T R I B U N E L I B R E

Les sept nouvelles techniques d'attaque les plus dangereuses

Par Johannes Ullrich, Directeur du SANS Internet Storm Center, Docteur et Directeur de Recherche, SANS Technology Institute

Paris, le 30 mars - Si le paysage des menaces informatiques évolue sans cesse, certaines menaces méritent qu'on leur accorde davantage d'attention de par leur nuisance.

Des ransomware lucratifs

Le chiffrement est un facteur de protection des activités commerciales, des communications et de la vie privée. Toutefois, allié aux crypto-monnaies utilisées pour le paiement des rançons, les ransomware (ou rançongiciels) sont le parfait exemple de l'exploitation du chiffrement à des fins cybercriminelles. Les ransomware constituent une technique d'attaque très efficace pour les pirates informatiques. Avec eux, ils n'ont pas besoin de recourir à un canal de commande et de contrôle, d'exfiltrer des données, ni d'établir de contact. Ce sont les victimes elles-mêmes qui appellent au secours le pirate pour remédier à l'attaque. On constate aujourd'hui une nette augmentation du nombre d'attaques par rançongiciel et de leur impact économique non seulement auprès des particuliers, mais aussi sur les entreprises. Les rançongiciels ciblent de plus en plus les serveurs de fichiers réseau, les sauvegardes et les grandes bases de données, ce qui accroît considérablement leurs effets.

De nouvelles attaques ciblant l'Internet des objets

Il y a quelques années, les appareils intelligents qui forment l'Internet des objets (IoT), comme les ampoules électriques, les thermostats, les webcams et bien d'autres encore, étaient considérés comme des cibles potentielles permettant aux attaquants d'activer ou de désactiver des groupes de périphériques pour porter préjudice aux consommateurs. Aujourd'hui, l'IoT ne représente plus une simple cible, mais une véritable plate-forme d'attaque. Avec des vers Open Source de grande portée, tels que Mirai, capables de se propager à des dizaines de millions d'appareils IoT, les attaquants peuvent exploiter ces systèmes pour générer un afflux massif de trafic et déconnecter d'Internet pratiquement n'importe quelle entreprise. Au-delà de l'attaque massive du réseau, ces plateformes d'attaque IoT peuvent présenter d'autres formes de menaces, comme le vol furtif d'information et le déchiffrement des mots de passe.

Quand les rançongiciels rencontrent l'IoT

Les organisations cybercriminelles tirent de gros profits des rançongiciels et réinvestissent une partie de leurs gains pour accroître l'efficacité, la portée et l'impact de leurs attaques. En combinant rançongiciels et IoT, les cybercriminels disposeront d'un moyen d'action

beaucoup plus dévastateur que les attaques par déni de service. Le chiffrement des configurations et des infrastructures de contrôle permettra aux attaquants de prendre en otage des thermostats, des infrastructures d'éclairage ou même des automobiles contre le versement d'une rançon. Pour pouvoir démarrer votre voiture ou allumer la lumière, il vous faudra payer la somme demandée, ou bien reconfigurer et réinstaller tous les micrologiciels de vos appareils, une procédure pour le moins complexe. L'Internet industriel des objets (IIoT) coure un danger encore plus grand : les rançongiciels pourront paralyser la capacité de production d'une usine ou l'activité d'une entreprise de service public.

Les attaques ciblées à l'encontre de systèmes de contrôle industriel

Les attaques visant les systèmes de contrôle industriel ont pris une tournure inquiétante. Les cybercriminels s'attaquent au cœur opérationnel d'infrastructures vitales (Opérateurs d'Importance Vitale - OIV) en profitant de leur vulnérabilité. Des attaques récentes ont non seulement perturbé la fourniture de services essentiels, tels que l'électricité, mais ont aussi endommagé les systèmes d'automatisation permettant le retour à la normale et le bon fonctionnement des opérations. Les attaques de 2015 et 2016 à l'origine de pannes de courant en Ukraine ont été parfaitement planifiées et coordonnées (lors de conditions climatiques d'une extrême rigueur). Les attaquants ont réussi à détourner les systèmes d'automatisation pour provoquer des pannes d'électricité, puis exécuter une succession bien ordonnée de charges utiles destructrices sur des stations de travail, des serveurs et des appareils intégrés.

A l'avenir, il sera plus difficile de se remettre des pannes causées par des attaques, et les interruptions risquent de se mesurer en jours et non plus en heures. Des événements de ce type obligent les fournisseurs en charge de ces infrastructures à réfléchir à la façon d'agir en cas d'attaque, et à faire un choix important entre utiliser leurs systèmes intelligents ou les mettre hors service.

Faiblesse des générateurs de nombres aléatoires

La création efficace de nombres aléatoires est un problème épineux. Avec les petits appareils, il est difficile de collecter une quantité suffisante d'événements aléatoires pour initialiser les algorithmes servant à la génération de nombres aléatoires. Des études récentes ont montré que cette faiblesse pouvait être exploitée pour casser le chiffrement WPA2. Mais le problème dépasse largement le cadre du Wi-Fi et du mécanisme WPA2. Le chiffrement sans vrais nombres aléatoires met en péril un large éventail d'algorithmes de sécurité.
La plupart des protocoles sans fil, et pas seulement le Wi-Fi, ont besoin de vrais nombres aléatoires pour chiffrer les connexions. Sans cela, elles ne sont pas sécurisées.

Des services Web utilisés en tant que composants logiciels

Les développeurs ne sont plus contraints de faire appel à des composants, tels que des librairies, qui doivent être téléchargées et installées pour appliquer des correctifs réguliers. De nouvelles technologies, comme les conteneurs et le Cloud computing, permettent la mise en œuvre de services qui n'existent que lorsqu'ils sont utilisés. L'exploitation de services à distance fait courir de nouveaux risques aux logiciels. Les services doivent être soigneusement authentifiés, et les données reçues validées. Les services ad hoc sont difficiles à inventorier et les analyses de sécurité doivent tenir compte du fait que ces services ne seront exécutés qu'en cas de besoin.

Un grand nombre de développeurs de logiciels utilisent des services réseau à distance au lieu de librairies pour les fonctions critiques. Les applications mobiles, en particulier, sont largement tributaires des services réseau. Sans une validation appropriée, des tests et une surveillance de ces services, les applications courent de grands risques.

Menaces contre les bases de données NoSQL
Les développeurs soucieux de la sécurité connaissent et combattent depuis longtemps les menaces qui pèsent sur les bases de données SQL traditionnelles. Jusqu'à présent, ils s'appuyaient sur des instructions préparées et sur une configuration appropriée des comptes utilisateurs. Le problème est que certaines de ces options n'existent pas pour les nouvelles bases de données NoSQL, comme MongoDB ou Elastic Search, mais aussi que de nouveaux types de menaces ont fait leur apparition. Des formats de données complexes, tels que JSON et XML, présentent de nouveaux risques et, en général, les développeurs et les administrateurs système ne savent pas encore comment protéger ces bases de données et leur transmettre des données de manière sécurisée.

Plusieurs milliers de bases de données NoSQL ont déjà été compromises ou supprimées. Une instance vulnérable de base de données NoSQL est découverte dans les heures qui suivent sont exposition sur Internet.

L'évolution des technologies, des techniques d'attaques et des manières de travailler et de collaborer avec les outils informatiques nécessite que les professionnels de l'informatique et de la cybersécurité s'informent et perfectionnent constamment leurs connaissances. De cette manière, ils pourront se maintenir au meilleur niveau et pourront appréhender efficacement les nouvelles menaces. Les professionnels de la sécurité peuvent également s'appuyer sur des solutions matérielles et logicielles, des SOC (centre de supervision de la sécurité) internes ou externes ou des outils tels que l'Internet Storm Center qui fournit un service d'analyse et d'alerte sur les menaces de sécurité avec l'aide de censeurs localisés dans plus de 50 pays. Ce qui est intéressant, c'est que le centre s'appuie sur la connaissance des spécialistes en sécurité à travers le monde et tous sont des bénévoles qui détectent les menaces, les examinent et fournissent des rapports d'analyse au public.

Pour suivre les actualités du SANS Institute :

- Evènement de formations SANS Paris : Juin 26 – Juillet 3, 2017
- www.sans.org/fr
- Ressources (webcasts, newsletters, white papers, etc.) : https://www.sans.org/security-resources
- Twitter : @SANSEMEA

À propos de SANS Institute (@SANSInstitute)
Créé en 1989, SANS est la référence mondiale en matière de formation, recherche et certification dans le domaine de la cybersécurité. Les formateurs mondialement reconnus de SANS ont déjà formés plus de 140 000 professionnels, issus du secteur public et privé et enseignent chaque année plus de 60 cours qui s'alignent sur les rôles, responsabilités et disciplines majeur des équipes de sécurité. SANS Institute propose des cours qui sont alignés sur les 30 certifications techniques GIAC dans le domaine de la sécurité de l'information. GIAC (Global Information Assurance Certification)

valide ainsi les compétences des professionnels de la sécurité de l'information, attestant que ceux qui sont certifiés ont les connaissances techniques nécessaires pour travailler dans des domaines clés de la cybersécurité.

SANS Institute développe et publie de nombreuses ressources mis à disposition gratuitement, y compris des bulletins d'information, des livres blancs et des webcasts (www.sans.org).

Contacts presse

Laëtitia Berché
Cymbioz
+33 1 42 97 93 30 / + 33 6 14 48 02 95
laetitia.berche@cymbioz.com
www.cymbioz.com