**Hakerzy fałszując firmowe maile wyłudzają pieniądze z funduszy inwestycyjnych oraz klubów piłkarskich**

**• Cyberprzestępcy podszywają się pod dyrektorów generalnych oraz finansowych wysyłając fałszywe maile z prośbami o realizację przelewów finansowych. To coraz popularniejszy sposób ataków na przedsiębiorstwa w czasie pandemii**

**• Na podobnej zasadzie hakerzy wyłudzili 1,3 mln dolarów od trzech współpracujących ze sobą spółek private equity**

**• Analogiczną technikę prawdopodobnie zastosowali hakerzy przejmujący korespondencję pomiędzy klubami piłkarskimi PSG oraz Boca Juniors. Za pomocą modyfikacji przesyłanych e-maili przestępcy zdołali przekierować środki na inne konto, w rezultacie pół miliona Euro trafiło na rachunek w Meksyku, przechodząc po drodze przez nowojorski CitiBank.**

Przeniesienie pracy biurowej do domu zainspirowało cyberprzestępców. Opracowali oni metodę oszustwa wykorzystującego fakt, że firmy coraz częściej komunikują się jedynie w oparciu o pocztę elektroniczną. Tak powstał nowy model oszustw nazwany „BEC” – ostrzegają badacze z firmy Check Point.

„BEC” to skrót od „business email compromise”, co oznacza naruszenie poczty biznesowej. Jest to typ oszustwa wykorzystujący e-maile podszywające się pod wiadomości przełożonych, w celu wyłudzenia przelewu pieniężnego lub poufnych danych. Zarówno eksperci Check Pointa jak i FBI uważają, że głównymi celami oszustw BEC są firmy private equity i venture capital, ponieważ hakerzy zdają sobie sprawę, że dla tego typu spółek potężne transfery pieniężne nie są niczym nietypowym.

W tym roku analitycy Check Pointa rozwikłali schemat, w którym cybergang „Florentine Banker” wyłudził ok. 1,3 mln dolarów, dzięki fałszowaniu korespondencji między trzema spółkami private equity. Przez miesiące „bankierzy florenccy” dokładnie badali wiadomości trzech spółek, a następnie zaczęli tak manipulować korespondencjami, by przejmować przelewy na wysokie sumy w strategicznych momentach. Interwencja ze strony firmy Check Point spowodowały odzyskanie ponad połowy kwoty, którą hakerzy starali się wykraść. Reszta bezpowrotnie zniknęła z kont ofiar.

**„BEC” znany jest również w środowisku… piłkarskim**

Podobną technikę zastosowali hakerzy przejmujący korespondencję pomiędzy klubami piłkarskimi PSG oraz Boca Juniors. Za pomocą modyfikacji przesyłanych e-maili przestępcy zdołali przekierować środki na inne konto, w rezultacie pół miliona Euro trafiło na rachunek w Meksyku, przechodząc po drodze przez nowojorski CitiBank.

Analogicznie wyglądała sytuacja przy spłacie ostatniej raty za transfer Stefana de Vrija, przechodzącego z Feyenoordu Rotterdam do Lazio Rzym. Wykorzystując scamming, przestępcy przejęli dwa miliony Euro, które powinny trafić na konto holenderskiego klubu. Sprawa wyszła na jaw dopiero, gdy klub z Rotterdamu wysłał upomnienie w sprawie zaległości ostatniej raty.

**Jak to działa?**

Oszustwo „BEC” rozpoczyna się shakowania poczty e-mail i wykorzystania fałszywej wiadomości pochodzącej od cyberprzestępców podających się za dyrektorów finansowych, dyrektorów generalnych bądź partnerów biznesowych. Żądając pozornie autentycznej płatności, cyberprzestępcy proszą pracownika działu finansów o transfer pieniężny lub zdeponowanie czeków. Niczego nieświadomy pracownik, będąc przekonanym o autentyczności wiadomości od przełożonego (adres email zgodny z oryginalnym), automatycznie dokonuje płatności pod wskazany przez hakerów nr konta. Cała procedura oparta jest na inżynierii społecznej i wymaga od przestępców internetowych wielomiesięcznych przygotowań, polegających na monitorowaniu i badaniu korespondencji firmowej oraz zwyczajów panujących w organizacji.

Oszustwa BEC są najczęściej przeprowadzane przez jedną osobę, jednak ostatnio badacze z firmy Check Point zauważyli, że działania te stają się coraz bardziej wyrafinowane i często mogą być klasyfikowane jako przestępczość zorganizowana.

*- Jesteśmy w trakcie poważnej zmiany paradygmatu aktywności hakerów. Przestępcy starają się wykorzystywać obecnie najsłabsze ogniwa pracy zdalnej. Oszustwa typu „BEC” spostrzegamy jako część szerszego trendu* *–* mówi Wojciech Głażewski, zarządzający polskim oddziałem firmy Check Point. - *Firmy i organizacje dokonujące transferów dużych sumy pieniężnych, powinny zdawać sobie sprawę, że mogą znajdować się w kręgu zainteresowania cyberprzestępców.*

W związku z rosnącą popularnością metody „BEC” Check Point rekomenduje kilka zasad bezpieczeństwa, które mogą pomóc w uniknięciu potencjalnego oszustwa:

Po pierwsze należy włączyć w poczcie biznesowej uwierzytelnianie wieloskładnikowe, co powinno utrudnić dostęp do poczty e-mail pracowników. Po drugie rekomenduje się dokładne sprawdzenie adresów e-mail i nieotwieranie żadnych wiadomości pochodzących z nieznanych lub wyglądających podejrzanie adresów. Trzecim punktem jest dokonywanie weryfikacji przelewu np. przez kontakt telefoniczny. Ostatnią rekomendacją jest przesyłanie dalej, a nie odpowiadanie na e-maile biznesowe. Przekazując wiadomość e-mail, należy ręcznie wpisać poprawny adres e-mail lub wybrać go z książki adresowej, co zapewni wpisanie właściwego adresu e-mail adresata.