UKE | Urząd Komunikacji Elektronicznej

we współpracy z

FUNDACJA bezpieczna cyberprzestrzeń

PORADNIK BEZPIECZNEGO KORZYSTANIA Z URZĄDZEŃ MOBILNYCH PODŁĄCZONYCH DO SIECI INTERNET

Warszawa, grudzień 2018 r.

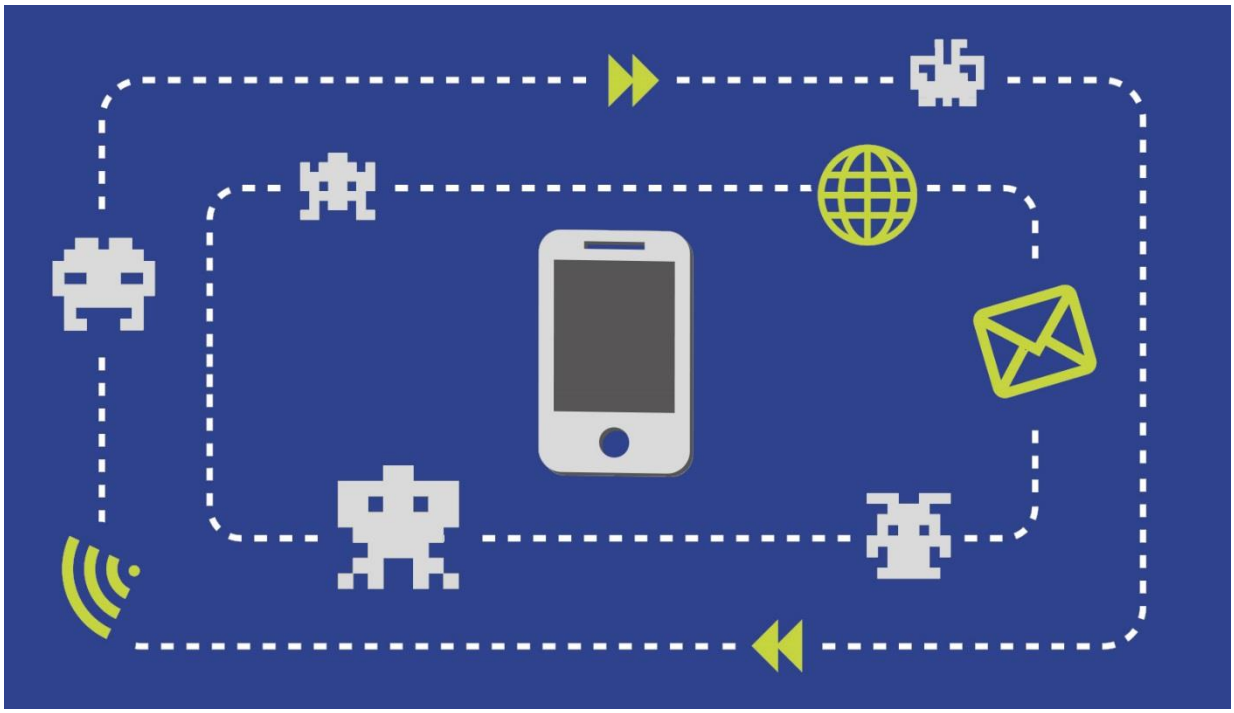
Spis treści

Wstęp

Technologie mobilne w coraz większym stopniu stają się elementem naszego życia codziennego. Z roku na rok moc obliczeniowa urządzeń mobilnych wzrasta, zwiększa się przepustowość przesłanych danych, a ich użytkownicy zyskują dostęp do informacji zawsze i wszędzie, niezależnie od miejsca i czasu. Prezes Urzędu Komunikacji Elektronicznej zauważając coraz większy postęp dostrzega również zagrożenia wynikające z jej korzystania. Stawia to nowe wyzwania przed bezpieczeństwem sieci i usług. Wychodząc naprzeciw nowym wyzwaniom publikuje niniejszy poradnik , który stanowi aktualizację materiału opublikowanego w 2015 roku, a jego niezmienionym celem jest zwiększenie świadomości zasad bezpiecznego korzystania ze środków komunikacji elektronicznej.

Publikowany aktualnie poradnik przeznaczony jest dla szerokiej grupy użytkowników urządzeń mobilnych. Składa się z pięciu rozdziałów. Każdy z nich zawiera najważniejsze informacje dotyczące bezpieczeństwa urządzeń podłączonych do Internetu. Podręcznik zawiera liczne przykłady, w których opisane są najczęstsze i potencjalne zagrożenia związane z korzystaniem z urządzeń mobilnych. Ponad to można w nim odnaleźć możliwe do zastosowania zabezpieczenia oraz dobre praktyki rekomendowane użytkownikom, które w łatwy sposób pomogą zrozumieć zasady bezpiecznego korzystania z urządzeń oraz ich praktyczne zastosowanie.

Z uwagi na ciągły rozwój technologii, pojawianie się nowych wyzwań i zagrożeń w cyberprzestrzeni Prezes UKE widzi potrzebę kontynuowania tej formy informowania konsumentów. Licząc na współpracę we współtworzeniu kolejnych wydań poradnika zachęcamy do przesyłania swoich sugestii i uwag do już opublikowanego materiału oraz propozycji tematów do ewentualnego wykorzystania w przyszłości na adres email: uke@uke.gov.pl z tytułem maila „Zagrożenia dla urządzeń mobilnych – uwagi”.



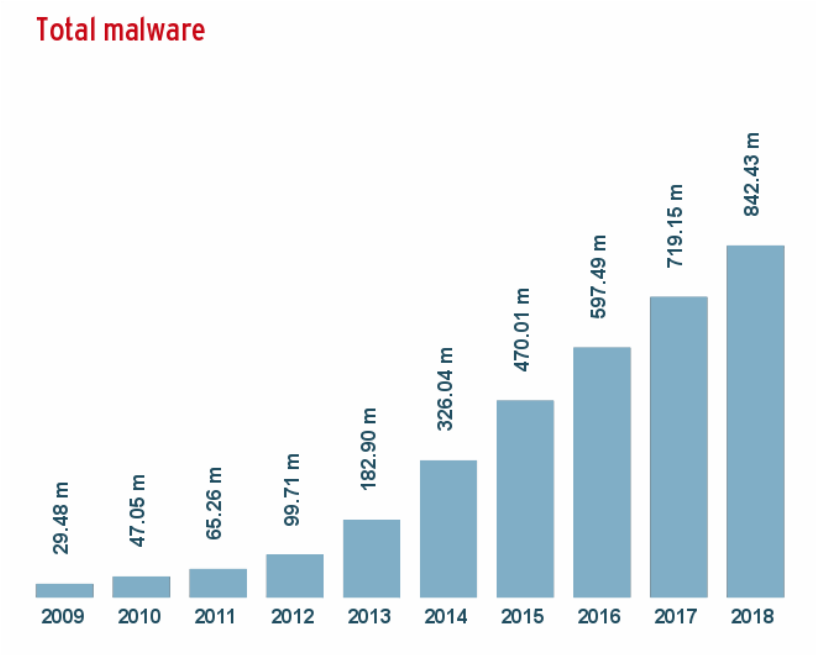
1 Ogólna charakterystyka zagrożeń dla urządzeń mobilnych

Urządzenia mobilne z całą pewnością w ciągu ostatnich kilku lat niezwykle zyskały na popularności. Ich wprowadzenie zrewolucjonizowało możliwości dostępu do danych własnych i zewnętrznych. Stało się to możliwe praktycznie w dowolnym momencie i niemalże w każdym miejscu. Tę rewolucję w dobrym stopniu charakteryzują liczba użytkowników aktywnie korzystających z bankowości mobilnej, która wynosiła w czerwcu 2018 roku- 10 mln osób.[1]

Oprócz wspomnianej usługi bankowości mobilnej innymi bardzo popularnymi usługami, z których korzystają właściciele urządzeń mobilnych jest poczta elektroniczna, media społecznościowe, przeglądanie stron internetowych oraz korzystanie z możliwości robienia zakupów online.

Niestety wraz z masowym korzystaniem z urządzeń mobilnych systematycznie wzrasta ryzyko związane z zagrożeniami sieciowymi. W szczególny sposób wzrasta liczba złośliwego oprogramowania, które cyberprzestępcy tworzą i wykorzystują do naruszania bezpieczeństwa urządzeń mobilnych. Trendy pokazujące to zjawisko wskazują na kilkukrotny wzrost rocznie, a z roku na rok mamy do czynienia z rekordowymi liczbami złośliwych aplikacji na urządzenia mobilne.

[1] Strona źródłowa, Bankier.pl



Rysunek 1 - Liczba złośliwych programów (ang. malware) w latach 2009 - 2018 (źródło AV-TEST GmbH)[2]

Poniżej znajduje się kilka przypadków, które charakteryzują często spotykane sytuacje związane z naruszeniem bezpieczeństwa urządzeń mobilnych i konsekwencje z tym związane.

Przypadek 1 – Atak na użytkownika bankowości mobilnej

Pan Adam otrzymał niepokojącego powiadomienie na swoim smartfonie z aplikacji banku. Otwierając je odczytał wiadomość jakoby jego konto zostało zablokowane. Zapoznał się z całą wiadomością i szczegółowo prześledził przesłaną instrukcję odblokowania konta bankowego. Zależało mu aby jak najszybciej odblokować konto, gdyż tego samego dnia miał wyjechać z rodziną na wakacje. Zdenerwowany podał swój login i hasło a następnie przeszedł do wpisania kodu jednorazowego z karty bądź tego przesłanego przez SMS. Pan Adam przeszedł cały proces i odetchnął z ulgą, gdyż będzie mógł bez problemu korzystać ze środków pieniężnych zgromadzonych na swoim koncie. Zdziwił się jednak, że z jego konta zniknęła pokaźna suma pieniędzy.

Przypadek 2 – Instalacja certyfikatu bezpieczeństwa

Pani Ewa od wielu lat była aktywną użytkowniczką konta w swoim banku. Jako osoba aktywna zawodowo chętnie korzystała z tego dobrodziejstwa, płacąc w ten sposób praktycznie wszystkie rachunki i wykonując inne operacje finansowe. Czasami również robiła to ze swojego komputera stacjonarnego. Właśnie

[2] Strona źródłowa Av-test

w trakcie korzystania z komputera w domu zauważyła mail przysłany z banku z informacją o ważnym komunikacie bezpieczeństwa. Informacja odsyłała ją do strony internetowej banku. Kliknęła na link i została przekierowana na tę stronę. Na stronie wyświetlony był komunikat: „Poprawiamy bezpieczeństwo naszego banku. Dlatego przygotowaliśmy dla Ciebie specjalny certyfikat bezpieczeństwa, który zapewni bezpieczeństwo Twoich transakcji w Internecie. Instalacja certyfikatu nie jest obowiązkowa, jednak w przypadku rezygnacji z jego instalowania bank nie ponosi odpowiedzialności za fałszywe transakcje, które są związane z atakami w Internecie. ”Panią Ewę nie trzeba było drugi raz namawiać, tym bardziej że od dłuższego czasu słyszała różne historie o włamaniach na konta bankowe w Internecie. W odpowiednim miejscu wybrała wersję swojego systemu na telefonie komórkowym i podała nr telefonu. Po chwili otrzymała SMS-a z linkiem do certyfikatu. Kliknęła i zainstalowała certyfikat.

Wszystko działało poprawnie. Niestety po kilku dniach, przeglądając swoje transakcje na koncie bankowym, zauważyła kilka przelewów o wysokości 1000 złotych każdy. Pieniądze zostały przesłane na dwa nieznane jej konta bankowe. Wszystkie one teoretycznie wymagały kodu potwierdzenia transakcji, które to kody Pani Ewa zazwyczaj otrzymywała SMS-em na swój telefon. Tym razem takich SMS-ów nie otrzymała.

Przypadek 3 – Aplikacja do edytowania zdjęć

Pani Agnieszka prowadzi profil swojej firmy w mediach społecznościowych. Spędza dużo czasu w sieci, aby wypromować swoje produkty. Ważne jest dla niej aby dodawane zdjęcia i filmy były jak najbardziej atrakcyjne wizualnie. Dlatego na jednej ze stron poświęconych kolekcjonowaniu materiałów wizualnych dostrzegła informacje o nowej aplikacji przeznaczonej do edytowania zdjęć. Pani Agnieszka ściągnęła ją na swój smartfon i uruchomiła. Aplikacja przy pierwszym użyciu wskazała na konieczność aktualizacji. Pani Agnieszka wykonała ją, chcąc jak najszybciej zaspokoić swoją ciekawość i edytować zdjęcia, które zrobiła tego samego dnia. Niestety gdy aplikacja dokonała aktualizacji ekran jej smartfona zablokował się. Pani Agnieszka wprowadziła kod odblokowania. Kod ten nie zadziałał. Na smartfonie wyświetlił się komunikat, że na telefonie wykryto nielegalne treści w postaci zdjęć pornograficznych i z tego powodu na właściciela telefonu nałożona została kara w wysokości 500 zł. Dopiero po jej wpłaceniu udało się odzyskać dostęp do telefonu przez Panią Agnieszkę.

Przypadek 4 – Telefon z nieznanego sklepu

Dla Pana Konrada najwygodniejszą metodą zakupów są zakupy poprzez internetowe sklepy. Wychodzi on z założenia że może tam znaleźć wszystkie szczegółowe informacje na temat danego produktu a co więcej może znaleźć najlepszą ofertę dzięki dostępności porównywarek cen. Szczególnie jeżeli planuje zakup sprzętu elektronicznego którego wachlarz ofert jest bardzo szeroki. W jednym ze sklepów internetowych znalazł upragniony telefon w znacznie niższej cenie niż w innych sklepach. Po zapoznaniu się z opisem

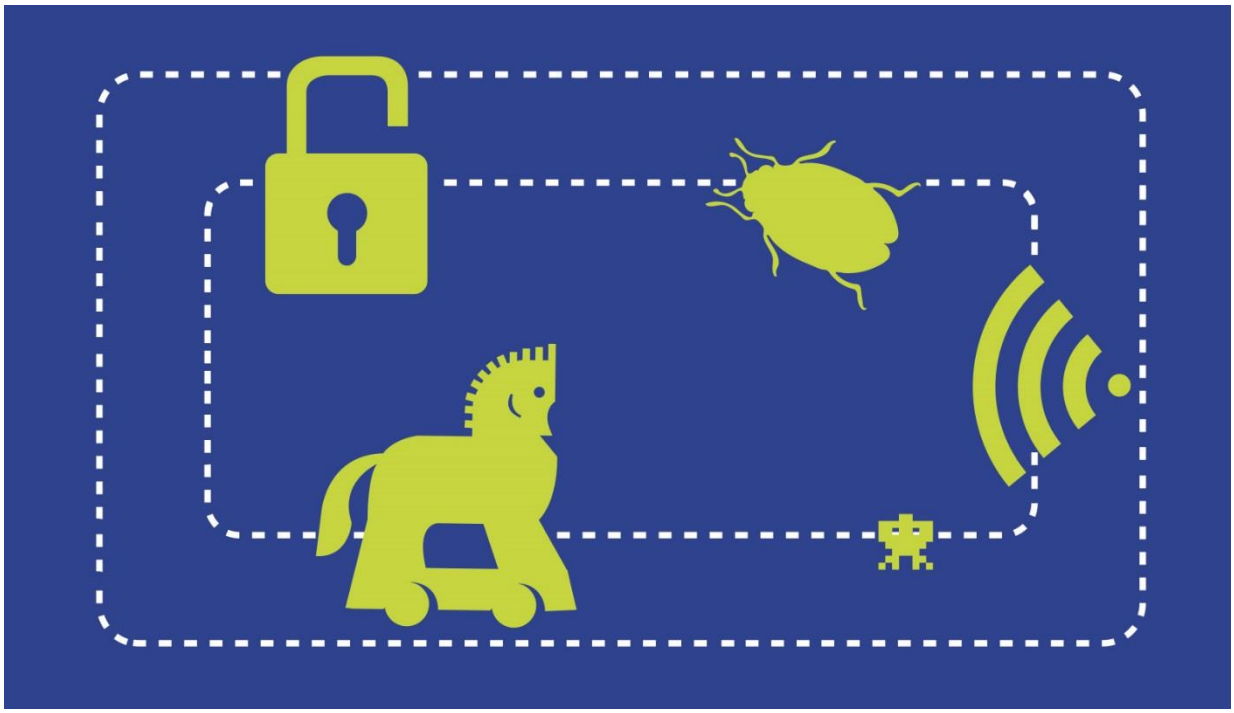
telefonu, mimo że nigdy wcześniej nie słyszał o danym sklepie, postanowił zakupić smartfon- taka okazyjna cena nie pojawia się często. Po kilku dniach użytkowania nowego telefonu okazało się że odnotowano utratę środków z karty kredytowej. Niestety środków tych nie wykorzystał Pan Konrad.

Przypadek 5 – Olbrzymi rachunek za SMS-y

Pani Agata była zafascynowana swoim nowym smartfonem. Dzięki szybkiemu procesorowi, dużemu ekranowi i fantastycznej ergonomii urządzenia, mogła jeszcze bardziej rozwijać swoją pasję, jaką było korzystanie z różnych technik poprawiających organizacji pracy. Dowiedziała się jednak od kolegi z pracy, że na smartfony, tak samo jak na komputery stacjonarne są wirusy, które mogą stać się prawdziwym problemem. Dlatego jeszcze tego samego dnia kiedy to usłyszała, zainstalowała na swoim smartfonie program antywirusowy. Do szybkiego załatwienia sprawy jeszcze bardziej skłonił ją fakt, że program wyglądał na profesjonalny, zresztą od razu wykrył kilka zagrożeń, i w dodatku był za darmo.

Mniej przyjemny był fakt, że kiedy po kilkunastu dniach otrzymała miesięczną fakturę za usługi telefoniczne, zobaczyła że jest ona o kilkaset złotych wyższa niż zazwyczaj. Sprawdziła dokładnie przyczynę wzrostu kosztów. Z informacji od operatora wynikało, że Pani Agata w ciągu ostatnich dwóch tygodni wysłała kilkadziesiąt SMS-ów premium, o podwyższonej opłacie.

„Powyższe przykłady to kilka typowych historii, które zdarzają użytkownikom urządzeń mobilnych, a które związane są zagrożeniami w Internecie, przy korzystaniu z takich urządzeń. Skonfrontuj je ze swoimi doświadczeniami i doświadczeniami swoich znajomych. Być może odnajdziesz opisy podobnych zdarzeń. Spróbuj je na nowo przemyśleć i zapoznaj się dokładnie z zamieszczonymi w dalszej części poradnika opisami mechanizmów ataków stosowanych przez cyberprzestępców, skutkami tych ataków i najważniejszymi metodami obrony przed nimi.”



2. Najważniejsze zagrożenia dla urządzeń mobilnych podłączonych do sieci Internet

Użytkownik urządzeń mobilnych narażony jest na zagrożenia, które mają różny charakter w zależności od cyklu użytkowania tego urządzenia. W tym rozdziale można znaleźć kilka najistotniejszych informacji związanych z zagrożeniami w poszczególnych fazach użytkowania urządzenia mobilnego.

2.1 Zakup

Sprawy związane z bezpiecznym użytkowaniem urządzenia mobilnego zaczynają się praktycznie już od momentu jego zakupu. Bardzo dużo osób dokonuje wyboru urządzenia w oparciu o zasłyszane, a jeszcze częściej przeczytane, opinie. Warto tę dobrą praktykę zastosować również w odniesieniu do spraw bezpieczeństwa, choć w tym wypadku chodzi głównie o opinie dotyczące źródła pochodzenia zakupywanego sprzętu.

Przy zakupie urządzenia powstają ryzyka:

- zakupu nielegalnego urządzenia
- zakupu uszkodzonego urządzenia
- zakupu urządzenia zainfekowanego wirusem

2.1.1 Jak się bronić?

W naturalny sposób ryzyko zakupu urządzenia, które może sprawić nam kłopoty, związane jest z zakupem sprzętu używanego. Dlatego warto sprawdzić źródło, próbując ustalić reputację sprzedawcy, sprawność urządzenia i legalność pochodzenia towaru. Prostym sposobem na to jest skorzystanie z systemów rankingu sprzedawcy na serwisach aukcyjnych i w ogóle w Internecie, przy wykorzystaniu wyszukiwarki. Proste wyszukiwanie „[nazwa sprzedawcy] opinie" lub „[nazwa sprzedawcy] uwaga oszustwo", powinny w większości przypadków zidentyfikować próbę oszustwa przy sprzedaży sprzętu.

Sprawność urządzenia używanego najpewniej sprawdzimy w przypadku odbioru osobistego urządzenia. Mimo różnych systemów ochrony konsumenta i regulaminów serwisów gdzie odbywa się sprzedaż, to nadal najpewniejszy sposób. Przy zakupie urządzenia o znacznej wartości i braku możliwości zweryfikowania sprzedawcy, to zdecydowanie najlepszy sposób, który jest unikany przez nieuczciwych kontrahentów, co można wykorzystać sprawdzając chociażby gotowość do tej formy sprzedaży. Dodatkowymi sposobami zwiększenia bezpieczeństwa, w szczególności w kontekście legalności posiadania sprzętu przez sprzedającego, jest oczywiście możliwość otrzymania oryginalnej faktury zakupu, na której podano numer seryjny urządzenia.

Z punktu widzenia technicznego, aby maksymalnie zredukować ryzyko posiadania zawirusowanego sprzętu, należy zdecydować się na wyczyszczenia zawartości urządzenia mobilnego. Poniżej zamieszczone są informacje jak to zrobić w najbardziej popularnych systemach iOS i Android[3].

iOS (iPhone/iPad)

Aby wyczyścić zawartość urządzenia od Apple, należy wykonać następujące kroki:

1. Wejść do **Ustawień**, wybrać zakładkę **Ogólne** i **Wyzeruj**.
2. Tutaj ukaże się nam kilka opcji, lecz jeśli zależy nam na całkowitym wyczyszczeniu urządzenia, wybieramy drugą - **Wymarz zawartość i ustawienia**.
3. System zapyta nas czy nie chcemy uaktualnić kopii zapasowej. Warto rozważyć tę opcję, jeśli nie zrobiliśmy tego wcześniej. Zachowamy wtedy nasze prywatne pliki, np. zdjęcia. Jeżeli już jesteśmy pewni, że nasze dane są zapisane w chmurze, wybieramy opcję **Wymaż teraz**.

[3] poradnik zawiera instrukcje konfiguracyjne dla dwóch najbardziej popularnych w Polsce systemów operacyjnych dla platform mobilnych – Android i iOS, których sumaryczny udział w rynku wynosi ponad 90% - Strona źródłowa Mobirank

4. Po akceptacji i wpisaniu hasła do konta Apple, urządzenie się zrestartuje i po kilku minutach powita nas ekran konfiguracji.
5. Wskazówka! Jeśli masz inne urządzenie od Apple, przy konfigurowaniu nowego urządzenia, wystarczy zbliżyć do „stare" urządzenie. Wówczas urządzenia synchronizują się.

Jeśli urządzenie mobilne nie odpowiada, można również przeprowadzić ten proces poprzez program **iTunes** na komputerze PC (Windows) lub Mac. Procedura również nie należy do skomplikowanych:

1. Należy podłączyć kablem USB nasze urządzenie razem z komputerem.
2. Po uruchomieniu programu **iTunes** i po wykryciu naszego urządzenia, pojawią się opcje z nim związane - wybieramy guzik **Odtwórz**.
3. Po akceptacji działań i ewentualnym pobieraniu najnowszej wersji oprogramowania (w przypadku nieaktualnego systemu operacyjnego), urządzenie przystąpi do procedury resetu i po kilku minutach ukaże się ekran konfiguracji.

Android

Na każdym urządzeniu pod kontrolą systemu Android, procedura ta, w zależności od konkretnego typu i producenta urządzenia może wyglądać nieznacznie inaczej. Oto jak wygląda standardowy proces resetu urządzenia mobilnego:

1. Należy wejść do Ustawień, wybrać opcję **Kopia i kasowanie danych** i następnie **Ustawienia fabryczne**.
2. Należy potwierdzić działanie wybierając opcję **Resetuj telefon/tablet**, a potem **Usuń wszystko**.
3. Po restarcie, trzeba poczekać kilka minut i ukazuje się czysty system operacyjny.

2.2 Użytkowanie

Największe ryzyko rodzi oczywiście użytkowanie urządzeń mobilnych. Są to zarówno ryzyka fizyczne, takie jak kradzież urządzenia, jak i teleinformatyczne, związane z działaniem systemów operacyjnych i ich naruszeń bezpieczeństwa. Szczegółowe informacje na temat ryzyka teleinformatycznego wraz z informacjami na temat środków bezpieczeństwa, można znaleźć w rozdziale 4.

Zagrożenia i zabezpieczenia dla kluczowych funkcji urządzeń mobilnych.

2.2.1 Porady jak się bronić – podstawowe zasady

Najważniejsze porady ograniczające ryzyka powstałe w wyniku fizycznej utraty urządzenia:

- nie pozostawiaj urządzenia bez nadzoru. Nie chodzi tylko o kradzież urządzenia, ale również wystawienie go na ryzyko nieuprawnionego dostępu przez osoby trzecie
- zawsze stosuj ustawienia związane z blokadą klawiatury. Twój kod blokady nie powinien być trywialny, tak samo w przypadku kodu cyfrowego, jak i wzoru blokady
- w sytuacjach kiedy nie używasz urządzenia mobilnego staraj się wyłączać jego dostęp do sieci. Nie tylko oszczędzi to baterię urządzenia, ale również zmniejszy ryzyko ataków
- spisz i zachowaj w bezpiecznym miejscu nr seryjny swojego urządzenia oraz nr IMEI – indywidualny numer identyfikacyjny Twojego urządzenia
- skorzystaj z opcji „zabezpieczenia” i wpisz informację o osobie, z którą ma się skontaktować znalazca Twojego urządzenia
- skorzystaj z funkcji lokalizacji swojego urządzenia. Taka funkcja jest dostępna bezpośrednio w systemie iOS i Android (patrz instrukcja poniżej)

Poniżej znajduje się instrukcja jak skorzystać z funkcji wyszukiwania urządzenia mobilnego w systemach iOS i Android.

iOS (iPhone/iPad)

Apple w swoich urządzeniach wbudowało darmową usługę „Znajdź mój iPhone" - jest ona domyślnie włączona po zalogowaniu się do konta Apple na urządzeniu.

Co więc się stanie, gdy nasz telefon przepadnie lub zostanie ukradziony? Producent daje nam cztery możliwości:

- zdalną lokalizację urządzenia na mapie
- zdalne odtworzenie dźwięku (nawet przy trybie wyciszonym) w celu lokalizacji położenia
- zdalne włączenie kodu blokady ekranu wraz z informacją na jaki telefon/adres ma się skontaktować potencjonalny znalazca – jest to „tryb utracony"
- zdalne wymazanie wszystkich danych na telefonie

Ponadto, Znajdź mój iPhone informuje nas też o stanie baterii. Jeśli korzystasz z usługi „Chmury rodzinnej", powyższe czynności możesz także wykonać na urządzeniach członków Twojej rodziny. Pamiętaj, że wyczyszczenie danych należy stosować w ostateczności, aby nasze prywatne dane nie zostały wykradzione. Należy się wtedy upewnić, czy na pewno mamy kopię zapasową danych.

UWAGA: aby wymienione opcje działały, nasze zgubione urządzenie musi być połączone z siecią komórkową bądź siecią Wi-Fi.

Wszelkie te czynności możemy uzyskać z poziomu strony iCloud bądź też po pobraniu aplikacji „Find my iPhone" na inny telefon w systemie iOS po uprzednim zalogowaniu.

Android

Urządzenia pracujące pod kontrolą Androida mają wbudowaną usługę Android Device Manager**,** która uaktywnia się automatycznie, gdy zalogujemy się na naszym telefonie/tablecie do wcześniej założonego konta Google. Dzięki niej uzyskujemy możliwość zdalnej lokalizacji telefonu, bądź też odtworzenia nań dźwięku w celu lokalizacji położenia.

Aby uzyskać dostęp do dwóch dodatkowych opcji:

- zdalnego włączenia kodu blokady ekranu.

- oraz zdalnego wyczyszczenia wszystkich danych na telefonie

należy wejść do Ustawień, wybrać opcję Google, Bezpieczeństwo następnie Znajdź moje urządzenie i upewnić się, czy usługa jest włączona.

Wszelkie czynności związane ze zdalnym dostępem do lokalizacji i funkcji telefonu możemy uzyskać poprzez wejście na adres Google Android.

2.3 Sprzedaż

O bezpieczeństwie urządzenia, a tak naprawdę także o zgromadzonych na nim danych, warto pamiętać również w momencie jego sprzedaży. Nie dopuśćmy do tego, aby w rękach przyszłego właściciela znalazły się poza samymi urządzeniami archiwa plików, kontakty i inne dane, które na nim przetrzymywaliśmy w okresie użytkowania, jak również dane przechowywane w aplikacjach z których korzystaliśmy – lokalnie i zdalnie poprzez funkcje łączenia się aplikacji z danymi zewnętrznymi.

2.3.1 Porady jak się bronić – podstawowe zasady

Najważniejsze zasady bezpieczeństwa w sytuacji sprzedaży urządzenia mobilnego:

- minimum bezpieczeństwa to usunąć dane kontaktowe, maile, dokumenty, zdjęcia i inne archiwa własne oraz aplikacje, które sami instalowaliśmy na telefonie
- przywrócić fabryczne ustawienia urządzenia mobilnego, a najlepiej zainstalować system od nowa. Warto zainstalować najnowszą wersję, tym samym przyczynimy się do poprawy bezpieczeństwa następnego użytkownika urządzenia mobilnego
- usunąć trwale dane przechowywane na urządzeniu mobilnym. Warto wiedzieć, że proste usunięcie danych, nie wiąże się z definitywnym ich usunięciem z pamięci urządzenia. Tak usunięte dane można przywrócić z pomocą specjalnych programów

3. Zagrożenia i zabezpieczenia dla kluczowych funkcji urządzeń mobilnych

Poniżej znajdują się informacje na temat największych zagrożeń związanych z użytkowaniem urządzeń mobilnych. Są one przedstawione w układzie:

Mechanizm zagrożenia

Skutki jego wystąpienia

Porady dotyczące zmniejszenia ryzyka

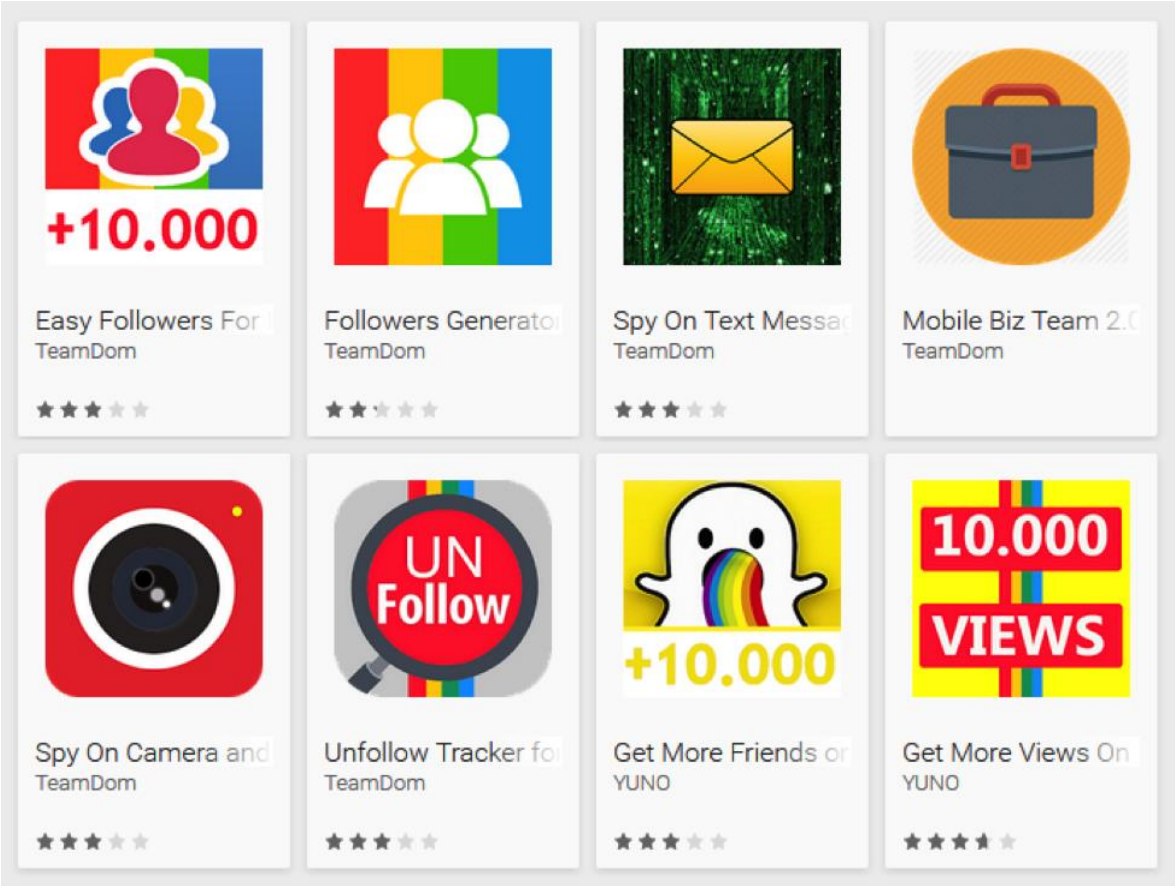
Odpowiednim częściom towarzyszą wskazane powyżej ikony ułatwiające nawigację. Warto zapoznać się ze wszystkimi zagrożeniami i zastosować zaproponowane porady.

W każdej kategorii wskazywane jest jedno charakterystyczne dla niej zagrożenie. Warto jednak pamiętać, że w praktyce bardzo często występują różne wektory ataków. Nawet w przypadku dominującej funkcjonalności, takiej jak np.: przechwytywanie SMS-ów, blokowanie dostępu czy szyfrowanie zasobów, pojawiają się inne, np.: służące do dołączenia przejętego urządzenia do sieci botnet.

3.1 Dostęp do urządzenia mobilnego

3.1.1 Mechanizm zagrożenia związany z instalacją złośliwego oprogramowania

Dostęp do urządzenia mobilnego może nastąpić w wyniku działania złośliwego oprogramowania lub przełamania zabezpieczeń ograniczenia dostępu. W większości przypadków tego typu atak zawiera elementy socjotechniczne, tzn. użytkownik urządzania jest namawiany do wykonania czynności, które w konsekwencji mogą się obrócić przeciwko niemu. Może to być na przykład namówienie do instalacji niebezpiecznej aplikacji, czy udzielenie zgody na dostęp do danych zgromadzonych na telefonie (np.: kontaktów, zdjęć, itp.). Najbardziej popularnym wektorem ataku w wyniku którego dochodzi do nieautoryzowanego dostępu do urządzenia mobilnego jest doprowadzenie do instalacji złośliwego oprogramowania w wyniku kliknięcia na link znajdujący się na stronie www, w wiadomości SMS lub w poczcie elektronicznej. Złośliwe oprogramowanie bardzo często ukrywa się lub jest częścią gier albo programów „zapewniających" bezpieczeństwo (np.: programów antywirusowych).



Rysunek 2 - Przykłady fałszywych aplikacji usuniętych z Google Play (źródło: Eset)[4]

3.1.2 Skutki ataku

[4] Strona źródłowa Welivessecurity.com

W wyniku instalacji złośliwego oprogramowania może dojść do wielu negatywnych skutków związanych z uruchomieniem jego funkcji. Najczęściej pojawiające się skutki to:

- wykonywanie działań szpiegowskich w postaci uruchamiania skanera klawiatury, wykonywania zdjęć wbudowanym aparatem, nagrywania filmów wbudowaną kamerą
- wykradanie kodów autoryzujących transakcje elektroniczne, a w szczególności kodów zatwierdzeń operacji bankowych
- wysyłanie nieautoryzowanych wiadomości SMS na numery premium i generowanie w ten sposób wysokich kosztów abonamentu

3.1.3 Porady jak się bronić

Aby bronić się przed próbami dostępu do urządzeń mobilnych warto zastosować następujące zasady:

- ograniczyć prawa dostępu do aplikacji i danych
- stosować oryginalne wersje systemów operacyjnych (rezygnacja z jailbreak - procesu usuwania ograniczeń systemowych narzuconych przez Apple)
- ustawić kody dostępu do telefonu w postaci cyfrowej, interfejsu graficznego, uwierzytelnienia biometrycznego (np. odcisk palca, rozpoznawanie twarzy)

3.2 Archiwa z dokumentami oraz zdjęciami i ważnymi informacjami

3.2.1 Mechanizm zagrożenia związany z instalacją oprogramowania typu ransomware

Urządzenia mobilne, ze względu na wygodę i możliwość natychmiastowego dostępu do informacji, stały się w praktyce podręcznym archiwum istotnych zasobów. Niestety rodzi to ze sobą duże ryzyko przejęcia lub utraty tych informacji. Tak może stać się poprzez ingerencję fizyczną (zguba, kradzież, nieuprawniony chwilowy dostęp) lub techniczną – poprzez cyberatak.

Jednym z najbardziej powszechnych metod naruszenia bezpieczeństwa zasobów składowanych na urządzeniu mobilnym, jest tzw. ransomware. Czyli oprogramowanie instalowane na urządzeniu przez cyberprzestępców, którego zadaniem jest wymuszenie okupu od użytkownika w zamian za przekazanie hasła do odszyfrowania zasobów, wcześniej zaszyfrowanych przez to złośliwe oprogramowanie lub odblokowania wygaszacza ekranu. W obydwu sytuacjach użytkownik, aby pozbyć się problemu jest zmuszany do realizacji opłaty. Wprowadza to dodatkowe ryzyko, gdyż ta opłata może być realizowana z wykorzystaniem karty kredytowej, co w oczywisty sposób daje szansę cyberprzestępcom na przejęcie danych takiej karty.

3.2.2 Skutki ataku

W wyniku ataku typu ransomware użytkownik traci dostęp do swoich danych w postaci zdjęć, dokumentów, czy danych składowanych w aplikacjach (np.: notatki, zapiski, informacje o spotkaniach). Może również stracić dostęp do całego urządzenia.

Warto zwrócić uwagę, że przy zadziałaniu programu typu ransomware możemy również utracić dostęp do bardzo krytycznego zasobu jakim jest repozytorium naszych haseł. Wielu użytkowników przechowuje swoje hasła. Przy blokadzie dostępu do nich w praktyce mogą utracić dostęp nie tylko do zasobów na telefonie, ale również do wielu zasobów sieciowych.

3.2.3 Porady jak się bronić

Obronę przed atakami typu ransomware możemy podzielić na prewencyjną i reakcyjną. Od strony prewencyjnej najistotniejsze jest aby wykonywać stałą archiwizację danych. Poniższa instrukcja zawiera podstawowe informacje, jak dokonać archiwizacji danych w najbardziej popularnych systemach.

Jeśli chodzi o reakcję na problem, który się pojawia w wyniku ransomware to nie ma jednej, uniwersalnej, skutecznej techniki pozbycia się ransomware, a tym bardziej odzyskania dostępu do danych i telefonu. W zależności od sytuacji następujące czynności powinny być pomocne:

- powtórne uruchomienie telefonu w bezpiecznym trybie (ang. „Safe Mode") i próba usunięcia złośliwego oprogramowania. Ta czynność jest szczególnie istotna przy ataku prowadzącym do blokowania ekranu
- usunięcie złośliwego oprogramowania. W sytuacji możliwości dostępu do aplikacji i pozyskania wiedzy na temat tego, które oprogramowanie spowodowało problem, należy je po prostu usunąć. Jeśli dostęp do aplikacji nie jest możliwy, ze względu na szybką blokadę ekranu, to trzeba skorzystać ze sposobu opisanego w punkcie powyżej. Do usuwania złośliwego oprogramowania wykorzystywane są również specjalne programy (rozdział 5 Przydatne linki))
- kluczowe jest wykonanie backupu. Poniżej znajdują się informacje jak to zrobić w systemach Android i iOS

iOS (iPhone/iPad)

Użytkownicy rozwiązań firmy Apple mają 2 możliwości:

- backup w chmurze, czyli na dysku internetowym (iCloud). Po włączeniu tej opcji (domyślnie jest ona aktywna) codziennie w nocy, gdy nasze urządzenie będzie w stanie spoczynku, zostanie wykonana kopia zapasowa. Pamiętaj jednak, że w zależności od wybranego pakietu, chmura obliczeniowa ma również swoje ograniczenia. Musisz sam zdecydować jak duże są Twoje potrzeby;
- jeśli wolimy przetrzymywać dane lokalnie (ta opcja jest bezpieczniejsza i rekomendowana), istnieje taka możliwość, poprzez program iTunes na komputerze PC (Windows) lub Mac. Wystarczy, że po podłączeniu urządzenia kablem USB do komputera, otworzymy wspomniany program i wybierzemy opcję „Archiwizuj". Realizując tę opcję wychodzimy też naprzeciw problemowi ograniczonego pakietu danych w ramach iCloud.

Android

Tutaj sytuacja jest trochę bardziej skomplikowana, głównie ze względu na fragmentację tego systemu. Istnieją jednak 3 możliwości, które powinny być uniwersalne dla większości telefonów:

- google backup - tą opcję znajdziemy raczej na nowszych wersjach systemu Android. Jest ona dostępna w głównych ustawieniach systemu i umożliwia przesyłanie danych na dysk internetowy Google przypisany do naszego konta. Ta metoda zachowuje wszystkie ustawienia telefonu oraz dane aplikacji
- backup przez aplikację, czyli kopia zapasowa przy użyciu specjalnego programu do tego przeznaczonego. Wszystko odbywa się z poziomu telefonu, a same pliki zapasowe są zapisywane na karcie pamięci. Przykładem tego typu aplikacji jest **Easy Backup & Contacts Export and Restore** - prosty w użytkowaniu program, który wykonuje całą pracę za nas
- backup na komputer (ta opcja jest najbezpieczniejsza i rekomendowana) – ,polegający na podłączeniu urządzenia do telefonu i przekopiowaniu wszystkich folderów w pamięci urządzenia oraz na karcie pamięci do nowego folderu na naszej maszynie

Oprócz tego, każdy producent telefonów z systemem Android (Samsung, HTC, etc.) posiada swoje własne rozwiązania do tworzenia kopii zapasowych, z którymi należy się zapoznać na stronie producenta.

3.3 Operacje bankowości elektronicznej

3.3.1 Mechanizm zagrożenia związany z instalacją oprogramowania atakującego bankowość elektroniczną

W związku z tym, że urządzenia mobilne są coraz częściej używane do korzystania

z usług bankowości elektronicznej, stały się one bardzo ważnym obiektem zainteresowania cyberprzestępców. Ataki na urządzenia mobilne, które mają za cel naruszenie finansów właściciela urządzenia są przede wszystkim atakami na proces realizacji usługi bankowości elektronicznej, a konkretnie wykonywania przelewu. Szczególnie zagrożeni takimi atakami są klienci tych banków, w których realizacja przelewu przebiega z uwzględnieniem potwierdzenia przelewu za pomocą kodu jednorazowego wysyłanego na urządzenie mobilne klienta banku. Typowy scenariusz związany z tym mechanizmem wygląda następująco:

- komputer klienta banku zostaje zainfekowany złośliwym oprogramowaniem
- w wyniku infekcji, po zalogowaniu się na stronę bankowości elektronicznej, pojawia się komunikat o koniecznej instalacji oprogramowania służącego do ochrony transakcji bankowych, np.: instalacji „certyfikatu bezpieczeństwa", do którego link zostaje przesłany wiadomością SMS na nr podany przez ofiarę i po zaznaczeniu systemu operacyjnego z jakiego korzysta[5]
- po instalacji „bezpiecznego programu/certyfikatu" atakujący w praktyce przejmuje kontrolę nad telefonem. Przede wszystkim potrafi „w tle" przesyłać otrzymywane na ten telefon SMS-y, co umożliwia mu otrzymywanie SMS-ów wysyłanych przez bank, zawierających kody potwierdzeń transakcji

3.3.2 Skutki ataku

Oczywiście wspomniany scenariusz zakłada, że atakującemu już udało się skutecznie zaatakować komputer ofiary i tylko brakuje mu możliwości kontroli nad urządzeniem mobilnym, które stanowi ważny element realizacji transakcji bankowości elektronicznej. Po ataku, atakujący w praktyce kontroluje obydwa kanały realizacji usługi bankowej online. Dzięki temu może realizować nielegalne transakcje na dowolne konta.

3.3.3 Porady jak się bronić

Ataki na klientów bankowości elektronicznej charakteryzują się zaawansowanym zastosowaniem mechanizmów socjotechnicznych. Przygotowywane są przez profesjonalne grupy przestępcze. Dlatego ochrona przed nimi wymaga szczególnego zaangażowania do strony klientów banku. Podstawowe zasady ochrony przed tymi atakami są następujące:

[5] mogą pojawić się inne metody nakłaniające do instalacji, np.: wyświetlony kod QR do zeskanowania telefonem

- kieruj się zdrowym rozsądkiem i nie ulegaj łatwo komunikatom, które zmuszają Cię do natychmiastowego działania na rzecz Twojego bezpieczeństwa, w szczególności jeśli te działania związane są koniecznością instalacji dodatkowego oprogramowania, „certyfikatów bezpieczeństwa" lub namawiają Cię do przekazywania istotnych informacji
- za każdym razem kiedy trafi do Ciebie informacja, która budzi Twoje wątpliwości koniecznie skontaktuj się ze swoim bankiem (np.: poprzez infolinię) i upewnij się czy jest to informacja prawdziwa. To również dobry sposób, aby bank przy Twojej pomocy wykrył nowe zagrożenie i ostrzegł innych klientów
- pobieraj aplikację bankową ze sprawdzonych źródeł. Koniecznie zweryfikuje reputację danej aplikacji
- jeśli posiadasz sprawdzone oprogramowanie antywirusowe, nigdy nie ulegają sugestiom, że ostrzeżenie generowane przez to oprogramowanie może być nieważne

3.4 Oprogramowanie pobierane z Internetu

3.4.1 Mechanizm zagrożenia związany z udzielaniem pozwolenia na dostęp do własnych danych

Jednym z największych dobrodziejstw jakie niesie ze sobą korzystanie z urządzeń mobilnych jest możliwość dostępu do wielu przydatnych programów, niemalże w każdym miejscu i czasie. Środowisko programistów aplikacji mobilnych wytworzyło miliony aplikacji – gier, programów użytkowych, programów pozwalających na dostęp do serwisów sieciowych, bankowości elektronicznej, etc. Niestety wśród tych milionów aplikacji znajduje się setki tysięcy takich, które w jakiś sposób naruszają bezpieczeństwo naszych urządzeń lub znajdujących się na nich danych. Aplikacje takie mogą zainfekować lub naruszyć zasady bezpieczeństwa urządzeń mobilnych w najróżniejszy sposób. Najczęstsze wektory ataków to:

- namówienie do instalacji „atrakcyjnej" gry.
- namówienie do pozwolenia, aby nowo zainstalowana aplikacja uzyskała możliwość dostępu do naszych danych kontaktowych, kalendarza, zdjęć itp.
- namówienie do instalacji oprogramowania pozwalającego do dostępu do usług bankowości elektronicznej.
- namówienie do instalacji oprogramowania „zwiększającego" poziom naszego bezpieczeństwa, najczęściej oprogramowania antywirusowego.

Przykłady tych ostatnich programów to: Virus Shield, Antivirus 360, Personal Antivirus, System Security, Kaspersky Mobile, Eset Nod32 Norton Security. Aktualizowana lista takich programów znajduje się na stronie Wikipedii.

3.4.2 Skutki ataku

Skutki działania złośliwego oprogramowania, oprócz tych szczegółowo opisanych, które związane są z działaniem programów typu ransomware, najczęściej dotyczą prowadzenia szkodliwej działalności szpiegowskiej. Najistotniejsze konsekwencje takich ataków to:

- dostęp do kalendarza i kontaktów
- podsłuch rozmów telefonicznych
- dostęp do wiadomości SMS, w tym przejmowanie tych wiadomości
- śledzenie lokalizacji właściciela urządzenia mobilnego
- dostęp do zdjęć i filmów
- możliwość uruchamiania aparatu i kamery wbudowanych w urządzeniu
- podsłuch otoczenia poprzez funkcję dyktafonu
- wyświetlanie natarczywych reklam

3.4.3 Porady jak się bronić

Jak widać w podanych powyżej przykładach, nazwy programów będących złośliwym oprogramowaniem są łudząco podobne do oryginalnych nazw renomowanych programów zabezpieczających, dlatego instalacja nowego programu zawsze powinna być związana z korzystaniem z w pełni zaufanego źródła, a jeszcze lepiej jeśli towarzyszy temu sprawdzenie opinii o danym programie lub wyszukanie informacji, czy nie jest ono związane z oszustwem. Proste wyszukiwanie według haseł: „[nazwa programu] malware” lub „[nazwa programu] oszustwo”, powinno dać nam szanse na wyłapanie zagrożenia. Ta uwaga szczególnie odnosi się do użytkowników systemu Android. Jego otwarta architektura dystrybucji oprogramowania, która daje wiele możliwości szerokiej i szybkiej dystrybucji nowych aplikacji, również jest systematycznie wykorzystywana przez cyberprzestępców w dystrybucji złośliwego oprogramowania.

3.5 Korzystanie z sieci bezprzewodowych

3.5.1 Mechanizm zagrożenia atakiem z wykorzystaniem fałszywej sieci Wi-Fi

Mechanizmy ataków związanych z sieciami bezprzewodowymi zasadniczo nie różnią się od tych, które dotyczą komputerów osobistych. Problem większego ryzyka związany jest z faktem, że urządzenia mobilne z naturalnych powodów znacznie częściej są wykorzystywane przy dołączaniu się do

nieznanych nam sieci Wi-Fi. W miejscach publicznych dostępnych jest wiele tych sieci, a użytkownicy chętnie z nich korzystają. Takie sieci najczęściej udostępniane są za darmo, posiadają popularne i zachęcające do korzystania nazwy (np.: „Free Wi-Fi", „Free Public WiFi", itp.), albo nazwy kojarzące się z miejscami, w których przebywamy (np.: „Café WiFi", „Airport Free WiFi", itp.).

Po dołączeniu się do takiej sieci atakujący może wykonać bezpośredni atak w postaci instalacji złośliwego oprogramowania. Może do tego wykorzystać na przykład procedurę dołączenia się do sieci, przekonując ofiarę, że aby to się stało, konieczne jest zainstalowanie darmowego programu lub specjalnego certyfikatu. Co gorsze, zaawansowany cyberprzestępca może dokonać takiej infekcji zupełnie bez interakcji z ofiarą.

Inną poważną konsekwencja dołączenia się do sieci bezprzewodowej zestawionej przez cyberprzestępcę jest możliwość całkowitego przejęcia ruchu przechodzącego przez taki punkt dostępowy. Warto pamiętać, że taka możliwość istnieje w praktyce we wszystkich sieciach, nawet tych udostępnianych legalnie, bez przestępczych zamiarów, w sytuacji kiedy ruch obsługiwany przez sieć nie jest ruchem szyfrowanym.

Bardziej zaawansowanym sposobem ataku na użytkowników urządzeń mobilnych, korzystających z sieci GSM, jest stawianie fałszywych stacji bazowych BTS (Base Transceiver Station). Taki atak prowadzi do przejęcia całości komunikacji z urządzenia mobilnego GSM.

3.5.2 Skutki ataku

Są dwa podstawowe skutki ataków na ofiary, które dołączyły się do fałszywych sieci bezprzewodowych:

- instalacja złośliwego oprogramowania na urządzeniu mobilnym
- przejęcie danych wysyłanych przez sieć przez ofiarę

Druga konsekwencja może wystąpić również przy dołączaniu się do sieci Wi-Fi, w których ruch nie jest szyfrowany lub jest szyfrowany słabym protokołem.

3.5.3 Porady jak się bronić

Najważniejsze porady, które powinny uchronić użytkownika od zagrożeń związanych z korzystania z sieci Wi-Fi są następujące:

- najlepszą opcją jest korzystanie z własnej sieci Wi-Fi. Pamiętaj o tym aby była poprawnie i bezpiecznie skonfigurowana[6]. Własna sieć Wi-Fi to zarówno sieć udostępniania przez Twój prywatny router, jak i urządzenie mobilne, poprzez funkcję „Hotspot osobisty" w iOS oraz „Przenośny hotspot Wi-Fi" w Androidzie;
- jeśli pozwala Ci na to Twój abonament to korzystaj z dostępu do sieci oferowanej przez operatora sieci komórkowej (3G, LTE). Postawienie fałszywej stacji BTS nie jest łatwe i takie zagrożenie rzadko występuje
- nie łącz się do sieci Wi-Fi z nieszyfrowanym ruchem. Unikaj protokołu szyfrowania WEP, najlepiej korzystaj tylko z protokołu WPA2, w ostateczności z WPA
- bądź ostrożny przy dołączaniu się do sieci, które mają nazwy sugerujące łatwy i darmowy dostęp, np.: „Free Internet", „Free WiFi Network", „Caffee Free WiFi", „City Free WiFi Internet", itp.
- nie zgadzaj się na instalację żadnego oprogramowania jako warunku skorzystania z darmowej sieci Wi-Fi
- jeśli musisz łączyć się z otwartą siecią, skorzystaj z usług tunelowania ruchu sieciowego (VPN – Virtual Private Network). Pamiętaj jednak, że najskuteczniejsze usługi tego typu należą do płatnych rozwiązań.

3.6 Korzystanie z mediów społecznościowych

3.6.1 Mechanizm zagrożenia

Podobnie jak przy korzystaniu z usług bankowości elektronicznej, również korzystanie z serwisów społecznościowych, w coraz większym stopniu jest realizowane z wykorzystaniem urządzeń mobilnych. Zagrożenia przy korzystaniu z urządzeń mobilnych w pełni pokrywają, te które dotyczą komputerów osobistych[7]. Co więcej, ograniczony sposób kontroli przetwarzania informacji w urządzeniach mobilnych, spowodowany chociażby mniejszymi rozmiarami ekranów urządzeń mobilnych, zwiększa ryzyko nierozważnego kliknięcia niebezpiecznego linku, czy wyrażenia zgody na dostęp do danych. Oprócz tych powtarzających się zagrożeń, przy korzystaniu z urządzeń mobilnych w szczególny sposób pojawia się dodatkowe, polegające na ujawnianiu własnej lokalizacji. Dzieje się tak przy włączonych usługach geolokalizacji, pozwalającej na to, aby informacja o naszym bieżącym miejscu przebywania była dostępna dla innych.

[6] Przeczytaj artykuł "Zabezpiecz swoją sieć WiFi. Kompleksowy poradnik.

[7] jeśli chcesz dowiedzieć się więcej na temat zagrożeń przy korzystaniu z mediów społecznościowych zapoznaj się z „Poradnikiem Bezpiecznego Korzystania ze Środków Komunikacji Elektronicznej w Cyberprzestrzeni"

3.6.2 Skutki ataku

Skutki zagrożenia związane z aktywną usługą geolokalizacji mogą być bardzo różne. Na przykład informacja o tym, że całą rodziną przebywamy właśnie daleko poza domem, może być podpowiedzią dla złodzieja, który chciałby się włamać do naszego domu. Bywają skutki znacznie poważniejsze. Znane są przypadki wykorzystywania tego typu informacji nawet w czasie działań wojennych, w których strony konfliktu mogą łatwo identyfikować położenia przeciwnika. W praktyce ocena skutków udostępniania informacji o swoim położeniu należy do właściciela urządzenia mobilnego. Jest ona uzależniona od subiektywnego poczucia ochrony własnej prywatności. Warto jednak tę sprawę poważnie rozważyć. Punktem wyjścia powinno być zadanie sobie pytania „Jak bardzo zgadzam się z tym, że informacja o moim obecnym położeniu trafi do innych?". To pytanie ma szczególne znaczenie przy prowadzeniu profilów społecznościowych o szerokim zasięgu (np.: konta w serwisie Twitter). Jeśli się zdecydujemy, aby automatycznie nie blokować takiej możliwości dla wszystkich naszych postów, to zdecydowanie powinniśmy sobie zadawać takie pytanie, przy każdorazowej publikacji.

3.6.3 Porady jak się bronić

Podstawową metodą ochrony przed publikacją danych na temat swojej lokalizacji jest odpowiednie ustawienie w preferencjach konfiguracji urządzenia mobilnego. Poniżej znajdują się informacje jak to zrobić w systemie iOS i Android.

iOS (iPhone/iPad)

Apple pozwala kontrolować nam, które aplikacje mają dostęp do usług lokalizacji (tj. do modułu GPS). Aby przejrzeć uprawnienia programów, należy udać się do **Ustawień**, wybrać opcję **Prywatność,** a następnie **Usługi lokalizacji**.

W tym menu mamy możliwość podjęcia decyzji, która aplikacja będzie miała dostęp do naszej lokalizacji oraz w jakim zakresie - możemy umożliwić korzystanie z niej tylko podczas uruchomienia danego programu, bądź też cały czas w tle.

Pozostaje również możliwość całkowitego wyłączenia usług lokalizacji, przez co żadna aplikacja, łącznie z tymi systemowymi, nie będzie miała do nich dostępu. W tym celu trzeba przełączyć główny włącznik, znajdujący się na pierwszej pozycji po wybraniu, wcześniej wspomnianej, opcji **Usługi lokalizacji** w **Ustawieniach**.

Apple umożliwia też wysyłanie swojego położenia członkom rodziny i znajomym. Warto rozważyć korzystanie z tej opcji, jeśli myślimy o bezpieczeństwie bliskich nam osób.

Android

W przypadku urządzeń pracujących pod kontrolą systemu Android, mamy możliwość sprawdzenia i włączenia/wyłączenia dostępu do lokalizacji przez aplikacje. Aby to przeprowadzić należy wejść w **Ustawienia**, **Google** następnie wybrać opcję **Lokalizacja** i wyłączyć dostęp do lokalizacje przez te aplikacje które według nas nie powinny mieć takich informacji.

Dodatkowo, jeśli chcemy, aby Google nie zbierało żadnych informacji o naszym położeniu, należy wybrać opcję **Historia lokalizacji Google**, w której powinniśmy odznaczyć pozycję odpowiedzialną za raportowanie naszego położenia.

Dodatkową zachętą do wyłączenia geolokalizacji może być fakt, że w istotny sposób odciąży to baterię urządzenia mobilnego, przez co będziemy mogli dłużej z niego korzystać bez ładowania.

4. Reagowanie na odnotowane ataki

4.1 Sposoby rozpoznawania ataków

Mimo tego, że w interesie cyberprzestępcy jest zazwyczaj maksymalnie skuteczne ukrycie skutecznego ataku na urządzenie mobilne, to atakom takim mogą towarzyszyć zjawiska, które pomogą użytkownikowi zidentyfikować problem:

- na wyświetlaczu pojawiła się na chwilę wiadomość SMS lub powiadomienie tekstowe, którego nie mogłeś odnaleźć na urządzeniu, ani powiązać z działaniem żadnej aplikacji.
- twój rachunek za usługi telefoniczne znacząco wzrósł, w szczególności w związku z opłatami za SMS-y.
- niektóre z Twoich aplikacji, w szczególności nowo zainstalowanych, wymieniają przez sieć bardzo dużo danych, liczonych w setkach MB-ów a nawet GB-ach.
- bateria urządzenia bardzo szybko się wyczerpuje, dodatkowo zdarza się, że jego temperatura wyraźnie wzrasta bez wyraźnej przyczyny.
- oprogramowanie antywirusowe na urządzeniu mobilnym nie działa, mimo że sam go nie wyłączałeś.
- w czasie wykonywania połączeń telefonicznych słyszysz niepokojące dźwięki i pogorszenie jakości rozmowy, które w Twojej opinii nie wynika ze słabego zasięgu.
- otrzymujesz informacje z oprogramowania antywirusowego, które niedawno zainstalowałeś i prowadzą one do konieczności płatnej aktualizacji systemu.

- otrzymujesz dużo natrętnych reklam, szczególnie z poziomu wyszukiwarki internetowej;
- strony reklamowe oraz „specjalne" oferty otwierają się samoistnie (tzw. pop-up)
- straciłeś dostęp do swojego telefonu – blokada ekranu pojawia się na nim w odstępach kilkusekundowych.
- straciłeś dostęp do swoich danych na urządzeniu mobilnym, wyświetlany jest komunikat o konieczności opłacenia możliwości przywrócenia dostępu.
- na urządzeniu pojawiają się informacje o rzekomym złamaniu prawa (np. przetrzymywania pornografii dziecięcej) i konieczności zapłacenia kary.

4.2 Reagowanie w przypadku ataku

Jeśli nie jesteś specjalistą bezpieczeństwa komputerowego będzie Ci trudno poradzić sobie ze skutkami ataku, dlatego warto w takiej sytuacji skorzystać z porad i pomocy osób, które się na tym znają. Niemniej jednak jest wiele rzeczy, które z pewnością potrafisz zrobić sam. Szybkie działanie i prawidłowa reakcja może Cię uchronić przed większymi, negatywnymi skutkami ataku na Twoje urządzenie mobilne i znajdujące się na nim dane.

Jeśli doszło do ataku pamiętaj o następujących działaniach:

- jeśli masz podejrzenie, że Twoje hasło dostępu do urządzenia (czterocyfrowy kod lub ustalony schemat graficzny) zostało skompromitowane, np.: podejrzane przez obcą osobę, to natychmiast je zmień. Jeżeli używasz tego samego hasła do innych usług lub urządzeń (czego nie rekomendujemy!), zmień je natychmiast.
- jeśli atak na Ciebie jest powiązany z atakiem na innych użytkowników urządzeń mobilnych, np.: są masowo rozsyłane SMS-y, które prowadzą do infekcji urządzenia, a ich źródłem jest rzekomo znana instytucja (np.: bank), to koniecznie skontaktuj się z tą instytucją i powiadom o procederze. Zapewne dostaniesz poradę co do dalszego postępowania, Twoje konto zostanie zabezpieczone, a instytucja będzie mogła skutecznie ostrzec innych odbiorców swoich usług
- jeśli uważasz, że zostałeś w szczególny sposób poszkodowany – na przykład wykradziono Twoje ważne dane osobowe, to możesz taki przypadek również zgłosić do UODO (możesz to zrobić online: Strona UODO)
- dokumentuj wszystkie swoje działania i to co odnotowałeś na swoim urządzeniu mobilnym. Prosta notatka z wszystkich kroków, które podjąłeś oraz zestaw wykonanych tzw. zrzutów ekranu może być decydująca w dochodzeniu Twoich roszczeń. Jeśli to możliwe to wszystkie te dane przechowuj

na innym urządzeniu mobilnym, komputerze lub nośniku pamięci zewnętrznej (np.: nośniku pamięci USB)

- jeśli to możliwe to zupełnie zrezygnuj z dalszych działań na skompromitowanym urządzeniu przenośnym. Wyłącz to urządzenie i zachowaj do przyszłej analizy przez specjalistę (np.: biegłego sądowego)
- warto wykonać skanowanie swojego urządzenia mobilnego, które może wykryć zainstalowane na nim złośliwe oprogramowanie
- sprawdź miejsce innych potencjalnych strat – np.: Twoje konto bankowe, czy nie pojawiły się tam objawy ataku na Ciebie. Jeśli jesteś przekonany o ataku na Twoje konto bankowe lub kartę kredytową koniecznie skontaktuj się z bankiem i zgłoś ten przypadek oraz poproś o instrukcję postępowania
- we wszystkich przypadkach kontaktów z podmiotami zewnętrznymi staraj się przekazywać konkretną, rzeczową informację. Jeśli nie znasz się wystarczająco dobrze na urządzeniach mobilnych i sieciach poproś o pomoc znajomą osobę, która posiada choćby minimum wiedzy z tego zakresu
- po wykonaniu wszystkich podstawowych działań, jeśli nadal masz przekonanie o tym, że Twój problem nie został rozwiązany, skontaktuj się profesjonalistami i poproś o pomoc. Spróbuj uzyskać pomoc bezpłatną. Jeśli nie jest to możliwe to dokonaj szybkiej analizy potencjalnych strat związanych z zaniechaniem działania i kosztów związanych z ich uniknięciem. Podejmij racjonalną decyzję.
- w przypadku kradzieży urządzenia mobilnego wyposażonego w kartę SIM, zablokuj u swojego operatora tę kartę

5. Przydatne linki

5.1 Serwisy dostawców usług telekomunikacyjnych

Sposoby zabezpieczania smartfona – Android: Strona Play

Bezpieczne korzystanie z urządzeń mobilnych: Strona Orange

5.2 Serwisy informacyjne z sektora bezpieczeństwa teleinformatycznego

Bezpieczeństwo bankowości mobilnej

RODO- bezpieczeństwo urządzeń mobilnych

Jak wybrać najbezpieczniejszy telefon dla dziecka

Niezbędnik e-commerce, czyli jak zadbać o bezpieczeństwo podczas przedświątecznych zakupów online

Wskazówki bezpieczeństwa dla urządzeń mobilnych

Avast Mobile Security & Antivirus 2019: Google Play

AVG Family Safety: Dobre Programy

Bezpieczeństwo bankowe: Strona ZBP

Słowniczek

Backup – czynność polegająca na archiwizowaniu zasobów przechowywanych na komputerze. Powinna być wykonywana na wydzielonym nośniku danych, niezależnym od urządzenia mobilnego.

Botnet – sieć komputerów przejętych przez cyberprzestępcę, nad którymi ma on kontrolę. Botnet może być wykorzystany do ataku na inne komputery lub serwisy – np.: do ataku DDoS.

„Certyfikat bankowy" – w przypadku przestępstw komputerowych termin używany przez cyberprzestępców, który ma oznaczać techniczny sposób na dodatkowe zabezpieczenie urządzenia mobilnego. W rzeczywistości jest złośliwym oprogramowaniem. Mogą występować różne warianty tego terminu, np.: „Certyfikat bezpieczeństwa".

GPS – (ang. Global Positioning System) system nawigacji satelitarnej, obejmujący swoim zasięgiem całą kulę ziemską, służy do określania położenia w terenie.

Kod weryfikujący CVV – trzycyfrowy kod weryfikujący użytkownika karty płatniczej, umieszczony na odwrocie karty. Kod wymagany jest przy transakcjach elektronicznych.

Jailbreak – proces usunięcia ograniczeń w systemie iOS firmy Apple, dzięki któremu użytkownik uzyskuje pełny dostęp do urządzenia, w szczególności może instalować w nim aplikacje pochodzące spoza oficjalnego systemu dystrybucji oprogramowania – sklepu internetowego Apple Store.

Malware – uniwersalna nazwa dla złośliwego oprogramowania. Malware może przybierać różne postaci i funkcje, np.: wirusa, robaka internetowego, konia trojańskiego, etc.

Ransomware – rodzaj malware'u polegający na wprowadzeniu złośliwych funkcji, np.: blokady klawiatury smartfona lub zaszyfrowania przechowywanych plików, w celu wymuszenia okupu na ofierze.

Ransomware removal – oprogramowanie służące do usuwania oprogramowania typu ransomware.

Repozytorium haseł – program dedykowany do przechowywania zestawu haseł do różnych aplikacji i serwisów. Dostęp do wszystkich haseł w nim przechowywanych uzyskuje się z wykorzystaniem jednego, głównego hasła.

Stacja bazowa BTS - (ang. Base Transceiver Station) w systemach łączności bezprzewodowej (np. popularnym GSM) urządzenie (często z wysokim masztem), wyposażone w antenę fal

elektromagnetycznych, łączące terminal ruchomy (telefon komórkowy, pager) z częścią stałą cyfrowej sieci telekomunikacyjnej[8].

Wektor ataku – sposób w jaki przeprowadzany jest atak na komputer. W odniesieniu do złośliwego oprogramowania określa sposób infekcji takiego urządzenia.

WEP – (ang. Wired Equivalent Privacy) standard szyfrowania komunikacji w sieciach Wi-Fi. Obecnie powszechnie używany jest za niewystarczający z punktu widzenia zapewnienia poufności danych.

Wi-Fi – popularne określenie na sieci bezprzewodowe powszechnie używane do zapewnienia łatwego dostępu do sieci Internet dla urządzeń wyposażonych w odpowiedni odbiornik.

WPA – (ang. Wi-Fi Protected Access) standard szyfrowania komunikacji w sieciach Wi-Fi. Mimo, że jest on bezpieczniejszym protokołem niż WEP, to od 2010 roku również nie jest zalecany jako bezpieczny sposób wymiany danych w sieci Wi-Fi.

WPA2 – (ang. Wi-Fi Protected Access II) standard szyfrowania komunikacji w sieciach Wi-Fi. Obecnie uznawany za dający największy poziom bezpieczeństwa, lepszy od standardów WEP i WPA.

[8] Strona źródłowa