Le nouveau rapport de sécurité de Fortinet révèle que les objets connectés résidentiels constituent une nouvelle cible pour le cryptojacking

96% des entreprises ont subi au moins un incident de sécurité majeur

« Les cybercriminels sont tenaces. Ils automatisent leurs processus et outils pour créer des variantes de leurs exploits connus. Ils gagnent en précision, ciblent davantage leurs attaques et laissent moins de place au hasard pour identifier leurs victimes. L'urgence, du côté des entreprises, est de repenser les stratégies de sécurité pour contrer les nouvelles tactiques des cybercriminels. Il s'agit de déployer des fonctions de défense automatisées et intégrées pour traiter les problématiques avec rapidité et à grande échelle, opter pour une détection comportementale, mais aussi tirer parti d'une veille sur les menaces et de l'intelligence artificielle pour corriger les vulnérabilités les plus critiques. »

Phil Quade, chief information security officer, Fortinet

L'essentiel :
Fortinet® (NASDAQ: FTNT), leader mondial des solutions de cybersécurité automatisées, intégrales et intégrées, annonce la publication de son tout dernier rapport trimestriel de sécurité Global Threat Landscape Report. L'étude révèle que les cybercriminels tirent parti des vulnérabilités de manière pertinente et rapide. Ils ciblent également plus précisément leurs attaques, étendent le périmètre de leurs exactions et adoptent des approches itératives de développement logiciel pour faire évoluer leurs méthodes d'attaque. Pour les résultats détaillés de cette étude et une synthèse décisionnelle à l'intention des DSI et RSSI, rendez-vous sur le blog. Voici néanmoins les principaux enseignements de ce nouveau rapport :

- ***Quasiment aucune entreprise n'échappe à un exploit majeur :*** l'analyse des événements critiques souligne une tendance inquiétante : 96% des entreprises ont subi au moins un incident majeur de sécurité. En clair, les entreprises, dans leur quasi-totalité, cèdent au moins une fois aux attaques des cybercriminels. De plus, près d'un quart des entreprises ont été confrontées à un malware de cryptojacking, tandis que six variantes de malwares ont, à elles seules, impacté plus de 10 % de toutes les organisations. FortiGuard Labs a également identifié 30 nouvelles vulnérabilités zero-day sur ce trimestre.

- ***Le cryptojacking s'en prend aux objets connectés résidentiels :*** pour renforcer le minage des crypto-monnaies, les objets connectés résidentiels – et notamment les dispositifs multimédias – sont désormais ciblés. Ces dispositifs présentent un attrait certain compte tenu de leurs ressources informatiques importantes pouvant être détournées à des fins malveillantes. Les assaillants tentent ainsi d'inoculer un malware qui assurera un minage permanent, puisque ces appareils sont généralement toujours actifs. De plus, leurs interfaces sont exploitées en tant que navigateurs web modifiés, ce qui étend le nombre de vulnérabilités et de vecteurs de minage. La segmentation devient ainsi essentielle pour cloisonner ces dispositifs personnels si leurs utilisateurs les connectent à des réseaux d'entreprise.

- ***La créativité des cybercriminels au service des botnets :*** la tendance en matière de botnets illustre comment les cybercriminels maximisent l'impact de ce type de malware grâce à de multiples actions malveillantes. WICKED, une nouvelle variante du botnet Mirai, s'est ainsi enrichi de trois nouveaux exploits pour cibler les objets connectés non patchés. VPNFilter, l'attaque sophistiquée qui cible les environnements industriels SCADA/ICS grâce à une surveillance des protocoles MODBUS, est devenue une menace majeure qui exfiltre les données et peut mettre à l'arrêt un dispositif, voire un groupe de dispositifs. La variante Anubis du malware Bankbot a fait l'objet de plusieurs innovations : elle agit en tant que ransomware

et enregistreur de frappe, mais peut également assurer une fonction de cheval de Troie (avec accès distant malveillant), intercepter des SMS, verrouiller les écrans et transférer des appels. Ces évolutions au niveau des attaques doivent être suivies précisément, grâce notamment à une veille pertinente sur les menaces.

- ***Les concepteurs de malware misent sur un développement agile :*** les malwares ont longtemps été polymorphes pour éviter de se faire détecter. Les récentes attaques soulignent une adoption des pratiques de développement agile pour rendre la détection des malwares plus complexe et contourner les toutes dernières fonctions des produits anti-malware. GandCrab compte déjà plusieurs versions cette année et ses concepteurs continuent à le faire évoluer rapidement. L'automatisation des attaques, tout comme les méthodes de développement agile, pose un réel défi aux organisations ciblées, ces dernières ne disposant pas toujours du savoir-faire nécessaire pour contrer des menaces toujours plus furtives. Le développement agile utilisé par les cybercriminels incite à déployer des fonctions évoluées de protection et de détection pour combattre ces attaques de nouvelle génération.

- ***Un ciblage efficace des vulnérabilités :*** les cybercriminels sélectionnent avec précision les vulnérabilités qu'ils souhaitent exploiter. Ces dernières sont sélectionnées compte tenu de leur prévalence et du volume d'exploits détectés : ainsi seules 5,7% des vulnérabilités connues sont réellement exploitées. Mais si la majorité d'entre elles ne seront pas exploitées, elles doivent néanmoins être restaurées proactivement par les entreprises.

- ***L'utilisation des applications dans les secteurs de l'enseignement et des services publics :*** lorsqu'on compare le nombre d'applications utilisées par secteur d'activité, l'utilisation d'applications SaaS dans le secteur public surperforme la moyenne de 108%. D'autre part, ce secteur est devancé par celui de l'enseignement sur le critère du nombre total d'applications utilisées chaque jour, ce chiffre étant de 22,5% et 69% supérieur à la moyenne, respectivement. Le besoin pour un panel diversifié d'applications explique le taux d'utilisation plus important sur ces deux secteurs d'activité. Il s'agira néanmoins de décloisonner ces différentes applications au sein des environnements multi-cloud, pour renforcer la visibilité et appliquer les fonctions de sécurité.

La lutte contre les attaques évoluées exige une sécurité intégrée et adossée à une veille sur les menaces

Sur ce trimestre, les données sur les menaces viennent à nouveau valider les prédictions des chercheurs FortiGuard Labs pour 2018. Une Security Fabric intégrée sur l'ensemble de la surface d'attaque s'impose. Cette approche permet aux informations de veille sur les menaces d'être partagées à grande échelle, accélère les processus de détection et offre la restauration automatique nécessaire à des exploits utilisant de multiples vecteurs d'attaque.

Méthodologie de l'étude

Le Fortinet Global Threat Landscape, rapport trimestriel issu des travaux collectifs de veille FortiGuard Labs, capitalise sur un large panel de capteurs déployés par Fortinet sur le second trimestre 2018. L'étude propose des données mondiales, par région et par secteur d'activité, et se penche sur trois volets essentiels et complémentaires de l'univers des menaces, à savoir les exploits applicatifs, les logiciels malveillants et les botnets. Sont également étudiées les vulnérabilités zero-day majeures. En complément de ces études trimestrielles, Fortinet propose ses publications Threat Intelligence Brief, gratuitement et sur abonnement, qui passent en revue les malwares, virus et menaces web découverts chaque semaine, et redirigent vers les études et travaux les plus pertinents des chercheurs de Fortinet.

Ressources supplémentaires

Rendez-vous sur notre blog pour davantage d'informations sur cette étude et accéder à la totalité du rapport.

Consultez notre blog pour en savoir davantage sur les nouveautés des services de sécurité FortiGuard.

Abonnez-vous aux FortiGuard Threat Intelligence Briefs ou au FortiGuard Threat Intelligence Service

Découvrez vos programmes Network Security Expert, Network Security Academy et FortiVets.

Découvrez ce qu'est la Security Fabric de Fortinet et la troisième génération de la sécurité réseau.

Suivez-nous sur Twitter, LinkedIn, Facebook, YouTube, and Instagram.

À propos de Fortinet

Fortinet assure la sécurité des entreprises, fournisseurs de services et administrations parmi les plus grandes au monde. Fortinet apporte à ses clients une protection intelligente et transparente, véritable ligne de défense d'une surface d'attaque qui s'étend. Cette sécurité affiche des performances pérennes, adaptées à des réseaux décloisonnés. Seule l'architecture Security Fabric de Fortinet est capable de déployer une sécurité sans compromis pour relever les défis de sécurité les plus critiques au sein des environnements réseaux, applicatifs, cloud ou mobiles. Plus de 360 000 clients dans le monde font aujourd'hui confiance à Fortinet pour les protéger.

Pour en savoir davantage : http://www.fortinet.com, http://www.fortinet.fr, le blog Fortinet ou FortiGuard Labs.

FTNT-O