OUCH! | Lipiec 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Czym jest CEO Fraud?
- Zabezpiecz się

CEO Fraud

Czym jest CEO Fraud?

Cyberprzestępcy są podstępni - stale wymyślają nowe sposoby by zdobyć to czego chcą. Jedną z ich najbardziej skutecznych metod jest wybranie za cel ataku ludzi takich jak Ty. Cyberprzestępcy przekonani, że osoby nieświadome są najsłabszym ogniwem każdej organizacji, zapomnieli o doświadczonych osobach, takich jak czytelnicy OUCH-a!, którzy mogą być najlepszą obroną dla swojej organizacji.

Redaktor gościnny

Angela Pappas jest dyrektorem ds. szkoleń z zakresu bezpieczeństwa informacji i świadomości w Thomson Reuters. Angela jest odpowiedzialna za program ambasadorski, eLearning i edukację pracowników na temat phishingu.

Cyberprzestępcy opracowali nowy sposób ataku o nazwie CEO Fraud, znany także jako Business Email Compromise (BEC). W atakach tych, cyberprzestępcy podszywają się pod dyrektora generalnego lub inną osobę z władz Twojej organizacji. Następnie wysyłają e-maile do pracowników starając się nakłonić ich do wykonania czegoś, czego nie powinni robić. Tego typu ataki są wyjątkowo skuteczne ze względu na rozeznanie prowadzone przez cyberprzestępców. Szukają oni bowiem na stronach internetowych Twojej organizacji informacji na temat lokalizacji firmy, osób na stanowiskach kierowniczych, a także informacji o Twoich współpracownikach. Następnie, z takich serwisów jak Linkedin, Facebook lub Twitter, próbują się dowiedzieć jak najwięcej o osobach z którymi pracujesz. Kiedy już atakujący poznają strukturę organizacji ich uwaga zaczyna się skupiać na wytypowanych pracownikach. Cel ataku jest wybierany w zależności od zakładanych efektów. Jeśli cyberprzestępcy są zainteresowani kradzieżą pieniędzy mogą kierować swoje działania przeciwko pracownikom działu płatności. Jeśli są zainteresowani informacjami o pracownikach celem ataku może być dział kadr. Jeśli natomiast przestępcy chcą uzyskać dostęp do baz danych wówczas ich celem będą pracownicy działu IT.

Kiedy przestępcy zdecydują już co chcą zdobyć i kto będzie ich celem, rozpoczynają przygotowania do ataku. Najczęściej używają techniki spear phishing. Z phishingiem mamy do czynienia wtedy, gdy atakujący wysyła maile do dużej liczby osób z zamiarem nakłonienia ich do zrobienia czegoś, np. otwarcia zainfekowanego załącznika lub spreparowanej strony internetowej. Spear phising jest podobny do phishingu, z tym że maile nie są wysyłane do dużej liczby osób, a jedynie do wąskiej, wybranej grupy. Takie spear-phishingowe maile wyglądają dość realistycznie i są trudne do wykrycia. Często sprawiają wrażenie jakby pochodziły od kogoś kogo znasz lub z kim pracujesz, np. od znajomego z pracy, czy nawet Twojego szefa. Maile te wyglądają realistycznie ponieważ jest w nich używany żargon, którego używacie w pracy, może pojawiać się logo

CEO Fraud

Waszej firmy lub nawet oficjalny podpis osoby z zarządu. Poza tym, maile te tworzą poczucie pośpiechu żądając od odbiorcy podjęcia natychmiastowych działań, o których nie powinien on nikomu mówić. Celem cyberprzestępcy jest nakłonienie Ciebie do jak najszybszego popełnienia błędu. Oto trzy typowe scenariusze:

CEO Fraud jest potężnym atakiem, który może obejść większość zabezpieczeń. W tym przypadku to Ty stanowisz najlepszą obronę.

- **Przelew**: celem cyberprzestępcy są pieniądze. Oznacza to, że atakujący będzie dociekał kto pracuje w dziale finansowym lub który zespół zajmuje się finansami organizacji. Następnie przestępcy przygotują i wyślą do odpowiedniego zespołu maila, podszywając się pod szefa zespołu, z informacją jakoby miał on nagły wypadek i prosił o natychmiastowe przelanie pieniędzy na wskazany numer konta.

- **Wyłudzanie informacji**: Cyberprzestępcy chcą wykraść informacje o Twoich współpracownikach aby móc się pod nich podszyć i wykradać dane. Cyberprzestępcy wnikliwie analizują strukturę organizacji i określają kto może posiadać wiedzę o pracownikach, np z działu kadr. Następnie, podszywając się m.in. pod pracowników wyższego szczebla wysyłaj maile, w których wymagają niezwłocznego udostępnienia danych.

- **Podszywanie się pod prawnika**: Nie wszystkie ataki CEO Fraud obejmują maile. Inną ścieżką ataku może być telefon. W tym scenariuszu, przestępcy zaczynają wymieniać z Tobą e-maile podając się za szefa i twierdząc, że zadzwoni do Ciebie prawnik w pilnej sprawie. W rezultacie dzwoni do Ciebie przestępca podając się za prawnika. Przestępca mówiąc przez telefon o sprawach pilnych i poufnych tworzy poczucie powagi sytuacji, które mylnie zmusza Cię do natychmiastowych działań.

Zabezpiecz się

Co można w takim razie zrobić, aby chronić siebie i swoją organizację? Pamiętaj, że najlepszą obroną jest zdrowy rozsądek. Jeśli otrzymasz maila od swojego szefa lub współpracownika i brzmi on nieco inaczej niż zwykle, może być to atak. Często mail może sprawiać wrażenie poczucia pilności, podpis może budzić zastrzeżenia, ton maila może być taki, jakiego nigdy byś się nie spodziewał. Zdarza się też, że nazwisko osoby z maila różni się od tej, która faktycznie do Ciebie dzwoni. Inną wskazówką do wykrycia ataku może być użycie przez atakującego adresu e-mail lub numeru telefonu, których nigdy przedtem nie używał lub są bardzo podobne, ale nieidentyczne z tymi, używanymi przez szefa lub Twoich współpracowników. W przypadku wątpliwości

CEO Fraud

zadzwoń do tej osoby na zaufany numer telefonu lub spotkaj się z nią osobiście (nie odpowiadaj na maila) i potwierdź, czy osoba faktycznie wysłała maila. Nigdy nie omijaj polityk i procedur bezpieczeństwa. Twoja organizacja może mieć zasady określające procedury autoryzacji przelewów pieniężnych czy też wydawania dostępu do informacji poufnych. Wnioski i prośby, które próbują obejść te zasady, niezależnie od osoby wnioskującego, powinny być podejrzliwie rozważone i zweryfikowane przed podjęciem jakichkolwiek działań. W przypadku otrzymania takiego wniosku i braku pewności co z nim zrobić, należy natychmiast skontaktować się ze swoim przełożonym, działem pomocy technicznej lub zespołem bezpieczeństwa.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.

Odwiedź securingthehuman.sans.org/ouch/archives i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.

WWW: http://www.cert.pl

Twitter: @CERT_Polska

Facebook: http://facebook.com/CERT.Polska

Źródła

Socjotechnika:	https://securingthehuman.sans.org/ouch/2014#november2014
Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
Czym jest złośliwe oprogramowanie:	https://securingthehuman.sans.org/ouch/2016#march2016
Dwuskładnikowe uwierzytelnianie:	https://securingthehuman.sans.org/ouch/2015#september2015

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Polski przekład (NASK/CERT Polska): Paweł Jacewicz, Małgorzata Dębska, Przemysław Zielony

