JAK NIE DAĆ SIĘ ZŁAPAĆ NA WĘDKĘ

O bezpieczeństwie urządzeń mobilnych

Aleksandra Boniewicz

Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/jasini
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-0438-5

Printed in Poland.

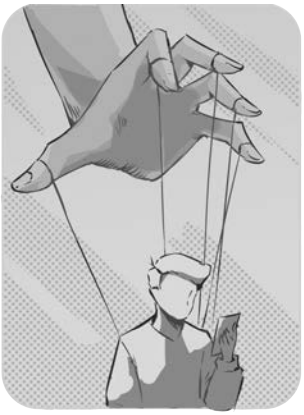
Spis treści

Rozdział 1.

O co to całe zamieszanie?

Ten rozdział zawiera krótki opis używanych w książce terminów związanych z popularnymi metodami wyłudzania danych gromadzonych na urządzeniach mobilnych. Terminologia ma oswoić czytelnika z zagrożeniami, z którymi może się mierzyć na co dzień, narażając się — czasem nieświadomie — na utratę tych danych pomimo założonych wielu „kłódek" na urządzeniu.

1.1. Prowadzenie za rączkę — socjotechnika



Socjotechnika — inaczej inżynieria społeczna, to „próby manipulowania ludźmi w taki sposób, aby w pewnym obszarze swojego życia podjęli określone działania" [2]. Sama definicja nie wygląda groźnie, nawet można powiedzieć, że brzmi znajomo. Bo ile razy zdarzyło nam się próbować nakłaniać inne osoby, żeby wykonały jakąś czynność? Ile razy używaliśmy „sztuczek", żeby dziecko zjadło owoce i warzywa, a nie kolejne słodycze? A ile razy to dziecko próbowało nas przekonać, że kolejny cukierek niewiele zmieni w jego diecie, a następna obejrzana bajka ma wartość edukacyjną? Gdy do tego dołożymy pewne działania naszych szefów, znajomych, partnerów oraz — o zgrozo — polityków, może się okazać, że obcujemy z tą inżynierią na co dzień, że jest dla nas chlebem powszednim, tylko zupełnie sobie z tego nie zdajemy sprawy. Nawet wizyta w sklepie, do którego poszliśmy po dosłownie jedną rzecz, może zakończyć się powrotem z dwiema wielkimi siatkami zakupów, bo tak dobrze zostaliśmy zmanipulowani i skuszeni promocjami. Nic więc dziwnego, że przestępcy próbują wykorzystywać te techniki, wiedząc, że jesteśmy przesiąknięci tymi metodami. Często nawet nie zauważymy, jak łatwo daliśmy się „podejść" i straciliśmy nasze dane, wierząc przy tym głęboko, że wygraliśmy los na loterii.

Oczywiście, nie należy tego terminu rozważać tylko w negatywnym kontekście. Jako inżynieria czy dziedzina nauki socjotechnika nie jest zła. Wszystko zależy od tego, w jakim celu zostanie użyta. Często jest stosowana przez policję, lekarzy czy nauczycieli, a nawet rodziców w celu nakłonienia kogoś do podjęcia działania mającego przynieść pozytywny efekt. Przykładowo, odpowiednie techniki mogą zmotywować drugą osobę do pracy nad sobą, do rozwijania swoich pasji czy pomocy innym. Jednak socjotechnika — jak każde narzędzie — w rękach uczciwych ludzi może przynieść

wymierne korzyści, natomiast w rękach hackerów i oszustów same straty. Na dodatek jest ona ciągle udoskonalana, co sprawia, że gdy już opracujemy dobre sposoby obrony, pojawią się nowe techniki, których nasz system odpornościowy jeszcze nie poznał i nie przygotował na nie odpowiednich „przeciwciał".

Najczęściej oszuści stosują sztuczki socjotechniczne wykorzystujące ludzkie emocje, jak np. nasz strach o siebie, o swoich bliskich i o swoje oszczędności albo chęć wzbogacenia się, najlepiej łatwym kosztem. Na pewno niejednej osobie znana jest metoda „na wnuczka". Wykorzystywała ona ludzką ułomność, wiarę w swoich bliskich i silne uczucia z nimi związane, żeby wykradać oszczędności życia starszych ludzi, którzy wierzyli, że przekazują te pieniądze swoim wnukom.

Dziś, dzięki technologii, dużo prościej przeprowadzić taką akcję na większą skalę. Bo dużo łatwiej i szybciej jest wysłać 1000 SMS-ów czy e-maili, niż odwiedzić 1000 osób i wyłudzić od nich pieniądze. W dobie darmowych SMS-ów w ramach abonamentu koszty takiego oszustwa są znikome. Na szczęście, taka działalność pozostawia po sobie ślad, który można odtworzyć nawet po usunięciu go z telefonu [1]. Jednak stracone mienie może być już nie do odzyskania. Okazuje się, że życie dostarcza oszustom wiele okazji do podjęcia próby zmanipulowania ludzi, aby uzyskać dane, na których im zależy. I tak, daleko nie szukając, pandemia przyczyniła się do wzrostu liczby ataków w postaci fałszywych wiadomości SMS o wygranej w loterii szczepionkowej czy o możliwości szybszego zapisu na szczepienia. Kryzys energetyczny z kolei zwiększył liczbę wysyłanych SMS-ów o zaleganiu z opłatami za prąd. Każda taka wiadomość była opatrzona linkiem do stron wyłudzających dane użytkownika.

Dlatego bardzo ważne jest, żeby wiedzieć, co to jest socjotechnika i jakie sztuczki są wykorzystywane, aby manipulować ludźmi. Wtedy będziemy odporni na tego rodzaju działania, niezależnie od tego, co jeszcze przyniesie życie, z jakimi pandemiami i kryzysami przyjdzie nam się mierzyć. Warto tę wiedzę poszerzać i uzupełniać, bo sztuczki i metody obrony znane dziś niekoniecznie nadal będą aktualne za dziesięć lat.

1.2. Łowienie na „wiadomość" — phishing

Phishing — „łowienie" ryb (czyt. ofiar oszustwa), atak polegający na zarzucaniu wędki w postaci fałszywych e-maili, SMS-ów czy wiadomości w komunikatorach, w których potencjalna ofiara jest nakłaniana do kliknięcia przesłanego linku lub do zainstalowania na urządzeniu podanej aplikacji. Ta metoda ataku ma za zadanie wyłudzić wrażliwe dane użytkownika dzięki zastosowaniu różnych socjotechnik. Po przejściu na stronę podaną w wiadomości może zostać wyświetlony formularz, do którego będzie należało wpisać swoje dane, np. do logowania do banku. Natomiast po zainstalowaniu aplikacji i wyrażeniu zgody na dostęp do zasobów urządzenia może ona sama pobierać sobie takie dane. Często atakujący podszywają się pod znane firmy i marki, jak np.

firmy kurierskie, handlowe, aukcyjne czy bankowe. Do bardzo wielu ludzi wysyłają wiadomości o tej samej treści w nadziei, że któraś osoba akurat złapie się na nią i wykona zalecone w wiadomości czynności. Nawet 1% „złowionych" osób jest w stanie zapewnić oszustom spory zysk, jeśli zdobyczą będą np. dane potrzebne do logowania się do banku.

1.3. Parodiowanie, czyli każdy może być aktorem — spoofing

Spoofing — „parodiowanie", jest to atak na systemy teleinformatyczne. Przestępcy podszywają się pod jakąś instytucję — bank, firmę czy urząd[1]. Spoofing może dotyczyć otrzymywanych SMS-ów lub odbieranych połączeń telefonicznych. Operacje te są wykonywane w celu wyłudzenia danych, które w jakiś sposób przyczynią się do wzbogacenia osób dokonujących ataku. Mogą to być np. dane do logowania w banku lub dane osobowe przydatne do zaciągnięcia kredytu. W takim ataku intensywnie wykorzystuje się techniki inżynierii społecznej. Obecnie bardzo popularny jest spoofing telefoniczny. W tym wypadku mamy do czynienia z kontaktem poniekąd osobistym. Nie jest to już zatem bezduszny mail czy SMS, ale rozmowa z prawdziwą osobą, która wykorzystując wiedzę socjotechniczną, próbuje przekonać rozmówcę, że reprezentuje firmę, z której numeru telefonu rzekomo dzwoni. W takich atakach przestępcy wykorzystują adres e-mail (spoofing e-mail), numer telefonu (spoofing telefoniczny) czy adres IP (spoofing IP), aby podszyć się pod pracownika danej firmy. Odmianą spoofingu e-mail jest phishing, gdyż nadawcy fałszywych wiadomości również podszywają się pod kogoś innego. Niebezpieczny jest spoofing telefoniczny (niekiedy nazywany też *vishing*, od słów *voice* i *phishing*), w którym atakujący, wykorzystując numer telefonu danej instytucji, próbują uśpić czujność rozmówcy. Na wyświetlaczu abonenta wyświetla się wówczas np. numer infolinii banku. W większości ataków telefonicznych atakujący próbują podszyć się pod przedstawiciela banku.

Na stronie *www.policja.pl* można znaleźć takie ostrzeżenie[2]:

> Scenariusz ataków wykorzystujących spoofing telefoniczny jest zwykle taki sam, a przynajmniej zbliżony. Oszust stara się wystraszyć rozmówcę, by działał pod wpływem emocji, najczęściej informując go o rzekomym włamaniu na konto bankowe i konieczności podjęcia szybkich działań, by zablokować możliwości włamywaczy. Każdą telefoniczną prośbę o przesłanie pieniędzy lub podanie danych

[1] *https://www.gov.pl/web/baza-wiedzy/czym-jest-spoofing-jak-go-rozpoznac-i-nie-dac-sie-nabrac*

[2] *https://www.policja.pl/pol/aktualnosci/218563,Uciekla-przed-wojna-Padla-ofiara-spoo*
↪fingu.html

konta bankowego powinno się traktować jako próbę oszustwa. Najlepiej w takiej sytuacji przerwać połączenie, samodzielnie wpisać numer banku, zadzwonić, poinformować o otrzymanym połączeniu i zweryfikować przekazane informacje lub osobiście udać się do siedziby banku.

Co odważniejsi oszuści podszywają się nawet pod samych policjantów, aby uwiarygodnić oszustwo „na przedstawiciela bankowego", również dzwoniąc rzekomo z komisariatu policji[3].

Spoofing telefoniczny jest możliwy w telefonii VoIP (*Voice over IP*). Można w niej bowiem samemu ustawić, z jakiego numeru jest wykonywane połączenie i jaka nazwa ma się pokazać dzwoniącemu. Operatorzy nie sprawdzają, czy abonent, który wykonuje dane połączenie, używa przypisanego numeru. Protokoły używane w telefonii komórkowej (o nazwie *Signaling System 7*) pochodzą z 1981 r., są zatem przestarzałe i nie uwzględniają wiarygodnych metod uwierzytelniania.

Atak ten jest możliwy, ponieważ abonent odbierający połączenie nie może sprawdzić, czy jest ono prawdziwe, czy „podrobione". Może to wykryć jedynie operator[4]. Po fakcie mogą to również ustalić organy ścigania, które mają dostęp do bilingów obu abonentów.

Na stronie portalu *niebezpiecznik.pl* można znaleźć artykuł poświęcony tego typu atakowi wraz z informacją, dlaczego operatorom trudno jest blokować spoofing[5].

1.4. „Podsłuchiwacz" — man in the middle (MitM)

Man in the middle — w wolnym tłumaczeniu „mężczyzna pośrodku", jest formą ataku sieciowego, „który polega na tym, iż pomiędzy nadawcą a adresatem pakietu pojawia się swoisty pośrednik" [3], przechwytujący pakiety danych wysyłane pomiędzy dwoma punktami. Jest to forma ataku zdarzająca się w sieciach bezprzewodowych (WiFi).

Aby skorzystać z WiFi, urządzenie (np. smartfon, tablet, laptop) musi połączyć się bezprzewodowo z urządzeniem, które serwuje dostęp do internetu. Tym urządzeniem może być np. router albo punkt dostępowy (*Access Point* — AP). W przypadku niewielkiej infrastruktury sieciowej, np. domowej, najczęściej spotykanym rozwiązaniem jest router. To z nim bezprzewodowo komunikują się wszystkie urządzenia,

[3] *https://www.policja.pl/pol/aktualnosci/214795,Stracila-50-tys-zl-bo-uwierzyla-oszustom.html*

[4] *https://niebezpiecznik.pl/post/spoofing-rozmow-telefonicznych/*

[5] *https://niebezpiecznik.pl/post/spoofing-rozmow-telefonicznych/*

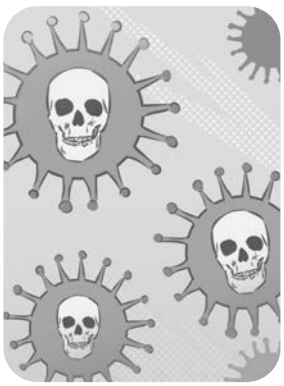
które chcą mieć dostęp do internetu. Znajdują się one w niewielkiej odległości od routera, nie powinien zatem występować problem z zasięgiem. Jednak w przypadku większych jednostek, np. uczelni czy galerii handlowych, jeden router nie wystarczy, gdyż odległości pomiędzy urządzeniem a routerem mogą być na tyle duże, że będzie można zaobserwować zanikanie zasięgu, co przekłada się na problemy z połączeniem sieciowym, potocznie zwane „brakiem internetu". Z pomocą przychodzą tu właśnie punkty AP, które można odpowiednio rozmieścić w danym budynku. To z nimi będą się łączyć urządzenia, a one z kolei będą łączyć się z routerem.

Często dostęp do sieci bezprzewodowej (WiFi) jest zabezpieczony hasłem. Jednak w miejscach publicznych, jak np. galerie handlowe, kawiarnie, hotele czy pociągi, nie ma takich zabezpieczeń. Takie ogólnodostępne punkty umożliwiające bezprzewodowe łączenie się z internetem są nazywane hotspotami.

Komunikacja sieciowa polega na przesyłaniu pakietów danych od użytkownika do np. punktu AP i na odwrót. Atakujący ustawia się pomiędzy tymi dwoma odbiorcami i przechwytuje te pakiety. Może wystawić swój własny punkt AP, z którym będzie łączyła się potencjalna ofiara. Dzięki temu może je odczytać, wysłać do prawdziwego punktu AP, otrzymać odpowiedź, po czym ją spreparować i wysłać do użytkownika. Użytkownik nie jest świadomy, że otrzymał fałszywe pakiety. Atak ten jest możliwy, gdy atakujący pozna klucz dostępu do sieci lub gdy sieć nie jest zabezpieczona hasłem, jak np. hotspoty w galeriach.

Używając niezabezpieczonych hotspotów, możemy narazić się na wyciek danych. Jeśli jednak nie mamy do wyboru innej, zabezpieczonej sieci, wówczas należy zadbać o to, aby dane wychodzące z urządzenia były szyfrowane. Dzięki temu, nawet jeśli ktoś je podsłucha, nie będzie mógł ich wykorzystać.

1.5. Wirus na koniu trojańskim — malware



Malware — to skrót od angielskiego określenia *malicious software*, oznaczającego złośliwe oprogramowanie. To aplikacja mająca za zadanie wykonać jakieś złośliwe działanie na urządzeniu, na którym została zainstalowana. Kto tworzy i kto instaluje takie aplikacje i czemu? Oprogramowanie tworzy osoba, która zamierza uszkodzić urządzenie lub przechwycić dane, by wykorzystać je w celu osiągnięcia korzyści, np. materialnych. Instaluje je natomiast posiadacz danego urządzenia. Często robi to w sposób nieświadomy. To znaczy świadomie potwierdza chęć instalacji aplikacji, ale nie spodziewa się, że może ona wykonać inną akcję niż ta, o której informuje strona z aplikacją. Dzieje się tak dlatego, że użytkownik jest celowo wprowadzany w błąd. Oszust zachęca klientów do instalacji aplikacji, wykorzystując socjotechniki w phishingu, np. przez informowanie w treści SMS-a czy e-maila, skąd można ją pobrać i jakie ma ona zalety. Aplikacje te z reguły nie znajdują

się w oficjalnym sklepie dostawców systemów operacyjnych i wymagają zgody użytkownika na zainstalowanie ich spoza sklepu. Niestety, znane są też przypadki, kiedy takie złośliwe oprogramowanie trafia do sklepu.

Wyróżniane są różne rodzaje szkodliwego oprogramowania, zależnie od sposobu działania i szkód, jakie może wyrządzić:

- **Wirus** — kod programu, który potrafi się powielać i infekować kolejne urządzenia, dodatkowo wyrządzając na nich szkody. Rodzaj szkód zależy od tego, co programista zaimplementował w tym oprogramowaniu. Może to być np. kasowanie danych, rozsyłanie spamu, przejmowanie danych do logowania do różnych serwisów.
- **Koń trojański** — przykład wirusa; wygląda jak zwykła przydatna aplikacja, ale dodatkowo wykonuje szkodliwą działalność, np. poprzez pobieranie danych lub odczyt wiadomości.
- **Dropper** — rodzaj konia trojańskiego; oprogramowanie, które samo w sobie nie jest zainfekowane, ale instaluje inne złośliwe oprogramowanie.
- **Ransomware** — oprogramowanie, które szyfruje pliki na urządzeniu i blokuje urządzenie do czasu zapłacenia okupu.
- **Adware** — oprogramowanie wyświetlające niechciane reklamy.
- **Spyware** — oprogramowanie, które szpieguje na urządzeniu, czyli zbiera pewne informacje o użytkowniku.
- **Keylogger** — oprogramowanie, które rejestruje wszystkie klawisze wciskane przez użytkownika.
- **Rootkit** — oprogramowanie, które pozwala na uzyskanie praw administratora urządzenia, a przez to dostępu do wszystkich zasobów i danych.

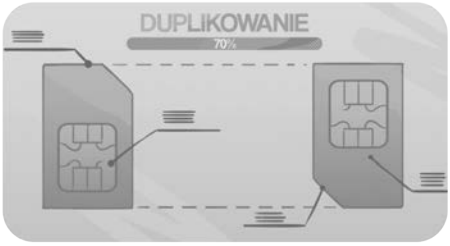
1.6. Szukanie dziury w całym — exploit

Exploit — jest to rodzaj oprogramowania[6], które wykorzystuje luki w zabezpieczeniach systemów operacyjnych lub oprogramowaniu używanym przez użytkownika. Pozwala przejąć kontrolę nad urządzeniem i uzyskać pełne prawa jego administratora. Podobnie jak w przypadku malware, potencjalna ofiara jest zachęcana do instalacji aplikacji, która po zainstalowaniu będzie umiała te luki wykorzystać. Infekcja może też odbywać się poprzez odwiedzenie stron internetowych posiadających skrypty z odpowiednio przygotowanym kodem, który pozwoli na przejęcie uprawnień administratora.

[6] *https://gdata.pl/przewodnik/exploit-co-to-jest*

- **Zero-day** — przykład exploita; oprogramowanie, które ma na celu zaatakowanie luki w programie czy w systemie, która do tej pory nie została wykryta i załatana. Nazwa pochodzi od tego, że twórca takiego oprogramowania nie miał czasu (0 dni) na „załatanie" tego wrażliwego punktu, ponieważ nie był świadomy jej istnienia. Każdy program przechodzi szereg testów, które sprawdzają go pod kątem funkcjonalności (czy rzeczywiście wykonuje czynności, do których został stworzony) oraz bezpieczeństwa (czy żadne dane użytkownika nie wycieką z urządzenia i nikt nie będzie miał do nich dostępu). Niestety, nie zawsze uda się wychwycić wszystkie błędy i aplikacja może być podatna na ataki hackerów.

1.7. Klonowanie — SIM swap



SIM swap — jest to atak polegający na uzyskaniu numeru telefonu ofiary. Przechwycenie numeru pozwala na odbieranie SMS-ów, które często są wykorzystywane do przesyłania kodów autoryzujących transakcje bankowe lub kodów będących drugim sposobem uwierzytelniania w różnych serwisach. Atak polega głównie na wyrobieniu duplikatu karty SIM u operatora na podstawie zgromadzonych wcześniej informacji o użytkowniku.

Zadbaj o swoje (cyber)bezpieczeństwo

Żyjemy w coraz bardziej ucyfrowionym świecie. Wszystko, co tylko można przenieść do internetu, przenosimy. W sieci się komunikujemy, oddajemy rozrywce i nauce, robimy zakupy, załatwiamy sprawy urzędowe. Bo tak jest szybciej, taniej, wygodniej. Zwłaszcza że „podręczne centrum operacyjne", czyli smartfon, mamy zawsze ze sobą. Dotąd ta opowieść brzmi jak bajka — niestety, jak każda bajka, i ta ma negatywnego bohatera. Temu na imię złodziej danych. Czyhający na nasze zdjęcia, kontakty, numery kart płatniczych, hasła do banków, poczty, aplikacji społecznościowych czy sklepów internetowych bandyta, który jest w stanie niepokojąco łatwo przeniknąć do oprogramowania przenośnych urządzeń i okraść nas ze wszystkiego, co w nich cenne.

Producenci sprzętu elektronicznego i twórcy stworzonego dla niego oprogramowania opracowują coraz doskonalsze zabezpieczenia przed aktywnością cyfrowych łupieżców. Są one skuteczne, o ile potrafi się z nich odpowiednio korzystać. Na szczęście dotycząca ich wiedza nie jest przeznaczona jedynie dla osób z wykształceniem informatycznym. Jeśli nie jesteś specjalistą w tej dziedzinie, ale chcesz się dowiedzieć, jak bezpiecznie korzystać ze swojego smartfona czy tabletu, ta książka jest dla Ciebie.

- Rodzaje ataków przeprowadzanych przez cyberprzestępców na urządzenia mobilne
- Podstawowe metody zabezpieczania urządzeń oferowane przez dostawców mobilnych systemów operacyjnych
- Użyteczne narzędzia mające na celu ochronę instalowanych i używanych aplikacji
- Zaawansowane rozwiązania zabezpieczające
- Dobre praktyki związane z kupnem i ze sprzedażą urządzenia mobilnego

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-0438-5
9 788328 904385
Cena: 59,00 zł