

McAfee®



Schützen Sie, was Sie schätzen.

Malware für Mobiltelefone: Bedrohungen und Vorbeugung

von Zhu Cheng

Malware für Mobiltelefone: Bedrohungen und Vorbeugung

Wenn Sie als Mobiltelefon ein Smartphone verwenden, tragen Sie praktisch einen leistungsstarken Computer in der Tasche. Immer mehr Mobiltelefone, die auf den Markt kommen, enthalten nicht nur eine Kamera, sondern auch umfassende Funktionen für den Onlinezugriff, eine Tastatur und andere typische Computerfunktionen.¹ Diese Leistungsfähigkeit und Bequemlichkeit bringen jedoch auch Probleme mit sich. Ebenso wie Desktop-PCs und Notebooks sind diese Mobiltelefone Sicherheitsbedrohungen ausgesetzt. Die traurige Ironie dieser Weiterentwicklung liegt darin, dass Mobiltelefone mit zunehmender Funktionalität immer anfälliger für die gleichen Arten von Bedrohungen werden, die Notebooks und Desktop-PCs heimsuchen.

Die häufigsten Betriebssysteme auf Mobiltelefonen und PDAs (persönlichen digitalen Assistenten) sind Microsoft Windows Mobile und Symbian OS. Windows Mobile 2003 und Windows Mobile 6 basieren auf Windows Mobile, für dessen Kernel eine Shared-Source-Strategie verwendet wird. Die Benutzeroberfläche des S60 von Nokia basiert auf Symbian OS, einem Betriebssystem, das von Symbian Ltd. entwickelt und gepflegt wird. (Zahlreiche andere Produkte verwenden ebenfalls S60, darunter Telefone von Samsung, Panasonic, Siemens und Lenovo.) Da Microsoft bei Windows Mobile eine entwicklerfreundliche Umgebung und Shared-Source-Politik verfolgt, wird dieses Betriebssystem inzwischen auch von anderen Mobiltelefon-Herstellern verwendet. Zugleich dürften dieselben Vorteile immer mehr Malware-Autoren anlocken, sodass die wachsenden Sicherheitsprobleme bei Mobiltelefonen den Benutzern inzwischen beträchtliche Sorgen bereiten sollten.

In diesem Whitepaper werden Sicherheitsrisiken bei Smartphones unter Windows Mobile erörtert. Die meisten dieser Sicherheitsrisiken finden sich auch bei den PDAs unter Windows Mobile.

Wie Erkennungsdaten und Bedrohungsmodellierungen von McAfee Avert[®] Labs zeigen, hat die Malware für Mobiltelefone in der letzten Zeit schnell zugenommen, und dieser Trend wird sich im Rest des Jahres voraussichtlich fortsetzen.² Was sind die Hauptgründe für die zunehmenden Risiken für Windows Mobile-Geräte?

- ➔ Mobiltelefone werden immer preiswerter, und immer mehr Anbieter produzieren Telefone.
- ➔ Die Shared-Source-Politik für den Kernel von Windows Mobile ermöglicht Malware-Autoren ein tief gehendes Verständnis des Betriebssystems.
- ➔ Benutzer von Mobiltelefonen geben meist umfangreiche private Daten in ihre Geräte ein. Dies zieht Malware-Autoren an, da sie aus Identitätsdiebstahl oder unrechtmäßiger Aneignung von Kreditkartendaten potenziell finanzielle Gewinne ziehen können.
- ➔ Mit zunehmenden Hardwarekapazitäten der Telefone wird auch die Funktionalität ihrer Betriebssysteme immer umfangreicher, sodass Malware-Autoren stets neue Aspekte ausnutzen können.
- ➔ Die Entwicklung von Software unter Windows Mobile und unter Win32 sind einander sehr ähnlich, sodass Autoren von Win32-Malware leichter zu Malware für Mobiltelefone übergehen können.

¹ http://telephia.com/html/Smartphonepress_release_template.html

² http://www.mcafee.com/us/about/press/corporate/2006/20061129_080000_f.html

Welche Funktionen sind den größten Risiken ausgesetzt?

Unserer Meinung nach liegen die größten Bedrohungen für Mobiltelefone in den folgenden sieben Bereichen:

- Textnachrichten
- Kontakte
- Videodaten
- Gesprächsmitschnitte
- Rufliste
- Dokumente
- Pufferüberläufe

Textnachrichten

Windows Mobile stellt eine Entwicklungs-API bereit, die hauptsächlich Funktionen zum Senden und Blockieren von Nachrichten umfasst. Mithilfe dieser Funktionen können Viren oder sonstige Malware Ihre privaten Daten stehlen und Sie potenziell finanziell oder anderweitig ruinieren.

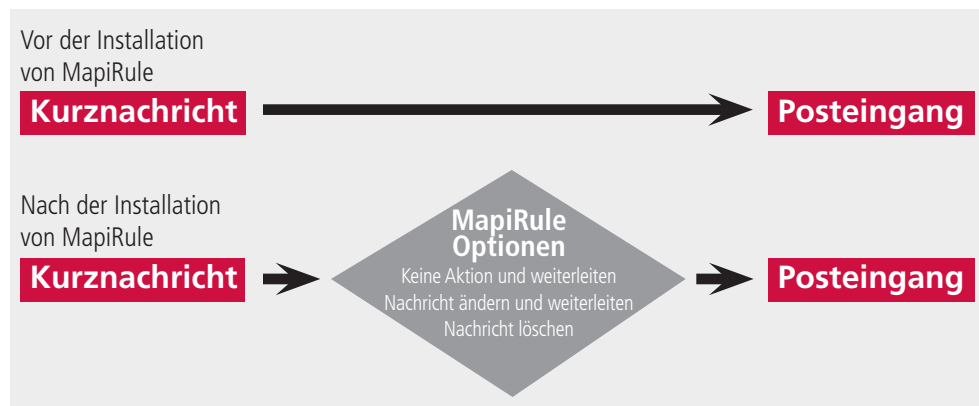
Forschern der McAfee Avert Labs sind Fälle bekannt, in denen SMS (Short Message Service) zum Phishing verwendet wurden (auch als SMiShing bezeichnet). Dies tritt offenbar zunehmend auf.³ Ein Beispiel ist Malware, die mithilfe der APIs für Textnachrichten unechte Nachrichten an Personen in Ihrer Kontaktliste sendet. Dies ähnelt dem Spoofing (Verwenden eines gefälschten Absenders) bei E-Mails. Diese Art des Phishing ist jedoch mit noch höherer Wahrscheinlichkeit erfolgreich, da die Opfer sich dieser Art von Bedrohung meist gar nicht bewusst sind. Wer einer eingehenden Nachricht lediglich anhand der zugehörigen Telefonnummer vertraut, ist anfällig für Schäden durch jede Person in der Kontaktliste, deren Gerät mit Malware infiziert wurde, da diese Malware leicht Nachrichten in ihrem Namen senden kann. Den Benutzern fällt es meist schwer, zu entscheiden, ob eine SMS böswillig ist.

Malware kann APIs für Textnachrichten auch verwenden, um Mobiltelefongebühren über das SMS-Zahlungsgateway anfallen zu lassen. In einem Fall wurden bereits Java-fähige Mobiltelefone (darunter solche mit Nokia S60- und Windows Mobile-Plattformen) Opfer dieser Bedrohung.⁴ Dieser Trojaner sendet spezielle Textnachrichten an einen Dienstanbieter in Russland und bucht die Gebühren vom Prepaid-Guthaben auf dem Mobiltelefon des Benutzers ab. Es kann angenommen werden, dass ähnliche Angriffe bald auf Geräte unter Windows Mobile gestartet werden, da diese Geräte immer beliebter werden.

Leider entstehen durch die Vielfalt der Windows Mobile-Plattform andere Ausnutzungsmöglichkeiten. Laut dem Windows Mobile SDK (Software Development Kit) kann ein Anwendungsentwickler Code basierend auf dem MapiRule-Beispielcode schreiben und laden, um Textnachrichten zu blockieren. Da Microsoft bereits ein MapiRule-Framework im SDK bereitstellt, muss der Entwickler es nur ein wenig ändern, um es als DLL zu verwenden. Die Abbildung auf der nächsten Seite zeigt die Verarbeitung von Kurznachrichten vor und nach der Installation von MapiRule. Nach der Installation wird MapiRule zu einem Filter zwischen Kurznachrichten und dem Mailprogramm tmail (text mail). Somit kann ein Programmierer den Verarbeitungsprozess für Kurznachrichten unterbrechen und in Form eines Man-in-the-Middle-Angriffs Nachrichten löschen, weiterleiten oder andere Vorgänge ausführen. In Malware kann diese Funktion verwendet werden, um auf dem Mobiltelefon eines Benutzers eine DLL zu installieren, mit der Kurznachrichten blockiert werden und die normale Kommunikation gestört wird und mit der Antworten auf Nachrichten gesendet oder Nachrichten weitergeleitet werden. Wenn SMS für die Unternehmenskommunikation verwendet werden, wird so ein Einfallstor für das Abfangen von Unternehmensdaten geschaffen.

³ <http://www.avertlabs.com/research/blog/?p=75>
<http://www.f-secure.com/weblog/archives/archive-042007.html#00001173>

⁴ http://vil.nai.com/vil/content/v_138726.htm



Durch Verwendung von MapiRule-Code mit SMS können Hacker eine Man-in-the-Middle-Bedrohung schaffen.

Trotz dieser Gefahr gibt es keinen Grund zur Panik! Die MapiRule-Technologie zum Blockieren von Kurznachrichten verwendet einen von Microsoft bereitgestellten festen Port, sodass die Benutzer leicht erkennen können, ob auf ihren Windows Mobile-System eine DLL eingeschleust wurde. Damit die Malware etwas über diesen Port installieren kann, muss sie das DLL-Filtermodul registrieren und dann den CLSID-Schlüssel der DLL unter folgendem Registrierungseintrag hinzufügen:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Inbox\Svc\SMS\Rules]
```

Sie muss dann dem Schlüssel den Wert 1 zuweisen, zum Beispiel:

```
"{3AB4C10E-673C-494c-98A2-CC2E91A48115}"=dword:1
```

Diese Schlüsselzuweisung zeigt daher an, dass auf dem System eine Filter-DLL für MapiRule installiert wurde. Die Leser sollten jedoch keine Inhalte unter diesem Eintrag entfernen, da die dort festgelegten DLLs möglicherweise nicht von Malware installiert wurden. Wenn der Benutzer die falschen Schlüssel entfernt, können Fehler bei einem wichtigen Programm auftreten. Wenn Sie einen solchen Schlüssel finden, sollten Sie sich darauf verlassen, dass die Antivirensoftware auf Ihrem Mobiltelefon das Problem behebt.

Kontakte

In einer Unternehmensumgebung ist die Kontaktliste eine der wichtigen Funktionen eines Smartphones. Ein Diebstahl von Kontaktdaten des Unternehmens kann schwerwiegende Konsequenzen für den Mitarbeiter und für das Unternehmen haben. Wie bereits erwähnt, kann Malware für Mobiltelefone eine Kontaktliste "stehlen" und Kurznachrichten mit Malware oder einem Link zu Malware versenden. Noch schlimmer ist es, wenn die Malware Ihre Kontaktinformationen als Paket an einen böswilligen Dritten sendet. Viele Smartphone-Benutzer verwenden die in das Smartphone integrierten Sicherheitstools für Kontakte. Diese verwenden in der Regel programmiersprachliche Aufrufe wie IPOutlookItemCollection, IFolder und IContact für die Pocket Outlook Object Model-API im Windows Mobile SDK. Entwickler von Malware können diese Aufrufe leicht verwenden, um Kontaktinformationen abzurufen und zu ändern und die Ergebnisse an eine andere Person zu senden.

Videodaten

Die meisten der heute angebotenen Mobiltelefone verfügen über eine Kamera für Videos und Fotos. Über die APIs von Microsoft kann Malware für Mobiltelefone die Kontrolle über das Gerät übernehmen und mit der Kamera Fotos aufnehmen – es würde der Malware jedoch wahrscheinlich schwer fallen, die Kamera dafür jeweils in eine geeignete Position zu bringen. Die Möglichkeit, das Telefon mithilfe einer Automatisierung der Kamera auszunutzen, ist also ziemlich gering. Sicherheitslücken bei Fotos und Videodaten, die sich bereits auf dem Gerät befinden, sind jedoch viel leichter auszunutzen. Malware kann über die Datei-API nach allen JPG-Dateien suchen und diese Dateien über das Funknetzwerk an einen böswilligen Dritten senden. Die Bilder können zwar groß sein. Im Allgemeinen ist jedoch in jedem Land bzw. jeder Region mit flächendeckendem Netzwerk für Mobiltelefone der dritten Generation (3G) genug Bandbreite verfügbar.

Gesprächsmitchnitte

Was wäre, wenn Ihr Mobiltelefon sich auf einmal in einen Kassettenrecorder verwandeln würde? Mithilfe der Sprachaufzeichnungs-API auf dem Mobiltelefon kann Malware dieses in der Tat in einen Kassettenrecorder verwandeln. Microsoft verwendet laut Windows Mobile SDK die Waveform-Audiofunktionen, um WAV-Dateien aufzuzeichnen und abzuspielen. Da Windows Mobile und Windows vergleichbar sind, können viele APIs und Codecs, die Windows für Aufzeichnungen verwendet, auch auf Windows Mobile angewendet werden – und können Autoren von Malware für Mobiltelefone als Referenz dienen. Beispielsweise haben wir beim Testen des Dopod-Telefonen festgestellt, dass die Aufnahmequalität sehr hoch war – sogar dann, wenn sich das Mobiltelefon in der Jackentasche eines Benutzers befand. Der Speicherplatz auf Mobiltelefonen ist jedoch begrenzt, sodass Malware nicht fortwährend Audiodaten aufzeichnen kann. Sie kann jedoch die aufgezeichnete Datei über E-Mail oder über den Multimedia Message Service (ähnlich wie SMS) an einen Angreifer senden. Wenn der Angriff mit der oben beschriebenen Technologie zum Abfangen von SMS kombiniert wird, kann die Malware die Aufzeichnungsfunktion über SMS aktivieren und so das Mobiltelefon in einen Kassettenrecorder verwandeln, der remote ein- und ausgeschaltet werden kann.

Rufliste

Die Rufliste kann sehr wertvoll sein, und böswillige Programme können diese Informationen auslesen. Die Benutzer sollten ihre Ruflisteneinträge im Auge behalten und nicht benötigte Daten möglicherweise regelmäßig löschen, um den Schweregrad einer Infektion zu mildern.

Dokumente

Viele Mobiltelefon-Benutzer lesen und speichern Word-, Excel- oder PDF-Dateien auf ihren Mobiltelefonen, besonders auf PocketPCs. Malware kann diese Dateien stehlen, wiederum mithilfe der API-Funktion. Es ist zu erwarten, dass Dateien mit den Erweiterungen *.DOC, *.XLS und *.PDF sich zu beliebiger Diebesbeute der Malware für Mobiltelefone entwickeln werden. Mobiltelefon-Benutzer sollten beim Speichern vertraulicher Unternehmensdaten oder privater Dateien auf ihrem Telefon Vorsicht walten lassen.

Pufferüberläufe

Auch mobile Geräte werden von Pufferüberläufen geplagt. Schon auf der Xcon 2005 gab es einen Vortrag zu Hackertätigkeiten für Windows Mobile.⁵ Der Vortrag umfasste Ratschläge zur Shell-Code-Entwicklung sowie Beispielcode.

Verhindern von Malware-Angriffen auf Mobiltelefone

Zum Schutz der Windows Mobile-API verwendet Microsoft standardmäßig ein Zertifikatsystem. Nur Programme mit signierten Zertifikaten können APIs auf den mobilen Geräten aufrufen. Dieses System ist so lange gut, bis ein Benutzer ein nicht signiertes Programm hinzufügen möchte. Eine Möglichkeit, die Standardsicherheit zu umgehen, ist die Verwendung eines Tools wie SDA_ApplicationUnlock von Novosec, das die Zertifikatsicherheit auf einem Mobiltelefon vollständig deaktiviert. Die Gefahr einer solchen Entsperrung besteht jedoch darin, dass die Sicherheit des Geräts verringert wird. Nach dem Entsperrern kann jedes Programm, auch Malware, die API-Aufrufe verwenden. Unser Rat ist einfach: Verwenden Sie derartige Programme nicht, wenn Sie die Sicherheit Ihres Mobiltelefons aufrecht erhalten möchten. (Weitere Informationen finden Sie im Überblicksartikel von Microsoft zur Anwendungssicherheit unter Windows Mobile 5.0.⁶)

⁵ <http://www.phrack.org/issues.html?issue=63&id=6#article>

⁶ <http://msdn2.microsoft.com/en-us/library/ms839681.aspx>

Vorsicht ist besser als Nachsicht

Der beste Schutz für Ihr Mobiltelefon besteht darin, Malware gar nicht erst hineinzulassen. Verwenden Sie für Ihr Telefon die gleichen Vorsichtsmaßnahmen wie für ein Notebook oder einen Desktopcomputer unter Windows. Antiviren- und Anti-Malware-Tools zur Verhinderung einer Infektion sind effektivere Lösungen als Produkte, die Viren nur erkennen oder entfernen. Wenn Ihr Mobiltelefon erst einmal mit Malware infiziert ist, kann es kompliziert sein, sie zu entfernen. Am besten verwenden Sie eine Kombination aus PC-basierter Antivirensoftware (mit aktiviertem Virenschanner bei Zugriff) und Antivirensoftware für das Mobiltelefon. Mobiltelefon-Benutzer sollten außerdem die gleichen Vorgehensweisen für eine sichere Browserverwendung befolgen, wie sie für ihre Computer verwenden. Des Weiteren empfehlen wir, nur Programme mit digitalen Signaturen zu akzeptieren: Programme, die den Zertifikatstest bestanden haben und von legitimen Herstellern kommerzieller Software entwickelt wurden.

Installieren Sie Prozessverwaltungssoftware

Mithilfe von Prozessverwaltungssoftware können erfahrene Benutzer auf Ihrem Mobiltelefon nach verdächtigen Prozessen suchen und diese beenden. Unter Windows Mobile können aufgrund von Hardwarebeschränkungen nicht allzu viele Prozesse ausgeführt werden. Protokollieren Sie daher alle Prozesse, die ausgeführt werden, wenn das Mobiltelefon sicher nicht infiziert ist. Zu jedem späteren Zeitpunkt sollte es einfach sein, einen böswilligen Prozess zu erkennen und ihn zu beenden, indem Sie die Anweisungen der Antivirensoftware für das Mobiltelefon befolgen.

Seien Sie vorsichtig mit Wi-Fi und Bluetooth

Deaktivieren Sie Wi-Fi und Bluetooth, wenn Sie sich außerhalb von Gebäuden befinden. Diese Funktionen können leicht zum Senden von böswilligem Code oder von Viren ausgenutzt werden. Außerdem können vertrauliche Informationen von Sniffer-Software abgefangen werden, wenn diese Funktionen aktiviert sind. Am besten sollten Sie diese Funktionen ausschließlich zu Hause sowie an vertrauenswürdigen Orten verwenden.

Erstellen Sie häufig Sicherungen

Kontaktlisten sind für Ihren Arbeitgeber und für Sie selbst äußerst wichtig. Wenn die Liste verloren geht oder gestohlen wird, kann dies verheerende Folgen haben. Sie sollten Daten, die auf mobilen Geräten gespeichert sind, häufig sichern. Auch wenn Ihr mobiles Gerät infiziert wird, können Sie so seine Standardeinstellungen wiederherstellen, um das System zu bereinigen.

Installieren Sie Antivirensoftware für Mobiltelefone

Die meisten großen Anbieter von Sicherheitssoftware bieten inzwischen eine Mobiltelefonversion ihrer Antivirenlösungen an, und viele Mobiltelefonanbieter bieten standardmäßig Antivirensoftware an. Es ist an der Zeit, Ihrem Smartphone den gleichen Schutz zukommen zu lassen wie Ihrem Desktopsystem.

Speichern Sie keine Unternehmensdaten auf Ihrem Mobiltelefon

Speichern Sie vertrauliche Dateien oder Fotos auf Wechseldatenträgern. Speichern Sie sie nicht auf mobilen Geräten. Mobiltelefone und PDAs sind nicht sehr sicher. Aus Profitgier werden voraussichtlich immer mehr Malware-Autoren Malware für Mobiltelefone schreiben. Das bedeutet im Endeffekt, dass die Gefahr nicht verschwinden wird.

Fazit

Mobiltelefone mit dem Betriebssystem Windows Mobile sind praktisch und werden immer beliebter. Da solche Mobiltelefone zahlreiche APIs enthalten, viele Benutzer ein zu geringes Sicherheitsbewusstsein haben und fette finanzielle Beute winkt, werden Malware-Autoren die Plattform in Anbetracht des sinkenden Risiko-Nutzen-Verhältnisses weiterhin angreifen. Der Großteil der heutigen Malware für Mobiltelefone stellt kein wesentliches Risiko für die Benutzer dar. Wir dürfen trotzdem nicht unachtsam werden. Momentan befinden wir uns am Anfang eines voraussichtlich lang andauernden Trends. Höchstwahrscheinlich kann es nur noch schlimmer werden, sodass Vorsicht bei der Verwendung Ihres Mobiltelefons unerlässlich ist.

Zhu Cheng betreibt wissenschaftliche Forschungen bei McAfee Avert Labs in Peking. Wenn er gerade nicht Code für das Produkt Network Access Control (NAC) von McAfee schreibt oder nach Malware für Mobiltelefone Ausschau hält, spielt er gern Tischtennis.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054, USA
888 847 8766
www.mcafee.com

© 2004-2007 McAfee, Inc. Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc. reproduziert werden. Die in diesem Dokument enthaltenen Informationen dienen lediglich Informationszwecken und stellen einen Service für Kunden von McAfee dar. Die hierin enthaltenen Informationen können ohne Vorankündigung geändert werden und werden "wie gesehen" ohne Gewähr bezüglich ihrer Richtigkeit oder Anwendbarkeit in einer bestimmten Situation zur Verfügung gestellt. McAfee, Avert und Avert Labs sind Marken oder eingetragene Marken von McAfee, Inc. in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.