CybercriminalitÃ© : Des menaces par email via leurs fournisseurs
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 12/4/2021 13:00:00

Les cyberattaques indirectes ont le vent en poupe et les attaquants exploitent de plus en plus les relations de confiance Ã©tablies entre les entreprises et leurs fournisseurs pour accÃ©der aux donnÃ©es confidentielles quâ□□ils convoitent.
Ils usurpent lâ□□identitÃ© et sâ□□approprient des comptes compromis de partenaires pour envoyer des logiciels malveillants, voler des informations d'identification et commettre des fraudes Ã la facturation.Â

Dans une Ã©tude rÃ©cente, Proofpoint indique que 98 % des organisations sur un panel mondial de 3000 entreprises ont reÃ§u une menace provenant d'un domaine fournisseur au cours d'une pÃ©riode de 7 jours en fÃ©vrier 2021.Â Â Ã□ quoi ressemblent les menaces liÃ©es aux fournisseurs ?Â Selon Proofpoint, les attaquants utilisent les fournisseurs et les partenaires commerciaux pour envoyer tous les types de menaces :Â phishing, logiciels malveillants ou attaques de compromission dâ□□emails professionnels de type BEC.Â

Lâ□□Ã©tude montre que ces menaces dans la supply chain provenant de fournisseurs usurpÃ©s ou compromis sâ□□appuient sur lâ□□ingÃ©nierie sociale pour maximiser leurs chances de succÃ¨s.Â

74 % des menaces sont du phishing et moins de 30 % des menaces envoyÃ©es depuis des domaines de fournisseurs Ã©taient liÃ©es Ã des logiciels malveillants dÃ©montrant ainsi que les attaquants ciblent les personnes plutÃ´t que les vulnÃ©rabilitÃ©s de l'infrastructure des entreprises.Â Â Les plateformes de collaboration populaires telles que Microsoft 365, Google G-Suite et Dropbox sont Ã©galement exploitÃ©es Ã un rythme alarmant pour hÃ©berger des menaces dans le cloud.Â Des pertes financiÃ¨res consÃ©quentesÂ Si les menaces de fraude par e-mail sont de faible volume et trÃ¨s ciblÃ©es, elles reprÃ©sentent souvent des pertes financiÃ¨res importantes. Proofpoint a observÃ© et arrÃªtÃ© des attaques de fraude Ã la facturation de fournisseurs se chiffrant en millions de dollars.Â
De plus, selon le rapport annuel Â« Internet Crime Report 2020 Â» du FBI, les escroqueries de type Business Email Compromise (BEC) et Email Account Compromise (EAC) reprÃ©sentent la plus grande perte financiÃ¨re en 2020, coÃ»tant aux entreprises victimes prÃ¨s de 1,9 milliard de dollars.Â Â Â Les secteurs les plus touchÃ©s concernent la finance, lâ□□industrie, ou encore les services publics, la communication, le commerce et transport, cependant, les entreprises de toutes tailles et de tous secteurs sont exposÃ©es aux risques liÃ©s aux fournisseurs confirmant qu'il s'agit d'une prÃ©occupation universelle.Â Â Les cybercriminels ont transformÃ© l'Ã©cosystÃ¨me des partenaires en un vecteur de menaces et les entreprises doivent tout mettre en Å□uvre pour sâ□□en prÃ©munir.Â
Sâ□□il nâ□□y a pas de solution miracle, il convient de mettre en place une dÃ©fense Ã plusieurs niveaux : une plateforme de protection contre les menaces complÃ¨te et intÃ©grÃ©e qui bloque les menaces envoyÃ©es par des fournisseurs compromis ou usurpÃ©s, forme les utilisateurs finaux Ã repÃ©rer et Ã signaler les e-mails suspects, automatise les enquÃªtes et les rÃ©ponses aux incidents et fournit une visibilitÃ© sur les fournisseurs qui prÃ©sentent un risque.