STUDIA INFORMATICA 2011
Volume 32 Number 3A (98)

Teresa MENDYK-KRAJEWSKA, Zygmunt MAZUR
Politechnika Wrocławska, Instytut Informatyki

PROBLEM BEZPIECZEŃSTWA URZĄDZEŃ MOBILNYCH

Streszczenie. W artykule przedstawiono zagadnienie bezpieczeństwa urządzeń mobilnych, wykorzystywanych do połączeń z siecią Internet. Zainteresowaniem objęto urządzenia rozwijające się na bazie telefonii komórkowej. Omówiono rodzaje urządzeń wraz z ich oprogramowaniem systemowym, opisano typy zagrożeń oraz skalę zjawiska, a także podano przykłady zagrożeń i przedstawiono narzędzia do ochrony takich systemów.

Słowa kluczowe: bezpieczeństwo sieciowe, urządzenia mobilne

THE PROBLEM OF MOBILE DEVICES SECURITY

Summary. This paper presents the issue of security of mobile devices used to connect with internet with the emphasis on the devices designed for cellular network. The types of the devices and their system software have also been discussed and the types of threats, the scale of problem have been described. The paper provides examples of threats and presents tools to protect such systems.

Keywords: network security, mobile devices

1. Wprowadzenie

Atrakcyjność bezprzewodowego dostępu do sieci Internet spowodowała duże zainteresowanie nową technologią i szybki rozwój urządzeń mobilnych (telefonów komórkowych, smartfonów, palmtopów)[1]. Wygoda użytkowania i coraz niższe koszty tych urządzeń przyczyniły się do wzrostu ich popularności. Urządzenia mobilne z dostępem do Internetu są wykorzystywane do realizacji zadań biznesowych, wykonywania usług bankowych czy do

[1] Do tej grupy zaliczają się też notebooki, jednak z uwagi na ich budowę i działanie narażone są na podobne zagrożenia co komputery stacjonarne i nie są tu brane pod uwagę.

zakupów. Używane są chętnie przez menedżerów i pracowników przedsiębiorstw, umożliwiając im stały kontakt oraz dostęp do wspólnych zasobów firmowych (nawet podczas wyjazdów służbowych). Wraz z rosnącą popularnością urządzeń mobilnych obserwuje się coraz większe zainteresowanie sieciowych przestępców możliwością uzyskania nielegalnych zysków za ich pośrednictwem, ponieważ niemal na każdym urządzeniu przechowywane są ważne i poufne informacje.

Pierwsze szkodliwe programy dla systemów mobilnych nie różniły się od kodów atakujących sieci komputerowe. Zjawisko zagrożenia bezpieczeństwa początkowo nie przybierało znacząco na sile z powodu dużej różnorodności wykorzystywanych platform systemowych, gdyż na rynku, oprócz smartfonów Nokii z systemem operacyjnym Symbian, wkrótce pojawiły się inne urządzenia – na przykład iPhone firmy Apple z systemem iOS, czy obsługiwany przez wielu producentów telefonów komórkowych Windows Mobile, firmy Microsoft. Praktyka pokazuje, że o wyborze systemu komputerowego na cel ataków (a więc tworzeniu szkodliwych kodów) przesądza właśnie jego popularność. W przypadku urządzeń mobilnych znaczący rozwój zagrożeń wiąże się z opracowaniem wirusów uniwersalnych, przystosowanych do atakowania wielu różnych platform systemowych.

2. Rodzaje urządzeń mobilnych

Do szerokiej gamy urządzeń mobilnych zalicza się: PDA (*Personal Digital Assistant*) – pierwszy, bardzo mały komputer osobisty zwany palmtopem (1992 r.), palmofon – PDA z telefonem, ekranem dotykowym i głośnikami, smartfon – połączenie telefonu i komputera, netbook – mniejszy od notebooka, o mniejszych możliwościach (na ogół bez napędu CD/DVD), tablet PC – rodzaj komputera wyposażonego w ekran dotykowy o parametrach porównywalnych z notebookami, MDA (*Mobile Digital Assistant*) – połączenie palmtopa z telefonem komórkowym oraz wbudowanym modemem GSM[2], e-book – tzw. książka elektroniczna (urządzenie do czytania tekstów pobieranych z Internetu), smartbook – wyposażony w mikrofon, głośniki, kamerę (umożliwia komunikację za pomocą komunikatorów internetowych). Jest jeszcze wiele innych urządzeń przenośnych umożliwiających przesyłanie plików, na przykład aparaty i kamery cyfrowe, urządzenia do nawigacji satelitarnej, odtwarzacze MP3, skanery.

Klasyfikacja urządzeń mobilnych staje się coraz trudniejsza, gdyż ich funkcjonalności są stale rozbudowywane. Poszczególne urządzenia, nawet w tej samej kategorii, różnią się między innymi: budową, wielkością, sposobem interakcji z użytkownikiem. Projektowanie dla

[2] *Global System for Mobile Communications* – obecnie najpopularniejszy standard telefonii komórkowej.

nich aplikacji użytkowych, rozpoznających rodzaj urządzenia i dostosowujących do ekranu wyświetlaną treść jest zadaniem złożonym [2].

Wśród urządzeń mobilnych obecnie trudno jest wskazać jednego lidera. Na rynku konkuruje ze sobą wiele firm, oferujących dużą gamę urządzeń pracujących na różnych platformach systemowych. Pierwsze miejsce należało przez pewien czas do fińskiej firmy Nokia, wkrótce jednak pojawiły się inne firmy, których produkty również zyskały dużą popularność. Obecnie dostępne są także urządzenia takich firm, jak: RIM, Apple, Google i wielu innych. Liczne urządzenia mobilne są ukierunkowane na najczęściej poszukiwane funkcjonalności, czyli możliwość komunikacji i dostęp do Internetu, ze szczególnym uwzględnieniem serwisów społecznościowych. Stąd w niektórych z nich są specjalne przyciski, umożliwiające bezpośredni dostęp do popularnych serwisów społecznościowych, jak Facebook czy Twitter. Rozwijające się technologie sprawiają, że dostęp do Internetu z wykorzystaniem urządzeń mobilnych jest coraz szybszy i wygodniejszy.

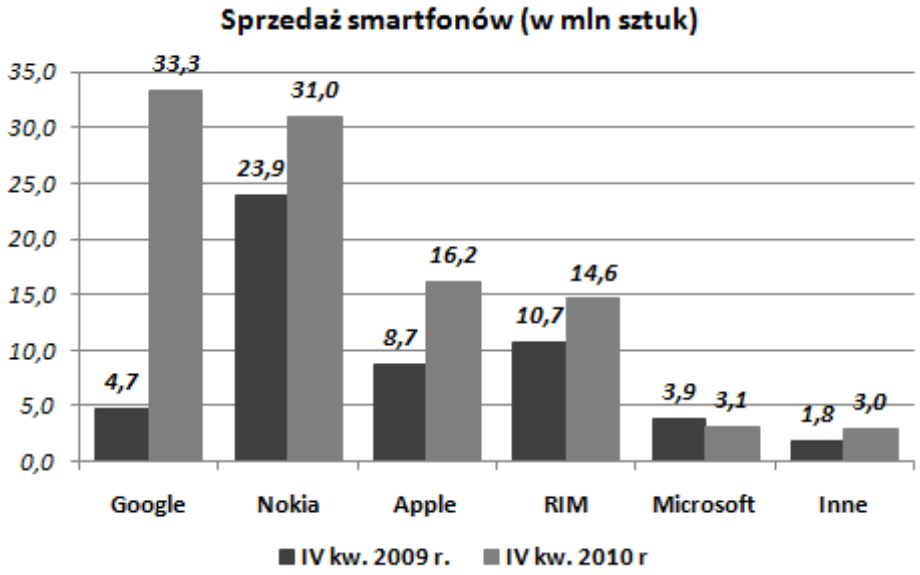
W grudniu 2010 roku firma Google udostępniała bezpłatnie testowe netbooki Cr-48 z automatycznie aktualizowanym systemem operacyjnym Google Chrome OS, bez dysku twardego, z łącznością Wi-Fi i z połączeniem w technologii 3G[3]. Netbooki miały zainstalowany w pamięci tylko jeden program – przeglądarkę internetową Chrome, a do wykonywania usług i przechowywania danych wykorzystano *Cloud computing* (tzw. obliczenia w chmurze). Zaletami takiego rozwiązania są: dostępność usług, wygoda użytkowania i oszczędność (brak konieczności instalowania oprogramowania i zakupu licencji), ale istnieje duże zagrożenie dla ich bezpieczeństwa (prywatności danych).

3. Platformy systemowe

Popularność urządzeń mobilnych w dużej mierze zależy od zainstalowanego systemu operacyjnego, gdyż ma to wpływ na ich funkcjonalność. Dla urządzeń mobilnych wiele firm opracowało różne systemy operacyjne, jednak żaden z nich nie zdominował pozostałych konkurentów w takim stopniu, jak system operacyjny Windows, firmy Microsoft, w przypadku systemów komputerowych. Popularnością cieszą się zarówno urządzenia z systemem Symbian firmy Nokia, jak i z Windows Mobile firmy Microsoft, urządzenia iPhone (smartfony) firmy Apple, wykorzystujące system operacyjny iOS (oparty na rdzeniu Mac OS X 10.5) czy z platformą Android firmy Google. Do tej listy można dodać jeszcze telefony z systemem Linux Mobile, urządzenia z bardzo elastycznym systemem mobilnym Brew firmy Qualcomm (np. smartfony, telefony), urządzenia z systemem MeeGo (telefony, netbooki, tablety) oraz

[3] Generacja telefonii komórkowej umożliwiająca szybki dostęp do Internetu i oferująca usługi multimedialne.

telefony firmy Siemens z platformą S/E GOLD. Na rynku amerykańskim mocną pozycję ma firma RIM *(Research In Motion)*, której urządzenia działają pod kontrolą własnego systemu operacyjnego BlackBerry OS. Popularność systemów operacyjnych smartfonów w IV kwartale w latach 2009 i 2010 przedstawiono na rys. 1.



Rys. 1. Popularność systemów operacyjnych smartfonów w IV kwartale w latach 2009 i 2010 (opracowanie własne na podstawie [1])
Fig. 1. Worldwide smartphone marketability: Q4 2009, Q4 2010 [1]

Ponieważ od zainstalowanego systemu operacyjnego w dużej mierze zależą możliwości urządzenia, bezpieczeństwo danych oraz wygoda użytkowania, dlatego bardzo ważny jest jego wybór. Podczas kongresu *Mobile World Congress* w Barcelonie w lutym 2011 roku największe zainteresowanie wzbudzały tablety i system Android, który zdominował inne systemy (w kongresie nie uczestniczyła firma Apple). Według analityków firmy RBC Capital Markets, w 2014 roku najpopularniejszymi systemami operacyjnymi tabletów będą: Android – 40% udziału, iOS – 34%, Microsoft – 13%, BlackBerry – 8% [7].

Obecnie dostępne urządzenia mobilne pełnią rolę podręcznego komputera z dostępem do zasobów internetowych. Niestety brak odpowiednich zabezpieczeń dla tych urządzeń oraz nieświadomość użytkowników sprawiają, że gromadzone tam dane nie są bezpieczne. Do najczęściej atakowanych platform aplikacji mobilnych należą: Symbian, J2ME (*Java 2 Micro Edition*), WinCE, Python, S/E GOLD i MSIL.

4. Zagrożenia urządzeń mobilnych

Wirusy w telefonach komórkowych nie stanowiły poważnego zagrożenia do czasu pojawienia się zaawansowanych modeli telefonów z systemami Symbian i Windows Mobile. Wraz z rozwojem urządzeń mobilnych rozwinął się rynek oprogramowania do ich infekowania, m.in. w celu osiągania korzyści finansowych. Często celem ataków jest chęć przejęcia poufnych danych użytkownika, przechowywanych numerów telefonów, a także treści prywatnych wiadomości.

Z powodu dużej różnorodności platform systemowych dla urządzeń mobilnych, twórcy wirusów skoncentrowali wysiłki na pisaniu szkodliwych kodów „wieloplatformowych". Zwrócili oni uwagę, że niemal wszystkie telefony komórkowe oraz smartfony obsługują aplikacje napisane w Javie, zatem można na nich uruchamiać pobrane z Internetu szkodliwe programy, napisane w tym języku.

Dotychczas zidentyfikowano około 2000 sygnatur szkodliwego oprogramowania, przeznaczanych dla urządzeń mobilnych.

Szkodliwe oprogramowanie dla urządzeń mobilnych może wykonać wiele bezprawnych działań, takich jak: infekowanie plików, instalowanie szkodliwego oprogramowania, blokowanie kart pamięci lub urządzenia, uszkadzanie lub usuwanie danych, kradzież danych, umożliwienie zdalnego dostępu do urządzenia (a tym samym np. do sieci lub poczty korporacyjnej), wysyłanie wiadomości SMS czy MMS[4], pobieranie plików z sieci Internet, wyłączanie mechanizmów bezpieczeństwa systemu, w tym programów antywirusowych. Do najważniejszych rodzin wirusów urządzeń mobilnych należą: Cabir, Skuller i Cardtrap.

W dotychczasowej historii zjawiska najbardziej rozpowszechnionymi zagrożeniami dla urządzeń mobilnych były wirusy Cabir[5] i ComWar. W Hiszpanii, w 2007 roku wariantem ComWara zostało zainfekowanych ponad 115 tys. użytkowników – był to jeden z najgłośniejszych zarejestrowanych incydentów tego typu. Oto kilka innych przykładowych zagrożeń:

- Trojan-SMS.SymbOS.Viver.b – koń trojański dla platformy Symbian,
- Trojan-Spy.SymbOS.Pbstealer.a – pierwszy koń trojański dla telefonii komórkowej, umożliwiający kradzież danych,
- Trojan.SymbOS.Delacon.a – uszkadza i usuwa dane z urządzenia z systemem Symbian,
- Not-a-virus:Porn-Dialer.SymbOS.Pornidal.a – wykonuje międzynarodowe połączenia z numerami o podwyższonej opłacie (do osiągania korzyści finansowych),
- Trojan:WinCE/InfoJack – przekazuje dane urządzenia z systemem Windows Mobile,

[4] *Short Message Service* – usługa przesyłania krótkich wiadomości tekstowych, *Multimedia Message Service* – usługa przesyłania wiadomości multimedialnych.

[5] Pierwszy prawdziwy wirus urządzeń mobilnych, powstał on w 2004 roku.

- Worm.SymbOS.Yxe – program dla telefonów z systemem Symbian, rozprzestrzeniany za pomocą SMS-ów, podpisany legalnym certyfikatem,
- Trojan-SMS.Python.Flocker – rodzina koni trojańskich dla platformy Symbian z zainstalowanym interpreterem języka Python i ustanowionym połączeniem Bluetooth.

Szkodliwe programy potrafią rozprzestrzeniać się za pośrednictwem nośników przenośnych (kart pamięci[6] – np. wirusy Cardtrop i Mobler), technologii Bluetooth[7], MMS-ów i SMS-ów. Istnieje wiele rodzajów ataków wykorzystujących technologię Bluetooth, np. BlueBug – pozwalający przejąć kontrolę nad urządzeniem (poprzez wykorzystanie ukrytych kanałów RFCOOM), Blueprinting – polegający na zebraniu informacji o aktywnych urządzeniach czy BlueChop – prowadzący do zakłócenia pracy innych urządzeń, znajdujących się w danej podsieci. Jeden z popularniejszych sposobów przenoszenia szkodliwych kodów polega na wykorzystaniu w tym celu portali WAP, na których można pobierać dzwonki, grafikę, gry i aplikacje dla telefonów komórkowych. Szkodliwe oprogramowanie dostaje się na urządzenia wraz z instalowanymi przez użytkownika elementami. Częstą przyczyną infekowania urządzeń jest właśnie instalowanie aplikacji pochodzących z niepewnych źródeł i ignorowanie wszelkich nieprawidłowości podczas ich wykorzystywania. Niestety, szkodliwe kody i podejmowane przez nie działania często są maskowane i to w coraz bardziej wyszukany sposób.

Nie wszystkie urządzenia stanowią jednakowo łatwy cel. Na przykład, żeby zainfekować iPhone'a, trzeba się do niego włamać i zainstalować odpowiednie aplikacje. Wszystko wskazuje na to, że głównym zagrożeniem dla tej platformy (a także dla systemu Android) będą luki w zabezpieczeniach oprogramowania, umożliwiające nieautoryzowany dostęp do urządzeń. Na początku 2009 roku wykryto lukę w kilku wersjach Symbiana (m.in. w S60 3rd edition, S60 2nd edition, Feature Pack 2 i Pack 3), wykorzystywaną przez exploit *The Curse of Silence*. Jeśli do urządzenia z takim systemem zostanie wysłana specjalnie spreparowana wiadomość SMS (dla użytkownika niewidoczna), nie będzie ono miało możliwości wysyłania i odbierania wiadomości SMS i MMS – lecz poza tym będzie funkcjonowało normalnie, co utrudnia wykrycie nieprawidłowości. Przykładami wirusów wykorzystujących luki w systemie są: Trojan.SymbOS.Skuller, Trojan.SymbOS.Dampig i Trojan.SymbOS.Romride.

Dużym zagrożeniem dla urządzeń mobilnych jest tzw. phishing SMS-owy. W tym przypadku od anonimowych nadawców przesyłane są wiadomości SMS, w których użytkownicy proszeni są (np. pod pretekstem „potwierdzenia" szczegółów transakcji) o wykonanie telefonu pod wskazany numer. Następnie, podczas realizacji połączenia, automatyczna sekretarka wymusza podanie poufnych informacji (np. danych bankowych). Często stosowane są ataki

[6] Na karty pamięci wirus trafia w czasie synchronizacji danych z komputerem stacjonarnym.

[7] Technologia używana do transferu plików, komunikacji głosowej, do automatycznej synchronizacji urządzeń; szkodliwe oprogramowanie wyszukuje znajdujące się w pobliżu urządzenia, pracujące w tej technologii i wysyła do nich wirusy.

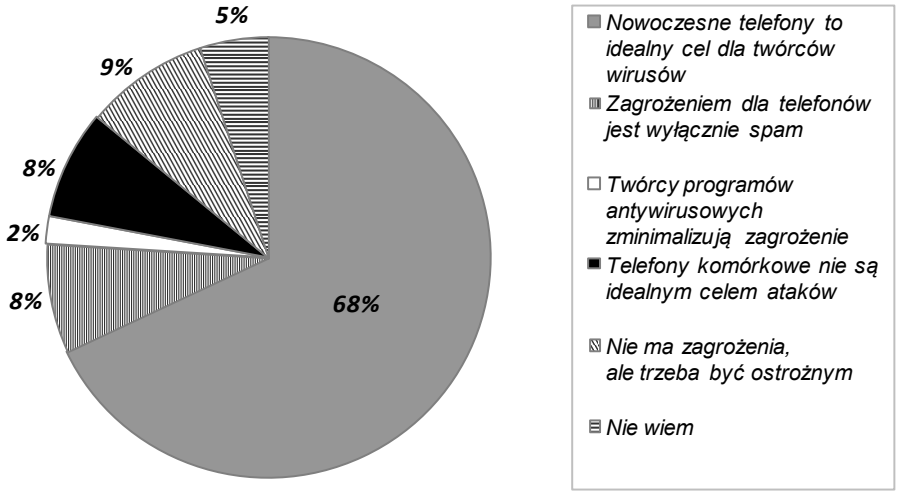
socjotechniczne, np. wyłudzanie pieniędzy poprzez opis rzekomych kłopotów i wystosowanie prośby o dokonanie przelewu gotówki pod wskazany numer konta lub podanie informacji o oczekującej wygranej, gotowej do odebrania po wysłaniu SMS-a (o określonym koszcie) pod podany numer. Inne, zaobserwowane zjawiska to: nakłanianie do odpłatnego pobierania plików z Internetu, zachęcanie do udziału w konkursach czy wymuszanie oddzwonienia pod numer najczęściej zaczynający się od cyfr 70 (koszt połączenia za 1 min. wynosi prawie 10 zł). Istnieje też grupa szkodliwego oprogramowania, którego celem jest zwiększenie kosztów użytkowania urządzenia poprzez automatyczne wysyłanie wiadomości lub inicjowanie połączeń. Wysyłanie wiadomości SMS pod numery o podwyższonej opłacie bez wiedzy użytkownika to około 35% wszystkich zagrożeń, zidentyfikowanych przez firmę Kaspersky Lab.

W 2009 roku wykryto pierwszego robaka (ikee) infekującego urządzenia iPhone, w których złamano zabezpieczenia systemowe i nie zmieniono domyślnego hasła dostępu do oprogramowania SSH. Szkodliwy kod potrafi wykradać dane, umożliwia przejęcie kontroli nad urządzeniem, wyszukuje nowe adresy IP i instaluje się na podatnych na infekcję urządzeniach. Zagrożenie jest poważne, gdyż możliwości tego robaka pozwalają na zbudowanie mobilnej sieci botnetów, która może być wykorzystywana przez kontrolujących ją przestępców do bezkarnych, szkodliwych działań [3]. Dużym zagrożeniem, przed którym ostrzegają banki na swoich stronach internetowych jest koń trojański Zeus, atakujący komputery i telefony komórkowe z systemem Symbian i BlackBerry. Użytkownikom proponowana jest instalacja programu przyspieszającego działanie procesora, gdy tymczasem instalowane jest szkodliwe oprogramowania przekierowujące na fałszywe strony banków (na których podczas logowania przechwytywane są hasła do kont bankowych).

5. Bezpieczne użytkowanie urządzeń mobilnych

Z przeprowadzonego w Internecie sondażu wynika, że użytkownicy są świadomi zagrożeń dla telefonii komórkowej. Aż 68% pytanych uważa nowoczesne telefony za idealny cel dla twórców wirusów [5]. Pełne wyniki tej ankiety przedstawiono na rys. 2. Jednocześnie wyniki sondażu opublikowanego w lutym 2011 roku przez AVG Technologies i Ponemon Institute pokazują, że ponad jedna trzecia użytkowników smartfonów nie ma świadomości zagrożeń związanych z ich używaniem do realizacji operacji finansowych i przechowywania danych poufnych [8].

Narastanie zjawiska zagrożenia bezpieczeństwa urządzeń mobilnych wymusiło rozwój sposobów ich ochrony. Użytkowanie tych urządzeń wymaga bowiem stosowania zabezpieczeń, analogicznie do przypadku komputerów, jednak dotąd nie wszyscy mają tego świadomość. Niewiedza użytkowników w tym zakresie przyczynia się również do łatwiejszego i szybszego rozprzestrzeniania zagrożeń.



Rys. 2. Wyniki sondażu dotyczącego świadomości zagrożeń dla urządzeń mobilnych
Fig. 2. The results of the survey on the awareness of the security threats on mobile devices

Wśród stosowanych sposobów ochrony systemów mobilnych można wymienić: skanowanie antywirusowe ruchu MMS przez operatorów telefonii komórkowej, preinstalowanie na urządzeniach mechanizmów antywirusowych, nieaktywowanie bez potrzeby połączeń Bluetooth, nieakceptowanie nieznanych połączeń Bluetooth, instalowanie i uruchamianie tylko podpisanych aplikacji, tworzenie kopii zapasowych systemu operacyjnego i danych.

Kontrowersyjnym rozwiązaniem jest zdalne usuwanie aplikacji, uznanych za szkodliwe, bez wiedzy i zgody użytkownika – przykładem są takie działania prowadzone przez firmę Google na telefonach z systemem Android [4].

Dla bezpieczeństwa bardzo ważne jest regularne używanie odpowiednio skonfigurowanego programu antywirusowego, rozbudowanego funkcjonalnie i chroniącego system na wielu płaszczyznach. Oprogramowanie takie działa analogicznie do przypadku komputerów – skanuje wykorzystywane łącza, sprawdza pliki i wiadomości, a znajdując szkodliwy kod, umożliwia jego usunięcie. Do blokowania niechcianych połączeń telefonicznych i wiadomości tekstowych wykorzystywany jest filtr antyspamowy.

Powstaje wiele programów ochronnych dedykowanych konkretnym urządzeniom czy systemom. Do najbardziej popularnych narzędzi należą F-Secure Mobile Security oraz Kaspersky Mobile Security – o zbliżonej funkcjonalności, oba przeznaczone dla systemów Symbian, Windows Mobile i Android (Kaspersky Mobile Security także dla BlackBerry OS). Z uwagi na możliwość zgubienia lub kradzieży urządzenia, istotna jest dostępność mechanizmu pozwalającego na jego blokadę bądź zdalne kasowanie danych (np. funkcje SMS Block i SMS Clean w module *Anti-Theft* narzędzia firmy Kaspersky). Można blokować dostęp do danych poufnych, usuwać zdjęcia, filmy i SMS-y. Aplikacja ochronna potrafi też zidentyfikować nową kartę i wysłać wiadomość z nowym numerem do legalnego właściciela (co ułatwia pracę organom ścigania). Przykładem oprogramowania ochronnego może być też program Ontrack

Eraser Mobile, umożliwiający skasowanie danych w smartfonie poprzez wysłanie SMS-a lub w trakcie podłączania urządzenia do komputera. Bezpowrotnie niszczona jest zawartość pamięci wewnętrznej urządzenia oraz dane przechowywane na kartach pamięci i SIM (*Subscriber Identity Module*)[8].

Niektóre programy antywirusowe posiadają funkcję namierzania sygnału GPS przydatną w poszukiwaniu skradzionego urządzenia (np. Kaspersky oferuje usługę *SMS Find*). Użytkownik po wysłaniu wiadomości SMS, zawierającej hasło do danego urządzenia, otrzymuje adres serwisu Google Maps, gdzie wyświetlana jest jego dokładna lokalizacja. Ponieważ oprogramowanie nie może zostać odinstalowane, urządzenie staje się dla nowego właściciela bezwartościowe. Telefony komórkowe i smartfony coraz częściej są wyposażane w zintegrowane odbiorniki GPS, a podstawową ich funkcją jest właśnie zabezpieczanie urządzenia przed kradzieżą (wysokiej jakości moduły GPS dają dokładność lokalizacji do 1 m).

Im większa funkcjonalność urządzenia, tym więcej konsekwencji w przypadku jego zawirusowania lub utracenia. Tymczasem zwykle urządzenia mają zabezpieczenia niewystarczające, a często jedynym jest kod PIN, wprowadzany w momencie aktywacji. Użytkownicy nie chcą ponosić dodatkowych kosztów uważając, że za bezpieczeństwo urządzeń i usług powinni odpowiadać odpowiednio producenci i operatorzy sieci.

Dla bezpieczeństwa transmisji danych w sieciach komórkowych stosowany jest szyfr strumieniowy A5 – niestety, nie jest to mocne zabezpieczenie, a szczególnie wersje A5/1 i A5/2. W 2008 roku dwaj specjaliści ds. bezpieczeństwa opracowali metodę łamania szyfru A5/1, wykorzystywanego w komunikacji GSM, który to system obejmuje około 80% światowego rynku telefonii komórkowej. Okazuje się, że można tego dokonać w czasie krótszym niż pół godziny, przy wykorzystaniu powszechnie dostępnych, niedrogich urządzeń i oprogramowania, a zasięg podsłuchu wynosi 20 km. Metody łamania szyfrów A5/1 i A5/2 opracowano już w 1998 roku, jednak barierę dla ich praktycznego stosowania stanowił wysoki koszt. W 2007 roku opublikowano mocniejszą wersję szyfru – A5/3. Niestety, już w 2010 roku szyfr ten został złamany [6].

6. Podsumowanie

Problem bezpieczeństwa urządzeń mobilnych przez wielu użytkowników jest marginalizowany, choć zagrożenia dla nich nieustannie są rozwijane i rozprzestrzeniają się na całym świecie. Nie mają one charakteru globalnych epidemii, lecz są to ataki lokalne, występujące w określonych państwach lub regionach. Do krajów o największym zagrożeniu należą: Rosja,

[8] Moduł identyfikacji abonenta – karta elektroniczna, identyfikująca abonenta i przechowująca dane.

Indonezja i państwa Europy Zachodniej. Według specjalistów, posiadacze smartfonów doświadczą takich samych problemów, jakie są związane z użytkowaniem komputerów. Między innymi, przewidują oni możliwość wykorzystania urządzeń mobilnych do tworzenia botnetów (używanych następnie do przeprowadzenia ataku DDoS na wybrane sieci bezprzewodowe) oraz możliwość infekowania urządzeń, w celu podsłuchiwania rozmów telefonicznych. Na pewno rozwinie się grupa wirusów odpowiedzialnych za spam. Znawcy problemu wskazują też, iż interesującym obiektem ataków wkrótce mogą stać się smartbooki (łączące zalety netbooków i smartfonów, wyposażone w pełną klawiaturę, duży ekran i baterie o długiej żywotności), oparte na podobnej architekturze, co telefony komórkowe. Wraz z rozwojem zagrożeń dla urządzeń przenośnych można zaobserwować szybki rozwój rozbudowanego funkcjonalnie oprogramowania ochronnego, które oferuje pomoc także w przypadku zgubienia czy kradzieży urządzenia. Pojawiają się nawet specjalne wersje tych narzędzi, przeznaczone dla firm, umożliwiające zarządzanie całą siecią urządzeń mobilnych, co wskazuje na wagę problemu.

BIBLIOGRAFIA

1. Alto P.: Google's Android becomes the world's leading smart phone platform. Singapore and Reading (UK), 2011, www.canalys.com/pr/2011/r2011013.html (31.01.2011).
2. Frederick G. R., Lal R.: Projektowanie witryn internetowych dla urządzeń mobilnych. Tytuł oryginału: Beginning Smartphone Web Development: Building Javascript, CSS, HTML and Ajax-Based Applications for iPhone, Android, Palm Pre, Blackberry, Windows Mobile and Nokia S60 (tłum. Szczepaniak M.), Helion, Gliwice 2010.
3. Turowicz A.: Pierwszy botnet iPhone'ów. 2009. http://pclab.pl/news39843.html.
4. www.h-online.com/open/news/item/Google-uses-remote-delete-to-remove-Android-apps-from-smartphones-Update-1029188.html.
5. http://rozmowy.onet.pl/5103,1,sonda_noscript.html.
6. www.securitystandard.pl/news/354691/Atak.na.szyfr.komorek.3G.html.
7. www.eweekeurope.co.uk/news/android-tablets-will-prevail-against-ipads-by-2014-22968.
8. http://news.webwweb.pl/2,44387,0,Uzytkownicy,smartfonow,nieswiadomi,zagrozen.html.

Recenzenci: Prof. dr hab. inż. Bolesław Pochopień
Prof. dr hab. inż. Tadeusz Wieczorek

Wpłynęło do Redakcji 12 marca 2011 r.

Abstract

The attractiveness of wireless internet access has brought a lot of interest in new technology and boom in mobile devices (e.g. mobile phones, smartphones, palmtops etc). Since when first malicious software appeared for mobile systems we have observed their constant increase in sophistication which is related, among others, to the development of viruses capable of attacking a variety of system platforms. It is important because of the many existing systems and platforms operating on these devices (Fig. 1). The most popular targets are Symbian, J2ME, WinCe, Python, S/E GOLD, and MSIL.

Malware can execute many malfeasance activities such as blocking devices (e.g. memory sticks), data corruption, data deletion or data stealing, enabling unauthorised remote access to the mobile device, sending SMS or MMS, downloading files or switching off security system mechanisms. Malicious software can be distributed through portable media, Bluetooth, SMS or MMS. Web pages, from which one can download rings, images, games and applications, can also be used as a distribution channel (malware is installed on the devices together with the downloaded elements).

Another threat is, so-called, SMS phishing. In this case an anonymous SMS is sent asking the recipient to do specified actions, e.g. make a phone call to a given number, send SMS or make a bank transfer. Currently, users are more aware of the threats than before (Fig. 2).

The explosion of safety threats for mobile devices enforced the necessity to apply protection means similar to those used for personal computers (e.g. using functionally well-developed antivirus program). According to experts, the users of smart phones or palmtops will experience the same problems which occur on computers.

Adresy

Teresa MENDYK-KRAJEWSKA: Politechnika Wrocławska, Instytut Informatyki, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Polska, teresa.mendyk-krajewska@pwr.wroc.pl
Zygmunt MAZUR: Politechnika Wrocławska, Instytut Informatyki, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Polska, zygmunt.mazur@pwr.wroc.pl