ANDROID MALWARE:

AKTUELLE GEFAHREN UND EINBLICKE IN EINES DER BEKANNTESTEN ANALYSESYSTEME

MICHAEL SPREITZENBARTH

Da sich Mobiltelefone immer größerer Beliebtheit erfreuen, rücken sie auch immer weiter in den Fokus von Kriminellen. Waren vor ein bis zwei Jahren nur einige hundert bösartige Applikationen für mobile Endgeräte in der freien Wildbahn bekannt, sind es heute schon weit über 200.000 und es kommen täglich neue Schädlinge hinzu. Der Funktionsumfang dieser Schädlinge reicht vom Versenden von einfachen premium SMS, über Banking-Trojaner bis hin zu ausgereiften Exploits, die das infizierte Telefon zu einem fernsteuerbaren Bot verwandeln. In diesem Artikel wird ein Überblick darüber gegeben wie die aktuelle Bedrohungslage für Android Telefone aussieht. Darüber hinaus wird eines der bekanntesten Analysesysteme für schadhafte Android Applikationen vorgestellt

Android: Die neue Nummer eins – auch bei Malware

In den vergangenen Jahren ist die Anzahl an verkauften Mobiltelefonen und deren Funktionsumfang stark gestiegen. Diese Entwicklung hat auch die Aufmerksamkeit von Kriminellen erregt, die inzwischen nicht nur versuchen die teuren Smartphones zu entwenden, sondern auch den Nutzer dazu zu bringen, schädliche Software auf ihrem Gerät zu installieren. Googles Smartphone Plattform Android ist, wenn man den Marktanteil betrachtet, das beliebteste Betriebssystem und hat inzwischen Symbian und auch iOS-basierte Geräte auf die hinteren Plätze verwiesen. Höchst wahrscheinlich ist dieses Wachstum der Offenheit der Plattform geschuldet, die es Nutzern erlaubt, auch Software von Drittanbietern oder sogar eigens geschriebene Apps zu installieren. Gleichzeitig nutzen Angreifer diese Offenheit jedoch aus, um schädliche Applikationen über inoffizielle Android Märkte oder präparierte Webseiten und Emails zu verteilen. Nach einer Studie von Kaspersky gehört Android auch in diesem Bereich die Spitzenposition (vgl. Abbildung 1).

Das Jahr 2012 im Fokus der Malware Autoren

Im Jahr 2012 wurden knapp 300.000 Android Apps aus den verschiedensten Quellen, darunter auch der Google Play Market und offizielle Märkte aus China und Russland, in der Mobile-Sandbox untersucht. Dabei wurden etwas über 43.000 Apps als schadhaft klassifiziert und in 115 Familien eingruppiert. Bei der Eingruppierung in Familien wird das schadhafte Verhalten und die dafür nötige Code-Basis zwischen den Apps verglichen. Ähneln sich diese Werte stark, so geht man davon aus, dass die verglichenen Apps den selben Ursprungscode haben und somit zur selben Malware-Familie gehören.

Aus diesen 115 Familien wurden gerade einmal Apps aus 13 verschiedenen Familien im Google Play Market gefunden. Die restlichen schadhaften Apps stammten aus russischen und chinesischen Drittanbieter-Märkten. Dies zeigt, dass Google mit Bouncer und weiteren implementierten Detektionsmaßnamen auf einem guten Weg ist seinen eigenen Marktplatz frei von Malware zu bekommen. Betrachtet man allerdings die gesamten schadhaften Android Applikationen so wird klar, welche Bedrohung hinter harmlos wirkenden Apps warten kann (vgl. Tabelle 1).

Wirft man einen genaueren Blick auf die Daten in Tabelle 1, so fällt auf, dass die Mehrzahl der schadhaften Apps darauf ausgelegt ist, persönliche Daten von dem infizierten Telefon zu stehlen. Dazu zählen meist die IMEI und IMSI, aber auch Einträge im persönlichen Kalender oder Adressbuch. Auch wenn

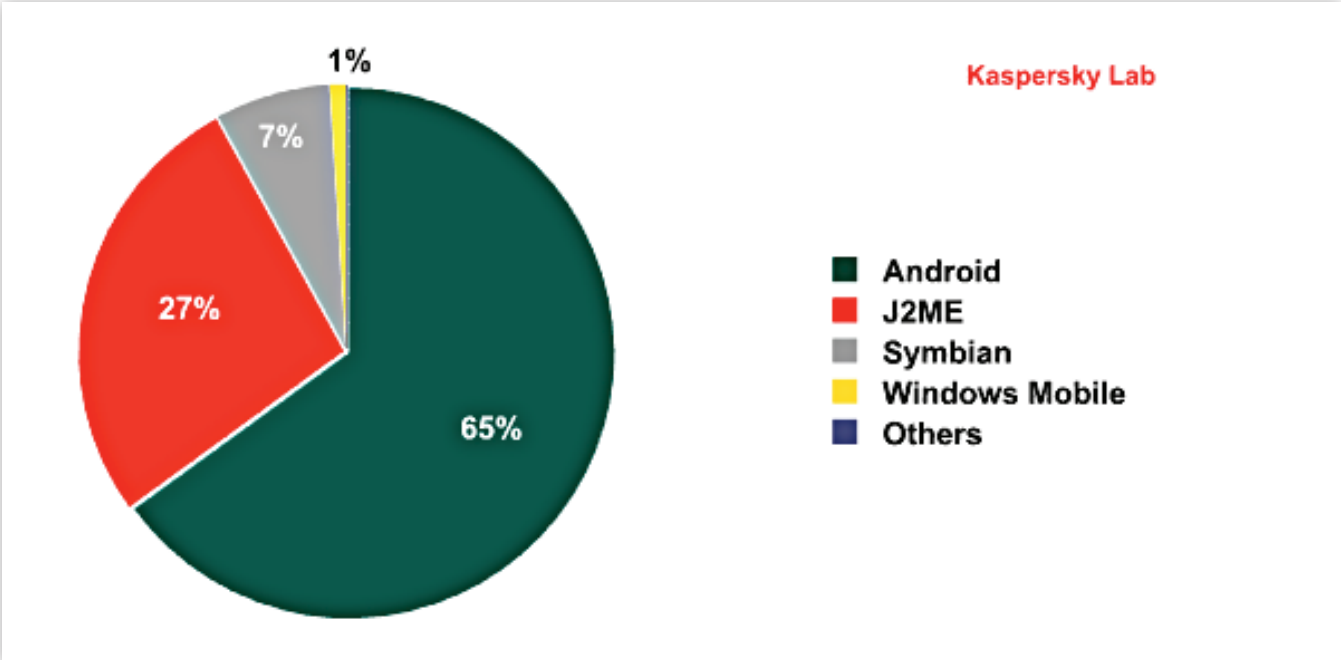

Abbildung 1: *Kaspersky-Studie über die Verbreitung von Schadcode auf den unterschiedlichen mobilen Plattformen.*

der Verlust dieser Daten bei Privatpersonen noch recht harmlos erscheint, wird der Ernst der Lage bei Firmentelefonen deutlich. Hier bedeuten Kontaktdaten und Hintergrundinformationen zu Besprechungen oft bares Geld. Aber auch die Daten von Privatpersonen können im Untergrund verkauft werden um damit personalisierte SPAM-Kampanien zu starten.

Am Zweithäufigsten wurden Apps gefunden, die premium SMS versenden. Dieses Verhalten war bei knapp 30% aller Familien zu sehen. Hierbei wird der Benutzer des infizierten Telefons direkt geschädigt, da diese Apps im Hintergrund SMS Nachrichten an Sonderrufnummern versenden, deren Preis zwischen 0,99€ und 4,99€ liegt. Dabei darf nicht vergessen werden, dass diese Apps auch deutlich mehr als nur eine dieser premium SMS versenden.

Mindestens genauso gefährlich für den Benutzer sind aber auch die Gruppe der schadhaften Apps, die einen sogenannten Root-Exploit mit sich bringen. Dieser Exploit ermöglicht es der App Vollzugriff auf das Telefon zu bekommen und dabei alle vom System integrierten Schutzmaßnamen zu umgehen. Mit einer solchen App, kann ein Angreifer mit dem infizierten Telefon anstellen was er möchte und das ohne, dass der Benutzer des Telefons dies wahrnimmt. In den meisten Fällen wurden die auf diese Weise infizierten Telefone aus der Ferne von sogenannten Command&Control-Servern (C&C-Server) gesteuert. Dabei wurden weitere Apps auf dem Telefon installiert, die Nummern für premium SMS geändert oder das Telefon für Denial-of-Service (DoS) Angriffe missbraucht.

Was in 2012 neu dazu kam, sind die Malware-Familien die sich auf das Abfangen und Manipulieren von Mobile-Banking-Tans (mTAN) spezialisiert haben. Bei einem solchen Angriff wird der Benutzer oft mit einer Phishing-Mail auf eine infizierte Bankseite geleitet (siehe Abbildung 2), wo er dann eine Meldung angezeigt bekommt, dass er für noch mehr Sicherheit im Onlinebanking eine App auf seinem Telefon installieren muss. Diese App fängt dann alle mTAN Nachrichten ab und ändert den Inhalt so ab, dass der Benutzer es nicht mehr merkt, wenn er Geld auf ihm unbekannte Konten überweist. Hat ein Angreifer auf diese Art und Weise die Banking-Seite des Benutzers und dessen Smartphone manipuliert, so bietet das mTAN-Verfahren keinerlei Schutz mehr.

Betrachtet man dieses Gefahrenpotential und die immer besser werdenden schadhaften Apps, so sollte jedem Android Benutzer deutlich werden, dass er inzwischen in das Schussfeld der Gauner und Kriminellen geraten ist. Um sich gegen diese Bedrohungen zu schützen sollte auf mobilen Endgeräten eine AntiVirus-Lösung installiert werden und Systemupdates, soweit diese verfügbar sind, zeitnah eingespielt werden.

Tabelle1: *Überblick über die Gefahren, die von Android Malware ausgehen.*

Familien, die persönliche Daten vom Telefon stehlen	51,3 %
Familien, die premium SMS versenden	30,1 %
Familien, die das infizierte Telefon zu einem Bot machen	23,5 %
Familien mit Root-Exploits im Gepäck	18,3 %
Familien, die aus dem Google-Play Market stammen	11,3 %
Familien, die weitere Apps nachladen und installieren	10,4 %
Familien, die GPS und andere Ortsdaten stehlen	8,7 %
„Hacker-Apps“ (WLan-Sniffer, ARP-Spoofer, usw...)	7,8 %
Online-Banking Trojaner	3,5 %

Abbildung 2: *Phishing-Seite der Postbank mit der Aufforderung eine schadhafte App zu installieren um so das mTAN-Verfahren auszuhebeln.*

Mobile-Sandbox: Automatisierte Analyse und Klassifizierung von Android Apps

Reichen einem die AntiVirus-Lösungen nicht aus, oder möchte man auch sichergehen, dass man vor noch unbekannten schadhaften Apps geschützt ist, so bleibt einem meist nichts anderes übrig, als seine Apps selbst auf verdächtiges Verhalten zu prüfen.

Um festzustellen, ob eine Applikation gut oder bösartig ist, muss diese mit großem Aufwand analysiert werden. Dabei ist nicht nur ein breites Wissen in Java und den Eigenschaften des Android System nötig, es wird auch ein ganzes Arsenal an Werkzeugen benötigt. Um diesen Prozess zu vereinfachen gibt es inzwischen ein paar wenige vollautomatisierte Systeme, die über ein Webinterfaces für Jedermann zugänglich sind. Darunter befindet sich unter Anderem die Mobile-Sandbox (*http://www.mobilesandbox.org*).

Diese Systeme starten die Analyse zumeist mit einer **statischen Analyse**. Bei diesem Schritt wird die App in ihre Bestandteile zerlegt und versucht durch dekompilieren und code-review verdächtige Funktionen zu finden. Auch die im Android System wichtigen Berechtigungen und Intents werden hierbei herausgefiltert. Oft wird hierbei auch geprüft, ob

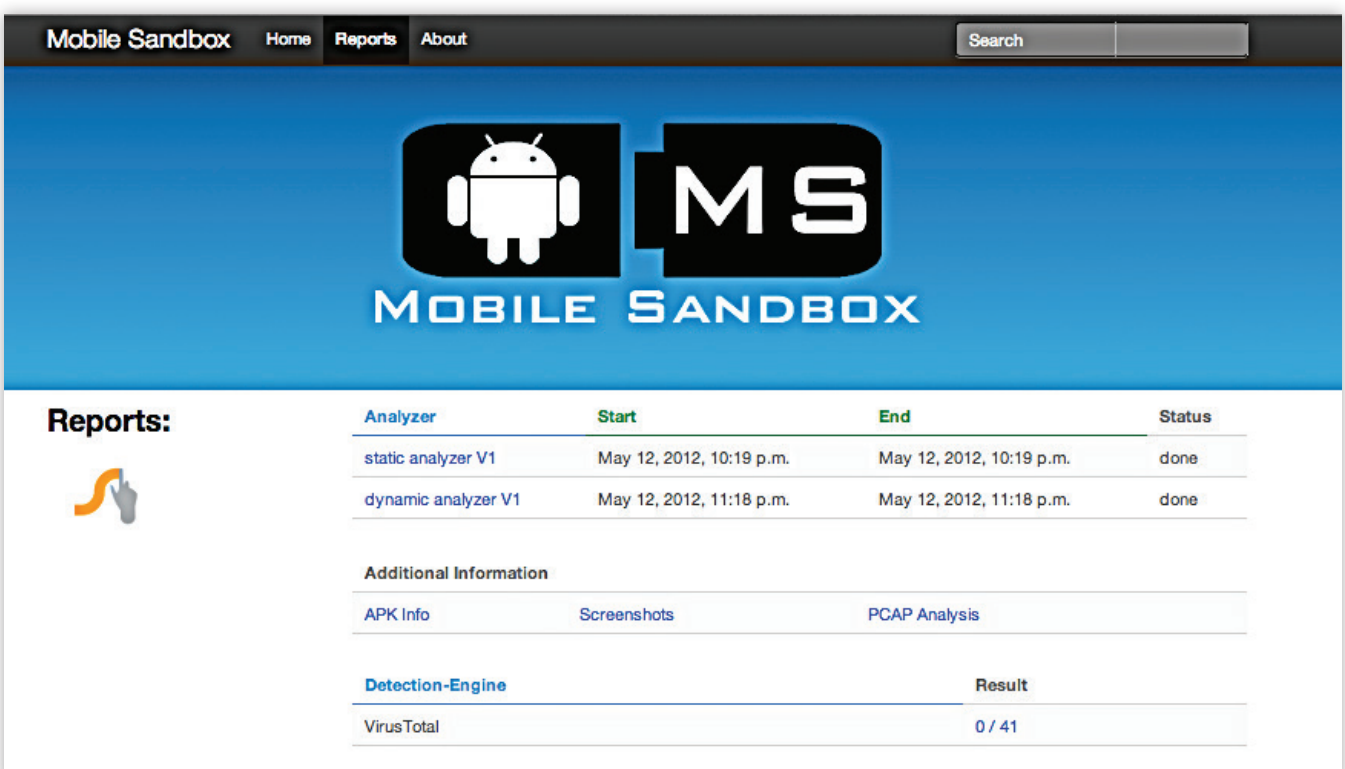

Abbildung 3: *Übersicht über eine bereits analysierte App in der Weboberfläche der Mobile-Sandbox*

eine App überberechtigt ist. Dies bedeutet, ob eine App bei der Installation mehr Berechtigungen vom Benutzer abfragt, als sie eigentlich zur Ausführung benötigt.

In einem weiteren Schritt wird die App dann in einer abgeschotteten Umgebung ausgeführt und ihre Aktionen zur Laufzeit überwacht. Dieser Schritt ist auch als **dynamische Analyse** bekannt. Bei Android wird meist auf einen modifizierten Emulator gesetzt, der mit Hilfe von Taint-Tracking (dem Nachverfolgen von Variablen und deren Inhalt) Verhaltensprofile der ausgeführten Apps anlegen kann. Der Vorteil einer dynamischen Analyse besteht unter anderem darin, dass auch versteckte oder verschlüsselte Code-Fragmente mitgeschnitten werden können, da diese zur Laufzeit kurzfristig im Klartext vorliegen.

Die Analyse, die bei der Mobile-Sandbox durchgeführt wird, besteht aus mehreren Komponenten, deren Zusammenspiel momentan einzigartig ist. So werden z.B. die Ergebnisse der statischen Analyse verwendet um spezielle Ereignisse oder Benutzerinteraktionen in einer späteren dynamischen Analyse auszulösen. Wartet eine Funktion mit ihrer Ausführung z.B. auf eine eingehende SMS Nachricht, evtl. sogar mit speziellem Nachrichtentext, so wird diese während der Ausführung an den Emulator gesendet. Mit diesem Zusammenspiel ist es möglich den Funktionsumfang einer App nahezu vollständig abzudecken und so zu verhindern, dass die App ihr schadhaftes Verhalten vor dem Analysesystem verstecken kann.

Zusätzlich wird in der Mobile-Sandbox auch der Netzwerkverkehr aufgezeichnet, um dort verdächtige Pakete oder ganze Kommunikationen mit möglichen C&C-Servern zu entdecken. Da es in neueren Android Versionen möglich ist, Code der App in externe Bibliotheken auszulagern, setzen die Analysekomponenten auf eine modifizierte Version von ltrace, die es ermöglicht, alle Operationen innerhalb dieser Bibliotheken zu überwachen.

Durch das gesamte Zusammenspiel der Komponenten ist es möglich, ein komplexes Profil einer App zu erstellen und dem Benutzer in der Weboberfläche zu präsentieren (siehe Abbildung 3). Anhand dieses Profils kann im Anschluss an die Analyse entschieden werden, ob es sich bei einer App um Schadcode handelt, oder ob sie doch nur das Verhalten an den Tag legt, das von ihr erwartet wird.

Schutzmaßnamen für Smartphone-Nutzer

In den letzten beiden Jahren stieg die Anzahl der schadhaften Applikationen stark an. Auch die Funktionen und Verschleierungstechniken der Kriminellen wurde in dieser Zeit immer ausgereifter, daher sollte sich jeder Smartphone-Nutzer selbst so gut es geht gegen diese Bedrohungen schützen.

Mögliche Schutzmaßnamen sind unter Anderem die folgenden:

- **PIN- bzw. Passwortschutz:** Aktivierung von PIN/Passwortschutz oder Aktivierung der eingebauten Vollverschlüsselung. Durch dieses Vorgehen sind die Daten auf dem Telefon auch bei Verlust deutlich besser geschützt.
- **Download nur aus dem Google Play Market:** Obwohl auch in diesem Marktplatz im vergangenen Jahr noch schadhafte Apps gefunden wurden, so ist die Rate doch gravierend geringer als in anderen Märkten und es werden Schutzmaßnamen eingesetzt um Schadcode von dem Marktplatz fern zu halten.
- **AV-Lösung:** Die Installation von AntiVirus-Lösungen oder anderen vergleichbaren Sicherheits-Produkten sorgt für ein deutlich höheres Maß an Sicherheit.
- **Kontrolle der Telefonrechnung:** Durch die regelmäßige Kontrolle der Telefonrechnung kann ein schadhaftes Verhalten schnell erkannt und höherer Schaden für den Benutzer vermieden werden.
- **Vorsicht beim mobilen Surfen:** Smartphones sind beim arglosen Surfen nahezu genauso anfällig für manipulierte oder mit Schadcode belastete Webseiten wie der heimische PC. Daher gilt es auch hier darauf zu achten, welche Webseiten man betrachtet und welche Daten man auf sein Smartphone herunterlädt.
- **Systemupdates:** Diese sollten zeitnah zum Veröffentlichungstermin auf dem Smartphone installiert werden. Hierdurch werden bekannte Sicherheitslücken auf den Telefonen geschlossen und somit die Sicherheit des Systems stark erhöht.

MICHAEL SPREITZENBARTH

ist wissenschaftlicher Mitarbeiter an der Friedrich-Alexander-Universität, Erlangen-Nürnberg. Seine Forschung umfasst die forensische Analyse und Auswertung von Mobiltelefonen sowie die Erkennung und Abwehr von mobilem Schadcode.

http://forensics.spreitzenbarth.de