



G Data  
**Mobile MalwareReport**

Halbjahresbericht  
Januar – Juni 2013

G Data SecurityLabs

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

# Inhalt

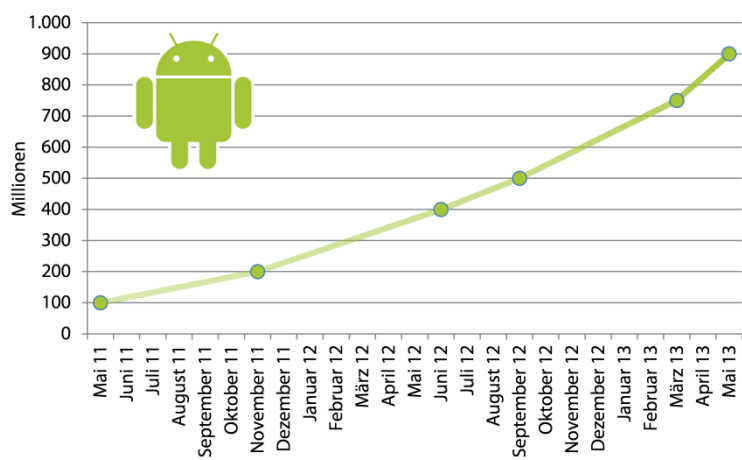
<b>Auf einen Blick.....</b>	<b>2</b>
<b>Android: Wachstum auf ganzer Linie .....</b>	<b>3</b>
<b>Android-Schadcode weiter auf dem Vormarsch.....</b>	<b>4</b>
<b>AndroRAT und Malware-Kits.....</b>	<b>6</b>
<b>Malware-Steckbriefe.....</b>	<b>8</b>
Android.Backdoor.AndroRAT.A .....	8
Android.Backdoor.Obad.A.....	9
Android.Trojan.FakeSite.A, alias Perkele.....	10
<b>Trends .....</b>	<b>11</b>

## Auf einen Blick

- ✦ Das Android Betriebssystem ist Angriffsziel Nummer 1 im Bereich Mobile.
- ✦ Inzwischen wurden über 900 Millionen Android Mobilgeräte aktiviert.
- ✦ Marktforscher sehen ein jährliches Wachstum des Smartphone-Segments von 33%.
- ✦ Prognosen zufolge werden im Jahr 2015 auf 20% der Smartphones und Tablet-PCs Sicherheitslösungen installiert sein.
  
- ✦ Die Anzahl neuer Mobile Malware-Samples ist im ersten Halbjahr 2013 rasant gestiegen – es waren 519.095 neue Schaddateien, gegenüber 185.210 neuen in H2 2012.
- ✦ Durchschnittlich erreichten die G Data SecurityLabs also täglich 2.868 neue Schaddateien!
  
- ✦ Malware Toolkits machen es auch unerfahrenen Angreifern einfach, Schadsoftware zu erstellen.
- ✦ Der Einsatz von Mobile Malware Toolkits wird die Anzahl neuer Malware auch in den nächsten Monaten weiter stark ansteigen lassen.
- ✦ Die Experten der G Data SecurityLabs rechnen damit, dass sich die Zahl neuer Android-Schadprogramme im nächsten Halbjahr voraussichtlich verdreifachen wird.
  
- ✦ Android.Backdoor.Obad.A nutzt gleich drei Sicherheitslücken aus, um Angriffe auf Android-Mobilgeräte durchzuführen.
- ✦ Der Trojaner FakeSite.A, alias Perkele, machte von sich reden, da er mit beliebigem Schadcode kombiniert werden kann, der Web-Inject Angriffe im Browser ausführt. Somit ist er ein flexibler, relativ einfach zu erstellender Cross-Plattform-Trojaner.
- ✦ Ein im Universitätskontext erstelltes, legitimes, Fernzugriffs-Tool namens „AndroRAT“ wurde von Cyberkriminellen missbraucht und für ihre böartigen Zwecke umgeschrieben.
  
- ✦ Einige neue Schädlinge versuchen sich den automatisierten und manuellen Analysen zu entziehen und werden mit kompliziert verschleiertem Programmcode ausgestattet.
- ✦ Das schnelle Geld als Motivation für Angriffe ist noch immer dominant. Jedoch werden durch neue Backdoor-Angriffe auch längerfristig angelegte und komplexere Angriffe ausgeführt.

## Android: Wachstum auf ganzer Linie

Längst sind die Zeiten vorbei, in denen Schadcode für Mobilgeräte wie Smartphones und Tablet-PCs eine Randerscheinung war. Die stetig wachsenden Absatzzahlen der Geräte tragen dazu bei, dass Cyber-Kriminelle nicht nur auf die Plattform aufmerksam wurden, sondern sie inzwischen als lohnenswertes Angriffsziel definiert haben. Ihr Fokus liegt hier unbestritten auf dem Betriebssystem Android, das inzwischen auf über 900 Millionen aktivierten Geräten<sup>1</sup> im Einsatz ist. Marktforscher erwarten weiter steigende Absatzzahlen im Smartphone-Segment (+33% pro Jahr), was mitunter am sinkenden Durchschnittspreis der Alleskönner liegen soll: Kostete ein solches Mobilgerät 2011 noch 443\$ (etwa 337€), so stehen im Jahr 2013 statistisch 372\$ (etwa 283€) zu Buche und im Jahr 2017 sollen die Preise auf 309\$ (etwa 235€) sinken.<sup>2</sup>



**Abbildung 1:** Anzahl der aktivierten Android-Geräte.

In Folge der Popularität entwickelte sich nach und nach eine breit gefächerte ökonomische Struktur rund um Angriffe auf die smarten Mobilgeräte, wobei bis heute das Hauptmotiv für Attacken monetäre Gründe sind. Aufwand und Ertrag stehen in einem lohnenswerten Verhältnis. Malware-Autoren erstellen Schadcode und nutzen diesen für Angriffe, verkaufen ihn aber auch häufig in zwielichtigen Online-Märkten. Gehandelt werden auch Entwickler-Accounts, die im offiziellen App Markt von Google (Google Play) registriert und verifiziert sind.<sup>3</sup> Schädliche Apps jeglicher Art in Google Play anzubieten birgt selbstverständlich weitaus größere Verbreitungschancen für die Angreifer und so werden die Accounts, die für 25\$ (etwa 19€) angemeldet werden können, dann für 100\$ (etwa 76€) gehandelt. Selbstverständlich sind auch Gmail Accounts beliebte Beute, vor allem, wenn sie Zugang zum Android-Mobilgerät und damit allen persönlichen Daten und dazu noch Einkaufsmöglichkeiten verschaffen. Es gibt inzwischen Audit Tools, die den Wert des eigenen Gmail Accounts ermitteln können.<sup>4</sup>

Toolkits sind eine noch nicht allzu verbreitete Technik im Mobil-Bereich, die es Angreifern erlaubt, Malware mit nur wenigen Vorkenntnissen und einigen Mausklicks binnen kürzester Zeit zu erstellen. Diese Toolkits sind Werkzeuge, um Schadcode nach dem Baukastenprinzip zu erstellen. Damit steigt einerseits die Qualität des Schadcodes durch fertig programmierte und getestete Schadroutinen, aber vor allem die Quantität infizierter Apps. Besonders stechen dabei die bei Angreifern beliebten und bewährten Trojanischen Pferde hervor und hier die Familie Android.Fakelinstaller, wie auf Seite 4 beschrieben wird.

<sup>1</sup> <http://venturebeat.com/2013/05/15/900m-android-activations-to-date-google-says/>

<sup>2</sup> <http://www.idc.com/getdoc.jsp?containerId=prUS24143513>

<sup>3</sup> <http://krebsonsecurity.com/2013/03/mobile-malcoders-pay-to-google-play/>

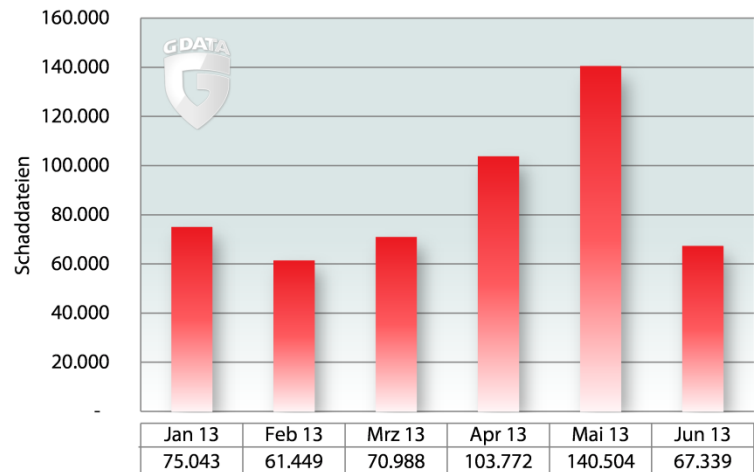
<sup>4</sup> <https://cloudsweeper.cs.uic.edu/>

## Android-Schadcode weiter auf dem Vormarsch

Die Zählung der Android-Malware basiert auf der Auswertung der Anzahl neuer Malware. In den G Data SecurityLabs wurden im ersten Halbjahr 2013 insgesamt 519.095 neue Schaddateien<sup>5</sup> erkannt. Das bedeutet eine Steigerung um 180% gegenüber dem zweiten Halbjahr 2012 (185.210<sup>6</sup>) und einem Wachstum um mehr als das Sechzehnfache gegenüber dem ersten Halbjahr 2012 (29.595<sup>6</sup>).

Durchschnittlich erreichten die G Data SecurityLabs also täglich 2.868 neue Schaddateien!

Die einzelnen Dateien kann man anhand von Eigenschaften des Schadcodes<sup>7</sup> bestimmten Familien zuordnen. 275.398 der neuen Schaddateien konnten eindeutig zu Malware-Familien klassifiziert werden<sup>8</sup>, wie in Abbildung 3 dargestellt. Innerhalb der Familien konnten 1.919 verschiedene Schädlingevarianten ermittelt werden. Diese 1.919 Schädlingevarianten basieren auf 454 unterschiedlichen Schädlingfamilien. Im letzten Halbjahr zählten die Experten 203 neue Familien. Eine Auflistung der produktivsten Familien, also den Familien mit den meisten Varianten, geht aus Tabelle 1 hervor.



**Abbildung 2:** Verteilung neuer Schaddateien, die H1 2013 zugeordnet werden konnten.

Es ist wenig verwunderlich, dass die Dominanz bei den Malware-Typen weiterhin bei den Trojanischen Pferden liegt, so wie es auch im Bereich der PC Malware seit langem der Fall ist. Insgesamt machen Trojaner im Bereich Mobile einen Anteil von knapp 46% an allen neuen Samples aus und sogar 86% bei den in Familien klassifizierten Schädlingen.

Insbesondere die Familie Android.Trojan.FakelInstaller trägt eine Menge zur Trojaner-Spitzenposition im vergangenen Halbjahr bei: 59% der in Familien klassifizierten Malware entfallen auf diese Familie.

Familie	# Varianten
Trojan.Agent	266
Trojan.FakelInstaller	168
Backdoor.GingerMaster	156
Trojan.SMSAgent	100
Trojan.SMSSend	92

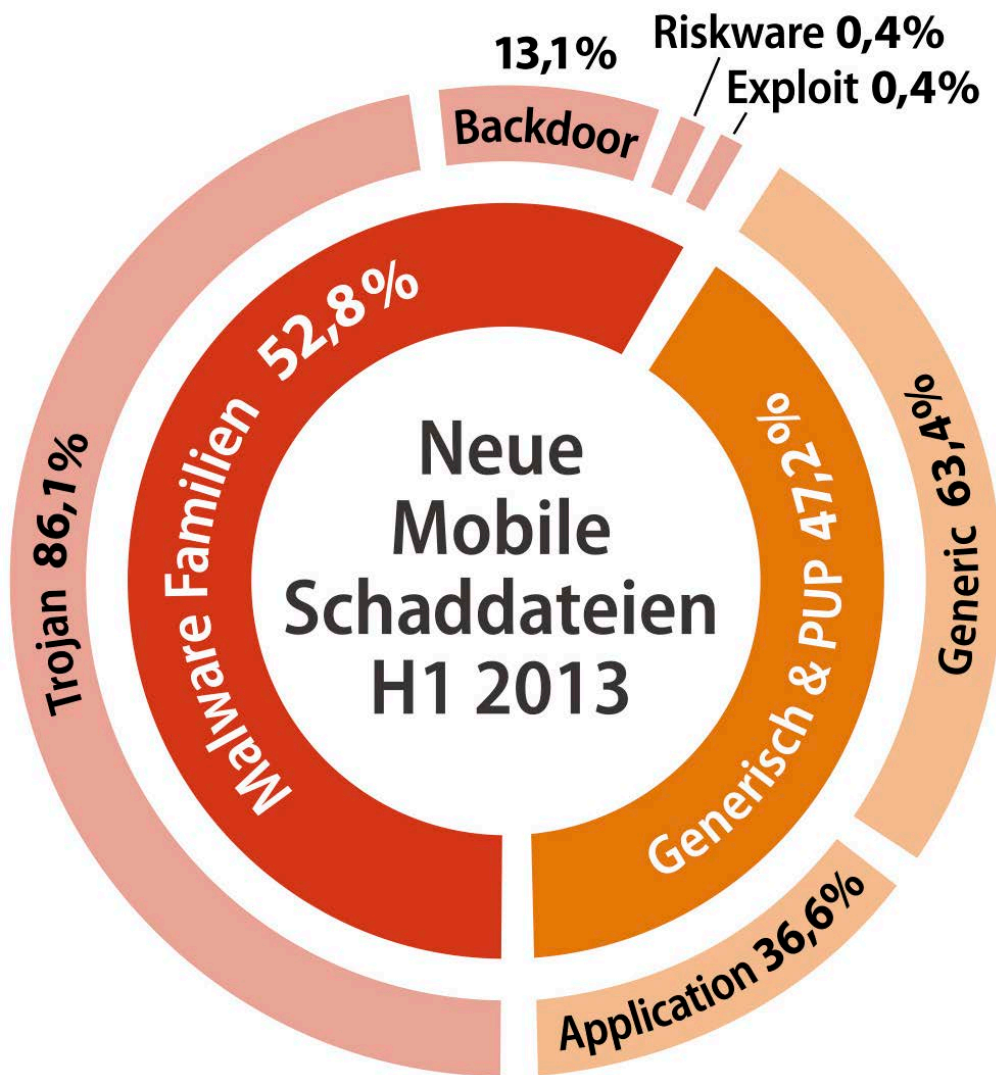
**Tabelle 1:** Liste der Android-Familien mit den meisten Varianten in H1 2013.

<sup>5</sup> Ein Android Schädling kann aufgrund mehrerer Dateien identifiziert werden. Das Installationspaket (APK) enthält viele weitere Dateien, die u.a. den Code und die Eigenschaften enthalten. Bei der vorliegenden Zählweise werden Erkennungen für APK und ihre jeweiligen Komponenten zu einer Schaddatei zusammengefasst, auch wenn tatsächlich mehrere Dateien in unserer Sammlung vorliegen.

<sup>6</sup> Die rückwirkenden Zahlen in diesem Halbjahresbericht fallen höher aus, als die in den zuvor veröffentlichten Berichten. In einigen Fällen empfangen die G Data SecurityLabs Datei-Sammlungen mit einer großen Anzahl neuer Schaddateien aus einem längeren Zeitraum und diese enthalten mitunter ältere Dateien, die dann dem entsprechenden Monat zugeordnet werden.

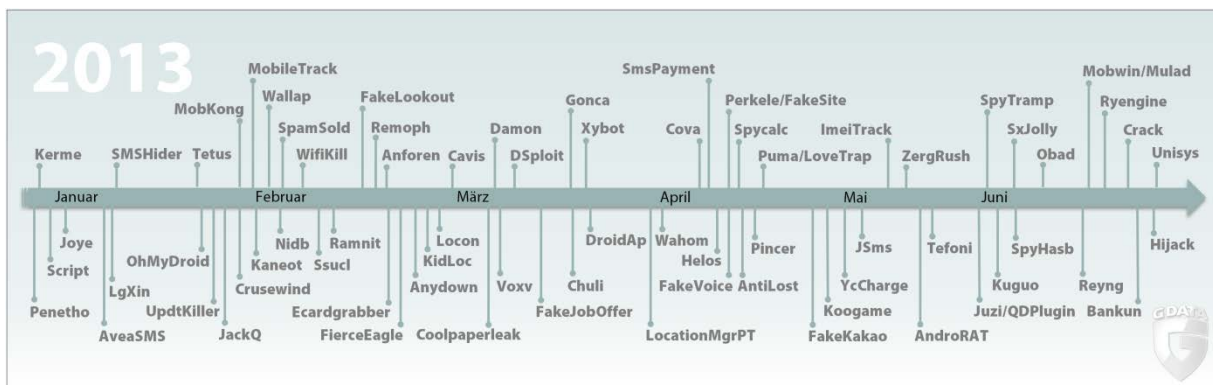
<sup>7</sup> Die Zählung der Signaturen und Varianten basiert auf den Signaturen der G Data MobileSecurity Produkte.

<sup>8</sup> Von 519.095 Samples wurden 243.697 Samples als „potenziell unerwünschte Programme“ oder mit generischen Signaturen identifiziert.



**Abbildung 3:** Zusammensetzung der neuen mobilen Schaddateien aus H1 2013 in Prozent.

Der innere Ring beschreibt die Aufteilung der neuen Schaddateien in Dateien, die zu Malware-Familien klassifiziert werden konnten und den Dateien, die generischer erkannt wurden sowie Dateien, die als potentiell unerwünschte Programmen (kurz: PUP) erkannt wurden. Der äußere Ring zeigt die respektive Zuordnung der Typen, wie sie mit den Signaturen der G Data MobileSecurity Produkte vorgenommen wird.



**Abbildung 4:** Auswahl von in 2013 erscheinender Malware für Mobilgeräte.

## AndroRAT und Malware-Kits

Weltweit wächst die Gefahr für Android Mobilgeräte, was unter anderem durch anwachsende Detektionszahlen und durch eine Vervielfachung der neu entdeckten Schaddateien eindrucksvoll untermauert wird. Ein Grund für die rasante Vermehrung von Schädlingen ist die Verfügbarkeit von Malware-Kits, die es auch nicht professionellen Schadcodeprogrammierern möglich macht, funktionsfähige, manipulierte Apps mit Hilfe einer Art Baukastensystem zu erstellen.

Bereits seit einiger Zeit gibt es eine Vielzahl von Tools um voll automatisiert Android-Malware wie den weit verbreiteten Android.Trojan.FakelInstaller<sup>9</sup> zu erstellen. Die bekannten FakelInstaller sind mannigfaltig und in hoher Anzahl vorhanden<sup>10</sup>, jedoch umfassen sie nur relativ geringe Schadfunktionen und wurden von Opfern häufig zeitnah wieder deinstalliert, da die App für sie unnötig erschien. FakelInstaller sind kostenpflichtige Installer für populäre Programme, die bei der

Ausführung Premium-SMS verschicken und den Nutzer damit gleich mehrfach Geld kosten.

Seit kurzem zeigt sich hingegen ein Trend hin zur Manipulation von voll funktionsfähigen Apps, wohl auch, weil Benutzer eine funktionierende App länger auf ihren Geräten belassen als quasi funktionsunfähige Trojaner wie den FakelInstaller. So steht den Angreifern mehr Zeit zur Verfügung, um das infizierte Gerät zu missbrauchen. Ein perfektes Beispiel hierfür ist die Backdoor AndroRAT.A.

Als Basis für diese Bedrohung von Mobilgeräten zeichnet sich die Open-Source-Software „Remote Admin Tool for Android“, kurz „AndroRAT“, aus. Der Code zu diesem Tool findet sich öffentlich zugänglich seit einiger Zeit bei GitHub, einem Hosting-Dienst für Software Entwicklungsprojekte und auch bei Google Code, einem ähnlich ausgerichteten Dienst. Auch wenn der ursprüngliche Autor seine Version schon vom Netz genommen hat, existieren noch immer Kopien und Modifikationen in den entsprechenden Communities.

Das „AndroRAT“-Projekt begann als wissenschaftliches Universitätsprojekt mit dem Ziel der legitimen und legalen Verwaltung von Android Mobilgeräten. Als solches würde das Tool im Bereich Endpoint Management und im Zusammenhang mit dem BYOD (Bring Your Own Device) Konzept zum Einsatz kommen können. Ein Administrator könnte die Installation von Apps verwalten, Kontaktlisten pflegen, etc.

Das Tool ist komfortabel zu benutzen und bequem auf die eigenen Bedürfnisse anzupassen. Leider haben das auch Schadcodeautoren bemerkt und darauf entsprechend reagiert: So fand sich zum Beispiel das Tool „AndroRAT APK Binder“ in einem internationalen Untergrundforum zum Verkauf. Es erlaubt auch Angreifern, die keine umfassenden



**ANDORAT APK BINDER**

**WHAT IS THIS?**

WHEN SOMEONE INSTALLS AN ANDROID APP THAT DOESNT DO ANYTHING, ITS SUSPICIOUS, AND THEY WILL SIMPLY UNINSTALL IT. THE SOLUTION IS TO BIND THE TROJAN TO A REAL ANDROID APP!

ANDORAT APK BINDER IS AN ANDROID APP BINDER MADE SPECIFICALLY FOR USE WITH THE FREE OPEN SOURCE ANDROID RAT "ANDORAT". IT WORKS BY DECOMPILING ANY LEGIT ANDROID APP, RE-WRITING THE ANDORAT CLIENT SOURCE TO INCLUDE YOUR IP + PORT, AND THEN INJECTING ANDORAT INTO THE DECOMPILED APP. ONCE REBUILT, YOU ARE LEFT WITH A FULLY FUNCTIONING REAL APP THAT ALSO CONTAINS YOUR ANDORAT TROJAN!

**WHAT YOUR GETTING FREE**

YOU GET ANDORAT SERVER COMPILED TO AN EXECUTABLE JAR FILE FOR WINDOWS/MAC - ALONG WITH THAT YOU ALSO GET THE ANDORAT CLIENT.

**PAYMENT**

THE PRICE IS \$37 NOT MORE OR LESS. CLICK THIS THREAD FOR PAYPAL BUYNOW PAGE!

AFTER BUYING SEND ME A PM WITH THE TRANSACTION ID, IF YOU DONT DO THAT I CAN'T GIVE YOU A COPY OF THE BINDER.

WHEN COMPLETE I WILL RESPOND WITH YOUR COPY WITHIN 24 HOURS.

NO BINDER SERVICES UNLESS YOU PAY ME A PERCENTAGE

**Screenshot 1:** Ausschnitte aus einer Werbung für den „AndroRAT APK Binder“

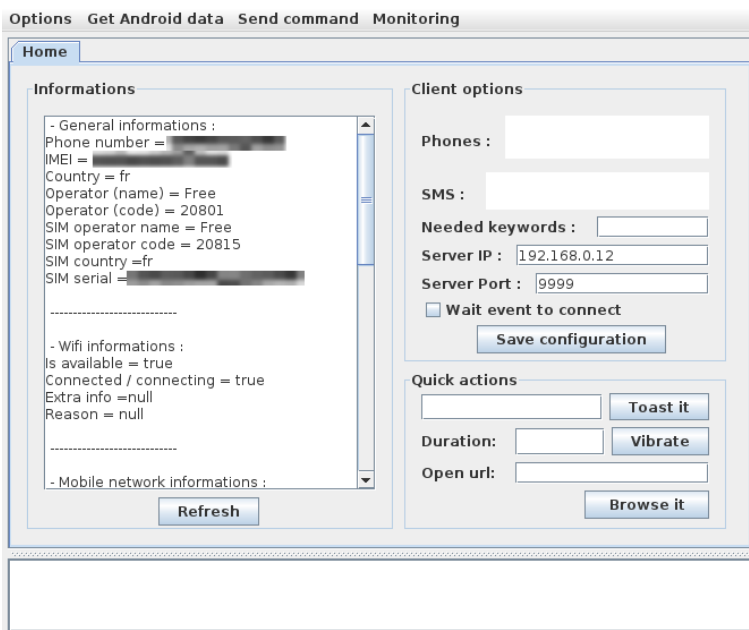
<sup>9</sup> <http://www.gdata.de/securitylab/mobile/mobile-malware.html>

<sup>10</sup> Siehe Seite 4



Programmierkenntnisse haben (sog. Skript-Kiddies), das Einbinden des oben beschriebenen „AndroRAT“ Frameworks in beliebige Android Apps. Zu Werbezwecken hat der Autor des Binders sogar entsprechende Anleitungsvideos ins Internet gestellt, um den Kauf für Interessenten noch attraktiver zu machen. Inzwischen findet man das Tool auch in weiteren internationalen Foren.

Bisher ist nur eine, im Vergleich zu den anderen Malwarefamilien, geringe Menge an Android.Backdoor.AndroRAT Samples gesichtet worden. Es ist jedoch zu erwarten, dass sich in diesem Bereich noch einiges tun wird. Die Kombination des „AndroRAT“ Tools mit dem „APK Binder“ wird weitere Trittbrettfahrer auf den Zug mit Android.Backdoor.AndroRAT aufspringen lassen. Gerade aufgrund der gegebenen Benutzerfreundlichkeit und den modularen Erweiterungsmöglichkeiten des Codes.



**Screenshot 2:** Das Panel des ursprünglichen Tools, aus der „AndroRAT“-Dokumentation

Einige technische Details zum „AndroRAT APK Binder“ und der Detektion durch die G Data MobileSecurity Produkte werden im nachfolgenden Kapitel Malware-Steckbriefe gegeben.



## Malware-Steckbriefe

### Android.Backdoor.AndroRAT.A

Android Apps können von sich aus mehrere Einstiegspunkte haben, welche entweder manuell vom Benutzer des Gerätes gestartet werden oder von speziellen Ereignissen wie dem Hochfahren des Smartphones, einem eingehenden Anruf oder ähnlichen Ereignissen automatisiert ausgelöst werden. So erlauben zum Beispiel Apps von Verkehrsverbänden das direkte Öffnen von gespeicherten Verbindungen zeitgleich mit dem normalen Start der App.

Der „Android APK Binder“ fügt einer manipulierten legitimen App einen weiteren Einstiegspunkt hinzu, so dass beim Booten des Gerätes die „AndroRAT“ Komponente – nicht die legitime App – im Hintergrund gestartet wird. Ab diesem Zeitpunkt ist das Telefon dann Teil eines Botnetzes und somit unter der vollen Kontrolle des Angreifers. In der öffentlich verfügbaren Version von „AndroRAT“ wurden folgende Befehle direkt unterstützt:

- ✦ Kontakte auslesen
- ✦ Anrufprotokoll auslesen
- ✦ SMS/MMS auslesen
- ✦ Lokalisierung des Gerätes per GPS/Funkzelle
- ✦ Alarm über eingehende Anrufe/Nachrichten etc.
- ✦ Live-Standbilder, Video und Ton an Server übertragen
- ✦ Toasts (kleine Nachrichtenfenster) anzeigen
- ✦ SMS versenden
- ✦ Anrufe tätigen
- ✦ Webseiten öffnen
- ✦ Vibrieren

Dadurch, dass der Code des legitimen „AndroRAT“ Tools quelloffen und somit frei verfügbar für jedermann ist, können Malware-Autoren ihn beliebig übernehmen, modifizieren und erweitern.

Veränderte Apps lassen sich zuweilen an den meist umfangreichen Berechtigungen erkennen, die sie einfordern. Viele der Berechtigungen benötigt die unveränderte Original-App nämlich nicht.



**Screenshot 3:** Umfangreiche Liste von angefragten Berechtigungen einer mit Backdoor.AndroRAT.A infizierten App.

## Android.Backdoor.Obad.A

Die Backdoor Obad.A ist ein sehr hoch entwickelter Schädling, der erstmals im Juni dieses Jahres in China in Erscheinung trat. Zum Angriff nutzt der Schädling gleich drei Sicherheitslücken aus: eine zuvor unbekannte Lücke im Android Betriebssystem sowie einen Fehler in einem Tool namens Dex2Jar und einen Fehler in Androids Behandlung der Datei AndroidManifest.xml, wobei die beiden zuletzt genannten die Analyse der Malware erschweren sollen.

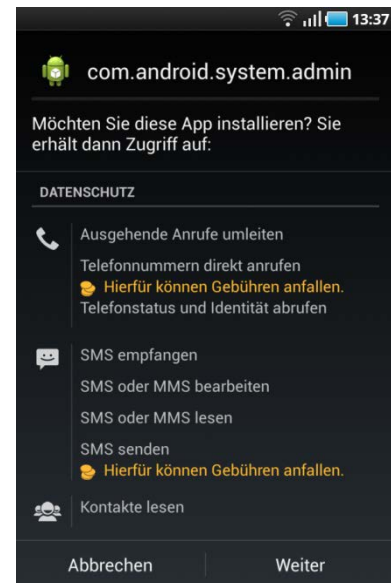
### Liste möglicher Befehle an ein infiziertes Gerät:

- ✦ Erlangen voller Kontrolle (Backdoor)
- ✦ Kommunikation mit dem Server
- ✦ Übertragung nach dem Gerätestart:
  - MAC-Adresse (Bluetooth)
  - Telefonnummer
  - IMEI
  - Abfrage der Admin-Berechtigung (ja/nein)
  - Zeitstempel
- ✦ Abfrage der installierten Apps oder bestimmter Apps
- ✦ Abfrage der Kontaktdaten
- ✦ Abfrage mit USSD Codes (z.B. Guthaben)
- ✦ Versand von SMS (Premium SMS)
- ✦ Löschen von SMS (Verbergen der Aktivität)
- ✦ Ausnutzen als Proxy
- ✦ Download/Installation von Dateien vom Server
- ✦ Versand von Dateien per Bluetooth
- ✦ Blockieren des Displays währenddessen

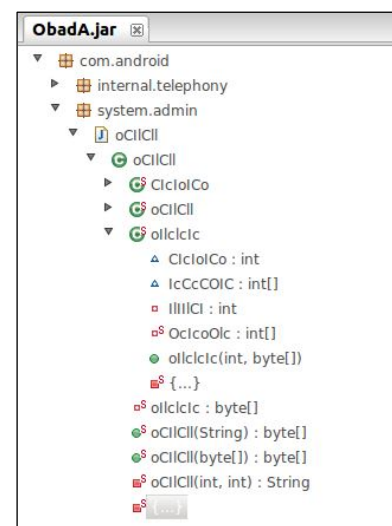
Das besonders Tückische an der Backdoor Obad.A ist, dass sie – einmal installiert – im Regelfall nicht mehr deinstalliert werden kann und zudem alle Aktivitäten im Hintergrund durchführt, nicht sichtbar für den Benutzer.

Der Funktionsumfang des Schädlings, eine aufwendige Verschleierung des Codes, sowie das sehr zeitnahe Ausnutzen von Sicherheitslücken (Zero-Day) lassen in der Backdoor Merkmale eines Windows Schädlings erkennen.

Man darf also in Zukunft nicht nur zahlenmäßig mehr Android-Malware erwarten, sondern auch ausgeklügeltere, durchdachtere und raffiniertere Schadsoftware, die die Analysten vor immer kniffligere Aufgaben stellt.



**Screenshot 4:** Der Schädling tarnt sich als System App. Verdächtig sind jedoch die Berechtigungen, die auf mögliche Gebühren hinweisen.



**Screenshot 5:** Verschleierte Klassennamen und Methoden machen es Analysten schwer, die Funktionsweisen der Backdoor nachzuvollziehen und aufzudecken.

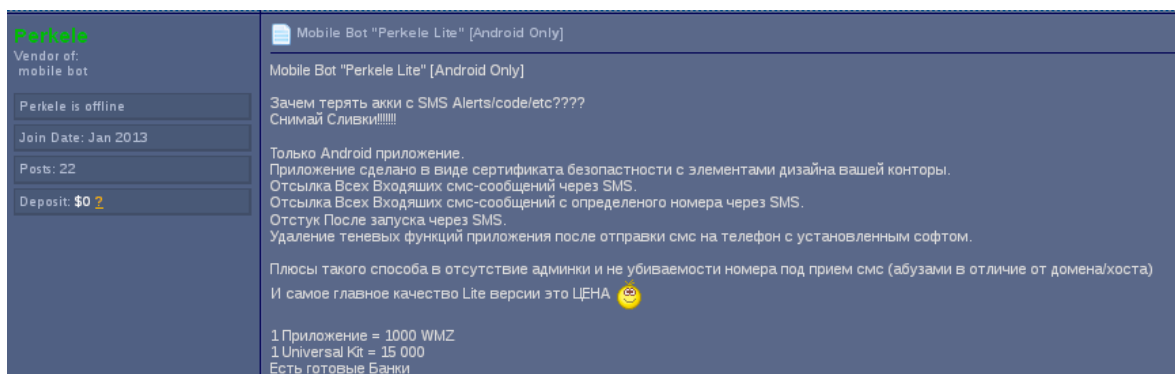
## Android.Trojan.FakeSite.A, alias Perkele

FakeSite.A, alias Perkele<sup>11</sup>, machte im ersten Halbjahr 2013 von sich reden. Dabei bestach der Trojaner jedoch nicht durch besonders herausragende, ausgeklügelte Schadfunktionen oder gut verschleierte Schadcode. Das Besondere an FakeSite.A war die Tatsache, dass er von Angreifern in Verbindung mit beliebigem Schadcode benutzt werden konnte, solange diese die Web-Inject Angriffstechnik verwendeten, die u.a. von vielen Banking-Trojanern unterstützt wird. Genutzt werden kann so eine Kombination von Cross-Plattform-Malware zum Beispiel zum Abfangen von SMS, die Bankkunden für Onlinebanking benötigen (mTAN).

### Angriffsszenario:

- ✦ Das mit einem Banking-Trojaner infizierte Opfer öffnet im PC-Browser wie gewohnt die Onlinebanking-Webseite seiner Bank. Der Banking-Trojaner manipuliert durch Web-Inject die Bankwebseite, die das Opfer im Browser angezeigt bekommt.
- ✦ Das Opfer surft die beworbene Seite an und loggt sich ein.
- ✦ Auf der manipulierten Seite erscheint dann eine durch Web-Inject eingefügte Meldung, die dem Opfer nahelegt, sich auf dem Mobilgerät ein Sicherheitszertifikat zu installieren, um sich zu authentifizieren und den Log-In abschließen zu können.
- ✦ Nach der Angabe der Mobilfunknummer bekommt das Opfer einen Link zum Download des vermeintlichen Zertifikats hinter dem sich die Schadsoftware FakeSite.A verbirgt.
- ✦ Ist die App installiert und ein Code zur Verifikation eingegeben, verschickt die App eine SMS an den Lizenzinhaber des Malware-Kits, um eine erfolgreiche Anmeldung zu signalisieren.
- ✦ Ab diesem Zeitpunkt fängt FakeSite.A alle SMS ab, die er Onlinebanking-Aktivitäten zuordnen kann und leitet sie an den Angreifer weiter.

Bei FakeSite.A handelt es sich um eine Malware, die nicht nur für erfahrene Angreifer zugänglich ist, sondern auch für vermeintliche Laien, da es einen modularen Aufbau mit vorgefertigten Malwarefunktionen hat. Außerdem stehen die Kosten in einem profitablen Verhältnis zum Gewinn: Der Autor bietet in einem Forum eine Applikation, erstellt für eine spezifische Bank, für 1.000 WMZ an und ein Universal Kit für 15.000 WMZ (WMZ = WebMoney; 1 WMZ = 1 US\$).



<b>Perkele</b> Vendor of: mobile bot <hr/> Perkele is offline <hr/> Join Date: Jan 2013 <hr/> Posts: 22 <hr/> Deposit: \$0 2	Mobile Bot "Perkele Lite" [Android Only] <hr/> Mobile Bot "Perkele Lite" [Android Only] Зачем терять акки с SMS Alerts/code/etc??? Снимай Сливки!!!!!! Только Android приложение. Приложение сделано в виде сертификата безопасности с элементами дизайна вашей конторы. Отсылка Всех Входящих смс-сообщений через SMS. Отсылка Всех Входящих смс-сообщений с определенного номера через SMS. Отступк После запуска через SMS. Удаление теневого функций приложения после отправки смс на телефон с установленным софтом. Плюсы такого способа в отсутствие админки и не убиваемости номера под прием смс (абузами в отличие от домена/хоста) И самое главное качество Lite версии это ЦЕНА 😊 1 Приложение = 1000 WMZ 1 Universal Kit = 15 000 Есть готовые Банки
--	---

**Screenshot 6:** Perkele bietet den Bot FakeSite.A in einem Forum an und preist den Funktionsumfang.

Es kann also, ähnlich wie bei Windows-Malware, mit einer weiterhin stark steigenden Anzahl von Android Schädlingen gerechnet werden. Selbst wenn FakeSite.A nicht als einer der ausgefeiltesten Schädlinge gilt, so hat dieser Trojaner dennoch hohes Schadpotential durch die schiere Masse, in der er erstellt und verbreitet werden kann.

<sup>11</sup> „Perkele ist ein in wenig gehobenen Kreisen gebräuchlicher finnischer Fluch (wörtlich ‚Teufel‘, sinngemäß etwa ‚verdammte‘).“  
 Quelle: <http://de.wikipedia.org/wiki/Perkele>

## Trends

Die Beliebtheit von Android Geräten – bei Nutzern und Schadsoftware Autoren gleichermaßen – wird auch im zweiten Halbjahr 2013 kaum abreißen. War die Malware im vergangenen Jahr noch sehr einfach gestrickt und nur für den kurzzeitigen Erfolg ausgelegt, hat sich dieser Trend nun gewandelt. Ähnlich wie zu den Anfängen der PC Malware werden Schad-Funktionen in Android Apps bereits im Programmiercode verschleiert. Damit werden sowohl die automatisierte Analyse, wie auch der menschliche Analyst daran gehindert, die schadhafte Funktionen direkt abzulesen. Wie im Fall von Obad.A steigt der Aufwand der Analyse erheblich.

Funktionen von installierter Malware sollen somit nicht nur für den Analysten, sondern auch für den Smartphone Besitzer unsichtbar sein. Wie bei FakeSite.A gesehen, ist das Grundwissen, um Malware Autor zu werden, relativ gering. Modular aufgebaute Bausätze ermöglichen es immer mehr Menschen mit krimineller Energie auf der Android Plattform aktiv zu werden und müssen mit nur einem geringen Abschlag an die ursprünglichen Hersteller des Malware Kits aufwarten.

Cyberkriminalität ist und bleibt in der Mehrheit finanziell motiviert – ob unmittelbar (Gewinn durch beispielsweise Premium-SMS Versand) oder mittelbar (z.B. durch den Weiterverkauf von gestohlenen Daten). Toolkits, wie die beschriebenen, machen es Angreifern nun deutlich leichter, eine große Masse an Schädlingen zu produzieren. Auch wenn diese nicht unbedingt technisch hochklassig sind, reichen die Funktionen aus, um Schaden anzurichten.

Die Experten der G Data SecurityLabs rechnen damit, dass sich die Zahl neuer Android-Schadprogramme im nächsten Halbjahr voraussichtlich verdreifachen wird.

Neben dem Verlangen nach dem schnellen Geld, was in der Vergangenheit immer wieder als das Hauptmotiv für die Angriffe angeführt wurde, lässt sich nun auch ein Anstieg an Backdoor-Aktivitäten feststellen, um langfristige Bindung an ein infiziertes Gerät zu gewährleisten und variablere Schäden anzurichten. Über die Backdoors entstehen Smartphone-Botnetze, die zahlreiche Schadfunktionen systematisch und strukturiert durchführen können, wie z.B. Datendiebstahl oder Versand von SMS.

Einen positiveren Ausblick erlaubt das gefühlte steigende Bewusstsein der Kunden dafür, dass es sich bei ihrem „Telefon“ um einen vollwertigen Computer handelt. Die Marktanalysten von Canalys berichten jedoch, dass lediglich 4% der Smartphones und Tablet-PCs in 2010 eine Mobile Security Lösung heruntergeladen und installiert hatten und rechnen mit einem Anstieg auf auch nur 20% im Jahr 2015.<sup>12</sup> Eine Erhöhung dieser Quote von geschützten Geräten ist unerlässlich!

Die smarten Geräte sollten genauso sorgsam behandelt werden, wie der heimische oder dienstliche PC, was das Absichern vor Viren, Trojanern, Backdoors, etc. angeht und damit den Schutz der persönlichen Daten und Werte. In diesem Fall stehen die Angreifer der Mobilgeräte den PC Angreifern in Zukunft in nichts nach.

Im Rennen um die immer noch junge Android Plattform bleibt es daher auch weiterhin spannend. Ein bewussterer Umgang mit dem Mobilgerät, sowie ein durch aktuelle Sicherheits-Software geschütztes Smartphone vergrößern dabei wesentlich die Chancen, nicht Opfer der sich etablierenden Angriffsszenarien zu werden.

---

<sup>12</sup> <http://www.canalys.com/newsroom/mobile-security-investment-climb-44-each-year-through-2015>