JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 4 (2017) 87-91
Wysłane: 2017-01-03
Przyjęte: 2017-01-05

Porównanie mechanizmów bezpieczeństwa popularnych systemów operacyjnych urządzeń mobilnych

Michał Buryta*, Piotr Kopniak
Politechnika Lubelska, Instytut Informatyki, Nadbystrzycka 36B, 20-618 Lublin, Polska

Streszczenie. Artykuł dotyczy różnic w mechanizmach zabezpieczających trzech najpopularniejszych platform mobilnych, jakimi są Android, iOS i Windows Phone. Głównie skupiono sie na odrębnościach związanych z dostępem do danych użytkowników, instalacją i uruchamianiem aplikacji, dostępem do Internetu, połączeniem sieciowym, obsługą chmury, tworzeniem kopii zapasowych, możliwości szyfrowania plików, stosowaniem podpisów elektronicznych oraz podłączaniem urządzenia do komputera.

Słowa kluczowe: bezpieczeństwo informacji; urządzenia mobilne; systemy operacyjne

*Autor do korespondencji.

Adres e-mail: buryta.michal@gmail.com

Comparison of the security mechanisms of popular operating systems for mobile devices

Michał Buryta*, Piotr Kopniak
Institute of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract. The article concerns the differences in the mechanisms of securing the three most popular mobile platforms, which are Android, iOS and Windows Phone. Mainly focuses on the differences related to access to user data, installing and running applications, Internet access, network connectivity, cloud services, backup, file encryption capabilities, the use of electronic signatures and connect the device to your computer.

Keywords: information security; mobile devices; operating systems

*Corresponding author.

E-mail address: buryta.michal@gmail.com

1. Wstęp

Obecnie zdecydowana większość ludzi używa telefonów komórkowych wszędzie i do wszystkiego. Telefon pozwala na szybkie porozumiewanie się z innymi osobami w dowolnym miejscu, ale nie tylko. Telefony udostępniają wiele innych możliwości takich jak przeglądanie stron www, odczytywanie i wysyłanie poczty elektronicznej, wykonywanie operacji bankowych, używania telefonu zamiast karty płatniczej, przesyłanie danych po między różnymi urządzeniami. Smartfon przez to że udostępnia szereg powyższych usług, przechowuje dużo informacji o swoim użytkowniku. Do takich informacji zaliczają się między innymi numery kart kredytowych, piny, hasła do serwisów internetowych, dane osobowe, zdjęcia i filmy czy rozmowy głosowe zapisywane na urządzeniu. Wszystkie te możliwości oraz to, że samo urządzenie jest wartościowe sprawia, że telefony często są celem kradzieży. Wszystko to sprawia ze bardzo istotną sprawą jest bezpieczeństwo, poufność, zachowanie prywatności danych przechowywanych na urządzeniu oraz samego telefonu. Problemem koniecznym do rozwiązania jest więc zapewnienie odpowiedniej ochrony bez nadmiernego ograniczenia użytkownika. Ma to szczególne znaczenie również dlatego, że na platformach mobilnych jest trudniej rozpoznać zagrożenie. Sposobami na zapewnienie odpowiedniej ochrony telefonu są między innymi ograniczanie możliwości aplikacji przez uruchamianie ich w odrębnych izolowanych częściach pamięci, przydzielanie uprawnień tylko tych, które są niezbędne do poprawnego działania oraz świadome działanie użytkownika. Właśnie dla tego użytkownik powinien wiedzieć w jakim zakresie platforma jego telefonu oferuje bezpieczeństwo oraz na co mogą być wrażliwe jej mechanizmy zabezpieczające. Wiedza ta jest istotna nie tylko dla przedsiębiorstw, ale i każdego użytkownika telefonu

Niniejszy artykuł przedstawia różnice pomiędzy trzema najbardziej popularnymi platformami jakimi są Android, iOS i Windows Phone. Większość użytkowników wybiera obecnie urządzenia z systemem firmy Google. W pierwszym kwartale roku 2016 jest to ponad 80% z pośród wszystkich sprzedanych w tym roku. Wszystkich sprzedanych aparatów jest ponad 349 milionów w pierwszym kwartale roku 2016. Poniższa tabela przedstawia liczbę sprzedanych smartphonów oraz procentowy udział w rynku.

Tabela 1. Światowa sprzedaż smartphone dla użytkownika końcowego 1 kwartał roku 2016 [1]

System operacyjny	1Q16	1Q16 Udział w rynku (%)	1Q15	1Q15 Udział w rynku (%)
Android	293771.2k	84.1	264941.9k	78.8
iOS	51629.5k	14.8	60177.2k	17.9
Windows	2399.7k	0.7	8270.8k	2.5
Blackberry	659.9k	0.2	1325.4k	0.4
Others	791.1k	0.2	1582.5k	0.5
Suma	349251.4k	100	336297.8k	100

Tabela 2. Światowa sprzedaż smartphone dla użytkownika końcowego 2 kwartał roku 2016 [2]

System operacyjny	2Q16	2Q16 Udział w rynku (%)	2Q15	2Q15 Udział w rynku (%)
Android	296912.8k	86.2	271647.0k	82.2
iOS	44395.0k	12.9	48085.5k	14.6
Windows	1971.0k	0.6	8198.2k	2.5
Blackberry	400.4k	0.1	1153.2k	0.3
Others	680.6k	0.2	1229.0k	0.4
Suma	349251.4k	100	330312.9k	100

2. Cel, przedmiot badań pytania badawcze

Celem przeprowadzanych badań była analiza i porównanie mechanizmów zabezpieczających instalację i uruchamianiem oprogramowania, dostępu do danych, dostępem do telefonu i podczas łączenia się z komputerem. Przedmiotem analizy był poziom zabezpieczeń trzech platform mobilnych jakimi są Android firmy Google, iOS firmy Apple oraz Windows Phone firmy Microsoft. Główne pytania jakie były stawiane przed rozpoczęciem prac to, która platforma jest najlepiej zabezpieczona i czy ocena zabezpieczeń ulegnie zmianie w zależności od sposobu użytkowania telefonu oraz jego przeznaczenia.

2.1. Obszar badań

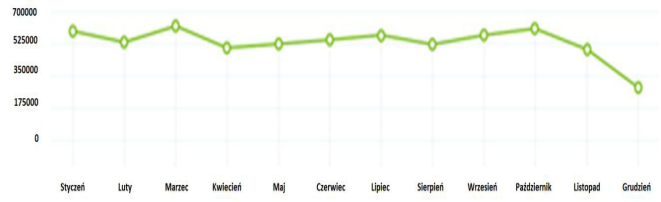
Wszystkie trzy platformy posiadają podobny zabezpieczenia, które różnią się stopniem zapewnianego bezpieczeństwa oraz wykonaniem. Częścią wspólną dla aplikacji uruchamianych w badanych systemach jest fakt, że każda z aplikacji jest uruchamiana na oddzielnej części pamięci i nie ma dostępu do innych aplikacji. Jest to tak zwana piaskownica, która ma za zadanie odizolować każdą aplikację na czas jej działania w przydzielonej części pamięci. Istnieją mechanizmy, które zapobiegają odwoływaniu się do tej samej komórki pamięci przez dwa różne programy gdy działają w tym samym czasie. Oznacza to, że aplikacja nie może się odwołać do pamięci zarezerwowanej dla innego programu przed zakończeniem działania programu, któremu przydzielona jest ta komórka pamięci. Z tego można wywnioskować że każda aplikacja musi być samodzielna i nie ma żadnego dostępu do danych zewnętrznych. Na szczęście nie jest tak. Aplikacje mogą używać danych pobranych z Internetu oraz przesyłać do innych aplikacji za pośrednictwem odpowiednich mechanizmów systemowych.

Kolejną częścią wspólną dla badanych platform związaną z aplikacjami jest miejsce z którego można je uzyskać. Każda z platform ma swoje własne miejsce, gdzie użytkownik może poszukiwać odpowiednich dla siebie programów oraz je pobierać na swój telefon. Dla iOS jest to Apple AppStore. Dla Androida jest to Google Play. Dla Windows Phone jest to Windows Phone Marketplace. Wszystkie firmy przed udostępnieniem aplikacji sprawdzają ją pod kontem złośliwego oprogramowania oraz poprawnością działania. Nie każdy może dodać aplikację do wybranej platformy. Każda firma wymaga aby programiści przed dodaniem pierwszej aplikacji założyli konto za pomocą którego będzie można dokładnie zweryfikować czyja jest to aplikacja. Najtrudniej założyć konto programisty dla systemu iOS, ponieważ firma Apple bardzo restrykcyjnie podchodzi do sprawy tworzenia nowych kont. Apple oraz Google nie zezwalają na uruchomienie aplikacji na ich telefonach, które nie posiadają ważnych licencji wystawionych przez ich serwis z aplikacjami. W systemie Android istnieje metoda, która umożliwia instalację oraz uruchamianie aplikacji z poza Google Play. Android posiada prawdopodobnie najsłabszą metodę sprawdzania czy dodawana aplikacja może być złośliwa, ponieważ są wykrywane wirusy w Google Play[3]. Android posiada też możliwość usunięcia dowolnej aplikacji z telefonów użytkowników, która została ściągnięta z Google Play. Wirusy, którym udaje się przejść przez zabezpieczenia Androida i dotrzeć do użytkownika mogą próbować doinstalować do siebie dodatki z poza marketu co może być poważnym zagrożeniem bezpieczeństwa. Jednak od Androida w wersji 6.0 uprawnienia aplikacji weryfikowane są na bieżąco przy każdej próbie wykorzystania zabezpieczanych części systemu co uniemożliwia doinstalowanym automatycznie aktualizacjom aplikacji wykonywanie niebezpiecznych operacji bez wiedzy użytkownika. W większości platform nie ma systemowego menadżera plików. Co spowodowało, że można pobrać tego typu aplikację z odpowiedniego miejsca, która działa jak zwykły menadżer plików. Za pomocą menadżera plików można zainstalować na platformie Android aplikację z karty pamięci lub komputera.

Jedyną platformą na której dostępne są programy antywirusowe jest Android. Spowodowane jest to tym, że jako jedyna potrzebuje takich aplikacji. Natomiast już wszystkie platformy posiadają wszelkiego typu programy zabezpieczające przed phishingiem, niebezpiecznymi

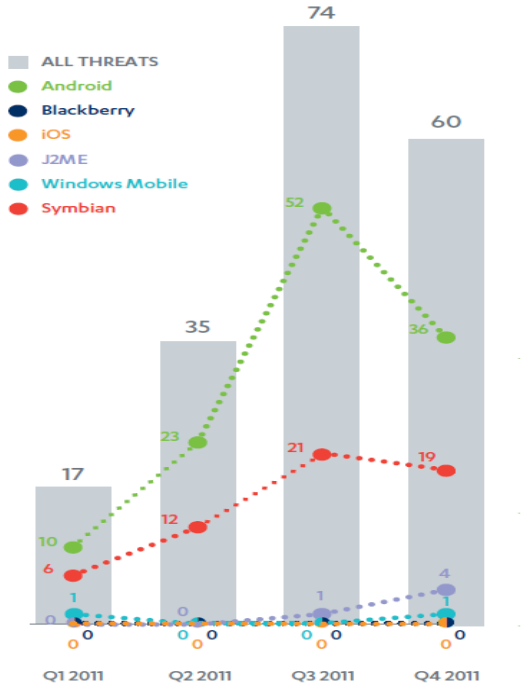
stronami czy sprawującymi tak zwaną kontrolę rodzicielską. Dla wszystkich trzech platform istnieją aplikacje, które umożliwiają bezpieczne przechowywanie poufnych danych takich jak hasła, zdjęcia prywatne czy dokumenty na telefonie. Programy tego typu używają algorytmów takich jak AES czy BlowFish do szyfrowania danych. Algorytmy te zapewniają wysoki poziom bezpieczeństwa. Każda platforma posiada również aplikacje za pomocą której można odnaleźć telefon, zdalnie go zablokować lub też przywrócić fabryczne ustawienia i wyczyścić całą pamięć telefonu. Należy jednak wcześniej wprowadzić dane telefonu do tego typu usługi. Możliwość zaszyfrowania danych na telefonie została dodana do wszystkich systemów przez ich producentów. Do szyfrowania konieczne jest ustawienia hasła lub pinu. Szyfrowanie może znacznie spowolnić pracę telefonu. Jedną z form zabezpieczenia danych przed utratą jest tworzenie kopii zapasowej. Producenci badanych systemów mobilnych udostępniają aplikacje, które pozwalają na tworzenie kopi zapasowej na komputerze. Są to proste i wygodne rozwiązania. Niestety firma Microsoft bardzo ograniczyła dane jakie można zabezpieczyć przed utratą w ten sposób, natomiast Firma Google pozwala nawet bez dodatkowych aplikacji na tworzenie kopi zapasowej na komputerze. W przypadku przywracania plików systemowych mogą wystąpić problemy. Oczywiście kopię zapasową można automatycznie tworzyć w chmurze udostępnianej przez producenta. Takie rozwiązanie istnieje na wszystkich trzech platformach i jest bardzo wygodne. W tym przypadku najlepiej wypada Android, ponieważ udostępnia najwięcej miejsca oraz pozwala na zrobienie kopii zapasowej całego telefonu łącznie z aplikacjami. Apple niestety nie pozwala na tworzenie kopii zapasowej plików, których pochodzenie jest nieznane. Czyli wszystkich plików, które nie zostały stworzone za pomocą telefonu[4,5,6].

Jednym z najbardziej popularnych Trojanów, za pomocą których cyberprzestępcy próbują zabrać nasze pieniądze są tak zwane Trojany SMS. Taka szkodliwa aplikacja wysyła SMS'y premium i zapisuje nas do różnych usług. Takie aplikacje zostały wykryte ponad 6 mln razy na urządzeniach z Androidem.

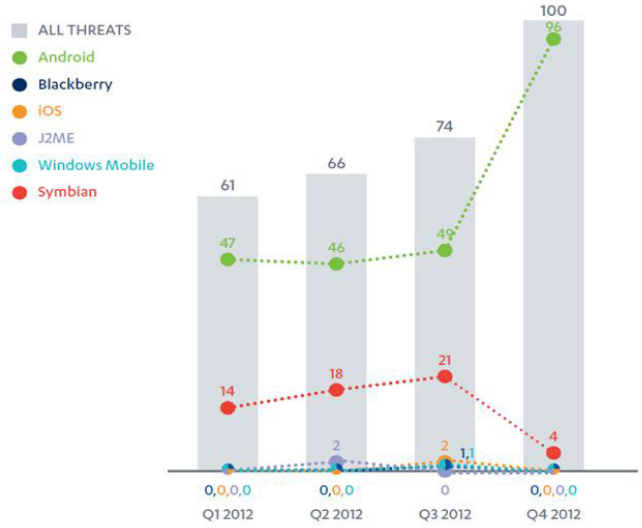


Rys. 1. Liczba wykrytych Trojanów SMS Android w roku 2015 [7]

Jak widać na Rys. 1 liczba takiego oprogramowania spada. Jest to spowodowane coraz lepszymi programami antywirusowymi, ale także coraz większą popularnością Trojanów bankowych pośród cyberprzestępców[7]. Firma F-Secure w 2014 roku opublikowała raport bezpieczeństwa dotyczący urządzeń mobilnych w pierwszym kwartale tego roku. Okazuje się, że aż 99% nowych zagrożeń mobilnych dotyczy Androida: z 277 nowych złośliwych programów aż 275 jest wymierzona w platformę Firmy Google. Pozostałe dwa są wycelowane w iOS i Symbiana[8]. W poprzednich latach sytuacja była podobna co przedstawiają poniższe wykresy przygotowane przez tą samą firmę.

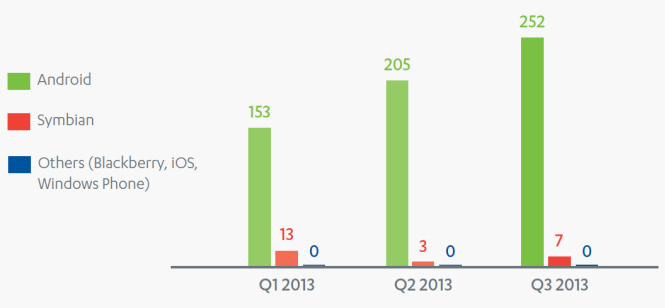


Rys. 2. Liczba wykrytego nowego złośliwego oprogramowania dla poszczególnych platform mobilnych w roku 2011 [9]

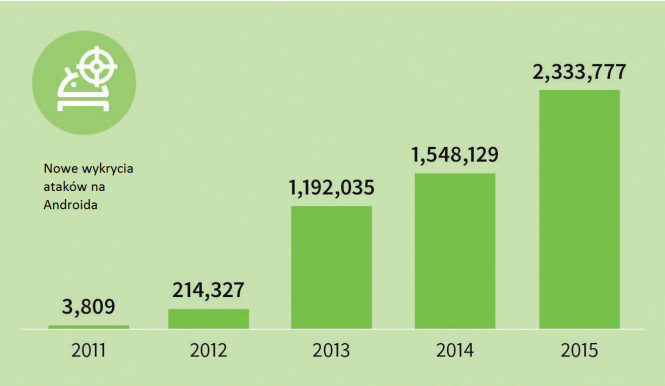


Rys. 3. Liczba wykrytego nowego złośliwego oprogramowania dla poszczególnych platform mobilnych w roku 2012 [10]

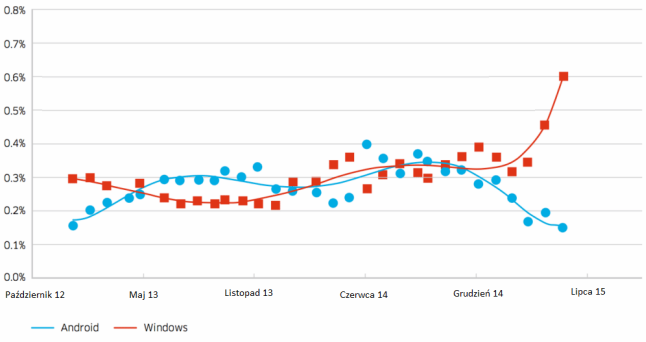
Na pierwszy rzut oka widać że najwięcej złośliwego oprogramowania pojawia się na platformę Android. Przyczynami tego zapewne jest to że na urządzenia te można instalować oprogramowanie z poza oficjalnego sklepu, platforma ta jest również najpopularniejszą co daje potencjalnie największą możliwą liczbę zainfekowanych telefonów.



Rys. 4. Liczba wykrytego nowego złośliwego oprogramowania dla poszczególnych platform mobilnych w roku 2013 [11]



Rys. 5. Liczba wykrytych ataków na Androida w poszczególnych latacha [12]



Rys. 6. Procent zarażonych urządzeń na poszczególnych platformach[13]

3. Wnioski

Artykuł prezentuje ogólny zarys systemów zabezpieczających trzech najpopularniejszych platform mobilnych. Głownie pod kontem analizy i porównania mechanizmów zabezpieczających instalację i uruchamianiem oprogramowania, dostępu do danych, dostępu do telefonu i podczas łączenia się z komputerem. Ze względu na stosowaną przez firmy Apple oraz Microsoft kontrolę nad dodawanymi do ich sklepów aplikacjami, dużą liczbę zabezpieczeń oraz politykę firm nastawioną na bezpieczeństwo można stwierdzić, że obie mają bardzo wysoki poziom zabezpieczeń, który jest bardzo zbliżony do siebie ale wyższy od tego jaki posiadają urządzenia firmy Google. Najsłabiej zabezpieczony jest Android. Prawdopodobnie spowodowane jest to polityką firmy, która bardziej niż konkurencja stawia na możliwość personalizacji telefonu. Firma Apple i Microsoft stawiają bardzo dużą wagę na zabezpieczenie danych w telefonach, które posiadają ich mobilny system operacyjny. Koleją przyczyną częstszego atakowania systemu Androida przez złośliwe oprogramowanie może być największa liczbę użytkowników, która obecnie wynosi około 80% z pośród badanych platform mobilnych oraz to że wielu użytkowników posiada za małą świadomość o zagrożeniach. Co sprawia że na ten system pisane jest najwięcej złośliwego oprogramowania. Z czego natomiast wynika że najwięcej ludzi pracuje nad złamaniem zabezpieczeń Androida. Platforma Windows Phone posiada zabezpieczenia na poziomie zbliżonym do zabezpieczeń firmy Apple. Spowodowane jest to podobną polityką firmy związana z poziomem zabezpieczeń danych na telefonach z ich systemem, oraz tym że obie firmy posiadają bardzo podobne wymagania klientów co do zabezpieczeń danych.
Fakt że Android ma najwięcej zarejestrowanych programistów aplikacji w serwisie Google Play, też sprawia, że Google ma najwięcej pracy przy sprawdzaniu i testowaniu nowych aplikacji. Przez co pracownicy mogą przeoczyć niektóre zagrożenia. Z faktu liczby programistów wynika też, że Android posiada zapewne najwięcej niedoświadczonych programistów, którzy popełniają błędy i piszą niezoptymalizowane aplikacje, które mogą wykorzystywać za dużo zasobów urządzenia. Przy wyborze systemu operacyjnego urządzenia należ zadać sobie kilka pytań. Czy będę używał telefonu do przechowywania bardzo ważnych i wrażliwych danych takich jak numery kart kredytowych, pin karty kredytowej czy hasła i loginy do portali internetowych. Jeżeli tak to najbezpieczniej jest wybrać urządzenie z systemem Windows Phone. Innym pytaniem jest czy nasz telefon powinien mieć możliwość szybkiego przywracania swoich poprzedniej wersji? Tego typu pytanie mogą zadać sobie na przykład programiści, którzy mają zamiar używać telefonu do testowania swoich aplikacji. Wszystkie platformy posiadają podobne rozwiązania problemów, które stawia przed nimi system operacyjny, użytkownicy oraz zagrożenia ze strony złośliwego oprogramowania. Wnioskować z tego można że poziom zabezpieczeń podyktowany jest polityką firmy lub poziomem rozwoju danego mobilnego systemu operacyjnego. W dalszej pracy nad zabezpieczeniami platform mobilnych należałoby zbadać świadomość użytkowników na zagrożenia jakie występują przy używaniu telefonu. Określić w jakim kierunku zamierzają podążać badane systemy. Przebadać poziom wiedzy i umiejętności programistów, którzy piszą programy dla poszczególnych platform.

Literatura

[1] Rob van der Meulen, Gartner Says Worldwide Smartphone Sales Grew 3.9 Percent in First Quarter of 2016, http://www.gartner.com/newsroom/id/3323017 [5.01.2016].

[2] Przeglad wirusów mobilnych – rok 2015, http://news.drweb-av.pl/show/review/?i=9779 [11.01.2016].

[3] Maciej Gajewski, 700 tysięcy złośliwych aplikacji w Google Play?, http://www.chip.pl/news/bezpieczenstwo/wirusy/2013/08/700-tysiecy-zlosliwych-aplikacji-w-google-play [13.01.2016].

[4] Krystian Bezdzietny, iOS jest tak bezpieczny, że nawet NSA nie jest w stanie go zhakować,

http://komorkomania.pl/5870,ios-jest-tak-bezpieczny-ze-nawet-nsa-nie-jest-w-stanie-go-zhakowac [11.01.2016].

[5] Mobile Threat Report Q3 2013, https://www.f-secure.com/documents/996508/1030743/Mobile_Threat_Report_Q3_2013.pdf [9.01.2016].

[6] Mobile Threat Report Q4 2012, https://www.f-secure.com/documents/996508/1030743/Mobile+Threat+Report+Q4+2012.pdf [9.01.2016] .

[7] Rob van der Meulen, Gartner Says Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016, http://www.gartner.com/newsroom/id/3415117 [5.01.2016].

[8] Mateusz Żołyniak, Android pod ostrzałem! Jak sprawdzić, czy twój telefon nie wykopuje bitcoinów, http://komorkomania.pl/1349,jak-sprawdzic-czy-twoj-telefon-nie-wykopuje-bitcoinow [5.01.2016].

[9] Mobile Threat Report Q3 2012, https://www.f-secure.com/documents/996508/1030743/Mobile+Threat+Report+Q3+2012.pdf [9.01.2016].

[10] Robert Hajduk, Szyfrowanie na WP8 (tylko) dla biznesu, https://wpworld.pl/12778/szyfrowanie-na-wp8-tylko-dla-biznesu [12.01.2016].

[11] Adam Golański, Trzeba było uczyć się od Apple, czyli jak całodyskowe szyfrowanie Androida okazało się do niczego, http://www.dobreprogramy.pl/Trzeba-bylo-uczyc-sie-od-Apple-czyli-jak-calodyskowe-szyfrowanie-Androida-okazalo-sie-do-niczego,News,74534.html [12.01.2016].

[12] G DATA Mobile Malware Report, http://pliki.gdata.pl/partner/materialy_prasowe/2016/02/MMWR_EN_Q42015.pdf [15.01.2016].

[13] Dan Rowinski, Less Than 1% Of Smartphones Are Infected With Malware, https://arc.applause.com/2015/09/21/android-malware-infection-rates [16.01.2016].