WatchGuard révèle une Multiplication des Attaques 'Macro less' via des Documents Word, et un Bond de 167% des Malwares Zero Day

Parallèlement, WatchGuard annonce Threat Landscape, un outil gratuit de visualisation de l'environnement des menaces, qui permet de mieux comprendre l'évolution du nombre et de la typologie des attaques.

WatchGuard® Technologies, un leader dans le domaine des solutions avancées de sécurité réseau, annonce les résultats de son rapport sur la sécurité Internet pour le quatrième trimestre 2017, qui dresse le bilan des menaces de sécurité les plus récentes affectant les ordinateurs et les réseaux des petites et moyennes entreprises (PME) et des entreprises distribuées. Parmi ses principales conclusions, le rapport révèle que le nombre total des attaques par malware a augmenté de 33% sur le trimestre, et que les cyber criminels exploitent de plus en plus des documents Microsoft Office pour délivrer des contenus malicieux. Parallèlement, WatchGuard annonce le lancement de l'outil de visualisation Threat Landscape, disponible gratuitement, qui donne aux utilisateurs accès à des mises à jour quotidiennes sur les principales menaces de sécurité affectant les réseaux et les ordinateurs des PME et des entreprises distribuées.

"Après une année complète de collecte et d'analyse des données provenant des boîtiers de sécurité Firebox installés à travers le monde, nous pouvons voir clairement que les cyber criminels continuent à exploiter des attaques sophistiquées et des schémas complexes de livraison de malwares afin de voler des données sensibles," a déclaré Corey Nachreiner, chief technology officer chez WatchGuard Technologies. "Même si leurs tactiques peuvent varier avec le temps, nous pouvons être certains que cette tendance générale va persister, ce qui veut dire que les risques n'ont jamais été élevés pour les petites et moyennes organisations qui disposent de ressources informatiques limitées. Nous encourageons les entreprises de toutes tailles à pallier ces menaces de façon proactive, via des services de sécurité multi-couches, des protections avancées contre les malwares et la formation de leurs employés sur les meilleures pratiques en matière de sécurité."

Le Rapport sur la Sécurité Internet de WatchGuard examine chaque trimestre le paysage actuel des menaces, et fournit des données stratégiques, des conseils et une analyse en profondeur afin d'aider ses lecteurs à comprendre les tendances les plus récentes en matière d'attaques, et à adapter leurs défenses en conséquence. Les principales conclusions du rapport du quatrième trimestre 2017 comprennent :

- **Des cyber criminels ont exploité des documents Office malicieux pour piéger leurs victimes.** Les attaques Dynamic Data Exchange (DDE) sont entrées dans le top 10 des malwares recensés par WatchGuard au quatrième trimestre, les criminels exploitant de façon accrue les faiblesses de ce protocole standard de Microsoft Office pour éxécuter du code. Egalement appelés "malwares macro-less", ces documents malicieux utilisent souvent des scripts PowerShell pour passer au travers des défenses. De plus, parmi les dix principales attaques réseau enregistrées au cours du trimestre, deux ont impliqué des 'exploits' Microsoft Office, ce qui souligne encore plus la croissance de ces attaques exploitant des documents malicieux.
- **Le nombre total des attaques de malwares s'est largement accru, et celui des variantes 'zero day' a fait un bond de 167%.** Les boîtiers WatchGuard Firebox ont bloqué plus de 30 millions de variantes de malwares au total au quatrième trimestre, ce qui représente une augmentation de 33% par rapport au trimestre précédent. Parmi l'ensemble des menaces bloquées au cours du trimestre, la catégorie des malwares nouveaux ou 'zero day' a fait un bond de 167% comparé au troisième trimestre. Il est probable que ces hausses sont dues à une activité criminelle accrue pendant la période des fêtes de fin d'année.
- **Près de la moitié des malwares sont passés au travers des solutions antivirus traditionnelles.** Les boîtiers WatchGuard Firebox bloquent les malwares en utilisant à la fois

des techniques traditionnelles basées sur des signatures et la solution proactive APT Blocker, qui repose sur l'analyse comportementale. Lorsqu'APT Blocker bloque une variante de malware, cela veut dire que les signatures antivirus traditionnelles l'ont manqué. Ces malwares 'zero day' ont représenté 46% de tous les malwares détectés au quatrième trimestre. L'importance de ce chiffre suggère que les criminels utilisent des techniques d'évitement plus sophistiquées capables de contourner les services antivirus tradtionnels, ce qui renforce la valeur des défenses basées sur une analyse comportementale.

- **Les attaques basées sur des scripts représentent 48% des principaux malwares.** Les attaques bloquées par des signatures de menaces JavaScript et Visual Basic Script, telles que des 'downloaders' et des 'droppers', ont représenté la majorité des malwares détectés au quatrième trimestre. Les utilisateurs doivent avoir conscience de la popularité continue de ces attaques et surveiller la présence de scripts malicieux dans les pages web et les attachements d'emails de tous types.

Le Rapport sur la Sécurité Internet rassemble des évaluations des principaux malwares et principales attaques réseau rencontrés au cours du trimestre, des recommandations relatives aux meilleures stratégies de defense dans l'environnement de menaces actuel, et une analyse détaillée de la "Krack Attack" – un événement majeure en matière de sécurité en 2017.

Le rapport est basé sur des données Firebox Feed anonymes provenant de près de 40.000 boîtiers UTM WatchGuard en service à travers le monde, qui ont bloqué plus de 30 millions de variantes de malwares (783 par boîtier) et 6,9 millions d'attaques réseau (178 par boîtier) au quatrième trimestre 2017. Il intègre également un nouveau projet de recherche mené par le WatchGuard Threat Lab, qui analyse une base de données contenant plus d'un milliard de vols de mots de passe pour déterminer la fréquence avec laquelle les utilisateurs choisissent des mots de passe trop simples et réutilisent les mêmes identifiants sur de multiples comptes.

Le nouvel outil de visualisation Threat Landscape

Le nouvel outil de visualisation Threat Landscape de WatchGuard fournit des mises à jour quotidiennes concernant les principaux malwares et les principales attaques réseau détectés dans le monde. La page d'accueil Threat Landscape permet aux utilisateurs de consulter les données issues du Firebox Feed par type d'attaque, par region ou par pays, et par périodes de temps, avec des graphiques interactifs qui sont mis à jour instantanément et faciles à lire.

Pour plus d'informations, le rapport au complet est disponible ici.

A propos de WatchGuard Technologies, Inc.

WatchGuard® Technologies, Inc. est un leader mondial dans le domaine de la sécurité réseau, et fournit une gamme complète de solutions UTM (Unified Threat Management), Firewall de Nouvelle Génération, WiFi sécurisé, d'intelligence réseau et de services associés à plus de 80.000 clients à travers le monde. La mission de la société est de rendre les solutions de sécurité les plus performantes accessibles à des entreprises de tous types et de toutes tailles grâce à un haut niveau de simplicité, ce qui rend les solutions WatchGuard idéales pour les entreprises distribuées et les PME. WatchGuard a son siège à Seattle, Washington, et possède des bureaux dans toute l'Amérique du Nord, en Europe, en Asie Pacifique et en Amérique latine. Pour en savoir plus, visiter WatchGuard.com.