Accenture Security

Communiqué de presse

Accenture identifie 5 menaces en matière de cybersécurité dans le monde

Paris, le 28 novembre 2018. Les entreprises devraient connaitre un nombre accru de cyberattaques pouvant causer des dommages matériels importants dans les mois à venir. Un nouveau rapport d'Accenture prédit notamment une escalade des cyber menaces perpétrées depuis l'Iran, une augmentation des attaques contre les chaînes d'approvisionnement mondiales, un ciblage accru des infrastructures critiques ainsi que l'émergence de nouvelles sources de cybercriminalité à motivation financière.

Le rapport fait le point sur les tendances observées au cours du premier semestre 2018 en matière de cybermenaces et modélise la manière dont les cyberincidents pourraient évoluer d'ici la fin de l'année. Il est basé sur la collecte et l'analyse de données tirées des opérations de renseignement menées par la division iDefense d'Accenture Security, y compris la recherche basée sur des éléments open-source primaires et secondaires. Le rapport révèle un nombre croissant d'attaques destructrices, l'utilisation agressive d'information par les Etats-nations, l'augmentation du nombre et de la diversité des acteurs ainsi qu'un accès plus large aux systèmes d'exploitations, outils, cryptage et systèmes de paiement anonymes par des personnes malveillantes.

« Cela fait 20 ans que nos équipes de renseignement surveillent de près les cyberescrocs et analysent les moyens toujours plus ingénieux qu'ils pourraient utiliser pour infiltrer les réseaux », a déclaré Eric Boulay, directeur d'Accenture Security en France et au Benelux. « Les entreprises doivent analyser ces menaces, leurs cibles et s'adapter en permanence aux stratégies d'attaques mouvantes et sophistiquées. Deux recommandations : protéger et surveiller tout son écosystème incluant les données circulant chez ses partenaires et sous-traitants, s'entrainer et planifier pour améliorer sa résilience. »

Le rapport identifie 5 menaces principales :

• Menace n°1: la cybermenace iranienne est bien réelle

Bien que l'Iran soit généralement perçu comme une cyberpuissance émergente, de nouveaux éléments tendent à démontrer que les cybercriminels basés en Iran ne cessent de développer leurs activités malveillantes. Les analystes du renseignement d'Accenture ont constaté que le groupe de cyberespionnage PIPEFISH continue d'être très actif et d'optimiser ses moyens d'action. Ce groupe de menaces visait principalement des organisations basées au Moyen-Orient dans le secteur de l'énergie, dans des pays tels que l'Arabie saoudite, le Qatar ou les Emirats arabes unis, à des fins de surveillance et d'espionnage. Les logiciels malveillants récemment découverts chez PIPEFISH peuvent lancer des commandes à distance et télécharger des fichiers à partir du système de la victime. En outre, une analyse a identifié l'émergence de logiciels de rançon basés en Iran, indiquant que les acteurs iraniens de la cybercriminalité sont susceptibles de cibler des organisations mondiales en utilisant des logiciels de rançon ainsi que des crypto-mineurs à des fins financières.

• Menace n°2: les Etats-nations cherchent à exploiter les environnements tiers

Les groupes cybercriminels, d'espionnage et d'hacktivistes continueront de cibler les chaînes d'approvisionnement et les partenaires commerciaux stratégiques qui y contribuent, en profitant du fait que seules 39% des entreprises intègrent la protection des données échangées avec leurs sous-traitants dans leur stratégie de défense. Par exemple, les analystes du renseignement d'Accenture estiment qu'un groupe de hackers basé en Chine, appelé PIGFISH, cible des organisations de nombreux secteurs dans le cadre de diverses missions d'espionnage, accumulant dans le même temps de nombreuses

ressources et capacités d'attaque de la chaîne logistique. Plus les cybercriminels utiliseront des tiers de confiance comme vecteurs d'intrusion, plus il sera difficile de remonter jusqu'aux sources de la menace.

• **Menace n°3: les infrastructures critiques constituent une cible de choix**

L'industrie pétrolière et gazière ainsi que l'industrie manufacturière continueront d'être une cible de choix pour les acteurs de la menace jusqu'à la fin de l'année 2018. Au niveau international, les acteurs étatiques russes pourraient parrainer des cyberopérations, liées à l'espionnage ou soutenir des hacktivistes au nom de la protection de l'environnement avec pour objectif de fausser la concurrence sur le marché de l'énergie. La hausse du prix du pétrole est un autre facteur clé, qui pourrait inciter les acteurs de la menace nord-coréens à lancer des attaques par ransomware et d'autres cybermenaces à motivation financière, telles que le crypto hacking, afin de contourner les sanctions et de collecter des fonds.

• **Menace n°4: transformation des logiciels malveillants de cryptominage**

L'utilisation de logiciels malveillants destinés aux cryptomineurs est l'une des tendances majeures en matière de cybercriminalité cette année, et sa croissance devrait se poursuivre en 2019, le bénéfice venant de la fluctuation rapide du cours des cryptomonnaies. L'observation récente d'activités criminelles souterraines a révélé une pléthore de publicités publiées par des auteurs et revendeurs de logiciels malveillants pour mineurs Monero. L'offre de programmes malveillants est très variée ; cela va des programmes d'entrée de gamme génériques et peu coûteux aux vastes réseaux périphériques de botnets personnalisés.

• **Menace n°5: les opérations avancées de menace persistante (APT en anglais) sont de plus en plus motivées par l'argent**

Alors que de nombreuses cyberattaques de type APT sont menées à des fins d'espionnage, les cybercriminels motivés par des raisons financières intensifient leurs activités depuis 2013. Ces cyberattaques de longue durée, en plusieurs étapes, sont de plus en plus souvent menées par des cybercriminels qui utilisent des outils, techniques et procédures habituellement réservées au cyberespionnage, ainsi que des technologies de pointe pour obtenir des avantages financiers. Le niveau d'activités de groupes générant des attaques ciblées à motivation financière, tels que Cobalt Group et FIN7, restera significatif, mais son volume sera inférieur en 2018 à celui de 2017.

A propos d'Accenture
Accenture, un des leaders mondiaux des services aux entreprises et administrations, propose une large gamme de services et solutions en stratégie, conseil, digital, technologie et gestion déléguée d'opérations. Combinant son expérience et son expertise dans plus de 40 secteurs d'activité et pour toutes les fonctions de l'entreprise - en s'appuyant sur le plus grand réseau international de centres de services - Accenture intervient à l'intersection de l'activité de ses clients et de la technologie pour les aider à renforcer leur performance et créer de la valeur sur le long terme pour leurs parties prenantes. Avec 449 000 employés intervenant dans plus de 120 pays, Accenture favorise l'innovation pour améliorer notre environnement de demain. Site Internet : www.accenture.com/fr.

Accenture Security aide les entreprises à devenir résilientes, pour qu'elles puissent se concentrer avec confiance sur l'innovation et la croissance. Grâce à son réseau global de laboratoires de cybersécurité et à son expertise approfondie de l'ensemble du cycle de vie de la sécurité dans les différents secteurs d'activité, Accenture offre aux entreprises une protection intégrale de leurs actifs sensibles. À travers des services tels que la stratégie et la gestion des risques, la cyberdéfense, l'identité numérique, la sécurité applicative et la sécurité managée, Accenture permet aux entreprises du monde entier de se protéger des menaces connues et inconnues. Suivez-nous sur Twitter @AccentureSecure ou consultez notre site www.accenture.com/security

Contact Presse :

Clémence Caradec
+ 33 1 53 23 55 23
Clemence.caradec@accenture.com

Giulia Goodwin
+33 1 56 03 13 83
Giulia.goodwin@bm.com