques par déni de service. Le nombre de botnets capables de prendre des appareils connectés en otage en 2017 augmentera proportionnellement au nombre d'appareils susceptibles d'être piratés - chaque nouveau terminal représentant une aubaine supplémentaire pour les hackers. C'est pourquoi il est indispensable de se renseigner sur les risques de sécurité inhérents à ces nouveaux objets, et de mettre les micro-logiciels ou firmware de ces derniers à jour.

Mais ce sont finalement les routeurs utilisés pour connecter cette mutlitude d'appareils à internet qui constituent les vulnérabilités les plus problématiques. La mise à jour du firmware ne suffit pas à contrer les menaces actuelles. Le routeur devra évoluer en 2017 pour devenir un terminal intelligent capable de bloquer les cybercriminels qui tentent de prendre les maisons connectées en otage. Dans un avenir très proche, plusieurs grands fournisseurs d'accès à internet proposeront des routeurs intelligents dotés d'une sécurité active ultra-performante leur permettant de faire face à l'inlassable évolution des menaces tout en offrant de nouveaux types de services à leurs clients.

Le machine learning au service des hackers

De nombreux experts désigneront à coup sûr le machine learning comme l'une des grandes

tendances de 2017. Les utilisateurs honnêtes utilisent actuellement l'intelligence artificielle (IA) pour se défendre et se protéger. Cependant, nous avons déjà pu assister aux premières batailles de cybersécurité au cours desquelles chaque adversaire utilisait une IA. Malheureusement, plusieurs facteurs inciteront les criminels à exploiter davantage cette technologie : la disponibilité d'infrastructures informatiques et de stockage à bas prix couplée aux algorithmes et aux codes d'apprentissage automatique. Espérons seulement que cette tendance sera d'actualité en 2018 ou plus tard encore !