28/04/2025

Des pirates bombardent des applications et VPN de millions de tentatives de connexion

Des pirates bombardent des applications et VPN de millions de tentatives de connexion

Un rapport de Cisco fait état d'une campagne mondiale de forçage d'identifiants ciblant des services VPN et SSH.

Les spécialistes de la sécurité de Cisco Talos mettent en garde les utilisateurs de diverses applications VPN et SSH contre d'éventuelles attaques par force brute à grande échelle. Par le biais de ces attaques qui consistent à « essayer » des noms d'utilisateur et des mots de passe, les cybercriminels cherchent avant tout à extraire les identifiants de connexion afin d'accéder aux appareils et aux systèmes sous-jacents. Dans la campagne identifiée par les chercheurs le 18 mars 2024, les cybercriminels utilisent une combinaison de noms d'utilisateur valides et génériques, ciblant des entreprises spécifiques. Si quelques noms tels que Cisco, CheckPoint, Fortinet, SonicWall et Ubiquiti sont évoqués, on ne sait pas combien d'autres entreprises ou organisations sont également touchées, ni quels cybercriminels sont à l'origine de ces attaques. La montée en puissance des attaques par force brute

La campagne découverte par Cisco Talos n'est pas une menace isolée, mais le symptôme d'une vulnérabilité persistante que les entreprises ont du mal à endiguer. Les services VPN et SSH, essentiels pour la confidentialité et la sécurité des échanges en ligne, sont devenus les cibles privilégiées des cybercriminels. En utilisant des combinaisons d'identifiants, les attaquants cherchent à obtenir un accès non autorisé aux réseaux internes, provoquant potentiellement des verrouillages de comptes et des dénis de service. La progression constante du trafic malveillant indique une tendance alarmante, avec des attaques de plus en plus sophistiquées et difficiles à détecter. Les services utilisés pour orchestrer ces attaques sont divers et comprennent des outils d'anonymisation tels que TOR, VPN Gate, IPIDEA Proxy, BigMama Proxy, Space Proxies, Nexus Proxy et Proxy Rack. Ces plateformes permettent aux cybercriminels de masquer leur identité et leur localisation, compliquant ainsi la tâche des équipes de sécurité pour les repérer et les bloquer. La liste des services ciblés est longue et variée, allant des VPN de pare-feu sécurisé Cisco aux services web de recherche en développement, en passant par les dispositifs Ubiquiti et Draytek. Des programmes capables de viser simultanément des milliers de comptes

Ces attaques ciblent principalement les VPN, les services SSH et les interfaces d'authentification des applications web. Pour contrer cette menace, Cisco Talos a publié sur son site une liste de près de 4 000 adresses IP associées aux attaquants ainsi qu'environ 2 100 identifiants génériques utilisés dans les attaques, incitant les organisations à bloquer ces adresses pour protéger leur trafic réseau. La sophistication de ces attaques est renforcée par la reconnaissance préalable, permettant aux acteurs malveillants de cibler leurs attaques avec précision. Les pirates utilisent des programmes automatisés qui peuvent simultanément viser des centaines, voire des milliers de comptes, augmentant ainsi les chances de succès. Pour éviter les mécanismes de sécurité qui bloquent les tentatives de connexion infructueuses, ils peuvent également opter pour la pulvérisation de mots de passe, où un grand nombre de mots de passe sont testés sur un petit nombre de comptes. Par exemple, la tête de réseau VPN Secure Firewall ASA de Cisco a enregistré jusqu'à des millions de tentatives d'authentification

rejetées, indiquant des attaques par pulvérisation de mots de passe. C'est une des raisons pour lesquelles Cisco Talos recommande aux organisations de revoir leur copie et leur stratégie de sécurité. L'activation des systèmes de journalisation et la configuration de la commande « no logging hide username » sont essentielles pour détecter toute tentative de connexion non autorisée. Les indicateurs de compromission (IOC) comprennent des messages d'erreur lors des tentatives de connexion aux services VPN, des échecs d'allocation de jetons Hostscan et un volume élevé de tentatives d'authentification rejetées dans les journaux système.

Ex-journaliste société, l'univers du web, des réseaux, des machines connectées et de tout ce qui s'écrit sur Internet m'ouvre l'appétit. De la dernière trend TikTok au reels le plus liké, je suis issu… Lire d'autres articles Ex-journaliste société, l'univers du web, des réseaux, des machines connectées et de tout ce qui s'écrit sur Internet m'ouvre l'appétit. De la dernière trend TikTok au reels le plus liké, je suis issue de la génération Facebook que la guerre intestine entre Mac et PC passionne encore. En daronne avisée, Internet, ses outils, pratiques et régulation font partie de mes loisirs favoris (ça, le lineart, le tricot et les blagues pourries). Ma devise: l'essayer, c'est l'adopter, mais en toute sécurité. Lire d'autres articles
https://www.clubic.com/actualite-524397-des-pirates-bombardent-des-applications-et-vpn-de-millions-de-tentatives-de-connexion.html