Zbieranie informacji

Atak socjotechniki podąża ścieżką, do której doszedł po ocenie informacji znanych o celu. Dlatego taktyki wyuczone w poprzednich częściach zostaną zastosowane w zależności od wyników tej części. Jednak gromadzenie informacji nie jest tak trudne, jak kilka lat temu, kiedy można było uzyskać szczegółowe informacje na temat celu albo bezpośrednio z celu, albo z pytania. Internet, a dokładniej korzystanie z mediów społecznościowych, uprościł ten etap dzięki nowszym i szybszym technikom gromadzenia danych. W procesie gromadzenia danych żadna część danych nie jest uważana za nieistotną. Wystarczy odrobina informacji, takich jak ulubiony staw celu, aby inżynierowi społecznemu udało się przekonać cel do działania w określony sposób. Ważne jest, aby inżynier społeczny wiedział, jakiego rodzaju informacji szukać. Istnieje przeciążenie informacją i może zostać zebranych wiele nieistotnych informacji. Dobrze jest również znać źródła, w których można znaleźć tego rodzaju informacje. Posiadanie informacji nie jest wystarczające, ważne jest, aby wiedzieć, jak wykorzystać zebrane informacje do profilowania celu i uczynienia ich bardziej przewidywalnymi. Wreszcie, ważne jest, aby wiedzieć, jak przechowywać te informacje w uporządkowany sposób, aby ułatwić ich wyszukiwanie. W tej części dowiesz się, jak to zrobić w następujących sekcjach:

* Zbieranie informacji o celach

* Techniczne i nietechniczne metody gromadzenia informacji

Wprowadzenie

Istnieje mnóstwo dostępnych i tworzonych dziś informacji. Wraz z pojawieniem się Internetu i pojawieniem się platform mediów społecznościowych szacuje się, że ludzie tworzą 2,5-quillillion bajtów danych. Informacje te są wykorzystywane przez wiele grup ludzi, marketingowcy są na szczycie łańcucha. Duże zbiory danych pozwalają organizacjom wydobywać znaczące informacje z tej niesamowitej ilości danych, które w przeciwnym razie zostałyby zmarnowane. Reklamodawcy znają dziś lepiej swoje cele, ponieważ profilowali je na podstawie informacji dostępnych w Internecie. Po 13 latach od założenia Facebook stał się już miesięczną bazą aktywnych użytkowników obejmującą ponad dwa miliardy ludzi. Instagram i Twitter łącznie mają prawie miliard aktywnych użytkowników miesięcznie. LinkedIn, który został niedawno przejęty przez Microsoft, ma około 106 milionów aktywnych użytkowników miesięcznie. Jest to interesująca platforma dla inżyniera społecznościowego, która jest specjalnie ukierunkowana na pracowników, ponieważ została stworzona dla profesjonalnej bazy użytkowników. Snapchat to kolejna nadchodząca platforma mediów społecznościowych, która codziennie przyciąga ponad 160 milionów użytkowników. Baza użytkowników tych platform może być większa niż te liczby, ale najważniejsza jest faktyczna liczba aktywnych użytkowników każdego miesiąca lub dnia. Są to generatory treści, czyli te, które wypuszczają treści, które powodują, że inni użytkownicy odwiedzają te platformy, i nadal są konsumentami treści przez innych użytkowników. Użytkownicy są wyjątkowo nieostrożni, jeśli chodzi o informacje, które umieszczają na swoich kontach w mediach społecznościowych. Ich biograficzne strony są pełne często poprawnych informacji o sobie i ich rodzinach. Pełna historia ich życia, w tym daty urodzenia, uczęszczane szkoły, relacje i historia pracy, można znaleźć na ich stronach profilowych. Regularnie aktualizują swoje konta o informacje, które można uznać za wrażliwe, takie jak miejsca, w których pracują, wyjazdy wakacyjne, w których przebywają, wydarzenia w miejscu pracy, bliscy przyjaciele i członkowie rodziny. Nic więc dziwnego, że inżynierowie społeczni czają się na platformach mediów społecznościowych, aby zbierać informacje o swoich celach. Jednak inżynierowie społeczni nadal korzystają ze starych zaufanych metod uzyskiwania informacji o swoich celach. Z biegiem lat udoskonalili taktykę, aby odnieść sukces w uzyskiwaniu informacji przy użyciu tych starych metod. Chociaż mogą nie być tak szybkie jak media społecznościowe, czasami są bardziej osobiste i dlatego mogą dostarczyć więcej informacji.

Zbieranie informacji o celach

Gromadzenie informacji można przeprowadzić za pomocą dwóch ogólnych kategorii metod - metod technicznych i nietechnicznych. Jak sama nazwa wskazuje, metody techniczne są oparte na komputerowych technikach zbierania informacji. Nie ma jednak pewności, że dane narzędzie lub urządzenie elektroniczne uzyska wystarczające informacje o celu. Dlatego do zebrania informacji o obiektach docelowych można użyć kombinacji następujących narzędzi i urządzeń. Inżynierowie społeczni wykorzystają wiele narzędzi / technik służących do zbierania informacji i połączą uzyskane informacje, aby stworzyć profil dla swoich celów.

Techniczne metody gromadzenia informacji

Obecnie opracowywanych jest wiele narzędzi służących do gromadzenia informacji podczas ataków socjotechnicznych. Prawdopodobnie najbardziej udanym narzędziem do tego jest Linux Distribution o nazwie Kali. Zawiera pakiet ponad 300 narzędzi specjalnie zaprojektowanych przez Kali do zbierania informacji o celu. Od 300 zawęźmy je do dwóch najpopularniejszych narzędzi, które wyróżniają się na liście, ponieważ nie zbierają danych, ale pomagają w ich przechowywaniu i wyszukiwaniu. Są to:

BasKet

BasKet to darmowy i otwarty program Linux, który działa bardziej jak zaawansowane narzędzie do przechowywania danych, aby pomóc inżynierowi społecznemu w procesie gromadzenia danych. Ma znajomy wygląd Notatnika, ale ma wiele funkcji. Służy jako repozytorium informacji tekstowych i graficznych, które inżynier społeczny gromadzi w określonym celu. Może wydawać się prosty lub nawet niepotrzebny podczas ataku inżynierii społecznej, ale w rzeczywistości służy celowi, który trudno jest powielić w edytorach tekstu, takich jak Microsoft Word. BasKet używa układu przypominającego tabulatory, aby umożliwić inżynierowi społecznościowemu umieszczanie każdego rodzaju informacji o celu w uporządkowany sposób, który jest łatwy do odczytania lub odzyskania. Na przykład zdjęcia mogą znajdować się na jednej karcie, informacje kontaktowe w innej, informacje w mediach społecznościowych na trzeciej, a informacje o fizycznej lokalizacji w osobnej. Inżynier społeczny będzie aktualizował te karty, ilekroć napotka więcej informacji. Pod koniec procesu BasKet pozwala inżynierowi społecznościowemu wyeksportować te informacje jako stronę HTML, dzięki czemu kompresuje wszystkie informacje razem, czyniąc je bardziej przenośnymi, dostępnymi i udostępnianymi.

Dradis

Dradis to darmowa i otwarta aplikacja Linux, Windows i macOS do przechowywania informacji. Ma bardziej zaawansowany wygląd, który ma wygląd podobny do notatnika BasKet. Dradis jest również bardziej zaawansowany pod względem funkcjonalności, ponieważ działa jako scentralizowane repozytorium i korzysta z internetowego interfejsu użytkownika, aby umożliwić użytkownikom interakcję z nim. Zamiast kart (takich jak BasKet), Dradis używa gałęzi, które pozwalają użytkownikowi dodawać różne rodzaje informacji razem. Dradis może obsługiwać ogromne ilości danych, które w innym przypadku byłyby problematyczne dla BasKet. Dlatego jest powszechnie stosowany, gdy istnieje wiele informacji, które mają zostać posortowane według celu. Po zakończeniu korzystania z dwóch głównych narzędzi do przechowywania danych, nadszedł czas, aby przyjrzeć się sposobom gromadzenia informacji przez inżynierów społecznych. Poniżej omówiono:

Strony internetowe

Jednym z uli zawierających informacje o celach są korporacyjne i osobiste strony internetowe. Witryny firmowe mogą zawierać informacje o ich pracownikach i klientach. Z drugiej strony prywatne strony

internetowe zawierają informacje wyłącznie o osobach fizycznych. Przy wystarczającym przekopywaniu strony internetowe mogą być w stanie ujawnić wiele informacji. Prywatne strony internetowe mogą informować o zaangażowaniu danej osoby pod względem pracy, fizycznej lokalizacji, danych kontaktowych i niektórych słów specjalnych, które mogą być użyte w profilowaniu haseł. Jeśli chodzi o ostatni punkt, wiadomo, że ze względu na znajomość ludzie zwykle zawierają pewne znane im frazy lub słowa, takie jak data urodzenia, imię partnera, imię zwierzaka lub własne imiona. Korporacyjne strony internetowe są w stanie dostarczyć biografie swoich pracowników, szczególnie tych o wysokich stanowiskach oraz dane kontaktowe do pracy. Jeśli chcesz atakować organizację za pomocą złośliwego załącznika e-mail, wysłanie jej na adresy e-mail podane w korporacyjnej witrynie internetowej ma większą szansę na dostarczenie ładunku bezpośrednio w organizacji.

Wyszukiwarki

Mówi się, że internet nigdy nie zapomina. Jeśli chcesz coś wiedzieć, znajomość właściwego sposobu zapytania może dać ci prawie wszystkie potrzebne informacje. Google, dominująca wyszukiwarka, jest kluczowym narzędziem dla inżyniera społecznościowego, służącym do odkrywania informacji o celach w Internecie. Omówimy niektóre wyszukiwane frazy, których używają inżynierowie społeczni, aby szukać informacji o celach za pomocą Google: Aby wyszukać informacje o celu. w ramach określonej domeny, takiej jak witryna firmowa, można zastosować następujące zapytanie:

Site: www.websitename.com „John Doe”

Jeśli w witrynie znajduje się coś na temat Johna Doe, Google zindeksuje ją w wynikach wyszukiwania zapytania. Aby wyszukać informacje o celu w tytule dowolnej witryny zaindeksowanej przez Google, używane jest następujące zapytanie:

Intitle: John Doe

Ważne jest, aby zrozumieć, że odstępy między tymi dwoma słowami instruują Google, aby szukał także tytułów z Johnem, a po nich następuje tekst zawierający słowo Doe. Jest to bardzo przydatne zapytanie, ponieważ przechwytuje informacje o celu zawarte w tytułach wielu stron internetowych. To zapytanie dostarczy informacji z witryn korporacyjnych do platform mediów społecznościowych, ponieważ często używają nazwiska osoby jako tytułu na niektórych stronach.

Aby wyszukać informacje o celu w 3. adresie URL dowolnej witryny, Google może dostarczyć następujące zapytanie:

Inurl: John Doe

W wielu organizacjach powszechną praktyką jest używanie słów w tytułach internetowych w adresach URL do celów SEO. To zapytanie identyfikuje nazwisko osoby na podstawie adresów URL indeksowanych przez Google. Ważne jest, aby pamiętać, że zapytanie wyszuka Johna w adresach URL i łania w podobny sposób, jak omówiono wcześniej. Jeśli w ogóle inżynier społeczny chce wyszukać wszystkie nazwy celu w adresie URL zamiast jednej w adresie URL i drugiej w tekście, można zastosować następujące zapytanie:

Allinurl: John Doe

Zapytanie ograniczy wyniki do tych, w których adres URL zawiera zarówno nazwę

John and Doe.

W niektórych przypadkach cel będzie ubiegał się o zadania przy użyciu tablic zadań. Niektóre tablice ofert pracy zachowują życiorys celu na swoich stronach internetowych. Ponadto niektóre organizacje zachowują w swoich witrynach życiorysy swoich kandydatów do pracy. Życiorys zawiera bardzo poufne informacje o osobie. Zawiera prawdziwe nazwisko, prawdziwy numer telefonu, prawdziwy adres e-mail, wykształcenie i historię pracy. Ma mnóstwo informacji bardzo przydatnych w ataku socjotechnicznym. Aby wyszukać prywatne dane celu, inżynier społeczny może użyć następującego zapytania:

„John Doe" intitle: „życiorys" „telefon" „adres" „e-mail"

To bardzo potężne zapytanie, które przeszuka cały internet w poszukiwaniu informacji o Johnie Doe, które mają tytuły z takimi informacjami, jak życiorys, numer telefonu, adres e-mail i adres pocztowy. Follo5w. Zapytanie to służy do zbierania informacji nie o konkretnej osobie, ale raczej organizacji. Jego celem jest ujawnianie poufnych informacji w organizacji, które mogą być publikowane na stronach internetowych:

intitle: „nie do dystrybucji" „poufne" witryna: websitename.com

Zapytanie wyszuka wszystko opublikowane z tytułem nieprzeznaczonym do dystrybucji lub na stronie internetowej. poufne To wyszukiwanie może odkryć informacje, o których niektórzy pracownicy organizacji mogą nawet nie wiedzieć. Jest to bardzo przydatne zapytanie w ataku socjotechnicznym, gdy inżynier społeczny chce być informowany o wewnętrznych sprawach organizacji do określonego celu. Jeden z nich. powszechnie używanymi pretekstami do wejścia do strzeżonych pomieszczeń jest osoba do spraw napraw IT lub sieci, z którą firma pilnie się kontaktuje. Strażnicy będą gotowi wpuścić taką osobę i będą mogli przeprowadzić atak pośród innych pracowników bez wywoływania alarmów. Aby móc przyjąć taki pretekst, inżynier społeczny musi posiadać wiedzę na temat wewnętrznej sieci lub infrastruktury organizacji. Oto grupa zapytań, które mogą przekazać te informacje inżynierowi społecznościowemu:

Intitle: „Raport z oceny podatności sieci"

Intitle: „Raport podsumowujący podatność hosta"

Informacje te mogą być również wykorzystane w niektórych częściach ataku, ponieważ ujawniają również słabości, które można wykorzystać w sieci celu lub w hostach podłączonych do sieci. Do wyszukiwanie dla haseł używanych przez użytkowników w sieci organizacyjnej – kopia zapasowa tych haseł może być przydatnym miejscem do rozpoczęcia wyszukiwania. W związku z tym przydatne może być następujące zapytanie:

Site:websitename.com filetype:SQL ("password values" || "passwd" || "old passwords" || "passwords" "user password")

To zapytanie wyszukuje pliki SQL przechowywane w domenie witryny, które mają wartości nazwy hasła, hasła, starych haseł, haseł lub hasła użytkownika. Pliki te, chociaż mogą nie mieć aktualnych haseł użytkownika, mogą dać atakującemu wystarczającą ilość informacji, aby profilować bieżące hasła użytkowników. Na przykład istnieje duże prawdopodobieństwo, że stare hasło e-mail pracownika zostanie zmienione na nowe hasło. Istnieje wiele innych zapytań służących do wyszukiwania danych, które można wykorzystać w Google i innych wyszukiwarkach. Te omówione są tylko najczęściej używane. Należy zachować ostrożność, ponieważ internet nigdy nie zapomina, a nawet po usunięciu niektórych informacji istnieją inne witryny, które przechowują buforowane pliki w witrynie. Dlatego najlepiej jest, aby organizacje nie publikowały swoich poufnych informacji.

Pipl

Innym często używanym narzędziem do zbierania informacji o celu jest Pipl. Pipl archiwizuje informacje o ludziach i oferuje je bezpłatnie każdemu, kto chce uzyskać do nich dostęp. Przechowuje informacje, takie jak prawdziwe imię i nazwisko, adres e-mail, numer telefonu, adres fizyczny i konta w mediach społecznościowych. Oprócz tego oferuje płatną opcję gromadzenia informacji o krewnych danej osoby, począwszy od rodzeństwa i rodziców. Jest to kopalnia złota dla inżynierów społecznych, ponieważ przy bardzo małym wysiłku są oni w stanie uzyskać dostęp do mnóstwa informacji o swoich celach. Weźmy prawdziwy przykład zamiast powszechnie używanego Johna Doe, co może przynieść wiele rezultatów.

W naszym przykładzie zbadaliśmy niektóre możliwości Pipl, jeśli chodzi o poszukiwanie informacji o celach. Ponieważ takie witryny są dostępne dla każdego, jasne jest, że prywatność jest niczym więcej niż iluzją. Takie strony uzyskują informacje z platform mediów społecznościowych, witryn korporacyjnych, danych sprzedawanych przez strony trzecie, danych udostępnianych przez hakerów, danych skradzionych z innych stron internetowych, a nawet danych przechowywanych przez agencje rządowe. Ta konkretna strona jest w stanie uzyskać rejestr kryminalny dotyczący celu, co oznacza, że ma dostęp do niektórych akt przestępczych. Niepokojące jest to, że strony te nie są nielegalne i jeszcze przez długi czas będą dodawać dane o ludziach. To dobra wiadomość dla inżyniera społecznego, ale zła wiadomość dla każdego, kto może być celem. Właścicieli witryn nie można zmusić do usunięcia zawartych w nich danych, dlatego też po dotarciu do nich danych nie można się ukryć. Strona może stać się silniejsza tylko dzięki większej ilości informacji.

Whois.net

Whois.net wciąż znajduje się w witrynach, które archiwizują informacje, i jest kolejnym, który służy prawie tak samo jak Pipl. Whois.net wyświetla informacje, takie jak adresy e-mail, numery telefonów i adresy IP celów, o których szuka się informacji. Whois.net ma również dostęp do informacji o domenach. Jeśli cel ma osobistą stronę internetową, Whois.net jest w stanie uzyskać dokładne informacje na temat rejestrującego i rejestrującego nazwę domeny, datę rejestracji i wygaśnięcia oraz dane kontaktowe właściciela witryny. Podobnie jak Pipl, informacje tutaj uzyskane mogłyby zostać wykorzystane do uzyskania dodatkowych informacji o celu, a tym samym do przeprowadzenia udanego ataku.

Media społecznościowe

Jak dotąd miliardy ludzi korzystają z mediów społecznościowych. Korzystając z tych platform, inżynierowie społeczni mogą znaleźć mnóstwo informacji na temat większości swoich celów. Większość celów będzie miała konta na Facebooku, Twitterze, Instagramie lub LinkedIn. Piękno mediów społecznościowych polega na tym, że zachęca ono użytkowników do dzielenia się osobistymi danymi z życia w Internecie. Użytkownicy mediów społecznościowych są dogodnie nieostrożni i w końcu przekazują nawet wrażliwe informacje całemu światu bez zastanowienia się nad konsekwencjami. Z tych stwierdzeń jasno wynika, że media społecznościowe nie robią nic więcej, jak tylko pogłębić problem. Tworzy bogatą pulę informacji, z której inżynierowie społeczni mogą uzyskać szczegółowe informacje na temat celów bez wzbudzania podejrzeń. W ciągu kilku minut wyszukiwania na wielu platformach społecznościowych inżynier społeczny jest w stanie zebrać hobby celu, miejsce pracy, upodobania i niechęci, krewnych i inne prywatne informacje. Użytkownicy mediów społecznościowych są gotowi chwalić się, że są na wakacjach, pracują w określonych miejscach, wykonują określone prace w swoich miejscach pracy, nowych samochodach i szkołach, do których zabierają swoje dzieci. Nie boją się pokazywać swoich odznak zawodowych w tych serwisach społecznościowych, odznakach, które inżynierowie społeczni mogą powielić i wykorzystać, aby dostać się do organizacji. Użytkownicy mediów społecznościowych będą również zaprzyjaźniać się z

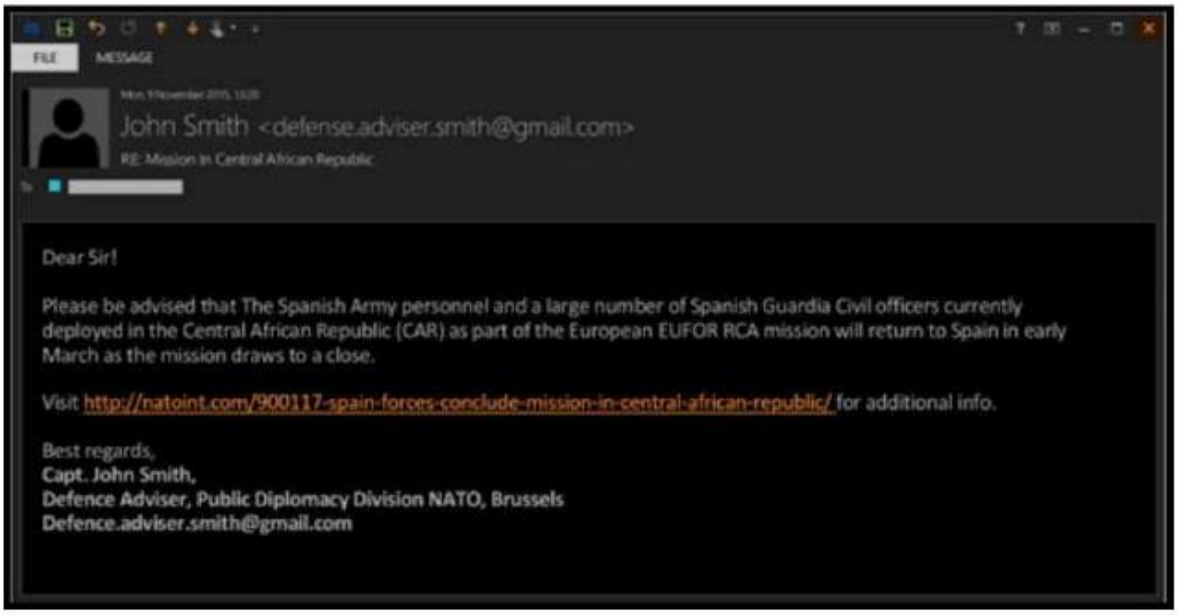
nieznajomymi lub podążać za nimi, pod warunkiem, że pasują do zainteresowań i zainteresowań. To szalony świat, który stawia potencjalne cele w niekorzystnej sytuacji, ponieważ te strony mają na celu umożliwienie ludziom otwarcia się na nieznajomych w Internecie. Informacje, które tradycyjnie były przechowywane do rozmów osobistych, są teraz udostępniane światu. Złe jest to, że dostęp do niego mają zarówno osoby dobrze, jak i źle motywowane. Informacje te mogą być wykorzystane przez inżyniera społecznościowego do profilowania celu. Informacje te mogą się przydać, gdy przekonasz cel do podjęcia pewnych działań lub ujawnienia pewnych informacji. Weźmy hipotetyczny przykład, że jesteśmy inżynierami społecznymi i chcemy uzyskać ściśle tajne projekty i specyfikacje od amerykańskiego kontrahenta wojskowego, abyśmy mogli nauczyć się, jak narażać na szwank jego sprzęt. Możemy zacząć od wejścia na platformę mediów społecznościowych takich jak LinkedIn i wyszukania nazwy tej firmy. Jeśli firma jest na LinkedIn, zostanie wyświetlony profil firmy i lista osób, które podały na LinkedIn, że tam pracują. Następnie identyfikujemy pracownika, który pracuje w dziale badań i projektowania, a nawet w dziale marketingu. Następnie koncentrujemy się na uzyskaniu informacji o tym celu, które mogłyby nam pomóc w postawieniu go w pozycji, w której mogą ujawnić tajne informacje, których szukamy. Zaczynamy od przeszukiwania profilu pracownika na Facebooku, aby znaleźć hobby, zainteresowania i inne dane osobowe. Przechodzimy na Instagram i przyglądamy się rodzajom zdjęć, które pracownik publikuje. Zaczynamy geolokalizować cel, kojarząc informacje, które otrzymujemy na wszystkich kontach mediów społecznościowych w jego imieniu. Dochodzimy do punktu, w którym dowiadujemy się o jego adresie fizycznym i miejscach, w których lubi spędzać czas. W tym momencie podchodzimy do niego i wykorzystujemy jedną z taktyk wyuczonych wcześniej w sztuczkach umysłowych i rozdziałach perswazji, aby zmusić go do włożenia do komputera dysku USB z złośliwym oprogramowaniem. Stamtąd złośliwe oprogramowanie zacznie gromadzić dla nas potrzebne informacje. To takie proste. Organizacje są atakowane w podobny sposób. Na początku 2017 r. 10 000 amerykańskich pracowników zostało oszukanych za pomocą mediów społecznościowych przez rosyjskich hakerów, którzy umieszczali złośliwe oprogramowanie w postach i wiadomościach w mediach społecznościowych. W połowie 2017 r. stworzono fałszywą postać dziewczynki o imieniu Mia Ash, która została wykorzystana do zaatakowania firmy sieciowej, atakując pracownika płci męskiej posiadającego szerokie prawa w organizacji. Atak został udaremniony tylko dlatego, że organizacja miała silną kontrolę, aby chronić się przed złośliwym oprogramowaniem. Pracownik płci męskiej już zakochał się w oszustwie przy użyciu fałszywego konta dziewczyny na Facebooku.

W sierpniu 2016 r. odkryto, że doszło do masowego oszustwa finansowego skierowanego do klientów, którzy śledzili dany bank w mediach społecznościowych. Uważa się, że osoby atakujące mogły przejąć kontrolę nad kontami mediów społecznościowych banku i wysyłać fałszywe oferty do obserwujących, którzy tylko stracili pieniądze. Istnieje wiele innych ataków inżynierii społecznej za pośrednictwem mediów społecznościowych. Winna jest jedynie szybka dostępność prywatnych informacji w mediach społecznościowych

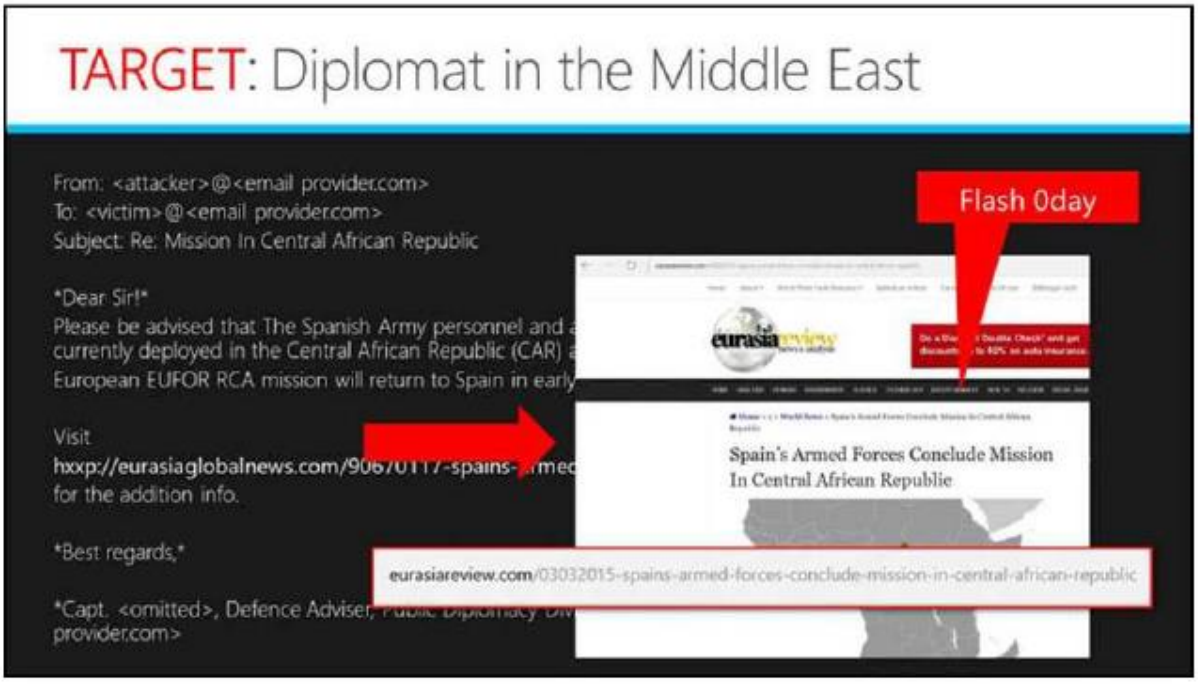
Phishing i spear phishing

Inżynierowie społecznościowi nadal używają technik phishingowych do gromadzenia informacji o celu. Chcą wykorzystywać emocje, takie jak strach i podniecenie, w połączeniu z pewnymi naciskami, takimi jak pilna potrzeba uzyskania maksymalnego wskaźnika zgodności. Obecnie phishing i ataki typu spear phishing stały się zaawansowane, ponieważ osoby atakujące mają możliwość doskonałego klonowania renomowanych stron internetowych i wykorzystywania ich do kradzieży danych klienta. Możliwość skrócenia adresów URL tych witryn pomaga również atakującym uniknąć wykrycia, ponieważ użytkownicy byliby zaniepokojeni, gdyby zauważyli pewną różnicę między prawidłowymi adresami URL witryn a linkami wysyłanymi przez atakujących. Atakujący wykorzystują klony witryn, takich jak systemy bankowości internetowej i konta w mediach społecznościowych, aby pozbyć się wielu danych

z niczego niepodejrzewających celów. Jeśli na przykład osoba atakująca wysłała wiadomość e-mail z informacją, że doszło do naruszenia Twojego konta PayPal, a hasło musi zostać zmienione w trybie pilnym, wraz z linkiem do zmiany hasła, możesz z łatwością je zastosować. Link doprowadziłby cię do wyglądu przypominającego PayPal, w którym poproszono by Cię o wpisanie aktualnego hasła i nowego hasła. Po przesłaniu tych informacji twoje aktualne hasło zostanie wysłane do atakujących. W bardzo krótkim czasie otrzymają od Ciebie bardzo poufne informacje, wykorzystując strach przed utratą pieniędzy, a następnie wywierając presję na szybką odpowiedź. Jak widać na zrzucie ekranu, e-mail został wysłany przez Johna Smitha, który najwyraźniej pracuje jako Doradca Obrony w NATO:

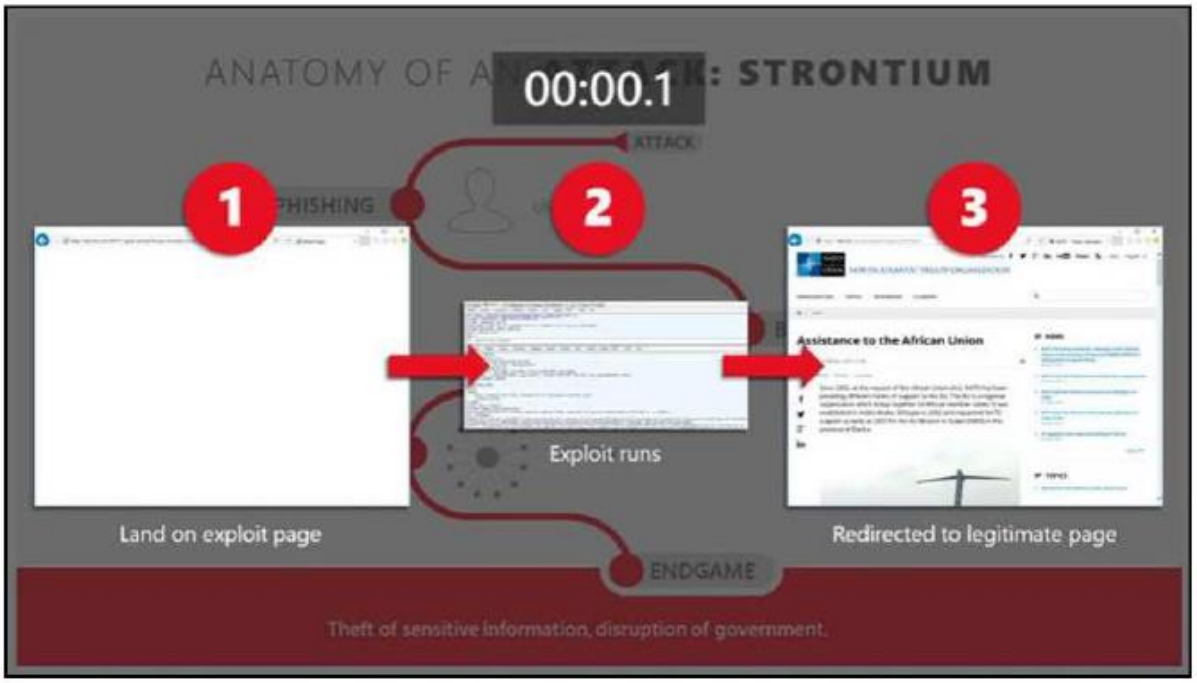


Poniżej znajduje się zrzut ekranu z phishingu włócznią wymierzoną w dyplomatę. Różnica w stosunku do poprzedniego zrzutu ekranu polega na tym, że możesz wyraźnie zobaczyć dołączony exploit:

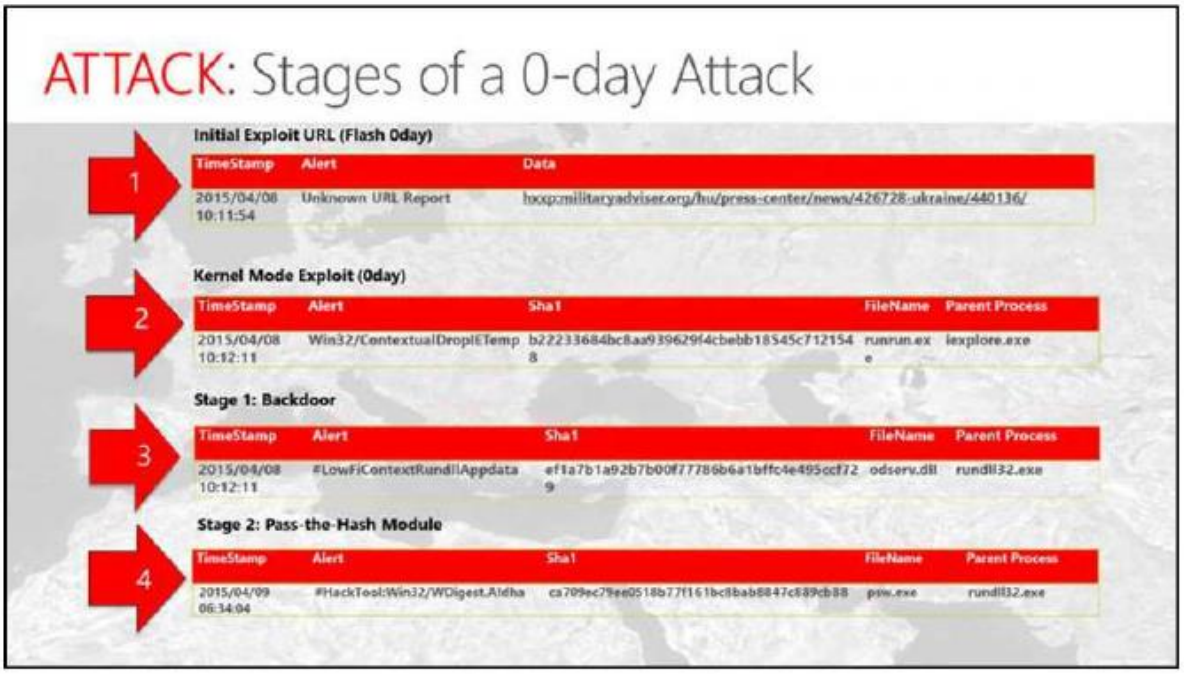


Na poniższym zrzucie ekranu widać wiadomość e-mail typu phishing spear o tematyce NATO:

Aby zademonstrować atak, najpierw przychodzi wiadomość e-mail, cel klika link, ląduje na stronie exploita, a exploit uruchamia się, gdy ofiara jest kierowana na legalną stronę:



Oba zrzuty ekranu były pierwszymi krokami do przeprowadzenia ataku zero-day na cel, a poniższy zrzut ekranu pokaże początkowy adres URL wykorzystania (Flash 0day), nazwę pliku, a także nazwę procesu, na przykład:



Wodopoje

Jest to technika zrodzona z potrzeby gromadzenia informacji o celach, które są dość oświecone o zagrożeniach internetowych i nie mogą zakochać się w tanich sztuczkach. W tym przypadku inżynier społeczny skompromituje listę kodową legalnej witryny internetowej, którą często odwiedza cel, a następnie osadzi w niej złośliwe oprogramowanie. Dobrymi stronami do tego są fora dyskusyjne, witryny z poradami giełdowymi, strony sportowe i witryny lifestyle. Gdy cel odwiedza witrynę, złośliwe oprogramowanie zainfekuje urządzenie i stamtąd zacznie gromadzić dane z przeglądarki lub z dysku twardego komputera. Wodopoje są skuteczne, ponieważ są ostatnim miejscem, w którym cel pomyśli, że może zostać zaatakowany.

Jednak odporni atakujący będą badać cel przez wystarczająco długi czas, aby wiedzieć, że odwiedzają tę stronę, a tym samym narażają ją na szwank, aby naruszyć cel. Symantec, jeden z wiodących producentów produktów z zakresu bezpieczeństwa cybernetycznego, na początku 2017 r. podkreślił, że nastąpił gwałtowny wzrost liczby ataków z otworami wodnymi. Ten rodzaj ataku jest szczególnie przydatny przeciwko pracownikom IT i kadrze kierowniczej wyższego szczebla w organizacjach, którzy mogą być w ciągłej gotowości, co utrudnia atak za pomocą innych bezpośrednich form ataku.

Blogi

Użytkownicy Internetu zawsze publikują duże ilości danych dla każdego, kto słucha , aby zwrócić ich uwagę. Z tego powodu istnieje wiele blogów. Niezadowoleni pracownicy mogą zabrać je na blogi, aby przedstawić niepokojące fakty dotyczące organizacji. Taka osoba jest dobrym źródłem informacji dla inżyniera społecznego. Inżynier społeczny musi jedynie wykazać troskę i wykorzystać byłego pracownika jako źródło poufnych informacji o firmie. W ten sposób inżynier społeczny zyska, zdobywając nowego celu do ataku, który ma wiarygodne źródło informacji, a bloger zyska ulgę, że ktoś będzie mógł podzielić się swoimi frustracjami. Niezadowoleni pracownicy mogą pogłębiać się, ujawniając organizacje, z którymi współpracowali. W 2015 r. Edward Snowden odkrył światowe daleko idące tajemnice na temat USA i tego, jak NSA śledzi wszystkich, otwiera wiadomości e-mail, zmusza operatorów do dzielenia się z nimi metadanymi na temat SMS-ów i połączeń, a także zmusza dostawców usług internetowych do udzielania im poufnych informacji o swoich użytkownikach.

Informacje były obszerne i szkodliwe dla organizacji. Snowden mógł być kluczowym źródłem informacji dla inżyniera społecznego, który mógł chcieć zaatakować NSA. Dlatego zawsze dobrze jest mieć otwarte uszy; na blogu może pojawić się interesujący artykuł, który może być źródłem informacji o organizacji lub osobie.

Telefon

Chociaż może to nie brzmieć jak zaawansowane narzędzie inżynierii społecznej, telefony są nadal używane do przeprowadzania ataków inżynierii społecznej. Sprawiają, że inżynierowie społeczności mówią bezpośrednio do celów i używają określonych dźwięków, wyboru słów i stresu na niektórych, wskazuje, aby cel ujawnił pewne informacje. Telefony są dziś używane do uzyskiwania poufnych informacji od niektórych grup ludzi. Było wiele skarg, w których napastnicy dzwonili do osób starszych i grozili im procesami sądowymi lub wysokimi grzywnami jeśli nie ujawnią pewnych informacji lub nie wyślą pieniędzy. Pojawiły się również skargi na osoby atakujące, które udają, że są działami IT, pomagają facetom, którzy dzwonią do ludzi i proszą ich o podanie pewnych informacji. Telefony zostały również wykorzystane do połączenia z organizacjami i potwierdzić obecność lub nieobecność niektórych pracowników w miejscu pracy. Telefony zostały również wykorzystane do bezpośredniej organizacji ataków z zakresu inżynierii społecznej. Złośliwi ludzie, po znalezieniu informacji, takich jak informacje bankowe lub instytucjonalne o swoich celach, mogą zadzwonić i udawać wiarygodne dane w takich organizacjach i poprosić o przekazanie im niektórych informacji w ramach zadania aktualizacji lub konserwacji. Inżynierowie społeczni również używają telefonów do zbierania informacji o celu od znajomych i rodziny, jeśli uda im się zdobyć ich numery, zadanie, które nie jest już trudne ze względu na media społecznościowe. Rozmowy telefoniczne są wyjątkowo udane, ponieważ nie dają wystarczająco dużo czasu celowi pomyśleć o negatywnej odpowiedzi. Stosując inne taktyki, takie jak przeciążanie bufora ludzkiego mózgu, inżynier społeczny może uzyskać cel, który spełni niektóre szalone żądania lub przekaże bardzo poufne informacje. Telefony mają poczucie natychmiastowości, jeśli chodzi o uzyskiwanie odpowiedzi i dlatego są bardzo skuteczne przeciwko celom.

Metody nietechniczne

Metody te mają zazwyczaj charakter fizyczny i nie można ich przeprowadzać zdalnie. Dlatego inżynier społeczny musi być na miejscu osobiście, aby zebrać potrzebne informacje. Konieczne jest również, aby inżynier społeczny posiadał wiedzę na temat pretekstu, perswazji i sztuczek umysłu, które wykorzystają do uzyskania poszukiwanych informacji. Najważniejszym narzędziem, którego inżynier społeczny będzie potrzebował w tego rodzaju gromadzeniu informacji, jest jednak aktywny mózg. Oto niektóre przykłady fizycznych metod gromadzenia informacji o celach:

Nurkowanie w śmietniku

Cele czasami dysponują poufnymi informacjami, takimi jak dokumentacja medyczna, wyciągi bankowe, wydrukowane życiorysy i listy aplikacyjne, a czasami osobiste zdjęcia. Organizacje napotykają również te same problemy, w których niektóre informacje, takie jak techniczne dzienniki wsparcia, wydruki e-mail, notatki samoprzylepne zawierające nazwy użytkowników i hasła, poufne dokumenty, pliki informacji o systemie i stare raporty oceny podatności trafiają do śmietników. Nawet w organizacjach, w których pracownicy są wyposażeni w niszczarki, nierzadko zdarza się, że poufne informacje są usuwane wraz z innymi śmieciami. Nurkowanie w kontenerach to miejsce, w którym inżynier społeczny przegląda przedmioty, które zostały zutylizowane zarówno przez osoby fizyczne, jak i organizacje w celu znalezienia przydatnych informacji. Wszystkie wymienione informacje są przydatne dla atakującego, ponieważ można je wykorzystać do przeprowadzenia ataku. Nurkowanie w kontenerach wymaga mniej wysiłku w porównaniu z innymi metodami, ponieważ nie przywiązuje się dużej wagi do śmieci. Tego rodzaju metoda gromadzenia danych nie jest również nielegalna w wielu krajach,

ponieważ jest całkowicie legalne, aby ktokolwiek wyrzucał śmieci, nawet jeśli do nich nie należy. Nie ma żadnych zasad regulujących własność śmieci, chociaż kilka firm wniosło o to, że intruzi przeszukują śmieci. Nurkowanie na śmietniku działa z powodu obecnego przeciążenia informacyjnego. Ludzie wytwarzają zbyt wiele informacji, aby je przechowywać, a jednocześnie nie dbają o to, jak je pozbyć. Nawet w organizacjach, które mają zasady usuwania plików, nie jest zaskoczeniem, że te zasady są rzadko przestrzegane. Dlatego istnieje duże prawdopodobieństwo, że inżynier społeczny zdobędzie złoto w misji nurkowania w śmietniku i znajdzie poufne informacje, które zostały niewłaściwie usunięte. Był serial telewizyjny o testerach penetracyjnych o nazwie Tiger Team, który pokazał, jak można atakować organizacje. W jednym odcinku zostały zawarte przez CEO Symbolic Motors. Ich misja zwiadowcza pokazała, że organizacja miała wiele kontroli bezpieczeństwa fizycznego, co utrudnia jej pośrednie złamanie. Jednak podczas misji zwiadowczej byli w stanie zdobyć śmieci organizacji i przeszukali je, aby znaleźć coś wartościowego. Mieli szczęście znaleźć szczegółowe informacje na temat zespołu IT, który organizacja zleciła utrzymanie swoich systemów. Zespół Tygrysa następnie przebrał jednego z nich, aby działał jako wsparcie techniczne od zakontraktowanej firmy. Wysłany agent został wprowadzony i bezpośrednio uzyskał dostęp do serwerowni firmy. Gdyby to był faktyczny atak, agent mógłby wejść i osadzić złośliwe oprogramowanie w celu wyłączenia systemów bezpieczeństwa lub zebrania poufnych informacji z serwerów, aby przygotować drogę do znacznie większego ataku. Jest to dowód na to, że nurkowanie w śmietniku jest bardzo skuteczne i niezwykle łatwe do wykonania.

Włamanie i podszywanie się

Jest to znacznie bardziej ryzykowny sposób uzyskiwania informacji, w którym inżynier społeczny uzyskuje dostęp do budynku celu w celu zbierania informacji, udając, że jest kimś innym. Inżynierowie społeczni podszywają się pod pracowników, zewnętrznych wykonawców, dostawców lub personel naprawczy. Korzystając z taktyk omówionych w Części 3, będą mogli przedostać się przez strażników i dostać się do budynku. Podczas pobytu w budynku inżynier społeczny wtapia się i zachowuje się tak, jak zwykle robią to podszywający się ludzie. Informacje mogą być gromadzone przez podsłuchiwanie, rozmowy z personelem w środku lub pozostawianie dysków USB z złośliwym oprogramowaniem w widocznych miejscach, które zostaną zebrane i włożone do komputerów. Inżynierowie społeczni mogą nawet przedostać się do biur wysokiej rangi, przekonując sekretarek lub recepcjonistów, aby wpuścili ich. Podszywanie się jest niebezpieczne, ponieważ może pozostawić inżyniera społecznego bezbronnego, gdy zostaną odkryte.

Tailgating

Jest to kolejna taktyka stosowana w celu uzyskania dostępu do organizacji, które mają potężne fizyczne zabezpieczenia, takie jak karty inteligentne lub dane biometryczne. Te kontrole bezpieczeństwa skutecznie zapobiegają przedostawaniu się nieupoważnionych osób do prywatnych pomieszczeń i często chronione pomieszczenia będą zawierać cenne informacje. Inżynierowie społeczni wykorzystują uprzejmość ludzi, którzy mają prawo wchodzić do tych budynków. Mogą wydawać się, że desperacko szukają przepustki w pobliżu zabezpieczonego punktu wejścia, a kiedy miły pracownik dotrze do tego samego punktu wejścia, może zaoferować pomoc inżynierowi społecznemu w dotarciu. W ten sposób inżynier społeczny przestaje grzebać i obficie dziękuje uprzejmemu pracownikowi za pomoc. Inna taktyka polega na tym, że inżynier społeczny biegnie, aby złapać drzwi, zanim się zamkną, a osoba, która je otworzyła, instynktownie je przytrzyma, umożliwiając dostęp do wrażliwej części budynku.

Surfowanie przez ramiona

Ta metoda zbierania informacji jest najprostsza ze wszystkich i nadal jest stosowana. W tym miejscu inżynier społeczny spogląda przez ramię celu, aby zebrać informacje o tym, co czyta lub pisze na swoich urządzeniach obliczeniowych. Zazwyczaj inżynier społeczny będzie widział hasła, poufne dane, dane

uwierzytelniające w postaci zwykłego tekstu i inne wrażliwe informacje, do których będzie miał dostęp cel. Odbywa się to wszędzie tam, gdzie ludzie używają komputerów, zwłaszcza w kawiarniach, na lotniskach, w parkach publicznych, a nawet w restauracjach.

Obserwacja

Tak prosta jak się wydaje, obserwacja może być bardzo przydatną techniką do zbierania informacji o celu. Inżynier społeczny po zidentyfikowaniu celu może zdecydować się na przestrzeganie codziennych czynności, aby znaleźć szanse na wykorzystanie. Na przykład atakujący może być w stanie zebrać informacje, takie jak czas, w którym cel idzie spać, budzi się, poranna rutyna, ścieżka do pracy, weryfikacja w punktach wejścia do miejsca pracy celu, czas, w którym cel wychodzi na lunch , czas powrotu celu do domu i ulubione stawy celu. Gromadząc wszystkie te informacje, inżynier społeczny będzie w lepszym momencie, aby nawiązać rozmowę z celem i zbudować relację, aby umieścić cel w miejscu, w którym mógłby zostać wykorzystany. Obserwacja wymaga tylko cierpliwości i czasu, ujawni wiele informacji o celu, które można wykorzystać w ataku.

Porady

Wskazówki dotyczące gromadzenia informacji są następujące:

* Zawsze pamiętaj - amatorzy hakują systemy, profesjonaliści hakują ludzi.

* Inżynieria społeczna ma miejsce, gdy haker wykorzystuje manipulację, wpływ lub oszustwo, aby skłonić inną osobę do ujawnienia informacji lub wykonania jakiejś czynności, która jest dla nich korzystna. Zasadniczo sprowadza się to tylko do nakłaniania ludzi do łamania normalnych procedur bezpieczeństwa, takich jak ujawnianie hasła.

* Pamiętaj o zniszczeniu papieru zawierającego cenne informacje.

* Upewnij się, że używasz klasyfikacji dokumentów w swojej sieci.

* Upewnij się, że masz ekran prywatności na ekranie laptopa.

* Zawsze korzystaj z VPN podczas łączenia się z publicznym Wi-Fi.