Tendances actuelles et émergentes pour la cybersécurité en 2017

	Tendances actuelles et émergentes pour la cybersécurité en 2017

L'année 2016 a été marquée par un grand nombre de cyberattaques très diverses, allant d'attaques de type DDoS par le biais de caméra de sécurité connectées, jusqu'au supposé piratage de partis politiques durant les élections américaines. Nous avons aussi constaté une forte augmentation des fuites de données, aussi bien au niveau des petites que des grandes organisations, avec des pertes significatives de données personnelles des utilisateurs. En cette fin d'année, nous réfléchissons donc aux directions que vont prendre ces tendances en 2017.

Les tendances actuelles et émergentes :
Les attaques destructives de type DDoS utilisant les objets connectés vont augmenter.
En 2016, Mirai a montré le potentiel destructeur important que pouvaient avoir les attaques DDoS, du fait notamment du manque de sécurité des objets connectés. Les attaques de Mirai exploitaient seulement un faible nombre d'équipements et de vulnérabilités, en utilisant des techniques simples pour deviner les mots de passe. Cependant, d'autres cybercriminels n'auront aucun mal à étendre la portée de ce type d'attaque, du fait du nombre considérable d'objets connectés contenant des codes obsolètes, ainsi que des applications et systèmes d'exploitation non mis à jour contenant souvent des vulnérabilités bien connues. Il faut s'attendre à une utilisation plus systématique des exploits présents au sein des objets connectés et de techniques avancées permettant de deviner les mots de passe, pour compromettre une plus grande variété d'objets connectés, afin de mener des attaques de type DDoS ciblant d'autres équipements connectés à votre réseau.

Les attaques ciblées d'ingénierie sociale seront plus sophistiquées.
Les cybercriminels sont de plus en plus expérimentés pour exploiter la première des vulnérabilités : l'être humain. Des attaques ciblées de plus en plus sophistiquées et convaincantes cherchent à duper et à amadouer les utilisateurs, afin de les pousser à se mettre en danger eux-mêmes. Par exemple, il est courant de voir des emails s'adressant à leurs destinataires par leurs noms et qui prétendent que ces derniers ont une dette impayée, que l'expéditeur en question serait autorisé à collecter. La peur, l'intimidation et les menaces de recouvrement au nom de la loi, sont des tactiques très utilisées et assez classiques. L'email en question vous redirige alors vers un lien malveillant, sur lequel les utilisateurs cliquent dans la panique, amorçant alors l'attaque. De telles attaques par hameçonnage (phishing), ne peuvent plus être détectées à la lecture par de simples erreurs grossières commises par les cybercriminels.

Les infrastructures financières deviendront des cibles privilégiées.
Les attaques ciblées de phishing, et particulièrement celles ciblant les dirigeants (whaling), vont continuer de croitre. Ces attaques utilisent des informations détaillées concernant les dirigeants d'entreprises, afin de duper les employés et les inciter à envoyer de l'argent à des cybercriminels, ou à compromettre certains comptes bancaires. Nous nous attendons aussi à voir davantage d'attaques ciblant des infrastructures financière sensibles, telles que l'attaque ayant pris pour cible les institutions connectées au système SWIFT, qui a coûté à la banque centrale du Bangladesh 81 millions $, en février dernier. SWIFT a récemment admis que d'autres attaques de ce type avaient eu lieu, et qu'il s'attendait à en voir davantage en déclarant, dans une lettre adressée aux clients de la banque : « La menace est très persistante, adaptative et sophistiquée. Il faut s'attendre à ce qu'elle continue de sévir. ».

L'exploitation de l'infrastructure intrinsèquement non sécurisée d'Internet va se poursuivre.
Tous les internautes font encore confiance à de vieux protocoles fondateurs, que leur omniprésence empêche de réorganiser ou de remplacer. Ces protocoles archaïques qui ont pendant longtemps été les piliers de l'Internet et des réseaux professionnels sont aujourd'hui fragilisés, parfois d'une manière surprenante. Par exemple, les attaques contre BGP (Border Gateway Protocol) auraient pu, en théorie, perturber ou même mettre hors service une bonne partie du Web. Les attaques DDoS visant Dyn en octobre dernier (lancées depuis une multitude d'objets connectés) ont mis hors service un fournisseur majeur de services DNS, et ont de ce fait rendu inaccessible une partie de l'Internet. Il s'agissait de l'un des plus importants assauts jamais observés, et ceux à l'origine de ces attaques ont déclaré qu'il s'agissait seulement d'un coup d'essai. Les fournisseurs d'accès Internet et les entreprises peuvent bien évidemment prendre des mesures pour se protéger, mais pourraient trouver difficile d'éviter tous les dégâts importants potentiellement causés par des individus ou des états qui auront choisi d'exploiter les failles de sécurité les plus profondes du Web.

La sophistication des attaques va augmenter.
Le nombre d'attaques continue à augmenter, avec une sophistication croissante des techniques et de l'ingénierie sociale, qui reflète une analyse minutieuse et répétée des organisations et des réseaux de leurs victimes. Les cybercriminels peuvent compromettre de nombreux serveurs et stations de travail bien avant de commencer à voler des données ou agir de façon plus agressive. Ces attaques, en général pilotées par des experts, sont plus stratégiques que tactiques, et peuvent au final causer des dommages considérables. Il s'agit ici d'un monde très différent des attaques par malwares programmés et automatisés dont nous avons l'habitude. C'est un monde où la stratégie et la patience jouent un rôle beaucoup plus important pour échapper aux détections.

De plus nombreuses attaques utiliseront des outils d'administration intégrés.
Nous voyons davantage d'exploits basés sur PowerShell, le langage et kit de développement de Microsoft pour l'automatisation des tâches administratives. En tant que langage de script, PowerShell contourne les détections visant les exécutables. Nous voyons également plus d'attaques utilisant des tests de pénétration et d'autres outils d'administration existants, sans qu'ils soient à priori infiltrés et en général suspectés. Ces outils puissants demandent une vigilance toute particulière et des contrôle plus robustes.

Les ransomwares vont continuer à progresser.
Comme de plus en plus d'utilisateurs sont conscients de l'existence du risque d'attaques par ransomware via les emails, les cybercriminels exploitent d'autres vecteurs. Certains expérimentent des malwares qui infectent à nouveau le système ultérieurement, longtemps après que la rançon ait été payée. D'autres commencent à utiliser des outils intégrés, à la place de malwares exécutables, afin d'éviter d'être détectés par les solutions de protection Endpoint qui se focalisent sur des fichiers exécutables. De récents exemples ont proposé de déchiffrer les fichiers de leurs victimes si elles acceptaient de diffuser le ransomware vers deux autre contacts, et que ces personnes acceptent de payer. Les ransomwares commencent également à utiliser des techniques autres que le chiffrement, par exemple en détruisant ou corrompant les en-têtes de fichiers. Qui plus est, avec le grand nombre de ransomwares qui persistent sur le Web, les utilisateurs peuvent se retrouver victimes d'attaques sans espoir de pouvoir payer en dernier recours, car le système de paiement ne fonctionne plus.

Des attaques visant des objets personnels connectés vont émerger.
Les utilisateurs d'objets connectés domestiques s'imaginent rarement que leur veilleuse écoute-bébé puisse être piratée pour attaquer des sites internet. Cependant, dès qu'un pirate contrôle un équipement connecté à un réseau domestique, il peut plus facilement pirater d'autres équipements de ce réseau, tels que des ordinateurs portables contenant des données personnelles sensibles. Nous nous attendons à voir plus d'attaques de ce genre, ainsi que des attaques impliquant des caméras vidéo ou des microphones afin d'espionner les foyers. Les cybercriminels trouvent toujours un moyen de tirer profit de leurs attaques.

Le malvertising et la corruption des écosystèmes de publicités en ligne vont s'étendre.
Le malvertising, qui fonctionne en répandant des malwares sur les réseaux publicitaires et les pages web, existe déjà depuis plusieurs années. Cependant, nous avons pu observer en 2016 une recrudescence de ce phénomène. Ces attaques mettent en évidence des problèmes plus importants au sein de l'écosystème des publicités en ligne, telle que la fraude au clic, qui génère des clics payants et ne correspondent pas en réalité aux véritables centres d'intérêts de l'internaute. Le malvertising a engendré la fraude au clic, mettant les utilisateurs en danger et abusant les annonceurs par la même occasion.

La diffusion du chiffrement entrainera des problèmes collatéraux.
Le chiffrement se diffuse très largement et il est devenu plus difficile pour les solutions de sécurité d'inspecter le trafic, facilitant ainsi la vie des cybercriminels qui cherchent à s'infiltrer sans être repérés. Sans surprise, les cybercriminels utilisent le chiffrement de manière créative. Les produits de sécurité vont devoir rapidement intégrer les protections réseaux et client afin de pouvoir détecter des évènements pouvant affecter la sécurité après que le code ait été déchiffré au niveau des systèmes Endpoint.

Les cybercriminels s'intéresseront aux exploits des systèmes virtualisés dans le Cloud.
Les attaques contre des composants physiques (exemple de Rowhammer) ouvrent la voie à de nouveaux exploits potentiellement dangereux contre des systèmes cloud virtualisés. Les cybercriminels peuvent abuser d'un hôte ou bien d'un invité sur un système hôte partagé, attaquer la gestion des privilèges et potentiellement accéder aux données de tiers. De plus, comme Docker et les écosystèmes de conteneurs logiciels (« serverless ») deviennent de plus en plus populaires, les cybercriminels vont certainement se mettre à chercher des failles à exploiter dans le cadre de cette nouvelle tendance des systèmes d'information. Nous nous attendons donc à voir des tentatives actives pour rendre de telles attaques opérationnelles.
Des attaques techniques visant les Etats et les populations apparaîtront. Les attaques technologiques sont devenues hautement politiques. Les populations doivent faire face à des risques grandissants en matière de désinformation (« les fausses nouvelles ») et concernant les systèmes de vote. Par exemple, les experts ont démontré l'existence d'attaques permettant à un électeur, au niveau local, de voter de manière répétitive sans aucune détection. Même si les Etats n'organisent jamais d'attaques contre leurs adversaires aux élections, le sentiment que ce type d'attaques puisse exister est en soi une arme puissante…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Original de l'article mis en page : Sophos : tendances actuelles et émergentes pour la cybersécurité en 2017 — Global Security Mag Online