# Handys im Visier der Virenschreiber

**Mobiltelefone der heutigen Generation sind mehr als blosse Kommunikationsgeräte: Sie sind intelligente Multimediacenter, die sich kaum von Palmtops unterscheiden – und deswegen auch anfällig für die Sicherheitsprobleme der PC-Welt sind.**

### *Wie alles begann*

Mit «Mosquitos» beginnt im Frühjahr 2004 die Ära der Handy-Piraterie: das Spiel wird von einem Trojaner infiziert und sendet Nachrichten an teure und gebührenpflichtige Rufnummern und verursacht dadurch erheblichen Schaden bei seinen unwissenden Opfern. Kurz darauf taucht im Juni 2004 der Wurm «Cabir» auf, der sich über eine aktive Bluetooth-Verbindung repliziert und Telefone mit Symbian-Betriebssystem attackiert. Im November 2004 werden erneut Symbianbasierte Smartphones zum Angriffsziel: Von Websites, auf denen Shareware-Anwendungen für das Symbian-Betriebssystem zu finden sind, laden sich Benutzer mit vermeintlich nützlichen Anwendungen «Skulls» herunter. Der Trojaner verbirgt sich hinter Dateien mit den Namen «Extended Theme Manager» oder «Timer Room» und blockiert nach Installation die Funktionsweise der Anwendungen. Benutzer können dann nur noch Anrufe tätigen und annehmen und die Infektion wird durch Totenköpfe, die anstelle der üblichen Symbole im Display erscheinen, sichtbar. Skulls ist nur schwer zu entfernen, und manchmal kann sogar der Verlust aller auf dem Telefon installierten Informationen die Folge sein. Unerwünschte Telefongebühren erzeugt der im März 2005 entdeckte Virus «CommWarrior». Er greift Series60-Mobiltelefone an und überrascht durch seine «Intelligenz». Tagsüber verbreitet er sich via Bluetooth und nachts versendet er MMS-Nachrichten mit der CommWarrior-SIS-Datei. Stimmt der Benutzer der Installation zu, wird das Handy infiziert.

### *Wo die Reise hingeht*

Bis heute ist die Zahl der Handyviren auf über 350 gestiegen. Die Viren verursachen Anomalien auf dem Telefon, zum Beispiel eine Zunahme der Kommunikationsaktivitäten, schnell aufgebrauchte Batterien, unerwünschte Nachrichten und das Löschen oder Verändern von Symbolen. Abgesehen von diesen lästigen Fehlfunktionen haben Handy-Nutzer durch die derzeitigen Mobiltelefonviren aber nur wenig zu befürchten.

Unterschätzt werden sollte die Situation jedoch nicht. Am meisten gefährdet ist die Privatsphäre der Handy-Nutzer. Denn das Mobiltelefon stellt mit seinen Rufnummern, Nachrichten, der Terminplanung und anderem eine allgemeine Quelle persönlicher Daten dar. Diese Informationen können durch eine Malware-Infektion gelöscht, verändert oder gestohlen werden. Auch Unternehmen sollten sich der Gefahr von mobilen Schädlingen bewusst sein, da über Smartphones heutzutage auch sensible Geschäftsdaten verbreitet werden und auch auf das Unternehmensnetzwerk zugegriffen wird. Mögliche Gefahren lauern zum Beispiel bei Viren, die von den Mobiltelefonen der Mitarbeiter auf die PCs springen und umgekehrt. So geschehen im Februar 2006 durch den Trojaner «RedBrowser», der mobile Telefone beliebiger Hersteller mit Java(J2ME)-Unterstützung befallen hat. Er gelangte über das Internet auf Mobiltelefone, aber auch über Bluetooth-Verbindungen oder direkt von PCs aus. Der Wurm «Mobler» konnte sich zwischen Symbian und Windows XP Plattformen bewegen; seine Auswirkung auf das Symbian-Gerät war zwar relativ harmlos, stellte jedoch einen gefährlichen Präzedenzfall dar.

### *Pssst, da hört jemand mit*

In der Grauzone zwischen mobiler Malware und nützlichen Add-on-Softwareanwendungen arbeitet mobile Spyware. Ein prominentes Beispiel ist «Flexispy», der im April 2006 für Furore sorgte. Typische Funktionen solcher Spyware sind SMS-Weiterleitung, Log-Informationen zu SMS und Telefonaten, Remote-Listening und verborgene Konferenzschaltungen. Einige verfügen sogar über Lokalisierungsdienste. Das Opfer eines mobilen Spionageangriffs verliert seine gesamte Privatsphäre, und die Person, die die Software kontrolliert, hat Zugriff auf alle, mit dem Handy durchgeführten Aktivitäten.

### *Schutzschild – auch für Handys sinnvoll*

Ohne eine Sicherheitsanwendung kann ein Virus kaum erkannt werden. Handy-Schädlinge nutzen zahlreiche Verbreitungswege. Die Hauptgefahr besteht in der zunehmenden Automatisierung wie bei Cabir, in der Anwendung von Bluetooth oder der Installation vermeintlich nützlicher Handyanwendungen, die sich dann als Trojaner oder Spyware entpuppen. Die Verbreitung kann zudem über das Senden infizierter Nachrichten erfolgen, wobei TCP/IP-Verbindungen direkt von den Anwendungen geöffnet werden und die Verbreitung der Malware erleichtern können. Damit sich Mobiltelefonbenutzer erst gar keinen Schädling einfangen, sollten sie vor der Installation einer neuen Software oder dem Herunterladen von Anwendungen aus dem Internet die Quelle der Software prüfen und die Funktionsweise des Telefons direkt nach der eingerichteten Änderung im Auge behalten. Schädlingen, die sich per Bluetooth verbreiten, kann durch das Ausschalten des «Discoverable Modus» vorgebeugt werden. Trotzdem gilt: Für ein ausreichendes Mass an Sicherheit ist eine sich automatisch aktualisierende Virenschutzsoftware erforderlich. Ein guter Virenschutz analysiert automatisch alle Dateien des Telefons, sobald es benutzt wird. Wichtig ist auch eine Echtzeit-Scan-Funktion, die zur Vorbeugung von Infektionen automatisch alle Dateien abfängt und analysiert, sobald sie gespeichert, kopiert oder herunter geladen werden.

*Klaus Jetter*