G Data

Mobile MalwareReport

Półroczny raport zagrożeń styczeń – czerwiec 2013

G Data SecurityLabs

G Data. Security **Made in Germany**.

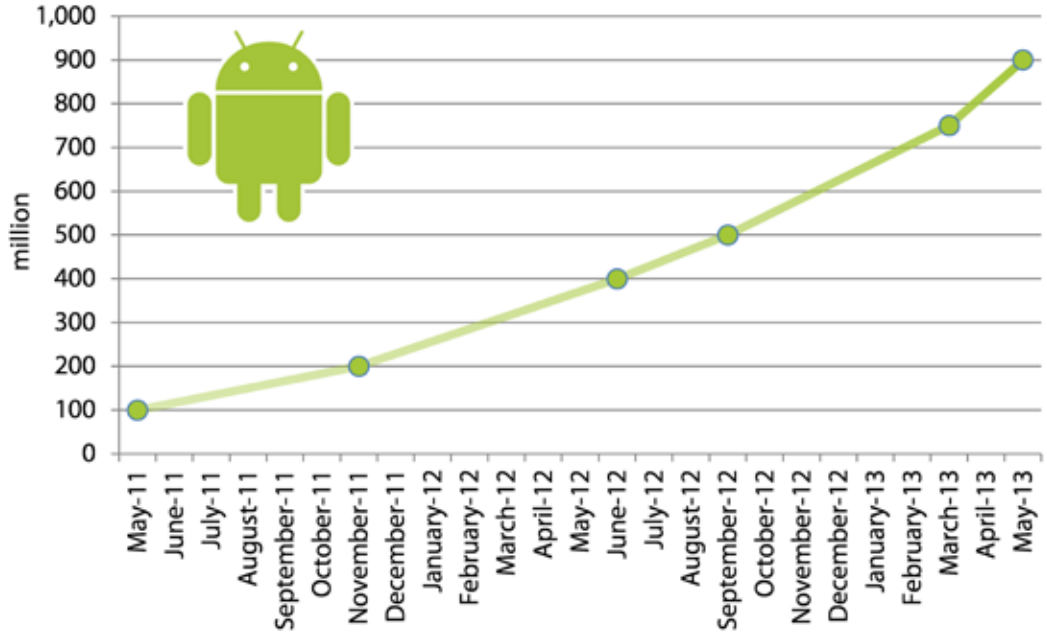
Spis treści

W skrócie

- System Android jest celem numer jeden wszystkich ataków skierowanych na urządzenia mobilne
- Liczba urządzeń z Androidem w rękach użytkowników na całym świecie osiągnęła już liczbę 1 miliarda
- Eksperci badający rynek urządzeń przenośnych przewidują 33% roczny wzrost w segmencie smartfonów
- Zgodnie z prognozami do roku 2015 co piąty telefon i tablet będzie chroniony odpowiednim oprogramowaniem zabezpieczającym
- Liczba nowych próbek złośliwego oprogramowania wzrosła gwałtownie w pierwszym półroczu 2013 roku do 519 095. W drugiej połowie roku 2012 eksperci z G Data SecurityLabs naliczyli 185 210 nowych próbek szkodliwych plików
- Średnio do naszego laboratorium trafiało 2868 nowych próbek dziennie!
- Specjalne zestawy do sporządzania szkodliwych programów oferowane przez twórców na podziemnych forach internetowych pozwalają na tworzenie złośliwych kodów przestępcom nieposiadającym wymaganej do tego wiedzy (tzw. script kiddies)
- Dzięki wspomnianym narzędziom do tworzenia złośliwych aplikacji na urządzenia mobilne (malware tool kits) eksperci z G Data prognozują znaczny wzrost liczby zagrożeń w drugiej połowie roku
- Android.Backdoor.Obad.A wykorzystuję aż trzy luki w oprogramowaniu by dokonać ataku na urządzenie z Androidem
- Trojan FakeSite.A (Perkele) nazwany tak ze względu na możliwość jego połączenia z dowolnym innym złośliwym oprogramowaniem dokonującym ataków webinject (wstrzykiwanie złośliwego kodu w treść strony wyświetlanej w przeglądarce użytkownika). Jest to elastyczny, wieloplatformowy trojan, który jest bardzo łatwy w użyciu i pozwala na ominięcie podwójnego uwierzytelniania przez SMS
- Legalne oprogramowanie pozwalające na zdalny dostęp do urządzeń z Androidem o nazwie „AndroRAT" zostało stworzone w celach akademickich i naukowych. Następnie zostało przejęte i przeprogramowane przez cyberprzestepców, by mogli je wykorzystać do swych kryminalnych celów
- Niektóre nowe szkodliwe programy mobilne starają się obejść automatyczną oraz ręczną analizę poprzez bardzo starannie zakamuflowany kod
- „Szybka kasa" to wciąż podstawowa motywacja dla atakujących. Jednakże eksperci spotykają się z coraz większą ilością złożonych i długoterminowych ataków

Czas Androida czyli wzrost totalny

Dawno minęły już czasy, kiedy złośliwe oprogramowanie na urządzenia przenośne było rzadkością. Nie łudźmy się że wrócą dni kiedy zdecydowanie częściej słyszeliśmy o mobilnych wirusach niż mieliśmy z nimi do czynienia. Cyberprzestępcy śledzą z wielką uwagą wyniki sprzedaży urządzeń z Androidem i są świadomi rosnącego potencjału tego rynku. W obecnej chwili koncentrują oni swoje wysiłki oraz działania na systemie z zielonym ludzikiem z którego korzysta już ponad miliard mieszkańców naszej planety[1]. Specjaliści badający rynek mobilny przewidują szybki wzrost liczby aktywowanych urządzeń, rzędu 33% rocznie, co tylko umacnia hakerów w podjętej już decyzji. Spowodowane jest to dużym spadkiem średniej ceny takich urządzeń. W 2011 za smartfon lub tablet płaciliśmy średnio 337€, by w 2013 cena ta osiągnęła 283€. W 2017 roku przewiduję się, że za średniej klasy sprzęt zapłacimy około 235€[2].



Rysunek 1 Liczba aktywowanych urządzeń z systemem Android

Konsekwencją tak dużej popularności jest różnorodność oraz duża liczba ataków na urządzenia mobilne z Androidem. Przestępcza nisza rozwinęła się dzięki wysokiej stopie zwrotu w stosunku do niewielkich kosztów poniesionych na tworzenie złośliwych aplikacji. Twórcy szkodliwego oprogramowania nie tylko wykorzystują je do przeprowadzania ataków, ale także oferują gotowe rozwiązania na przestępczych forach internetowych. Przykładem może być trojan Perkele (fin. diabeł) oferowany na rosyjskojęzycznych serwisach w dwóch wersjach. Jako „android malware kit" stargetowany wyłącznie na jeden bank w cenie 1000$ lub w pełnej wersji obejmującej swym zakresem nawet do 66 banków w cenie 15000$. Dostawcy gotowych narzędzi dla przestępców, którzy chcą rozszerzyć swoją działalność na wirtualny świat, nie ograniczają się jedynie do dostarczenia samego instrumentu. Prócz zestawów pozwalających na dokonanie ataku, oferują także kanał dystrybucyjny dla stworzonego wcześniej złośliwego kodu. Za odpowiednią opłata dostarczają zarejestrowane oraz zweryfikowane konta developerskie w serwisie Google Play. Pozwalają one na dotarcie do ogromnej liczby użytkowników ze złośliwym mobilnym oprogramowaniem oraz jego rozpowszechnianie. Konto które oficjalnie można zarejestrować za 25$ oferowane jest w cenie 100$[3].

[1] http://androidandme.com/2013/09/news/android-passes-a-billion-activations-next-version-will-be-kitkat/
[2] http://www.idc.com/getdoc.jsp?containerId=prUS24143513
[3] http://krebsonsecurity.com/2013/03/mobile-malcoders-pay-to-google-play/

Rysunek 2 Reklama zestawu zawierającego trojan Perkele

Popularnością cieszą się także przechwycone konta w usłudze Gmail, które mogą zawierać prawa dostępu do urządzeń mobilnych użytkownika a tym samym kontakty i inne ważne dane osobiste. Obecnie dostępne są narzędzia, które potrafią ustalić wartość danego konta Gmail na podstawie zawartych w nim informacji[4].

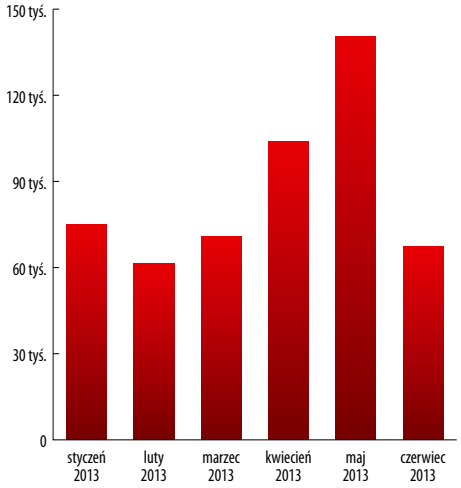
Oferowane zestawy pozwalają atakującym na tworzenie złośliwych aplikacji w bardzo krótkim czasie, bez specjalistycznej wiedzy jedynie dzięki kilku kliknięciom komputerowej myszy. Jak do tej pory rozwiązania te nie są jeszcze szeroko rozpowszechnione. W skutek wykorzystywania nowych rozwiązań i technologii, które stale poprawiają jakość nowych złośliwych programów oraz dzięki modułowej budowie i złośliwym kodom, które zostały już przetestowane w działaniu, lista zainfekowanych aplikacji wciąż wzrasta. Sprawdzone i przetestowane trojany są niezwykle popularne wśród sieciowych przestępców, czego przykładem może być opisany w dalszej części raportu trojan z rodziny Android.FakeInstaller.

[4] https://cloudsweeper.cs.uic.edu

Androidowy malware na fali

Liczba złośliwych aplikacji zależy od ilości ich nowych odmian, szkodliwych kodów opracowanych przez atakujących. W pierwszej połowie 2013 roku specjaliści z G Data SecurityLabs wykryli łącznie 519 095 nowych zainfekowanych plików[5]. Oznacza to wzrost o 180% w porównaniu do drugiej połowy 2012 roku (185 210 plików) i ponad 16-krotny wzrost w stosunku do pierwszej połowy 2012 (29 595 plików)[6]!

Średnio do laboratorium G Data SecurityLabs docierało 2868 nowych próbek szkodliwego oprogramowania na Androida każdego dnia.



Rysunek 3 Dystrybucja złośliwych plików, które mogą zostać przypisane do konkretnej rodziny

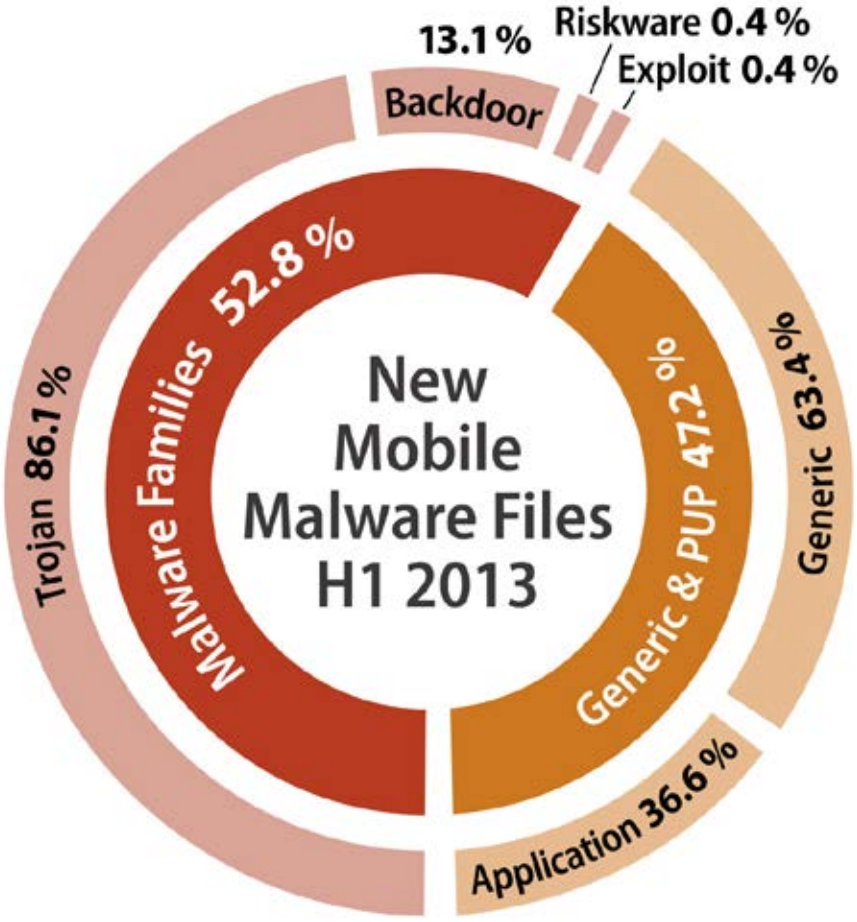
Opierając się na właściwościach złośliwego kodu[7], poszczególne pliki mogą zostać przypisane do określonych rodzin. Ponad 275 tysięcy nowych szkodliwych plików zostało jednoznacznie przypisanych do konkretnych rodzin złośliwego oprogramowania. W ramach wszystkich rodzin 1919 różnych wariantów złośliwego oprogramowania zostało scharakteryzowanych, zaliczają się one do 454 odmiennych rodzin. W ciągu sześciu miesięcy obejmujących badany okres, eksperci G Data zarejestrowali 203 całkowicie nowe rodziny. Tabela poniżej ilustruje najbardziej popularne i rozpowszechnione rodziny z największą ilością wariantów.

Nie dziwi fakt bezsprzecznej dominacji koni trojańskich w zestawieniu najpopularniejszych rodzin. Tak jak przez wiele lat miało to miejsce na komputerach osobistych, tak teraz trojany opanowały urządzenia mobilne. Wśród mobilnego malware'u trojany stanowią 46% wszystkich złośliwych plików, a wśród przypisanych do konkretnych rodzin aż 86% wszystkich sklasyfikowanych próbek.

Najbardziej do wzrostu znaczenia mobilnych trojanów w pierwszych sześciu miesiącach 2013 roku przyczyniła się rodzina Android. Trojan.FakeInstaller odpowiedzialna za 59% sklasyfikowanego złośliwego oprogramowania.

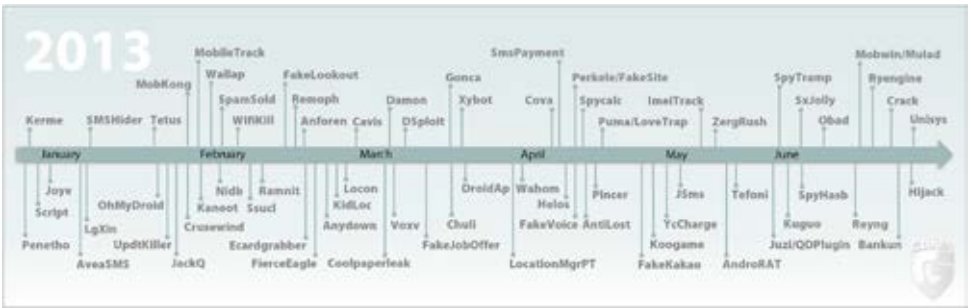
Rodzina	Liczba wariantów
Trojan.Agent	266
Trojan.FakeInsteller	168
Backdoor.GingerMaster	156
Trojan.SMSAgent	100
Trojan.SMSSend	92

[5] Androidowy malware może być zidentyfikowany na podstawie kilku plików. Plik instalacyjny (APK) zawiera pliki o charakterystycznym kodzie i właściwościach. Dzięki tej metodzie liczenia wykrycie wirusa w pliku APK i w jego poszczególnych częściach składowych są zestawione jako jeden szkodliwy plik.
[6] Dane mogą nieznacznie różnić się od wcześniej publikowanych przez SecurityLabs. W niektórych przypadkach pracownicy naszego laboratorium otrzymywali paczki nowych szkodliwych plików zbieranych przez długi okres czasu, które zawierały starsze pliki które zostały przypisane do wcześniejszych miesięcy.
[7] Liczba wariantów oparta jest na bazach sygnatur z których korzysta G Data MobileSecurity 2.



Rysunek 4 Podział nowych szkodliwych programów na urządzenia mobilne w I poł. 2013 roku

Wewnętrzny okrąg obrazuje podział nowych szkodliwych programów na pliki zaklasyfikowane do konkretnych rodzin na podstawie baz sygnatur (Malware Families) oraz te które zostały wykryte jako potencjalnie niebezpieczne na podstawie kontroli zachowania. Zewnętrzny okrąg ilustruje złośliwe pliki przypisane według ich rodzaju podstawie baz sygnatur G Data MobileSecurity 2 lub na podstawie analizy heurystycznej.



Rysunek 5 Wybrane szkodliwe programy dla urządzeń mobilnych w 2013 roku

Android.Backdoor.AndroRAT.A

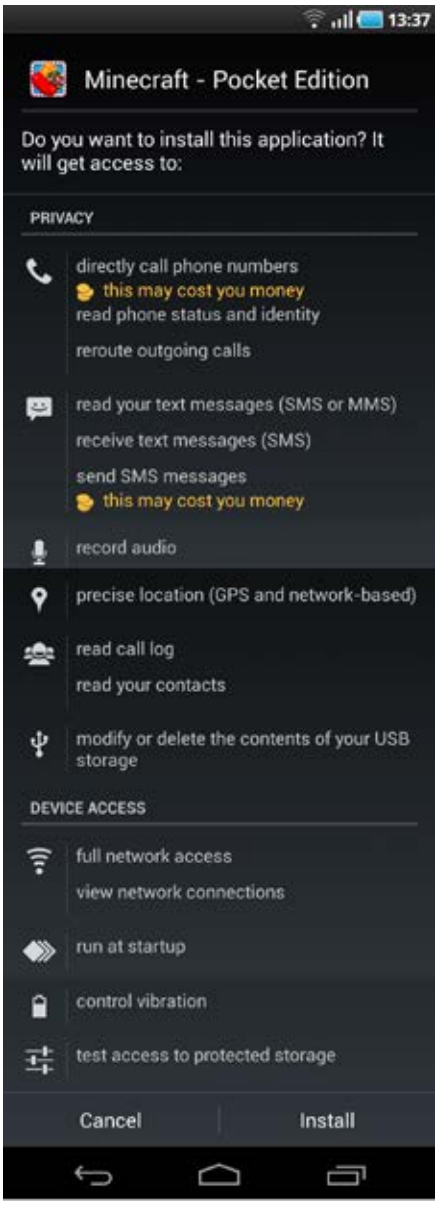
Androidowe aplikacje mogą mieć kilka punktów dostępowych (uprawnień), które mogą być uruchamiane ręcznie lub automatycznie przez konkretne działania wykonywane na urządzeniu. W przypadku smartfonu może to być np. przychodzące połączenie głosowe. Przykładowo taka sytuacja pozwala aplikacji na organizacje połączeń w smartfonie w taki sposób, by wznowić zawieszone połączenie kiedy program znów będzie funkcjonowała w normalnym trybie.

„Android APK Binder" dodaje nowy punkt dostępowy do zmodyfikowanej listy legalnej aplikacji. Tym samym kiedy urządzenie mobilne jest uruchomione, „AndroRAT" działa w tle bez wiedzy użytkownika. Od tego momentu smartfon lub tablet jest częścią botnetu, a osoba odpowiedzialna za atak posiada pełną kontrolę nad urządzeniem.

Obecnie dostępna wersja „AndroRAT" oferuje następujące funkcje:

- Przeglądanie kontaktów
- Przeglądani listy połączeń
- Dostęp do wiadomości SMS/MMS
- Lokalizacja urządzenia za pomocą GPS lub sieci komórkowej
- Informowanie o przychodzących połączeniach i wiadomościach
- Przekazywanie obrazów, nagrań wideo oraz audio na serwer atakującego
- Wyświetlanie komunikatów w formie niewielkich okien na urządzeniu użytkownika
- Wysyłanie SMS
- Wykonywanie połączeń
- Otwieranie witryn internetowych
- Włączanie alarmu wibracji

Od momentu kiedy to kod źródłowy legalnego „AndroRat" został udostępniony dla każdego, przestępcy mogą go kopiować, modyfikować oraz rozwijać w dowolny sposób. Zmodyfikowane aplikacje niekiedy mogą zostać wykryte na podstawie rozległych uprawnień na które trzeba wyrazić zgodę podczas instalacji (niezmodyfikowane aplikacje nie wymagają tak daleko idących uprawnień).



Rysunek 8 Szczegółowa lista uprawnień, których wymaga aplikacja zainfekowana Backdoor.AndroRAT.A.

Android.Backdoor.Obad.A

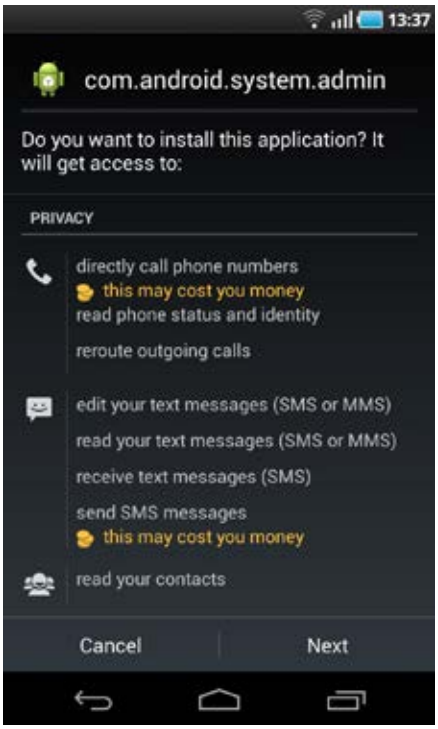
Backdoor.Obad.A to wysoce wyrafinowany złośliwe oprogramowanie, które po raz pierwszy pojawiło się w czerwcu 2013 na terytorium Chin. Backdoor wykorzystuje podczas ataku trzy luki systemowe: nieznaną wcześniej lukę w systemie Android, błąd w narzędziu o nazwie Dex2Jar oraz błąd w obsłudze pliku AndroidManifest.xml. Dwie ostatnie luki mają za zadanie utrudnić wykrycie samej infekcji.

Lista możliwych poleceń, które atakujący może przesłać do zainfekowanego urządzenia:

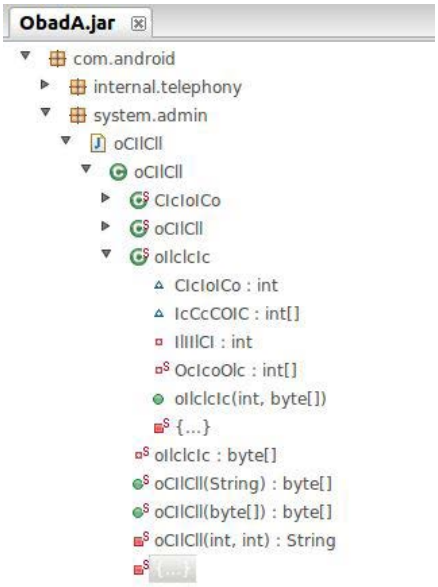
- Pełna kontrola nad urządzeniem
- Komunikacja z serwerem
- Przesłanie informacji po uruchomieniu urządzenia:
- Adres MAC
- Numer telefonu
- IMEI
- Zapytanie o uprawnienia administratora
- Zapytanie o zainstalowane aplikacje
- Zapytanie o kontakty
- Zapytania wykorzystujące kody USSD
- Kasowanie wiadomości pozwalające ukryć aktywność atakującego
- Pobieranie i instalowanie plików z serwera
- Wysyłanie plików poprzez Bluetooth
- Blokowanie wyświetlacza

Co jest szczególnie zdradliwe w opisywanym backdoorze Obad.A? Raz zainstalowany nie może zostać zwyczajnie usunięty przez użytkownika. Przez cały czas działa w tle, będąc niewidocznym dla właściciela urządzenia, które zostało zainfekowane.

Złośliwe oprogramowania ma bardzo szeroki zakres funkcji, wysoce wyszukaną metodę ukrywania złośliwego kodu oraz bardzo szybki czas reakcji na najnowsze luki bezpieczeństwa tzw. 0-day exploit. Wszystkie te cechy są charakterystyczne dla szkodliwego oprogramowania skierowanego na system Windows. Dlatego w przyszłości, możemy nie tylko oczekiwać zwiększenia ilości zagrożeń na Androida, ale także coraz bardziej rozbudowanego i złożonego oprogramowania infekującego urządzenia mobilne, które będzie o wiele cięższe do wykrycia dla analityków badających mobilne złośliwe kody.



Rysunek 9 Malware kamufluje się jako aplikacja systemowa. Jednak zezwolenie aplikacji na wykonywanie połączeń czy wysyłanie wiadomości tekstowych powinno wydać się użytkownikowi podejrzane.



Rysunek 10 Ukrycie nazwy klas i metod utrudnia śledzenie i wykrywanie działań backdoor'ów.

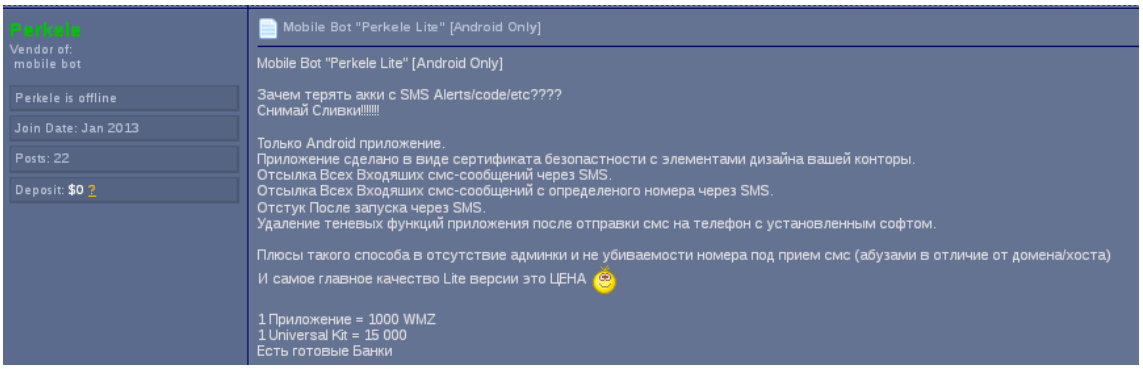
Android.Trojan.FakeSite.A (Perkele)

FakeSite.A (Perkele)[8] po raz pierwszy odkryty i nazwany został w pierwszej połowie 2013. Trojan ten nie jest znany z powodu wyszukanej budowy złośliwego kodu. Więc co czyni Perkele wyjątkowym? Atakujący mogą używać FakeSite.A z dowolnie wybranym malware'm wykorzystującym w swych atakach technikę webinject. Praktycznie są to wszystkie trojany bankowe, które są aktywne i obecnie wykorzystywane przez cyberprzestępców. Dzięki tej funkcjonalności możliwe jest użycie kombinacji Perkele wraz z dowolnym trojanem bankowym, co umożliwia przeprowadzanie ataków wieloplatformowych (Android/Windows).

Scenariusz ataku:

- Ofiara ataku trojana bankowego otwiera stronę logowania do konta w przeglądarce na swoim komputerze. Trojan wykorzystuje webinject, by zmanipulować stronę banku, którą w swojej przeglądarce widzi ofiara.
- Użytkownik nieświadomie przechodzi do spreparowanej przez przestępców strony i loguje się do swojego konta.
- Na zmanipulowanej stronie napastnicy wyświetlają odpowiednie komunikaty zmuszające użytkownika do zainstalowania rzekomego certyfikatu autentyczności na swoim telefonie. Jest to niezbędne do ukończenia procesu logowania.
- Ofiara w specjalnym oknie podaje numer telefonu dzięki czemu przestępcy są w stanie przesłać wiadomość tekstową zawierającą link do fałszywego certyfikatu. Pod odnośnikiem znajduję się plik zawierający złośliwy kod FakeSite.A.
- Gdy proces pobierania certyfikatu zostanie ukończony, a bankowy kod weryfikacyjny zostanie wprowadzony aplikacja wysyła SMS z informacją do posiadacza licencji „malware kit" dzięki, której przeprowadzono cały atak.
- Od tego momentu trojan przechwytuje wszystkie SMS-y, które zostaną określone jako potwierdzenia logowania do systemów bankowych i przesyła je do przestępcy. Cel został osiągnięty napastnik ma dostęp do konta bankowego ofiary i w prosty sposób ominął dwustopniowe uwierzytelnianie za pomocą telefonu komórkowego.

Złośliwe oprogramowanie FakeSite.A dzięki swojej modułowej budowie i odpowiednio zaprogramowanym funkcjom jest dostępne nie tylko dla doświadczonych cyberprzestępców, ale także dla nowicjuszy.



Rysunek 11 Perkele Lite Kit. Oferta zestawu obejmującego wyłącznie jeden bank - 1000$ oraz zestaw uniwersalny - 15000$.

Analogicznie do sytuacji z zagrożeniami dla systemu Windows, liczba złośliwego oprogramowania na Androida będzie rosła w zastraszającym tempie. Nawet jeśli FakeSite.A nie jest najbardziej zaawansowana odmianą złośliwego oprogramowania, to właśnie ten trojan odpowiada za znacząca liczbę szkód oraz jest bardzo popularny wśród osób stawiających swoje pierwsze kroki w świecie cyberprzestępczości.

[8] (fin) diabeł

Prognozy

Popularność urządzeń z systemem Android – wśród użytkowników i twórców złośliwego oprogramowania – nie zmniejszy się pod koniec 2013 roku. Patrząc wstecz na złośliwe aplikacje dla Androida, można śmiało stwierdzić, że były to proste programy których twórcy nastawiali się na krótkoterminowe i zyskowne działania. Dziś jesteśmy świadkami zmiany tej tendencji. Tak jak we wczesnych latach wirusów przeznaczonych na komputery osobiste, złośliwe funkcje aplikacji są już dobrze ukryte w ich kodzie źródłowym. Ma to na celu utrudnienie prac związanych z ich wykryciem i opisaniem. Jak pokazuje to sytuacja z malware'm Obad.A, analiza złośliwego pliku wymaga o wiele większego wysiłku od ekspertów bezpieczeństwa.

Funkcje instalowanych złośliwych aplikacji mają być niewidoczne nie tylko dla osób, które zawodowo lub hobbystycznie z nimi walczą, ale także dla zwykłych użytkowników. FakeSite.A jest przykładem dla wielu cyberprzestępców, jak niewielką wiedzę programistyczną trzeba posiadać w dzisiejszych czasach by stać się autorem złośliwego oprogramowania. Modułowe zestawy pozwalają coraz większej liczbie ludzi z przestępczymi ambicjami stać się aktywnymi twórcami na Androidowej scenie wirusów. Muszą jedynie zapłacić niewielką sumę prawowitym twórcą zestawów do tworzenia złośliwych aplikacji.

Główną siłą sprawczą działań wszelkich cyberkriminalistów zawsze jest i będzie szybki zarobek. Czy to bezpośrednio dzięki wysyłaniu kosztownych wiadomości premium z zainfekowanych telefonów czy pośrednio dzięki sprzedaży wykradzionych wrażliwych danych z urządzeń mobilnych. Zestawy narzędzi do tworzenia złośliwych aplikacji pozwalają na tworzenie niezliczonej ilości malware'u. nawet jeśli programy te nie są wysoce zaawansowane, ich funkcje mogą z łatwością dokonać kradzieży naszych danych czy też pieniędzy.

Eksperci G Data SecurityLabs spodziewają się potrojenia liczby nowych zagrożeń w najbliższych trzech miesiącach!

Prócz chęci szybkiego wzbogacenia się, wymienianej jako głównego powodu działań wszelkich hakerów w przeszłości, obecnie obserwujemy wzrost wykrytych backdoorów, które zapewniają długoterminowe działania i kontrole nad zainfekowanymi urządzeniami. Backdory są wykorzystywane do tworzenia mobilnych botnetów, które są służą następnie do przeprowadzania systematycznych i zorganizowanych działań, jak kradzieże danych czy seryjne wysyłki wiadomości SMS.

Wzrasta świadomość użytkowników z faktu, iż ich telefon jest obecnie w pełni funkcjonalnym komputerem. To zmienia perspektywę postrzegania takiego urządzenia. Jednakże, nie przekłada się to na świadomość możliwych zagrożeń. Według raportu firmy Canalys w 2010 roku jedynie 4% wszystkich urządzeń mobilnych było chronionych oprogramowaniem antywirusowym, ta liczba ma zwiększyć się do 20% w 2015 roku. To zdecydowanie za mało! Liczba urządzeń chronionych dobrym oprogramowaniem antywirusowym dla systemu Android musi się zwiększyć natychmiastowo, by móc dorównać wzrostowi liczby samych urządzeń. Kiedy mówimy o ochronie antywirusowej, tablety i smartfony powinny być postrzegane oraz traktowane tak samo jak komputery PC. Urządzenia w naszych kieszeniach przenoszą takie same ilości informacji o takim samym stopniu poufności jak komputery, a ataki na nie są tak samo groźne jak na urządzenia z systemem Windows i póki co o wiele łatwiejsze do przeprowadzenia.

Wyścig z przestępcami o użytkowników wciąż młodej platformy Android rozpoczęty! Świadomość korzystania z urządzeń mobilnych, zawsze aktualne oprogramowanie chroniące naszego smartofna zdecydowanie poprawi nasze szanse by nie zostać kolejna ofiarą mobilnych cyberprzestępców.