Rapport Cisco du 1er semestre 2017 sur la cybersécurité

Synthèse

Cisco publie des rapports complets sur la cybersécurité depuis près de dix ans. L'objectif de ces rapports est d'informer les équipes de sécurité et les entreprises des nouvelles cybermenaces et vulnérabilités, ainsi que des mesures à prendre pour améliorer la sécurité et la cyber-résilience. Nous essayons d'alerter les acteurs de la protection de la sophistication croissante des menaces et des techniques utilisées par les hackers pour usurper l'identité des utilisateurs, voler des informations et créer des perturbations.

Dans ce nouveau rapport, nous relevons encore le niveau d'alerte. Nos experts s'inquiètent de plus en plus de l'accélération des changements et de la sophistication des cybermenaces mondiales. Les acteurs de la protection améliorent leurs méthodes de détection et de défense et aident les entreprises à se protéger et à réparer les conséquences d'une attaque. Cependant, deux tendances mettent à mal ces résultats obtenus si difficilement, ralentissant leurs progrès et précipitant leur entrée dans une nouvelle ère de cybercriminalité :

L'impact croissant des failles de sécurité

La génération de revenus reste le principal objectif de la majorité des cybercriminels. Les hackers ont désormais la capacité et la volonté de bloquer les systèmes et de détruire les données par leurs attaques. Nos chercheurs considèrent que ces activités plus malveillantes annoncent une nouvelle forme d'attaque dévastatrice qui devrait émerger dans un avenir proche : la destruction de services (DeOS).

Au cours de l'année écoulée, nous avons également constaté que certains hackers utilisaient des objets IoT dans leurs attaques par déni de service (DDOS). L'activité des botnets dans les environnements IoT suggère que certains opérateurs sont en train de préparer le terrain pour une attaque de grande envergure aux retombées majeures pouvant même compromettre Internet.

Le rythme et l'ampleur des technologies

Nos chercheurs spécialistes des menaces étudient depuis des années la manière dont la mobilité, le cloud computing et les autres évolutions et tendances technologiques modifient l'ampleur du périmètre de sécurité devant être défendu par les entreprises. Or, il apparaît clairement aujourd'hui que les cybercriminels tirent parti de cette surface d'exposition aux attaques toujours plus grande. L'ampleur des dernières attaques par ransomware témoigne à elle seule de l'inclination des hackers à exploiter les vulnérabilités et les failles des appareils et des réseaux pour avoir un maximum d'impact.

Le manque de visibilité sur les environnements informatiques dynamiques, les risques présentés par le « Shadow IT », le déferlement constant des alertes de sécurité et la complexité de l'environnement de sécurité informatique sont quelques-unes des raisons pour lesquelles les équipes de sécurité à court de ressources peinent à garder une longueur d'avance sur les cybermenaces actuelles, toujours plus furtives et puissantes.

Contenu de ce rapport

Le *rapport Cisco du 1er semestre 2017 sur la cybersécurité* explore les dynamiques précédemment évoquées en abordant les points suivants :

Tactiques des hackers

Nous examinons certaines des méthodes employées par les hackers pour compromettre les données des utilisateurs et infiltrer leurs systèmes. Il est essentiel que les acteurs de la protection comprennent les changements de tactique des hackers pour pouvoir adapter leurs pratiques de sécurité et former les utilisateurs. Ce rapport couvre les nouveautés en matière de malwares, les tendances en matière d'attaques web et de spams, les risques liés aux applications potentiellement indésirables (PUA) comme les spywares, les attaques de messageries d'entreprise (BEC), l'évolution des modèles économiques des hackers et les menaces visant les systèmes médicaux. Nos chercheurs spécialistes des menaces présentent également leur analyse de l'évolution rapide des outils et des techniques de certains hackers, et fournissent des informations actuelles sur les efforts déployés par Cisco pour réduire le temps de détection des menaces.

Vulnérabilités

Dans ce rapport, nous donnons également un aperçu des vulnérabilités et autres expositions qui accroissent le risque de compromission ou d'attaque des utilisateurs et des entreprises. Nous évoquons aussi les pratiques de sécurité insuffisantes, comme l'application trop tardive des correctifs de vulnérabilités connues, la non-limitation des accès privilégiés aux systèmes cloud et l'absence de gestion de l'infrastructure et des terminaux. Autre aspect important : les raisons pour lesquelles le développement de l'IoT et la convergence des départements IT et OT (technologies opérationnelles) accroissent les risques encourus par les entreprises, leurs utilisateurs et leurs clients, et les mesures à prendre dès maintenant pour limiter ces risques avant qu'il soit trop tard.

Opportunités pour les acteurs de la protection

Le *rapport Cisco du 1er semestre 2017 sur la cybersécurité* présente d'autres conclusions de l'enquête Cisco sur l'efficacité des mesures de sécurité. Nous proposons une analyse approfondie des principaux problèmes de sécurité dans huit secteurs : opérateurs télécoms, secteur public, commerce, production industrielle, distribution d'énergie, santé, transports et services financiers. Les experts de Cisco fournissent des recommandations pour aider ces entreprises à améliorer leur solution de sécurité, notamment en utilisant des services qui comblent les manques de compétences et de connaissances, en réduisant la complexité de leur environnement informatique et en adoptant l'automatisation.

La conclusion du rapport invite les responsables de la sécurité à discuter dès que possible des risques et des budgets relatifs à la cybersécurité avec leurs dirigeants et leurs conseils d'administration, et fournit des recommandations pour commencer cette conversation.

Principales conclusions

- Les attaques de messagerie d'entreprise (BEC) sont devenues un vecteur de menace très lucratif pour les hackers. Selon l'Internet Crime Complaint Center (IC3), les fraudes BEC ont permis le vol de 5,3 milliards de dollars entre octobre 2013 et décembre 2016. En comparaison, les exploits de type ransomware ont permis le vol d'un milliard de dollars en 2016.
- Un logiciel espion de type PUA (attaque par applications potentiellement indésirables) est une forme de malware. Or, ce risque est sous-estimé, voire complètement ignoré, par beaucoup d'entreprises. Pourtant, un logiciel espion peut voler les données des utilisateurs et de l'entreprise, affaiblir le dispositif de sécurité des appareils et accroître les infections par malware. Par ailleurs, les infections par logiciel espion se propagent. Les chercheurs Cisco spécialistes des menaces ont étudié trois familles de logiciels espions et découvert qu'ils étaient présents dans 20 % des 300 entreprises de l'échantillon.
- L'Internet des objets (IoT) est porteur de promesses pour la collaboration et l'innovation dans l'entreprise. Mais à mesure qu'il se développe, le risque pour la sécurité augmente. Le manque de visibilité est un problème : les acteurs de la protection n'ont tout simplement pas connaissance des appareils connectés à l'IoT dans leur réseau. Ils doivent agir vite pour surmonter ce problème, ainsi que les autres freins à la sécurité IoT. Les cybercriminels exploitent déjà les failles de sécurité des appareils connectés à l'IoT. Les appareils servent de bastions aux hackers. Ils leur permettent de s'infiltrer discrètement et relativement facilement dans les réseaux.
- Cisco analyse son temps de détection moyen depuis novembre 2015. Depuis cette date, la tendance globale est à la baisse. Nous sommes passés d'un peu plus de 39 heures au début de notre étude à environ 3,5 heures pour la période de novembre 2016 à mai 2017.

5,3 milliards de dollars US

ont été volés lors d'attaques de type BEC entre octobre 2013 et décembre 2016.

- Cisco a observé une croissance globale du volume de spams depuis le 2e semestre 2016, ce qui semble coïncider avec une baisse sensible de l'activité des kits d'exploit pendant la même période. Les hackers qui utilisaient principalement des kits d'exploit pour diffuser des ransomwares optent désormais pour des spams, qui contiennent notamment des documents malveillants exécutant des macros capables de contourner la plupart des technologies de sandboxing car l'interaction de l'utilisateur est requise pour infecter les systèmes et propager les charges utiles.
- Les attaques de chaîne d'approvisionnement sont un moyen pour les hackers de propager un malware vers de nombreuses entreprises par le biais d'un seul site compromis. Dans le cas d'une attaque étudiée par RSA, un partenaire de Cisco, la page web de téléchargement d'un éditeur de logiciels a été compromise, permettant à l'infection de se propager vers toutes les entreprises ayant téléchargé le logiciel de cet éditeur.
- Selon Radware, un partenaire de Cisco, l'augmentation spectaculaire de la fréquence, de la complexité et de l'ampleur des cyberattaques au cours de l'année écoulée suggère que le modèle économique du piratage a passé un cap. Radware observe que la communauté des hackers bénéficie aujourd'hui d'un accès immédiat aisé à une gamme étendue de ressources aussi peu coûteuses qu'efficaces.

La génération de revenus reste le principal objectif de la majorité des cybercriminels. Toutefois, certains hackers ont désormais la capacité de verrouiller des systèmes et de détruire des données dans le cadre de leur processus d'attaque.

- En matière de sécurité d'entreprise, le cloud n'est pas suffisamment pris en compte. Pourtant, le risque lié à OAuth (Open authorization) et la gestion insuffisante des comptes d'utilisateur privilégiés créent des failles facilement exploitables par les hackers. Selon les chercheurs Cisco spécialistes des menaces, le cloud intéresse désormais les hackers qui cherchent par tous les moyens à entrer dans les environnements cloud d'entreprise.
- L'activité des kits d'exploit a considérablement diminué, et l'innovation dans ce domaine a stagné, depuis qu'Angler et d'autres kits d'exploit ont disparu ou changé de modèle économique. Mais les tendances passées sur ce marché indiquent que cette situation est probablement temporaire. Toutefois, d'autres facteurs comme la difficulté à exploiter les vulnérabilités des fichiers créés avec la technologie Adobe Flash pourraient ralentir cette résurgence.
- Selon une étude menée par Rapid7, un partenaire de Cisco, les services DevOps déployés de façon incorrecte ou intentionnellement laissés ouverts pour faciliter l'accès des utilisateurs légitimes représentent un risque non négligeable pour les entreprises. En fait, beaucoup de ces instances ont déjà été rançonnées.
- L'analyse par ThreatConnect des domaines colocalisés utilisés par les hackers du groupe de cyberespionnage Fancy Bear a démontré l'intérêt d'étudier l'infrastructure IP de ces cybercriminels. En étudiant cette infrastructure, les acteurs de la protection peuvent établir une liste plus complète des domaines, adresses IP et adresses e-mail qui doivent être bloqués de façon proactive.
- À la fin de l'année 2016, les chercheurs Cisco spécialistes des menaces ont découvert et signalé trois vulnérabilités de type exécution de code à distance sur des serveurs Memcached. Quelques mois plus tard, une analyse d'Internet a révélé que 79 % des quelque 110 000 serveurs Memcached exposés précédemment identifiés étaient toujours sensibles aux trois vulnérabiltés, car ils n'avaient pas été corrigés.

Téléchargez le rapport Cisco complet du 1er semestre 2017 sur la cybersécurité à l'adresse www.cisco.fr/mcr2017.

Siège social aux États-Unis
Cisco Systems, Inc.
San José. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : www.cisco.com/go/offices.