Le FBI alerte sur l'explosion de la fraude au président

Le Bureau fédéral d'enquête américain (FBI) base son analyse sur des plaintes déposées aux États-Unis et dans 100 pays auprès des forces de l'ordre et d'institutions financières. 22 143 entreprises sont concernées. La fraude au président aurait déjà coûté 3,1 milliards de dollars. Et les montants que les escrocs ont ainsi tenté de voler auraient bondi de 1 300 % depuis janvier 2015.

Les « scammers » (escrocs à l'origine de l'arnaque) auraient tenté d'obtenir des virements à destination de 79 pays. Mais la majeure partie se concentre dans des banques installées en Chine et à Hong Kong, sa région administrative spéciale, d'après le FBI. Dans certains cas, alerte l'agence fédérale américaine, la fraude au président est suivie par une attaque par ransomware qui chiffre les données et verrouille les terminaux d'utilisateurs appelés à payer pour en reprendre le contrôle.

Tromper la vigilance de cibles en ligne

La fraude au président consiste à obtenir un virement bancaire d'un collaborateur ou d'un partenaire en se faisant passer pour le dirigeant d'une entreprise. L'escroc cible des sociétés qui travaillent avec des fournisseurs ou d'autres entreprises à l'international. Il trompe son monde en usant de techniques d'ingénierie sociale, utilise les réseaux sociaux pour mieux connaître sa cible et lance des opérations d'hameçonnage (phishing), voire de harponnage (spear phishing), pour obtenir un transfert d'argent. Et le phénomène prend de l'ampleur auprès d'entreprises de toutes tailles.

Lire aussi :

Ingénierie sociale : les employés sont-ils le maillon faible de la cybersécurité ?

Créer des ransomwares, une petite entreprise qui rapporte