RAPORT NA TEMAT ZAGROŻEŃ MOBILNYCH

4 KWARTAŁ 2012 R.

F-Secure

F-Secure Labs

W laboratoriach F-Secure w Helsinkach w Finlandii i w Kuala Lumpur w Malezji eksperci od bezpieczeństwa nieustannie pracują, aby zapewnić Internautom ochronę przed zagrożeniami czyhającymi w sieci.

W każdym momencie personel laboratoriów F-Secure monitoruje światową sytuację w zakresie bezpieczeństwa, aby szybko i efektywnie radzić sobie z nagłymi epidemiami wirusów oraz złośliwego oprogramowania.

Ochrona przez całą dobę

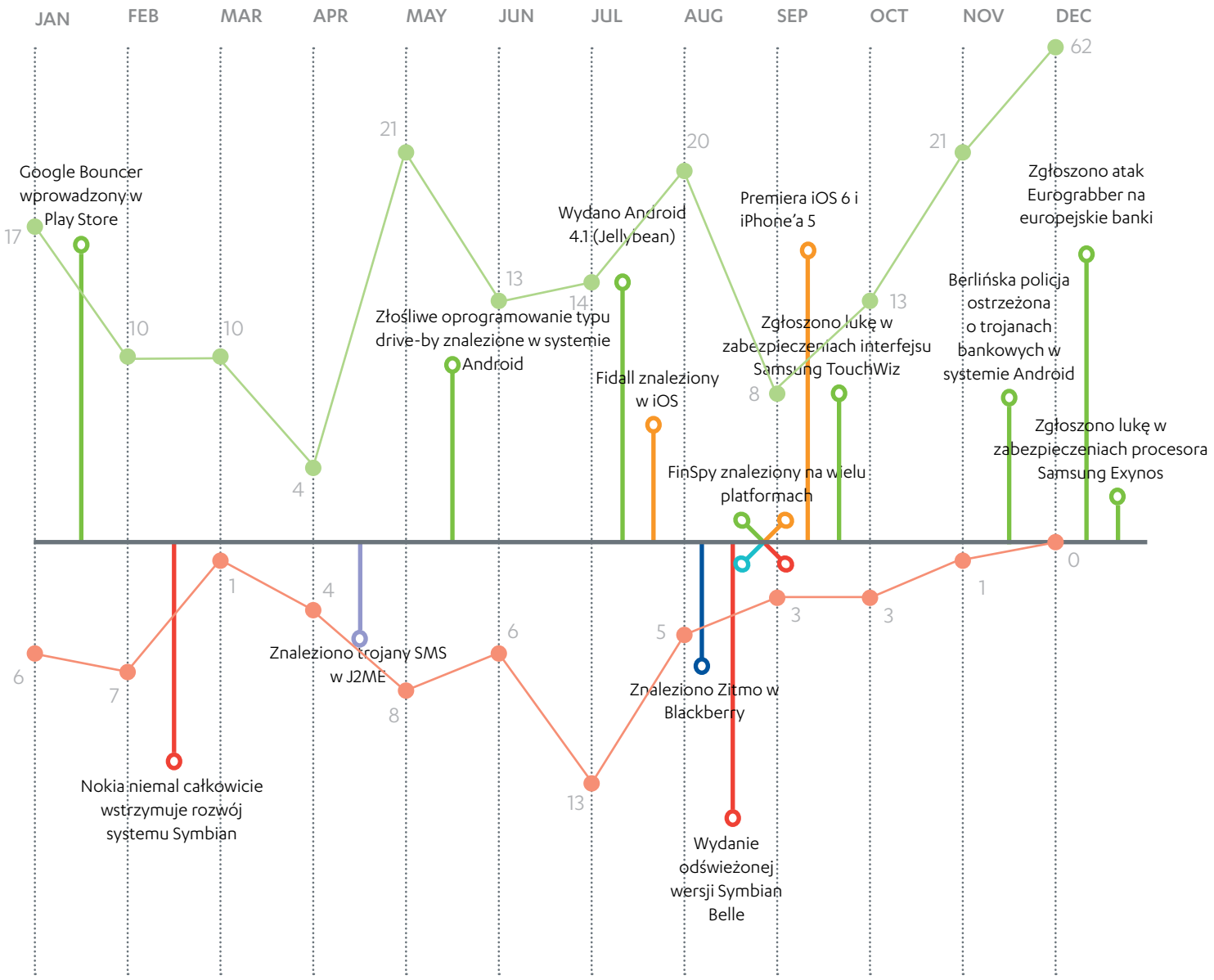
Pracę laboratoriów F-Secure wspierają automatyczne systemy, które śledzą zagrożenia w czasie rzeczywistym, gromadząc i analizując setki tysięcy próbek danych każdego dnia. Przestępcy, którzy wykorzystują wirusy i złośliwe oprogramowanie do celów zarobkowych, nieustannie pracują nad nowymi sposobami ataku. Sytuacja wymaga ciągłej czujności, aby użytkownicy internetu zawsze byli skutecznie chronieni.

PODSUMOWANIE

TEN RAPORT OMAWIA KRAJOBRAZ ZAGROŻEŃ MOBILNYCH W CZWARTYM KWARTALE 2012 ROKU I ZAWIERA DANE STATYSTYCZNE ORAZ SZCZEGÓŁOWE INFORMACJE NA TEMAT ZAGROŻEŃ, KTÓRE W TYM OKRESIE ZOSTAŁY ZAOBSERWOWANE I PRZEANALIZOWANE PRZEZ LABORATORIA F-SECURE. DANE PREZENTOWANE W RAPORCIE ZOSTAŁY OSTATNIO ZAKTUALIZOWANE 31 GRUDNIA 2012 R.

SPIS TREŚCI

KALENDARZ ZAGROŻEŃ MOBILNYCH W 2012 R.



STATYSTYKI ZAGROŻEŃ

- Nowe rodziny/warianty w systemie Android
- Nowe rodziny/warianty w systemie Symbian

GODNE UWAGI WYDARZENIA

- Android
- Blackberry
- iOS
- J2ME
- Windows Mobile
- Symbian

STRESZCZENIE

Złośliwe oprogramowanie dla Androida umacnia swoja pozycję na arenie zagrożeń mobilnych. W każdym kwartale autorzy złośliwego oprogramowania wprowadzają jego nowe rodziny i warianty, aby zwabić więcej ofiar. Tylko w czwartym kwartale odkryto 96 nowych rodzin i wariantów zagrożeń związanych z Androidem, co oznacza niemal podwojenie liczby zarejestrowanej w poprzednim kwartale. Prym wiedzie tu PremiumSMS — rodzina złośliwego oprogramowania, której twórcy czerpią zyski z przesyłania wiadomości SMS, rozpowszechniana w 21 nowych wariantach.

Wiele innych złośliwych programów dla Androida działa w sposób przypominający PremiumSMS. Jest to popularna metoda bezpośredniego zarabiania pieniędzy. Złośliwe oprogramowanie wysyła po cichu wiadomości SMS na numery premium albo bez wiedzy użytkownika rejestruje go w usłudze SMS. Wszystkie komunikaty lub powiadomienia z tych numerów i (lub) usług są przechwytywane i usuwane - użytkownicy pozostają więc niczego nieświadomi, dopóki nie otrzymają rachunku.

Niektórzy autorzy lub dystrybutorzy złośliwego oprogramowania zarabiają również na trojanach bankowych. W czwartym kwartale zadebiutował Citmo.A (mobilna wersja trojana Carberp). Działa on podobnie jak Zitmo (Zeus do urządzeń mobilnych) i Spitmo (SpyEye do urządzeń mobilnych) — wykrada kody mTAN (mobile Transaction Authorization Number), które bank wysyła do swoich klientów w wiadomościach SMS w celu autoryzowania transakcji internetowych. Za pomocą tego kodu może przelać pieniądze z konta ofiary, natomiast banki realizują tego typu transakcję, ponieważ wyglądają one na zatwierdzone przez prawowitego właściciela konta.

Tak działa Eurograbber, wariant trojana Zeus; witryna Bank Info Security podaje, że Eurograbber zdołał ukraść 47 mln dol. z ponad 30 000 indywidualnych i firmowych kont w Europie1. Najpierw infekował komputer osobisty ofiary, a następnie skłaniał ją do zainstalowania swojej wersji w mobilnym tabletach i smartfonach. Działając zarówno w komputerze, jak i urządzeniach przenośnych, Eurograbber może podszywać się pod ofiarę i przeprowadzać transakcje bez budzenia podejrzeń użytkownika ani instytucji bankowej. Trojan infekuje nie tylko urządzenia działające pod kontrolą Androida, ale również systemów operacyjnych Symbian i BlackBerry.

Coraz większą ilość złośliwego oprogramowania dla Androida można przypisać rosnącemu udziałowi tego systemu operacyjnego w rynku mobilnym. W 2012 r. udział rynkowy Androida wzrósł do 68,8 proc. w porównaniu z 49,2 proc. w 2011 r.[2] Jeśli chodzi o zagrożenia, w 2012 r. jego udział wzrósł do 79 proc. w porównaniu z 66,7 proc. w 2011 r. Natomiast sytuacja Symbiana jest odwrotna. W 2012 r. jego udział w rynku wynosił 3,3 proc., co stanowi znaczny spadek w porównaniu z 16,5 proc. rok wcześniej[3]. Jego udział w globalnym rynku zagrożeń zmniejszył sięz 29,7 proc. w 2011 r. do 19 proc. w 2012 r. Decyzja Nokii o wstrzymaniu prac nad Symbianem w lutym 2012 r. mogła przyczynić się do tych dużych spadków. W miarę, jak zmniejsza się udział rynkowy Symbiana, twórcy złośliwego oprogramowania są coraz mniej zainteresowani tą platformą. Odzwierciedlają to statystyki czwartego kwartału, w którym wykryto zaledwie cztery nowe rodziny i warianty złośliwego oprogramowania.

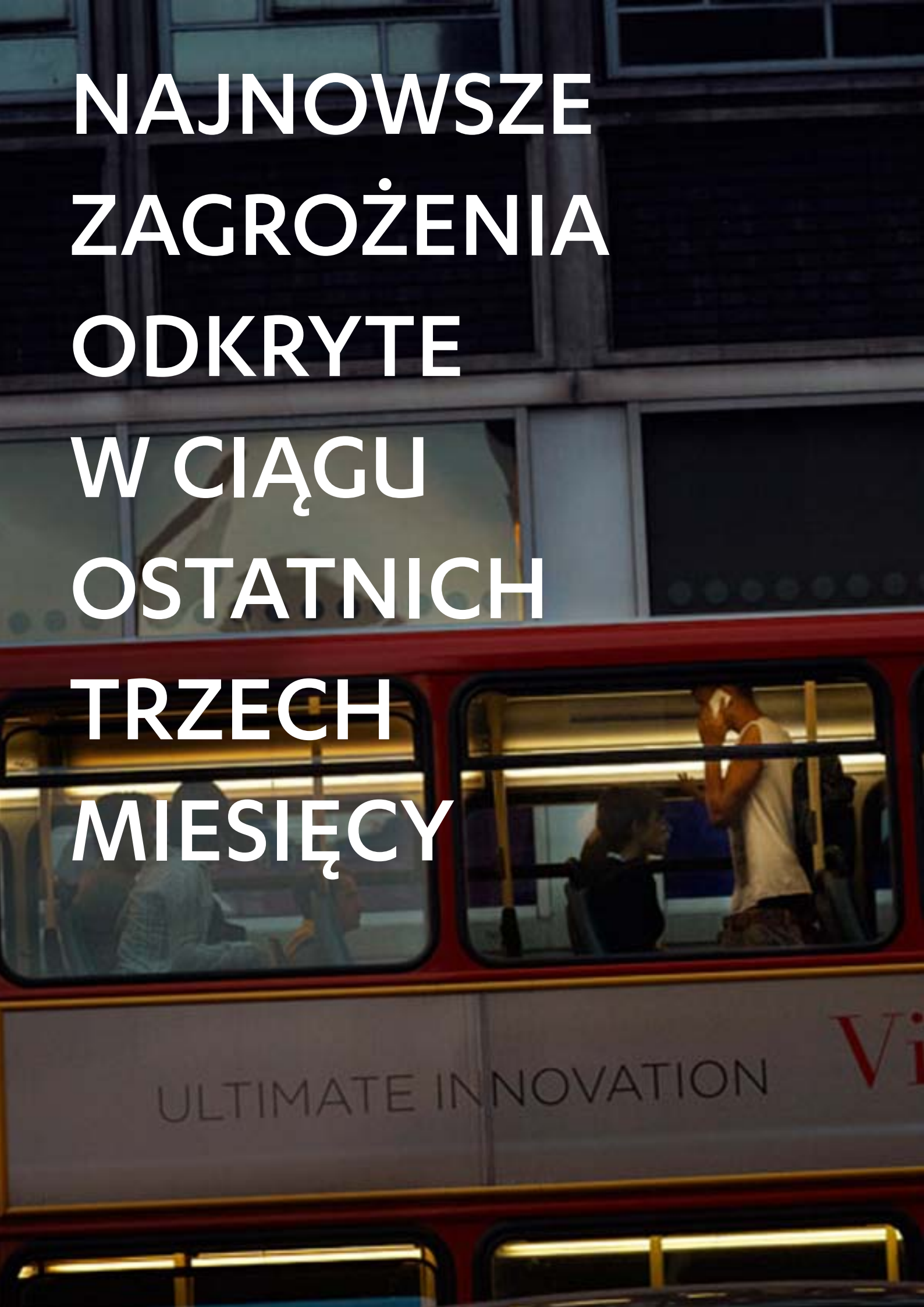
Co do innych platform, tzn. Blackberry, iOS i Windows Mobile, od czasu do czasu były one celem ataków. W większości przypadków były to jednak zagrożenia wieloplatformowe, podobne do FinSpy[4].

"Bank Info Security oszacował, że Eurograbber zdołał okraść ponad 30 000 indywidualnych i firmowych kont bankowych w Europie"

[1] Bank Info Security; Tracy Kitten; Eurograbber: A Smart Trojan Attack; opublikowano 17 grudnia 2012 r.; http://www.bankinfosecurity.com/eurograbber-smart-trojan-attack-a-5359/op-1

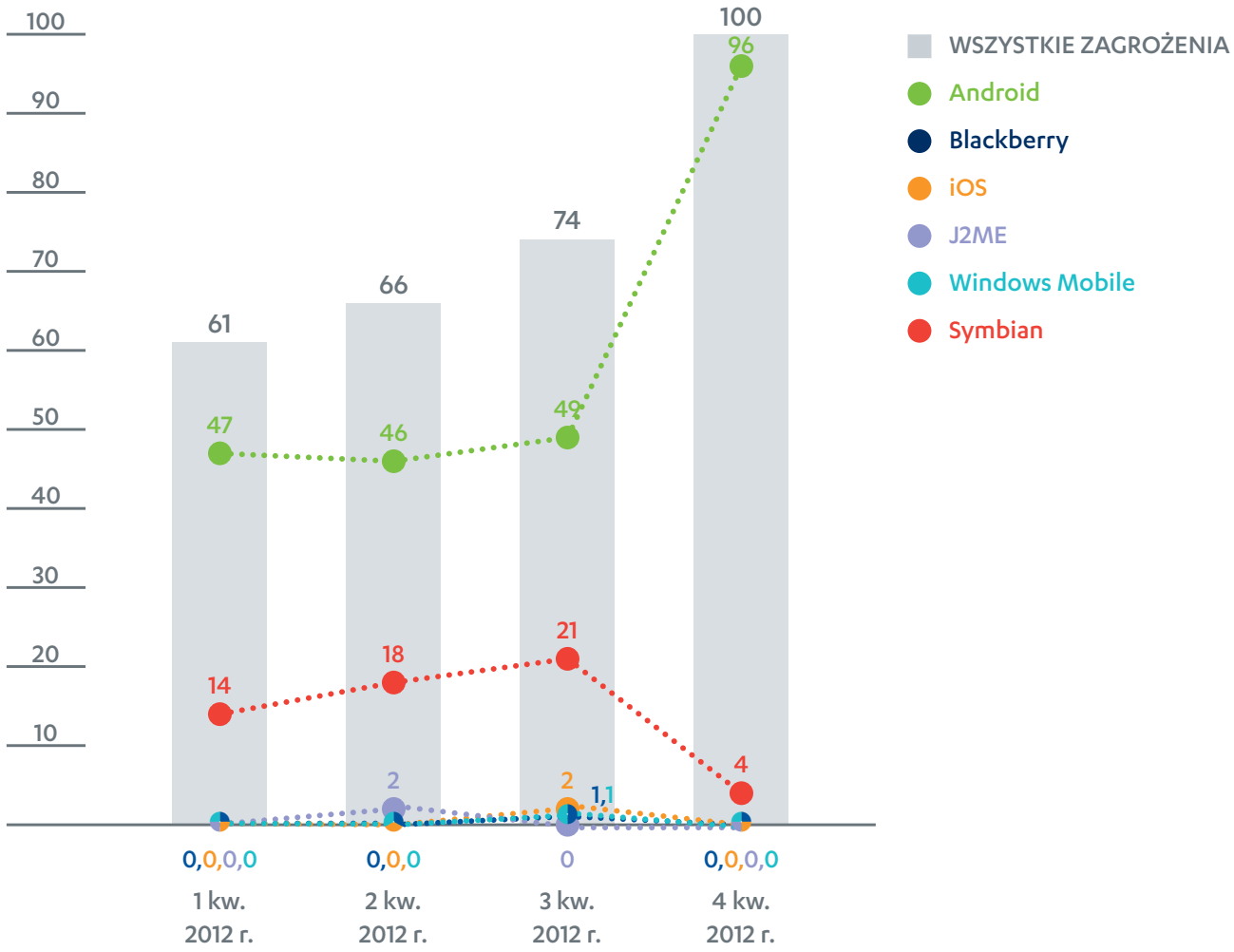
[2,3] Engadget; Jon Fingas; IDC: Android surged to 69 percent smartphone share in 2012, dipped in Q4; opublikowano 14 lutego 2013 r.; http://www.engadget.com/2013/02/14/idc-android-surged-to-69-percent-smartphone-share-in-2012/

[4] F-Secure Weblog; Mikko Hyppönen; Egypt; FinFisher Intrusion Tools and Ethics; opublikowano 8 marca 2011 r.; https://www.f-secure.com/weblog/archives/00002114.html



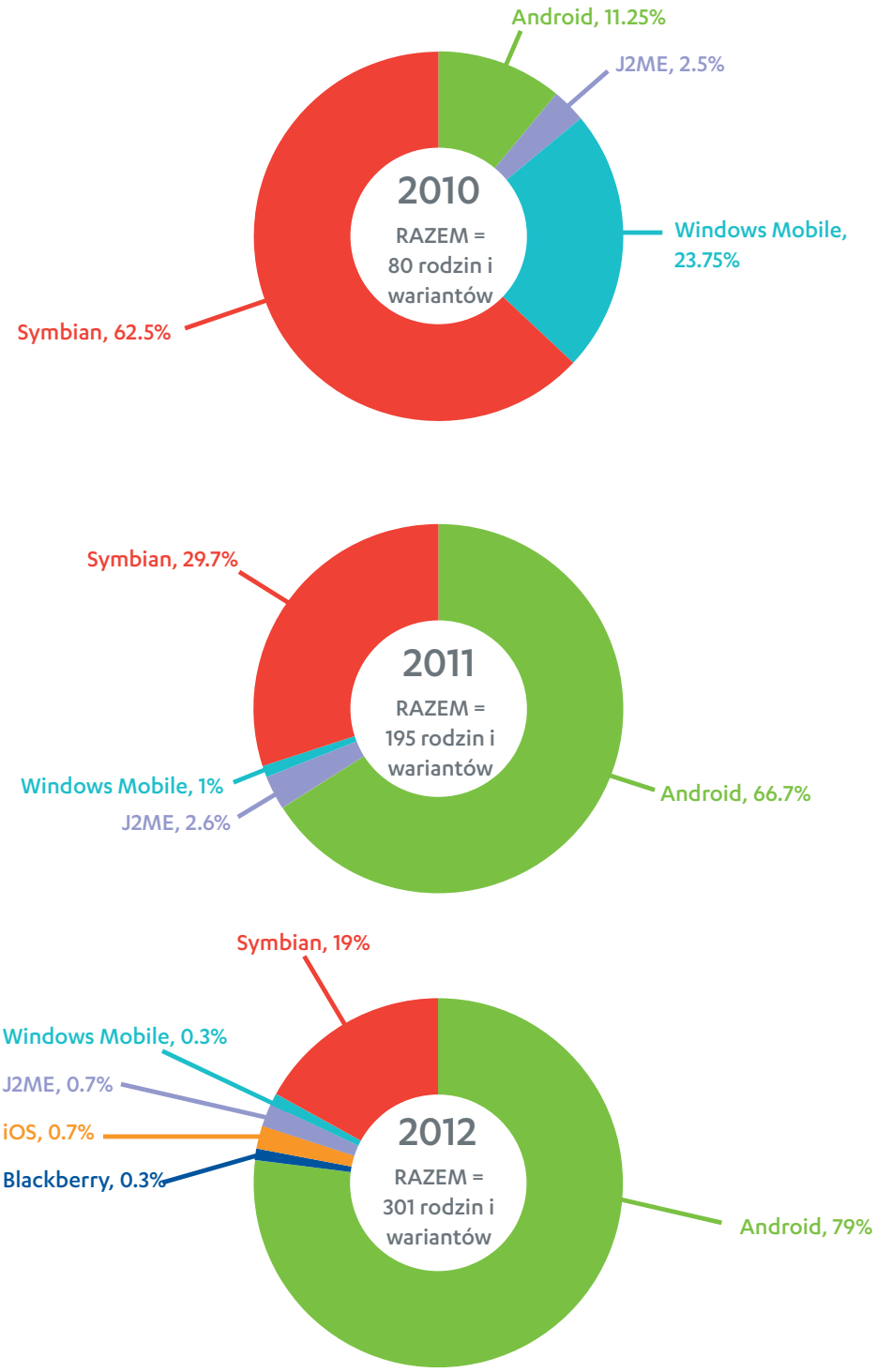
NAJNOWSZE ZAGROŻENIA ODKRYTE W CIĄGU OSTATNICH TRZECH MIESIĘCY

RYSUNEK 1. NOWE RODZINY I WARIANTY ZAGROŻEŃ MOBILNYCH WEDŁUG KWARTAŁU, 1-4 KWARTAŁ 2012 R.



UWAGA: statystyki przedstawione na **rysunku 1** reprezentują rodziny i warianty zagrożeń, a nie unikatowe pliki. Jeśli na przykład dwie próbki wykryto jako Trojan:Android/GinMaster.A, w statystykach liczy się je jako jedną.

RYSUNEK 2. RODZINY I WARIANTY ZAGROŻEŃ WEDŁUG PLATFORMY, 2010-2012 R.



UWAGA: statystyki przedstawione na **rysunku 2** reprezentują rodziny i warianty zagrożeń, a nie unikatowe pliki. Jeśli na przykład dwie próbki wykryto jako Trojan:Android/GinMaster.A, w statystykach liczy się je jako jedną.

Potencjalnie niepożądane oprogramowanie

PONIŻSZE PROGRAMY UWAŻAMY ZA POTENCJALNIE NIEPOŻĄDANE. OZNACZA TO PROGRAMY, KTÓRE UŻYTKOWNIK MOŻE UZNAĆ ZA NIECHCIANE LUB NATRĘTNE, JEŚLI SĄ WYKORZYSTYWANE W NIEODPOWIEDNI SPOSÓB.

Hack-Tool:Android/Aniti.A

Znane też jako Android Network Toolkit, Aniti.A , pozwala użytkownikowi przeprowadzić pewne testy z wykorzystaniem zautomatyzowanego interfejsu. Za pomocą tego narzędzia użytkownik może zidentyfikować słaby punkt w sieci poprzez:

- skanowanie sieci,
- generowanie raportu sieciowego,
- sprawdzanie siły haseł,
- wyszukiwanie w sieci komputerów podatnych na atak,
- atakowanie podatnego komputera,
- monitorowanie niezabezpieczonych połączeń,
- wyszukiwanie napastników korzystających z metody „człowiek w środku”,
- blokowanie usług (DoS).

Podobnie jak większość programów do testów penetracyjnych, narzędzie to opracowano w dobrej wierze. Może jednak zostać wykorzystane przez przestepców.

Hack-Tool:Android/DroidSheep.A

DroidSheep.A to narzędzie, które umożliwia przejęcie sesji użytkownika zalogowanego we współdzielonej sieci bezprzewodowej. Ma ono demonstrować niewystarczające zabezpieczenia połączenia sieciowego, ale może zostać użyte przez nieodpowiedzialne osoby.

Hack-Tool:Android/EksyPox.A

EksyPox.A to program, który pozwala prowizorycznie załatać lukę w zabezpieczeniach układu Exynos 4. Luka ta umożliwia dowolnej aplikacji uzyskanie przywilejów superużytkownika w urządzeniach z układem Exynos 4. EksyPox.A eliminuje tę lukę, choć nie bez jej uprzedniego wykorzystania.

Exynos 4: „system w układzie” (SoC) używany w niektórych urządzeniach Samsunga, takich jak Galaxy S III, Galaxy Note II, Galaxy Camera itd.

UWAGA: Dodatkowe informacje można znaleźć w artykule pod adresem (http://www.xda-developers.com/android/dangerous-exynos-4-security-hole-demoed-and-plugged-by-chainfire/).

Monitoring-Tool:Android/GpsSpyTracker.A I wariant B

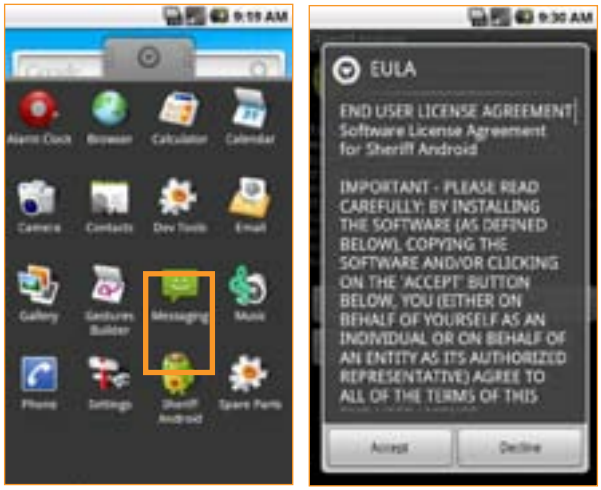
GpsSpyTracker.A to narzędzie do śledzenia lokalizacji, które pełni swoją funkcję z wykorzystaniem określonego klucza i adresu e-mail przypisanego do konkretnego urządzenia. Po aktywacji ustala lokalizację urządzenia co 15 minut. Wyświetla bieżącą lokalizację na mapie i zapisuje historię w lokalnym pliku.

Monitoring-Tool:Android/SheriDroid.A

SheriDroid.A jest reklamowany jako aplikacja, która pozwala użytkownikowi wykonywać poniższe czynności z wykorzystaniem funkcji monitoringu i ustawiania alarmów:

- nagrać wiadomość ostrzegawczą poprzedzającą alarm,
- zdalnie uruchomić śledzenie lokalizacji za pomocą hasła,
- w przypadku zgubienia lub kradzieży urządzenia włączyć wysyłanie ukrytych wiadomości SMS związanych z alarmami lub śledzeniem lokalizacji,
- ustawić wzór odblokowywania systemu.

Jednak aplikacja bez zgody i wiedzy użytkownika śledzi strony internetowe przeglądane przez użytkownika oraz inne czynności wykonywane za pomocą urządzenia.



Ikona SheriDroid.A (po lewej stronie) i umowa licencyjna (po prawej stronie)

Monitoring-Tool:Android/SmsSpy.A

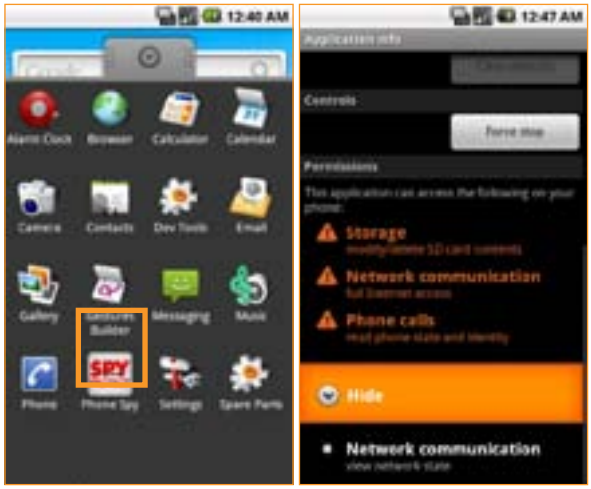
Zob. Riskware:Android/SmsSpy.A na stronie 16.

Monitoring-Tool:Android/SmsUploader.A

SMSUploader.A wysyła do zdalnego serwera wszystkie wiadomości SMS znalezione w urządzeniu. Podczas instalacji SmsUploader.A umieszcza w menu aplikacji ikonę zatytułowaną „SMSUpload". Po uruchomieniu prosi użytkownika o zrestartowanie urządzenia i informuje, że będzie działać w tle.

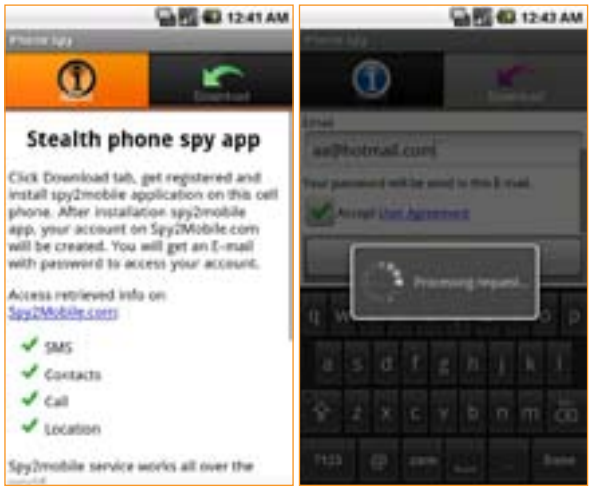
Monitoring-Tool:Android/SpyMob.A

SpyMob.A to komercyjne narzędzie monitorujące, które gromadzi informacje związane z wiadomościami SMS, listą kontaktów, dziennikiem połączeń oraz lokalizacją GPS urządzenia. Informacje te są następnie przesyłane do serwerów Spy2Mobile i można je przeglądać po zalogowaniu się na koncie użytkownika w witrynie Spy2Mobile.com.



Ikona SpyMob.A (po lewej stronie) i uprawnienia, o które prosi aplikacja (po prawej stronie)

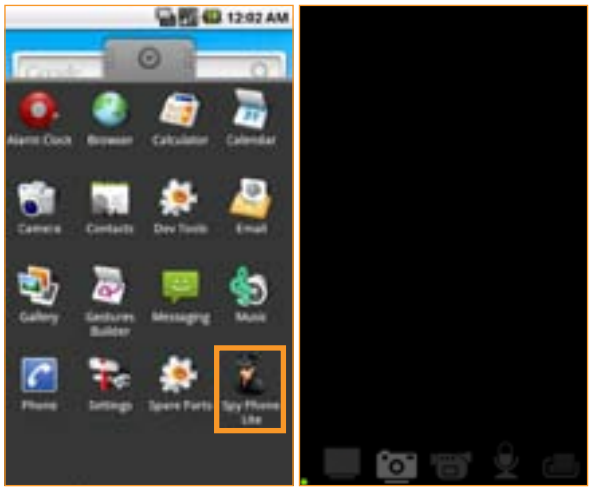
Aby skorzystać z aplikacji, użytkownik musi najpierw zainstalować SpyMob.A w docelowym urządzeniu i zarejestrować konto w witrynie SpyMobile.com.



Instalacja i rejestracja

Monitoring-Tool:Android/SpyPhone.A

SpyPhone.A jest reklamowany jako aplikacja, która pozwala użytkownikowi po kryjomu robić zdjęcia albo rejestrować wideo/dźwięk. Jednakże śledzi ona również aktywność w urządzeniu i gromadzi takie informacje, jak wpisy dziennika zdarzeń, lokalizacje GPS, odwiedzone adresy URL oraz identyfikator użytkownika.



Ikona SpyPhone.A (po lewej stronie) i interfejs użytkownika (po prawej stronie)

Monitoring-Tool:Android/TheftAware.A

TheftAware.A to komercyjne narzędzie monitorujące, które pomaga użytkownikowi zlokalizować skradzione lub zgubione urządzenie. Pozwala określić lokalizację GPS urządzenia, zablokować je i usunąć dane poprzez wysyłanie poleceń w wiadomościach SMS.

Monitoring-Tool:Android/TrackPlus.A

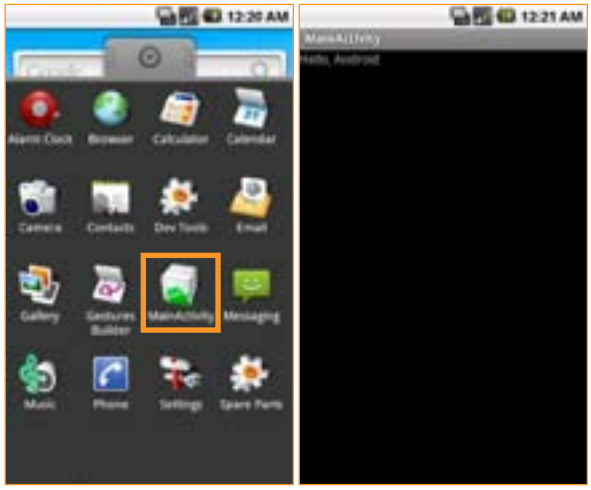
TrackPlus.A to narzędzie śledzące, którego można użyć do zlokalizowania urządzenia. Wysyła numer International Mobile Equipment Identity (IMEI) do zdalnego serwera oraz posiada portal internetowy, który pozwala śledzić lokalizację urządzenia.

Podczas instalacji TrackPlus.A nie umieszcza ikony w menu aplikacji, ale pojawia się w urządzeniu jako przezroczysty widget.

Riskware:Android/AutoRegSMS.A

Po uruchomieniu AutoRegSMS.A wyświetla wiadomość „Hello, Android”, ale w tle po kryjomu uaktywnia grę z wykorzystaniem informacji o użytkowniku. Wysyła też wiadomości SMS do kontaktów użytkownika, aby uzyskać aktywacyjny numer seryjny.

AutoRegSMS.A jest reprezentowany przez ikonę zatytułowaną „Main Activity”, która znajduje się w menu aplikacji.



Ikona AutoRegSMS.A (po lewej stronie) i wiadomość wyświetlana przez aplikację (po prawej stronie)

Riskware:Android/SmsReg A i wariant B

SmsReg.A jest sprzedawany pod nazwą „Battery Improve" jako aplikacja, która rzekomo maksymalizuje czas pracy urządzenia na zasilaniu bateryjnym.

SmsReg.A jako „Battery Improve"

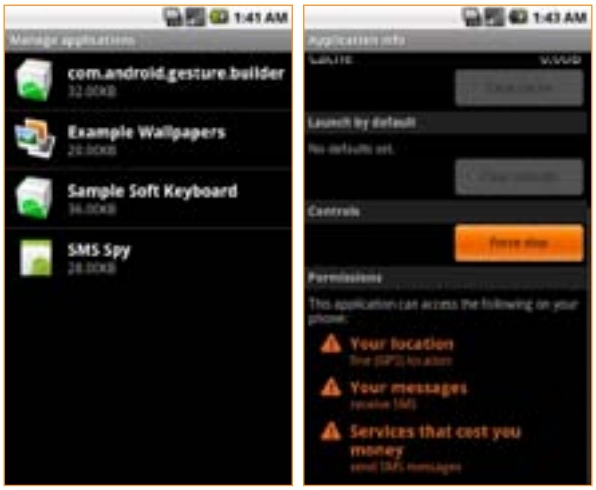
Bez wiedzy użytkownika aplikacja gromadzi następujące informacje:

- klucz API,
- identyfikator aplikacji,
- operator,
- producent urządzenia,
- model urządzenia,
- lokalizacja GPS,
- numer IMEI,
- operator sieci,
- nazwa pakietu,
- wersja SDK.

Riskware:Android/SmsSpy.A

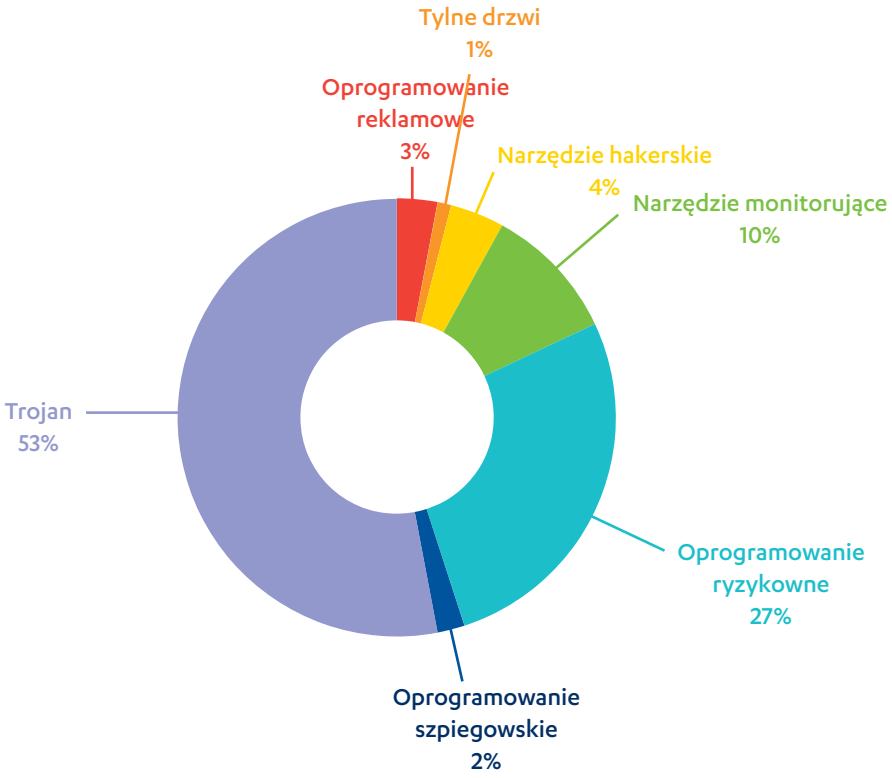
SmsSpy.A to ukryta aplikacja, która nie umieszcza widocznej ikony w menu aplikacji; jej obecność można stwierdzić tylko za pomocą opcji „Zarządzaj aplikacjami” w menu „Ustawienia”.

Aplikacja wykonuje wszystkie operacje w tle. Działania te obejmują śledzenie lokalizacji GPS urządzenia, odczytywanie odebranych wiadomości SMS oraz wysyłanie wiadomości SMS.

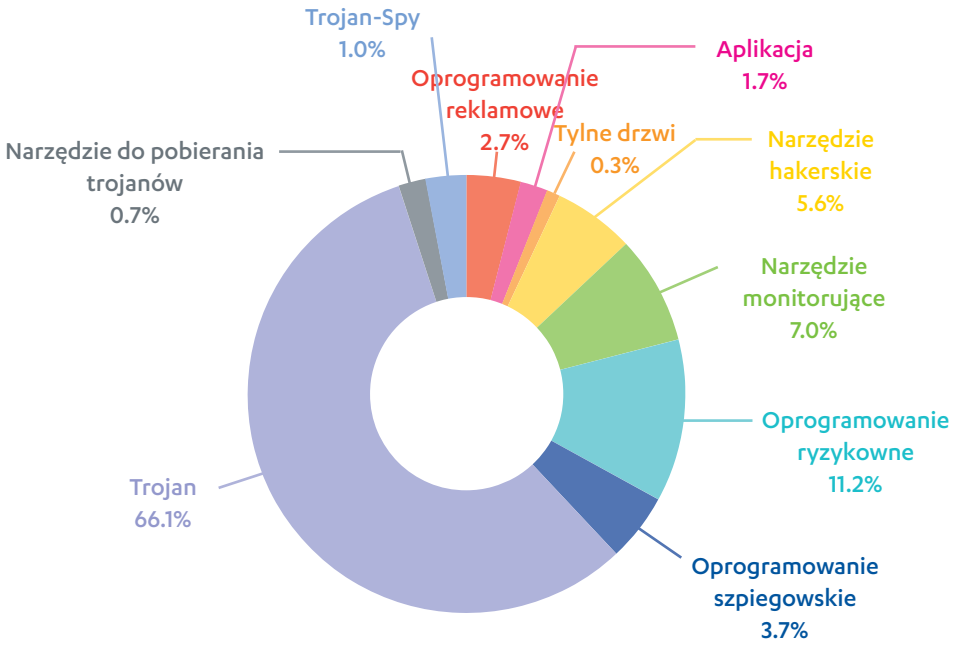


SmsSpy.A w menu „Zarządzaj aplikacjami” (po lewej stronie) i uprawnienia, o które prosi aplikacja (po prawej stronie)

RYSUNEK 3. ZAGROŻENIA MOBILNE WG TYPU, 4 KWARTAŁ 2012 R.



RYSUNEK 4. ZAGROŻENIA MOBILNE WG TYPU, 2012 R.



UWAGA: statystyki przedstawione na **rysunkach 3 i 4** reprezentują rodziny i warianty zagrożeń, a nie unikatowe pliki. Jeśli na przykład dwie próbki wykryto jako Trojan:Android/GinMaster.A, w statystykach liczy się je jako jedną.

Złośliwe oprogramowanie

PROGRAMY SKLASYFIKOWANE JAKO ZŁOŚLIWE ZWYKLE STANOWIĄ ZNACZNE ZAGROŻENIE DLA SYSTEMU I (LUB) INFORMACJI UŻYTKOWNIKA.

ZŁOŚLIWE OPERACJE WYKONYWANE PRZEZ TE PROGRAMY TO M.IN. INSTALOWANIE UKRYTYCH OBIEKTÓW I UKRYWANIE OBIEKTÓW PRZED UŻYTKOWNIKIEM, TWORZENIE NOWYCH ZŁOŚLIWYCH OBIEKTÓW, USZKADZANIE LUB MODYFIKOWANIE DANYCH BEZ AUTORYZACJI ORAZ KRADZIEŻ DANYCH ALBO POŚWIADCZEŃ DOSTĘPU.

Backdoor:Android/FakeLook.A

FakeLook.A nie umieszcza ikony w menu aplikacji, aby ukryć swoją obecność przed właścicielem urządzenia. Jest jednak wymieniony jako „Updates" na liście „Zarządzaj aplikacjami" w menu „Ustawienia".

FakeLook.A łączy się z serwerem dowodzenia (C&C), aby otrzymać dalsze instrukcje. Gromadzi takie informacje, jak identyfikator urządzenia i wiadomości SMS, pobiera listę plików z karty SD i kompresuje pliki przed wysłaniem ich do serwera FTP z wykorzystaniem nazwy użytkownika „ftpuser" i hasła „upload".

Trojan:Android/Citmo.A

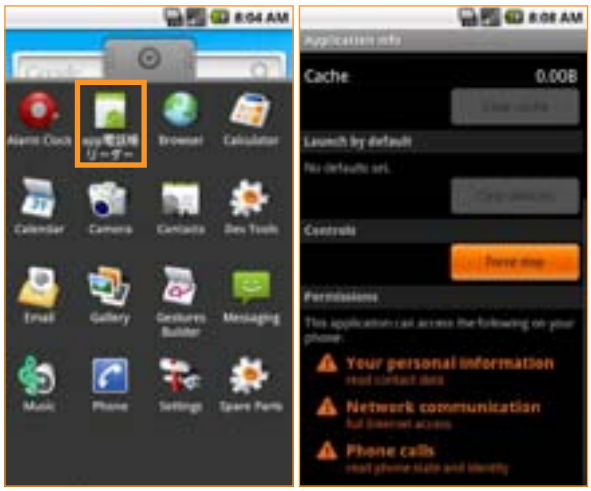
Citmo.A to mobilna wersja trojana Carberp, który infekuje komputery osobiste w celu kradzieży poświadczeń bankowych. Citmo.A działa podobnie jak Zitmo (Zeus do urządzeń mobilnych) i Spitmo (SpyEye do urządzeń mobilnych) — monitoruje przychodzące wiadomości SMS i wykrada kody mTAN, które banki wysyłają do klientów w celu zweryfikowania transakcji internetowych.

mTAN: Mobile Transaction Authentication Number. Jest to kod używany do uwierzytelniania internetowych transakcji bankowych.

UWAGA: Dodatkowe informacje o trojanach bankowych można znaleźć w artykule „Berlin Police: Beware Android Banking Trojans" pod adresem (http://www.f-secure.com/weblog/archives/00002457.html).

Trojan:Android/EcoBatry.A

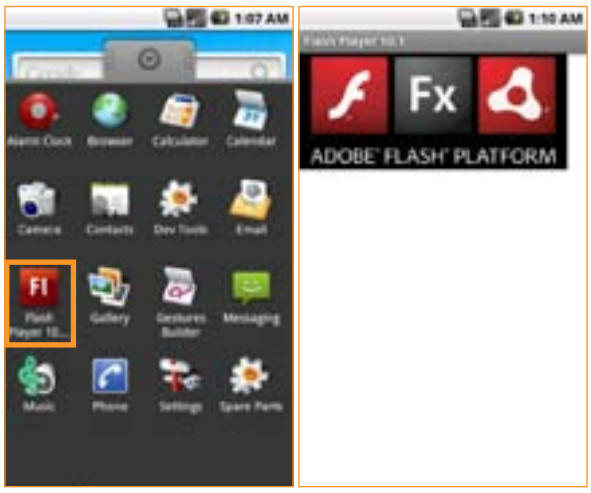
Podczas instalacji EcoBatry.A prosi o uprawnienia, które umożliwiają mu dostęp do internetu, danych kontaktowych oraz informacji o urządzeniu. Następnie program nawiązuje połączenie wychodzące ze zdalnym serwerem, po czym gromadzi dane kontaktowe i wysyła je do serwera.



Ikona EcoBatry.A (po lewej stronie) i uprawnienia, o które prosi aplikacja (po prawej stronie)

Trojan:Android/FakeFlash.A

FakeFlash.A podszywa się pod legalną aplikację Flash. Po uruchomieniu wyświetla komunikat o pomyślnym zainstalowaniu aplikacji Flash Player i przekierowuje użytkownika do innej witryny.



Ikona FakeFlash.A (po lewej stronie) i rzekomo zainstalowana aplikacja (po prawej stronie)

Trojan:Android/FakeGuard.A

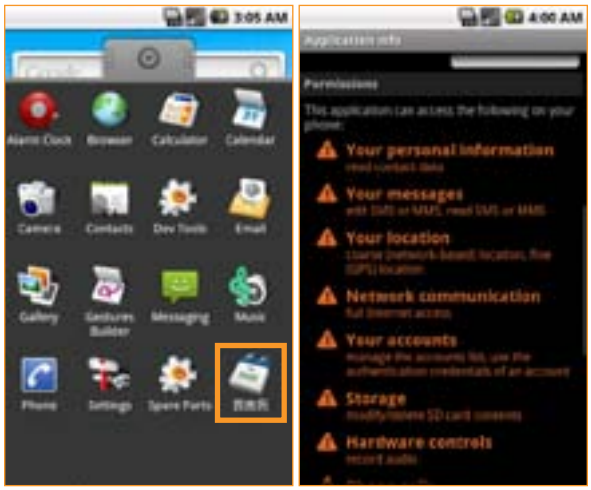
FakeGuard.A to złośliwy program, który rozpoznaje przychodzące wiadomości SMS/WAP Push. Wykrada informacje o użytkowniku i nawiązuje połączenie ze zdalnym serwerem. Odpowiedź serwera jest dekodowana za pomocą zestawu znaków MS949, natomiast wychodzące dane są kodowane za pomocą zestawu znaków EUC_KR.

WAP Push:specjalnie zakodowana wiadomość, która zawiera łącze do adresu WAP.

Trojan:Android/GeoFake.A i wariant B

GeoFake.A jest dystrybuowany jako aplikacja chińskiego kalendarza, ale podczas instalacji prosi o niepotrzebne uprawnienia, takie jak:

- zarządzanie listą kont,
- dostęp do danych uwierzytelniania konta,
- odczytywanie i edycja wiadomości SMS lub MMS,
- odczytywanie systemowych plików dziennika,
- dostęp do informacji o lokalizacji.



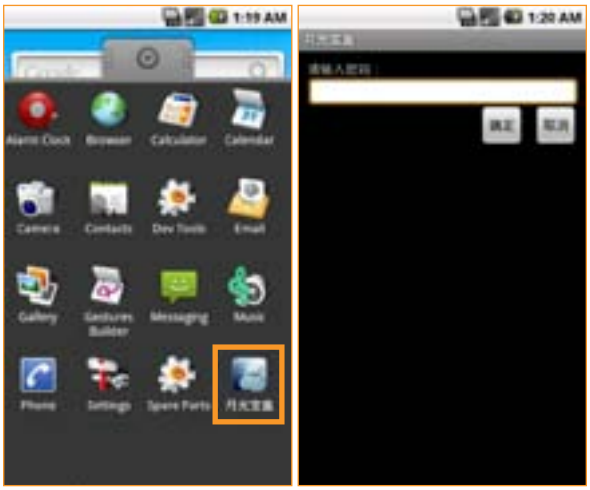
Ikona GeoFake.A (po lewej stronie) i uprawnienia, o które prosi aplikacja (po prawej stronie)

Po pomyślnej instalacji w urządzeniu program wysyła wiadomości SMS na numery premium. Używa GoogleMaps API, aby wybrać właściwą usługę premium w zależności od geograficznego położenia urządzenia.

GeoFake.A jest dystrybuowany jako aplikacja chińskiego kalendarza

Trojan:Android/Gmuse.A

Gmuse.A jest sprzedawany jako aplikacja, która pozwala użytkownikowi przechowywać pliki i dokumenty w tajnej, chronionej hasłem lokalizacji. Jednakże bez zgody użytkownika synchronizuje listę plików za pośrednictwem serwera SMTP z kontem nieznanego użytkownika, używając adresu e-mail „hbwhhouse.gmail.com” i hasła „whwxhjbu”.



Ikona Gmuse.A (po lewej stronie) i interfejs użytkownika (po prawej stronie)

Gmuse.A łączy się również ze zdalnym serwerem w celu pobrania zaktualizowanej wersji aplikacji, która nosi nazwę „lightbox.apk".

Trojan:Android/InfoStealer.A

InfoStealer.A, jak łatwo wywnioskować z jego nazwy jest złośliwym programem, który wykrada informacje kontaktowe i wysyła je do zdalnego serwera MySQL. Do kradzionych informacji należą:

- identyfikator urządzenia,
- adres e-mail,
- szerokość i długość geograficzna,
- numer telefonu,
- kod pocztowy,
- region,
- ulica,
- nazwa użytkownika.

Trojan:Android/MaleBook.A

MaleBook.A gromadzi informacje o urządzeniu, a następnie wysyła je do kilku zdalnych serwerów. Do gromadzonych informacji należą:

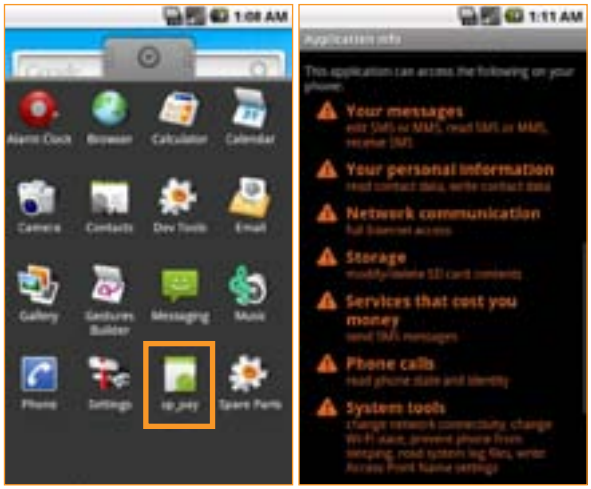
- identyfikator aplikacji,
- wersja aplikacji,
- kod kraju,
- nazwa urządzenia,
- typ urządzenia,
- szerokość i wysokość urządzenia,
- numer International Mobile Equipment Identity (IMEI),
- numer International Mobile Subscriber Identity (IMSI),
- język,
- wersja systemu operacyjnego,
- wersja SDK.

Ponadto program próbuje pobrać reklamy z serwerów do zainfekowanego urządzenia.

Ikona MaleBook.A (po lewej stronie) i interfejs użytkownika (po prawej stronie)

Trojan:Android/Placsms.A

Placsms.A pojawia się jako „sp_pay" w menu aplikacji i prosi o uprawnienia, które pozwalają mu na dostęp do internetu, wiadomości SMS, zawartości karty SD oraz systemu urządzenia podczas procesu instalacji.



Ikona Placsms.A (po lewej stronie) i uprawnienia, o które prosi aplikacja (po prawej stronie)

Aplikacja gromadzi takie informacje, jak numer International Mobile Equipment Identity (IMEI) i numer telefonu, a następnie wysyła je do zdalnego serwera.

UWAGA: Placsms.A działa w sposób zbliżony do trojanów z rodziny PremiumSMS (http://www.f-secure.com/v-descs/trojan_android_premiumsms.shtml).

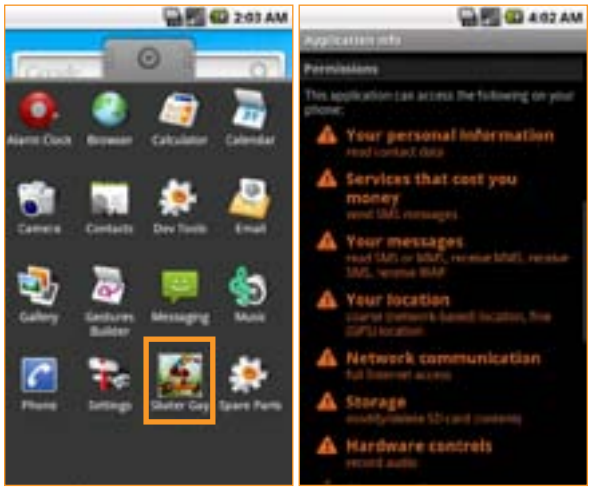
Trojan:Android/QdPlugin.A

QdPlugin.A jest przepakowywany jako inna legalna aplikacja przed dystrybucją do potencjalnych ofiar. Po instalacji i aktywacji w urządzeniu program wysyła do zdalnych serwerów takie informacje, jak numery IMEI i IMSI.

Program otrzymuje też polecenia od serwerów, które mogą nakazać mu wykonanie takich operacji, jak instalowanie i usuwanie pakietów. Adresy URL serwerów dowodzenia (C&C) są przechowywane w złośliwym pakiecie APK w postaci zakodowanej prostym algorytmem przesuwania bajtów.

Trojan:Android/SMSAgent.A

SMSAgent.A podszywa się pod grę, ale w tle wykonuje złośliwe procedury. Próbuje pobrać potencjalnie złośliwe pliki ze zdalnego serwera i wysyła wiadomości SMS i MMS, które obciążają rachunek użytkownika.



Ikona SMSAgent.A (po lewej stronie) i przywileje, o które prosi aplikacja (po prawej stronie)

Ponadto SMSAgent.A wyświetla reklamy i gromadzi poniższe informacje, które następnie wysyła do zdalnego serwera:

- identyfikator urządzenia,
- numer IMEI,
- typ sieci,
- operator.

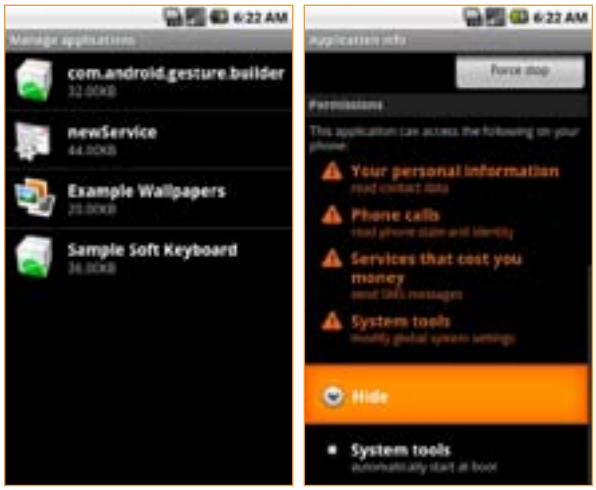
Trojan:Android/SpamSoldier.A

SpamSoldier.A jest rozpowszechniany za pośrednictwem wiadomości SMS, które zawierają łącze do pobrania bezpłatnej aplikacji. Po pomyślnej instalacji w urządzeniu program kontaktuje się z serwerem dowodzenia (C&C) i pozyskuje listę numerów telefonu. Na numery te wysyła dalsze wiadomości z łączem, które zachęca do pobrania atrakcyjnych bezpłatnych programów.

Trojan:Android/Stesec.A

Po instalacji w urządzeniu Stesec.A nie umieszcza żadnej ikony w menu aplikacji, aby ukryć swoją obecność przed użytkownikiem. Jest jednak wymieniony jako „newService" na liście „Zarządzaj aplikacjami" w menu „Ustawienia".

Stesec.A wysyła do zdalnego serwera wiadomości SMS z takimi informacjami o urządzeniu, jak numer IMEI, wersja oprogramowania i inne szczegóły.



Aplikacja Stesec.A wymieniona jako „newService" (po lewej stronie) i przywileje, o które prosi (po prawej stronie)

Trojan:Android/Stokx.A

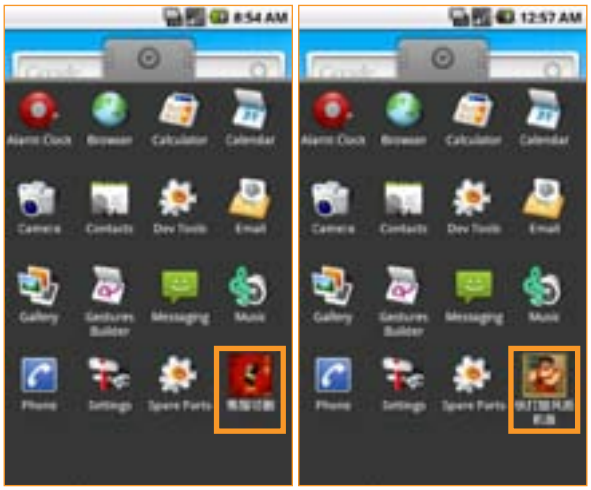
Stokx.A łączy się ze zdalnym serwerem i otrzymuje plik XML. Plik ten zawiera takie informacje, jak identyfikator klienta, numer telefonu, na który program ma wysyłać wiadomości SMS, oraz adres URL do pobrania dodatkowych pakietów APK.

Program przekazuje do zdalnego serwera numer International Mobile Equipment Identity (IMEI) i wysyła wiadomości o treści „SX357242043237517" na numer 13810845191.

Trojan:Android/Temai.A

Temai.A gromadzi poniższe informacje o urządzeniu, które następnie wysyła na kilka zdalnych adresów:

- identyfikator aplikacji,
- wersja aplikacji,
- kod kraju,
- numer IMEI,
- numer IMSI,
- wersja systemu operacyjnego.



Różne ikony używane przez Temai.A

Oprócz gromadzenia i wysyłania informacji program pobiera oraz instaluje w zainfekowanym urządzeniu potencjalnie złośliwe pakiety APK i pliki skryptów. Użytkownicy mogą być również narażeni na inne niebezpieczeństwa związane z uprawnieniami, o które prosi program podczas instalacji.

Uprawnienia, o które prosi Temai.A podczas instalacji

Trojan:Android/Tesbo.A

Tesbo.A nawiązuje połączenia z kilkoma zdalnymi serwerami, do których wysyła takie informacje, jak numer International Mobile Subscriber Identity (IMSI) oraz nazwa pakietu aplikacji.

Co więcej, program wysyła wiadomość SMS o treści *„[IMSI]@[losowa liczba z zakresu 1-10]" na numer 10658422.*

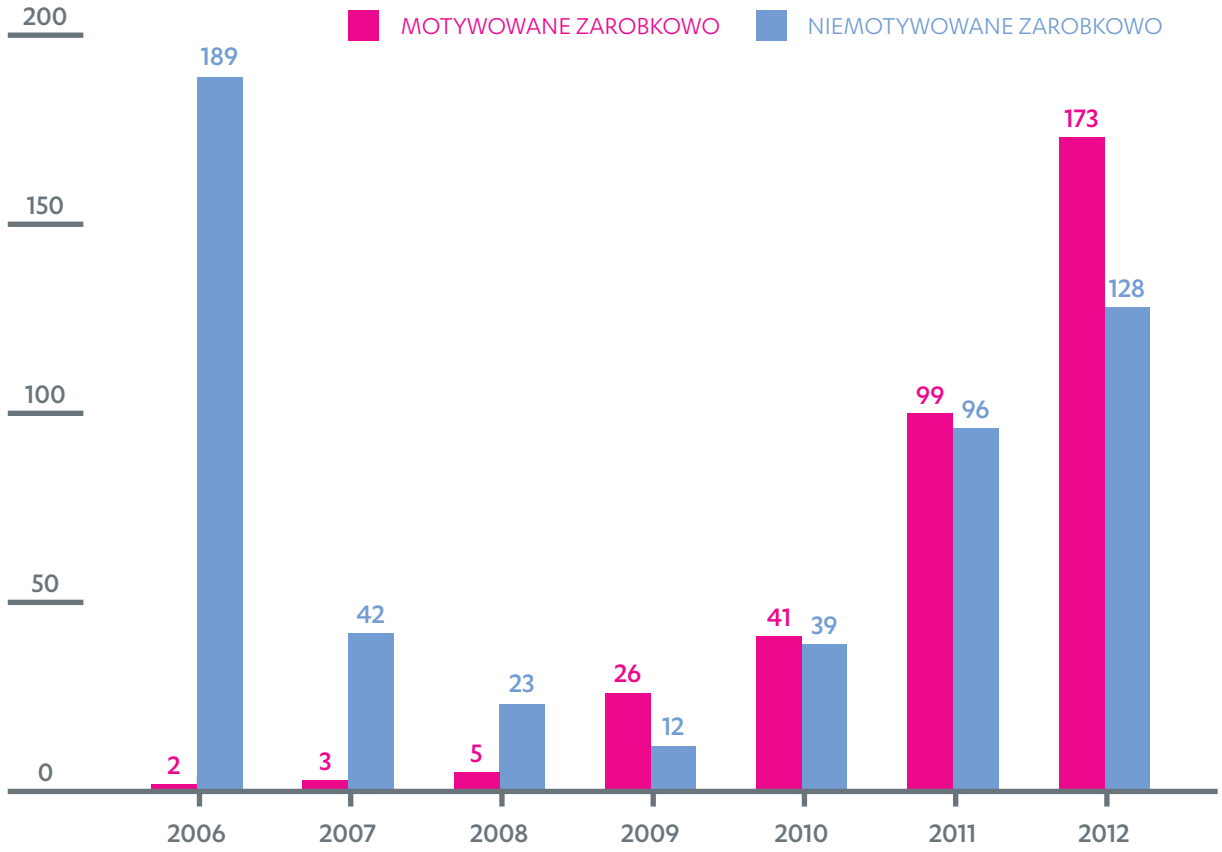
Trojan:SymbOS/Ankaq.A

Ankaq.A to program, który wysyła wiadomości SMS na numery premium i po cichu instaluje nowe oprogramowanie w zainfekowanym urządzeniu. Aby uniknąć wykrycia, przerywa wszystkie procesy należące do produktów antywirusowych.

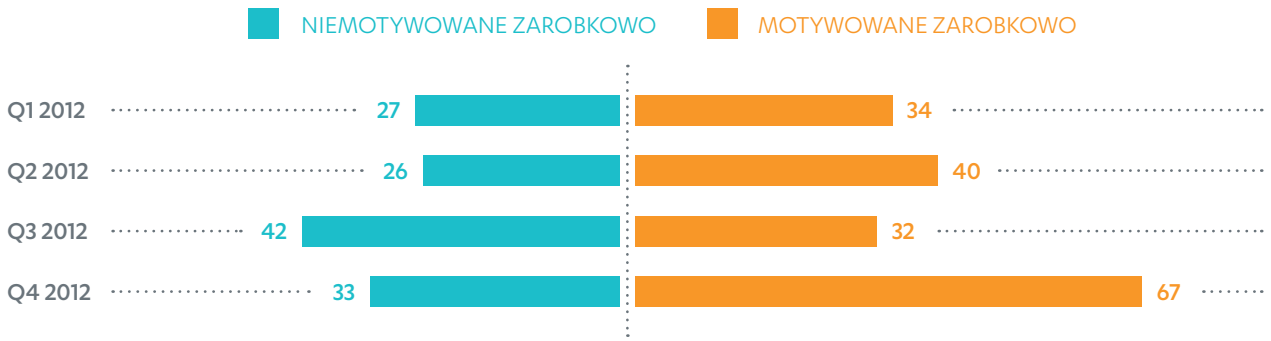
Trojan:SymbOS/Khluu.A

Khluu.A to program, który wysyła wiadomości SMS na numery premium i po cichu instaluje nowe oprogramowanie w zainfekowanym urządzeniu. Aby uniknąć wykrycia, przerywa wszystkie procesy należące do produktów antywirusowych.

RYSUNEK 5. ZAGROŻENIA MOBILNE MOTYWOWANE ZAROBKOWO WG ROKU, 2006-2012 R.

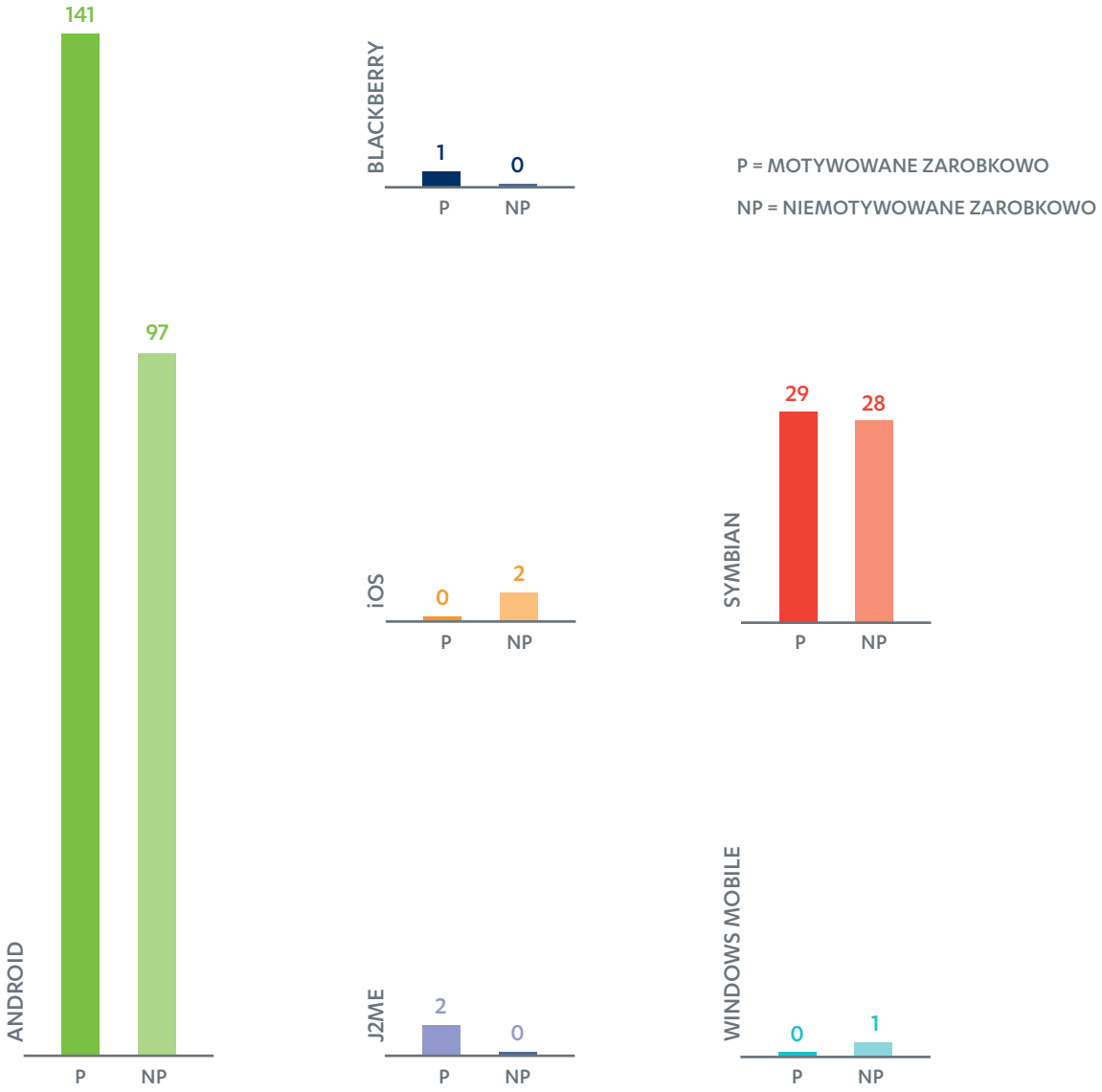


RYSUNEK 6. ZAGROŻENIA MOBILNE MOTYWOWANE ZAROBKOWO WG KWARTAŁU, 1-4 KWARTAŁ 2012 R.



UWAGA: statystyki przedstawione na **rysunkach 5 i 6** reprezentują rodziny i warianty zagrożeń, a nie unikatowe pliki. Jeśli na przykład dwie próbki wykryto jako Trojan:Android/GinMaster.A, w statystykach liczy się je jako jedną.

RYSUNEK 7: ZAGROŻENIA MOBILNE MOTYWOWANE ZAROBKOWO WG PLATFORMY, 2012 R.



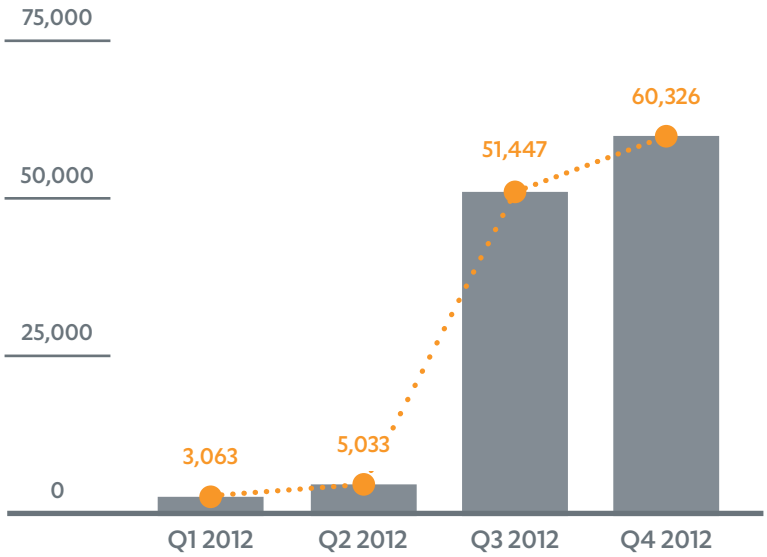
UWAGA: statystyki przedstawione na **rysunku 7** reprezentują rodziny i warianty zagrożeń, a nie unikatowe pliki. Jeśli na przykład dwie próbki wykryto jako Trojan:Android/GinMaster.A, w statystykach liczy się je jako jedną.

Nowe warianty znanych rodzin

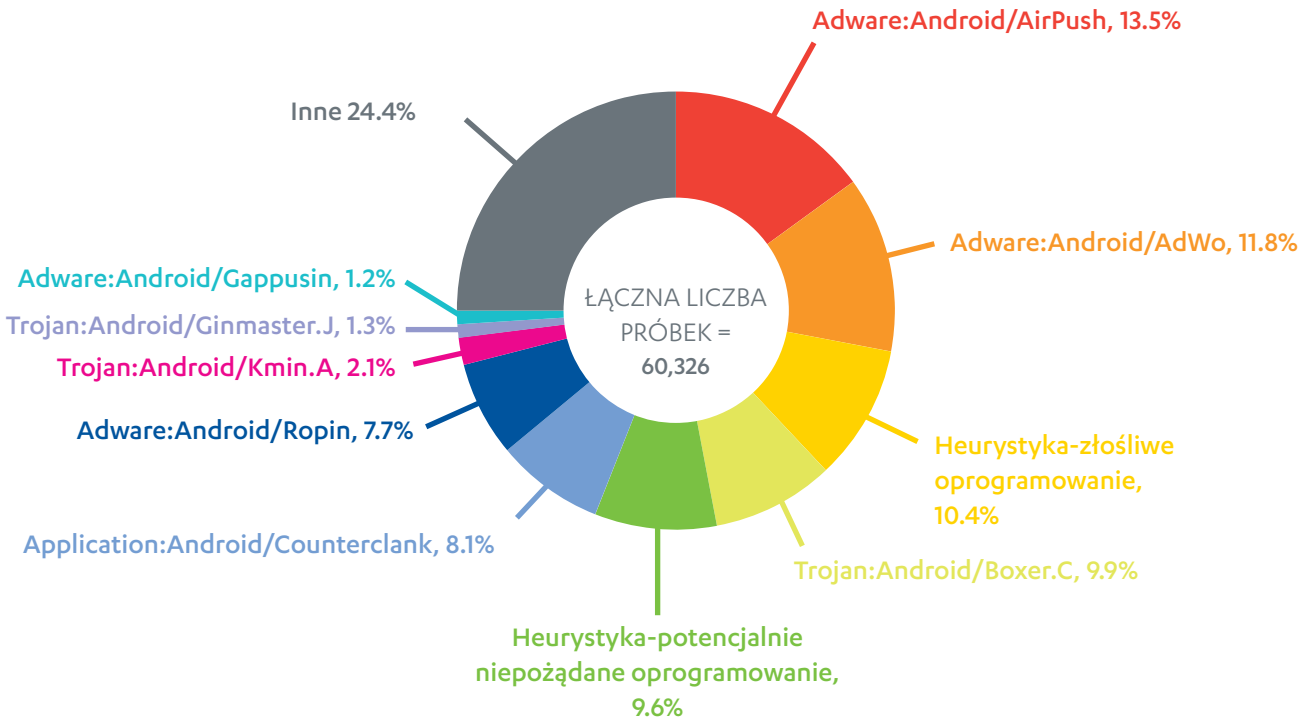
PONIŻEJ ZAMIESZCZONO LISTĘ NOWYCH WARIANTÓW ISTNIEJĄCYCH RODZIN ZŁOŚLIWEGO OPROGRAMOWANIA. NIE RÓŻNIĄ SIĘ ONE ZNACZNIE POD WZGLĘDEM FUNKCJONALNOŚCI OD STARSZYCH WARIANTÓW OPISANYCH W POPRZEDNICH RAPORTACH.

- Adware:Android/AdWo.C
- Adware:Android/AirPush.B
- Adware:Android/Gappusin.B
- Hack-Tool:Android/SmsBomber.B
- Monitoring-Tool:Android/AccuTrack.B
- Riskware:Android/Boxer.E
- Riskware:Android/Maxit.B
- Riskware:Android/PremiumSMS.F-Z (21 wariantów)
- Spyware:Android/EWalls.B
- Spyware:Android/SmsSpy.I
- Trojan:Android/DroidDream.H
- Trojan:Android/FakeInst.S-Y (7 wariantów)
- Trojan:Android/GinMaster.E-J (6 wariantów)
- Trojan:Android/GoldDream.B i wariant D
- Trojan:Android/HippoSms.B
- Trojan:Android/IconoSys.B
- Trojan:Android/JiFake.J
- Trojan:Android/MarketPay.B
- Trojan:Android/OpFake.I, L-O, (5 wariantów)
- Trojan:Android/SmsSend.E-G
- Trojan:Android/SmsSpy.G, H
- Trojan:Android/Vdloader.B
- Trojan:SymbOS/Foliur.B
- Trojan:SymbOS/CCAsrvSMS.D

RYSUNEK 8. LICZBA ZAGROŻEŃ ZWIĄZANYCH Z ANDROIDEM WEDŁUG KWARTAŁU, 1-4 KWARTAŁ 2012 R.



RYSUNEK 9. NAJCZĘŚCIEJ WYKRYWANE ZAGROŻENIA ZWIĄZANE Z ANDROIDEM, 4 KWARTAŁ 2012 R.



UWAGA: statystyki na **rysunkach 8 i 9** reprezentują liczbę unikatowych pakietów aplikacji Androida (APK).

TABELA 1. NAJBARDZIEJ ROZPOWSZECHNIONE ZŁOŚLIWE I POTENCJALNIE NIEPOŻĄDANE OPROGRAMOWANIE DO ANDROIDA, 4 KWARTAŁ 2012 R.

30 NAJCZĘŚCIEJ WYKRYWANYCH ZŁOŚLIWYCH PROGRAMÓW

WYKRYCIE	LICZBA
Heurystyka – złośliwe oprogramowanie	6265
Trojan:Android/Boxer.C	5989
Trojan:Android/Kmin.A	1270
Trojan:Android/Ginmaster.J**	775
Trojan:Android/FakeInst.A	723
Trojan:Android/Ginmaster.G**	615
Trojan:Android/FakeBattScar.A	608
Trojan:Android/SmsSend.A	543
Trojan:Android/FakeInst.K	502
Trojan:Android/SMStado.A	472
Trojan:Android/Temai.A**	443
Trojan:Android/Ginmaster.I**	434
Trojan:Android/Ginmaster.F**	423
Trojan:Android/Ginmaster.E**	368
Trojan:Android/Ginmaster.C	347
Trojan:Android/Ginmaster.B	336
Trojan:Android/Geinimi.D	295
Trojan:Android/FakeBattScar.B	269
Trojan:Android/RuFailedSMS.A	257
Trojan:Android/DroidKungFu.C	238
Trojan:Android/FakeInst.T**	230
Trojan:Android/OpFake.F	199
Trojan:Android/FakeInst.U**	188
Trojan:Android/Nyearleak.A	186
Trojan:Android/SMSLoader.A	163
Trojan:Android/FjCon.A	158
Trojan:Android/Kmin.B	146
Trojan:Android/JiFake.E	144
Trojan:Android/Kmin.C	139
Trojan:Android/IconoSys.A	118

30 NAJCZĘŚCIEJ WYKRYWANYCH POTENCJALNIE NIEPOŻĄDANYCH PROGRAMÓW

WYKRYCIE	LICZBA
Adware:Android/AirPush	8137
Adware:Android/AdWo	7127
Heurystyka – potencjalnie niepożądane oprogramowanie	5783
Application:Android/Counterclank	4860
Adware:Android/Ropin	4647
Adware:Android/Gappusin	733
Application:Android/FakeApp	549
Hack-Tool:Android/DroidRooter.A	230
Hack-Tool:Android/DroidRooter.B	161
Riskware:Android/Boxer	115
Riskware:Android/MobileTX	106
Spyware:Android/EWalls	91
Riskware:Android/PremiumSMS.F	69
Hack-Tool:Android/DroidRooter.I	51
Riskware:Android/SMSAgent	46
Application:Android/Steveware	39
Riskware:Android/FakeAngry	34
Monitoring-Tool:Android/MobileSpy.C	33
Hack-Tool:Android/TattooHack.A	32
Application:Android/NandroBox	32
Monitoring-Tool:Android/SpyTrack.B	28
Riskware:Android/AutoRegSms	25
Riskware:Android/PremiumSMS.J	23
Riskware:Android/PremiumSMS.AA	22
Riskware:Android/SmsReg	19
Riskware:Android/PremiumSMS.L	18
Monitoring-Tool:Android/MobileTracker.A	16
Monitoring-Tool:Android/SpyBubble.B	16
Riskware:Android/PremiumSMS.M	15
Hack-Tool:Android/DroidSheep.A**	15

**Nowa rodzina lub wariant wykryty w 4 kwartale 2012 r.

UWAGA: statystyki w **tabeli 1** reprezentują liczbę unikatowych pakietów aplikacji sytemu Android(APK).

F-SECURE MOBILE SECURITY

Przeciwdziałanie mobilnym zagrożeniom wymaga od producentów błyskawicznego czasu reakcji. Dzięki częstym automatycznym aktualizacjom i całodobowej pracy laboratoriów F-Secure, telefon z zainstalowanym programem Mobile Security jest chroniony również przed najnowszymi wynalazkami przestępców. Aplikacja F-Secure skutecznie chroni smartfony oraz tablety przed wszystkimi typowymi zagrożeniami, powstrzymując złośliwe oprogramowanie i zapewniając pełne bezpieczeństwo podczas przeglądania Internetu. Zabezpiecza także przed skutkami utraty i kradzieży urządzenia oraz dodatkowo oferuje zaawansowane funkcje kontroli rodzicielskiej.

Chronimy to, co dla Ciebie ważne

F-Secure®