

Schutz mobiler Geräte: Gegenwart und Zukunft

McAfee® Labs™ untersucht die aktuelle Situation bei Smartphones und anderen Mobilgeräten sowie die Sicherheitsrisiken, die durch die neuen Funktionen entstehen. Außerdem erfahren Sie, mit welchen Bedrohungen für diese praktischen Geräte Sie rechnen müssen.

Dr. Igor Muttik

Trotz der kontinuierlichen Fortschritte beim Schutz von Desktop-Computern durch sichere Hardware, Betriebssysteme und Anwendungen wird Malware nie aussterben. Bei der heutigen rasanten Zunahme von Smartphones, Tablet-Computern und anderen mobilen Geräten müssen sich ihre Benutzer die Frage stellen, ob sich diese Geräte auch schützen lassen. Aufgrund unserer umfangreichen Kenntnisse im Bereich Desktop-Computerschutz könnte man vermuten, dass die neue Generation mobiler Hardware relativ sicher sein sollte, weil wir von unseren gewonnenen Erkenntnissen profitieren. In diesem Artikel soll detailliert untersucht und beschrieben werden, warum das recht unwahrscheinlich ist.

Um es gerade heraus zu sagen: Mobile Geräte werden auch in Zukunft nicht weniger anfällig für Sicherheitsprobleme sein. Die Bedrohung durch Malware mag insgesamt abnehmen, aber der mithilfe mobiler Geräte verursachte Schaden wird hoch sein, weil Smartphones dauerhaft mit dem Internet verbunden sind, stets persönliche Daten umfassen und sogar mit kleinen Kameras, Mikrofonen und Positionierungsgeräten ausgestattet sind. Genau solche Technik hatten die Spione in alten Filmen immer dabei. Durch die größere Auswahl an integrierten Geräten im Vergleich zu Desktop-Computern (oder Notebooks) werden Betriebssysteme und Anwendungen komplexer. Dadurch nehmen die Angriffsmöglichkeiten sogar zu.

Der Kern heutiger Betriebssysteme wie iOS und Android basiert auf Unix/Linux, wodurch das System vergleichsweise sicher ist. Aufgrund des Drucks auf dem Markt stellen die Hersteller jedoch häufig schnelle Markteinführung über Sicherheit und bieten ihre Produkte möglicherweise mit wichtigen Treibern und Anwendungen an, die noch nicht ausreichend getestet wurden. Wenn bei der Implementierung von Updates für Firmware und Betriebssystem zusätzlich Fehler auftreten, kann der Betriebssystemkern noch so gut geschützt sein: Angreifer bekommen eventuell die Möglichkeit, ihn komplett auszutauschen.

Nahezu alle in den letzten Jahren aufgetretenen Formen von Desktop-Computer-Bedrohungen sind auch auf mobilen Geräten möglich. (Parasitäre Viren bilden möglicherweise die große Ausnahme bei modernen Mobilgeräte-Betriebssystemen. Mehr dazu weiter unten.) Darüber hinaus werden Bedrohungen zwangsläufig neu für mobile Umgebungen angepasst. Außerdem wird es sicher auch neue Malware-Formen geben, die auf Desktops nicht vorhandene Smartphone-Funktionen nutzen.

In diesem Artikel werden die Bezeichnungen „Mobilgerät“ und „Smartphone“ synonym gebraucht. Der erste Begriff ist zwar weiter gefasst (weil er unter anderem auch tragbare Spielekonsolen, Reader, Tablet-Computer umfasst), die Überschneidung der Funktionen und Merkmale ist jedoch sehr groß. Zudem können die heutigen Telefone so gut wie alles, was spezialisierte Geräte können.

Inhaltsverzeichnis

Besonderheiten von Mobilgeräten	4
Bisherige Umgebungen	7
Android	8
iOS, Windows Phone 7 und andere Plattformen	12
Aktuelle und künftige Ökosysteme	12
Entwicklungen und Prognosen	16
Fazit	26
Danksagung	27

Besonderheiten von Mobilgeräten

Mobilität führt zu Schwachstellen

Da Mobilgeräte unterwegs genutzt werden, können sie einfacher verloren gehen oder gestohlen werden und sind zudem anfälliger Ziele für Mitlesende („Over-the-Shoulder“-Browsing). Selbst wenn Geräte ordnungsgemäß mit einer PIN oder Passphrase gesichert sind, haben entschlossene Angreifer eine reelle Chance, die PIN bei der Eingabe mitzulesen. Die restliche Kompromittierung hängt vom Talent des Angreifers als Taschendieb sowie der Unachtsamkeit des Mobilgerätebesitzers ab. Selbst ein kurzer Kontrollverlust über ein Smartphone kann zu einer Kompromittierung führen.¹

Die meisten von uns haben statt mehrerer Geräte lieber ein einziges Smartphone mit vielen Funktionen bei sich. Dadurch werden diese Geräte natürlich flexibler und teurer – und folglich auch attraktiver für Diebe. Diese sind möglicherweise nur an der Hardware interessiert. Ihr Augenmerk richtet sich aber auch zunehmend auf die Gerätedaten, die sehr wertvoll und unter Umständen wesentlich wertvoller als das Gerät selbst sein können.

Die heutigen Sicherheitsmaßnahmen erschweren den Weiterverkauf gestohlener Geräte. In vielen – leider aber nicht in allen – Ländern kann der Anbieter, wenn ihm die eindeutige Kennnummer (IMEI, International Mobile Station Equipment Identity) eines verloren gegangenen Mobiltelefons gemeldet wird, das Gerät sperren. Es ist zwar möglich, die IMEI umzuprogrammieren, doch ist der Besitz entsprechender Geräte in einigen Ländern unter Umständen illegal. Im Gegensatz zu den jährlich sinkenden Gerätekosten verhält es sich mit den Kosten für die darauf gespeicherten Daten genau umgekehrt. Heute sind die aus einem Mobiltelefon extrahierten Daten in vielen Fällen wertvoller als das Gerät selbst. Und sie werden immer wertvoller, da Smartphones zunehmend für Bankgeschäfte (einschließlich Nahfeldkommunikation) und Geschäftsanwendungen (z. B. für Betriebsgeheimnisse, Entwürfe, Roadmaps und Patentdokumentation) genutzt werden.

Akkubetrieb

Mobilgeräte müssen regelmäßig aufgeladen werden. Ressourcen-intensivere Rechenaufgaben und Kommunikation wie die WLAN-Nutzung oder Telefonate führen zu einer beschleunigten Entladung des Akkus. Um dem entgegenzuwirken, wechseln Mobiltelefone in einen energiesparenden Ruhemodus. In diesem Modus wird die Software durch einen Timer regelmäßig reaktiviert, um notwendige Aufgaben auszuführen. Einige Anwendungen verhindern jedoch eventuell, dass das Mobilgerät in den Ruhemodus wechselt. Auch schlecht geschriebene Software kann zu einer schnelleren Akku-Entladung beitragen. Bei der Ausführung von Malware wird der Akku natürlich ebenfalls beansprucht. Dies zeigte sich bei konkreten Erfahrungen mit den Würmern SymbOS/Cabir und SymbOS/Commwarrior, die zu ihrer Verbreitung aktiv die Bluetooth-Schnittstelle nutzten. Anders als Software-Hersteller kümmern sich Malware-Autoren im Allgemeinen wesentlich weniger um Benutzerfreundlichkeit. Daher dürfte Malware womöglich häufig reaktiviert werden und so die Akku-Entladung beschleunigen. Eine Ausnahme bilden Malware-Formen wie hochentwickelte hartnäckige Bedrohungen (Advanced Persistent Threats, APTs), die möglichst lange im Verborgenen bleiben wollen. In diesem Fall treffen die Malware-Autoren Vorkehrungen zur Energieeinsparung, um zu verhindern, dass ein Benutzer Verdacht schöpft. Es könnte also manchmal das Ziel des Angreifers sein, den Bedarf an energieintensiven Operationen zu senken, um die Lebensdauer der Malware zu erhöhen.

Auf der Sicherheitskonferenz BlackHat 2011 führte ein Forscher die Kompromittierung von Akku-Firmware vor – ein Ereignis, das zweifellos zumindest einen DoS-Angriff (Denial-of-Service) verursachen könnte, nachdem ein Akku unbrauchbar gemacht wurde.² Als Beispiel sei hier Malware genannt, die auf eine für den Umgang mit einer Notsituation verantwortliche Person (oder Gruppe) abzielt: Falls Malware – etwa ein ferngesteuertes Botnet oder eine auf Kriegsführung ausgelegte APT – einen Remote-Befehl erhält und dann einen Akku unbrauchbar machen kann, würde für die betroffene Person bzw. das Team eine bequeme (und möglicherweise die einzige verfügbare) Kommunikationsmethode entfallen.

GPS

Überwachung des Besitzers

Viele Mobilgeräte nutzen GPS (Global Positioning System), um Anwendungen mit Informationen über die aktuelle Position des Geräts zu versorgen und standortspezifische Dienste zuzulassen (z. B. die Anzeige einer lokalen Umgebungskarte oder die Ergänzung von Fotos mit Daten zum Aufnahmeort). Dies bedeutet natürlich, dass die Software den Gerätestandort und in der Regel auch den Besitzer des Geräts kennt. Es bedarf nicht viel Fantasie, um die Probleme einer Offenlegung oder Weitergabe dieser Informationen zu erkennen. Die Tracking-Malware GPS Spy (oder TapSnake) für Android ist bereits im Umlauf. Es bedarf wirksamer Kontrollen, um den Datenschutz von Mobiltelefonbesitzern zu gewährleisten und die Verteilung von GPS-Daten zu beschränken (moderne Betriebssysteme für Mobilgeräte wie iOS und Android verfügen über spezielle Mechanismen zur Beschränkung des Zugriffs auf GPS-Daten).

Der nachlässige Umgang mit GPS-Daten durch die Anwendung oder das Betriebssystem könnte leicht Datenschutzprobleme verursachen. Besonders eindrucksvoll wurde dies bei einem Vorfall deutlich, bei dem die GPS-Standorte von iPhones mit einem Desktop-Computer synchronisiert und ungeschützt in der Datei „consolidated.db“ gespeichert wurden, welche bei jeder Synchronisierung aktualisiert wurde und für alle Benutzer mit Zugriff auf die Datei sichtbar war. Diese schwerwiegende Datenschutzlücke wurde von Apple relativ schnell geschlossen.

Tyler Shields von Veracode stellte eine Spionage-App für BlackBerries vor, die den Standort von Mobiltelefonen verfolgen kann.³ Diese Malware-Form könnte beispielsweise beim Kidnapping hochkarätiger Ziele helfen.

Wenn Benutzer ihre GPS-Daten automatisch freigeben (z. B. durch die Nutzung eines Dienstes wie Foursquare, d. h. eines standortbasierten Social-Networking-Systems), geben sie freiwillig ihre Privatsphäre auf.⁴ Falls dann jedoch der Anbieter kompromittiert wird und die Standortverfolgungsdaten vieler Benutzer offengelegt werden, erhöht sich der Verlust an Privatsphäre um ein Vielfaches.

Auch bei deaktivierter GPS-Hardware werden Standortdaten auf Mobilgeräten gespeichert. Das Netzwerk verfügt über die Information, zu welcher Zelle (Mobilfunkmast) jedes einzelne Gerät eine Verbindung herstellt. Diese Information ist zwar ungenauer als GPS-Koordinaten, dennoch lassen sich Mobiltelefone damit im Allgemeinen relativ genau – auf einen Umkreis von 100 Metern – lokalisieren. Diese Daten stehen aber unter Umständen nur dem Betriebssystem zur Verfügung. Die meisten Anwendungen sollten im Normalfall keinen Zugriff darauf haben – es sei denn, sie können sich durch Ausnutzung einer Schwachstelle im Betriebssystem umfassendere Berechtigungen aneignen. Selbst wenn es also Betriebssystemsteuerungen zur Deaktivierung von GPS-Hardware gibt, lässt sich ihre Wirksamkeit aufgrund dieser Netzwerkdaten nicht hundertprozentig garantieren.

Verfolgung von Dieben

Theoretisch könnte ein GPS-fähiges Mobiltelefon im Falle eines Diebstahls vom Besitzer oder einer Strafverfolgungsbehörde über GPS geortet werden. Das Problem liegt aber natürlich darin, dass die GPS-Daten zur Verfolgung von Dieben aus der Ferne erfassbar sein müssen. Würden die Mobiltelefone über entsprechende Mechanismen verfügen, könnten wir tatsächlich Diebe lokalisieren, doch stünde dies in Konflikt mit der Privatsphäre des Besitzers. Zur Lösung dieses Problems muss der Besitzer des Geräts zuverlässig identifiziert werden. Die meisten gängigen Methoden (PIN oder Passphrase) sind nicht so gut wie beispielsweise biometrische Authentifizierung – diese wird jedoch wahrscheinlich noch einige Jahre unerschwinglich teuer bleiben.

Kamera und Mikrofon

Mit Smartphones können Fotos sowie Video- und Audiodateien aufgenommen werden. Auch in tragbaren Spielkonsolen und Tablets ist diese Funktion verfügbar. Diese Geräte werden durch Software gesteuert, und in vielen Fällen ist der Betrieb der Kamera oder des Mikrofons möglich, ohne dass der Benutzer diese Aktivität überhaupt bemerkt.

Zwar verfügen die meisten Betriebssysteme über Optionen zur Deaktivierung von Kamera und Mikrofon, doch könnte Malware durch eine erfolgreiche Ausnutzung von Betriebssystem-Schwachstellen (und die daraus resultierende Erweiterung der Berechtigung zur Steuerung der Hardware) die Benutzer und ihre Umgebung ausspähen. Derartige Schwachstellen werden regelmäßig entdeckt und ausgenutzt.⁵ Es gibt bereits Trojaner, die Telefonate aufzeichnen und die Aufnahme dann an einen anderen Ort senden.⁶ Auch Strafverfolgungsbehörden könnten versuchen, Smartphone-Diebe mittels Tönen und Bildern vom Gerät zu verfolgen.

3. <http://www.veracode.com/blog/2010/02/is-your-blackberry-app-spying-on-you>

4. [http://en.wikipedia.org/wiki/Foursquare_\(website\)](http://en.wikipedia.org/wiki/Foursquare_(website))

5. <http://www.cs.ncsu.edu/faculty/jiang/GingerMaster/>

6. <http://blogs.mcafee.com/mcafee-labs/latest-android-malware-records-conversations>

Praktische Auswirkungen des Multiprozessor- bzw. Mehrkern-Designs

Smartphones und andere tragbare Geräte dienen mit ihrer Rechenleistung dem Benutzer (Bildschirm, Tastatur, Anwendungen) und verwalten die Baseband-Kommunikation (mobiles Signal: GSM und 3G). Letztere erfordert eine Verarbeitung in Echtzeit, denn falls empfangene oder übertragene Daten nicht schnell genug verarbeitet werden, kommt es auf dem Smartphone zu Kommunikationsunterbrechungen und damit zu Frust beim Nutzer des Geräts. Zur Aufrechterhaltung der Verbindung nutzt das Gerät unter Umständen zwei Prozessoren (oder eine Implementierung als Ein-Chip-System- bzw. „System-on-Chip“-Paket, das auf einem SoC-Chip mehrere Gerätesubsysteme umfasst). Die Hersteller werden die Funktionalität künftig wahrscheinlich weiter aufteilen, beispielsweise durch zusätzliche SoC-Kerne für Grafik und Sicherheit.

Aufgrund dieser Design-Entscheidungen werden die Prozessorsubsysteme möglicherweise isoliert, was einige Probleme bei der Aufrechterhaltung der Sicherheit aufwerfen wird. Ralf-Philipp Weinmann hat bereits erfolgreiche Angriffe auf Baseband-Prozessoren (Qualcomm-Prozessor im HTC und Infineon im iPhone) demonstriert.⁷ Ein weiteres Beispiel veranschaulicht, dass die Kompromittierung eines Kommunikationssubsystems (über Bluetooth-Schwachstellen) der auf einem anderen Prozessor – oder einem separaten bzw. dedizierten Kern – ausgeführten Sicherheits-Software völlig verborgen bleiben kann.⁸ Separate Prozessoren können mit anderen Worten separat ausgenutzt werden. Allein die Erkennung solcher Situationen ist unter Umständen schwierig.

Andere Mobilgeräte

Tablets

Die heutigen Tablets sind leistungsfähiger, als es Laptops vor einigen Jahren waren. Auch wenn sie wegen der fehlenden physischen Tastatur für viele Aufgaben (Textbearbeitung, Programmierung und Design) ungeeignet sind, eignen sie sich sehr gut zum Surfen im Internet, das heute die Hauptquelle von Malware ist. Diese Malware gelangt häufig über Schwachstellen des Browsers (und seiner Acrobat-, Flash- oder Java-Plug-Ins) auf Computer, weswegen wir davon ausgehen müssen, dass sich dieser Trend auf Tablet-Computern fortsetzen wird.

Tablet-Computer müssen nicht getrennt von Mobiltelefonen betrachtet werden. Tablets unterscheiden sich hauptsächlich in der Größe des Bildschirms, verfügen aber über dieselbe Software, dieselben Betriebssysteme und Prozessoren, sodass die Sicherheitsbedenken nahezu identisch sind. Der einzige Unterschied besteht im Grunde darin, dass einige Tablets wie das Thrive von Toshiba als USB-Master verwendet werden können, wodurch solche Geräte eine größere Angriffsfläche bieten.

Smart-Media-Player (MP3 und Video)

Musik-Player sind normalerweise nicht mit Browsern ausgestattet, sodass das Risiko einer Infektion mit Malware deutlich niedriger ist. Gefährlich wird es, wenn diese Geräte netzwerkfähig und programmierbar sind. Diese Umgebung bietet Raum für Malware.

Es ist jedoch unwahrscheinlich, dass Musik-Player in den Fokus von Angreifern rücken, da auf ihnen normalerweise keine sensiblen Daten gespeichert sind. Der Diebstahl von Musik oder Videos mithilfe von Malware ist noch nicht verbreitet, da diese recht problemlos als Raubkopien erhältlich sind. Mit zunehmenden Beschränkungen durch die digitale Rechteverwaltung (Digital Rights Management, DRM) könnte sich die Situation jedoch ändern. Angriffe auf Unterhaltungsmedien wie Musik, Filme oder Spiele werden unter Umständen wirtschaftlich tragfähiger. Wir gehen davon aus, dass derartige Angriffe auf Geräte abzielen, die DRM nicht unterstützen, auf denen aber trotzdem wertvolle Medien gespeichert sind. Weitere Möglichkeiten bieten Angriffe auf das DRM selbst (über Schwachstellen in seiner Implementierung oder Hardware) sowie Man-in-the-Middle-Angriffe (MITM) bei der Schlüsselverteilung.

Außerdem könnten diese Geräte böswillig zur Schaffung eines Einstiegspunkts in einen Computer oder ein Netzwerk genutzt werden. Die Kompromittierung eines Computers über einen angeschlossenen MP3-Player kann einfacher sein als ein entsprechender Remote-Angriff über ein Netzwerk. Bei einem Angriff, der W32/Stuxnet ähnelte, wurde eine LNK-Schwachstelle für die automatische Ausführung von USB-Sticks ausgenutzt. Ein angeschlossener Medien-Player würde häufig eine umfangreichere Oberfläche nutzen als ein USB-Stick und so eine größere Angriffsfläche bieten.

Angreifer könnten Mediengeräte auch für die Erhaltung oder Verbreitung von Malware missbrauchen. Malware-Würmer können sich verbreiten, indem sie sich auf alle verfügbaren Speichergeräte kopieren und über Mediengeräte auf die gleiche Weise ausbreiten (oder einen bereinigten Computer erneut infizieren), wie dies bei USB-Sticks bereits praktiziert wird. Wir wissen von gut dokumentierten Fällen, in denen Malware über infizierte USB-Sticks verteilt wurde. Es ist vorstellbar, dass auch Medien-Player oder Tablets für diese Zwecke verwendet werden. Übt ein toller neuer Medien-Player nicht den unwiderstehlichen Reiz aus, ihn anzuschließen? Daher kommen solche Geräte ebenfalls für zielgerichtete Angriffe infrage.

7. <http://blogs.mcafee.com/enterprise/mobile/27th-chaos-communications-congress-mobile-security-and-more>

8. <http://www.technologyreview.com/computing/35094/>

Tragbare Spielegeräte

Spielkonsolen sind im Grunde Computer. Viele von ihnen sind inzwischen vernetzt und bieten Internetzugang. Tragbare Spielegeräte wie das Nintendo DS oder die Sony PSP zeichnen sich durch ein Merkmal aus, durch das sie potenziell gefährlicher sind als andere Mobilgeräte: Sie bieten Peer-to-Peer-Funktionen (P2P) für die direkte Kommunikation von Gerät zu Gerät, durch die Spiele mit mehreren Spielern unterstützt werden. Wenn bei diesen Verbindungen die Übertragung von Programmen zulässig ist (was vom Cabir-Wurm auf der Symbian-Plattform bereits ausgenutzt wurde), lassen sich problemlos Würmer implementieren. Selbst wenn die P2P-Kommunikation auf Datenübertragungen beschränkt ist, kann die Ausnutzung von Schwachstellen Remote-Code-Ausführungen und Virenverbreitung ermöglichen.

Neue Spielegeräte nutzen oftmals spieleunabhängige Technologien. Ein Beispiel ist hier die PlayStation Vita mit 3G, WLAN, Bluetooth, GPS, Kameras und Mikrofon.⁹ Die Unterschiede zwischen Spiele- und Mobilgeräten werden sehr schnell geringer.

Gerätevielfalt

Für die Malware-Verbreitung stellt die Mobilgeräte-Vielfalt eine Barriere dar. Aufgrund der vielen Hardware-Modelle und Betriebssysteme ist es kostspieliger, auf mehr als ein Gerät abzu zielen. Wir gehen jedoch von einer zunehmenden Konsolidierung und Standardisierung von Hard- und Software aus. Erste Informationen über das demnächst erscheinende Android Ice Cream Sandwich (ein Android-Betriebssystem für Mobiltelefone und andere Mobilgeräte) sowie Windows 8 (für Multi-Touch-Bildschirme und ARM-Prozessoren) untermauern diese These.

Mit der Standardisierung steigt die Gefahr einer Monokultur (wie bei Windows auf Desktop-Computern) und damit die Anfälligkeit für groß angelegte Angriffe mit vielen gleichzeitigen Zielen.

Vielfalt bietet Schutz vor groß angelegten Angriffen, jedoch keinen vollständigen Schutz für zielgerichtete Malware. Die begrenzte Anzahl von Zielen können Angreifer durch eine Erhöhung ihrer potenziellen Rendite ausgleichen. Hier sind enorme Steigerungen möglich, wenn Angriffe auf sehr wertvolle Ziele gerichtet werden oder der Zeitraum bis zur Erkennung der Malware verlängert wird. Stealth- (oder Rootkit-)Funktionen sowie die komplizierte Erkennung und Entfernung könnten bei der Erreichung dieser Ziele eine wichtige Rolle spielen.

Bisherige Umgebungen

Mobile Geräte waren von Anfang an Ziele für Malware-Angriffe. Proof-of-Concept-Angriffe auf Symbian OS führten schließlich zu tatsächlichen Infektionen und zur Ausweitung von Malware-Risiken.

Symbian-Malware

Nokia und Ericsson waren die ersten Hersteller, die 1996/1997 Smartphones entwickelten. Als „Smartphones“ wurden sie ab dem Jahr 2000 vermarktet und relativ schnell auf Symbian OS standardisiert. Die meisten im Handel erhältlichen Telefone waren damit ausgestattet. Zu den Spitzenzeiten war Symbian auf über 350 Millionen Geräten installiert.

Die ersten Varianten von Proof-of-Concept-Malware für Mobiltelefone nutzten die Unsicherheiten von Symbian OS. (Vor Symbian gab es auch die eine oder andere Malware für Palm OS.)¹⁰

Die Software für Symbian-Telefone wird in Form eines SIS-Pakets (Software Installation Script) bereitgestellt. Für seine Verteilung bestehen verschiedene Möglichkeiten – über Internet-Downloads, per E-Mail, SMS, Bluetooth, Infrarotverbindung, SD-Karten, PC-Verbindung und per Funk.¹¹

Der erste tatsächlich gefundene Virus wurde 2004 gemeldet: Dabei handelte es sich um den Symbian-Wurm Cabir, der per Bluetooth verbreitet wurde.¹² Cabir folgten zahlreiche andere Malware-Familien. Es waren meist Trojaner, und seit 2004 haben wir hunderte Varianten registriert. Der größte Teil dieser Malware gelangte über das Internet auf die Geräte.

9. http://en.wikipedia.org/wiki/PlayStation_Vita

10. <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=98801>

11. http://www.developer.nokia.com/Community/Wiki/Deploy_SIS_file_on_hardware

12. <http://www.f-secure.com/weblog/archives/archive-012006.html>

J2ME-Malware

J2ME, das heute als Java ME (oder JME) bezeichnet wird, ist eine auf Java basierende Programmierumgebung für die Nutzung auf mobilen Geräten und eingebetteten Systemen.¹³ Vor einiger Zeit gab es über zwei Milliarden dieser Geräte, heute wird J2ME jedoch von moderneren Betriebssystemen wie Android abgelöst. (Der Kern von Android ist wie bei J2ME eine virtuelle Maschine auf Java-Basis.)

Die starke Verbreitung von J2ME in den Jahren 2006 bis 2010 zog eine entsprechende Malware-Flut für diese Plattform nach sich. Ganz besonders beliebt waren Trojaner, die Anrufe mit hohen Gebühren tätigten und teure SMS-Nachrichten versendeten.¹⁴ Irgendwann gab es dann so viel J2ME-Malware, dass sie die Zahl der Symbian-Malware überstieg.¹⁵ (Ein großer Teil der Java-Malware sind sprachspezifische Trojaner. Diese Malware-Form war besonders in Russland sehr gängig, weil das Land nur über schwache Vorschriften für die Telekommunikationsbranche verfügt.)

Die erste weit verbreitete Android-Malware (FakePlayer.A) war im Wesentlichen das Android-Gegenstück eines J2ME-Trojaners, der bei kostenpflichtigen Nummern anrief und SMS-Nachrichten versendete. Wahrscheinlich wurde hier der vorhandene Programmcode für Android modifiziert und neu kompiliert.

Android

Im Folgenden wird Android näher besprochen. Es ist das am stärksten wachsende Betriebssystem für mobile Geräte und zieht schon jetzt eine relativ hohe Zahl von Malware an.

Einzigartig

Android hat auf dem Markt eine einzigartige Position. Es ist kostenlos und bietet deshalb ein außergewöhnlich gutes Kosten-Nutzen-Verhältnis. Anbieter und Mobilfunkbetreiber erzielen sehr viel höhere Gewinnspannen, wenn sie Geräte auf Android-Basis verkaufen und unterstützen. Zudem handelt es sich um ein Open-Source-Betriebssystem, d. h. es lässt sich leicht für neue Geräte anpassen. Angesichts dieser Tatsachen ist es nicht überraschend, dass Android den Markt im Sturm erobert hat.

Android ist das am schnellsten wachsende Betriebssystem für Smartphones. Es wurde 2008 erstmals veröffentlicht und ist bereits führend auf dem Markt. In Abbildung 1 ist der Marktanteil des Betriebssystems Ende 2010 zu sehen.

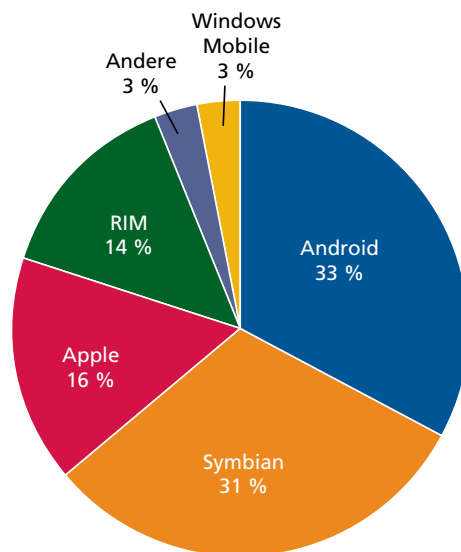


Abbildung 1: Das Android-Betriebssystem macht nach nur vier Jahren den größten Anteil des Smartphone-Kuchens aus.

13. http://en.wikipedia.org/wiki/Java_Platform,_Micro_Edition

14. http://www.securelist.com/en/analysis/204792080/Mobile_Malware_Evolution_An_Overview_Part_3

15. http://www.securelist.com/en/analysis/204792080/Mobile_Malware_Evolution_An_Overview_Part_3

Die Android-Mitbewerber geben natürlich nicht auf. Eine Taktik zur Begrenzung des Android-Erfolgs besteht darin, rechtliche Hürden aufzubauen.¹⁶

Android führt nicht nur hinsichtlich der Anzahl mobiler Geräte, sondern holte Symbian im letzten Quartal leider auch beim Aufkommen neuer Malware-Varianten ein.

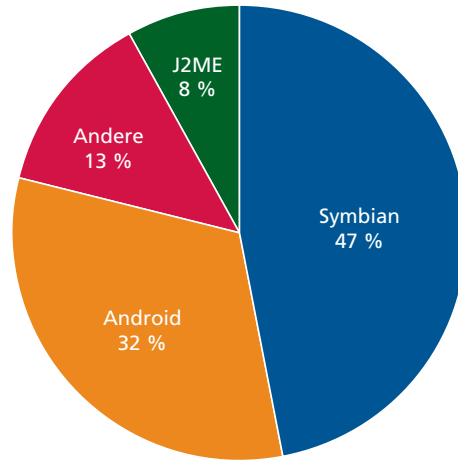


Abbildung 2: Symbian war bisher das bei Malware-Autoren beliebteste Mobilgeräte-Betriebssystem. Android holt jedoch schnell auf.

Abbildung 2 zeigt, dass der Gesamtanteil der Symbian-Malware (zusammengerechnet für alle Jahre) größer ist als der von Android. Wenn wir uns jedoch nur ein aktuelles Quartal ansehen, wird ein weiterer Aspekt der „Marktführung“ von Android deutlich.

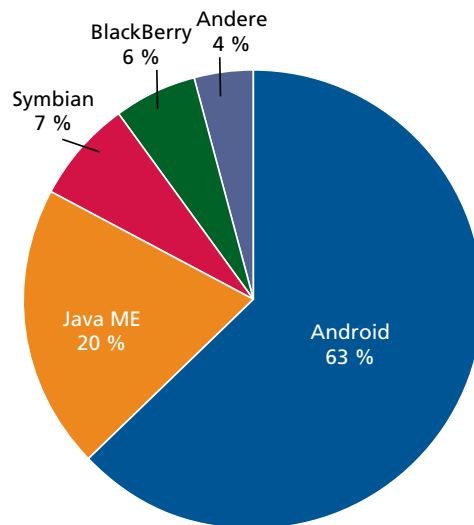


Abbildung 3: Im zweiten Quartal 2011 war das Aufkommen bei Android-Malware größer als das aller anderen Mobilgeräte-Betriebssysteme.¹⁷

Wir sind überzeugt, dass diese explosionsartige Malware-Zunahme durch geänderte Verteilungsmethoden verursacht wurde. In der Vergangenheit wurden die Würmer meistens von einem Gerät zum nächsten übertragen (z. B. über Bluetooth wie beim Cabir-Wurm). Für diese Methode müssen sich viele potenzielle Opfer in allernächster Nähe befinden und bereit sein, eine Übertragung „anzunehmen“. Alternativ musste die Malware von einer Nokia-Webseite (oder von einer anderen Seite, auf der Symbian-Programme angeboten wurden) heruntergeladen werden.

Heute kommen nahezu alle Infektionen von App-Märkten/Stores (dem globalen Android Marketplace und beliebten Drittanbieter-Stores, die zum Teil nur in bestimmten Ländern genutzt werden). Es gibt viele Beispiele für aktuelle Android-Malware. Beschreibungen finden Sie in der McAfee Virus Information-Bibliothek.¹⁸

Sicherheitsmodell

Das Android-Sicherheitsmodell ist einfach: Anwendungen geben bei der Installation an, welche Aktionen sie beabsichtigen (und fordern dafür „Berechtigungen“ an).¹⁹ Der Benutzer kann nun diese Anforderung genehmigen oder ablehnen (und dies nur komplett, denn angeforderte Berechtigungen können nicht einzeln abgelehnt werden). Durch die Genehmigung werden die festgelegten Einschränkungen nach der Installation in Kraft gesetzt. Durch Ablehnen wird die Installation blockiert. Es ist auch nicht möglich, Genehmigungen nach der Installation oder während der Laufzeit zu steuern (also sie weder abzulehnen noch sie zu gewähren).

Dieses Modell ist aus drei Gründen unzureichend:

- Es beruht darauf, dass die Benutzer die richtige Wahl treffen. Dabei sieht die Beschreibung vieler Berechtigungen sogar für technisch versierte Benutzer kryptisch aus.
- Programme fordern zuweilen mehr Rechte als nötig an, sodass die Benutzer an ungewöhnliche und „gierige“ Anfragen gewöhnt sind.
- Benutzer gewähren Berechtigungen eher, wenn sie das Programm unbedingt verwenden möchten. Dieser Wunsch kann durch Social-Engineering-Methoden ausgenutzt werden.

Sicherheits-APIs

Android bietet eine kleine Auswahl an APIs für die Verwaltung des Geräts. Das Betriebssystem kontrolliert die Kennwort-/PIN-Richtlinien und ermöglicht das ferngesteuerte Zurücksetzen des Telefons.²⁰ Leider sind das sehr begrenzte Maßnahmen, die beim Aufbau eines Sicherheitsprodukts zudem wenig hilfreich sind.

Es wäre von großem Vorteil, wenn Android eine Standard-Sammlung universeller Sicherheits-APIs im Betriebssystemkern unterstützen würde (die den Zugriff auf den Kernel-Speicher sowie ein nahtloses Überwachen der Datei-Eingabe/Ausgabe und der Netzwerkdatenströme ermöglichen). Apps mit einem derart umfangreichen Zugriff müssten in besonderer Weise signiert werden. Eine weitere sinnvolle Maßnahme wäre die Einbindung einer Verschlüsselungsauthentifizierung in die Betriebssystem-APIs, sodass Sicherheitsanwendungen den Daten vertrauen können, die sie vom Betriebssystem empfangen (und sicher ist, dass diese nicht manipuliert wurden). Dieser Schritt sollte das Rootkit-Problem auf Android-Geräten verringern und einige MITM-Angriffe ausbremsen.

Schwächen

Bei einer Präsentation auf der DefCon 2011 wurden verschiedene Unzulänglichkeiten im Android-Design und der Dokumentation offengelegt:²¹

- Gegensätzliche und fehlende API-Beschreibungen wirken sich negativ auf die Sicherheit der Anwendungen aus, weil Entwickler falsche Entscheidungen treffen. In Android Version 2.2 wurden nur 78 von 1.207 APIs dokumentiert, sechs davon falsch.
- Das Interprozess-Messaging erfolgt in Android entweder explizit (mit Angabe des Empfängernamens) oder implizit (mit einer spezifischen Meldung ohne bestimmtes Ziel wie „my.special.action“). Diese Unterscheidung sorgt dafür, dass einige Meldungen von Malware abgefangen oder gefälscht werden können, sodass Datenkompromittierung oder DoS-Angriffe möglich werden.
- Speicher (SD-Karten) kann uneingeschränkt ausgelesen werden. Dateien (und Ordnernamen) bleiben auch dann erhalten, wenn die Apps, von denen sie stammen, deinstalliert werden oder das Gerät komplett zurückgesetzt wird.
- Viele Apps fordern mehr Berechtigungen an, als sie benötigen, und verstoßen damit gegen das Prinzip der minimalen Rechtevergabe. Für dieses Problem, das nach Angaben der Autoren 31 Prozent des Apps betrifft, gibt es verschiedene Gründe:
 - » Unzureichende Dokumentation darüber, welche APIs welche Berechtigungen benötigen
 - » Testartefakte: Debugging-Code, der nach der Entwicklung oder den Qualitätstests nicht gelöscht wurde
 - » Fehler, die durch Forumsbeiträge verbreitet werden: Der gleiche unzulängliche Quell-Code wird von Entwicklern immer wieder kopiert und eingefügt, auch wenn er Fehler enthält, die die Autoren nachträglich korrigiert haben.

18. <http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501748>, <http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=509500>, <http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=522281>, <http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=518925>, <http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501599>, <http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501639>, <http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=527859>

19. <http://developer.android.com/guide/topics/security/security.html>

20. <http://developer.android.com/guide/topics/admin/device-admin.html>

21. Tsepenyuk O'Neil, Y. und Chin, E.: „Seven Ways to Hang Yourself with Google Android“ (Sieben Möglichkeiten, sich mit Google Android aufzuhängen), DefCon 19, Las Vegas 2011.

Einem Bericht auf der BlackHat 2011 zufolge, in dem das Verhalten aktiv genutzter und in einer Sandbox ausgeführter Android-Anwendungen zusammengefasst wurde, versenden 8,4 Prozent der Apps IMEI-Daten unverschlüsselt.²² Da die meisten mobilen Geräte personengebunden sind, werden die IMEI meist als personenbezogene Daten eingestuft. Im selben Bericht wird angegeben, dass etwa 22 Prozent der Apps während der Installation den Zugriff auf IMEI anfordern. Der Unterschied zwischen 22 Prozent und 8,4 Prozent untermauert die an früherer Stelle aufgestellte These der „gierigen“ Berechtigungsanforderung.

Dalvik Virtual Machine

Android-Software wird in Form eines APK-Pakets bereitgestellt, das über ein Verzeichnis mit einer Beschreibung der gewünschten Berechtigung verfügt. Wenn Android-Anwendungen während der Installation nicht ausdrücklich den Zugriff auf bestimmte Datenarten oder Operationen anfordern, erhalten sie auch keinen Zugriff darauf. Nach der Installation arbeiten Apps im DEX-Format, das in einer auf Java basierenden Just-in-Time Dalvik Virtual Machine (VM) ausgeführt wird.

Die Prozessisolierung wird über das Betriebssystem realisiert, da die Dalvik-VM die Ausführung nativen Codes zulässt, der im Android-NDK integriert ist. Daher kann die Isolierung nicht durch die VM allein erreicht werden.²³ Alle Arten von Android-Anwendungen (reine Dalvik-Apps, nativ oder gemischt) weisen die gleichen Sicherheitsbeschränkungen auf.

Laut Ausgabe 11 der Microsoft-Analyse zur IT-Sicherheit wurden Windows-Systeme vom dritten Quartal 2010 bis zum zweiten Quartal 2011 in den meisten Fällen über Java-Exploits angegriffen.²⁴ Das zeigt: Sandboxing auf Java-Basis ist eindeutig unsicher. Darüber hinaus sind wir der Meinung, dass einige Exploit-Techniken auch für spätere Dalvik-Angriffe verwendet werden könnten. (Derselbe Bericht enthält die interessante Beobachtung, dass ein Android-Exploit mit dem Namen Lotoor häufig auf PCs gefunden wird. Laut Microsoft gelangt er dort dorthin, weil Benutzer infizierte Apps herunterladen, um sie auf ihre mobilen Geräte zu übertragen.)

Signieren von Anwendungen

Android-Anwendungen müssen signiert werden. Die Zertifizierung durch eine offizielle Stelle ist jedoch keine Pflicht. Deshalb verfügen viele Apps über selbstsignierte Zertifikate. Dieser Mechanismus hilft dabei, gute Software von derselben Quelle zu verfolgen und baut Vertrauen zu dieser Quelle auf. Für die Verfolgung von Malware ist er jedoch nicht geeignet, da Signaturen für diese Anwendungen uneingeschränkt generiert werden können und neue Signaturen keine Informationen über die Glaubwürdigkeit liefern.

Ebenso wie vertrauenswürdige digitale Signaturen unter Windows (die als Authenticode bezeichnet werden) haben auch Zertifikate vertrauenswürdiger Quellen für Android-Apps einen gewissen Wert – selbst dann, wenn sie selbstsigniert sind. Deshalb müssen wir davon ausgehen, dass sie von Malware-Autoren angegriffen werden. Wenn die Angreifer sie stehlen, können sie den Namen einer vertrauenswürdigen Quelle auf ihre eigenen Entwicklungen schreiben, wodurch die Malware schneller verbreitet wird. Wenn viele digitale Schlüssel kompromittiert werden, könnten die am weitesten verbreiteten Schlüssel von den Kriminellen für gezielte Angriffe verwendet werden. Damit steigen die Erfolgchancen für den Angriff.

Unter dem Dach der IEEE haben sich Sicherheits-Software-Hersteller zusammengeschlossen. Ihr Ziel ist die Implementierung des „IEEE Software-Taggant-Systems“.²⁵ (Ein Taggant ist eine Chemikalie, die beispielsweise Plastiksprengstoff zugesetzt wird. Sie hilft bei der Bestimmung der Fabrik, in der der Sprengstoff produziert wurde, und damit bei der Analyse von Sprengstoffpartikeln.) Das IEEE-Taggant-System baut bei der Erstellung automatisch eine kryptografisch starke Markierung in die Software ein und ermöglicht dadurch die Zurückverfolgung jedes Programms zu seiner Quelle. Dadurch bietet das Taggant-System unter anderem zwei Vorteile: Zum einen werden Scans durch Sicherheits-Software beschleunigt. Zudem profitieren Entwickler davon, dass diese Markierungen im Gegensatz zu Authenticode- und anderen Signaturen kostenlos sind. Das Taggant-System sollte dabei helfen können, schlechte Software-Quellen von zuverlässigen zu unterscheiden. Allerdings muss das System in die Entwicklertools integriert werden. Das Taggant-System würde keinen Mehrwert für iOS und/oder Android bedeuten, da hier bereits die App-Signierung erforderlich ist. Jedes andere Betriebssystem kann das System jedoch nutzen, um einen sicheren Reputations-Mechanismus in seine Umgebung einzubinden.

22. Daswani, Neil: „Mobile Malware Madness, and How to Cap the Mad Hatters“ (Mobilgerätewahnsinn und wie sich der Wahnsinn beherrschen lässt)

23. <http://developer.android.com/sdk/ndk>

24. <http://www.microsoft.com/security/sir/default.aspx>

25. http://standards.ieee.org/news/2011/icsg_software.html,

https://media.blackhat.com/bh-us-11/Kennedy/BH_US_11_KennedyMuttik_IEEE_Slides.pdf

iOS, Windows Phone 7 und andere Plattformen

Apple iOS ist derzeit der größte Konkurrent von Android. Apple hat bisher ausgezeichnet für die Sicherheit seiner Geräte gesorgt. Als dieser Artikel verfasst wurde, gab es keine gemeldeten Malware-Fälle für iPhones, bei denen kein Jailbreak angewendet worden war. (Beim Jailbreaking wird das iPhone für nicht autorisierte Apps geöffnet. Dies bedeutet ein Sicherheitsrisiko, weil es die Ausführung nicht signierter Software ermöglicht.) Den Sicherheitsrisiken im iPhone-Bereich werden wir uns in den folgenden Kapiteln widmen.

Abgesehen von Android und iOS können auch andere Betriebssysteme in Zukunft eine wichtige Rolle spielen. Da sich diese Betriebssysteme noch in der aktiven Entwicklung befinden, halten wir uns mit unserer Analyse ihrer Sicherheitsrisiken noch zurück. Dies sind die bekanntesten Initiativen:

- Windows Phone 7.²⁶ Nokia hat sich entschlossen, dieses Betriebssystem für seine zukünftigen Geräte zu nutzen. Eine IDC-Studie prognostiziert, dass Windows Phone 20 Prozent des Marktanteils erzielen und enger Verfolger des Apple- als auch des RIM-Betriebssystems werden wird.
- Samsung Bada²⁷ hat einen winzigen Marktanteil. Allerdings arbeitet Samsung zusammen mit Intel an der Entwicklung von Tizen²⁸, das wahrscheinlich mit MeeGo zusammengefasst wird²⁹.
- WebOS³⁰.
- Cloud-basierte Betriebssysteme wie Google Chrome OS³¹.

Aktuelle und künftige Ökosysteme

Beschäftigen wir uns nun mit den Umgebungen, in denen Mobilgeräte eingesetzt werden. Die Sicherheit jedes Geräts wird nicht nur durch die Robustheit seiner Software, sondern auch vom gesamten Ökosystem bestimmt, in dem es genutzt wird. Aus Sicherheitssicht umfasst dieses System Schutzmaßnahmen in der Hardware, im Betriebssystem (und jeder beliebigen App mit Berechtigungen, die als Root-Konto ausgeführt wird), im Betriebssystem-Aktualisierungsvorgang sowie in externen Ressourcen (z. B. App Stores), die ein Gerät kontaktiert.

Sicherheit der Ökosysteme

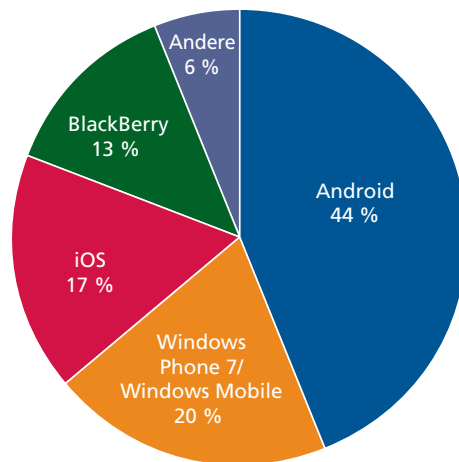


Abbildung 4: Diese IDC-Studie von Juni 2011 enthält eine Prognose der Anteile der im Jahr 2015 ausgelieferten Mobilgeräte-Betriebssysteme.³²

Für einen aussagekräftigen Sicherheitsvergleich der heutigen Smartphones genügt es nicht, sich lediglich die jeweiligen Betriebssysteme anzusehen und die Implementierung ihrer Sicherheitsfunktionen auszuwerten.³³ Mobilgeräte sind darauf ausgelegt, Verbindungen herzustellen. Sie funktionieren in zahlreichen Netzwerken (mit deren Anzahl auch das Risiko steigt) und laden Programme aus dem Internet herunter.

26. www.microsoft.com/windowsphone

27. [http://en.wikipedia.org/wiki/Bada_\(operating_system\)](http://en.wikipedia.org/wiki/Bada_(operating_system))

28. <http://en.wikipedia.org/wiki/Tizen>
<https://www.tizen.org/>

29. <https://meego.com/>, <http://en.wikipedia.org/wiki/MeeGo>

30. <http://en.wikipedia.org/wiki/WebOS>

31. http://en.wikipedia.org/wiki/Google_Chrome_OS

32. <http://www.idc.com/getdoc.jsp?containerId=prUS22871611>

33. http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

Der Vergleich muss die gesamten Umgebungen berücksichtigen:

- Android OS und Android Market
- iOS und der App Store von Apple

Viele Hardware-Hersteller nehmen ihre eigenen, zum Teil sicherheitsbezogenen Änderungen an dem von Google bereitgestellten Open-Source-Kern vor und erhöhen so die Komplexität des Android-Geräts. Hierdurch wird der Betriebssystem-Speicherplatz in viele proprietäre Teilbereiche fragmentiert, die parallel zum Kernbetriebssystem (und gewöhnlich mit Verzögerungen) verwaltet werden. In einer solchen Situation nehmen Betriebssystem-Aktualisierungen von diesen Herstellern mehr Zeit in Anspruch, da HotFixes für den Android-Kern in angepasste Betriebssystemversionen ein- und anschließend separat ausgebracht werden müssen. Mit der Einführung von Android Ice Cream Sandwich (AICS) wird dieses Problem möglicherweise behoben. Der Einfluss von AICS lässt sich allerdings erst beurteilen, wenn es zur gängigen Betriebssystemvariante wird.

Die vielleicht wichtigsten Elemente im Ökosystem jedes Mobilgeräts sind sein App Store und die Herkunft seiner Software-Aktualisierungen.

App Stores

Die Software-Verteilung für Smartphones unterscheidet sich erheblich von der für Desktop-Computer. Dabei stellt die Bindung von Benutzern eines bestimmten Anbieters an dessen internetbasierten Marktplatz einen wichtigen mobilen Trend dar. Dieser lässt sich relativ einfach umsetzen, da die Bindung an ein bestimmtes GSM-/3G-Netz von den Mobiltelefonkunden inzwischen akzeptiert wird. Die Anbieter erhalten durch die Bindung von Mobilgerätekunden an ihre Marktplätze (oder App Stores) einen klaren finanziellen Anreiz, der sich potenziell auch positiv auf die Sicherheit auswirken kann: Wenn ein Großteil der Software aus einer einzigen Quelle stammt, kann dies die Prüfung von Programmen und die Entfernung von unerwünschten Inhalten vereinfachen.

Zur Bindung von Kunden an einen Marktplatz setzen Anbieter unter Umständen auf die digitale Anwendungssignatur – und damit im Endeffekt auf eine Form von DRM. Andernfalls können leicht austauschbare Inhalte wie Software dazu führen, dass die Anbieter Probleme durch Piraterie bekommen. Apple setzt auf diesen Ansatz: Nur auf iPhones im Jailbreak-Modus können nicht von Apple signierte Programme ausgeführt werden.

Smartphone-Anbieter setzen viel daran, sich als „den sichersten Anbieter“ bezeichnen zu können. Dieser Wettbewerb lässt hoffen, dass den Anbietern die Mobilgeräte-Sicherheit am Herzen liegt.

Angesichts der zentralen Software-Verteilung und des starken Engagements bei der Bereitstellung eines sicheren Ökosystems sollten die Anbieter die Zahl der Malware durch Filterung der an ihre Online-Stores eingesendeten Apps eigentlich unter Kontrolle halten können (ein Ziel, das bei einer dezentralisierten Software-Verteilung nahezu unerreichbar wäre). Dennoch passen sich die Kriminellen immer schnell an neue Umgebungen an.

Reaktiv oder proaktiv?

Die Software-Verteilung für Mobilgeräte wird durch den App Store von Apple und Android Market von Google dominiert. Sie setzen vollkommen unterschiedliche Richtlinien und Filterungsmethoden ein.

- Bei der streng zentralisierten Verteilung von Apple kann eine neue App nur auf zwei Arten bezogen werden:
 - » Durch einen Download aus dem App Store.
 - » Über den iOS-Dienst Mobile Device Management zur Verwaltung von Mobilgeräten (für den eine Genehmigung von Apple erforderlich ist).³⁴ Jedes legitime Unternehmen kann seine Software auf diese Weise verteilen.
- Google stellt die Inhalte in Android Market bereit und kontrolliert sie auch darüber. Diese Plattform ist sehr beliebt, doch kann jedes Gerät auch Anwendungen aus Märkten von Drittanbietern im Internet oder mittels Browser ein APK (Android Package File) von einer URL herunterladen.

Der Apple Store wird strenger kontrolliert und ist – zumindest vorerst – sicherer. Bei Android ist die Software-Verteilung offener, weshalb sie bereits etliche Male durch Malware in Mitleidenschaft gezogen wurde. Als Beispiel sei hier der DroidDream-Vorfall im Frühjahr 2011 genannt, als über 50 legitime Anwendungen verteilt wurden, die mit Malware infiziert waren.³⁵ Diese Apps erfassten Informationen und warteten auf Anweisungen von einem Befehls-Server, wiesen also ein typisches Botnet-Verhalten auf. DroidDream war der erste große Trojaner-Angriff, der sich gegen einen beliebten Marktplatz für Apps richtete. Google musste über 50 böswillige Apps aus Android Market entfernen.

Apple verfolgt einen proaktiven Ansatz und legt den Schwerpunkt auf Prävention. Die Zielsetzung von Google besteht offenkundig darin, die Entwicklung von Apps zu fördern und sich erst beim Auftreten von Problemen – also reaktiv – um diese zu kümmern. Der Google-Ansatz mag zur Generierung einer großen Anzahl und Vielfalt von Apps sinnvoll sein. Doch unter Sicherheitsgesichtspunkten schafft er genau die Art von Umgebung, in der sich Malware-Banden wohlfühlen.

Die Anzahl der Malware in einem Online-Store hängt offenkundig davon ab, wie gut die Filter (sowie die darin integrierten Qualitäts- und Sicherheitsprüfungen) zulässige Apps erkennen können. Angreifer beziehen auch die für jede Umgebung mögliche Rendite in ihre Erwägungen ein. Hierzu zählt der zeitliche und finanzielle Aufwand, der erforderlich ist, um Malware durch einen entsprechenden Filter zu schleusen.

Das Angebot von Google wird im Hinblick auf die Software-Vielfalt wahrscheinlich recht bald das von Apple übertreffen. Doch auch wenn die Kunden eine breite Auswahl zu schätzen wissen, möchten sie auch auf eine sichere Umgebung zugreifen. Es ist nicht leicht, diese beiden Ziele gleichzeitig zu erreichen. Daher müssen die Anbieter unter Umständen erheblich investieren, um ihre Ökosysteme frei von Malware zu halten. Kleinere Mitbewerber werden es wahrscheinlich schwer haben, mit den großen Anbietern zu konkurrieren, weil der Aufwand bei der Implementierung wirksamer Software-Filter ihre Betriebskosten zu sehr erhöhen würde.

Angriffe auf Internetmarktplätze

Die Manipulation von App Stores läuft wahrscheinlich ähnlich ab wie der Missbrauch von Suchmaschinen, durch den URLs bei Internetsuchen in den Suchergebnissen ganz oben angezeigt werden.³⁶ Durch die Angriffe würden die Bewertungen ausgewählter Anwendungen in App Stores künstlich erhöht, um mehr Benutzer dazu zu bringen, sie herunterzuladen. Da für legitime Software sowie Malware dieselben Methoden verwendet werden können, wird es fast unmöglich sein, von Malware-Autoren initiierte Angriffe auf das Ranking von Anwendungen zu ermitteln.

Es gab Angriffe, bei denen legitime (und in der Regel beliebte) Apps mit Malware oder Werbung neu aufgesetzt und – manchmal in einem anderen Marktplatz – erneut zum Benutzer-Download hochgeladen wurden.³⁷ Solche Neuveröffentlichungen gehen unter Umständen auch mit einer Änderung der App-Identität (Name/Symbol/Autor) einher. Gelegentlich behalten die Angreifer die Original-Software absichtlich bei, um vorzugeben, dass sie aus einer seriösen Quelle stammt. Übernommen werden auch die digitale Signatur und die Identität des ursprünglichen Autors, dessen Software jetzt als attraktive Komponente in einem böswilligen Paket enthalten ist.

Wir gehen auch davon aus, dass Malware-Funktionen (wie böswillige Datenkompromittierungen, die Benutzerdaten stehlen) in an sich nützliche Anwendungen eingebettet werden. Einige dieser Anwendungen werden eventuell sogar kostenpflichtig sein. Hierdurch könnten Malware-Autoren zweifach profitieren: einmal durch die Gebühren für die App und einmal durch die gestohlenen Daten. Findet der Diebstahl unverdächtig im Verborgenen statt, so kann er, nachdem diese Doppelzweck-Software erst einmal durch die App Store-Filter geschlüpft ist, lange von der Sicherheits-Software unentdeckt fortgesetzt werden. Beispielsweise lässt sich Doppelzweck-Software so programmieren, dass die gestohlenen Daten nur übertragen werden, wenn sie wertvoll genug sind, damit sich das Risiko einer Offenlegung lohnt. Soweit wir wissen, könnten einige Anwendungen im App Store über verborgene böswillige Funktionen verfügen. In Anbetracht der Tatsache, dass Apple bislang alle iPhones mit Ausnahme der per Jailbreak geöffneten erfolgreich schützen konnte, ist diese Art von Angriff auf den App Store wahrscheinlich der wahrscheinlichste Vektor.³⁸

Obwohl die Architekturen von App Stores robuster gegen die massenhafte Malware-Verteilung werden, gehen wir davon aus, dass sie weiterhin gezielt und mit Erfolg angegriffen werden. Malware-Entwickler könnten beispielsweise eine Anwendung mit verborgener Funktionalität veröffentlichen, Benutzer zu deren Installation verleiten und dann die verborgene böswillige Funktion aktivieren. Die Entfernung von derart präparierter Software aus App Stores würde sich ausgesprochen schwierig gestalten.

Falls böswillige Angriffe auf App Stores zu schwierig werden (was sehr unwahrscheinlich ist), könnten Malware-Banden ihre Malware in von legitimen Unternehmen entwickelte Anwendungen injizieren, indem sie deren Desktop-Computer infizieren und die in Entwicklung befindliche Software verändern. Dies wird vermutlich nicht sehr oft geschehen. Wenn doch, kann es eine sehr weit reichende und schnelle Verteilung von Malware ermöglichen.

Kriminelle versuchen häufig, durch Schwachstellenausnutzung oder Verteilung einer nur geringen Anzahl von Malware über App Stores unbemerkt zu bleiben. Diese Strategien waren in der Vergangenheit erfolgreich. Es gibt keinen Grund, warum sie nicht auch in der mobilen Welt funktionieren sollten. Dabei handelt es sich jedoch um anspruchsvollere Alternativen zur Infizierung von Marktplätzen, sodass wir bis zu dem Punkt, an dem sich die Betreiber der App Stores mit der Bereinigung ihrer Märkte gegenseitig übertreffen, wahrscheinlich nicht viel davon bemerken.

36. http://en.wikipedia.org/wiki/Search_engine_optimization

37. <http://www.home.mcafee.com/VirusInfo/VirusProfile.aspx?key=363542>

38. <http://blogs.mcafee.com/mcafee-labs/get-out-of-jail-not-so-free>

DRM und Fernsteuerung

Alle gängigen mobilen Betriebssysteme erfordern digitale Signaturen für Anwendungen und können die Software-Verbreitung beschränken und steuern (wobei die Steuerung im Grunde eine Form von DRM ist, das normalerweise zur Vermeidung der Verteilung von Filmen und anderen Unterhaltungsmedien eingesetzt wird). Google hat die in Android integrierte Funktion zur Remote-Entfernung von Anwendungen nach einem Malware-Ausbruch bereits eingesetzt, um auf Geräten installierte Trojaner zu löschen.^{39, 40}

Zur Blockierung von schädlichen Aktivitäten und zur Schadensbeseitigung kann Google mehrere Beschränkungen implementieren:

- Entfernung einer App aus Android Market (wobei Google nur seinen eigenen Store kontrolliert – Märkte von Drittanbietern sind hiervon nicht abgedeckt)
- Remote-Entfernung bereits installierter Apps
- Verteilung eines speziellen Android-Sicherheitstools auf die infizierten Geräte
- Blockierung von Google-Konten, die in Zusammenhang mit einer böswilligen App stehen

Selbstverständlich riskiert Google, bei der Implementierung all dieser Maßnahmen Fehler zu machen. So wurden bereits Bedenken im Hinblick auf den Verlust von Google-Konten und der damit verknüpften Daten geäußert.⁴¹ Bei einem falschen Alarm wegen einer App könnte Google ein Benutzerkonto, das in Zusammenhang mit dieser App steht, auf die Blacklist setzen oder entfernen. Dies hat Konsequenzen, die weit über das normalerweise mit Falscherkennungen in Sicherheits-Software verbundene Maß hinausgehen.

Soweit uns bekannt ist, musste Apple noch keine Remote-Entfernung von Apps vornehmen (und angesichts einiger Datenschutzprobleme wäre Zurückhaltung bei der Verwendung dieser Funktion plausibel). Wir wissen jedoch, dass iOS über dieselbe Remote-Entfernungsfunktion verfügt. Sie wurde von Entwicklern von Jailbreaking-Routinen für iOS gefunden.

Entwickler

Die Software in den App Stores wird von Entwicklern erstellt. Aufgrund der digitalen Signatur von Apps sind auch sie Teil des Ökosystems und eng mit den Märkten verbunden.

Die Bewertungen und das Ranking der Software (und der Entwickler) in App Stores sowie in beliebten externen App-Ranking-Webdiensten sind für Kunden wahrscheinlich ausschlaggebend bei der Entscheidung, welche Anwendungen sie installieren. Bewertungen werden zu einem Wirtschaftsgut – und damit zu einem Ziel für Malware-Banden. Wahrscheinlich werden auch Sekundärmärkte entstehen, auf denen Bewertungen gehandelt werden.

Folglich gehen wir davon aus, dass Entwickler zum Ziel böswilliger Angriffe werden. Vor kurzem wurde ein derartiger Angriff auf das Symbian-Forum gemeldet. Die Anmeldedaten zahlreicher Entwickler wurden kompromittiert.⁴² Da einige Entwickler auf mehreren mobilen Plattformen tätig sind, hat diese Sicherheitslücke möglicherweise nicht nur Auswirkungen auf Symbian, sondern beispielsweise auch auf Android und iOS. Gestohlene Identitäten (oder sogar identische Anmeldedaten auf mehreren Webseiten) können den Malware-Banden den Missbrauch des Rufes von Entwicklern legitimer mobiler Apps vereinfachen.

Alternativen

Die Einführung von HTML5 hat das Potenzial, die derzeit von Apple und Google dominierte App Store-Umgebung aufzumischen.⁴³ Mit diesem neuen HTML-Standard ist es möglich, Inhalte wie Video- oder Audiodateien nicht über spezialisierte Apps, sondern über den Browser bereitzustellen. Über HTML5 können Apps betriebssystemspezifische Oberflächenelemente verwenden und daher wie native, nahtlos integrierte Apps genutzt werden.

Für einige unabhängige Entwickler könnte es wirtschaftlich sinnvoll sein, zentrale App-Marktplätze (in denen für alle Verkäufe eine Gebühr fällig wird) zu umgehen und ihre Inhalte über HTML5-fähige Browser zu verteilen.⁴⁴ Dies wiederum wird wahrscheinlich dazu führen, dass anstelle angepasster Apps vermehrt HTML5 für die Bereitstellung von Inhalten eingesetzt werden wird.

39. <http://android-developers.blogspot.com/2010/06/exercising-our-remote-application.html>

40. <http://blogs.mcafee.com/enterprise/mobile/google-tool-cleans-up-mobile-malware-dream>

41. <http://www.itworld.com/it-managementstrategy/187543/when-google-kills-your-account-what-happens-your-android-phone>

42. <http://www.infosecurity-us.com/view/20396/nokia-shuts-down-developer-site-after-members-data-was-compromised/>

43. <http://en.wikipedia.org/wiki/HTML5>

44. <http://www.zdnet.com/blog/btl/amazons-cloud-reader-beginning-of-the-html5-surge-vs-apples-app-store-vig/54587?tag=nl.e539>

Entwicklungen und Prognosen

In diesem Kapitel betrachten wir den aktuellen Stand böswilliger Software und wie die Besonderheiten mobiler Geräte die Möglichkeiten der Kriminellen erweitern.

Der finanzielle Anreiz

Die Motivation hinter dem Großteil der von McAfee Labs entdeckten Malware ist ganz eindeutig das Geld. Es gibt viele Möglichkeiten, Malware-Operationen zu einem einträglichen Geschäft zu machen. Leider gehören auch Mobilgeräte dazu.

Man-in-the-Browser-Angriffe

Der Diebstahl oder die Manipulation von Finanzinformationen im Browser während einer Online-Banking-Sitzung ist eine der bekanntesten Funktionen von PC-Malware. Einige dieser Trojaner können ihre böswilligen Transaktionen vollständig vor den Benutzern verbergen. Wenn die Kompromittierung von Smartphone-Browsern genauso einfach wäre, würde dies mit Sicherheit zu weitaus häufigeren Angriffen führen. Glücklicherweise ist dies aber noch nicht der Fall. Die Mobilgeräte-Betriebssysteme iOS und Android bieten eine zuverlässige Prozessisolierung. Lediglich im Fall einer Kompromittierung des Betriebssystems und der Ausführung der Malware mit Root-Rechten ist die Browser-Kommunikation für andere Programme sicht- oder manipulierbar.

Multiplattform-Bedrohungen (Zeus und SpyEye)

Einige Mobiltelefone bieten mittlerweile zusätzlichen Online-Banking-Schutz.⁴⁵ Diese Sicherheitsmaßnahmen verfolgen einen doppelten Ansatz:

- Sie erfordern zusätzliche Anmeldeinformationen (doppelte Authentifizierung).
- Sie informieren den Benutzer (z. B. per SMS-Nachricht) über Transaktionen oder den Kontostand.

Im Jahr 2010 führte der Trojaner Zitmo für Android einen erfolgreichen Angriff auf die doppelte Authentifizierung durch.⁴⁶ Zitmo, das für „Zeus in the Mobile“ steht, ist eine Erweiterung der PC-basierten Zeus-Banking-Trojaner-Familie.

Der Trojaner Spitmo („SpyEye in the Mobile“) für Android erschien im September 2011 und greift ebenfalls die doppelte Authentifizierung an. Er gehört zu einer weiteren großen Familie von PC-Banking-Trojanern.⁴⁷

Premium-Anbieter und SMS-Nachrichten

Eine der einfachsten Möglichkeiten, Profit aus Malware-Angriffen auf Mobilgeräte zu schlagen, ist das Absetzen eines Anrufs oder einer SMS-Nachricht (Short Message Service) an Premium-Anbieter. Wenn diese Aktionen unregelmäßig (z. B. einmal wöchentlich in der Nacht) und versteckt erfolgen (durch Löschung der Protokolle und Nutzung der Tarnfunktionen von Rootkits), bleiben sie oft lange unentdeckt.

Die Erfassung derartiger Aktivitäten sollte eigentlich relativ einfach sein, da alle Netzanbieter über Listen von Unternehmen mit Premium-Nummern verfügen sollten und die Geldflüsse nachvollzogen werden können. Tatsächlich wird diese Aufgabe jedoch häufig erschwert, wenn Anrufe und SMS-Nachrichten ins Ausland gehen. Einige Länder handhaben Missbrauchsfälle relativ lax, vor allem wenn die Aktivitäten zwischenzeitlich eingestellt wurden (was häufig der Fall ist). Wie bereits erwähnt, waren böswillige SMS-Dienste in Ländern wie Russland auf J2ME besonders häufig vertreten. Der Hauptgrund für die Beliebtheit dieser Malware ist ihre Fähigkeit, heimlich SMS-Nachrichten zu senden. In diesem Fall ist Android riskanter als iOS, da die Berechtigungen in Android einmal während der Installation festgelegt werden und anschließend nicht mehr dynamisch geändert werden können. (Eine externe Prüfung mit einem Tool wie App Alert ist eine Möglichkeit, diese Funktion zu überwachen.)⁴⁸

Microsoft Windows 8 soll Unterstützung für SMS sowie für mobile Dienste bieten. Es sind zwar noch keine vollständigen Details bekannt, doch es ist vorstellbar, dass Malware auf einem PC über ein per Bluetooth angeschlossenes Mobiltelefon SMS-Nachrichten (oder Anrufe) absetzen kann. Wir werden das sobald wie möglich genauer untersuchen.

Near-Field Communication

Mobilgeräte benötigen für Geldtransaktionen per NFC (Near-Field Communication) besondere Hardware. Die Reichweite von NFC ist auf wenige Zentimeter beschränkt.

45. <http://blogs.mcafee.com/mcafee-labs/mobile-reunion-hackers-and-banks>

46. <http://blogs.mcafee.com/mcafee-labs/dissecting-zeus-for-android-or-is-it-just-an-sms-spyware>,
<http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=290717>

47. <http://blogs.mcafee.com/mcafee-labs/spitmo-vs-zitmo-banking-trojans-target-android>

48. <https://market.android.com/details?id=com.mcafee.mobile.privacy>

Es gibt zwei gebräuchliche Methoden zur Verhinderung von NFC-Missbrauch:

- Beschränkung der Größe der Transaktionen. (Die durchschnittliche NFC-Transaktion in Großbritannien liegt bei weniger als 5 £, nach aktuellem Wechselkurs weniger als 6 EUR.)
- Blockierung von Nur-NFC-Profilen, um zu verhindern, dass gestohlene Karten ohne PINs, Signaturen oder Identifizierungsmaßnahmen jeglicher Art verwendet werden können.

Diebe könnten jedoch besondere Geräte entwickeln, die die Reichweite von NFC in belebten Gebieten (Flughäfen, Nahverkehrsmittel, Theatern, Kinos, Stadien usw.) erhöhen und kurzzeitig genutzte Händlerkonten speziell zum Skimming verwenden. Wir gehen davon aus, dass mit solchen Angriffen zu rechnen ist, sobald genügend Geräte für NFC-Bezahlung, Kreditkarten, elektronische Geldbörsen (E-Wallets) und Bitcoins ausgerüstet sind.

Auf vielen Telefonen sind Finanzdaten gespeichert (entweder direkt oder in Form gespeicherter Anmeldeinformationen für Banking-Webseiten). Sobald sich E-Wallets durchsetzen, werden Diebe mit Sicherheit nach Möglichkeiten suchen, diese leerräumen. Die Sicherheitsrisiken von E-Wallets sind mindestens vergleichbar mit PIN-geschützten Kreditkarten. Möglicherweise sind sie sogar als noch höher einzustufen, da die Angriffe über Software auf dem Gerät erfolgen.

Android-Apps, in denen Bitcoins (eine Art Online-Geld) gespeichert sind, existieren bereits jetzt schon, und diese Art von virtuellem Geld kann beispielsweise in NFC-Transaktionen umgesetzt werden.⁴⁹ Bitcoin-Transaktionen auf Grundlage von QR-Codes (Quick Response) sind ebenso möglich.⁵⁰

Der Verlust von Finanzdaten oder Geld kann schwerwiegende Auswirkungen auf die Besitzer haben. Daher sollten auf Mobilgeräten strenge Maßnahmen zum Schutz vor Datenkompromittierung (Data Loss Prevention, DLP) eingesetzt werden, um die Risiken überschaubar zu halten. (DLP-Software dient normalerweise als Sicherheitsnetz, um den Verlust wichtiger Daten zu verhindern, wenn ein Computer trotz anderer Schutzmaßnahmen kompromittiert wird. Es handelt sich also letztendlich um ein Mittel zur Schadensbegrenzung.)

Einige Daten (z. B. Geschäftsgeheimnisse) können für Angreifer sehr wertvoll sein, jedoch wenig unmittelbaren Gewinn versprechen, da die Diebe erst den richtigen Käufer finden müssen und damit ein Risiko eingehen. Diese Gefahr macht Bitcoins umso beliebter, da solche digitalen Ressourcen schwer nachzuverfolgen sind. Nicht einmal herkömmliche Handlanger werden mehr benötigt, um direkten Zugang zu den Gewinnen durch gestohlene Bitcoins zu erlangen. Wenn sich diese virtuelle Währung durchsetzt, müssen wir damit rechnen, dass sie in der Aufmerksamkeit von Kriminellen einen höheren Platz einnimmt.

Konnektivität

Nach dem Überwinden der Sicherheitsmaßnahmen auf einem Smartphone stehen den Malware-Entwicklern viele Möglichkeiten offen. Sehen wir uns die verschiedenen Konnektivitätsmöglichkeiten mobiler Geräte genauer an.

Femtozellen

Femtozellen sind eine kostengünstige Möglichkeit, die Abdeckung des Mobilnetzwerks zu erweitern, indem eine kleine Mobiltelefon-Basisstation mit einer Reichweite von 10 bis 30 Metern aufgestellt wird.⁵¹ Diese Geräte können zu Hause oder in kleinen Büros eingesetzt werden. Femtozellen verbinden sich über das Internet mit der Infrastruktur des Netzanbieters. Es handelt sich meist um kleine, vorkonfigurierte Geräte mit einem Ethernet-Anschluss und einem Netzstecker. Femtozellen sind für die Netzanbieter sehr attraktiv, da sie auf diese Weise selbst in Gebieten Netzabdeckung bieten können, in denen das Signal der großen Mobilfunkmasten schwach und das Aufstellen weiterer Masten unrentabel ist. Zudem bringt der Verkauf von Femtozellen den Netzbetreibern zusätzliche Gewinne.

Weitere Zellentypen und ihre Reichweite:

- Mikrozellen: weniger als zwei Kilometer
- Pikoellen: weniger als 200 Meter
- Femtozellen: ca. 10 Meter (AT&T bezeichnet seine Produkte in dieser Reihe als Mikrozelle)

Leider birgt der Einsatz von Femtozellen erhebliche Sicherheitsrisiken. Im Wesentlichen handelt es sich um kleine Mobilfunkmasten zum Preis von 100 bis 200 US-Dollar, die per Reverse-Engineering untersucht werden können. Sie kommunizieren über das Internet (per TCP/IP) mit der Infrastruktur des Netzbetreibers und können – sofern sie nicht sehr gut abgesichert sind – auf vielfältige Weise missbraucht werden. Die offensichtlichste Angriffsmethode ist der Aufbau einer gehackten Femtozelle in der Nähe eines Wohnhauses oder eines Büros, um eine Man-in-the-Middle-Attacke auf alle mobilen Kommunikationswege durchzuführen. Auf diese Weise ist der vollständige Zugriff auf alle Sprach- und SMS-Verbindungen aller mit dieser Zelle verbundenen Geräte möglich.

Einige Netzbetreiber geben – möglicherweise aus Sicherheitsgründen – keine Femtozellen an ihre Kunden heraus. Auf der BlackHat-Konferenz 2011 wurden zahlreiche Schwachstellen bei einem bestimmten Femtozellen-Modell vorgeführt (das ein proprietäres eingebettetes Linux ausführt und in Frankreich 99 EUR kostet).⁵² Eines der Probleme mit diesem Modell ist die vollständige Löschung der lokalen Konfiguration nach einem Zurücksetzen auf die Werkseinstellung. Anschließend wird das Gerät vollständig neu konfiguriert. Diese Zurücksetzungen können mehrfach durchgeführt werden und erlauben eine genaue Analyse des Datenaustauschs während der Initialisierung. Auf diese Weise wird auch Reverse Engineering möglich. Dieses Modell tauscht beispielsweise Zertifikate mit der Infrastruktur eines Netzanbieters aus, prüft dabei jedoch nicht die Authentizität des Anbieters. Außerdem erfolgt die Übertragung des Schlüssels für die zukünftige Verschlüsselung im Klartext.

Femtozellen werden häufig mithilfe des TR-069-Protokolls fernverwaltet. Dieser Dienst kann ebenfalls verwundbar sein.⁵³

Ein allgemeines Problem bei eingebetteten Geräten wie Femtozellen besteht darin, dass diese meist im Root-Modus ausgeführt werden. Ein erfolgreicher Exploit erhält also Vollzugriff auf das Gerät. (Es ist dann nicht mehr notwendig, nach weiteren Schwachstellen zu suchen, mit denen die Berechtigungen hochgesetzt werden können.) Anweisungen zum erfolgreichen Einbruch in bestimmte Femtozellen-Modelle finden sich online. Zudem gibt es mehrere Implementierungsschwachstellen.

Femtozellen haben auch Datenschutzprobleme. Beispielsweise können sie (zu Lokalisierungszwecken) eine Liste aller nahen Funkmasten enthalten. Sie speichern auch die Subscriber-ID (IMSI) sowie die Telefon-ID (IMEI). Bei einigen Femtozellen erfolgt die Konfiguration über eine Webseite. Wenn dieser Web-Zugang offen, schwach geschützt oder gecrackt ist, können die Auswirkungen schwerwiegend sein. Auf der BlackHat-Konferenz 2011 wurde ein weiteres Datenschutzproblem angesprochen: Bei einem bestimmten Femtozellen-Modell wird das gespeicherte Protokoll als unverschlüsseltes Paket in regelmäßigen Zeitabständen per FTP an den Betreiber gesendet. Zu den gesendeten Daten gehören auch Informationen zu den Aktivitäten aller Benutzer.

Speichergeräte

Speicher-Hardware bietet einen weiteren Verbreitungsvektor für Malware. So kann eine SD-Karte mit einem Programm oder einem Installationspaket (z. B., wenn der Besitzer kurz abgelenkt ist) einfach in die meisten Geräte eingesteckt und dort belassen werden. Es kann eine Weile dauern, bis einige der Programme auf der Karte ausgeführt (oder die Dateien mit den Exploits geöffnet) werden. Dieser Ansatz eignet sich ideal für gezielte Malware. Die gestohlenen Daten können später durch Entnehmen der SD-Karte in den Besitz der Kriminellen gebracht werden.

Wir empfehlen strikte Sicherheitsmaßnahmen für die physische Sicherheit von SD-Karten (d. h. das Erschweren des Einsteckens und Entfernens der Speicherkarten) oder sogar eine stärkere Kontrolle durch das Betriebssystem, um die Manipulation der Medien zu verhindern.

Einige SD-Karten dienen zur dauerhaften Erweiterung des Speicherplatzes in einem Gerät. Sie fungieren als Festplatte und sollten entsprechend geschützt werden, zum Beispiel durch die vollständige Verschlüsselung des Karteninhalts mit modernen kryptographischen Verfahren).

Android-Telefone würden zweifellos von einer Funktion profitieren, die Zugangskontrollen sowie die Verschlüsselung der Anwendungsdatendateien auf SD-Karten (oder beliebigen anderen Wechselmedien) bietet.

Eine weitere Bedrohung für Mobilspeicher (internen Speicher, SD-Karten oder beides) entsteht durch das Verbinden mit einem PC. Wenn ein Mobilgerät als „Slave“ (meist per Mikro-USB-Anschluss) an einen Laptop oder Desktop angeschlossen wird, kann sein interner Speicher von Windows als externes Laufwerk genutzt werden. Dadurch steht das Gerät für einige Angriffsmethoden (z. B. Autostart-Schwachstellen oder die LNK-Schwachstelle, die vom Stuxnet-Wurm ausgenutzt wurde) ungeschützt offen, die automatisch Malware auf einem PC ausführen können. Die Gefahr ist gegeben, sobald eine Kabelverbindung hergestellt oder die SD-Karte in den PC eingesteckt wird. Wenn die Malware nicht automatisch ausgeführt wird, können die Angreifer das böswillige Programm einfach auf einer SD-Karte speichern und hoffen, dass es irgendwann auf einem PC ausgeführt wird. Dieser Ansatz vergrößert das Ausmaß einer Mobilgeräte-Kompromittierung.

Bluetooth

Vor kurzem wurden Möglichkeiten vorgestellt, wie der Bluetooth-Netzwerk-Stack ausgenutzt werden kann, um Remote-Code auszuführen und KFZ ohne physische Verbindungen zu steuern.⁵⁴ Ebenso ist es möglich, per Bluetooth Angriffe auf Mobiltelefone auszuführen. Ein Angriff erfordert physische Nähe, doch die Verbreitung des Cabir-Wurms auf Symbian-Telefonen, die während eines Besuchs in einem Stadium erfolgte, macht die geringe Bedeutung dieser Einschränkung offensichtlich. Eine Bluetooth-Stack-Schwachstelle (oder selbst einfaches MAC-Spoofing) wäre ein einfacher Ansatz für einen erfolgreichen Angriff: Aufgrund der physischen Nähe ist es einfach, eine bestimmte Person (oder eine Gruppe) gezielt anzugreifen. Daher ist dieser Ansatz ideal für gezielte APTs (Advanced Persistent Threats, hochentwickelte hartnäckige Bedrohungen) geeignet.

Netzwerkbrücken

Eine Eigenschaft, die Mobilgeräte von allen anderen Geräten abhebt, ist ihre Verbindungsfreizügigkeit. Sie sind meist permanent mit mindestens einem Mobilfunkmast (z. B. per GSM oder 3G) und parallel mit lokalen Netzwerken (meist per WLAN) und im Nabereich (per Femtozelle, Bluetooth und Infrarot) verbunden. Aufgrund ihrer Mobilität bauen die meisten Geräte über den Tag verteilt viele solcher Verbindungen auf. Das erleichtert Angreifern ihre Arbeit, da sie aus einer größeren Anzahl an Eindringungspunkten und -protokollen wählen können. Dabei suchen sie sich das schwächste Glied der Kette – meist die Heimverbindung.

Weiterhin stellen auch Neuverbindungen ein Problem dar. Die Möglichkeiten der Angreifer, Netzwerkverkehr bei einer erneuten Verbindung wiederholt zu erfassen (z. B., wenn eine Person von der Arbeit nach Hause kommt und sich das Mobiltelefon mit der gleichen Femtozelle verbindet) kann ihnen Angriffswege öffnen, die andernfalls ausgeschlossen wären.

Wenn eines der Netzwerke kompromittiert ist, kann selbstverständlich auch das Mobilgerät kompromittiert werden. Wenn sich dieses Gerät dann an einem Unternehmensnetzwerk anmeldet, kann es zum Einfallstor für weitere böswillige Aktionen werden.

Missbrauch von Sicherheitsfunktionen

Datensicherung und Verschlüsselung

Bei vielen Mobilgeräten sind Datensicherungen fest in der Nutzung des Geräts vorgesehen. So synchronisieren sich iPhones beispielsweise mit einem Computer. Android-Geräte speichern Daten hingegen online in einem verknüpften Google-Konto. Wir kennen Berichte über das Durchbrechen der iOS-Verschlüsselung, doch dazu ist physischer Zugang zum Gerät erforderlich.⁵⁵ (Außerdem kann bei dieser Methode keine Datensicherung auf einem PC entschlüsselt werden, mit dem sich ein iPhone synchronisiert.)

Mit der Sicherung sind stets auch Sicherheitsrisiken verbunden:

- Bei der Remote-Sicherung kann es vorkommen, dass die Daten während der Übertragung nicht ausreichend geschützt sind. Der Verlauf der Änderungen, die Apple im Laufe der Zeit am Synchronisierungsprozess vorgenommen hat, zeigt die Verbesserungen bei der Sicherheit bei jedem Betriebssystem-Update. Gleichzeitig zeigen die Aktualisierungen, dass immer wieder Schwachstellen gefunden und behoben wurden.⁵⁶
- Sicherungsdaten sind für Internetkriminelle ein wertvolles Ziel. iPhone-Sicherungen sind standardmäßig verschlüsselt, während bei Android mehrere Drittanbieter Apps zu diesem Zweck bereitstehen.
- Bestimmte Angriffstypen haben sogar dann Erfolg, wenn die Daten ausreichend stark verschlüsselt sind. Beispielsweise kann die Ermittlung der Sicherungsdauer (oder die Größe der Sicherungsdatei) einen groben Schätzwert über die Intensität der Gerätenutzung liefern – und so Kriminelle auf besonders lohnenswerte Ziele aufmerksam machen.
- Mobilgeräte, die eigene Sicherungssysteme einsetzen, bergen sogar ein noch höheres Risiko, da diese Systeme weniger Aufmerksamkeit von der Forscher-Community erhalten.
- Der Start einer Fernsicherung (oder Wiederherstellung) kann auf vielen Geräten ein DoS-Szenario auslösen. Daher muss diese Funktion ausreichend geschützt sein.

54. <http://www.technologyreview.com/computing/35094>

55. <http://www.itproportal.com/2011/05/25/russian-security-group-breaks-ios-encryption-says-few-groups-capable-repeating-steps>

56. Zovi, D.D.: „Apple iOS Security Evaluation: Vulnerability Analysis and Data Encryption“ (Einschätzung der Apple iOS-Sicherheit: Schwachstellenanalyse und Datenverschlüsselung). BlackHat 2011, Las Vegas.

Fernlöschung

Dabei handelt es sich um eine gebräuchliche Funktion, die zum Teil von Add-On-Software bereitgestellt wird und ein verloren gegangenes oder gestohlenen Gerät aus der Ferne löscht. Die Funktion kommt häufig in Unternehmensumgebungen zum Einsatz, deren Richtlinien von IT-Teams verwaltet werden. (Eine IT-Richtlinie kann beispielsweise ein BlackBerry-Gerät löschen.)⁵⁷ Durch die Fernlöschung können sensible Informationen geschützt werden. Der Missbrauch dieser Funktion kann aber auch katastrophale Folgen haben.

IT-Administratoren, die eine Löschung aus der Ferne auslösen können, sollten strenge Richtlinien für diese Aktion aufstellen. Fernlöscher- und -wiederherstellungsfunktionen sollten so gestaltet sein, dass physischer Zugang zu der dazu erforderlichen Ausrüstung notwendig ist. Wenn das Auslösen aus der Ferne zugelassen ist, kann das Risiko sehr hoch sein.

Kennwortspeicherung

Auf Mobilgeräten werden häufig sensible Daten gespeichert. Nokia-Telefone hatten noch vor dem Beginn der Smartphone-Ära eine Geldbörsenfunktion, die sensible Daten wie Anmeldenamen-/Kennwort-Kombinationen, Kreditkartennummern, PINs, Bankdetails und Passphrasen speicherte.

Mobilgeräte speichern Daten in Apps, wodurch die Daten wahrscheinlich angreifbarer werden. Es gibt mehrere mögliche Stolperfallen:

- Wenn Anwendungen nicht vollständig voneinander getrennt sind, können sensible Daten in anderen Programmen gefährdet sein.
- Bei schwacher Verschlüsselung kann es möglich sein, die Daten zu entschlüsseln und anschließend zu übertragen. Es gibt beispielsweise eine Schwachstelle in einer Skype-Version für Android, die private Daten in einer unverschlüsselten SQLite-Datenbank ablegt.⁵⁸

Um den Bedienkomfort zu erhöhen, arbeiten einige Kennwortspeicher im aktiven Modus und stellen Anmeldeinformationen automatisch bereit. Dies bringt jedoch eine geringere Kontrolle darüber mit sich, wann die sensiblen Daten entschlüsselt werden (sowie weniger Kontrolle des Benutzers über diese Daten).

Sperrung des Geräts

Falls Mobilgeräte verloren gehen, muss nicht autorisierter Zugriff verhindert werden. Das gilt auch für den Fall, dass der rechtmäßige Besitzer das Telefon kurze Zeit später wiederbekommt. Die häufigste Lösung besteht in der Sperrung eines Geräts nach einem kurzen Zeitraum der Inaktivität. Diese Sperrung wird anschließend durch die Eingabe einer PIN oder eines Kennworts wieder aufgehoben.

Dieser Schritt bietet zwar grundlegende Sicherheit, stellt jedoch eine alles andere als eine perfekte Lösung dar, da PINs leicht beim Blick über die Schulter abgelesen können werden.

Manche sensiblen Anwendungen erfordern ein zweites Kennwort. Diese im Grunde gute Sicherheitsmaßnahme ist jedoch nutzlos, wenn sie von einer Sicherheitsrichtlinie begleitet wird, die von Benutzern aus Bequemlichkeit deaktiviert werden kann.

Sicherheitsrichtlinien nutzen standardmäßig vierstellige PINs (iPhone) oder Mustererkennung (Android). Dieser schwache Schutz muss vor allem bei geschäftlich genutzten Telefonen auf eine stärkere Alternative (zumindest auf eine längere alphanumerische Zeichenfolge) umgestellt werden.

Sehr viele Besitzer sichern ihre Geräte mit einer kurzen PIN.⁵⁹ Häufig sind sie sich möglicher Alternativen wie „nicht einfacher“ Sicherheitsoptionen für das iPhone nicht bewusst. Außerdem neigen Menschen allgemein dazu, sehr schwache PINs auszuwählen. (Etwa 11 Prozent aller PINs bestehen aus einer dieser fünf Kombinationen: „1234“, „0000“, „1111“, „2580“ oder „0852“.)⁶⁰

Leider gehören Fingerabdruck-Scans und Iriserkennung noch nicht zum Alltagsgebrauch.

57. http://docs.blackberry.com/en/admin/deliverables/4222/Remote_Wipe_Reset_to_Factory_Defaults_250402_11.jsp

58. <http://www.androidpolice.com/2011/04/14/exclusive-vulnerability-in-skype-for-android-is-exposing-your-name-phone-number-chat-logs-and-a-lot-more>

59. Zovi, D.D.: „Apple iOS Security Evaluation: Vulnerability Analysis and Data Encryption“ (Einschätzung der Apple iOS-Sicherheit: Schwachstellenanalyse und Datenverschlüsselung). BlackHat 2011, Las Vegas.

60. <http://www.gadgetnew.info/iphone-top-10-pin-codes-picked-by-users>

Mehrere Identitäten

Viele Mobilgeräte sind nicht wirklich personengebunden, weil sie beispielsweise von Familienmitgliedern, Freunden und Verwandten mitgenutzt werden. Diese gemeinsame Nutzung birgt jedoch neue Sicherheitsrisiken:

- Eine größere Zahl von Anwendungen auf dem Gerät
- Persönliche Daten mehrerer Personen
- Weniger Kontrolle über Bezahldienste
- Eine höhere Wahrscheinlichkeit, dass das Gerät verlegt wird
- Konfrontierung von Kindern mit unerwünschten Inhalten

Daher können sich Sicherheitsmaßnahmen, die die gemeinsame Nutzung einschränken, vor allem bei geschäftlich genutzten Geräten als sehr hilfreich erweisen. Diese Maßnahmen könnten folgende Punkte umfassen:

- Eine Whitelist für zulässige Anwendungen
- Beschränkung der Funktionen von Anwendungen für mehrere Benutzer (sodass beispielsweise nur eine einzelne Identität bei E-Mail-Programmen zulässig ist)
- Sperrung von Geschäftsdaten (starke Verschlüsselung) außerhalb der Unternehmensumgebung
- Kindersicherungs-Software

Consumerization of IT

Viele Privatgeräte werden mittlerweile auch in Unternehmen genutzt und verbinden sich mit den Netzwerken vor Ort. Angestellte möchten ihre persönlichen Mobilgeräte im Unternehmen nutzen, während IT-Administratoren lieber Systemen vertrauen, die sie selbst aufgebaut haben und kontrollieren können. Der Trend, nicht von der IT-Abteilung bereitgestellte Geräte in der Unternehmensumgebung zu nutzen, wird als Consumerization of IT bezeichnet. Dieser Prozess ist nicht unbedingt sicher: Einige Mitarbeiter könnten Malware-verseuchte internetfähige Geräte mit sich führen, die ohne ihr Wissen Ton- und Videoaufnahmen aufzeichnen.⁶¹

Wir beobachteten ähnliche Probleme (allerdings in geringerem Umfang), als die ersten privaten Laptops in Unternehmensumgebungen eingeführt wurden. Bei Smartphones tritt dieses Problem jedoch weitaus häufiger auf.

Es ist unumgänglich, dass in Mobilgeräten Verwaltungsfunktionen integriert werden, dank derer die IT-Abteilungen bestimmte Richtlinien durchsetzen können. Die Telefone werden über DLP-Funktionen verfügen, die entweder in das Betriebssystem integriert oder von Sicherheits-Software zur Verfügung gestellt werden. Damit diese Maßnahme effektiv ist, müssen die Regeln von IT-Administratoren aufmerksam verwaltet werden.

Man-in-the-Middle-Angriffe

Die unterschiedlichen Verbindungsmöglichkeiten von Mobilgeräten und der häufige Aufbau neuer Verbindungen erhöhen die Erfolgswahrscheinlichkeiten von MITM-Angriffen (Man-in-the-Middle), sodass wir von einem Anstieg ausgehen. Diese Gefahr wird durch die kleinen Bildschirme und daraus folgende eventuell fehlende SSL-Anzeigen (Secure Sockets Layer) im Browser noch verschärft. Software-Entwickler, die den kleinen Bildschirm mit immer mehr Informationen zu füllen versuchen, könnten auf den Gedanken kommen, ausgerechnet bei den Sicherheitsinformationen zu sparen.

Sogar die SSL-Funktion selbst kann Fehler aufweisen oder ausnutzbar sein, wie wir in einem Fall feststellen mussten.⁶² So wurden bereits vertrauenswürdige Zertifikatanbieter kompromittiert (Comodo und vor kurzem DigiNotar).⁶³ Wenn ein häufig genutztes und vertrauenswürdigen SSL-Zertifikat gehackt wird, kann es zu einem MITM-Angriff kommen, bei dem Daten (z. B. von Anmeldeinformationen) gestohlen oder (durch Rückgabe falscher anstelle korrekter Daten) manipuliert werden. Zu ähnlichen Angriffen kann es kommen, wenn das Domain Name System (DNS) kompromittiert wird.

Schwachstellen in Anwendungen

Mobilgeräte-Malware findet man nicht nur in App Stores. Ebenso wie auf einem PC kann Malware auf einer böswilligen oder kompromittierten Webseite über eine Anwendungsschwachstelle auf ein Smartphone gelangen. Angreifer benötigen lediglich Zugang zu einer bekannten Schwachstelle in einer beliebigen App.

61. http://droidsecurity.appspot.com/securitycenter/securitypost_20110804.htm

62. <https://www.trustwave.com/spiderlabs/advisories/TWSL2011-007.txt>

63. http://www.computerworld.com/s/article/9218676/Sniffer_hijacks_secure_traffic_from_unpatched_iPhones
<https://community.mcafee.com/thread/38704?tstart=0>

Sobald die Angreifer Zugang zu bestimmten Schwachstellen erlangen, müssen sie einen zweistufigen Angriff durchführen:

- Unsignierten Code ausführen, wenn ein Benutzer eine Webseite aufruft oder ein Dokument öffnet. Schwachstellen in Browsern (z. B. Safari, Opera) oder in Software für PDF/DOC/HTML-Dokumente können diese Art von Code-Injektion und -Ausführung möglich machen. (Der aktuellste Jailbreak-Exploit für iOS nutzt beispielsweise eine Schwachstelle in der Verarbeitung von PDF-Schriften aus.)
- Den Betriebssystem-Kernel verändern, damit Malware mit den höchstmöglichen Berechtigungen ausgeführt werden kann. (Dazu muss eine Schwachstelle zur Erhöhung von Berechtigungen ausgenutzt werden.) Dabei müssen die Malware-Autoren Aktualisierungen des Betriebssystems oder der Virenschutz-Software unterbinden, um die langfristige Nutzung der Schwachstellen zu gewährleisten.

Es ist ein Missverständnis, dass Geräte ohne Jailbreak (z. B. iPhones) vor Malware geschützt sind, weil die Software aus einer vertrauenswürdigen Quelle stammt (Apple App Store). Erstens ist es zwar unwahrscheinlich, aber nicht ganz auszuschließen, dass Malware es bis in den App Store schafft. Der zweite und wichtigere Punkt ist, dass alle Geräte Schwachstellen haben, die eine Erhöhung der Berechtigungen und Ausführung von unsigniertem Code im Kernel erlauben. Ohne solche Exploits wäre Jailbreaking unmöglich. Die bloße Tatsache, dass es für alle iOS-Versionen (bis Version 4.3.3) Jailbreaks gibt, beweist das Vorhandensein solcher tiefgehender Schwachstellen.

Replizierende Malware

Parasitäre Viren

Die meisten Mobilgeräte-Betriebssysteme verlangen für jede App eine Signatur. Diese Tatsache bietet Schutz vor parasitären Viren, da beim Eindringen in ein Programm dessen Signatur gebrochen wird. Wenn die Sicherheit des Betriebssystems geschwächt ist (z. B. iPhones mit Jailbreak), können sich solche Viren dennoch verbreiten. In jedem Fall bieten sie Malware-Autoren keine Vorteile, da die Benutzer keine Apps mehr direkt von Gerät zu Gerät weitergeben.

Um in einer solchen Umgebung zu überleben, müssen parasitäre Viren ihren eigenen Quell-Code mitbringen und diesen zur Laufzeit in den Quell-Code anderer Apps einfügen. Diese Gefahr ist größer, als es auf den ersten Blick aussieht. Ein Virus, der diese Methode unter Windows aktiv nutzt, heißt W32/Induc.⁶⁴ Zur Weiterverbreitung muss ein Virus jedoch von einem Mobilgerät auf ein Quellenkontrollsystem überwechseln, das zur Entwicklung von Apps genutzt wird. Dieser Fall könnte am ehesten bei schwacher Netzwerksicherheit auftreten (z. B. bei einer offenen SMB-Freigabe in einem WLAN-Netzwerk, das ein App-Entwicklungs-Repository enthält), sodass ein Virus auf einem Telefon den Quell-Code der Apps auf dem Entwicklungs-PC ändern und eine Kopie von sich selbst einfügen könnte. Da es jedoch unwahrscheinlich ist, dass Malware auf Mobilgeräten Zugang zu App-Entwicklungs-Repositories erlangt, stufen wir diese Bedrohung als außerordentlich gering ein.

Im wahrscheinlichen Szenario sind es Hintertür-Trojaner oder Botnets, die nicht autorisierten Zugriff auf Quellenkontroll- und Erstellungssysteme für Mobilgeräte-Software auf Standard-PCs bieten. In diesen Fällen könnten die Angreifer Änderungen an in der Entwicklung befindlichen Apps vornehmen und die Quellen infizieren.

Würmer

Bei Würmern handelt es sich um Malware, die sich nicht verändert. Wenn ein Wurm digital signiert ist, bleibt diese Signatur stets gültig. Dadurch ist diese Malware-Form im Vergleich zu parasitären Viren einfacher aufgebaut. Die oben beschriebene Methode zur Infizierung von App-Quellen durch parasitäre Viren funktioniert auch bei Würmern. Ein Wurm ist jedoch in der Lage, den schwierigsten Schritt zu überspringen: die Veränderung von App-Quellen. Stattdessen kann er beim Auffinden ungeschützter App Store-Anmeldeinformationen sofort eine Kopie (oder mehrere, möglicherweise unter verschiedenen Namen) von sich in den App Store hochladen und sich so auf die Geräte anderer Benutzer ausbreiten.

Auch dieses Szenario ist nicht sehr wahrscheinlich, da die entsprechenden Anmeldeinformationen nur sehr selten zu finden sein sollten. Sofern also ein Wurm keine vorkompilierte Liste von Anmeldeinformationen (in eingebetteter oder aus der Ferne zugreifbarer Form) besitzt, ist die Replizierung sehr schwierig.

Autowürmer

Möglicherweise könnte eine Schwachstelle entdeckt werden, die die Ausführung von Remote-Code auf bestimmten Mobilgeräten ermöglicht. Wenn ein derartiger Fehler in einem beliebigen Netzwerkprotokoll auftaucht, das von einer beliebigen häufig eingesetzten Anwendung genutzt wird, könnte er einem Autowurm die Übertragung von einem Gerät zum anderen erlauben. (Als Autowürmer bezeichnen wir Viren wie W32/CodeRed oder W32/Slammer, die sich ohne menschliches Zutun verbreiten.)

Netzbetreiber und Sicherheitsunternehmen sollten auf ein solches Ereignis vorbereitet sein, da ein Ausbruch (sofern der Wurm sich nicht freiwillig beschränkt) eine massive Datenverkehrszunahme nach sich ziehen und die mobilen Kommunikationswege erheblich stören könnte.

Schwachstellen sind meist auf eine ganz bestimmte Umgebung beschränkt und funktionieren nicht auf unterschiedlichen Betriebssystemen und Geräten. Es ist also unwahrscheinlich, dass ein sich selbstverbreitender Wurm mehr als einen Mobilgerätetyp betreffen würde. Durch die zunehmende Standardisierung bei Smartphones könnte es zu Angriffen kommen, die unterschiedliche Geräte umfassen (z. B. eine Schwachstelle, die in diversen Android-Geräten auftritt).

Infizierung und Drive-By

Anwendungen werden nur selten von einem Gerät auf ein anderes übertragen. Wir rechnen mit Angriffen, die sich auf die Infizierung von App Stores und die Bewerbung von dort zuvor platzierter Malware konzentrieren. Angriffe zur Manipulation der Anwendungsbewertung in App Stores (analog zu Angriffen mit Suchmaschinen-Optimierung auf Google und andere Suchmaschinenanbieter) werden immer weiter zunehmen.

Sobald es eine Malware in einen App Store geschafft und dort eine gute Bewertung (Reputation) erreicht hat, spricht nichts dagegen, dass ein Link darauf verbreitet wird (z. B. im Rahmen einer Spam-Kampagne oder in einem sozialen Netzwerk). Der App Store würde dann für einen konstanten Zustrom von Opfern sorgen.

Schwachstellen in Browsern oder ihren Plug-Ins werden häufig ausgenutzt, indem die Malware beim Aufrufen einer Webseite automatisch heruntergeladen wird. Diese Vorgehensweise wird auch als Drive-By-Download bezeichnet. Die Wirksamkeit solcher Angriffe auf Mobilgeräte ist von den Schwachstellen in den Browsern und internetfähigen Anwendungen abhängig, die häufig gemeinsam genutzte Dateien wie PDF-, JPG-, DOC-, XLS-, PPT-, HTML- sowie andere Dokumente öffnen können. Wenn sich die Anzahl der Schwachstellen in diesen Anwendungen nicht verringert, rechnen wir mit zunehmenden Angriffen mithilfe böswilliger URLs.

Phishing und Whaling

Wir konnten bereits Phishing-Angriffe auf Mobilgeräte beobachten, und wir sind sicher, dass sie nicht die letzten waren.⁶⁵ Bei Phishing handelt es sich im Grunde um einen Social-Engineering-Angriff. Die eingesetzten Methoden sind auf Desktop-Computern und Smartphones identisch.

Whaling ist eine Phishing-Form, bei der hochkarätige Ziele wie CEOs, CFOs und CTOs angegriffen werden. Sie wird häufig bei mehrstufigen gezielten Angriffen eingesetzt. Wenn die erste Whaling-Stufe Erfolg hat, kann sich der Angriff innerhalb eines Unternehmens in unterschiedliche Richtungen ausbreiten. APTs sind die wahrscheinlich effektivste Methode zum fortwährenden Diebstahl sensibler Daten.

APTs und Rootkits

Hochentwickelte hartnäckige Bedrohungen (APTs) sind darauf ausgelegt, ihre Anwesenheit zu verbergen, weshalb sie als „hochentwickelt“ bezeichnet werden. Sie beinhalten meist den Einsatz von Rootkits in Form von Stealth-Malware.

Rootkits stellen unter Windows – trotz der Verbesserungen am Betriebssystem – ein zunehmendes Problem dar. Auf der DefCon 2010 wurde demonstriert, dass die Rootkit-Implementierung unter Android relativ einfach ist.⁶⁶ Bei dieser Präsentation wurde auch eindrucksvoll gezeigt, dass der Erfolg des Rootkits sehr stark von der Version des Android-Betriebssystems abhängig ist. Die Entwicklung eines Rootkits, das unterschiedliche Android-Versionen erfolgreich angreifen kann, ist und bleibt eine komplizierte Angelegenheit.

Abgesehen von der Lösung des Portabilitätsproblems, das Rootkit-Operationen auf unterschiedlichen Betriebssystemversionen erlauben würde, möchten Malware-Entwickler ein Rootkit per Fernzugriff (d. h. ohne physischen Zugang zum Gerät) bereitstellen. Dazu ist Remote-Ausführung von böswilligem Code mit Root-Berechtigungen erforderlich. Mit anderen Worten: Es bedarf eines Exploits zur Remote-Code-Ausführung sowie eines Exploits zur Erhöhung von Berechtigungen. Die Remote-Ausbringung ist nur dann möglich, wenn die Angreifer über beide Exploits verfügen – es sei denn, der erste Exploit kann im Kernel ansetzen und sofort Code mit Root-Berechtigungen ausführen.

Ein Rootkit kann jedoch auch vor der Übergabe an den Benutzer auf einem Smartphone installiert werden (z. B. beim Hersteller oder im Geschäft). Das ist für den Angreifer der Idealfall, da er dadurch Zugang, eindeutige Spezifikationen sowie die Betriebssystemkonfiguration erhält und sich nicht mit Problemen mit der Portabilität oder Remote-Bereitstellung herumschlagen muss. Am einfachsten lassen sich APTs jedoch heimlich installieren, wenn die Angreifer ein schwach gesichertes Smartphone finden und es sich „ausleihen“.

Bei häufig genutzten Betriebssystemen dauert es im Durchschnitt weniger als zwei Wochen, bis Patches für Exploits bereitstehen (bei Geräten mit angepassten Android-Versionen kann es auch etwas länger dauern). Die Angreifer haben also nur ein eingeschränktes Anfälligkeitsfenster. Laut Google ermöglicht der Open-Source-Ansatz von Android Programmierern und Sicherheitsexperten das schnellere Auffinden von Fehlern und dadurch letztendlich sichereren Code. Dieser Ansatz scheint zu funktionieren: Die Gesamtzahl der gemeldeten Schwachstellen in Android liegt niedriger als bei iOS. Andererseits könnte es durch den Open-Source-Ansatz auch einfacher sein, tiefgehende Sicherheitsprobleme zu finden und auszunutzen. Einige dieser ausnutzbaren Fehler wären ohne eine genaue Analyse des Quell-Codes unmöglich zu finden.

Die Gefahr hält sich jedoch in Grenzen, da Zero-Day-Exploits schwer zu finden und auf dem Untergrundmarkt sehr teuer sind. Wir gehen auch davon aus, dass die Zahl dieser Exploits mit zunehmender Absicherung von Betriebssystemen abnehmen (und das Jailbreaking noch weiter erschwert) wird. Gleichzeitig werden die Schwarzmarktpreise für Zero-Day-Exploits unweigerlich anziehen. Durch diese Dynamik sollte viele Exploits für die meisten Malware-Autoren unerreichbar sein.

Selbst wenn Malware-Autoren nicht mehr mit den marktüblichen Preisen mithalten können, wird sie das nicht von der Entwicklung von APTs abhalten, die staatlich unterstützt zu sein scheinen (wie es höchstwahrscheinlich bei W32/Stuxnet der Fall war).

Die Patch-Installation und Aktualisierung von Mobiltelefon-Apps erfolgt schneller als auf Desktop-Computern. Die dazu erforderlichen Mechanismen sind in den Betriebssystemen integriert, und die meisten Geräte sind permanent mit dem Internet verbunden. Dadurch wird sichergestellt, dass alte (ungepatchte) Betriebssystemversionen schneller aktualisiert werden, als dies bei Desktop-Computern der Fall ist. Durch die schnellere Ausbringung von Patches und Aktualisierungen verringert sich das Anfälligkeitsfenster.

Virtuelle Betriebssysteme

Das ultimative Rootkit kann das Betriebssystem davon überzeugen, dass es auf realer Hardware ausgeführt wird, während das Rootkit unterdessen alle Signale des Betriebssystems an die Hardware abfängt und beliebige Daten manipuliert. Diese auf Virtualisierung basierende Angriffsmethode wird als Blue Pill (blaue Pille) bezeichnet.⁶⁷ Im Gegensatz zu Man-in-the-Middle-Angriffen handelt es sich hierbei um einen Man-in-the-Hardware-Angriff.

Bei der aktuellen Mobilgeräte-Generation hat sich Virtualisierung – wahrscheinlich aufgrund der geringen Akku-Laufzeit – noch nicht durchgesetzt. Die Virtualisierung wird jedoch auch bei Smartphones unweigerlich zunehmen (z. B. beim Einsatz mehrerer Betriebssysteme auf demselben Gerät) und einige entsprechende Angriffe nach sich ziehen. Wir gehen davon aus, dass dieses Problem erst in einigen Jahren relevant wird.

Jede Menge Unterhaltung

Wenn Mobilgeräte nicht beruflich eingesetzt werden, dienen sie häufig der Unterhaltung. In vielen Fällen werden Geräte für beide Zwecke genutzt.

Allgemein betrachtet ähneln sich Unterhaltungsdaten (Filme und Musik) und Unternehmensdaten – beide sollen geschützt werden. Dazu werden meist die Sicherheitstechniken DRM und DLP verwendet. Wir erwarten, dass Mobilgeräte die Daten schützen (vom Speicher bis zum Bildschirm, und von Eingabegeräten bis hin zu Apps und dem Netzbetreiber) und an ein bestimmtes Gerät binden. In der Zwischenzeit werden Bedrohungen für Mobilgeräte-Hardware (einschließlich Neuflashen oder Ersetzen von Komponenten-Microcode) unweigerlich zunehmen. Die Angreifer werden versuchen, die Gerätebindung aufzubrechen. Dabei ist diese Vorgehensweise auf Mobilgeräten einfacher, da der physische Zugang hier eher möglich ist.

Aus diesem Grund wünschen wir uns manipulationssichere Geräte, die ihre Daten automatisch löschen, sobald sie geöffnet werden oder nicht autorisierte Versuche entdecken, die Hardware neu zu programmieren oder zu ersetzen. Bei einem akkubetriebenen Gerät ist das nicht einfach umzusetzen – wenn der Akku entfernt ist, merkt das Gerät nichts. (Könnte dies der Grund dafür sein, dass Apple den Akku des iPhone nicht zugänglich gemacht hat? Selbst wenn das nicht die ursprüngliche Absicht war, halten wir es trotzdem für eine gute Sache!)

Die meisten sensiblen Mobilgeräte könnten ihre Bewegungssensoren einsetzen, um beispielsweise das Gerät sicher zu sperren (oder zu löschen), wenn es sich zu weit vom Benutzer entfernt.

Gefälschte Mobilgeräte-Warnungen

Gefälschte Virenschutz-Software ist eine der häufigsten und bekanntesten Malware-Formen für Windows-Computer. Dieser Social-Engineering-Betrug wird auch als Scareware, nicht autorisierte Virenschutz-Software oder Falschalarm-Software bezeichnet. Die Malware gibt gefälschte Sicherheitswarnungen aus, die den Benutzer dazu verleiten sollen, Geld für die „Beseitigung“ der Probleme zu bezahlen. (Gefälschte Virenschutz-Software gibt vor, einen kostenlosen Scan durchzuführen, und verlangt anschließend Geld für die „Vollversion“, die angeblich das System „bereinigen“ soll.)

Wir rechnen damit, dass sich gefälschte Virenschutz-Software auch auf Mobilgeräten ausbreiten wird, da sich diese Betrugsmasche auf dem PC als sehr einträglich erwiesen hat. Uns sind bereits Berichte von mehreren Fällen bekannt: einer unter J2ME⁶⁸ sowie ein weiterer von April 2011, bei dem sich die Android-Malware als Sicherheitstool ausgab⁶⁹.

Soziale Netzwerke

Der Zugriff auf soziale Netzwerke wie Twitter, Facebook und LinkedIn über Mobilgeräte wird immer beliebter, da diese Art der schnellen Kommunikation perfekt auf diese Art von Geräten zugeschnitten ist. Gleichzeitig sind viele Informationen auf den Social-Network-Servern als privat gekennzeichnet. Doch selbst wenn die Sicherheitseinstellungen der sozialen Netzwerke funktionieren, könnten Daten mithilfe eines kompromittierten Mobilgeräts gestohlen werden.

Wir machen uns vor allem über kostenlose WLAN-Netzwerke Sorgen (die von den meisten Menschen anstelle kostenpflichtiger Alternativen genutzt werden), da auf diese Weise mit Leichtigkeit unverschlüsselter Datenverkehr mitgelesen und Kennwörter erfasst werden können (sofern keine SSL-Verbindung verwendet wird). Sie können beispielsweise facebook.com über HTTPS sowie über HTTP erreichen, wobei vielen Benutzern die sichere Variante unbekannt ist.

Fernsteuerung

Mobilgeräte werden immer häufiger für die Fernsteuerung verwalteter Ressourcen⁷⁰ oder zum Fernvollzugriff auf PCs verwendet.⁷¹ Tablet-Geräte bieten sich ebenfalls für die schlanke Verwaltung und Kontrolle an. (Tablet-Computer bieten Bildschirme, die fast Laptop-Größe erreichen. Da regelmäßige Überprüfungen von Unternehmens-Ressourcen oder -Prozessen nur selten umfangreiche Testeingaben erfordern, stellt das Fehlen von Maus und Tastatur meist keinen Hinderungsgrund dar.)

Wenn jedoch das Mobilgerät kompromittiert wird, erweisen sich Eindringungsversuche ins Unternehmensnetzwerk (z. B., um einen internen Server öffentlich zugänglich zu machen, wodurch Unternehmensgeheimnisse an Hacktivisten wie Anonymous oder LulzSec gelangen könnten) oder die Manipulation gesteuerter Prozesse (Stilllegung einer Produktionsumgebung) als erheblich einfacher. Ein unsicheres Mobilgerät könnte Manipulation, Sabotage und sogar Terroraktionen oder Internetkriegsführung Tür und Tor öffnen.

Industriesteuerung

Nach dem spektakulären Angriff durch den W32/Stuxnet-Wurm auf die Uran-Anreicherungsanlage im Iran müssen wir uns fragen, wie es um die Sicherheit von Industrieanlagen bestellt ist, die Mobilnetzwerke zur Kommunikation, Berichterstattung oder Warnung nutzen. Es gibt mehrere Möglichkeiten, wie Mobilkommunikation in SCADA-Industrieleitsystemen verwendet werden kann:⁷²

- Datenakquise (im schreibgeschützten Modus): Erfassung der Daten von Thermometern, Türen usw.
- Kontrolle (Schreibmodus): Wenn das SCADA-System beispielsweise elektronische Schlösser öffnet, Ventile verschließt oder die Drehgeschwindigkeit von Motoren oder Zentrifugen verändert
- Warnung bei Notfällen oder anderen Zwischenfällen: Senden einer SMS oder E-Mail, wenn beispielsweise die Temperatur in einem Gewächshaus unter ein bestimmtes Niveau fällt

Remote-Einheiten werden häufig über Mobilnetzwerke mit dem zentralen Controller eines SCADA-Systems verbunden. Solche Systeme sind allgemein verfügbar⁷³ und werden häufig eingesetzt (suchen Sie im Internet nach „SCADA+GSM+RTU“, und Sie erhalten fast eine Million Treffer). Die Gefahr ist also sehr real.

68. http://www.securelist.com/en/blog/208187561/Antivirus_Fraudware_Goes_Mobile

69. <http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=TrojanSpy%3AAndroidOS%2FLanucher.A>

70. <http://itunes.apple.com/us/app/vmware-vsphere-client-for/id417323354?mt=8>

71. <http://itunes.apple.com/us/app/remote-desktop-lite-rdp/id288362576>

72. <http://en.wikipedia.org/wiki/SCADA>

73. <http://www.ff-automation.com/products/gsm-rtu.shtml>

Mobiltelefone werden häufig für Notfallmeldungen eingesetzt. Die meisten Industrie- und IT-Überwachungs-Tools sowie Alarmanlagen für Unternehmen und Privathäuser können Warnmeldungen per SMS oder Sprachanruf senden, wobei in letzterem Fall eine aufgezeichnete oder synthetisierte Stimme zum Einsatz kommt. Die Blockierung oder Erzeugung einer gefälschten Warnung könnte in Zukunft fester Bestandteil von Angriffen werden. Bei einer verteilten SCADA-Installation sollten gerade in Bezug auf Mobilgeräte verstärkte Sicherheitsmaßnahmen integriert sein.

Allgemein könnten Angriffe auf verteilte SCADA-Systeme folgende Punkte umfassen:

- Störung der Kommunikation (DoS-Angriff)
- Diebstahl von Daten (passiver Man-in-the-Middle-Angriff)
- Manipulation von Daten (aktiver Man-in-the-Middle-Angriff)

Durch die Manipulation von Daten könnten Angreifer die vollständige Kontrolle über Remote-Prozesse sowie die Meldungen an die Kontrolleinheit erlangen. Dieser Zugriff ermöglicht vollkommen unerkannte Operationen, die für die zentralen Kontrollstellen unsichtbar sind.

Botnets

Mobilgeräte können genauso gut wie Windows-PCs für Botnets eingesetzt werden. Einige Mobilgeräte-Malware-Varianten zeigen bereits Botnet-Eigenschaften.⁷⁴

Durch den Einsatz von Mobilgeräten in Botnets können sich ganz spezielle Probleme ergeben. Beispiele für Probleme bei Netzbetreibern:

- Gesteigerter Datenverkehr außerhalb des TCP/IP-Protokolls (GPRS oder 3G)
- Mobilgeräte-Bots können die Infrastruktur des Anbieters angreifen. Ein Teil eines Botnets könnte in einem bestimmten Gebiet Neustarts oder Neuanmeldungen durchführen. Dabei handelt es sich um aufwändige Vorgänge, die einen DoS-Angriff für einen oder mehrere Funkmasten oder sogar den gesamten Anbieter bedeuten können. Da die maximale Reichweite von Mobiltelefonen bei 20–25 Kilometern liegt, würde eine ausreichende Anzahl von Bots in einem bestimmten Bereich (vor allem in dicht bevölkerten Gebieten) rund um einen Mast genügen, um diesen auszuschalten.

In einigen Fällen kann ein Botnet eine bestimmte Person oder Telefonnummer angreifen, indem sie mit SMS-Nachrichten oder Sprachanrufen überflutet wird.

Aufgrund der breiten Hardware-Basis können Botnets unterschiedliche Arten von Angriffen durchführen (Sprache, Video, GPS) und als Ausgangspunkt für die Infektion anderer Computer über beliebige Verbindungen (z. B. PC, WLAN, Bluetooth, SD-Karten und USB) dienen.

Fazit

Die Sicherheitsmaßnahmen für Mobilgeräte-Betriebssysteme entwickeln sich schnell weiter, wodurch einigen Malware-Formen wie beispielsweise parasitären Viren der Nährboden entzogen wird. Da Smartphones jedoch ständig mit Netzwerken verbunden sind und – viel schwerwiegender – das Filtern von Malware in App Stores sehr schwierig ist, wird sich Mobilgeräte-Malware wahrscheinlich noch weiter verbreiten.

Wir rechnen mit massiven Angriffen auf App Stores, die mit einfachen Malware-Posts beginnen und schrittweise durch Beeinträchtigungen des Rufes von Entwicklern sowie die Infiltration von App-Quellenkontrollsysteme ausgeweitet werden. Die meiste Malware wird auf finanzielle Vorteile abzielen – von NFC-Transaktionen über Bitcoins bis hin zur elektronischen Geldbörse.

Aufgrund der fortschrittlichen Hardware-Funktionen der meisten Smartphones wie Sprache, Kamera und GPS können Angreifer sensiblere Informationen stehlen, was zu höheren durchschnittlichen Kosten von Kompromittierungen führt.

Wir erwarten eine Zunahme von Man-in-the-Middle-Angriffen mithilfe von SSL- und DNS-Kompromittierungen oder Femtozellen. Hierbei werden im Unternehmens- und Industriebereich vor allem APT/Rootkit-Malware und Zero-Day-Schwachstellen zum Einsatz kommen.

Sicherheitsfunktionen in Betriebssystemen (insbesondere Android) müssen parallel zur physischen Sicherheit mobiler Geräte verbessert werden.

Danksagung

Ich danke meinen Kollegen Carlos Castillo, Michael Price und Jimmy Shah für ihre wertvolle Unterstützung und ihre Hinweise.

Informationen zum Autor

Dr. Igor Muttik ist Leitender Architekt bei McAfee Labs. Er hat einen Ph.D. in Physik und Mathematik inne. Seine Untersuchungen zu den ersten Computerviren brachten ihm den Einstieg bei Dr. Solomon's Software ein. Dieses Unternehmen wurde später von McAfee übernommen. Neben seiner Malware-Forschung hält Muttik regelmäßig Vorträge auf Sicherheitskonferenzen in aller Welt.

Über McAfee Labs

McAfee Labs ist das weltweit agierende Forschungsteam von McAfee. Es ist die einzige Forschungsorganisation, die alle Bedrohungsvektoren – Malware, Internet, E-Mail, Netzwerk und Schwachstellen – abdeckt. McAfee Labs erfasst Daten von Millionen Sensoren und seinem cloudbasierten Dienst McAfee Global Threat Intelligence™. Die 350 multidisziplinären Forscher, die in 30 Ländern für McAfee Labs arbeiten, überwachen permanent das gesamte Bedrohungsspektrum, identifizieren Anwendungsschwachstellen, analysieren und korrelieren Risiken und arbeiten an Fehlerbehebungsmaßnahmen, um Unternehmen und Privatpersonen zu schützen.

Informationen zu McAfee

McAfee ist ein hundertprozentiges Tochterunternehmen der Intel Corporation (NASDAQ: INTC) und der weltweit größte auf IT-Sicherheit spezialisierte Anbieter. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer, ITK-Netze und Mobilgeräte auf der ganzen Welt vor Angriffen schützen und es den Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von der einzigartigen Global Threat Intelligence-Technologie entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. McAfee ist stets auf der Suche nach neuen Möglichkeiten, seine Kunden zu schützen. www.mcafee.com/de

