Le secteur financier: secteurs ciblÃ©s par les groupes de ransomware
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 4/3/2024 15:00:00

Le Threat Labs de Netskope a publiÃ© son dernier rapport de recherche, rÃ©vÃ©lant que le secteur financier reste l'un des principaux secteurs ciblÃ©s par les groupes de ransomware.Â Â Les chercheurs de Netskope ont observÃ© une adoption croissante des applications cloud dans le secteur des services financiers, et un abus inquiÃ©tant de ces canaux, afin dâ□□Ã©chapper aux contrÃ´les de sÃ©curitÃ© rÃ©guliers, pour les attaques de malware et de ransomware.Â Leurs principales conclusions sont les suivantes :Â â□¢Les applications cloud de Microsoft dominent le secteur de la finance : Microsoft OneDrive, Microsoft Teams et Sharepoint figurent parmi les plus populaires dans le secteur des services financiers, Microsoft Teams Ã©tant nettement plus populaire que dans les autres secteurs.â□¢Des cibles changeantes pour les tÃ©lÃ©chargements de malwares : OneDrive et Sharepoint, ainsi que Github sont identifiÃ©s comme des canaux utilisÃ©s pour les abus potentiels d'applications cloud - les trois Ã©tant en haut de la liste de maniÃ¨re constante depuis septembre 2023.Â

â□¢Sharepoint Ã©tait plus important dans la finance que dans d'autres secteurs, ce qui est principalement liÃ© Ã la popularitÃ© de Microsoft Teams qui utilise Sharepoint pour le partage de fichiers.Â â□¢Cible clÃ© pour les attaques de ransomware : le secteur financier reste l'un des plus attaquÃ©s par les groupes de ransomware, les chevaux de Troie Ã©tant le principal mÃ©canisme d'attaque, incitant les utilisateurs du secteur financier Ã tÃ©lÃ©charger d'autres charges utiles de malwares. Le gang de ransomwares Clopp a notamment Ã©tÃ© particuliÃ¨rement actif au cours du second semestre 2023, exploitant la vulnÃ©rabilitÃ© CVE-2023-34362 MOVEit.Â â□¢LockBit Ã©tait Ã©galement un groupe de ransomwares de premier plan qui ciblait principalement le secteur de la finance et qui a rÃ©cemment Ã©tÃ© ciblÃ© et arrÃªtÃ© par les forces de l'ordre.Â Â« Il est clair que les tendances macroÃ©conomiques de l'utilisation et de l'abus des applications cloud sont restÃ©es cohÃ©rentes dans le secteur financier au cours de l'annÃ©e Ã©coulÃ©e, dÃ©clare Paolo Passeri, Cyber Intelligence Specialist chez Netskope. Il est intÃ©ressant de constater que le secteur financier reste l'un des secteurs les plus attaquÃ©s par les groupes de ransomware qui se concentrent sur l'exploitation des vulnÃ©rabilitÃ©s Ã grande Ã©chelle. Ces chiffres nous rappellent que chaque organisation devrait prendre le temps d'Ã©valuer et de sÃ©curiser sa propre infrastructure, tout en prenant conscience que de simples erreurs opÃ©rationnelles peuvent l'exposer Ã des menaces importantes. Â»Â Les malwares diffusÃ©s sur le cloud reprÃ©sentent 50 % des tÃ©lÃ©chargements de logiciels malveillants dans le secteur financier, ce qui est conforme Ã la tendance observÃ©e dans d'autres secteurs, Ã©tant donnÃ© la capacitÃ© des cybercriminels Ã Ã©chapper aux contrÃ´les de sÃ©curitÃ© habituels, qui reposent sur des outils tels que les listes de blocage de domaines et la surveillance du trafic web, mais qui n'appliquent pas les principes du zero trust pour inspecter systÃ©matiquement le trafic cloud.Â Le rapport est basÃ© sur des donnÃ©es d'utilisation anonymes collectÃ©es sur un sous-ensemble de plus de 2 500 clients de Netskope appartenant au secteur financier, qui ont tous donnÃ© leur autorisation prÃ©alable pour que leurs donnÃ©es soient analysÃ©es de cette maniÃ¨re.