

NOWA GRUPA PRZESTĘPCZA ATAKUJE. STRATY SIĘGAJĄ 12 MLD DOLARÓW

Nowa grupa przestępcza „London Blue” jest autorem masowej kampanii oszustw na całym świecie. Na liście jej ofiar figuruje 35 tys. dyrektorów finansowych, a straty wynoszą ponad 12 miliardów dolarów.

Oszustwo polegało na przekonaniu dyrektorów finansowych do przesłania dużych sum na nieznanne konta. Najczęściej miało to miejsce za pomocą spreparowanych e-maili, które wyglądały jakby pochodziły od członków zarządu. Działaniami grupy dotkniętych zostało prawie 80 tys. przedsiębiorstw z całego świata.

Zdaniem ekspertów z firmy Agari „The London Blue” jest jedną z największych zorganizowanych grup przestępczych. Jej członkowie działają na całym świecie, a główna siedziba znajduje się w Nigerii.

Grupa miała sporządzić listę ponad 50 tys. celów, z czego 71 proc. to dyrektorzy finansowi. Resztę stanowili członkowie zarządów, kontrolerzy i księgowi. Głównym celem przestępców są firmy oferujące pożyczki hipoteczne, ale również największe banki na świecie. Zaatakowane zostały również małe i średnie przedsiębiorstwa. Najwięcej oszustw wykryto w miało miejsce w Stanach Zjednoczonych, Wielkiej Brytanii, Hiszpanii, Finlandii i Egipcie. Nie oznacza to jednak, że tylko te państwa stały się celem ataku.

Najczęściej cyberprzestępcy posługują się metodami inżynierii społecznej, głównie spearphishingiem. Uzyskują oni dokładne informacje na temat swojej ofiary. Następnie wysyłają odpowiednio spreparowane maile. Fałszywe wiadomości są tworzone przez hakerów z wielką precyzją przez co trudno jest je odróżnić od prawdziwych. Nie zawierają również złośliwego oprogramowania w załącznikach przez co nie zostają wykryte przez antywirusy.

Eksperci odkryli, że grupa „London Blue” znacznie szybciej zebrała potrzebne informacje i przygotowała się do kampanii spearphisingowej poprzez nawiązanie współpracy z brokerami informacji, którzy specjalizują się w wyszukiwaniu określonych danych. Dostarczają oni takie dane jak: imiona, nazwy firmy, tytuły, adresy emaili służbowych, ale również prywatnych.

Grupa cyberprzestępcy operuje jak dobrze zorganizowane przedsiębiorstwo. Posiada zespoły odpowiedzialne za prowadzenie wywiadu biznesowego, operacji finansowych, poszukiwania nowych członków czy nawet komórki odpowiedzialnej za sprzedaż i marketing.

Eksperci z firmy Agari pierwszy raz spotkali się z działalnością grupy przestępczej, kiedy ta zaatakowała ich dyrektora finansowego. Otrzymał on fałszywego maila, który wzbudził podejrzenia. Jego autorem rzekomo był dyrektor wykonawczy firmy. Szacuje się, że z „London Blue” współpracuje 17 osób z Europy Zachodniej i Stanów Zjednoczonych.