RAPORT NA TEMAT ZAGROŻEŃ MOBILNYCH

2 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.

Całodobowa praca odbywa się na trzy zmiany - jedną w Helsinkach, a dwie w Kuala Lumpur. W każdym momencie eksperci ds. bezpieczeństwa z F-Secure Response Labs monitoruje światową sytuację w zakresie bezpieczeństwa, aby szybko i efektywnie radzić sobie z nagłymi epidemiami wirusów i złośliwego oprogramowania.

Ochrona przez całą dobę

Pracę Response Labs 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 w celach zarobkowych, nieustannie pracują nad nowymi metodami ataku. Sytuacja wymaga stałego monitoringu, aby internauci zawsze byli chronieni.

STRESZCZENIE

RAPORT OMAWIA KRAJOBRAZ ZAGROŻEŃ MOBILNYCH W DRUGIM KWARTALE 2012 ROKU I ZAWIERA DANE STATYSTYCZNE ORAZ SZCZEGÓŁOWE INFORMACJE NA TEMAT ZAGROŻEŃ, KTÓRE W TYM OKRESIE ZOSTAŁY ZAOBSERWOWANE I PRZEANALIZOWANE PRZEZ F-SECURE RESPONSE LABS. DANE PREZENTOWANE W RAPORCIE ZOSTAŁY ZGROMADZONE W OKRESIE OD 1 KWIETNIA DO 27 LIPCA 2012 R.

SPIS TREŚCI

STRESZCZENIE DLA KIEROWNICTWA

ZMIANY W KRAJOBRAZIE ZAGROŻEŃ DLA ANDROIDA

Liczba złośliwych programów na Androida rośnie w każdym kwartale, a II kwartał 2012 r. nie był wyjątkiem. Łącznie otrzymaliśmy 5033 złośliwe aplikacje na Androida (.apk), spośród których większość pochodziła z niezależnych od Androida źródeł. Oznacza to wzrost o 64 proc. w porównaniu z poprzednim kwartałem. W tej liczbie zidentyfikowaliśmy 19 nowych rodzin i 21 wariantów istniejących rodzin. Ogólnie rzecz biorąc, nowe warianty podejmują te same złośliwe działania, co poprzednie, ale wykorzystują skuteczniejsze metody zwalczania technologii antywirusowych w celu uniknięcia wykrycia.

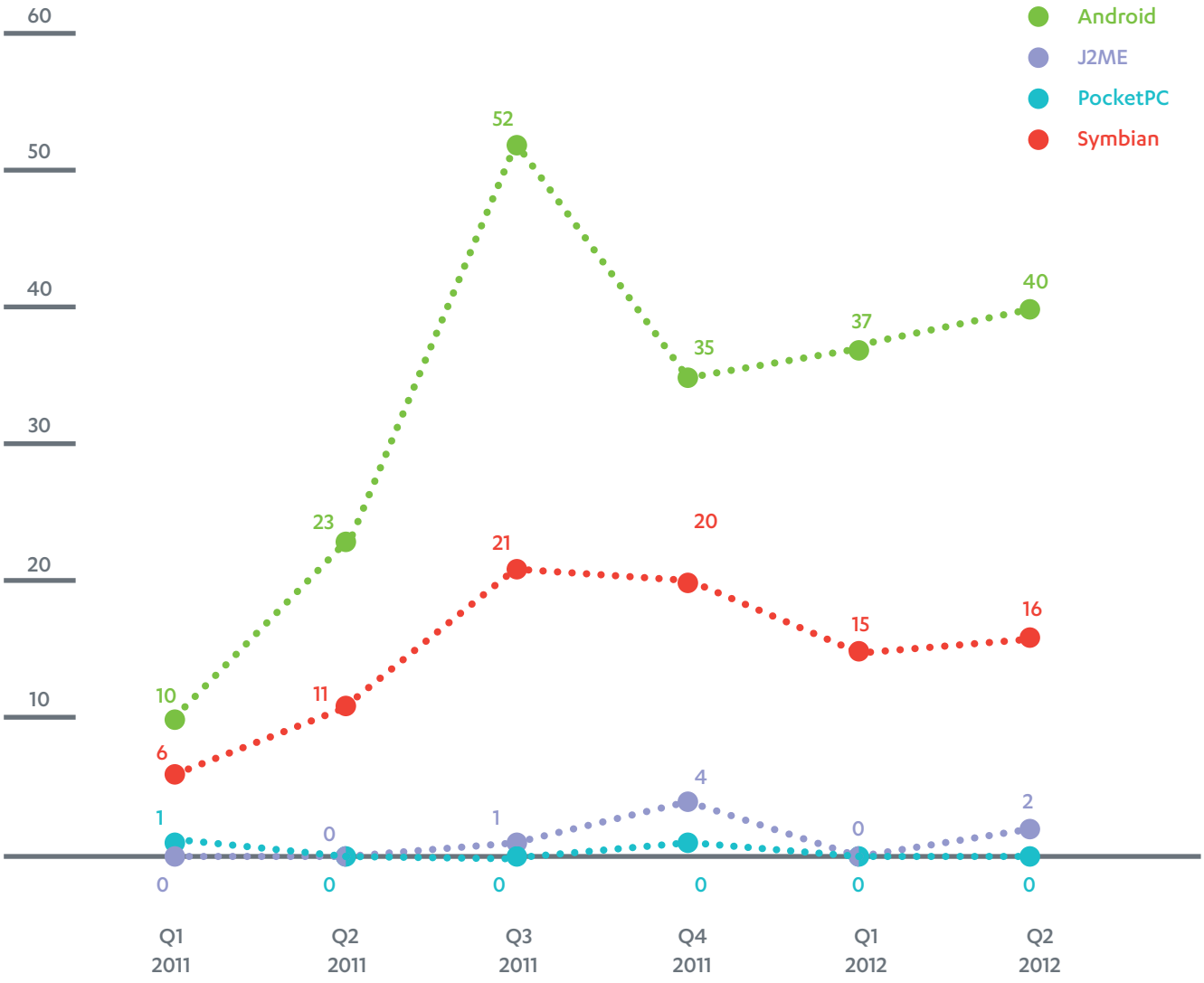
"W maju 2012 r. znaleziono pierwszy złośliwy program posługujący się metodą drive-by download."

Z biegiem czasu złośliwe oprogramowanie na Androida zaczęło wykorzystywać nowe metody infekcji, o czym świadczą warianty NotCompatible.A i Cawitt.A. W maju 2012 r. znaleziono pierwszy złośliwy program posługujący się metodą drive-by download (pobieranie szkodliwych programów ze stron internetowych bez wiedzy użytkownika), wykryty jako Trojan-Proxy:Android/NotCompatible.A. Do zainfekowania urządzenia mogła wystarczyć wizyta w złośliwej witrynie, jeśli urządzenie było skonfigurowane tak, aby zezwalać na instalację z nieznanych źródeł. Podczas wizyty na specjalnie stworzonej www urządzenie automatycznie pobiera aplikację, która jest następnie wyświetlana w menu powiadomień, oczekując na zainstalowanie przez użytkownika. Aby przekonać go do instalacji, złośliwe oprogramowanie wykorzystuje metody socjotechniczne, nadając aplikacji taką nazwę, jak „com.Security.Update", a plikowi – „Update.Apk". Zainfekowane urządzenie zaczyna działać jako proxy albo staje się częścią sieci botów.

Oprócz drive-by download inną metodą infekcji odkrytą w tym kwartale jest wykorzystanie Twittera jako mechanizmu zarządzania botami. Na przykład Cawitt.A uzyskuje dostęp do konta na Twitterze (być może założonego przez złośliwe oprogramowanie), aby uzyskać adres serwera, z którym następnie się komunikuje i od którego otrzymuje polecenia. Po otrzymaniu instrukcji program wysyła wiadomości SMS na pewne numery i przekazuje numer IMEI (International Mobile Equipment Identity), numer telefonu i identyfikator Androida do wspomnianego wyżej serwera.

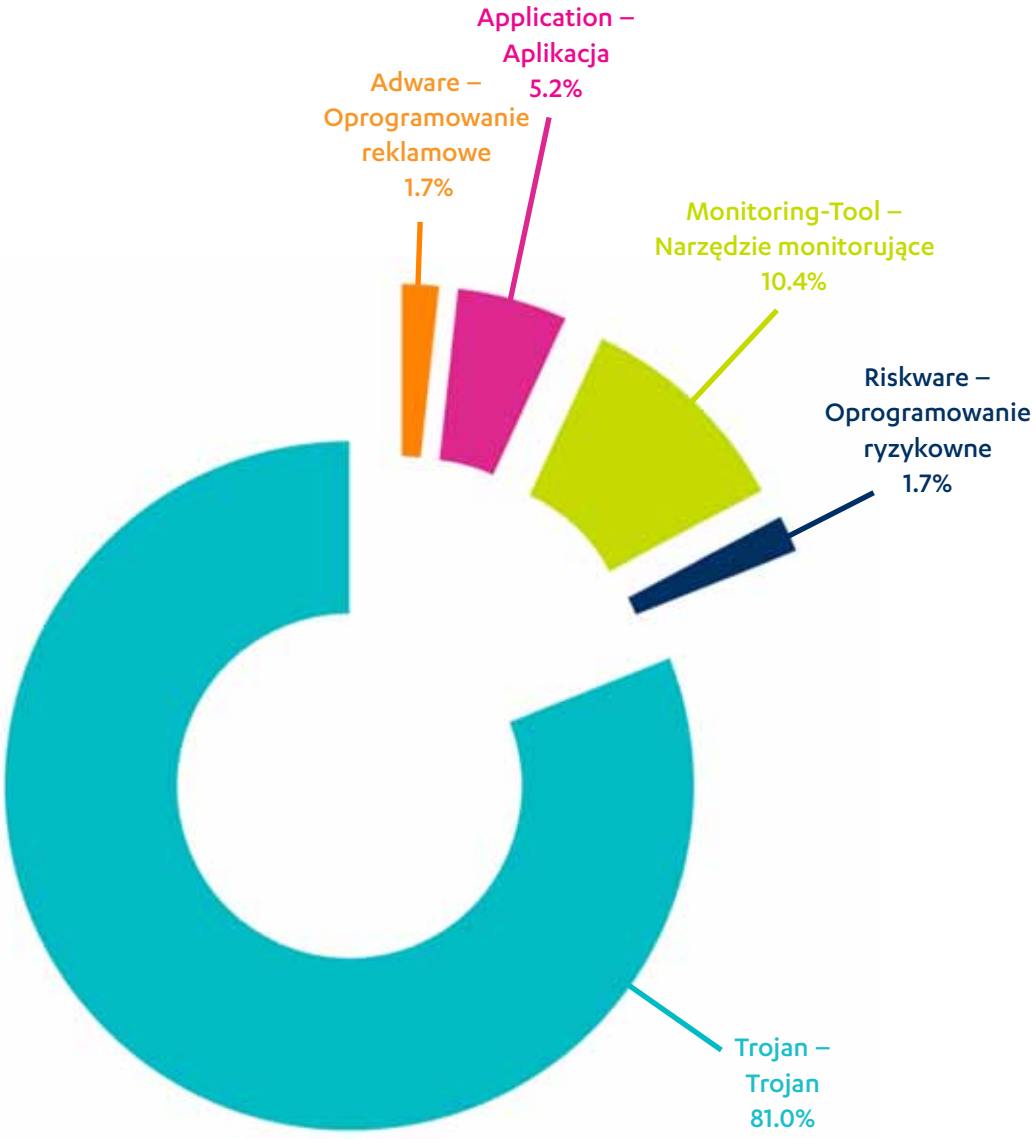
Oprócz dalszego wzrostu liczby złośliwych programów Androida oraz odkrycia nowych metod infekcji, w drugim kwartale można było również zaobserwować trend ataków regionalnych. Na przykład w Hiszpanii pojawiło się wiele ataków związanych z bankowością. W tym kwartale dość często zgłaszany był program SmsSpy.F, spokrewniony z Zitmo. Oprogramowanie wydaje się wycelowane specjalnie w użytkowników, którzy przeprowadzają internetowe transakcje bankowe i potrzebują kodów Mobile Transaction Authorization Number (mTAN).Złośliwa aplikacja jest dostarczona jako wiadomość SMS, zalecając użytkownikowi pobranie aplikacji zabezpieczającej spod podanego łącza.

NAJNOWSZE ZAGROŻENIA ODKRYTE W CIĄGU OSTATNICH TRZECH MIESIĘCY



RYSUNEK 1. NOWE RODZINY I WARIANTY WEDŁUG KWARTAŁU

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. ZAGROŻENIA MOBILNE WEDŁUG TYPU, 2 KWARTAŁ 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.

Adware:Android/Mobsqueeze.A

Mobsqueeze.A to moduł oprogramowania reklamowego używany wyłącznie przez trojany z rodziny FakeBattScar do reklamowania złośliwego programu Battery Optimizer lub Battery Optimizer Application. Dodano też oddzielną kategorię wykryć, do której należą aplikacje, które promują trojany FakeBattScar.

Zezwolenia, o które prosi Mobsqueeze.A

Application:Android/AdOp.A

AdOp.A to aplikacja, która tworzy skróty oraz reklamowe powiadomienia z łączem do witryny internetowej albo aplikacji. Aplikacja, do której prowadzi łącze, może być nieobecna w urządzeniu, ale to nie powstrzymuje AdOp.A przed utworzeniem odpowiedniego skrótu.

Aplikacja AdOp.A nie jest bezpośrednio szkodliwa dla urządzenia, ale może stwarzać pewne zagrożenie, jeśli skrót lub powiadomienie prowadzi do niezaufanej witryny.

Monitoring-Tool:Android/AndSpy.A

AndSpy.A to program monitorujący i antykradzieżowy, który pochodzi z Chin, ale jest również oferowany w kilku regionach anglojęzycznych. Jego funkcje można włączyć zdalnie przez wysłanie specjalnej wiadomości SMS do urządzenia. Jeśli wiadomość zawiera prawidłowe polecenie, urządzenie po cichu wykona odpowiednie zadanie, na przykład:

- 0# : rejestracja numeru głównego, który będzie używany do wysyłania odpowiedzi
- 1# : włączenie przekazywania SMS-ów
- 2# : wyłączenie przekazywania SMS-ów
- 8# : wysłanie kontaktów z pamięci urządzenia
- 10# : wysłanie bieżącej lokalizacji

AndSpy.A to program działający w ukryciu. Wykonuje złośliwe operacje po cichu i nie pozostawia widocznych śladów swojej obecności w urządzeniu.

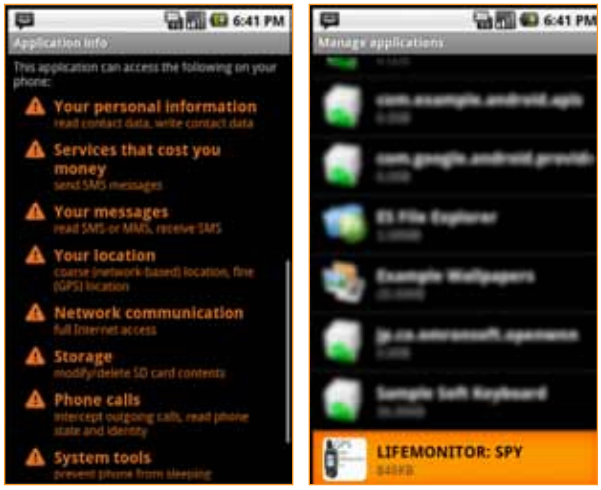
Monitoring-Tool:Android/Lifemonspy.A

Lifemonspy.A to program monitorujący i antykradzieżowy, który umożliwia użytkownikom sterowanie urządzeniem za pośrednictwem wiadomości SMS. Pozwala zdalnie wykonać następujące operacje:

- Usunięcie kontaktów
- Usunięcie zawartości pamięci zewnętrznej (karty SD)
- Przeniesienie wiadomości SMS ze skrzynki odbiorczej na konto Gmail
- Usunięcie poprzednio wysłanych wiadomości ze skrzynki nadawczej
- Wyłączenie urządzenia

Program nie umieszcza widocznej ikony na ekranie menu, ale znajduje się na liście w oknie „Zarządzaj aplikacjami". Od czasu do czasu przekazuje lokalizację urządzenia do zdalnej witryny.

Po wykryciu zmiany karty Subscriber Identity Module (SIM) w urządzeniu, Lifemonspy.A wysyła wiadomość alarmową na skonfigurowany numer i rejestruje zdarzenie we wspomnianej wyżej witrynie.



Uprawnienia, o które prosi Lifemonspy.A (po lewej stronie, oraz Lifemonspy.A widoczny w oknie „Zarządzaj aplikacjami" (po prawej stronie)

Monitoring-Tool:Android/MobileTracker.A

MobileTracker.A to część bezpłatnej usługi Samsung DIVE, która pozwala właścicielowi zdalnie śledzić i kontrolować urządzenie. W przypadku kradzieży właściciel może zablokować urządzenie i wymazać jego zawartość, otrzymać powiadomienie o zmianie karty SIM, a także śledzić lokalizację urządzenia.

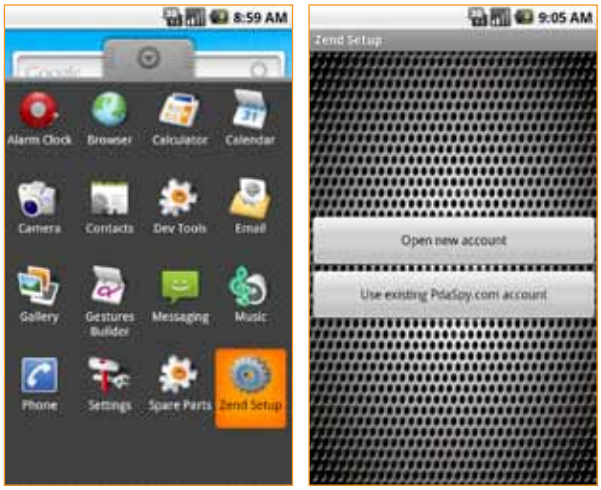
Monitoring-Tool:Android/PdaSpy.A

PdaSpy.A to komercyjna aplikacja monitorująca z 24-godzinnym bezpłatnym okresem próbnym. Musi zostać ręcznie zainstalowana na docelowym urządzeniu i wymaga utworzenia konta w witrynie PdaSpy.com.

Po instalacji nie umieszcza ikony w menu aplikacji, żeby uniknąć wykrycia. Działa po cichu w tle, rejestrując następujące informacje:

- Rozmowy telefoniczne
- Wiadomości SMS
- Lokalizacje GPS

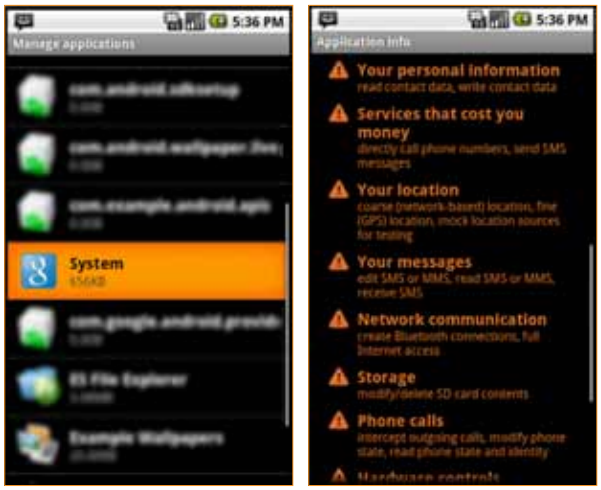
Informacje można obejrzeć po zalogowaniu się na koncie użytkownika w witrynie PdaSpy.



Do obejrzenia zarejestrowanych danych wymagane jest konto w witrynie PdaSpy.com

Monitoring-Tool:Android/SpyEra.A

Program SpyEra.A służy do monitorowania i pobierania danych z urządzenia. Rozpoczyna złośliwą działalność, kiedy urządzenie otrzyma specjalnie skonstruowaną wiadomość SMS.
SpyEra.A nie umieszcza widocznej ikony w menu aplikacji, ale jego obecność można stwierdzić w oknie „Zarządzaj aplikacjami" w ustawieniach urządzenia.
.

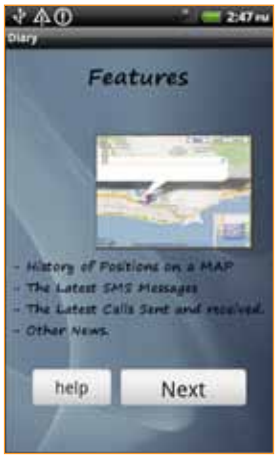


Program SpyEra.A wymieniony w oknie „Zarządzaj aplikacjami" (po lewej stronie) oraz uprawnienia, o które prosi (po prawej stronie)

Monitoring-Tool:Android/SpyHasb.A

SpyHasb.A to komercyjne narzędzie monitorujące, które jest reklamowane m.in. jako „Phone Tracker", „Husband Tracker", „Wife Tracker" i „Android Locator". Umożliwia monitorowanie następujących informacji:

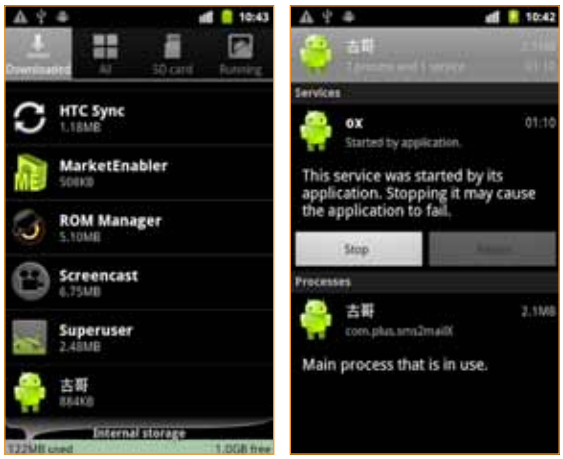
- Rozmowy telefoniczne
- Wiadomości SMS
- Lokalizacje GPS



Interfejs użytkownika SpyHasb.A na ekranie urządzenia

Riskware:Android/QPlus.A

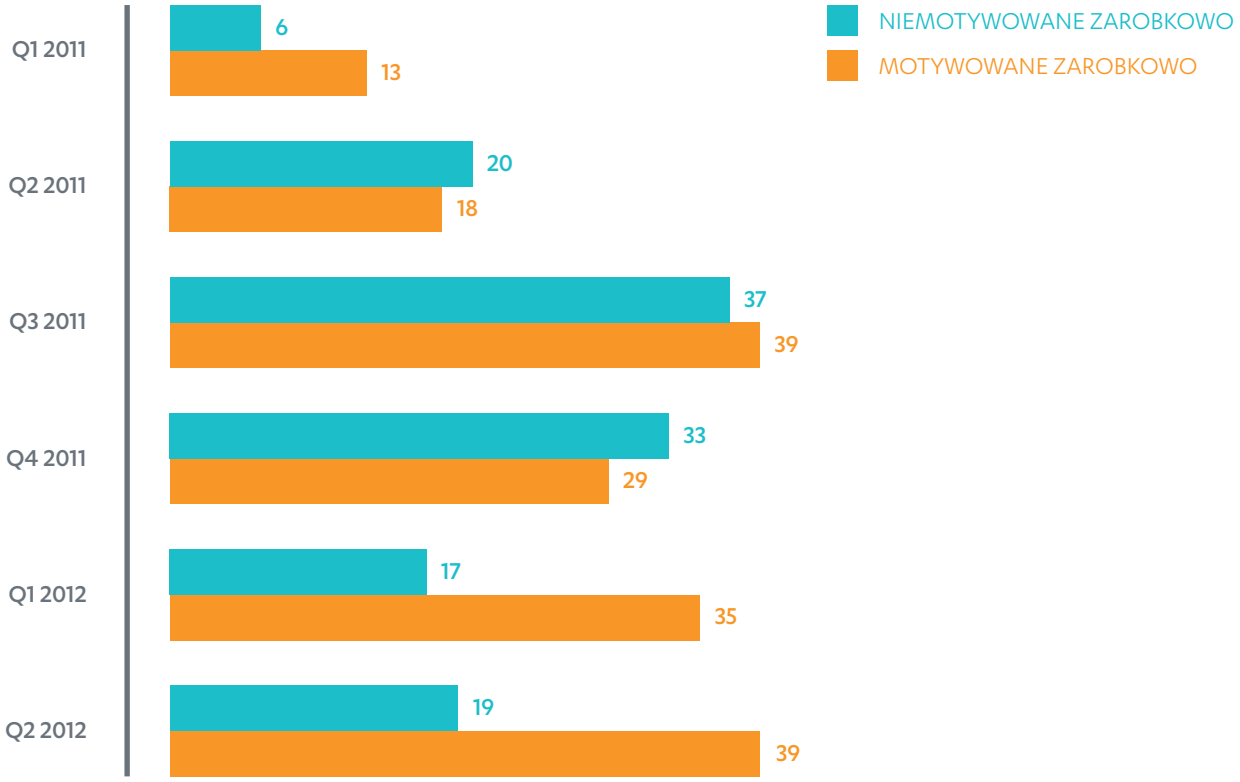
QPlus.A to narzędzie, które gromadzi informacje z urządzenia, w którym je zainstalowano. Działa po cichu w tle i nie jest widoczne na liście aplikacji. Można je natomiast znaleźć na ekranie „Zarządzaj aplikacjami".



QPlus.A działa w tle jako usługa

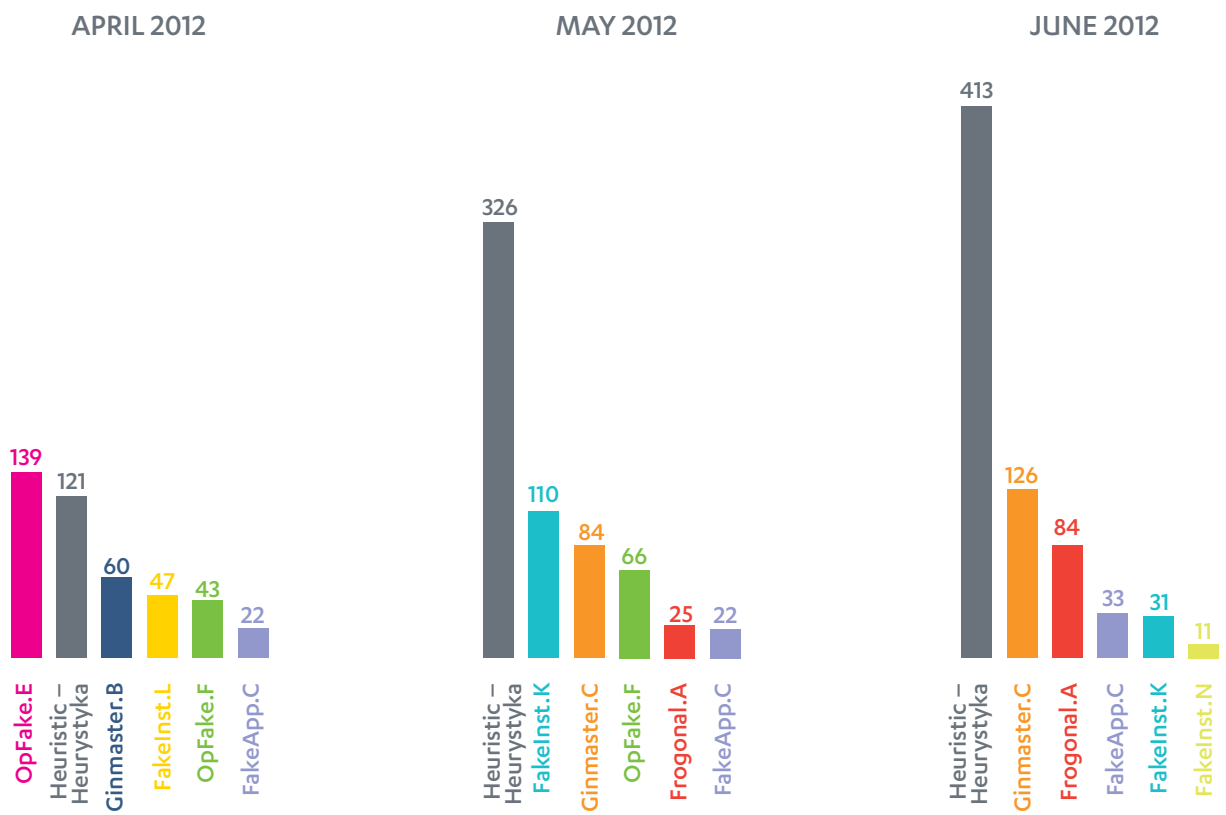
Podczas monitorowania urządzenia QPlus.A działa w tle jako usługa. Monitoruje i gromadzi następujące informacje, które następnie wysyła do pośredniczącego serwera pocztowego:

- Dzienniki połączeń
- Wiadomości SMS
- Historia czatów przez komunikatory internetowe

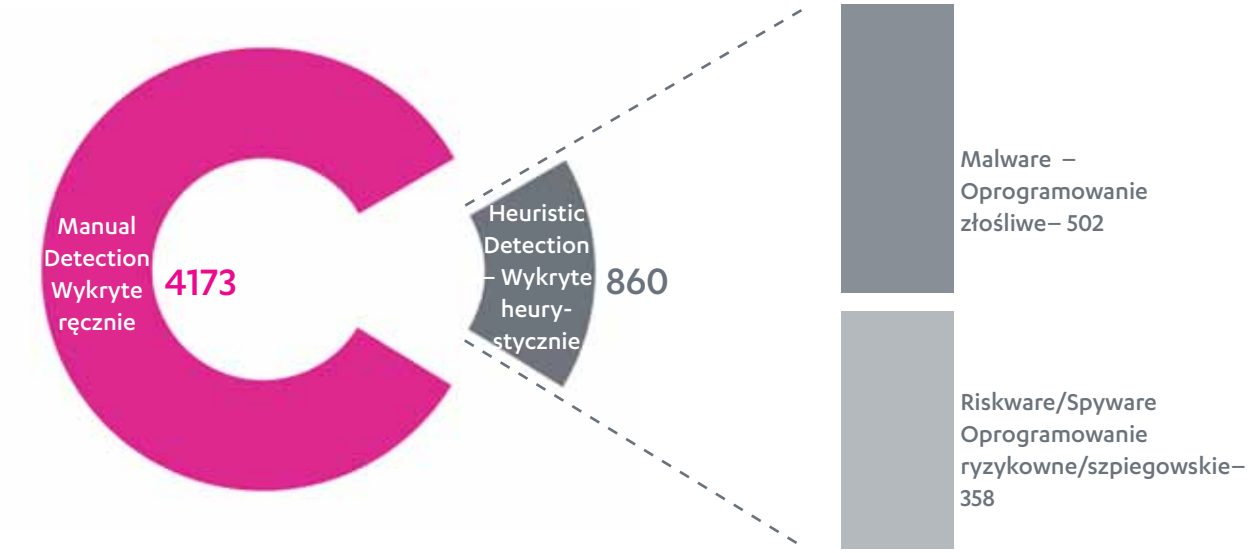


RYSUNEK 3. ZAGROŻENIA MOBILNE MOTYWOWANE ZAROBKOWO

UWAGA: statystyki przedstawione na rysunku 3 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 4. 6 NAJCZĘŚCIEJ WYKRYWANYCH ZAGROŻEŃ DLA ANDROIDA WEDŁUG MIESIĄCA, 2 KWARTAŁ 2012 R.



RYSUNEK 5. PODZIAŁ WEDŁUG METODY WYKRYCIA, 2 KWARTAŁ 2012 R.

UWAGA: statystyki na rysunkach 4 i 5 reprezentują liczbę unikatowych pakietów aplikacji Androida (.apk).

Złośliwe oprogramowanie

PROGRAMY SKLASYFIKOWANE JAKO ZŁOŚLIWE ZWYKLE STANOWIĄ DUŻE 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, NISZCZENIE LUB MODYFIKOWANIE DANYCH BEZ AUTORYZACJI ORAZ KRADZIEŻ DANYCH ALBO POŚWIADCZEŃ DOSTĘPU.

Trojan:Android/AcnetSteal.A

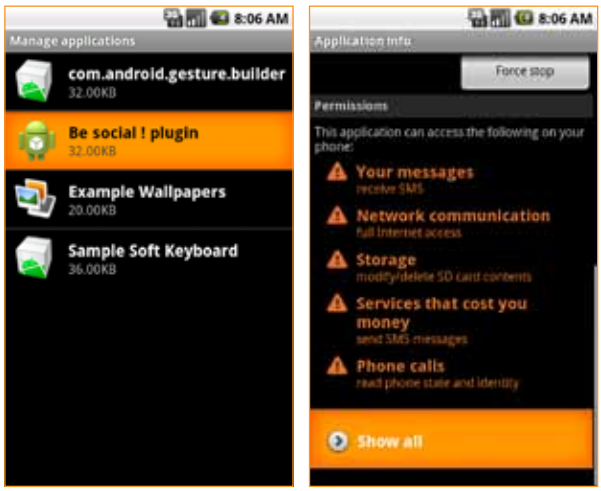
AcnetSteal.A to program, który gromadzi dane z urządzenia. Uzyskuje następujące informacje:

- Adresy e-mail
- Numery telefonu

AcnetSteal.A na ekranie urządzenia

Trojan:Android/Cawitt.A

Po instalacji Cawitt.A nie umieszcza ikony w menu aplikacji, aby użytkownik go nie zauważył. Jego obecność można jednak stwierdzić w oknie „Zarządzaj aplikacjami" w ustawieniach urządzenia.



Cawitt.A na liście aplikacji oraz uprawnienia, o które prosi

Cawitt.A działa po cichu w tle, gromadząc informacje, które następnie przekazuje do zdalnego serwera. Do gromadzonych informacji należą:

- Identyfikator urządzenia
- Numer IMEI (International Mobile Equipment Identity)
- Numer telefonu
- Identyfikator bota
- Moduły

Po otrzymaniu polecenia od zdalnego serwera program wysyła też z urządzenia wiadomości SMS typu premium.

Trojan:Android/Frogonal.A

Frogonal.A to oprogramowanie „strojanizowane", zmodyfikowana wersja oryginalnej aplikacji, do której dodano funkcje służące do złośliwych celów.

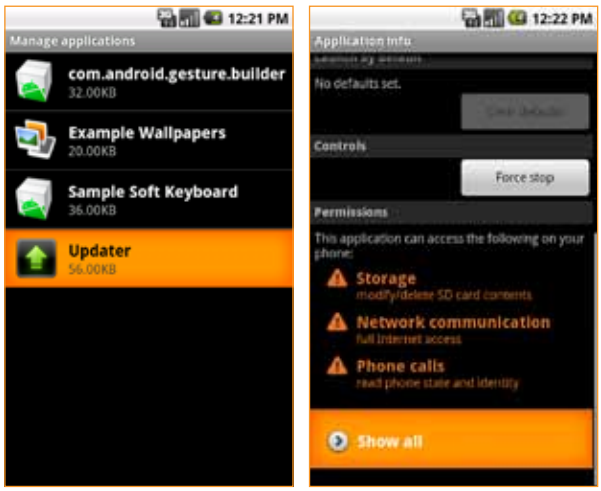
Frogonal.A gromadzi następujące informacje z zainfekowanego urządzenia:

- Identyfikacja strojanizowanej aplikacji
  - » Nazwa pakietu
  - » Kod wersji
- Numer telefonu
- Numer IMEI
- Numer IMSI
- Numer seryjny karty SIM
- Model urządzenia
- Wersja systemu operacyjnego
- Dostępność administratora

Uprawnienia, o które prosi Frogonal.A, i gry, które oferuje

Trojan:Android/Gamex.A

Gamex.A ukrywa swoje złośliwe komponenty w pliku pakietu. Kiedy otrzyma od użytkownika administracyjne przywileje dostępu, łączy się z serwerem dowodzenia (C&C), aby pobrać więcej aplikacji i przekazać numery IMEI i IMSI. Ponadto nawiązuje połączenie z zewnętrznym adresem, pod którym znajduje się zmieniony plik .apk, po czym pobiera i instaluje plik.



Trojan Gamex.A wymieniony jako „Updater" (po lewej stronie) oraz uprawnienia, o które prosi (po prawej stronie)

Trojan:Android/KabStamper.A

KabStamper.A to złośliwy program, który krążył w Japonii podczas „wyborów" AKB48. AKB48 to japońska grupa popowa, która składa się z 48 członków. „Wybory" miały wyłonić najbardziej popularnego członka, który stanie się twarzą grupy.

AKB48: popularna japońska grupa popowa licząca 48 członków.

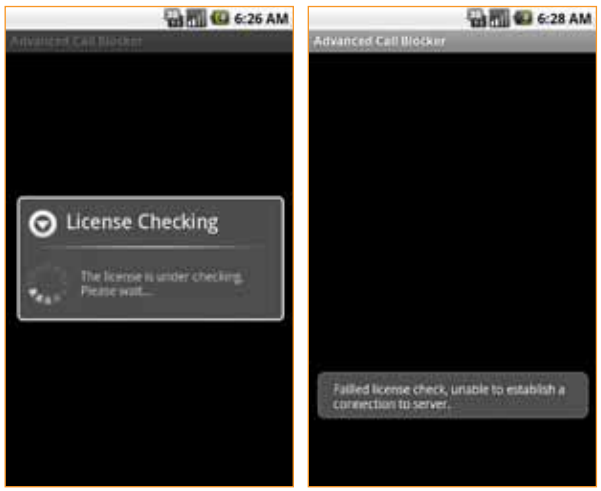
KabStamper.A jest rozpowszechniany za pośrednictwem „strojanizowanych" aplikacji, które dostarczają wiadomości i filmy poświecone grupie AKB48. Złośliwy kod jest bardzo destrukcyjny; niszczy pliki w folderze **sdcard/DCIM/camera**, w którym przechowywane są zdjęcia zrobione aparatem urządzenia. Co pięć minut program sprawdza ten folder i zastępuje znalezione zdjęcia wstępnie zdefiniowanym obrazem.

Porównanie: przed i po infekcji KabStamper.A

Trojan:Android/Mania.A

Mania.A to złośliwy program SMS-owy, który wysyła wiadomości o treści „tel" lub „quiz" na numer 84242. Każda odpowiedź z tego numeru jest przekierowywana do innego urządzenia, aby nie budzić podejrzeń użytkownika.

Kiedy Mania.A działa, pozoruje sprawdzanie licencji, ale proces ten zawsze kończy się niepowodzeniem. To sprawdzanie licencji jest przykrywką dla wysyłania wiadomości SMS, które odbywa się w tle..



Mania.A udaje, że sprawdza licencję, co zawsze kończy się niepowodzeniem

Program Mania.A jest znany z techniki „trojanizacji", która polega na dołączaniu złośliwego kodu do pakietu innej oryginalnej aplikacji w celu oszukania ofiar. Oto niektóre znane, legalne aplikacje, w których znaleziono ten złośliwy kod:

- Phone Locator Pro
- CoPilot Live Europe
- Setting Profile Full
- Tasker

Trojan:Android/PremiumSMS.A, and variant B

PremiumSMS.A to trojan, który czerpie zyski z wysyłania wiadomości SMS. Ma plik konfiguracyjny, który zawiera dane dotyczące treści wiadomości oraz numerów odbiorców.

Przykłady wysyłanych wiadomości:

- Numer: 1151
- Treść: 692046 169 BGQCb5T3w

- Numer: 1161
- Treść: 692046 169 BGQCb5T3w

- Numer: 3381
- Treść: 692046 169 BGQCb5T3w

- Numer: 1005
- Treść: kutkut clsamg 6758150

- Numer: 5373
- Treść: kutkut clsamg 6758150

- Numer: 7250
- Treść: kutkut clsamg 6758150

Trojan:Android/SmsSpy.F

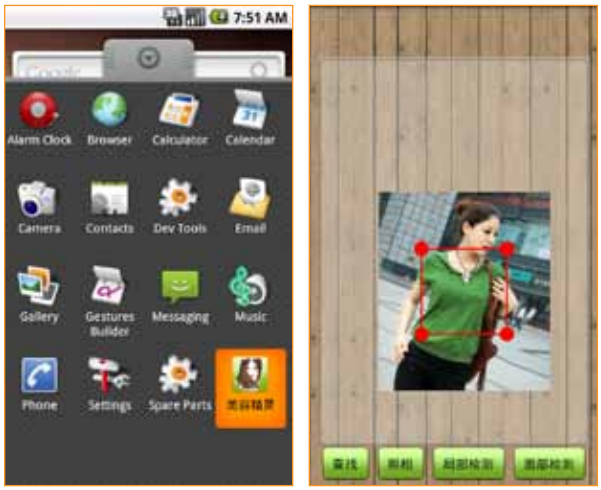
SmsSpy.F podaje się za aplikację Android Security Suite, która w rzeczywistości nie robi nic, żeby zapewnić bezpieczeństwo urządzenia. Rejestruje natomiast otrzymane wiadomości SMS w pliku secsuite.db.

SmsSpy.F podaje się za aplikację Android Security Suite

Oprogramowanie to jest wymierzone w użytkowników bankowości internetowej w Hiszpanii. Rozprzestrzenia się z wykorzystaniem wiadomości, która informuje użytkownika, że jest dostępny do pobrania dodatkowy program rzekomo chroniący urządzenie.

Trojan:Android/UpdtKiller.A

UpdtKiller.A łączy się z serwerem dowodzenia (C&C), do którego przekazuje dane użytkownika i od którego odbiera polecenia. Program ten potrafi również przerywać procesy antywirusowe, aby uniknąć wykrycia.



UpdtKiller.A na ekranie urządzenia

Trojan:Android/Uranico.A

Uranico.A to trojan, który gromadzi następujące informacje z zainfekowanego urządzenia:

- Numer telefonu
- Numer IMEI
- Numer IMSI
- Kontakty lub książka adresowa (numery telefonu i adresy e-mail)

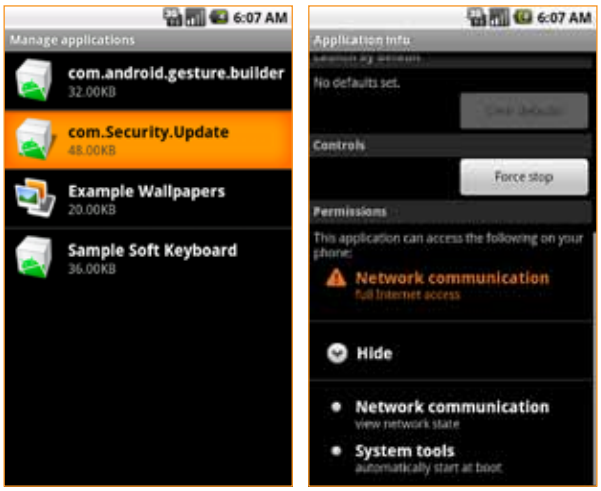
Zgromadzone informacje są następnie przekazywane do zdalnego serwera.

Uranico.A na ekranie urządzenia

Trojan-Proxy:Android/NotCompatible.A

NotCompatible.A działa podobnie, jak wirusy typu drive-by download. Zyskuje dostęp do urządzenia, kiedy użytkownik odwiedza zainfekowaną witrynę, i przystępuje do pobierania pakietu update.apk. Aby jednak instalacja się rozpoczęła, użytkownik musi kliknąć pakiet.

Po instalacji program może komunikować się z serwerami dowodzenia (C&C), o czym świadczą dwa adresy, które znajdują się w zaszyfrowanym pliku dołączonym do programu.



NotCompatible.A udaje plik z aktualizacją zabezpieczeń

Trojan:J2ME/CuteFreeSMS.A

CuteFreeSMS.A to trojan, który czerpie zyski z wysyłania wiadomości SMS na numery premium. Wysyłanie wiadomości odbywa się w tle, bez autoryzacji i wiedzy użytkownika.

Trojan:J2ME/ValeSMS.A

ValeSMS.A to trojan, który czerpie zyski z wysyłania wiadomości SMS na numery premium. Wysyłanie wiadomości odbywa się w tle, bez autoryzacji i wiedzy użytkownika.

Trojan:SymbOS/AndroGamer.A

AndroGamer.A to trojan, który – jak się zdaje – gra w tle w gry internetowe lub WAP. Podejmuje też inne złośliwe czynności:

- Pobieranie i instalowanie nowego oprogramowania
- Pobieranie danych konfiguracyjnych ze zdalnego hosta
- Wysyłanie informacji o urządzeniu do zdalnego hosta
- Wybieranie numerów w celu nawiązywania połączeń

Trojan:SymbOS/Kensoyk.A

Kensoyk.A zawiera odwołania do producentów oprogramowania antywirusowego i potrafi przerywać procesy antywirusowe. Pobiera też oprogramowanie i instaluje je w zainfekowanym urządzeniu.

Trojan:SymbOS/LaunchOut.A

LaunchOut.A jest ukryty i niewidoczny w interfejsie urządzenia, co pomaga mu uniknąć wykrycia. Wykonuje w tle następujące czynności:

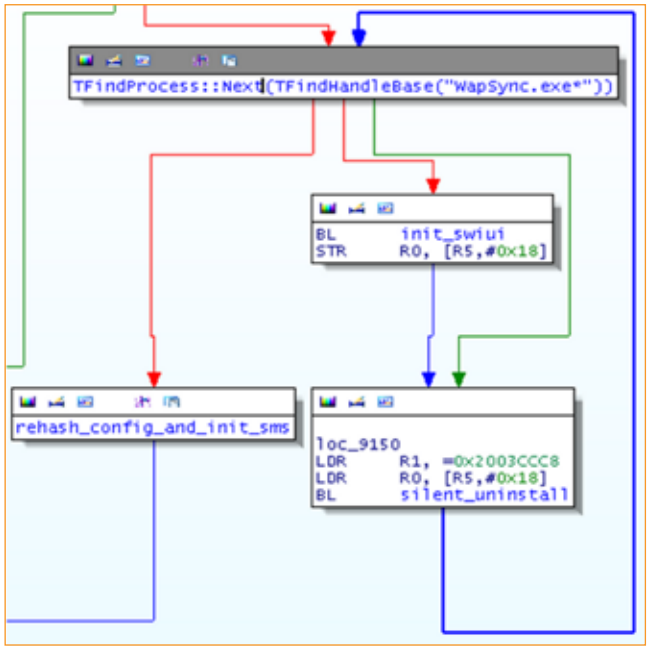
- Pobieranie i instalowanie nowego oprogramowania
- Monitorowanie i wysyłanie wiadomości SMS

Trojan:SymbOS/Lipcharge.A

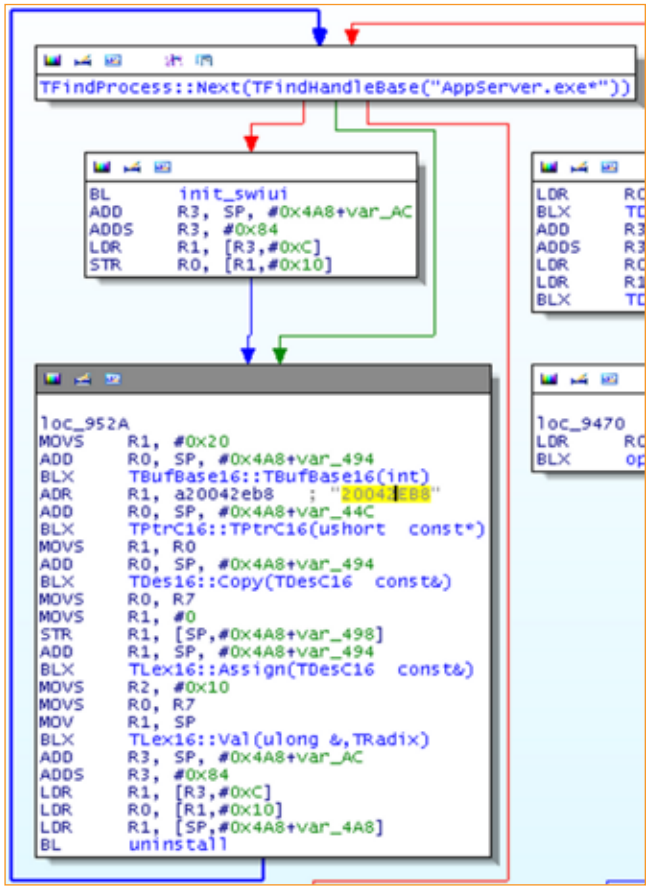
Lipcharge.A jest prawdopodobnie pobieranym z sieci komponentem innego trojana. Pobiera dane konfiguracyjne i nowe oprogramowanie, a następnie instaluje je w zainfekowanym urządzeniu. Inne funkcje obejmują wysyłanie i odbieranie wiadomości SMS oraz filtrowanie pewnych wiadomości SMS w dzienniku systemowym.

Trojan:SymbOS/Monlater.A, and variant B

Monlater.A zawiera funkcję, która wykrywa procesy AppServer.exe i odinstalowuje pakiet z identyfikatorem UID 0x20042EB8 z zainfekowanego urządzenia. Podobne funkcje znajdują się również w próbce Monlater.B, ale używają innej nazwy pliku i identyfikatora UID.



Adnotowana dezasemblacja próbki Monlater.B, pokazująca podobieństwa z Monlater.A



Adnotowana dezasemblacja funkcji z próbki Monlater.A

Próbki z rodziny Monlater wykazują wiele podobieństw z inną rodziną, Monsoon, która została odkryta po raz pierwszy na początku 2011 r. Jest bardzo prawdopodobne, że Monsoon i Monlater łączą się z tym samym serwerem dowodzenia (C&C). Ten sam kanał aktualizacji może być również używany do przesyłania nowych wersji złośliwego oprogramowania i ukrywania pierwotnych w celu uniknięcia wykrycia.

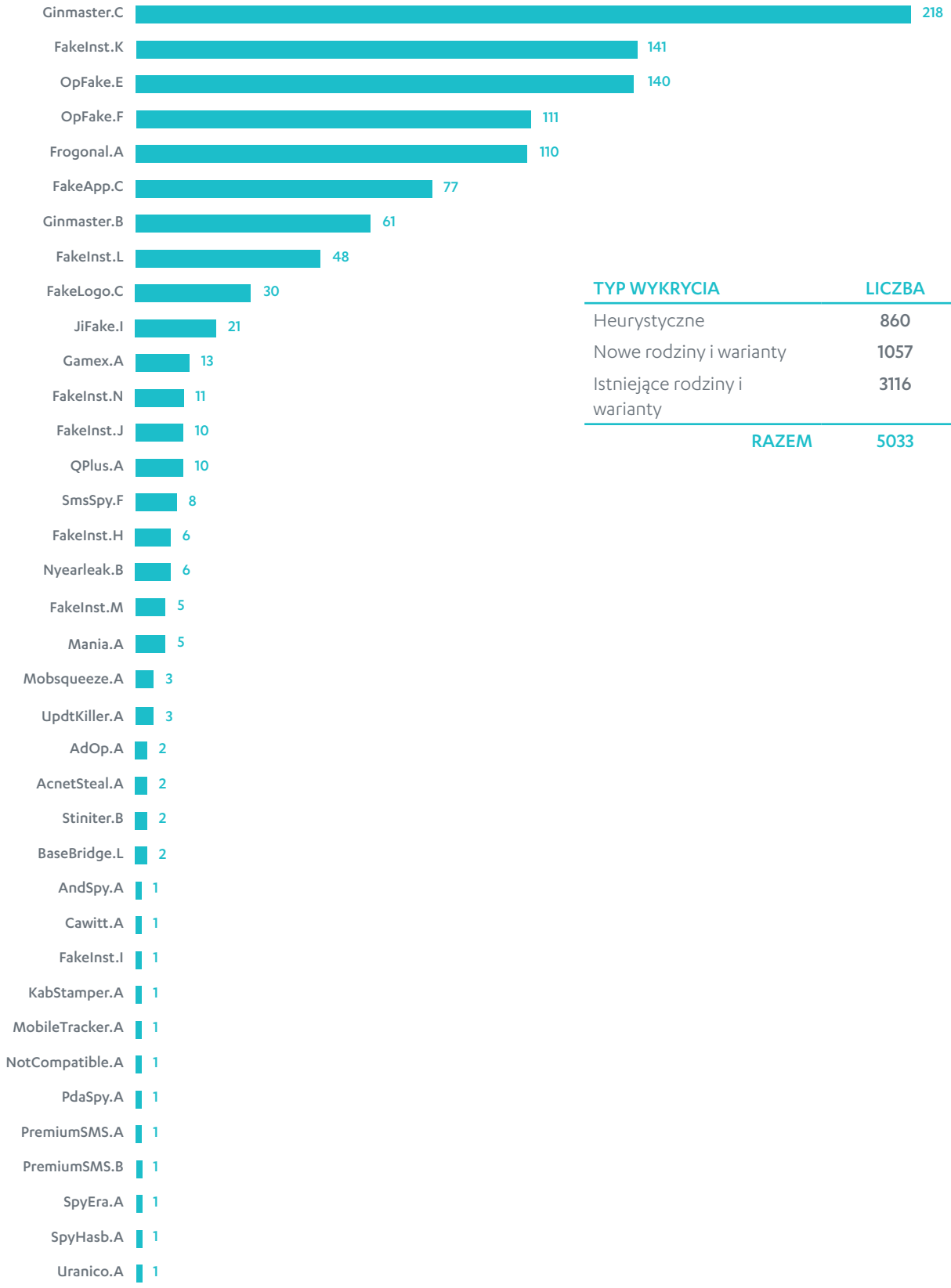
Trojan:SymbOS/RandomTrack.A

RandomTrack.A to trojan, który nie został stworzony w celach zarobkowych. Pobiera instalator ze zdalnego hosta i po cichu instaluje ten plik w zainfekowanym urządzeniu. Potrafi też przerywać procesy antywirusowe w celu uniknięcia wykrycia.

Nowe warianty znanych rodzin

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

- Trojan:Android/BaseBridge.L
- Trojan:Android/DroidKungFu.I
- Trojan:Android/FakeApp.C
- Trojan:Android/FakeInst.H, oraz warianty I, J, K, L, M and N
- Trojan:Android/FakeLogo.C
- Trojan:Android/Ginmaster.B, i wariant C
- Trojan:Android/JiFake.I
- Trojan:Android/Nyearleak.B
- Trojan:Android/OpFake.E, i wariant F
- Trojan:Android/SmsSpy.F (zob. opis na stronie 22)
- Trojan:Android/Stiniter.B
- Trojan:Android/Zsone.C
- Trojan:Symbian/AndroGamer.B, i wariant C
- Trojan:Symbian/FakeApp.C
- Trojan:Symbian/Melon.C
- Trojan:Symbian/Moporil.C
- Trojan:Symbian/SystemSync.B, oraz warianty C and D
- Trojan:Symbian/Yorservi.E



TYP WYKRYCIA	LICZBA
Heurystyczne	860
Nowe rodziny i warianty	1057
Istniejące rodziny i warianty	3116
RAZEM	5033

RYSUNEK 6. NOWE ZŁOŚLIWE OPROGRAMOWANIE DO ANDROIDA POSORTOWANE WEDŁUG LICZBY PRÓBEK, 2 KWARTAŁ 2012 R.

UWAGA: statystyki na rysunku 6 reprezentują liczbę unikatowych pakietów aplikacji Androida (APK).

TABELA 1. PRÓBKI ANDROIDA OTRZYMANE W 2 KWARTALE 2012 R.

30 NAJCZĘŚCIEJ WYKRYWANYCH ZŁOŚLIWYCH PROGRAMÓW

WYKRYCIE	LICZBA
Trojan:Android/Boxer.C	389
Trojan:Android/Ginmaster.C **	218
Trojan:Android/FakeInst.K **	141
Trojan:Android/OpFake.E **	140
Trojan:Android/OpFake.F **	111
Trojan:Android/Frogonal.A **	110
Trojan:Android/FakeInst.E	86
Trojan:Android/OpFake.C	77
Trojan:Android/Ginmaster.B **	61
Trojan:Android/Ginmaster.A	49
Trojan:Android/FakeInst.L **	48
Trojan:Android/Kituri.A	46
Trojan:Android/DroidKungFu.C	32
Trojan:Android/FakeLogo.C **	30
Trojan:Android/FakeInst.C	29
Trojan:Android/DroidKungFu.H	27
Trojan:Android/JiFake.I	21
Trojan:Android/BaseBridge.A	20
Trojan:Android/FakeBattScar.A	20
Trojan:Android/Bizimovie.A	16
Trojan:Android/Gamex.A **	13
Trojan:Android/Kmin.C	11
Trojan:Android/FakeInst.N **	11
Trojan:Android/JiFake.F	10
Trojan:Android/FakeInst.J **	10
Trojan:Android/SmsSpy.F **	8
Trojan:Android/SMStado.A	8
Trojan:Android/BaseBridge.B	7
Trojan:Android/DroidKungFu.F	6
Trojan:Android/FakeInst.H **	6

OPROGRAMOWANIE SZPIEGOWSKIE I RYZYKOWNE

WYKRYCIE	LICZBA
Adware:Android/Ropin.A	1617
Application:Android/Counterclank.A	545
Application:Android/FakeApp.C **	77
Spyware:Android/EWalls.A	14
Riskware:Android/QPlus.A **	10
Riskware:Android/Boxer.D	8
Application:Android/Nyearleak.B **	6
Exploit:Android/DroidRooter.B	4
Monitoring-Tool:Android/MobileSpy.C	3
Adware:Android/Mobsqueeze.A **	3
Application:Android/AdOp.A **	2
Hack-Tool:Android/TattooHack.A	2
Monitoring-Tool:Android/SpyBubble.B	1
Hack-Tool:Android/DroidRooter.M	1
Monitoring-Tool:Android/SpyHasb.A **	1
Exploit:Android/DroidDeluxe.A	1
Riskware:Android/MobileTX.A	1
Hack-Tool:Android/DroidRooter.A	1
Monitoring-Tool:Android/SpyEra.A **	1
Monitoring-Tool:Android/MobileMonitor.A	1
Monitoring-Tool:Android/Spyoo.A	1
Hack-Tool:Android/DroidRooter.B	1
Riskware:Android/GoManag.B	1
Monitoring-Tool:Android/MobileTracker.A **	1
Exploit:Android/DroidRooter.A	1
Monitoring-Tool:Android/PdaSpy.A **	1
Spyware:Android/SndApps.A	1
Monitoring-Tool:Android/AndSpy.A **	1
Monitoring-Tool:Android/CellShark.A	1

** New family or new variant discovered in Q2 2012

NOTE: statystyki w tabeli 1 reprezentują liczbę unikatowych pakietów aplikacji Androida (APK).

Ochrona niezastąpionego

Niniejszy dokument został poprzednio wydany w kontrolowanej dystrybucji i był przeznaczony tylko dla wybranych odbiorców.

Dokument został upubliczniony 6 sierpnia 2012 r.