G Data

Focus paper 01/2012

Android pod ostrzałem – analiza przyczyn i zagrożeń

G Data SecurityLabs
by Eddy Willems

Go safe. **Go safer. G Data.**

Android pod ostrzałem – analiza przyczyn i zagrożeń

System Android ma duże predyspozycje, aby stać się drugim systemem najbardziej narażonym na cyber-ataki, zaraz za Microsoft Windows. Tak twierdzi większość specjalistów IT, w tym specjaliści G Data, podsumowując 2011 rok. Ale dlaczego akurat Android spośród wszystkich systemów na urządzenia mobilne zasłużył sobie na taką ocenę? Artykuł ten stara się rzucić więcej światła na tę kwestię oraz pokazać, że trzy główne cechy każdego przestępstwa zagościły w Androidzie: motyw, środki i możliwości.

Motyw

Przestępczość komputerowa zaczęła się wraz z rozpowszechnieniem systemu Windows. Jednak przyczyna tego nie leżała w słabości systemu czy ilości dziur bezpieczeństwa, jak wiele ludzi sądzi. Każdy utalentowany haker po jakimś czasie odnajdzie słabe strony systemu. Tak więc przyczyną odkrycia wszelkich błędów zabezpieczeń Windows jest taka, że miliony osób spędziło miliony godzin na odnajdywanie ich. Te poświęcenie czasu podyktowane jest prawdopodobieństwem przyszłych zysków. Około 90% użytkowników komputerów korzysta z systemu Windows[1], co przekłada się na około 1,35 miliarda osób na świecie (zakładając, że na świecie działa 1,5 miliarda aktywnych komputerów[2]). Znalezienie „właściwego" błędu zabezpieczeń i napisanie wydajnego złośliwego oprogramowania, które go wykorzystuje, oznacza potencjalny rynek dla hakerów. *„Posiadając odpowiednie oprogramowanie, można przejąć kontrolę nad komputerami wpinając je do sieci botnet i przeglądając w celu zlokalizowania danych, zarówno prywatnych, jak i finansowych, które mogą zostać użyte zarówno jako przedmiot handlu na czarnym rynku, bądź bezpośrednio w celu wykorzystania skradzionej tożsamości do przestępczych działań."* – Komentuje Łukasz Nowatkowski, Dyrektor Bezpieczeństwa IT G Data Security. Szacuje się, że roczne zarobki hakerów przekraczają wartością obroty przemysłu narkotykowego. W skrócie: niektórym osobom opłaca się poświęcić czas na tworzeniu niebezpiecznego oprogramowania na system Windows.

Oczywiście pojawią się i wciąż będą się pojawiać inne popularne platformy oprócz Windowsa. Chociażby OS X firmy Apple, czy Linux, których popularność wciąż rośnie. Wielu użytkowników wierzy, że systemy te są o wiele bezpieczniejsze od Windowsa. Jednak taki wniosek można postawić dopiero po spędzeniu tyle czasu na szukaniu usterek, jaki czas spędzono na szukaniu ich w systemie Windows. Co nie miało miejsca, dlatego powstrzymamy się od takiego wartościowania bezpieczeństwa jednych systemów nad innymi. Taka teoria odnosi się również do platform mobilnych. Smartfony istnieją od wielu lat. I pomimo faktu, że w lutym 2011 r. sprzedano więcej smartfonów niż komputerów osobistych3, odpowiednik systemu Windows na platformy mobilne nie utrzymał pozycji monopolisty. Istniało wiele różniących się systemów operacyjnych, z których żaden nie osiągnął pozycji lidera przez wiele lat. Nadal za aktualne możemy uznać stwierdzenie, że wszystkie one mają swoje słabości, jednak niewiele osób poświęca swój czas na odnalezienie ich z powodu małych zwrotów z zainwestowanego czasu. Jednak zaczyna się to zmieniać.

W roku 2010 Android zaczął wysyłać nieśmiałe sygnały, że chce większej części tortu z rynku urządzeń mobilnych. Już rok później ambicje te przerodziły się w największy udział Androida na rynku oprogramowania urządzeń mobilnych. Badania przeprowadzone przez szereg analityków i badaczy dowiodły pierwszeństwa tego systemu w badaniu preferencji konsumenckich. Gartner dowiódł, że Android osiągnął największą przewagę na rynku światowym w trzecim kwartale 2011 r.: 52,5% wszystkich sprzedanych smartfonów zainstalowane miało właśnie ten system operacyjny. Na miejscu drugim plasował się Symbian z 16%, co czyni dużą różnicę. Trzecią pozycję zajmował Apple z 15% rynku. Ze wszystkich systemów, tylko Android relatywnie zwiększył swój udział w rynku w trzecim kwartale 2011 r.[4] Środowisko naukowe zajmujące się bezpieczeństwem IT potwierdza, że Android wygrywa ten wyścig. Natomiast środowiska programistów piszących złośliwe oprogramowanie przyklaskuje temu stwierdzeniu. „Rozgryzienie" systemu, którego używa ponad połowa użytkowników stwarza wiele możliwości i jest poważnym motywem do tworzenia wysokiej jakości oprogramowania wykorzystywanego w cyber-przestępczości.

[1] http://en.wikipedia.org/wiki/Microsoft_Windows#Usage_share
[2] http://www.worldometers.info/computers/
[3] http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22689111&sectionId=null&elementId=null&pageType=SYNOPSIS
[4] http://www.gartner.com/it/page.jsp?id=1848514

Copyright © 2012 G Data Software

Środki

Przed Androidem inny konkurent wydawał się prowadzić w zestawieniu: Symbian. Dlaczego więc nie byliśmy świadkami epidemii złośliwego oprogramowania na ten system? Odpowiedź jest prosta: brak środków do rozprzestrzenienia złośliwego oprogramowania. Wszystkie mobilne systemy operacyjne mają jedną wspólną cechę: architektura ich kodu źródłowego różni się w dużym stopniu od systemu Windows. Mówiąc ogólnie, wygląda na to, że dostawcy systemów operacyjnych przyjrzeli się bliżej błędom pierwotnych wersji pecetowych systemów operacyjnych i stworzyli daleko bardziej bezpieczną wersję (która mimo wszystko nie jest wolna od potencjalnych zagrożeń). Zarażenie smartfona i rozprzestrzenianie niebezpiecznego oprogramowania wykorzystując tradycyjne metody nie jest proste. Najbardziej efektywny sposób ataków na Symbian przeprowadzany jest poprzez łącze Bluetooth. Jednak taka forma ingerencji wymaga fizycznego zbliżenia się do urządzenia, które do tego musi mieć uruchomione łącze Bluetooth. Zmniejsza to grono osób mogących doświadczyć potencjalnego ataku. Fakt ten mocno zniechęcił hakerów, dla których nie był to łakomy kąsek. Sprawa z Androidem wygląda zupełnie inaczej. Tutaj mamy proste narzędzie służące rozprzestrzenianiu się potencjalnych zagrożeń: aplikacje. Ściągamy i instalujemy je manualnie, tak jak właściciele smartfonów na całym globie. Darmowa lokalna aplikacja o średniej popularności pobierana jest średnio 10000 razy. Międzynarodowe aplikacje o podobnej popularności już 1 milion razy. Fałszywe aplikacje pojawiające się w Android Market, jak te które ukrywały konia trojańskiego DroidDream, zostały pobrane ponad 250000 razy w ciągu zaledwie kilku dni. Dlatego to właśnie aplikacje są najbardziej atrakcyjnym sposobem rozprzestrzeniania niebezpiecznego oprogramowania do smartfonów. Środki stosowane przez tzw. inżynierię społeczną czynią aplikacje atrakcyjnymi i skłaniają użytkowników do ich ściągania i instalowania. Nie powstały jak dotychczas automatyczne procesy instalacji, jednak może to być tylko kwestią krótkiego czasu.

Możliwości

Trzeba tu jednak podkreślić fakt, że Android nie jest jedyna platformą, na którą powstały popularne aplikacje. To Apple, aż do drugiego kwartału 2011 r.[5], wygrywał tę rywalizację. Spodziewano się, że system stosowany przez Apple wypełni lukę po spadku popularności Symbiana. Więc jak udało się popularnemu koncernowi z symbolem jabłka uniknąć fali włamań? Był motyw, a aplikacje dostarczały teoretycznie środków do infekowania.

Odpowiedź kryje się w możliwościach. A raczej w ich ograniczeniach. Apple i Android posiadają różne procesy tworzenia i zarządzania aplikacjami. W tym wypadku trzeba uznać, że system Apple wygląda na lepiej zabezpieczony. Co nie znaczy, że sam w sobie jest bezpieczniejszy niż Android. Jednak trudniejsze jest rozpoznanie słabych stron Apple z powodu bardziej zamkniętej natury systemu. Natomiast kiedy słabość systemu Apple zostanie wykryta, bardzo ciężko umieścić wykorzystującą ją aplikację w Appstore, z powodu restrykcyjnej polityki tworzenia nowych, autoryzowanych aplikacji przez Apple.

Systuacja z Adroidem przedstawia się zupełnie inaczej. Android stworzony został jako platforma open-source, co oznacza że duża część kodu jest powszechnie dostępna. Ułatwia to znajdywanie luk bezpieczeństwa. Czyni to także łatwiejszym tworzenie niebezpiecznych aplikacji. W przeciwieństwie do Apple, Android opiera się na użytkownikach, którzy sami okreslają jakie nadać uprawnienia instalowanym przez nich aplikacjom. Raczej naiwne wydaje się domniemanie że użytkownicy są zawsze uważni i przywiązują wagę do instalowania aplikacji. Wszystkie te fakty połączone z niezbyt restrykcyjną selekcją autoryzowanych aplikacji, czynią z Androida dużo łatwiejszy cel i dają duże pole do popisu dla cyber-przestępców.

Warunki publikowania aplikacji		
	Apple	Android
Opłata rejestracyjna dla wydawców (karta kredytowa)	€ 99	€ 25
Opłata roczna dla wydawców (karta kredytowa)	€ 99	-
Sprawdzanie aplikacji przez dział techniczny marketu przed publikacją	Tak	Nie

[5] http://www.abiresearch.com/press/3799-Android+Overtakes+Apple+with+44%25+Worldwide+Share+of+Mobile+App+Downloads

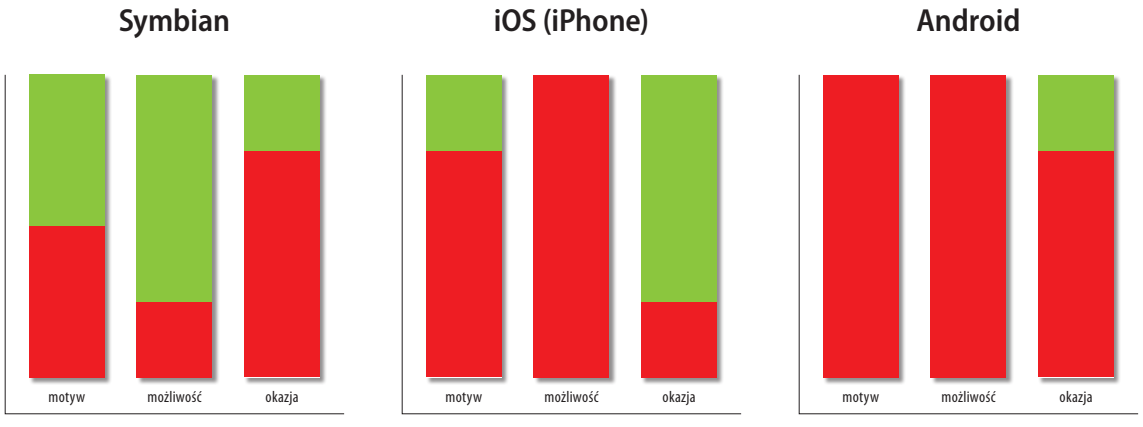
Copyright © 2012 G Data Software

Kolejnym czynnikiem, który sprawia że Android jest atrakcyjnym systemem dla twórców niebezpiecznego oprogramowania, jest sposób w jaki formułowane jest nadawanie uprawnień aplikacjom. Zamiast pytać użytkownika o pozwolenia dla konkretnej aplikacji, Android prosi o nadanie uprawnień twórcom/autorom aplikacji. Jeśli użytkownik w przyszłości zainstaluje aplikację stworzoną przez tych samych twórców/wydawcę, aplikacja ta może użyć uprawnień nadanych wcześniej innemu programowi. Z drugiej strony, wcześniej zainstalowana aplikacja może użyć uprawnień nadanej późniejszej aplikacji. Sytuacja ta daje duże ułatwienia twórcom złośliwego i niebezpiecznego oprogramowania w uzyskaniu uprawnień. Oszczędza to twórcy problemów z koniecznością stosowania specjalnych trików w celu wysyłania niebezpiecznych aktualizacji poprawnie działających aplikacji zainstalowanych na smartfonie.

Łukasz Nowatkowski, Dyrektor Bezpieczeństwa IT G Data Security: *„Łatwo wyobrazić sobie jak bardzo podekscytowani muszą być cyber-przestępcy na myśl o aplikacjach poprzez które wykonywane są płatności poprzez urządzenia mobilne, bądź które dają dostęp do bankowości internetowej. Będzie to dużo bardziej zyskowne, niż wysyłanie z zainfekowanych urządzeń drogich sms-ów, co już jest popularnym procederem zarobkowym. Na Bliskim Wschodzie i w Rosji płacenie za pomocą telefonów staje się coraz bardziej popularne. Zauważamy że niebezpieczne oprogramowanie nakierunkowane na tego typu płatności rozprzestrzeniają się dużo szybciej właśnie w tych regionach, co tylko potwierdza fakt, że cyber-przestępczość skupiać się będzie na tego typu przepływach pieniężnych."*

Konkluzje

Patrząc na trzy element przestępstwa i w jakim stopniu kolejne trzy najpopularniejsze mobilne systemy operacyjne im sprzyjają, czas dokonać ostatecznego porównania. Android jest jedynym systemem, który posiada mocno rozwinięte wszystkie te elementy, co czyni go doskonałym celem. Jedyny element, który broni się w pewnym stopniu, wynika z wymogu akceptacji przez użytkownika uprawnień nadawanych instalowanej aplikacji. Jednak nie byliśmy jeszcze świadkami samo instalującej się aplikacji, której powstanie jest jedynie kwestią czasu. Obawiamy się, że kiedy ta ostatnia przeszkoda zostanie usunięta, tworzenie groźnych aplikacji na Androida stanie się praktycznie przestępstwem idealnym.



Copyright © 2012 G Data Software