

Handyviren – Mythos oder realistische Bedrohung?

Marko Rogge
Februar 2007

Viren, Würmer und Trojaner auf herkömmlichen Computern gehören fast schon zum Alltag in der heutigen Zeit. Auf Mobiltelefonen sind sie bislang noch weitgehend unentdeckt.

Mit der Verbreitung von Windows Mobile sowie SymbianOS auf Mobiltelefonen wird sich dies in naher Zukunft schnell ändern.

Immer öfter kann man in einschlägigen Medien von Viren und Trojanern hören, die sich auf Handys ausbreiten können.

Die Möglichkeiten sind bereits weit gefächert, da Trojaner und Viren Schnittstellen der Handys in vollem Umfang nutzen können.

Einmal in ein Handy eingepflanzt und installiert kann sich ein Schädling über WLAN, Bluetooth oder MMS weiter ausbreiten.

Bislang ist die Ausbreitung von Schädlingen für mobile Devices noch nicht weit voran geschritten.

Da aber die Hersteller die Geräte immer weiter entwickeln dürfte es nur noch eine Frage der Zeit sein, bis sich Viren, Würmer und Trojaner für SymbianOS [1] Handys oder Handys mit Windows Mobile schneller ausbreiten.

Sofern man sich ein wenig im Internet umschauf findet man ausreichend Programmierer, die derzeit an Schädlingen arbeiten, die diverse Schadroutinen vereinigen.

Es ist schon erschreckend wie leicht man an diese Schädlinge kommt.

Aber nicht nur Viren und Trojaner sind als Gefahr einzustufen, auch Spyware nimmt stetig zu.

CommWarrior – ein Vertreter der Handyschädlinge

Einer der ersten Schädlinge nennt sich CommWarrior und wurde vermutlich von einem russischen Programmierer entwickelt. Dieser Wurm hat 2 Schadroutinen mit denen er sich selbständig weiter ausbreitet.

Zum einen nutzt er die Bluetooth Schnittstelle des befallenen Mobiltelefons um sich auf andere Mobiltelefone zu verbreiten und er nutzt die MMS (Multimedia Service) um sich dann über das Adressbuch selbständig zu verschicken.

Der CommWarrior sendet sich mit immer wechselnden Dateinamen weiter, so das man hier nicht vor einem bestimmten Dateinamen warnen könnte.

Einen tatsächlichen Schaden am Gerät kann man jedoch nicht feststellen. Andere Schädlinge hingegen löschen das Menü oder die Schrift im Gerät.

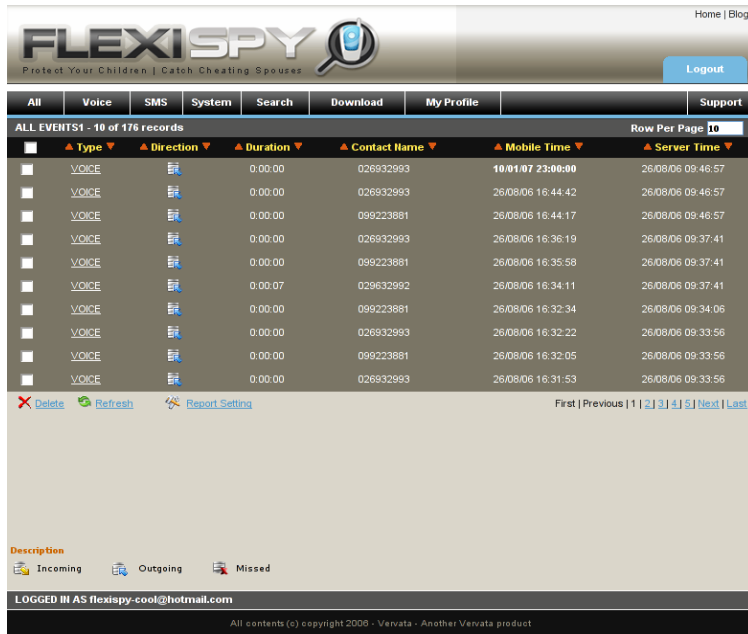
Flexispy – Software die Handys ausspioniert

Eine Software, die von den meisten Anti-Viren Softwareherstellern als Schadcode eingestuft wird ist Flexispy und hat überwiegend Fähigkeiten eines trojanischen Pferdes.

Flexispy sendet eine Kopie aller SMS Nachrichten weiter und protokolliert eingehende



und abgehende Anrufe inklusive der Gesprächsdauer. Sämtliche Informationen werden auf einem Server im Ausland gespeichert und stehen zum Abruf bereit um dann bequem per Browser heruntergeladen oder angeschaut zu werden. Auch das Ermitteln des Aufenthaltsortes ist mittels Flexispy möglich, da die jeweilige GSM Zelle übermittelt wird.

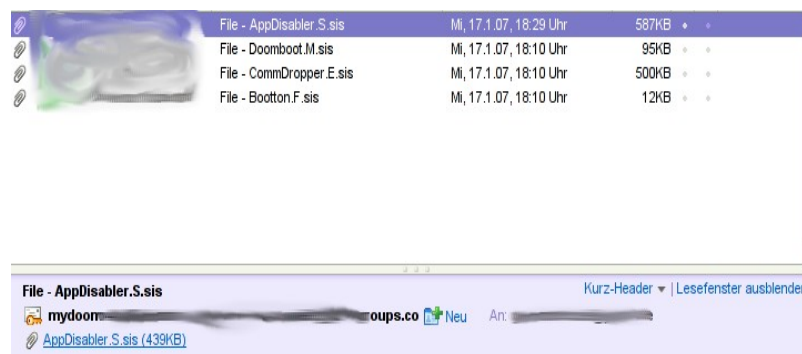


Flexispy listet im Browser alle geführten Gespräche auf und zeigt mit einem Mausklick die Details dieser an.

Die gleichen Funktionen stehen auch dem Spion bei den SMS zur Verfügung. Man kann exakt einsehen von wo nach wo eine SMS geschickt wurde und welcher Inhalt eine SMS hatte.

Die Ausbreitung von derartigen Schädlingen geschieht zum einen über das weiter verschicken per MMS oder aber auch auf dem direkten Weg mittels Bluetooth an empfangsbereite Geräte. So genannte Bluetooth Hotspots [2] können sehr einfach bei der Ausbreitung von mobilen Schädlingen dienlich sein.

Einschlägige Foren und Gruppen im Internet beschäftigen sich mit der Entwicklung und Verbreitung der neusten Schädlinge. So ist es zum Beispiel möglich durch reines Anmelden an einer Group sich die neuesten Viren und Trojaner über E-Mail bereitstellen zu lassen. Natürlich hat man hier auch die Möglichkeit auf Archive sämtlicher älteren Schädlinge zuzugreifen.



File : AppDisabler.S.sis
Description : AppDisabler.S

Your use of Yahoo! Groups is subject to <http://docs.yahoo.com/info/terms/>

Anti-Virus im Einsatz

Durch den Einsatz einer Anti-Viren Software für mobile Geräte kann hier ein erheblicher Schutz geboten werden. So wurden bei einem Test mit der mobilen Security Software F-Secure die derzeit bekannten und auf den im Internet angebotenen Viren mit hoher Sicherheit erkannt. Im Test wurde die aktuellste Version von F-Secure (Version 3.0 Build 13010, Scanner Build 6420 (117)) verwendet.



Nach einer Installation von F-Secure wird das Handy zuerst einer vollständigen Untersuchung unterzogen und sämtliche Dateien gescannt. Das Ergebnis wird anschliessend übersichtlich dargestellt. Eine Infektion durch einen Schadcode wird von F-Secure direkt auf dem Bildschirm gemeldet.

Wurde eine Infektion durch einen Schädling ausgemacht, kann man sich die Details anschauen um dann zu entscheiden ob die befallene Datei direkt gelöscht oder in Quarantäne gestellt werden soll.

Durch beide Aktionen kann der Schädling dem mobilen Gerät keinen Schaden mehr zufügen.

Im Bild zu sehen: Infektion eines Mobiltelefons durch drei Schädlinge.



Das größte infektionsrisiko besteht im Moment bei Geräten basierend auf der Symbian, bzw. der WindowsMobile Plattform.

Aber auch hier gibt es noch Unterschiede: So konnte zum Beispiel der Virus DoomBoot [3] nicht ein System der 3. Generation des SymbianOS befallen, da die meisten Schädlinge im Moment noch für das ältere Betriebssystem der 2. Generation programmiert wurden.



Fazit und Ausblick

Abschließend bleibt festzustellen, dass man in der Zukunft wesentlich mehr für die Sicherheit seines Handys tun muss als man es bis heute gewohnt war.

Viele Menschen werden erst spät die Gefahren von mobilen Schädlingen für mobile Geräte erkennen und zunächst keine Sicherheitsmechanismen einsetzen.

Hier im Bericht wurde überwiegend von Schädlingen berichtet die sich auf SymbianOS Telefonen ausbreiten, jedoch sind auch Windows Mobile Geräte nicht sicherer.

Grundsätzlich sollte man beim Empfang von Daten genau darauf achten, von wem diese gesendet wurden und, sofern man keine Daten erwartet, diese auch ablehnen.

Mobiltelefone werden immer flexibler in den Anwendungen und bieten immer mehr Speicherplatz an um Daten auszutauschen oder zu transportieren.

Auch die Kommunikationsmöglichkeiten um Bluetooth, Infrarot und WLAN nehmen stetig zu und bieten somit immer mehr Angriffsfläche für Schädlinge aber auch für aktive Angreifer.

Durch die zunehmende Ausbreitung von Betriebssystemen wie Microsoft Windows Mobile oder SymbianOS sind ebenfalls Angriffe durch Schwachstellen in den Architekturen und Protokollen möglich.

Viren, Würmer und Trojaner werden es in der Zukunft leichter haben sich per Mail, Schwachstellen und Mobiltelefonen auszubreiten.

In der heutigen Zeit sollte man einen ähnlich hohen Sicherheitsstandard an mobilen Endgeräten einsetzen wie es auf dem PC Bereich bereits üblich sein sollte um nicht unverhofft zum Opfer zu werden.

Verweise:

[1] <http://www.symbian.com/>

[2] <http://www.heise.de/security/artikel/81447>

[3] http://www.f-secure.com/v-descs/doomboot_a.shtml

F-Secure Mobile Security:

http://www.f-secure.de/home_user/mobile_security.html

Einblick in Flexispy:

http://msecure.blog.de/2007/01/12/handys_ausspionieren~1546236

Neue Bluetooth Hacks:

<http://www.heise.de/security/news/meldung/83043>

Trifinite:

http://trifinite.org/trifinite_org.html

Trend Micro Mobile Security:

<http://www.trendmicro.com/en/products/mobile/tmms/>

(War jedoch nicht für SymbianOS 9.1 erhältlich. Daher kein Vergleich)

Literatur:

Daniel Bachfeld, Wurmflug, Bedrohung von Smartphones durch Handy-Viren, c't 13/06, S. 156

Daniel Bachfeld, Wurmklatsche, Virens Scanner für Symbian-Handys, c't 13/06, S. 160

Fotos:

Mit freundlicher Genehmigung von F-Secure

Marko Rogge, <http://www.marko-rogge.de>

Vervielfältigen mit Genehmigung des Autors erlaubt.