Studia przypadków inżynierii społecznej

Jak wyjaśniono wcześniej, inżynieria społeczna jest sztuką manipulowania zachowaniem przy użyciu specjalnie spreparowanych technik komunikacji. Inżynier społeczny to haker, który używa mózgów zamiast technicznych procesów komputerowych. Inżynierowie społeczni to hakerzy, którzy wykorzystują słabość występującą w prawie każdej organizacji, czynnik ludzki. Korzystając z różnych technik i narzędzi, inżynier społeczny może wykonywać połączenia telefoniczne i korzystać z mediów społecznościowych lub usług e-mailowych, aby nakłonić ludzi do podania poufnych informacji lub poświadczeń. Cyberprzestępcy stosują taktykę socjotechniki, ponieważ zwykle łatwiej jest manipulować naturalnymi tendencjami jednostki niż hakować systemy komputerowe lub oprogramowanie. Bezpieczeństwo polega na tym, aby wiedzieć, komu i kiedy zaufać, a także wiedzieć, kiedy, a kiedy nie, wierzyć słowu danej osoby. Inżynierowie społeczni wykorzystują przede wszystkim to podstawowe zjawisko - zaufanie. Dlatego dziś wiele firm chce włączyć testy socjotechniczne (phishing i inne symulacje) dla swoich pracowników, jako część ogólnego planu bezpieczeństwa informacji. Phishing, vishing, ransomware i inne rodzaje ataków socjotechnicznych są celami. Słabym ogniwem w każdym bezpieczeństwie sieci jest element ludzki. Dlatego czasami przestępcy podszywają się pod grupę osób trzecich, aby być bardziej przekonującym, zmuszać ludzi do wykonywania instrukcji bez pytania i odnieść sukces, lub udawać, że jest policjantem lub urzędnikiem państwowym. W całym badaniu ujawniono cykl ataków inżynierii społecznej i znane międzynarodowe przypadki ataków inżynierii społecznej. Ponadto oceniono pytania dotyczące tego, dlaczego ataki socjotechniki są tak skuteczne i jak przeprowadzają je inżynierowie socjalni. Ustalono, że cykl ataku inżynierii społecznej składa się z czterech następujących etapów:

*Zbieranie informacji

* Rozwijanie relacji

*Eksploatacja

*Wykonanie

Ujawniono również, że inżynieria społeczna jest tak skuteczna, ponieważ wykorzystuje naturę ludzką, z odniesieniami do statystyk z badania Black Hat 2017. Ponadto pokazano niektóre przypadki inżynierii społecznej, takie jak:

* Oszustwo CEO

* Phishing finansowy

* Phishing w mediach społecznościowych

* Wyłudzanie oprogramowania typu ransomware

* Phishing Bitcoin

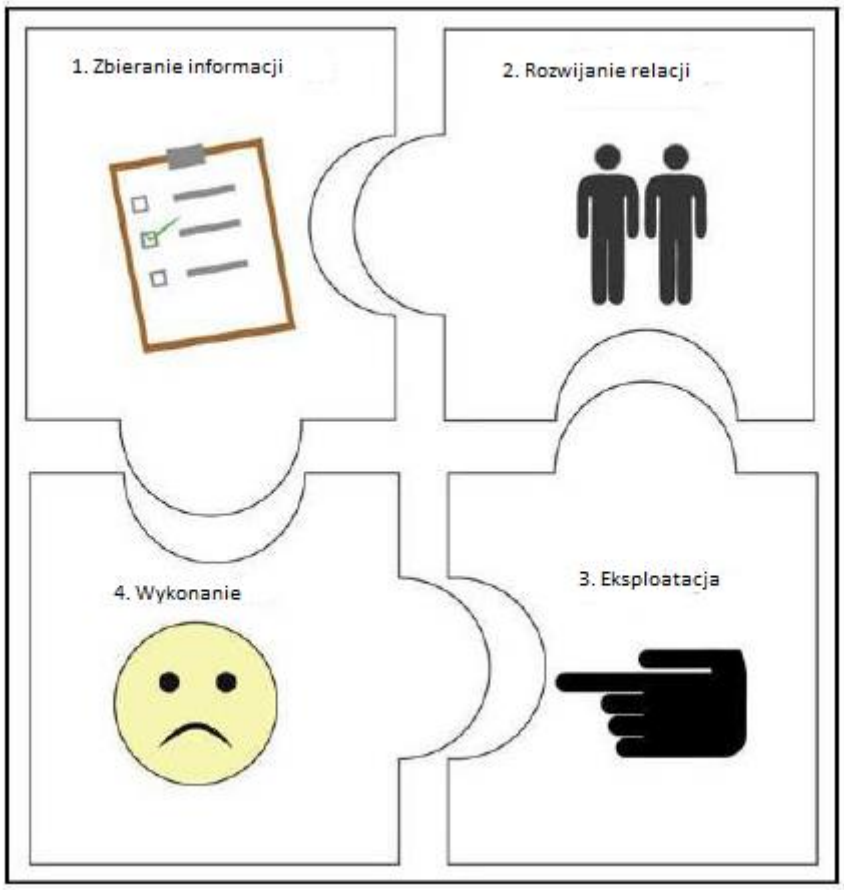
Przeprowadzono także studium przypadku. W tym celu zebrano dane z platformy symulacyjnej phishing Keepnet Labs. Oceniono jeden rok wszystkich działań w ramach kampanii phishingowej wykonanych między 1 stycznia 2017 a 1 stycznia 2018 r. Zaobserwowano te same zmienne (firmy, działy i użytkownicy / osoby) w ciągu jednego roku. Przeanalizowano dziesięć największych branż zarejestrowanych i korzystających z platformy symulacyjnej phishing Keepnet Labs i skomentowano, które rodzaje firm są bardziej zagrożone. Aby udzielić odpowiedzi na pytanie: Jaki jest procent ryzyka według branży? Zmierzyono procent ryzyka według branży i pokazaliśmy je na wykresie. Ponadto ujawniono dlaczego ryzyko pojawiło się w różnych formach w różnych branżach. Ponadto

przeanalizowaliśmy całkowitą liczbę wiadomości e-mail wysłanych między 1 stycznia 2017 r. a 1 stycznia 2018 r. do 86 448 użytkowników w 85 firmach w ciągu roku. Przebadano całkowitą liczbę użytkowników, którzy otworzyli fałszywe wiadomości e-mail (wiadomości phishingowe przygotowane do kampanii symulacyjnych), kliknęli linki w wiadomości e-mail lub nie udzielili odpowiedzi w przypadku symulacji phishingu w ciągu roku. Okazało się, że prawie połowa użytkowników stanowi zagrożenie dla ich firm. Ponadto zbadano pięć największych firm z największą liczbą użytkowników i ich statystyki symulacji phishingu, aby odkryć, jaki jest prosty motyw użytkowników do manipulacji przez inżynierów społecznościowych. Zakodowano firmy jako numery 1, 2, 3, 4 i 5 w celu zachowania anonimowości. Odkryto, że główne instynkty, które skłoniły użytkowników do otwarcia fałszywych wiadomości e-mail ufające fałszywemu nadawcy wiadomości e-mail, a zatem innymi słowy, poczucie zaufania jest nadużywane. Ponadto status użytkownika w zakresie otwierania fałszywych wiadomości e-mail lub klikania fałszywego łącza w wiadomościach e-mail zmienił się w zależności od tematu fałszywych wiadomości e-mail wybranych do symulacji; jeśli użytkownicy byli zainteresowani tematem wiadomości e-mail, są zainteresowani i pochopnie się potknęli.

Co to jest inżynieria społeczna?

Inżynieria ma wiele definicji, które ostatecznie sprowadzają się do sztuki celowego manipulowania zachowaniem przy użyciu specjalnie spreparowanych technik komunikacji. Na przykład SANS opisuje to jako eufemizm dla nietechnicznych lub nisko technologicznych środków, takich jak kłamstwa, podszywanie się, sztuczki, łapówki, szantaż i groźby wykorzystywane do atakowania systemów informatycznych, a socjotechnik to haker, który używa mózgów zamiast komputerówwych . Hakerzy dzwonią do centrów danych i udają klientów, którzy stracili hasło lub pojawiają się w witrynie i po prostu czekają, aż ktoś otworzy przed nimi drzwi.

Inne formy inżynierii społecznej nie są tak oczywiste. Hakerzy znani są z tworzenia telefonicznych witryn internetowych, loterii lub kwestionariuszy, które proszą użytkowników o podanie hasła. Definicje te charakteryzują interakcję z wieloma fazami poprzez użycie kłamstwa, jak również popełnianie niemoralnych czynów w celu zdobycia informacji. Jak ujawnił instytut SANS, istnieje powszechny wzorzec związany z atakami inżynierii społecznej. Ten wzorzec nosi nazwę Cykl, który składa się z czterech faz (gromadzenie informacji, rozwijanie relacji, wykorzystywanie i wykonywanie). Każdy atak inżynierii społecznej jest unikalny, z możliwością, że może obejmować wiele faz / cykli i / lub może obejmować zastosowanie innych bardziej tradycyjnych technik ataku w celu osiągnięcia pożądanego efektu końcowego. Cykl życia inżynierii społecznej można przedstawić na poniższym rysunku w następujący sposób:



Zbieranie informacji

Inżynierowie społeczni mogą wykorzystywać wiele technik do gromadzenia informacji o swoich celach. Kiedy zbierają informacje, mogą je wykorzystać do komunikacji z celem lub kimś ważnym dla powodzenia ataku. Informacje mogą obejmować listę telefonów, daty urodzenia, schemat organizacyjny organizacji i tak dalej.

Rozwijanie relacji

Inżynierowie społeczni mogą skorzystać z zaufania celu, aby nawiązać z nimi bliską i harmonijną relację. Podczas rozwijania tej relacji inżynier społeczny zorganizuje się w szczególny sposób, aby zdobyć zaufanie, z którego następnie w pełni skorzysta.

Eksploatacja

Następnie zaufanym inżynierem społecznym można manipulować celami, aby ujawnić informacje, takie jak hasła, poświadczenia e-mail, informacje bankowe i tak dalej. Ta akcja może być końcem ataku lub początkiem następnego etapu.

Wykonanie

Gdy cel wykona zadanie zlecone przez inżyniera społecznego, cykl jest zakończony.

Dlaczego jest tak skuteczny?

Inżynieria społeczna jest skuteczna, ponieważ jest ukierunkowana na ludzi. Najsłabszym ogniwem w łańcuchu bezpieczeństwa zawsze był element osób ujawniający ważne dane. W erze cyfrowej

komputerów i sieci fałszywe przekonujące wiadomości e-mail, wiadomości i połączenia mogą uprzejmie otworzyć drzwi intruzom. Mimo że są wzmocnione wyrafinowanymi systemami bezpieczeństwa IT, może być łatwo przeniknąć do systemów bezpieczeństwa w nowoczesnym miejscu pracy dzięki różnym technikom inżynierii społecznej. Firmy zdały sobie sprawę, że niektóre z tych zagrożeń kompleksowo oceniły zagrożenia związane z inżynierią społeczną. Jednak wielu uważa, że chodzi o technologię i że tylko hakerzy są prawdziwymi zagrożeniami atakującymi i włamującymi się do systemów, ignorując niewłaściwe korzystanie z Internetu, które ma rzeczywisty potencjał do zniszczenia systemu bezpieczeństwa organizacji i tak dalej. Z uwagi na fakt, że przy fizycznym lub elektronicznym dostępie do dowolnej części systemu użytkownik końcowy niesie poważne zagrożenie bezpieczeństwa. W 2017 r. 50% respondentów ankiety Black Hat wskazało na phishing, exploity w sieciach społecznościowych lub inne formy inżynierii społecznej, w porównaniu z 46% w 2016 r. 45% wymieniło wyrafinowane ataki wymierzone bezpośrednio w organizację z 43% w 2016 r. Oprócz te dwie kategorie zagrożeń były jednak mieszane w swoich obawach - przypadkowe wycieki danych (21%) zajęły trzecie miejsce w kolejności, w porównaniu z 15% w 2016 r., a złośliwe oprogramowanie polimorficzne (20%) zajęło czwarte miejsce, w porównaniu z 15% ostatnimi rok. Respondenci zarejestrowali wyrafinowane, ukierunkowane ataki jako drugą kwestię w ankiecie. Te kluczowe ustalenia pokazują, że dziś jedna z głównych obaw związanych z cyberbezpieczeństwem jest głównie związana z czynnikiem ludzkim. Biorąc pod uwagę fakt, że inżynieria społeczna jest sztuką nakłaniania ludzi do spełniania intencji lub życzeń, ważne jest wzmocnienie najsłabszego ogniwa łańcucha bezpieczeństwa cybernetycznego, elementu ludzkiego, przed wszelkimi atakami inżynierii społecznej. Wiadomości e-mail mogą zawierać złośliwe kody, linki lub załączniki o interesującym temacie, który wzbudzi ciekawość adresatów i zachęci ich do otwarcia. Taki zestaw przypadków jest obecnie prostą metodą inżynierii społecznej. Mimo to, w technikach socjotechniki, można praktykować wiele sposobów, aby kusić nieostrożnych użytkowników od filmów online do fałszywych ostrzeżeń lub porad bezpieczeństwa. W związku z tym wyłączną ochroną lub ochroną przed atakami inżynierii społecznej jest dokładna świadomość i szkolenie. Przyjmując zdroworozsądkowe podejście do bezpieczeństwa cybernetycznego, użytkownicy końcowi mogą wcześnie wykryć możliwe problemy z bezpieczeństwem. Inżynieria społeczna jest tak skuteczna, ponieważ nawet jeśli instytucje mają silne zapory ogniowe, systemy ochrony przed złośliwym oprogramowaniem i wszystkie środki technologiczne w celu zabezpieczenia swoich wrażliwych informacji, element krytyczny, element ludzki, może powodować podatność w dowolnej architekturze bezpieczeństwa. Powody tego są różne: użytkownicy końcowi zwykle mają fałszywe poczucie bezpieczeństwa podczas działań online. Zazwyczaj podejmują ryzyko w Internecie, w przeciwieństwie do ich prawdziwego życia. Cyberprzestępcy używają spreparowanych metod inżynierii społecznej do kontrolowania użytkownika końcowego i znają najłatwiej wejście do danych organizacji i uzyskanie poświadczeń lub wrażliwych danych

Studia przypadków inżynierii społecznej

Studia przypadków inżynierii społecznej są następujące:

Oszustwo na prezesa

Oszustwo dyrektora generalnego ma miejsce, gdy inżynierowie społeczni podszywają się pod kierownictwo firmy i manipulują innymi pracownikami w celu przekazywania nieautoryzowanych finansów lub informacji. Według FBI od stycznia 2015 r. Odnotowano 270% wzrost liczby zidentyfikowanych ofiar oszustw CEO, a 2,3 miliarda USD straciło na oszustwach na CEO. Cyberprzestępcy dokonują ataków phishingowych na kierownictwo i uzyskują dostęp do swojej skrzynki odbiorczej lub wysyłają wiadomości e-mail do pracowników z podobnej nazwy domeny, która zawiera jedną lub dwie litery od prawdziwej nazwy domeny firmy docelowej. W odróżnieniu od tradycyjnych ataków phishingowych, sfałszowane wiadomości e-mail wykorzystywane w oszustwach

CEO rzadko są spamem, ponieważ w atakach oszustów CEO inżynierowie społeczni poświęcają czas na zrozumienie relacji, działań, zainteresowań oraz planów podróży i / lub zakupów organizacji docelowej wiadomości e-mail odpowiednio. Zbierają adresy e-mail pracowników i inne informacje ze strony docelowej, aby wiadomości były bardziej przekonujące. Gdy cyberprzestępcy włamią się do skrzynek odbiorczych swoich celów, przeszukują korespondencję e-mailową, filtrując słowa, które mogą stwierdzić, czy firma rutynowo zajmuje się przelewami, takimi jak faktura, depozyt lub prezes. FBI oszacowało, że organizacje, które padły ofiarą inżynierów społecznych wykorzystujących ataki oszustwa CEO, tracą średnio od 25 000 do 75 000 USD. Jednak niektóre oszustwa na CEO incydenty kosztowały miliony dolarów.

Phishing finansowy

Korzystając z metody phishingu finansowego, inżynierowie społeczni atakują banki lub ich klientów. Dzisiaj pojawiające się trendy, takie jak bankowość internetowa, otwierają przed cyberprzestępcami nowe backdoory. Według FBI, najnowszym trendem wykorzystywanym przez inżynierów społecznościowych jest zdobywanie poświadczeń logowania pracowników za pomocą spamu i wiadomości phishingowych, rejestratorów naciśnięć klawiszy i trojanów dostępu zdalnego. Te techniki ataku zostały zaobserwowane we wrześniu 2012 r., Kiedy Bank of America i Wells Fargo znalazły się wśród atakowanych.

Cyberprzestępcy atakują dziś głównie organizacje finansowe, a prawie połowa wszystkich zarejestrowanych ataków phishingowych ma na celu uzyskanie korzyści finansowych. Bankowe systemy phishingowe są absolutnymi liderami wśród wszystkich rodzajów phishingu finansowego. Dostęp online, a także zapewnienie klientowi łatwego dostępu do jego kont, umożliwił również cyberprzestępcom dostęp do naszych portali bankowych. Przypadki takie jak Carbanak to kolejny przykład phishingu finansowego. Miało to miejsce pod koniec 2014 r., kiedy nastąpił gwałtowny napad na bank, a jego wynikiem było kradzież ponad 1 miliarda dolarów z kont w 100 instytucjach finansowych na całym świecie. Kradzież Carbanak została przeprowadzona przy użyciu standardowych technik phishingowych e-mail, w których zainstalowano złośliwe oprogramowanie zaprojektowane do kradzieży danych logowania i innych danych. Naruszenie JP Morgan w 2014 r. Jest kolejnym przykładem tej udanej metody działania. Naruszenie JP Morgan było jednym z największych naruszeń bankowości wszech czasów, w którym włamano się do 83 milionów kont klientów. Atak z powodzeniem wykradł dane logowania przy użyciu techniki socjotechniki, e-maila typu phishing spear, który był skierowany do znanych użytkowników. Po kradzieży danych uwierzytelniających cyberprzestępcy uzyskali dostęp do serwera JP Morgan i danych ich kont klientów. Ponieważ serwer używał tylko nazwy użytkownika i hasła, aby uzyskać dostęp do systemu, cyberprzestępcom łatwiej było odnieść sukces. Gdyby zaimplementowano uwierzytelnianie dwuskładnikowe, cyberprzestępcy ponieśliby klęskę. Do niemieckiego banku Postbank doszło do masowego ataku phishingowego. W tym przypadku inżynierowie społeczni spreparowali wiadomość e-mail, a strona phishingowa wyglądała bardzo podobnie do legalnej witryny Postbank, dlatego zwykłym użytkownikom trudno było zauważyć, że to w rzeczywistości wyłudzanie informacji. Nieświadomi niczego goście zostali poproszeni o potwierdzenie danych logowania. Po tym, jak użytkownicy podali dane logowania na fałszywej stronie internetowej, cyberprzestępcy uzyskali dane logowania użytkownika w celu kradzieży tożsamości lub sprzedaży informacji. Nieumyślni użytkownicy wiadomości e-mail uwierzyli w ten fałszywy e-mail, ponieważ zawierał on legalne logo oraz podpis. Gdy użytkownicy kliknęli fałszywy link w wiadomości e-mail, zostali przekierowani na fałszywą stronę docelową.

Phishing w mediach społecznościowych

Wyłudzanie informacji jest również rodzajem złośliwej kradzieży tożsamości online, a także uzyskiwania danych logowania lub informacji o koncie poprzez maskowanie się jako renomowany podmiot za pomocą fałszywej lub skradzionej tożsamości. Dlatego użytkownicy mediów społecznościowych stają się jednymi z najłatwiejszych celów dla inżynierów społecznych. Mogą używać linków do fałszywych stron internetowych, które kradną dane logowania i hasła lub inne dane osobowe, lub mogą zbierać rzekomo nieistotne dane osobowe udostępniane niedbale w mediach społecznościowych. Inżynierowie społecznościowi używają fałszywych adresów witryn do manipulowania użytkownikami w celu wprowadzenia ich danych uwierzytelniających.

Gdy nastąpi atak phishingowy na jednego z pracowników, organizacje mogą ucierpieć z powodu naruszenia bezpieczeństwa całej sieci, kradzieży danych lub własności intelektualnej i tak dalej. Co więcej, markę firmy można również zdewaluować, szczególnie gdy cyberprzestępca korzysta z mediów społecznościowych.

Wyłudzanie oprogramowania ransomware

Ransomware to złośliwe oprogramowanie, które blokuje pliki lub ogranicza użytkownikom dostęp do ich systemów komputerowych do momentu zapłaty okupu (pieniędzy). Dzisiejsze ataki ransomware są bardzo złożone i wyrafinowane zagrożenia, a inżynierowie społeczni używają wielu strategii do rozprzestrzeniania ransomware. Najpopularniejsze metody to wiadomości e-mail spam, media reklamowe i zestawy exploitów. Inżynierowie społeczni z powodzeniem zainfekowali Hollywood Presbyterian Medical Center , systemy komputerowe z oprogramowaniem ransomware. Gdy pracownik otworzył dokument, który wyglądał jak faktura szpitalna (był to program phishingowy), szybko rozprzestrzenił się w systemie i zlikwidował całą sieć szpitalną. Sieć szpitali nie działała przez ponad tydzień. Przykład ransomware znajduje się na poprzednim zrzucie ekranu, a mianowicie VirLock Ransomware, który jest prawdopodobnie jednym z najgorszych rodzajów złośliwego oprogramowania w kategorii trojanów ransomware. Blokuje komputer, uniemożliwiając korzystanie z niego. Następnie wymaga zapłaty, aby odblokować system / pliki.

Phishing Bitcoin

Cyfrowe kryptowaluty, takie jak Bitcoin, są zagrożone cyberatakami. Poważne cyberataki są organizowane na kontach tych, którzy korzystają z cyfrowych pieniędzy, co już się stało bardzo popularne. Pieniądze kryptograficzne stały się obecnie jednym z najczęściej omawianych narzędzi inwestycyjnych. Nawet zwykli ludzie używają teraz kryptowalut jako narzędzia inwestycyjnego zamiast złota, wymiany walut i odsetek. Chociaż niektóre rynki kryptowalut, takie jak Dash (Dash), Ethereum (ETH), Ripple (XRP), Litecoin (LTC) i IOTA (MIOTA) były na rynku, Bitcoin był na szczycie i został opracowany przy użyciu technologii blockchain . Wartości bitcoinów znacznie wzrosły, zwiększając się o 250-250% w ciągu jednego roku. Ale ten skok wzbudził apetyt hakerów. Cyberprzestępcy używający różnych metod inżynierii społecznej i ataków phishingowych poszukują korzyści materialnych.

Studium przypadku inżynierii społecznej - symulacja phishingu w laboratoriach Keepnet

Cyberprzestępcy znają wiele drzwi do otwarcia na wiele innych rodzajów ataków lub wykorzystania luk w zabezpieczeniach. Dlatego jako podejście oparte na rolach do edukacji uświadamiającej w zakresie bezpieczeństwa, symulacje i szkolenia phishingowe są ważne dla każdej organizacji, która będzie integralną częścią ogólnych programów edukacyjnych i szkoleniowych dotyczących świadomości bezpieczeństwa. Symulacja phishingu może pomóc organizacjom w zapewnieniu właściwego szkolenia właściwym osobom we właściwym czasie, biorąc pod uwagę, że dzięki phishingowi koledzy lub pracownicy stali się słabym ogniwem w łańcuchu bezpieczeństwa cybernetycznego. Symulacja phishingowa Keepnet Labs jest ważna, ponieważ zasadniczo wybrała element ludzki jako linię bazową.

Keepnet Labs to firma zajmująca się podnoszeniem świadomości w zakresie cyberbezpieczeństwa, która opracowała pakiet produktów w zakresie świadomości i obrony w zakresie bezpieczeństwa cybernetycznego. Obejmuje holistyczne podejście do ludzi, procesów i technologii w celu zmniejszenia ryzyka cybernetycznego. Jego celem jest przede wszystkim zwiększenie świadomości na temat ataków z zakresu inżynierii społecznej, pomagając im w rozwijaniu umiejętności i wiedzy.

Analiza dziesięciu najlepszych branż

Przeanalizowano dziesięć największych branż zarejestrowanych i korzystających z platformy symulacyjnej phishing Keepnet Labs, a także skomentowano, które rodzaje firm są bardziej zagrożone. Aby uzyskać odpowiedź na pytanie: Jaki jest procent ryzyka według branży? Zmierzono procent ryzyka według branży i pokazano je w tabeli. Ponadto ujawnilono, dlaczego ryzyko pojawiło się w różnych formach w różnych branżach. Kampanie phishingowe były przeprowadzane w firmach od 1 stycznia 2017 r. do 1 stycznia 2018 r. Obserwowano te same zmienne (firmy, działy i użytkowników / osoby) w ciągu jednego roku i uzyskano dane. W tym badaniu śledzono te same firmy zarejestrowane w platformie symulacyjnej phishing Keepnet Labs i obserwowanomy różne fazy ataków socjotechnicznych oraz ich wyniki dla użytkowników. W wyniku tego stworzyliśmy tabelę ryzyka dla branż i ujawniliśmy, które branże były bardziej zagrożone.

Ze względu na firmy należące do różnych branż na platformie postanowilono pokazać dziesięć największych firm zagrożonych. Dziesięć najbardziej narażonych kategorii biznesowych obejmowało odpowiednio technologię, usługi finansowe, produkcję, energię, edukację, transport, nieruchomości, doradztwo i sektor oprogramowania, sprzedaż detaliczną i hurtową. Firmy technologiczne są bardziej narażone na ryzyko z różnych powodów. Jednym z oczywistych powodów jest to, że firmy te mają bardzo cenne informacje do kradzieży, a także charakter samych organizacji technicznych. Pracownicy firm technologicznych zazwyczaj lepiej stosują nowe technologie, chętnie też widzą nowe oprogramowanie lub aplikacje, co czyni je szczególnie podatnymi na ataki i exploity. Pomimo tego, że pracownicy firm technologicznych lepiej rozumieją ryzyko płynące z Internetu, byli pierwszymi na liście osób najbardziej oszukanych przez systemy inżynierii społecznej. Powodem tego jest, w przeciwieństwie do innych branż, fakt, że prawie wszyscy pracownicy firm technologicznych używają komputerów, systemów i różnych narzędzi jako codziennej rutyny łączącej ich z Internetem. Są bardziej podatni na zagrożenia z powodu intensywnego obciążenia Internetu i charakteru wykonywanej pracy. Ponadto inżynierowie społeczni mają więcej programów do manipulowania pracownikami firm technologicznych niż w przypadku innych firm. Jest to również kolejny powód, dla którego firmy technologiczne znajdują się na szczycie listy. Firmy finansowe są prawie tak samo zagrożone jak firmy technologiczne. Pomimo tego, że wielu pracowników usług finansowych zdaje sobie sprawę z ataków phishingowych lub innych socjotechniki, nadal, zgodnie z wynikami symulacji przeprowadzonych w ciągu jednego roku, są drugą branżą, która jest najbardziej zagrożona. Ponieważ, podobnie jak w przypadku firm technologicznych, istnieje tak wiele systemów inżynierii społecznej dla sektora bankowego lub finansowego, aby manipulować wyszkolonym i dobrze świadomym pracownikiem. Jeśli celem phishingu jest podszywanie się pod zarząd, łatwiej jest manipulować pracownikami. Innym powodem, dla którego usługi finansowe są zagrożone, jest to, że mają wielu pracowników. Na przykład, prywatny bank zarejestrowany na platformie symulacyjnej phishing Keepnet ma codziennie ponad 15 000 pracowników pracujących na komputerach. Awaria tylko jednego pracownika może spowodować poważną katastrofę dla całego systemu. W świetle tych statystyk, biorąc pod uwagę czynnik ryzyka, można stwierdzić, że usługi finansowe są najbardziej ryzykownymi przedsiębiorstwami w rzeczywistości, biorąc pod uwagę fakt, że cyberprzestępcy wolą przede wszystkim atakować firmy finansowe. Niemniej jednak symulacje wykonane na tej platformie były przeprowadzane w określonych odstępach czasu w zaplanowany sposób. W rzeczywistości wielu cyberprzestępców może

atakować wieloma scenariuszami w tej samej instytucji finansowej w celu uzyskania korzyści finansowych. W każdym razie najbardziej ryzykownymi branżami są usługi finansowe, gdy uwzględniamy czynnik cyberprzestępczości na scenie. Jeśli chodzi o sektory produkcyjny, energetyczny, edukacyjny, transportowy, nieruchomości, doradztwa i oprogramowania, a także sektory handlu detalicznego i hurtowego, wszystkie są bardzo zagrożone; jednak w porównaniu z technologią i usługami finansowymi częściowo znajdują się w lepszej sytuacji, co wynika z charakteru ich pracy i codziennej działalności. Jednak gdy analizujemy roczny proces symulacji phishingu, widok reakcji największych firm ujawnił prawdziwe zagrożenie.

Badanie wszystkich wiadomości e-mail wysłanych w ciągu jednego roku

Na tej platformie ponad sto firm przeprowadziło symulacje phishingu; w ciągu roku przeanalizowano jednak 126 firm. Wiadomości e-mail zostały wysłane do 126 000 użytkowników między 1 stycznia 2017 r. a 1 stycznia 2018 r. Odsetek użytkowników, którzy otworzyli fałszywe wiadomości e-mail (wiadomości phishingowe przygotowane do kampanii symulacyjnych) wyniósł 48,2% całkowitej liczby użytkowników zarejestrowanych w symulacji phishingowej Keepnet Lab w ciągu roku. Statystyki te wskazują na zagrożenia, z jakimi mogą się zmagać firmy, ponieważ ponad połowa pracowników otworzyła wiadomości e-mail typu phishing. Przyczyną tych słabych wyników są nieumyślne błędy, ponieważ użytkownicy celowo reagują na wiadomości e-mail typu phishing i działania powodujące to:

* Poślizg: Częste działanie, wymagające niewielkiej świadomej uwagi, coś idzie nie tak

* Pomyłka: Określone działanie zostało pominięte, ponieważ zostało zapomniane

* Błąd oparty na regułach: przestrzegana jest procedura, ale niewłaściwie stosowany jest dobry proces lub stosowana jest zła zasada

* Błąd oparty na wiedzy: procedura nie jest dostępna, a zastosowanie wiedzy i doświadczenia nie jest wystarczające, aby bezpiecznie wykonać działanie

Niemniej jednak, biorąc pod uwagę metody inżynierii społecznej, to właśnie ze względu na konsekwencje przypadkowych błędów wiele firm padło ofiarą cyberataków. Cyberprzestępcy stosują taktykę inżynierii społecznej, aby wykorzystać nieświadomość ludzi lub ich naturalną ludzką skłonność do krzątania się, aby nakłonić ich do szybkiego działania. Co więcej, w operacjach online pracownicy zwykle mają fałszywe poczucie bezpieczeństwa. Ponadto odsetek użytkowników, którzy kliknęli łącze w wiadomościach e-mail dotyczących symulacji, wynosił 31,5% całkowitej liczby użytkowników zarejestrowanych na platformie symulacyjnej phishing Keepnet Labs. Ta statystyka ujawniła, że 16,7% użytkowników otworzyło fałszywe e-maile, ale nie kliknęli linków, co jest kolejnym powodem dużej liczby kliknięć użytkowników zakorzenionych w szablonach phishingowych i tematach phishingowych. Kierownictwo firm wybrało dla nich treść phishingową a ponieważ wiedzieli, że pracownicy nie mają wiedzy na temat najlepszych praktyk w zakresie bezpieczeństwa cybernetycznego, zredagowali e-mail phishingowy zgodnie z życzeniem, aby uczynić go bardziej realnym, myśląc tak, jak robi to inżynier społeczny. W rzeczywistości obecnie 91% udanych ataków to spear phishing, kiedy cyberprzestępcy zbierają informacje o swoich celach i wytwarzają fałszywe e-maile, aby ich zwabić. W świetle tych ustaleń widzimy, że firmy są bardzo zagrożone. Ponieważ w prawdziwym życiu link albo prowadzi użytkowników do fałszywej witryny, która wygląda na prawdziwą i prosi o zalogowanie się przy użyciu nazwy użytkownika i hasła, lub może przekierowywać pracowników do witryny, która infekuje całe systemy komputerowe złośliwym oprogramowaniem, takim jak ransomware lub keylogger, a nawet może pobrać wirusa bezpośrednio, bez wchodzenia na stronę internetową. Ponadto w symulacjach phishingowych odsetek użytkowników, którzy przesłali formularz po kliknięciu linków w wiadomościach e-mail, wyniósł 7,9. % wszystkich użytkowników. Pomimo bardzo dużej liczby

użytkowników klikających łącza w wiadomościach e-mail, wskaźnik ten spadł, gdy użytkownicy zostali przekierowani na inną stronę w celu wprowadzenia swoich danych uwierzytelniających. Niezależnie od tego, 7,9. Stosunek procentowy jest niski w porównaniu do 31,5% klikania wiadomości e-mail, nadal stanowi duże zagrożenie dla firm. W prawdziwych przypadkach, gdy nawet jeden pracownik podaje hasło, cyberprzestępcy mogą stanowić zagrożenie dla wszystkich systemów. Mogą podszywać się pod dyrektorów generalnych lub personel wysokiego szczebla, aby manipulować innymi użytkownikami. The Yahoo! może być dobrym tego przykładem.

Ocena ataków socjotechnicznych na pięć firm z największą liczbą użytkowników Przeanalizowaliśmy pięć największych firm z największą liczbą użytkowników należących do różnych branż i uzyskaliśmy dostęp do ich statystyk phishingowych na podstawie otwartych wiadomości e-mail, klikniętych łączy w wiadomościach e-mail, przesłanych formularze, otwarte załączniki, reporter phishingowy i odsetek braku odpowiedzi.

Firmy zostały wybrane zgodnie z liczbą ich użytkowników; w związku z tym zbadano firmy z pięcioma największymi użytkownikami. Zakodowao firmy, aby nie podawać wyraźnie ich nazw. W związku z tym, aby celowo ich nie sprecyzować, zakodowaliśmy je jako numery 1, 2, 3, 4 i 5.

Firma numer 1: Podczas analizy statystyk phishingowych naszej pierwszej firmy, numer 1, firmy finansowej z ponad 15 000 użytkowników . Liczba otwartych wiadomości e-mail, kliknięte łącza w wiadomościach e-mail, przesłane formularze, otwarte załączniki, reporterzy phishingowi i brak odpowiedzi wskazują na podatność pracowników systemu na zagrożenia związane z inżynierią społeczną. Pomimo faktu, że większość użytkowników ma wykształcenie i jest dobrymi użytkownikami komputerów, 4 198 wszystkich użytkowników otworzyło fałszywą wiadomość e-mail, zatytułowaną Zmień hasło. Jak stwierdzonona początku tego badania, inżynierowie społeczni stosują proste metody. Wykorzystują poczucie zaufania. W tych ramach wiadomość e-mail „Zmień swoje hasło" nie wzbudziła podejrzeń u prawie 30% użytkowników. Wielu użytkowników zaufało źródłu wiadomości e-mail. Poza tym 5,1% użytkowników (791 wszystkich użytkowników) przekazało nawet dane logowania na fałszywych stronach phishingowych. W takiej instytucji finansowej, nawet jeśli tylko jedna osoba poda swoje dane uwierzytelniające, może powodować poważne kryzysy, ponieważ inżynierowie społeczni są w stanie uzyskać informacje o innych pracownikach za pomocą prostych metod, wykorzystując informacje, które już uzyskali. Interesujące jest również ujawnienie, że żaden z użytkowników nie zgłosił tego e-maila jako phishing. Większość użytkowników wolała nie podejmować żadnych działań zamiast zgłaszać phishing. To kolejna kwestia - brak dobrych nawyków bezpieczeństwa online dla bardzo dużej firmy finansowej. Podczas gdy reporterzy phishingowi dostarczaliby zespoły SOC do terminowej identyfikacji zagrożeń i blokowali ataki użytkowników na szkodliwe wiadomości e-mail:

Firma 2: Jeśli chodzi o numer 2, firma technologiczna, która korzystała z symulatora phishing firmy Keepnet Labs, i nie wykazuje innej sytuacji niż poprzednia firma finansowa, ujawniając zawrotne wyniki. Nasz argument w tym badaniu sugeruje, że inżynierowie społeczni stosują proste metody, takie jak poczucie zaufania, które ponownie sprawdziło się w tym przypadku. E-mail phishingowy został wysłany do 1569 użytkowników numeru 2, zatytułowanych Przełącz do programu Outlook nowej generacji. W tym fałszywym e-mailu użytkownicy zostali poproszeni o kliknięcie linku, aby pobrać nowe wersje programu Outlook. Wiadomość e-mail została wysłana tak, jakby została wysłana przez ich firmę. Czujni i świadomi użytkownicy zrozumieli, że to fałszywy e-mail, gdy sprawdzili link, a 585 użytkowników z 1569, czyli 37,3% wszystkich użytkowników, nie odpowiedziało. Najbardziej niebezpieczna sytuacja polega na tym, że znaczna liczba użytkowników wprowadziła swoją nazwę użytkownika i hasło w fałszywej witrynie, która jest kierowana przez fałszywą pocztę. Liczba osób, które kliknęły link w wiadomościach e-mail, wyniosła 659, czyli 42% wszystkich użytkowników, a liczba osób, które przesłały swoje nazwy użytkowników i hasła, wyniosła 598, czyli 38,1% wszystkich użytkowników.

Ponadto liczba osób, które tylko otwarło wiadomości e-mail stanowiły 324, czyli 20,7% wszystkich użytkowników

* Firma numer 3: Widzimy, że ryzyko związane z numerem 3 również jest ogromne. Większość użytkowników uwierzyła i zaufała źródłu wiadomości e-mail, nie sprawdzając go ani nie weryfikując. Numer 3 to kolejna firma technologiczna, która używa symulatora phishing firmy Keepnet Labs. Podczas symulacji wiadomości phishingowe zostały wysłane do 344 osób. Tematy wiadomości e-mail związanych z phishingiem dotyczyły kont WhatsApp użytkowników, zgłaszając, że dostęp do ich kont uzyskano z różnych lokalizacji, co zirytowało znaczną liczbę pracowników. Pomimo tego, że firma numer 3 jest firmą technologiczną, a jej użytkownicy to osoby, które dobrze wiedzą, co zrobić z atakami cybernetycznymi lub atakami inżynierii społecznej, nadal ujawniono, że 1,2% użytkowników podało swoje dane uwierzytelniające. Liczba użytkowników, którzy otworzyli wiadomości e-mail, wynosiła 19, czyli 5,5% wszystkich użytkowników. Liczba użytkowników, którzy kliknęli link w wiadomościach e-mail, wyniosła 12, czyli 3,5% wszystkich użytkowników. Biorąc pod uwagę te statystyki, ujawniono problemy, które mogą powodować inżynierowie społeczni, a nawet firma zajmująca się bezpieczeństwem technologicznym może stać się ofiarą inżynierów społecznościowych, którzy wytwarzają swoje fałszywe wiadomości e-mail za pomocą logo, spraw i alertów, które powodują, że użytkownicy działają bez myślenia o sytuacji . Ponadto żaden z użytkowników nie zgłosił tego e-maila jako phishing. 325 użytkowników, co stanowiło 94,5% wszystkich użytkowników, wolało nie robić nic, niż klikać narzędzie do raportowania i analizy phishingu Keepnet Labs. Mimo że numer 3 był lepszy w porównaniu z pozostałymi czterema firmami, statystyki te nadal stanowią poważne zagrożenie dla firmy, ponieważ firma jest tak silna, jak jej najsłabsza część. Ten fałszywy e-mail umożliwił naturalnemu użytkownikowi zmartwienie i pilne zrobienie czegoś, aby rozwiązać problem w jego wiadomości, umożliwiając osobom działanie bez zastanowienia i zaufanie do źródła wiadomości e-mail. Mimo że są to osoby świadome, znaczna ich liczba łatwo wpadła w tę pułapkę. To kolejna wskazówka, która potwierdziła naszą hipotezę, że proste taktyki inżynierii społecznej są skuteczne, ponieważ żerują na zaufaniu.

* Firma numer 4: Jeśli chodzi o numer 4, jest to uniwersytet, który wykorzystał symulator phishingowy Keepnet Labs do oceny działań swoich pracowników wobec wiadomości phishingowych. Wykorzystali wcześniej istniejący szablon wiadomości e-mail phishingowej kampanii świątecznej i wysłali fałszywe wiadomości e-mail do 1 286 pracowników, w tym pracowników naukowych, oficerów, księgowych i tak dalej. Powszechnie wiadomo, że nawet 1% niepowodzeń w atakach inżynierii społecznej może powodować ogromne kłopoty i konsekwencje. Użytkownicy pod numerem 4 również wykazywali nieskuteczne wyniki, ponieważ aż 38 pracowników podało swoje dane uwierzytelniające, co stanowiło 3% wszystkich użytkowników. 376 użytkowników, 29,2% wszystkich użytkowników, otworzyło e-maile, 178 użytkowników, czyli 13,8% wszystkich użytkowników kliknęło link phishingowy w wiadomości e-mail. Ponownie żaden z użytkowników nie zgłosił podejrzanych e-maili do reporterów phishingowych. Liczba osób, które nie udzieliły odpowiedzi, wyniosła 910 (70,8 wszystkich użytkowników). W tym badaniu stwierdziliśmy, że sukces lub porażka użytkowników w zakresie bezpieczeństwa cybernetycznego zależy od schematów inżynierów społecznych, czyli ich wyboru tematów phishingowych. Kiedy inżynierowie społecznościowi zdobywają zaufanie użytkowników, odnoszą sukcesy. Na przykład wysłaliśmy kolejną symulację phishingu na numer 4 do tych samych użytkowników, tydzień później, zmieniają temat phishingu na Przełącz na Outlook następnej generacji, w którym okazało się, że wyniki były znacznie gorsze: Tym razem liczba użytkowników, którzy przesłali formularze phishingowe, wyniosła 338, prawie dziewięć razy więcej niż w poprzedniej symulacji. 518 użytkowników, czyli 40,3% wszystkich użytkowników, otworzyło wiadomości e-mail i 419 użytkowników, czyli 32,6% wszystkich użytkowników kliknęło link phishingowy w wiadomościach e-mail. Liczba osób, które nie udzieliły odpowiedzi, wyniosła 768, czyli 59,7% wszystkich użytkowników. Ponownie żaden z użytkowników nie zgłosił podejrzanych e-maili do reporterów phishingowych. Kiedy

porównujemy różne symulacje phishingowe wykonane dla tych samych osób po tygodniu, użytkownicy wzięli drugą symulację poważniej, ponieważ podszywali się pod menedżerów lub osoby odpowiedzialne. Ta symulacja odniosła większy sukces w oszukiwaniu użytkowników, ponieważ instynktownie słuchali swoich przełożonych lub bezsprzecznie wymagań kierowanych przez personel i ufali przełożonym. Jeśli chodzi o poprzednią symulację, użytkownicy zainteresowani wakacjami stali się surową krewetką dzięki fałszywemu e-mailowi.

* Firma numer 5: Nasz ostatni przypadek to numer 5, ważna firma tekstylna, która stanowi znaczną część sprzedaży w Internecie. Kampanie phishingowe zostały zainicjowane dla 1009 użytkowników. Tematy phishingowe zostały wybrane przez decydentów pod numerem 5. Przełącz na następną generację Wiadomości e-mail programu Outlookm zostały wysłane do pracowników, jednak, podobnie jak w innych przypadkach, wyniki były rozczarowujące, tak że 50% użytkowników lub 504 osób dało ich dane uwierzytelniające do fałszywych stron. Liczba użytkowników, którzy otworzyli wiadomości e-mail, wyniosła 625, czyli 69,1% wszystkich użytkowników. Liczba użytkowników, którzy kliknęli linki w wiadomości e-mail, wyniosła 545, czyli 54% wszystkich użytkowników. Biorąc pod uwagę te statystyki, jeśli symulacja wyłudzania informacji byłaby prawdziwa, konsekwencje spowodowałyby sprzeciw wobec firmy wśród jej klientów, ponieważ cyberprzestępcy mogliby przejąć informacje o kartach kredytowych klientów. Ponadto żaden z użytkowników nie zgłosił tego e-maila jako phishingu, jak w pozostałych czterech przypadkach. 384 użytkowników, co stanowiło 38,1% wszystkich użytkowników, wolało nic nie robić, niż zgłaszać phishing.

Porady

Wskazówki dotyczące rzeczywistych przypadków są następujące:

* Wszystkie przypadki, które zostały omówione, są prawdziwe. Najlepszą wskazówką dla tej części będzie przestanie klikać.

* Jeśli uważasz, że jesteś ofiarą możliwego ataku socjotechniki w Twojej organizacji, zgłoś to jak najszybciej odpowiednim osobom w organizacji, w tym administratorom sieci. Mogą być czujni na wszelkie podejrzane lub nietypowe działania.

* Jeśli uważasz, że Twoje konta finansowe zostały naruszone, natychmiast zadzwoń do instytucji finansowej i zamknij wszystkie konta, które mogły zostać naruszone, i oczywiście uważnie obserwuj wyciągi.

* Jeśli masz wrażenie, że ktoś szuka informacji, których nie powinien, przerwij rozmowę.

Podsumowanie

Ponieważ jest to sztuka manipulowania zachowaniem przy użyciu specjalnie spreparowanych technik komunikacyjnych, inżynieria społeczna żeruje na ludzkiej słabości, nakłaniając ludzi do dostarczania wrażliwych informacji. Ponieważ łatwiej jest manipulować jednostkami niż hakować systemy komputerowe, cyberprzestępcy stosują taktykę socjotechniki. W tym badaniu zdefiniowaliśmy, w jaki sposób cykl ataku inżynierii społecznej składa się z czterech etapów gromadzenia informacji, rozwijania relacji, - wykorzystywania i wykonywania. Ujawniliśmy również, że inżynieria społeczna jest tak skuteczna, ponieważ wykorzystuje naturę ludzką, w odniesieniu do statystyk w Black Hat Survey 2017. Ponadto studia przypadków inżynierii społecznej, takie jak oszustwa CEO, phishing finansowy, phishing w mediach społecznościowych, phishing ransomware i Phishing bitcoinami został zbadany. Ponadto przeanalizowaliśmy 10 największych branż zarejestrowanych i korzystających z platformy symulacyjnej phishing Keepnet Labs i skomentowaliśmy, które rodzaje firm są bardziej zagrożone. Aby odpowiedzieć

na pytanie: Jaki jest procent ryzyka według branży? Zmierzyliśmy procent ryzyka według branży. Ponadto ujawniliśmy, dlaczego ryzyko pojawiło się w różnych formach w różnych branżach.