RAPORT NA TEMAT ZAGROŻEŃ MOBILNYCH

1. KWARTAŁ 2012

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 naszym użytkownikom ochronę przed zagrożeniami czyhającymi w sieci. Całodobowa praca odbywa się na trzy zmiany: jedną w Helsinkach, a dwie w Kuala Lumpur. Personel Laboratoriów F-Secure w każdym momencie monitoruje światową sytuację w zakresie bezpieczeństwa, aby szybko i efektywnie radzić sobie z nagłymi epidemiami wirusów i złośliwego oprogramowania.

Ochrona przez całą dobę

Pracę Laboratoriów 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 od nas ciągłej czujności, by zagwarantować naszym klientom najwyższy z możliwych poziom ochrony.

STRESZCZENIE

TEN RAPORT OMAWIA KRAJOBRAZ ZAGROŻEŃ MOBILNYCH W PIERWSZYM KWARTALE 2012 ROKU I ZAWIERA DANE STATYSTYCZNE ORAZ SZCZEGÓŁOWE INFORMACJE NA TEMAT ZAGROŻEŃ, KTÓRE ZOSTAŁY W TYM OKRESIE ZAOBSERWOWANE I PRZENALIZOWANE PRZEZ LABORATORIA F-SECURE. DANE PREZENTOWANE W RAPORCIE OSTATNIO ZAKTUALIZOWANO 29 MARCA 2012 ROKU.

SPIS TREŚCI

ZMIANY W KRAJOBRAZIE ZAGROŻEŃ MOBILNYCH

Od czasu swojego debiutu system Android szybko zdobył znaczny udział w rynku mobilnym. Niestety, duża popularność (i inne czynniki) sprawiają, ze Android jest lukratywnym celem dla twórców złośliwego oprogramowania. Nowe rodziny i warianty złośliwego oprogramowania pojawiają się w każdym kwartale i nie widać żadnych oznak, by ten trend zwalniał. W pierwszym kwartale 2011 r. odkryto 10 nowych rodzin i wariantów. Rok później liczba ta wzrosła niemal czterokrotnie — tylko w pierwszym kwartale 2012 r. odkryto 37 nowych rodzin i wariantów (zob. rysunek 4 na stronie 18). Porównanie liczby złośliwych pakietów aplikacji Androida (APK) zidentyfikowanych w pierwszym kwartale 2011 i 2012 roku ujawnia bardziej szokujący fakt — wzrost liczby nowo wykrytych pakietów z 139 w I kw. 2011 do 3063 w I kw. 2012. Jest to spowodowane tym, że twórcy złośliwego oprogramowania modyfikują swoje zainfekowane aplikacje, aby uniknąć wykrycia sygnatur – elektronicznych podpisów – przez programy antywirusowe, rozpowszechniają złośliwe oprogramowanie pod różnymi nazwami i używają popularnych aplikacji (np. gier) do maskowania złośliwego działania.

„Porównanie liczby złośliwych pakietów aplikacji Androida (APK) zidentyfikowanych w pierwszym kwartale 2011 i 2012 roku ujawnia szokujący fakt — wzrost ich liczby ze 139 do 3063”.

Ze względu na stale zwiększające się tempo wzrostu liczby złośliwych programów na Androida, pojawia się potrzeba bardziej aktywnej ochrony użytkowników przed zagrożeniami. Dzięki wykorzystaniu technologii chmury, mechanizm heurystyczny wykorzystany w naszym nowym produkcie radził sobie dobrze z identyfikowaniem niesklasyfikowanych dotąd zagrożeń na podstawie złośliwego zachowania, a także z odkrywaniem nieznanych rodzin i wariantów złośliwego oprogramowania. Ważnym wydarzeniem w tym kwartale było odkrycie trojana FakeToken.A, który podszywa się pod generator tokenów dla aplikacji bankowości mobilnej. Początkowo został wykryty jako wariant FakeInst, ale okazuje się, że należy do nowej, choć spokrewnionej rodziny. Ponadto technologia heurystyczna odkryła Boxer.H - nowy wariant istniejącej rodziny Boxer, który podszywa się pod usługę Google Play.

W pierwszym kwartale 2012 r. twórcy złośliwego oprogramowania skupiają się na technikach unikania wykrycia oraz nowych metodach infekcji. Istniejące rodziny złośliwego oprogramowania, takie jak DroidKungFu, GinMaster i Fakeinst (do której należą podrodziny Boxer, JiFake, SMSTado, FakeNotify, oraz OpFake), zaczynają stosować techniki szyfrowania i randomizacji celem uniknięcia wykrycia. Jednocześnie niektóre złośliwe programy – na przykład FakeRegSMS – potrafią ukrywać swoje dane w pliku graficznym.

Do ważniejszych złośliwych programów odkrytych w tym kwartale należą program pobierający trojana Android/RootSmart.A oraz trojany Android/DroidKungFu.H i Android/Stiniter.A, które obrazują rosnącą złożoność ewolucji lub metod infekcji mobilnych zagrożeń. Na przykład RootSmart.A pobiera program wykorzystujący luki

DALEJ >>

zabezpieczeń celem przedostania się do jądra systemu zainfekowanego urządzenia, co pozwala mu zainstalować kolejne aplikacje. Zawiera też automatyczny mechanizm – bota, który może odbierać polecenia z serwera i wykonywać złośliwe czynności – takie jak nawiązywanie połączeń, wysyłanie SMS-ów premium oraz dostęp do płatnych filmów wideo – bez wiedzy użytkownika.

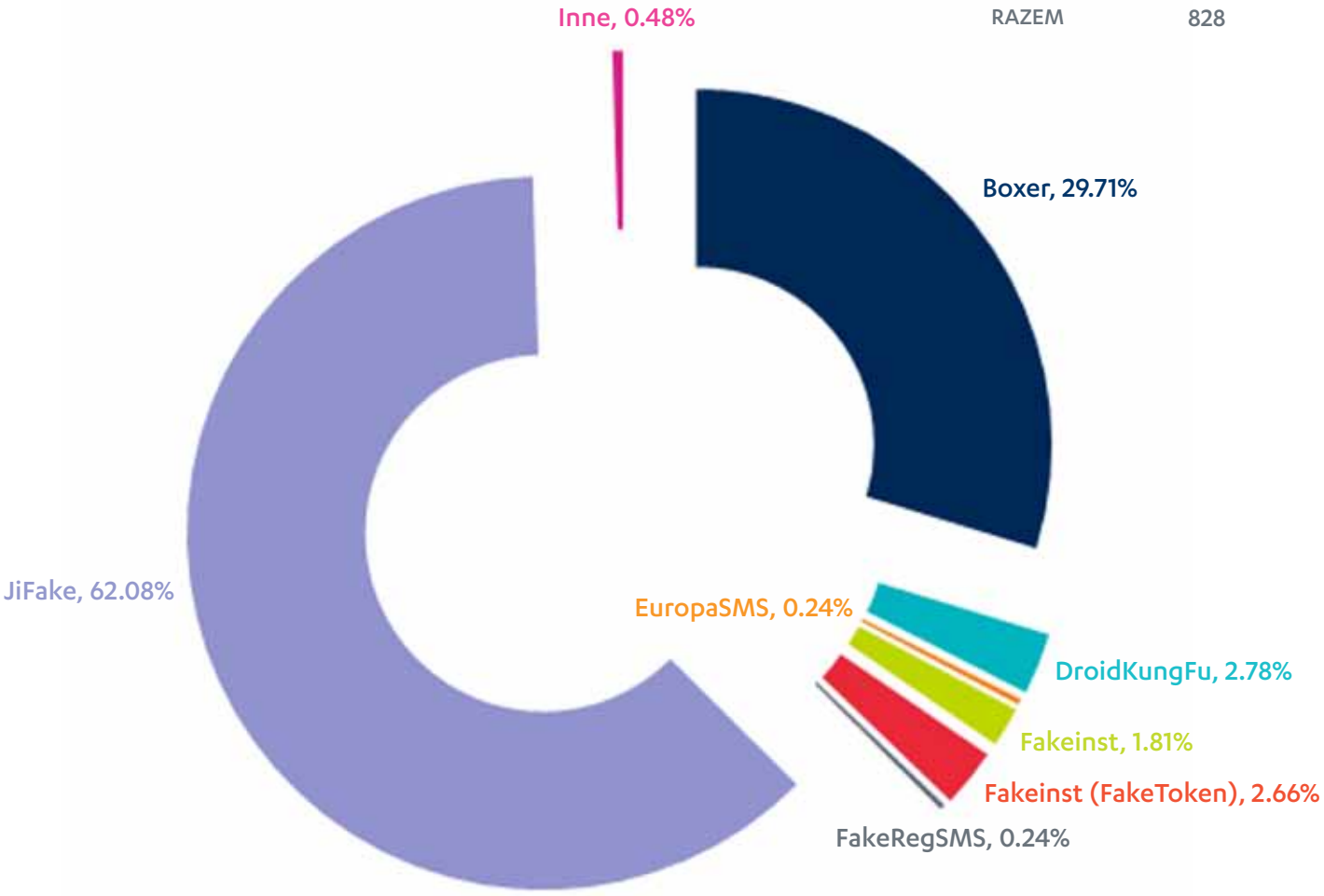
DroidKungFu.H wykorzystuje znacznie ulepszoną metodę infekcji. Obecnie potrzebuje tylko jednej usługi w zainfekowanej aplikacji, by umieścić w telefonie lub tablecie element pozwalający na przejęcie kontroli. Kiedy trojan zdobędzie przywileje użytkownika, może dokonywać zmian w systemie – na przykład skopiować się do folderu zawierającego kluczowe dla systemu pliki oraz zmienić konfigurację w taki sposób, aby umożliwić automatyczne uruchamianie zainfekowanego elementu podczas restartu. Dzięki tej metodzie trojana nie można usunąć w tradycyjny sposób, tzn. przez odinstalowanie aplikacji.

Kolejne nowo odkryte zagrożenie - Stiniter.A – stosuje inną, równie skomplikowaną technikę infekcji. Jest to złośliwy program złożony z wielu komponentów, który składa się z trzech zainstalowanych aplikacji oraz komponentu służącego do przejęcia kontroli nad systemem i instalowania kolejnych programów. Podobnie jak w przypadku DroidKungFu.H, komponent przejmujący kontrolę nad systemem nie wymaga dodatkowych mechanizmów dostępu do rdzenia systemu. Jeden z komponentów aplikacji może pełnić rolę samodzielnego złośliwego programu i zostać zainstalowany jako usługa, która zajmuje się gromadzeniem danych i wysyłaniem SMS-ów.

Sposób działania trzech wspomnianych wyżej programów (RootSmart.A, DroidKungFu.H i Stiniter.A) ukazuje, że złośliwe oprogramowanie tworzone na Androida skupia się obecnie na wykorzystaniu komponentu zagnieżdżającego się w jądrze systemu i pobiera dodatkowy element służący do zdobycia dodatkowych przywilejów tylko wtedy, gdy jest to konieczne. Nawet wtedy jest on jednak szybko usuwany, by zapobiec wykryciu przez produkty antywirusowe, nie rozpoznające jeszcze komponentu natywnego.

W ciągu roku złośliwe programy do Androida wykorzystywały coraz bardziej zawansowane techniki unikania wykrycia i ulepszone metody infekcji, jednak ich działania związane z generowaniem zysków zmieniły się bardzo nieznacznie. Większość złośliwego oprogramowania wykrytego w sklepach z aplikacjami na Androida zarabia poprzez wysyłanie SMS-ów na numery premium. Programy te zwykle znajdują się w sklepach z aplikacjami nieautoryzowanymi przez producentów, ale od czasu do czasu przedostają się również do oficjalnego serwisu Android Marketplace (teraz zintegrowanego z Google Play).

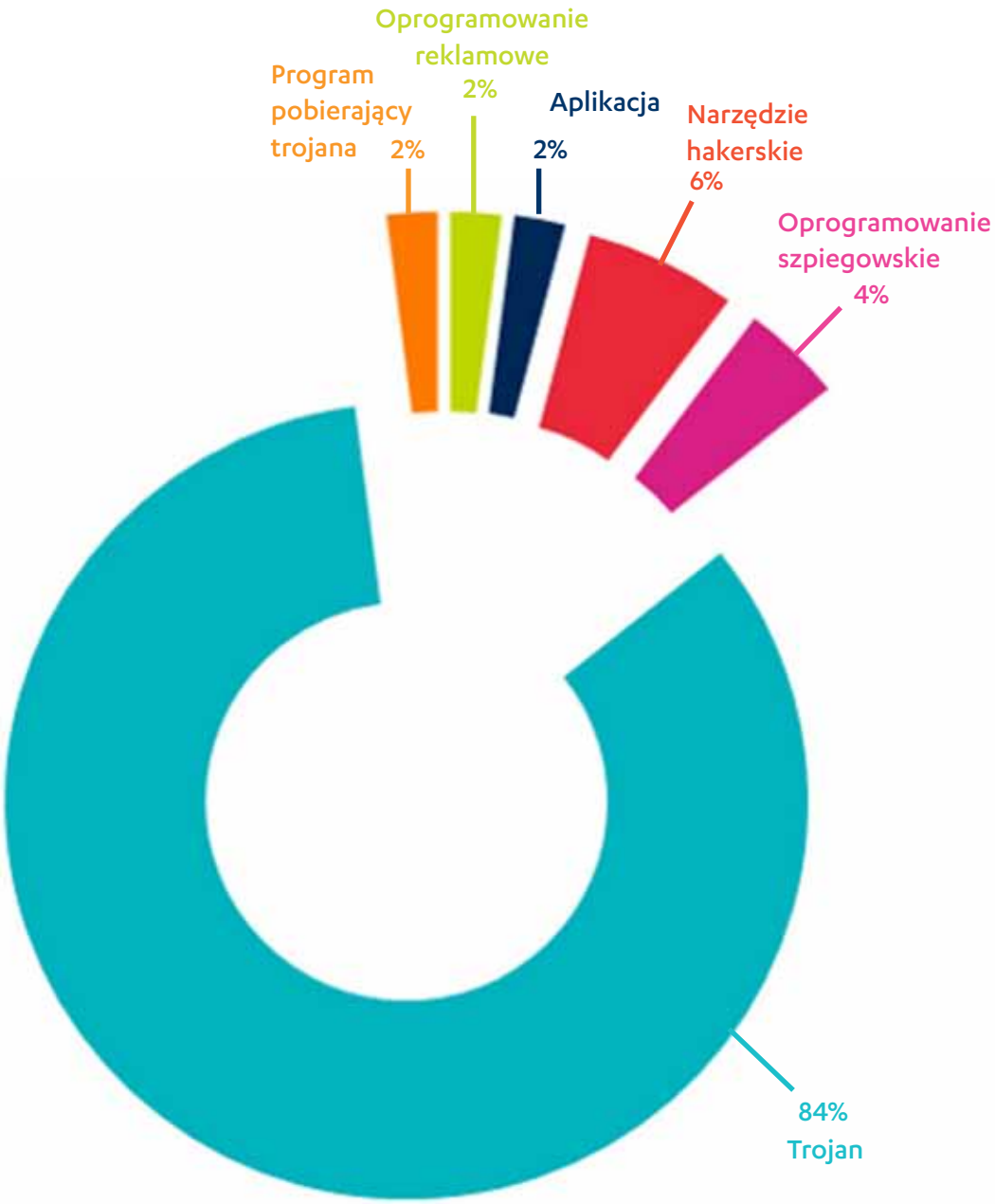
RODZINA	LICZBA
Boxer	246
DroidKungFu	23
EuropaSMS	2
Fakeinst	15
Fakeinst (FakeToken)	22
FakeRegSMS	2
JiFake	514
Inne	4
RAZEM	828



RYSUNEK 1. RODZINY ZŁOŚLIWEGO OPROGRAMOWANIA WYKRYTE METODAMI HEURYSTYCZNYMI, PIERWSZY KWARTAŁ 2012 ROKU

UWAGA: statystyki przedstawione na rysunku 1 reprezentują rodziny i warianty zagrożeń, a nie poszczególne zainfekowane pliki lub aplikacje. Jeśli na przykład dwie próbki wykryto jako trojan:android/ginmaster.A, liczy się je jako jedną.

NAJNOWSZE ZAGROŻENIA ODKRYTE W CIĄGU OSTATNICH TRZECH MIESIĘCY



RYSUNEK 2. ZAGROŻENIA MOBILNE WEDŁUG TYPU, PIERWSZY KWARTAŁ 2012 ROKU

UWAGA: statystyki przedstawione na rysunku 2 reprezentują rodziny i warianty zagrożeń, a nie poszczególne zainfekowane pliki lub aplikacje. Jeśli na przykład dwie próbki wykryto jako trojan:android/ginmaster.A, 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.

Aplikacja:Android/Counterclank.A

Counterclank.A To trojan, który podszywa się pod grę. Kiedy działa, gromadzi informacje z urządzenia, w którym został zainstalowany. Informacje te obejmują:

- **IMEI (International Mobile Equipment Identity)**
- **Numer telefonu**
- **Wersję systemu operacyjnego**

Trojan następnie łączy się ze zdalnym serwerem i przekazuje zebrane informacje.

Counterclank.A podszywa się pod grę

Aplikacja:Android/Steveware.A

Steveware.A Przyciąga użytkowników, oferując bezpłatne wersje próbne popularnych gier.

Podczas instalacji wyświetla komunikat, prosząc użytkownika o wprowadzenie adresu e-mail w celu odblokowania pełnej wersji. Komunikat brzmi następująco:

> **"Please click here to finish the installation process.**
> **To unlock the full version of this game for free, enter your email on the page and return to this application."**

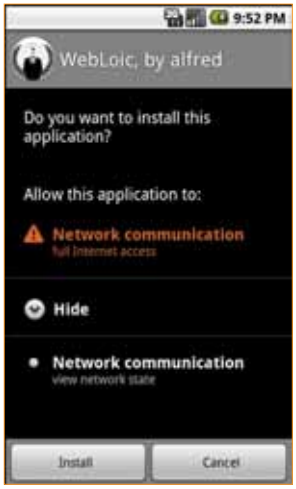
Komunikaty wyświetlane przez Steveware.A, proszące użytkowników o podanie adresu e-mail

Exploit:Android/DroidRooter.F

DroidRooter.F dostaje się do urządzenia za pośrednictwem innego programu; jest pobierany przez Trojan-Downloader:Android/RootSmart.A. Po instalacji przedostaje się do jądra systemu, co umożliwiają mu uruchamianie usług lub wykonywanie działań bez wiedzy użytkownika.

Narzędzie hakerskie:Android/LoicDos.A

Po instalacji LoicDos.A prosi o zezwolenie na „komunikację sieciową", które zapewnia mu pełny dostęp do Internetu w zainfekowanym urządzeniu.



LoicDos.A prosi o pełen dostęp do internetu

Po uruchomieniu łączy się z witryną internetową, która zawiera kod JavaScript do przeprowadzenia ataku blokady usług (DoS) na wybrany serwer.

LoicDos.A przygotowuje się do ataku DoS

Narzędzie hakerskie:Android/MemPoDroid.A

Jest to androidowa wersja niedawno opublikowanego exploitu „Mempodipper", który wpływa na nieandroidowe wersje jądra Linuksa.

MemPoDroid.A to plik wykonywalny Androida, który wykorzystuje lukę w zabezpieczeniach funkcji mem_write w jądrze wersji Android Linux 2.6.39 i nowszych. Ta wersja jądra Android Linux często znajduje się w nowszych modelach urządzeń, które działają w systemie Android 4.0 (Ice Cream Sandwich).

Udane przełamanie zabezpieczeń może umożliwić napastnikowi przejęcie kontroli nad urządzeniem i przeprowadzenie dowolnej operacji

UWAGA: dodatkowe informacje o exploicie Mempodipper można znaleźć w artykule „Linux Local Privilege Escalation via SUID /proc/pid/mem Write" (http://blog.zx2c4.com/749).

Narzędzie monitorujące:Android/AndroidAgent.A

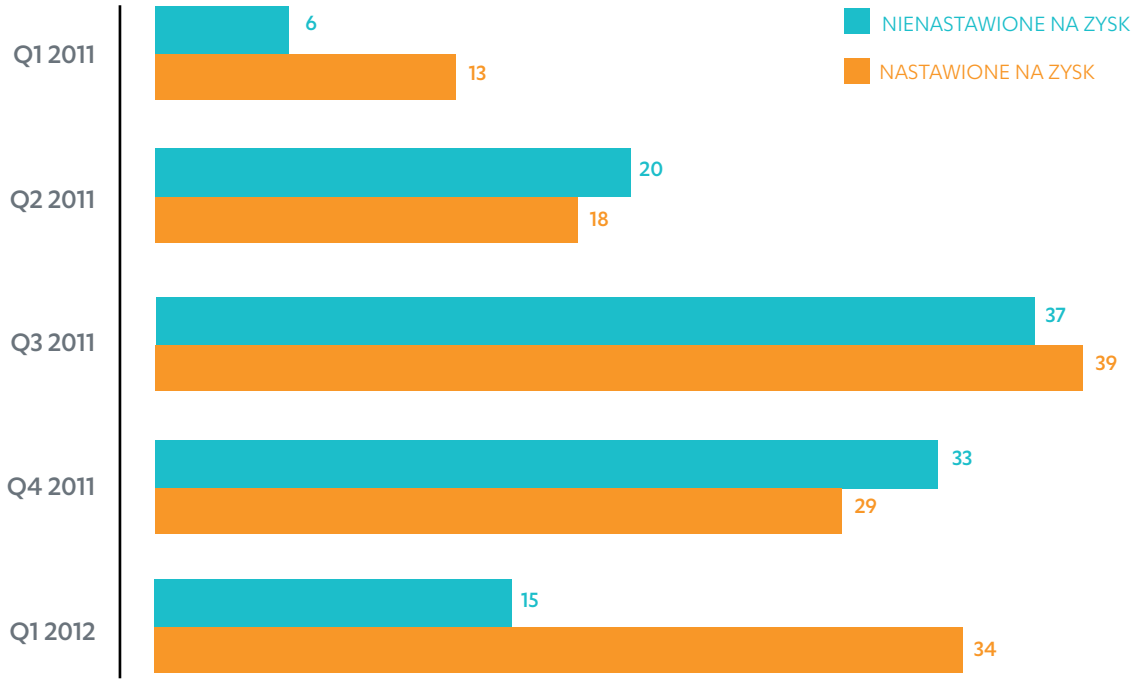
Podczas instalacji AndroidAgent.A prosi o przyznanie kilku zezwoleń, które pozwalają mu na dostęp do danych kontaktowych, wiadomości SMS, informacji o położeniu oraz połączenia internetowego w zainfekowanym urządzeniu.
Po instalacji program ukrywa swoją obecność, nie umieszczając żadnej ikony na ekranie głównym.

Zezwolenia, o które prosi AndroidAgent.A

AndroidAgent.A niepostrzeżenie dla użytkownika rejestruje wszystkie połączenia przychodzące i wychodzące oraz monitoruje przychodzące wiadomości SMS. Treść na początku tych wiadomości określa dalsze działania programu.

- **0# : Numer główny. Zapisać numer nadawcy i nadać mu przywileje administratora systemu.**
- **99# : Rejestracja shareware'u. Wykorzystać numer do zarejestrowania shareware'u.**
- **9# : Wysłać SMS z kodem IMEI i numerem seryjnym karty SIM na numer główny.**
- **18# : Zapisać ciąg występujący po znaku „#" jako nazwę użytkownika („UserName") i użyć jej w celu wysyłania zarejestrowanych plików do zdalnej lokalizacji.**
- **10# : Uruchomić usługę „MyPeopleService", która wysyła na numer główny SMS-y z informacjami kontaktowymi z książki telefonicznej.**
- **8# : Uruchomić usługę „MyLocationService", która wysyła na numer główny położenie urządzenia.**

Shareware: oprogramowanie oferowane w wersji próbnej o ograniczonej funkcjonalności lub dostępności.



RYSUNEK 3. ZAGROŻENIA MOBILNE MOTYWOWANE ZAROBKIEM WEDŁUG KWARTAŁU, 2011-2012 ROK

UWAGA: statystyki przedstawione na rysunku 3 reprezentują rodziny i warianty zagrożeń, a nie poszczególne zainfekowane pliki lub aplikacje. Jeśli na przykład dwie próbki wykryto jako Trojan:Android/GinMaster.A, liczy się je jako jedną.

Oprogramowanie szpiegowskie

PROGRAMY SKLASYFIKOWANE JAKO SZPIEGOWSKIE POTAJEMNIE GROMADZĄ INFORMACJE O ZWYCZAJACH UŻYTKOWNIKA, WYSZUKIWANYCH POJĘCIACH, PREFEROWANYCH WITRYNACH I APLIKACJACH. ZGROMADZONE INFORMACJE SĄ WYSYŁANE NA ZEWNĄTRZ ALBO PRZECHOWYWANE W ZAINFEKOWANYM URZĄDZENIU.

Program szpiegowski:Android/Adboo.A

Adboo.A to aplikacja, która pozwala użytkownikom wybrać gotową wiadomość z listy i wysłać ją do kontaktów. Wiadomości są podzielone na cztery kategorie: życzenia noworoczne, przyjaźń, miłość i żarty.

Adboo.A prezentuje listę wiadomości do wyboru

Kiedy użytkownik wybierze wiadomość, aplikacja wyświetla okno dialogowe z pytaniem o następną akcję: Kontakt, Edycja lub Anuluj. W przypadku wybrania opcji Kontakt próbuje odczytać zapisane dane kontaktowe. Prawdopodobnie musi wiedzieć, do kogo należy wysłać wiadomość.

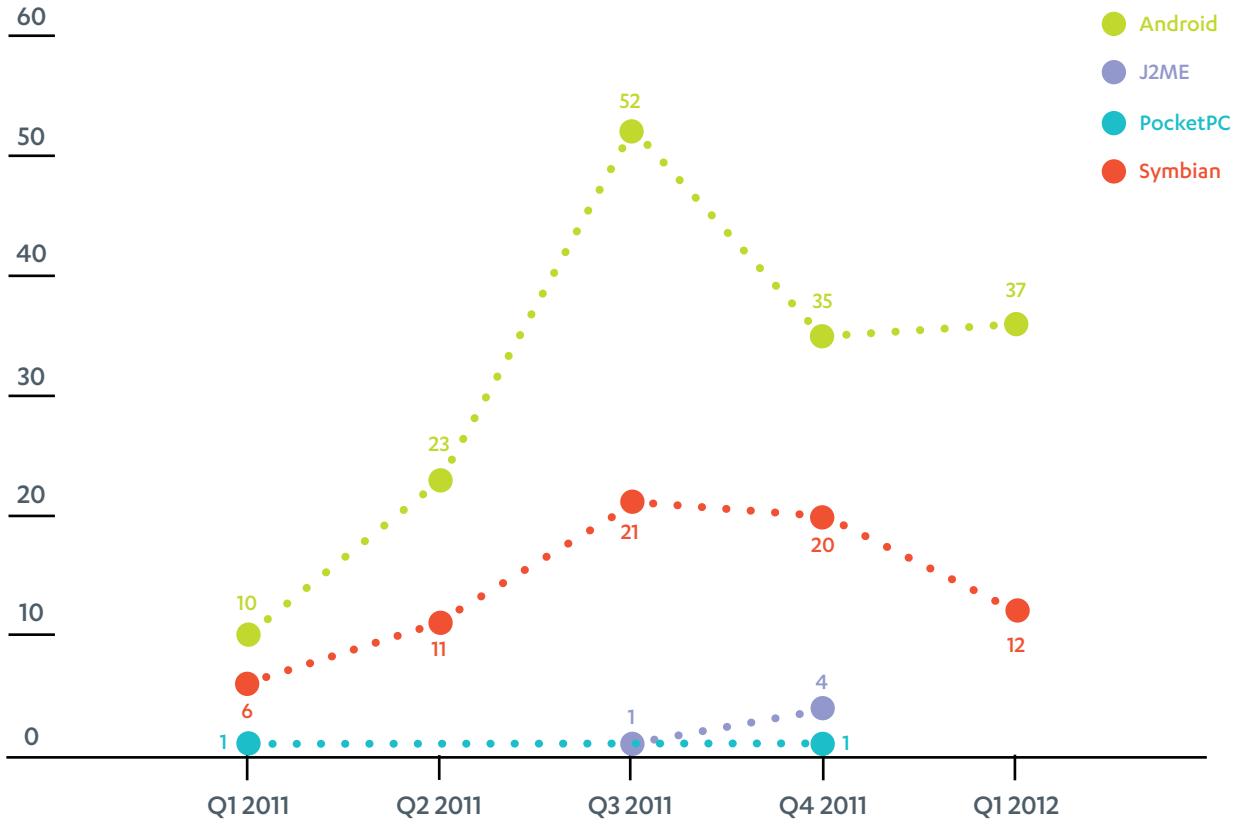
Jednak po uzyskaniu danych kontaktowych aplikacja wyświetla komunikat „Błąd wysyłania" i nie wysyła wiadomości do zamierzonego odbiorcy. Zamiast tego niepostrzeżenie dla użytkownika gromadzi następujące informacje o urządzeniu:

- **Model urządzenia**
- **Wersja systemu operacyjnego**
- **Numer telefonu**
- **Numer IMEI (International Mobile Equipment Identity)**

Informacje te są przekazywane do zdalnego serwera. Badanie certyfikatu Adboo.A pokazuje, że należy on do twórcy trojana Android/Zsone.A, który odkryto w drugim kwartale 2011 r.

POWIĄZANY WPIS NA BLOGU

Życzenia noworoczne – z przystawką w postaci gromadzenia danych
http://www.f-secure.com/weblog/archives/00002293.html



RYSUNEK 4. LICZBA NOWYCH RODZIN LUB WARIANTÓW WEDŁUG KWARTAŁU, 2011-2012 ROK

UWAGA: statystyki przedstawione na rysunku 4 reprezentują rodziny i warianty zagrożeń, a nie poszczególne zainfekowane pliki lub aplikacje. Jeśli na przykład dwie próbki wykryto jako Trojan:Android/GinMaster.A, liczy się je jako jedną.

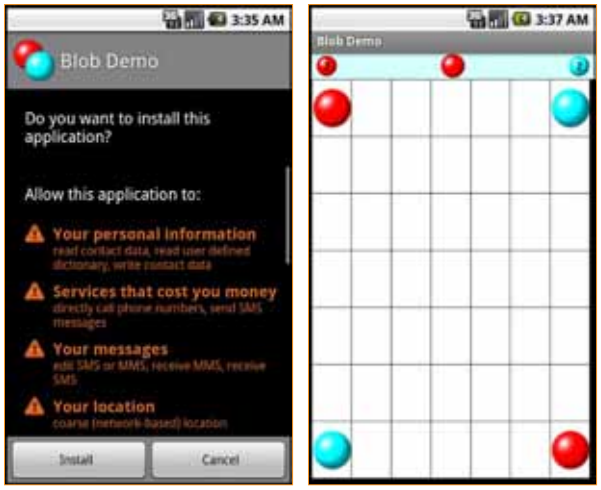
Złośliwe oprogramowanie

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

ZŁOŚLIWE OPERACJE WYKONYWANE PRZEZ TE PROGRAMY TO M.IN. INSTALACJA KOLEJNYCH PROGRAMÓW W UKRYCIU PRZED UŻYTKOWNIKIEM, TWORZENIE NOWYCH WARIANTÓW ZŁOŚLIWEGO KODU, USZKADZANIE LUB MODYFIKOWANIE DANYCH BEZ AUTORYZACJI, A TAKŻE KRADZIEŻ DANYCH ORAZ LOGINÓW I HASEŁ DOSTĘPU DO KONT W SERWISACH INTERNETOWYCH.

Trojan:Android/Binder.B

Podczas instalacji Binder.B prosi o przyznanie zezwoleń, które zapewniają mu dostęp do danych kontaktowych, wiadomości SMS i informacji o położeniu urządzenia.



Binder.B udaje aplikację o nazwie Blob Demo i prosi o przyznanie pewnych zezwoleń

Program gromadzi następujące informacje o urządzeniu:

- **Numer seryjny karty SIM**
- **Numer IMSI (International Mobile Subscriber Identity)**
- **Numer IMEI (International Mobile Equipment Identity)**
- **Numer telefonu**

Następnie łączy się ze zdalnym serwerem, z którego otrzymuje dalsze polecenia wykonania następujących operacji:

- **Wysłanie wiadomości SMS na pewien numer określoną ilość razy**
- **Pobranie pakietów APK z określonej witryny internetowej i instalacja ich w urządzeniu**

Oto aplikacje, które może instalować Binder.B:

- **com.taobao.mobile.dipei**
- **com.tencent.qqpimsecure**
- **com.renren.mobile.android**
- **com.kandian.hdtogoapp**
- **com.uc.browser**
- **com.tencent.mtt**

```
private void installAPK()
{
  copyAPK("android_dipei_1.4.0.apk");
  copyAPK("QQSecure2.0_(Android)_Build289(1).apk");
  copyAPK("Renren_Android_3.0.2.7.20110510.apk");
  copyAPK("KSHDToGo-v0.1.48-1.6-20110526_youyoucun3.apk");
  copyAPK("UCBrowser_V7.8.1.96_Android_pf139_bi800_(Build11060915).apk");
  copyAPK("QQBrowser2.0(Android)_Build0095_60058.apk");
  installApk("com.taobao.mobile.dipei", "android_dipei_1.4.0.apk");
  installApk("com.tencent.qqpimsecure", "QQSecure2.0_(Android)_Build289(1).apk");
  installApk("com.renren.mobile.android", "Renren_Android_3.0.2.7.20110510.apk");
  installApk("com.kandian.hdtogoapp", "KSHDToGo-v0.1.48-1.6-20110526_youyoucun3.apk");
  installApk("com.uc.browser", "UCBrowser_V7.8.1.96_Android_pf139_bi800_(Build11060915).apk");
  installApk("com.tencent.mtt", "QQBrowser2.0(Android)_Build0095_60058.apk");
}
```

Binder.B zaprogramowano do instalowania wybranych pakietów APK w urządzeniu

Każda wiadomość, która zawiera w treści poniższe słowa kluczowe, zostanie zablokowana:

- **83589523**
- **83589523**
- 客服电话 **(“Numer telefonu obsługi klienta”)**
- 元/条 **(“dolar/jedna wiadomość”)**
- 元/次 **(“dollar /raz”)**
- 本次1元 **(“jeden raz 1 dolar”)**
- 本次2元 **(“jeden raz 2 dolary”)**

Trojan:Android/Boxer.G

Boxer.G udaje instalator zwykłej aplikacji, ale w rzeczywistości jest trojanem wysyłającym SMS-y. Wysyła wiadomości SMS na numery premium i przynosi twórcom zyski z opłat naliczanych użytkownikowi urządzenia.

Oto numery premium, na które Boxer.G wysyła wiadomości SMS:

- **2855**
- **7151**
- **9151**

Trojan:Android/DroidDream.G, i wariant H

Podobnie jak poprzednie odmiany, warianty G i H trojana DroidDream gromadzą i wysyłają informacje o zainfekowanym urządzeniu do zdalnego serwera. Chodzi o następujące informacje:

- **IMEI number**
- **IMSI number**
- **Model urządzenia**
- **Informacje kontaktowe**
- **Wiadomości SMS ze skrzynki odbiorczej i nadawczej**

Trojany te mogą również wysyłać wiadomości SMS do każdego kontaktu zapisanego w urządzeniu oraz tworzyć w skrzynce odbiorczej wiadomości pozornie pochodzące od jednego z kontaktów.

Trojan:Android/FakeAngry.A

FakeAngry.A jest zawarty w złośliwym pakiecie „com.i22.angrybirds", który znajduje się w zainfekowanej aplikacji (com.katecca.screenofflock).

Program gromadzi informacje o zainfekowanym urządzeniu i wysyła je do zdalnej lokalizacji. Poniżej wymieniono informacje gromadzone przez FakeAngry.A:

- **Identyfikator urządzenia**
- **Numer IMEI**
- **Numer IMSI**
- **Wersja SDK**
- **Numer seryjny karty SIM**
- **Identyfikator abonenta**

POWIĄZANY WPIS NA BLOGU

Złośliwe oprogramowanie do Androida stosuje steganografię? Niezupełnie...
http://www.f-secure.com/weblog/archives/00002305.html

Trojan:Android/FakeRegSMS.A, i wariant B

Trojany FakeRegSMS to fałszywe instalatory, które nie umieszczają w urządzeniu żadnej rzeczywistej aplikacji, ale rejestrują użytkowników jako abonentów płatnych usług.

Podczas instalacji trojany proszą o zezwolenia, które umożliwiają następujące operacje:

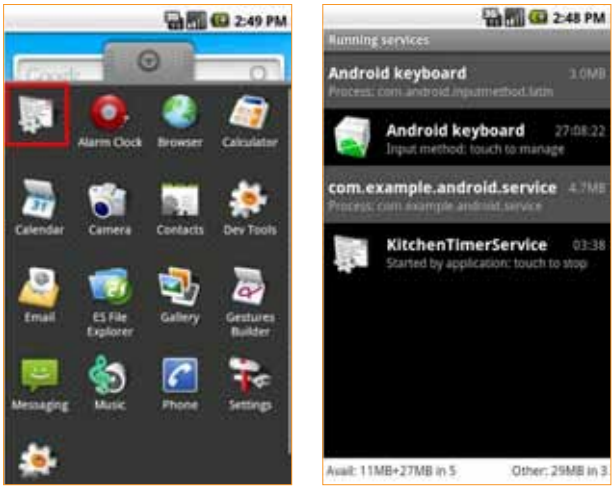
- **Modyfikowanie zawartości karty SD**
- **Wysyłanie wiadomości SMS**
- **Odczytywanie informacji o urządzeniu**

W drugim wariancie trojan wykorzystuje technikę pseudoszyfrującą, aby ukryć informacje w pliku graficznym PNG. Ten sam obrazek jest używany jako ikona widoczna w czasie instalacji i po jej zakończeniu.

Zezwolenia, o które prosi FakeRegSMS.B oraz ikona używana do ukrycia danych

Trojan:Android/FakeTimer.A

FakeTimer.A instaluje w urządzeniu usługę o nazwie „KitchenTimerService" i uzyskuje dostęp do witryny z treścią przeznaczoną dla osób dorosłych albo pornografią.



FakeTimer.A instaluje w urządzeniu usługę „KitchenTimerService"

Program pobiera następujące informacje, które są następnie przekazywane do zdalnego serwera:

- **Numer telefonu**
- **Identyfikator urządzenia**

mTAN: jednorazowy numer (token) generowany przez bank i wysyłany do urządzenia użytkownika w celu zweryfikowania transakcji online. Użytkownik musi wprowadzić ten numer, zanim sfinalizuje transakcję.

Trojan:Android/FakeToken.A

FakeToken.A udaje mobilny generator tokenów służących do potwierdzania transakcji mobilnych (Mobile Transaction Authentication Number, mTAN), np. przelewów, a w rzeczywistości służy do ich przechwytywania. Po zainstalowaniu przechwytuje wiadomości SMS i szuka numerów mTAN, które następnie przekazuje do zdalnej lokalizacji lub do wskazanego użytkownika.

FakeToken.A udaje generator tokenów

Trojan instaluje usługę, które może generować następujące komendy:

- SMS_RECEIVED w momencie odebrania wiadomości SMS
- PHONE_STATE w momencie wykrycia zmiany stanu urządzenia, na przykład przejścia od blokady lub stanu gotowości do trybu aktywnego
- BOOT_COMPLETED w momencie zakończenia rozruchu urządzenia

Program przechowuje też plik konfiguracyjny XML z informacjami o tym, gdzie należy wysyłać przechwycone wiadomości SMS.

```
<setingsSet>
    <catchSmsList class="java.util.ArrayList"/>
    <deleteSmsList class="java.util.ArrayList"/>
    <number>79021121067</number>
    <version>1.0</version>
    <smsPrefix>santander</smsPrefix>
    <sendSmsResultList class="java.util.ArrayList"/>
    <serverList class="java.util.ArrayList">
        <string>http://[redacted]hop.ru/[redacted].php</string>
        <string>http://[redacted]best.com/[redacted].php</string>
    </serverList>
    <serverPrefix>qe4faf23r4e2</serverPrefix>
    <sid>sid_1</sid>
    <period>43200</period>
    <timeConnection>1334662815611</timeConnection>
    <sendInitSms>false</sendInitSms>
</settingsSet>
```

Plik konfiguracyjny XML z informacjami dotyczącymi wysyłania wiadomości SMS

Ponadto trojan może wysyłać następujące informacje do zdalnej lokalizacji:

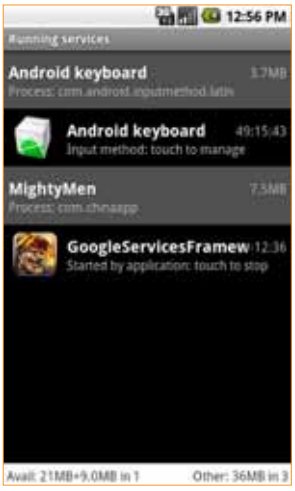
- Numer IMEI
- Numer IMSI
- Model urządzenia
- Numer telefonu
- Kod SID (System Identification Number)

Trojan:Android/FakeUpdates.A

Po instalacji Trojan FakeUpdates.A niepostrzeżenie dla użytkownika uruchamia w tle usługę o nazwie „GoogleServicesFramework".

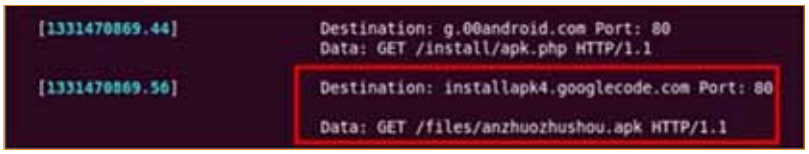
Usługa łączy się ze zdalnym serwerem i wysyła następujące informacje:

- Numer IMEI
- Numer IMSI
- Wersja systemu operacyjnego
- Model urządzenia



FakeUpdates.A niewidocznie dla użytkownika uruchamia usługę „GoogleServicesFramework"

Trojan deszyfruje też adresy stron internetowych przechowywane w innej zdalnej lokalizacji, z której pobiera listę aplikacji. Aplikacje te są później pobierane i zapisywane w folderze pobranych plików na karcie SD.



FakeUpdates.A próbuje pobrać aplikację z listy

Pobrane aplikacje są zapisywane w folderze pobranych plików na karcie SD

Trojan:Android/FakeVoice.A

FakeVoice.A to trojan, który promuje się jako aplikacja zmieniająca barwę głosu przeznaczona dla użytkowników z Izraela. Po uruchomieniu zadaje następujące pytania:

- Pod jaki numer chcesz zadzwonić?
- Jak ma brzmieć Twój głos?
  - » Niski i groźny
  - » Zwykły
  - » Wysoki i zabawny

Usługa ma kosztować 6 NIS za minutę. Podczas połączenia użytkownik może nacisnąć „9”, aby zmienić głos na wyższy, albo „8”, aby zmienić go na niższy.

NIS: nowa szekla izraelska, waluta Izraela

Oprócz tej płatnej usługi FakeVoice.A nawiązuje połączenie z 01240900720674, numerem premium w Rumunii..

FakeVoice.A proszący użytkownika o wprowadzenie numeru i wybranie barwy głosu

Trojan:Android/Kituri.A

Po uruchomieniu Kituri.A wyświetla „umowę użytkownika", aby odciągnąć uwagę od podejrzanych działań wykonywanych w tle.

Trojan wysyła numer IMEI urządzenia do zdalnego serwera. Łączy się również ze zdalną lokalizacją, aby pobrać listę numerów premium, na które będzie wysyłać SMS-y.

Kituri.A wyświetla „umowę użytkownika"

CYTAT KWARTAŁU

JEDNYM Z NAJBARDZIEJ INTERESUJĄCYCH TRENDÓW ZWIĄZANYCH ZE ZŁOŚLIWYM OPROGRAMOWANIEM MOBILNYM, JAKI POJAWIŁ SIĘ W NIEDAWNYCH MIESIĄCACH, JEST ROSNĄCA LICZBA TROJANÓW „SPEŁNIAJĄCYCH OBIETNICE". W PRZESZŁOŚCI WIĘKSZOŚĆ MOBILNYCH TROJANÓW NASTAWIONYCH NA ZYSK WYŚWIETLAŁA KOMUNIKAT O BŁĘDZIE I PRÓBOWAŁA PRZEKONAĆ UŻYTKOWNIKA TELEFONU, ŻE INSTALACJA TAK ZWANEJ „BEZPŁATNEJ PRZEGLĄDARKI" (ZWYKLE PRZEZNACZONEJ DO SYSTEMU SYMBIAN LUB WINDOWS MOBILE) NIE POWIODŁA SIĘ. WIELU UŻYTKOWNIKÓW POSZUKIWAŁO INFORMACJI NA TEMAT TEGO KOMUNIKATU W INTERNECIE, PONIEWAŻ NABIERALI PODEJRZEŃ ALBO CHCIELI ROZWIĄZAĆ PROBLEM. DZIĘKI TEMU CZĘSTO ODKRYWALI, ŻE KOMUNIKAT JEST FAŁSZYWY, A ICH TELEFON PADŁ OFIARĄ ATAKU.

OBECNIE POJAWIAJĄ SIĘ ZŁOŚLIWE APLIKACJE NA ANDROIDA, DO KTÓRYCH DOŁĄCZONE SĄ NIEZAINFEKOWANE PROGRAMY, TAKIE JAK GRA ANGRY BIRDS IN SPACE FIRMY ROVIO. NAJPIERW ZŁOŚLIWA „NAKŁADKA" PODSTĘPNIE NAKŁANIA UŻYTKOWNIKA DO PRZYZNANIA UPRAWNIEŃ, KTÓRE UMOŻLIWIAJĄ TROJANOWI ABONOWANIE PŁATNYCH USŁUG. ALE PÓŹNIEJ... ZŁOŚLIWY PROGRAM RZECZYWIŚCIE INSTALUJE DZIAŁAJĄCĄ KOPIĘ GRY. NIE MA ŻADNEGO ZNAKU BUDZĄCEGO POWAŻNIEJSZE WĄTPLIWOŚCI, ANI ŻADNYCH PROBLEMÓW DO ROZWIĄZANIA. UŻYTKOWNIK OTRZYMUJE GRĘ, KTÓRĄ MU OBIECANO.

W TEJ SYTUACJI TRUDNO JEST POWIEDZIEĆ, ILE CZASU ZAJMIE UŻYTKOWNIKOM ODKRYCIE, ŻE PADLI OFIARĄ OSZUSTA.

> "OBECNIE POJAWIAJĄ SIĘ ZŁOŚLIWE APLIKACJE NA ANDROIDA, DO KTÓRYCH DOŁĄCZONE SĄ NIEZAINFEKOWANE PROGRAMY, TAKIE JAK GRA ANGRY BIRDS IN SPACE FIRMY ROVIO"

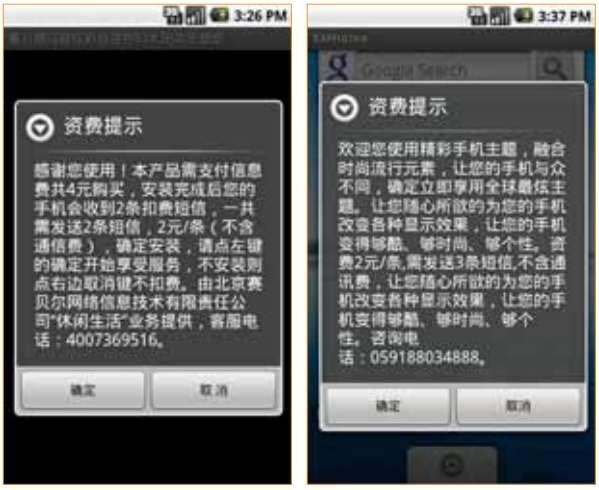
-SEAN SULLIVAN,

GŁÓWNY DORADCA DS. BEZPIECZEŃSTWA, LABORATORIA F-SECURE

@FSLabsAdvisor

Trojan:Android/Kmin.B, i wariant C

Po uruchomieniu trojany Kmin wyświetlają komunikat z pytaniem, czy użytkownik chce zainstalować aplikację, która doliczałaby pewne opłaty do jego rachunku.



Kmin.B i Kmin.C pytające użytkownika, czy chce zainstalować płatną aplikację

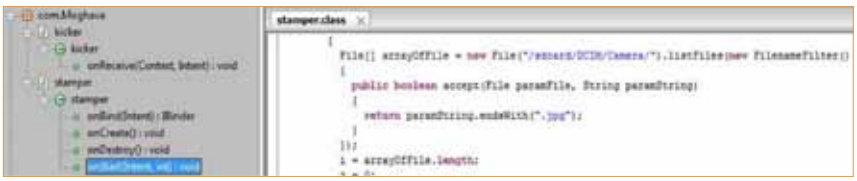
Jeśli nawet użytkownik odmówi zainstalowania aplikacji, trojan mimo to wykonuje jedno z poniższych złośliwych działań:

- **Wysyłanie numeru IMEI i numeru telefonu do zdalnego serwera**
- **Wysyłanie wiadomości SMS na numer premium, 10669500718**
- **Pobieranie i instalowanie innej aplikacji**
- **Uruchamianie usług w tle**

Trojan:Android/Moghava.A

Moghava.A to zainfekowana aplikacja, która pojawiała się w nieautoryzowanych sklepach. W przeciwieństwie do większości złośliwego oprogramowania na Androida nie napisano jej z myślą o zysku, ale ośmieszeniu przeciwników politycznych.

Złośliwe działanie Moghava.A rozpoczyna się po rozruchu urządzenia i trwa przez określony czas. W czasie rozruchu uruchamiana jest usługa o nazwie „stamper" (ang. pieczątka). Usługa ta czeka pięć minut, a następnie zaczyna wyszukiwać pliki JPEG przechowywane na karcie pamięci, zwłaszcza w folderze /sdcard/DCIM/Camera/, gdzie przechowywane są zdjęcia zrobione aparatem urządzenia.



Moghava.A wyszukuje pliki JPEG w folderze /sdcard/DCIM/Camera

W przypadku każdego znalezionego pliku program nakłada na zdjęcia inny obraz, swoistą „pieczątkę". Procedura ta jest powtarzana co pięć minut, co powoduje zwiększenie rozmiaru plików graficznych i zużycie wolnego miejsca na karcie pamięci.

Poniżej pokazano przykładowy obraz przed i po modyfikacji:

Zdjęcie przed (po lewej) i po nałożeniu obrazu (po prawej)

Trojan:Android/Nyearleak.A

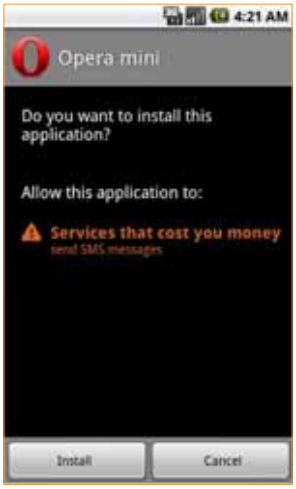
Nyearleak.A to trojan, który udaje aplikację do wyświetlania tapety z motywem Nowego Roku 2012, a zarazem potajemnie gromadzi i wysyła następujące informacje o urządzeniu:

- Identyfikator urządzenia
- Konto Google
- Adres e-mail
- Zainstalowane pakiety

Nyearleak.A udaje noworoczną tapetę

Trojan:Android/OpFake.D

Trojan OpFake został początkowo odkryty w urządzeniach Symbian i Windows Mobile, ale teraz trafił również na platformę Android.



OpFake.D proszący o zezwolenie na wysyłanie SMS-ów

Podobnie jak jego odpowiedniki na innych platformach, Opfake.D podszywa się pod miniaplikację do przeglądarki Opera. Podczas instalacji prosi tylko o zezwolenie na wysyłanie SMS-ów.

Po uruchomieniu OpFake.D wysyła SMS-y na określone numery. Treść wiadomości i numery telefonu są przechowywane w zakodowanym pliku o nazwie „config.xml", ale można je zdekodować algorytmem base64.

```
[Sent SMS]
----------
        Number: 2332
        Message: 5+656tm-339-a43
        Number: 7250
        Message: 5+656tm-339-a43
        Number: 7099
        Message: 5+656tm-339-a43
```

Treść wiadomości SMS i numer odbiorcy

POWIĄZANY WPIS NA BLOGU

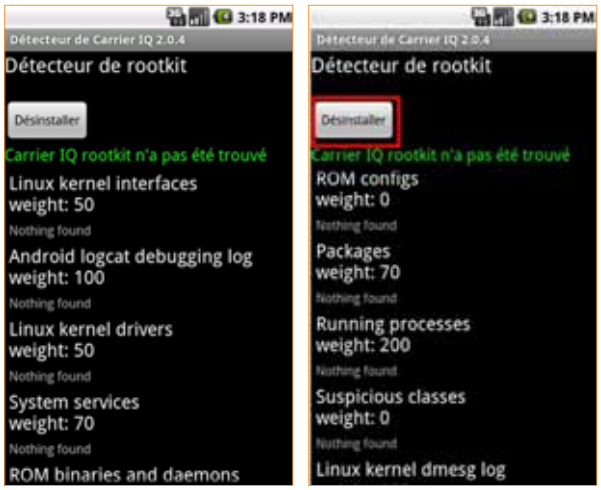
Trojan:Android/OpFake.D nadal koduje swój plik konfiguracyjny
http://www.f-secure.com/weblog/archives/00002306.html

Trojan:Android/Qicsomos.A

Qicsomos.A promuje się jako aplikacja o nazwie „Détecteur de Carrier IQ", co po francusku oznacza „Detektor Carrier IQ". Rzekomo ma wykrywać i usuwać z urządzenia kontrowersyjną aplikację Carrier IQ.

W 2011 r. aplikacja Carrier IQ budziła obawy wśród badaczy zabezpieczeń i zwolenników piractwa, ponieważ miała być potajemnie instalowana przez operatorów telekomunikacyjnych na urządzeniach klientów w celu gromadzenia informacji, m.in. o używanych danych i lokalizacji użytkownika.

Trojan Qicsomos.A wykorzystuje te obawy, aby skłonić użytkowników do zainstalowania go.

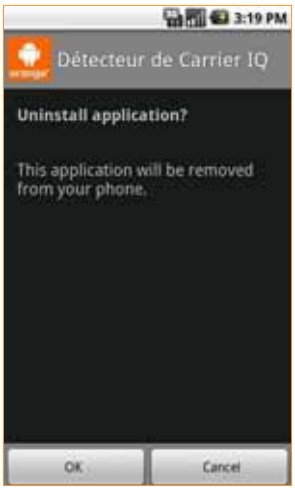


Qicsomos.A wyświetla przycisk „Desinstaller" (Odinstaluj)

Kiedy użytkownik kliknie przycisk „Désinstaller" (Odinstaluj), program wysyła na numer 81168 cztery SMS-y o następującej treści:

- AT37
- MC49
- SP99
- SP93

Następnie program prosi o zezwolenie na odinstalowanie się.



Qicsomos. prosi o zezwolenie na odinstalowanie się.

UWAGA: Dodatkowe informacje w artykule: "Carrier IQ: czym jest, czym nie jest i co powinieneś o nim wiedzieć (http://www.engadget.com/2011/12/01/carrier-iq-what-it-is-what-it-isnt-and-what-you-need-to/)

Trojan:Android/RuFailedSMS.A

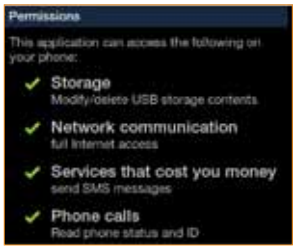
Trojan RuFailedSMS.A, znaleziony w nieautoryzowanych sklepach z aplikacjami na Androida wymierzony jest w użytkowników w Rosji, Białorusi, Kazachstanie i Azerbejdżanie. Udaje instalatory różnych aplikacji, z których część wymieniono poniżej:

- Add_It_Up
- Advanced_Launcher_Lite
- AmazingMaze_supLitesup
- Analog_Clock_Collection
- Animal_Sudoku
- AnySoftKeyboard
- AnySoftKeyboard_Slovak_Language_Pack
- AppInventor_Toggle
- Arrow_Caz
- Astronomical_Flashlight
- BentoCam!
- Bimaru_-_Battleship_Sudoku
- BlackJack
- Carve_a_Pumpkin_supLitesup
- Chinese_Chess
- Christmas_Ringtones
- Coloring_pages
- Contact_Finder_supLitesup
- Converter
- Countdown_Widget

POWIĄZANY WPIS NA BLOGU

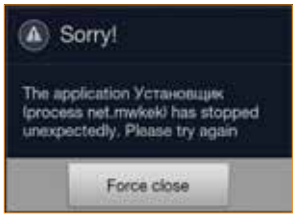
Niedziałający trojan do wysyłania SMS-ów premium w Androidzie
http://www.f-secure.com/weblog/archives/00002289.html

- Crayon_Ball
- Cyan_aHome_Theme



Zezwolenia, o które prosi RuFailedSMS.A

Po instalacji RuFailedSMS.A prosi o zezwolenia, które umożliwiłyby mu m.in. dostęp do Internetu i wysyłanie wiadomości SMS. Został zaprojektowany z myślą o czerpaniu zysków z SMS-ów wysyłanych na numery premium, ale ze względu na usterkę w kodzie nie przeprowadza swojej złośliwej procedury.



RuFailedSMS.A nie wykonuje swojej procedury i zawiesza się

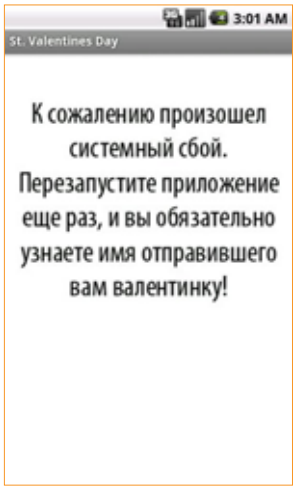
Trojan:Android/Saiva.A

Trojan Saiva.A odkryto w Dniu Św. Walentego. To kolejny złośliwy program, który czerpie zyski z wysyłania wiadomości SMS. Po uruchomieniu wyświetla fałszywy pasek postępu.

Saiva.A wyświetla fałszywy pasek postępu.

Program udaje, że pobiera dane, a w rzeczywistości wysyła SMS-y o treści „rb9816" na numer „5370". Następnie wyświetla po rosyjsku komunikat o rzekomym błędzie systemu. Komunikat ten, przetłumaczony na polski, brzmi następująco:

> **„Niestety, wystąpił błąd systemu. Ponownie uruchom aplikację, a poznasz imię osoby, która wysłała Ci walentynkę".**



Komunikat o błędzie wyświetlany przez Saiva.A

Trojan:Android/SMSFisher.A

SMSFisher.A zawiera złośliwy pakiet o nazwie „fish". Kiedy zostanie uruchomiony, po cichu wysyła wiadomości SMS bez zgody użytkownika. Aby zatrzeć za sobą ślady, trojan blokuje powiadomienia o opłatach za SMS-y, anulując wysyłanie wiadomości, które zawierają ciąg znaków „+86" albo „10".

Trojan:Android/SMSHandler.A

SMSHandler.A znajduje się w pakiecie o nazwie „com.google.smshandler". Podczas instalacji prosi o zezwolenie na dostęp do wiadomości SMS, połączeń telefonicznych i zawartości pamięci.

Po instalacji program nie umieszcza żadnej ikony na ekranie, aby nie wzbudzać podejrzeń użytkownika. SMS-y wysyłane są w momencie ponownego uruchamiania urządzenia.

Zezwolenia, o które prosi SMSHandler.A

Trojan:Android/SMSLoader.A

SMSLoader.A ma postać aplikacji o nazwie „Fail_Android". Po uruchomieniu wyświetla pasek postępu oraz komunikat, który można przetłumaczyć jako:

„Uwaga! Proszę zaczekać na pobranie pliku..."

Fałszywy pasek postępu i komunikat wyświetlany przez SMSLoader.A

Trojan ten niepostrzeżenie wysyła wiadomości SMS o treści „5+125 7-14-654-13233359428100" na następujące numery premium:

- 5373
- 7250
- 7099

TABELA 1. STATYSTYKI ZAGROŻEŃ MOBILNYCH WEDŁUG PLATFORMY, 2004-2011 ROK

	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL
Android							9	120	129
iOS						2			2
J2ME			2		2	7	2	5	18
PocketPC	1		1	2	7	8	19	2	40
Symbian	24	124	188	44	19	21	50	58	528
	25	124	191	46	28	38	80	185	717

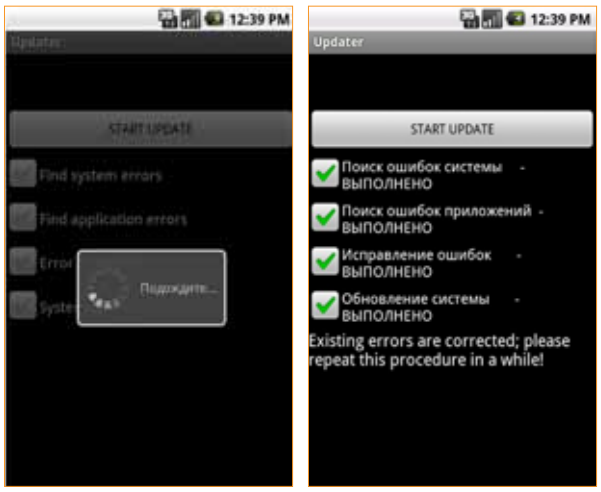
TABELA 2. STATYSTYKI ZAGROŻEŃ MOBILNYCH WEDŁUG TYPU, 2004-2011 ROK

	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL
Oprogramowanie reklamowe									-
Aplikacja								5	5
Furtka							3		3
Śmieci			8						8
Narzędzie hakerskie							4	8	12
Narzędzie monitorujące							1	15	16
Ryzykowne oprogramowanie			1		1	8	1	10	21
Oprogramowanie szpiegowskie			5	15	6		2	5	33
Trojan	11	105	160	23	13	24	47	141	524
Program pobierający trojana								1	1
Wirus	14	19	17	6					56
Robak				2	8	6	22		38
	25	124	191	46	28	38	80	185	717

UWAGA: statystyki przedstawione w tabelach 1 i 2 reprezentują rodziny i warianty zagrożeń, a nie poszczególne zainfekowane pliki lub aplikacje. Jeśli na przykład dwie próbki wykryto jako Trojan:Android/GinMaster.A, liczy się je jako jedną.

Trojan:Android/SMStealer.A

SMStealer.A udaje „aktualizator", rzekomo lokalizujący i poprawiający błędy w systemie oraz aplikacjach urządzenia.



SMStealer.A pozoruje lokalizowanie i poprawianie błędów w systemie

Jednak jego rzeczywiste działanie polega na łączeniu się ze zdalną lokalizacją i wysyłaniu następujących informacji:

- Numer IMEI
- Identyfikator urządzenia i operator
- Wiadomości SMS w skrzynce odbiorczej i nadawczej

Trojan:Android/SpyService.A

Po instalacji SpyService.A nie umieszcza żadnej ikony na ekranie głównym, aby ukryć swoją obecność przed użytkownikiem. Potajemnie wysyła następujące informacje z zainfekowanego urządzenia:

- Numer IMEI
- Numer IMSI
- Numer seryjny karty SIM
- Numer telefonu
- Model urządzenia
- Operator sieci
- Wiadomości SMS

Program pobierający trojana:Android/RootSmart.A

RootSmart.A podaje się za '系统快捷设置' (szybkie ustawienia systemu).

RootSmart.A zamaskowany jako „szybkie ustawienia systemu"

Po uruchomieniu łączy się z serwerem dowodzenia (C&C) i przekazuje mu następujące informacje:

- **Numer IMEI**
- **Numer IMSI**
- **Wersja systemu operacyjnego**
- **Nazwa pakietu**

Następnie łączy się ze zdalną lokalizacją, aby pobrać kod GingerBreak niezbędny do zdobycia uprawnień administratora w zainfekowanym urządzeniu. RootSmart.A pobiera z tej lokalizacji plik o nazwie „shells.zip", który zawiera trzy komponenty:

- **Exploit – kod GingerBreak (wykrywany jako Exploit:Android/Droidrooter.F)**
- **Skrypt Install – skrypt bash, który instaluje powłokę administratora w katalogu systemowym**
- **Skrypt Installapp – skrypt bash, który instaluje inne złośliwe aplikacje.**

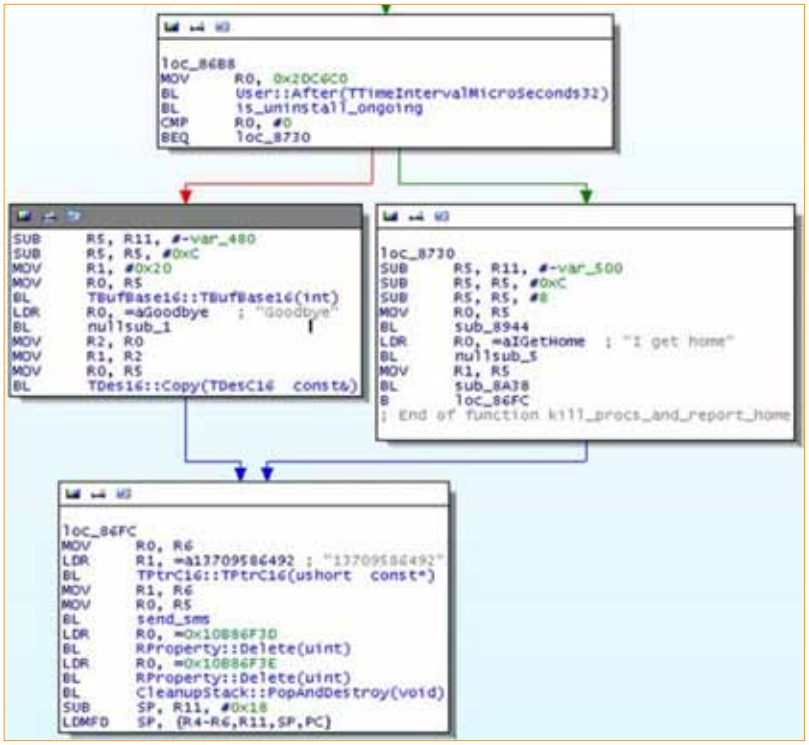
Ponadto trojan pobiera inne złośliwe aplikacje z serwera dowodzenia i niepostrzeżenie dla użytkownika instaluje je w zainfekowanym urządzeniu.

UWAGA: więcej informacji o exploicie GingerBreak znajduje się w artykule „Android Botnet Exploits Gingerbread Root Access" (http://www.informationweek.com/news/security/mobile/232600576)

Trojan:SymbOS/Farewell.A

Farewell.A zaprogramowano tak, aby przerywał działanie programów rozpoznanych jako produkty producentów oprogramowania antywirusowego. Po zainstalowaniu umieszcza w systemie plik binarny, który wysyła wiadomość SMS o treści „I get home" na numer „13709586492". Podczas deinstalacji działanie pliku binarnego jest wykonywane podobnie, tym razem z przesłaniem wiadomości „Goodbye" na ten sam numer.

Instalator Farewell.A zawiera również polecenie wywołujące kolejne działanie podczas rozruchu urządzenia – pobieranie konfiguracji ze zdalnego serwera i wysyłanie wiadomości SMS. Dalsze połączenia sieciowe są nawiązywane za pośrednictwem zwykłego stosu HTTP i „surowych" gniazd TCP. Jednak z jakiejś przyczyny – jeśli urządzenie jest zablokowane – każdy proces ze znakami „360" w nazwie jest przerywany przed nawiązaniem połączenia.



Farewell.A mówi „Goodbye"

Trojan:SymbOS/SivCaller.A

SivCaller.A to trojan, który pobiera nowe komponenty i instaluje je w zainfekowanym urządzeniu bez wiedzy użytkownika. Po uruchomieniu głównego pliku wykonywalnego przerywa procesy należące do produktów antywirusowych. Modyfikuje również zakładki w przeglądarce internetowej i przechwytuje przychodzące wiadomości SMS, zanim trafią do skrzynki odbiorczej.

```
LDR     R1, =aVtelwd    ; "*vtelwd*"
MOV     R0, R9
BL      TPtrC16::TPtrC16(ushort const*)
MOV     R0, R8
MOV     R1, R9
BL      kill_matching_procs
LDR     R1, =aAnxin     ; "Anxin*"
MOV     R0, R9
BL      TPtrC16::TPtrC16(ushort const*)
MOV     R0, R8
MOV     R1, R9
BL      kill_matching_procs
LDR     R1, =aQh        ; "Qh*"
MOV     R0, R9
BL      TPtrC16::TPtrC16(ushort const*)
MOV     R0, R8
MOV     R1, R9
BL      kill_matching_procs
LDR     R1, =a360       ; "*360*"
MOV     R0, R9
BL      TPtrC16::TPtrC16(ushort const*)
MOV     R0, R8
MOV     R1, R9
BL      kill_matching_procs
LDR     R1, =aAgile     ; "*Agile*"
MOV     R0, R9
BL      TPtrC16::TPtrC16(ushort const*)
MOV     R0, R8
MOV     R1, R9
BL      kill_matching_procs
LDR     R1, =aAgj       ; "Agj*"
MOV     R0, R9
BL      TPtrC16::TPtrC16(ushort const*)
MOV     R1, R9
MOV     R0, R8
BL      kill_matching_procs
ADD     R0, R8, #0xC
BL      create_smsengine
STR     R0, [R8,#0x20]
BL      start_sms_listener
MOV     R1, #1
BL      nullsub_31
BL      create_smshandler
STR     R0, [R8,#0x1C]
BL      create_downloadmanager
```

SivCaller.A zaprogramowano tak, aby przerywał procesy należące do produktów antywirusowych

Trojan:SymbOS/SilentPusher.A

SilentPusher.A to trojan, który wysyła i monitoruje wiadomości SMS. Aby ukryć operacje wysyłania SMS-ów, blokuje wyświetlanie powiadomień o wysłaniu wiadomości. W tym celu zmienia dzwonek SMS na bezgłośny plik MP3 dołączony do pakietu instalacyjnego oraz przerywa działanie usługi powiadamiania (ncnlist.exe).

```
.text:00010AE6                  MOVS    R0, R6
.text:00010AE8                  BLX     RProcess::SecureId(void)
.text:00010AEC                  LDR     R3, =0x100058F1 ; ncnlist.exe
.text:00010AEE                  MOVS    R5, #0
.text:00010AF0                  CMP     R0, R3
.text:00010AF2                  BEQ     loc_10B26
```

SilentPusher.A przerywa działanie usługi powiadamiania, aby zablokować powiadomienia o wysłaniu wiadomości

```
LDR     R0, =aCSystemDataSms ; "c:\\system\\data\\smsring\\sms4_ring.mp3"
BL      nullsub_2
MOVS    R3, R0
MOVS    R1, R3
MOVS    R0, R7
BL      swap_sms_ringtone
B       loc_86C8
```

SilentPusher.A zmienia dzwonek SMS na bezgłośny plik MP3

Operacja blokowania powiadomień jest jednak wykonywana tylko wtedy, kiedy SilentPusher.A czeka na własne wiadomości, prawdopodobnie potwierdzenia z usług premium. Zwykły tryb powiadomień jest następnie przywracany.

Oprócz wysyłania SMS-ów SilentPusher.A przerywa procesy, które należą do produktów antywirusowych, gromadzi numery IMEI i IMSI oraz kontaktuje się z różnymi zdalnymi serwerami przez połączenie internetowe.

```
LDR     R1, =aAgilemoncon ; "AgileMonCon"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
LDR     R1, =aAgileserver ; "AgileServer"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
LDR     R1, =aQh360keeper ; "Qh360Keeper"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
LDR     R1, =aQh360safesvr ; "Qh360SafeSvr"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
LDR     R1, =aMcleanerserver ; "MCleanerServer"
MOV     R0, SP
BLX     TPtrC16::TPtrC16(ushort  const*)
MOVS    R0, R5
MOV     R1, SP
BL      kill_matching_processes
```

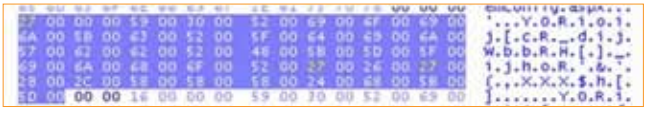
SilentPusher.A zaprogramowano tak, aby przerywał procesy należące do produktów antywirusowych.

Trojan:SymbOS/Yorservi.A, oraz wariant B i D

Pierwszy wariant, Yorservi.A, łączy się z kilkoma zdalnym hostami z wykorzystaniem „surowych" gniazd TCP. Następnie po cichu pobiera i instaluje kilka komponentów bez zgody użytkownika urządzenia.

Drugi wariant, Yorservi.B, zawiera funkcję związaną z deinstalacją. W przypadku próby usunięcia go z urządzenia natychmiast przerywa proces deinstalacji. Inne jego możliwości to m.in. monitorowanie połączeń, odczytywanie dzienników połączeń oraz odczytywanie i wysyłanie wiadomości SMS.

Yorservi.D, kolejny wariant, zaprogramowano tak, aby przerywał działanie usługi pliku „connmon.exe", a przez to uniemożliwiał użytkownikowi zauważenie nowo utworzonych połączeń sieciowych. Trojan ma zakodowany plik konfiguracyjny z listą unikatowych identyfikatorów (UID). Wariant ten uruchamia także potajemnie nowe procesy oraz pobiera i instaluje oprogramowanie.



Zakodowana nazwa pliku w Yorservi.D

Zakodowana konfiguracja (Yorservi.D)

Zdekodowana konfiguracja (Yorservi.D)

Trojan:SymbOS/Zhaomiao

Trojany z rodziny Zhaomiao są w obiegu od zeszłego roku, ale niedawne analizy ujawniły, że niektóre warianty używają podobnych kluczy do deszyfrowania swoich plików konfiguracyjnych.

Fast-flux: technika nadużywania systemu nazw domenowych (DNS) w celu ochrony adresu IP przed identyfikacją. Często używana przez cyberprzestępców, którzy chcą uniknąć wykrycia.

Próbki z rodziny Zhaomiao zawierają zaszyfrowany plik konfiguracyjny; można go odszyfrować za pomocą klucza DES „DDH#X%LT”, który jest zapisany „na sztywno” w złośliwym kodzie bajtowym. Odszyfrowany plik ujawnia listę witryn fast-flux.

Zaszyfrowany plik konfiguracyjny w próbkach Zhaomiao

Odszyfrowany plik z listą witryn

Ten sam klucz odkryto w kilku próbkach, które są wykrywane jako Trojan:SymbOS/Zhaomiao.E. Jednakże Zhaomiao.B używa tego klucza również do deszyfrowania lokalnego pliku konfiguracyjnego.

Zaszyfrowany plik konfiguracyjny znaleziony w innych próbkach Zhaomiao

Odszyfrowany plik z listą witryn

Rodzina Zhaomiao często używa również innego klucza DES, „DOW#MD%D". W jednym przypadku był on używany do odszyfrowania lokalnego pliku konfiguracyjnego.

Zaszyfrowany plik konfiguracyjny znaleziony w innych próbkach Zhaomiao

Plik odszyfrowany za pomocą podobnego klucza DES

W tej samej próbce na Symbiana, klucz użyty do rozszyfrowania danych konfiguracyjnych jest podobny do klucza używanego przez trojana Android/DroidDream.B. W próbce na Symbiana, klucz rozszyfrowuje dane konfiguracyjne pobrane ze zdalnej lokalizacji, natomiast w przypadku DroidDream.B jest on użyty do rozszyfrowania lokalnego pliku konfiguracji.

```
; Attributes: bp-based frame

update_config

plaintext_storage= -0x28
ciphertext_tptr= -0x24
context_obj= -0x10

MOV     R12, SP
STMFD   SP!, {R11,R12,LR,PC}
SUB     R11, R12, #4
SUB     SP, SP, #0x20
STR     R0, [R11,#-0x10] ; store and load context object
LDR     R3, [R11,#-0x10]
LDR     R3, [R3,#0x10]
SUB     R0, R11, #-ciphertext_tptr8
LDR     R1, [R3,#0x18]  ; get ciphertext buffer from context
BL      HBufC8::Des(void)
LDR     R0, =aDDmxLt_6  ; "DDmMxLt"
BL      prep_key
SUB     R3, R11, #-ciphertext_tptr8
MOV     R1, R3
BL      des_decrypt
STR     R0, [R11,#plaintext_storage]
LDR     R0, [R11,#plaintext_storage]
BL      CleanupStack::PushL(void *)
LDR     R3, [R11,#context_obj]
LDR     R3, [R3,#0x10]
LDR     R0, [R3,#0x10]
BL      combine_plaintext
LDR     R3, [R11,#context_obj]
LDR     R0, [R3,#0x20]
LDR     R1, [R11,#plaintext_storage]
BL      parse_xml
LDR     R0, [R11,#plaintext_storage]
BL      cleanupstack_popanddestroy
LDR     R0, [R11,#context_obj]
BL      save_config
SUB     SP, R11, #0xC
LDMFD   SP, {R11,SP,PC}
; End of function update_config
```

Związek odkryty między Zhaomiao a DroidDream.B

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.

- Trojan:Android/Boxer.H
- Trojan:Android/DroidDream.G
- Trojan:Android/DroidKungFu.H
- Trojan:Android/Fakeinst.E, oraz wariant F iG

TABELA 3. LICZBA WYKRYĆ W PRÓBKACH ANDROIDA OTRZYMANYCH W PIERWSZYM KWARTALE 2012 ROKU

WYKRYTY PROGRAM	LICZBA
Heurystyka	828
Aplikacja:Android/Counterclank.A	9
Aplikacja:Android/Steveware.A	21
Exploit:Android/DroidRooter.F	1
Narzędzie hakerskie:Android/LoicDos.A	1
Narzędzie hakerskie:Android/MemPoDroid.A	2
Narzędzie monitorujące:Android/AndroidAgent.A	2
Program szpiegowski:Android/Adboo.A	1
Trojan:Android/Binder.B	115
Trojan:Android/Boxer.G	14
Trojan:Android/Boxer.H	15
Trojan:Android/DroidDream.G	10
Trojan:Android/DroidKungFu.H	2
Trojan:Android/FakeAngry.A	1
Trojan:Android/FakeNotify.A **	256
Trojan:Android/FakeNotify.B **	12
Trojan:Android/FakeRegSMS.A	11
Trojan:Android/FakeRegSMS.B	6
Trojan:Android/FakeTimer.A	28
Trojan:Android/FakeUpdates.A	22
Trojan:Android/FakeVoice.A	1
Trojan:Android/Fakeinst.E	97
Trojan:Android/Fakeinst.F	51
Trojan:Android/Fakeinst.G	21
Trojan:Android/Kituri.A	24
Trojan:Android/Kmin.C	1
Trojan:Android/Moghava.A	1
Trojan:Android/Nyearleak.A	2
Trojan:Android/OpFake.D	4
Trojan:Android/Qicsomos.A	1
Trojan:Android/RuFailedSMS.A	145
Trojan:Android/Saiva.A	4
Trojan:Android/SMSFisher.A	69
Trojan:Android/SMSHandler.A	1
Trojan:Android/SMSLoader.A	1
Trojan:Android/SMStealer.A	1
Trojan:Android/SpyService.A	3
Trojan:Android/Stiniter.A	4
Program pobierający trojana:Android/RootSmart.A	33

* Ten wariant został odkryty pod koniec czwartego kwartału 2011 r.

RYSUNEK 5. OTRZYMANE PRÓBKI ANDROIDA W PIERWSZYM KWARTALE 2012 ROKU, POSORTOWANE WEDŁUG LICZBY WYKRYĆ

Chronimy to, co dla Ciebie ważne

Dokument został upubliczniony 11 maja 2012 r.

F-Secure