Zwischen Hysterie und falscher Sicherheit

Handyviren Alle bisher aufgetauchten Handy- und Smartphone-Viren sind zwar lästige, aber harmlose Laborratten. Dennoch sind sich Sicherheitsexperten einig, dass es nur noch eine Frage der Zeit ist, bis sich wirklich bösartige Krabbler in Mobiltelefonen einnisten.

Claudia Bardola

Sicherheitsexperten sind sich einig, dass es nur noch eine Frage der Zeit ist, bis sich fiese Viren und Würmer auch auf Quasselknochen breit machen. Bild:CW/gis

Bis vor gar nicht allzu langer Zeit galten Mobiltelefone als relativ unintelligente, aber abgeschottete Systeme: Mehr als Telefonieren und das Verfassen von Textnachrichten lag nicht drin. Inzwischen bringen die Herstellerinnen ihre Geräte mit jeder neuen Generation ein Stück näher an den PC. Selbst die billigsten Quasselknochen verfügen heute über ausgeklügelte Funktionen, sind erweiterbar und beherbergen damit eine Fülle von Daten. Damit werden sie auch für die Virenschreiber interessant. Panik sei zwar nicht angesagt, in absoluter Sicherheit sollten sich Mobiltelfonierer aber dennoch nicht wiegen, kommentiert Christoph Baumgartner, Chef des Thalwiler Security-Beratungshauses Oneconsult.

Der 14. Juni 2004 ist sowohl in die Mobilfunk- als auch in die Virengeschichte eingegangen: Er gilt als Geburtstag des ersten Handywurms. Cabir, so sein Name, befällt mit Vorliebe die aktuellsten Mobiltelefonmodelle, die auf dem offenen Betriebssystem Symbian laufen. Dabei verbreitet sich Cabir über die Kurzstreckenfunktechnik Bluetooth, die eigentlich für die Synchronisation mit anderen Gerätschaften vorgesehen ist. Er kann sich allerdings nur auf jenen Geräten einnisten, die so konfiguriert sind, dass sie eingehende Verbindungen akzeptieren. Ausserdem benötigt er, um sich installieren zu können, die aktive Zustimmung des Benutzers.

In diesem Beitrag:

- Warum die Verbreitung von Handy-Viren über die Nahfunktechnik Bluetooth erfolgen wird.
- Welchen Schaden die Minischädlinge theoretisch anrichten könnten.
- Was die Hersteller von Security-Software und vonMobiltelefonen gegen die drohende Virenwelle unternehmen wollen.

Einfallstor Bluetooth

Waren sich Sicherheitsexperten vor Cabir noch einig, dass die Verbreitung von Handyviren vor allem über SMS (Short Massage System) erfolgen würde, so sind sie inzwischen überzeugt, dass in erster Linie der Bluetooth-Standard als breites Einfallstor herhalten wird. So gibt etwa Mark Rowe, Consultant bei der britischen Sicherheitsberaterin Pentest zu Protokoll: «Wir haben verschiedene, noch nicht publizierte Lücken entdeckt, durch die Würmer ohne das Zutun des Gerätebesitzers hochgeladen und ausgeführt werden können.» Offiziell schafft der Blauzahn-Standard eine Distanz von rund zehn Metern. Rowe widerlegt: «Mit entsprechenden Richtantennen konnten wir Reichweiten bis weit in den Hundertmeter-Bereich erzielen. Damit könnte eine Vielzahl von Mobiltelefonen gleichzeitig infiziert werden.» Dass Blue tooth ein idealer Einfallsport ist, liegt laut Baumgartner nicht an Sicherheitslecks im Protokoll selbst, sondern vielmehr an einer unsauberen Implementierung der Hersteller. Der Sicherheitsexperte empfiehlt, die Nahfunkfunktion generell zu deaktivieren oder sie nur in sicherer Umgebung zu benutzen.

Zwei Monate nach Cabir wurde Duts entdeckt, der erste Virus, der es auf das Microsoft-Betriebssystem Pocket PC abgesehen hat. Verfasst hat ihn die russische Hackertruppe 29a, die auch für Cabir verantwortlich zeichnet. Beide Viren hatten eigentlich nur eine Aufgabe: Sie sollten lediglich die Machbarkeit von dedizierten Handyschädlingen beweisen. Die Hackerszene spricht in diesem Zusammenhang von Proof-of-Concept-Viren. Diese haben quasi einen Demo-Charakter und werden von den Autoren selbst an die Sicherheitslabors entsandt.

Im August schliesslich machte der Smartphone-Virus Bardor von sich reden, der das Microsofts Betriebssystem Windows CE bevorzugt. Im Gegensatz zu seinen beiden harmlosen Vorgängern meint er es ernst. «Bardor ist voll funktionsfähig und kommt in zerstörerischer Absicht», kommentierte die russische Antivirenspezialistin Kaspersky Labs. Bei Bardor handelt es sich um einen klassischen Trojaner. Er schickt die IP-Adresse des von ihm befallenen Pocket-PC an seinen Autor. Letzterer kann schliesslich über eine geöffnete Hintertüre die Kontrolle über das Gerät übernehmen. Damit ist er etwa in der Lage, Daten einzuspeisen und herunterzusaugen oder kann auch Applikationen starten. Bardor verfügt allerdings über keine eigene Verbreitungsroutine, sondern wird ausschliesslich als E-Mail verschickt. Das heisst, nur wenn der Empfänger den Mail-Anhang auf seinem Hosentaschenrechner öffnet, kann er sich auch installieren

Eine Frage der Zeit

Alle bisherigen Handy- und Smartphone-Viren sind zwar lästig, aber als Laborraten harmloser Natur zu bezeichnen. Die Sicherheitsexperten sind sich jedoch einig, dass es nur noch eine Frage der Zeit ist, bis wirklich bösartige Krabbler die mobilen Telefonierer heimsuchen. So prognostiziert etwa Eugene Kaspersky, Chef von Kaspersky Labs, dass die Handyschädlinge derzeit die gleiche Entwicklungsphase wie einst ihre PC-Vorfahren durchlaufen. Er prophezeit gar einen «recht baldigen ernsten Ausbruch» der Miniviren. In die gleiche Kerbe haut Baumgartner und zeichnet ein ziemlich düsteres Bild: Der Experte ist überzeugt, dass sich das Problem innerhalb des nächsten Jahres massiv verschärfen wird. «Mit der Einführung von Standards wie UMTS erwarten uns ungeahnte Bandbreiten für den Mobilfunk. Die Handys selbst mutieren immer mehr zu Minicomputern mit vollem Funktionsumfang und stellen damit potenzielle Access-Points dar. Die Spam-Industrie ihrerseits sucht nach neuen Kanälen für den Versand ihrer Werbemails und könnte einen solchen in den Mobiltelefonen finden. Mit Hilfe von eingeschleusten Programmen könnten sie letztere als Vermittlungspunkte missbrauchen.»

Derweil geht die Antivirenspezialistin F-Secure da von aus, dass viele der künftigen Schädligen darauf abzielen werden, die Kommunikation auf teure Dienstnummern umzuleiten. Ebenfalls denkbar wäre, dass die Malware-Schreiber Spyware auf die Mobiltelefone verschicken, die den Benutzer ausspionieren.

Frisches Ackerland

Für die Virenschutzspezialistinnen erschliesst sich mit dem Auftauchen der Handyviren neues Ackerland, das sie bearbeiten können. Mittelfristig dürften sich Sicherheitsapplikationen für Mobiltelefone zu einem geschäftsträchtigen Segment entwickeln, glauben Marktbeobachter.

Als erste ist F-Secure auf den rollenden Zug aufgesprungen und hat kürzlich eine kommerzielle Antivirensoftware für Smartphones auf den Markt geworfen. Das Tool, das auf den Namen Mobile Anti-Virus hört, soll Geräte in Echtzeit vor den Viren und Würmern schützen. Dabei sollen die Virensignaturen automatisch über das Mobilfunknetz aktualisiert werden, verspricht F-Secure.

Baumgartner ist überzeugt, dass bald auch die Gerätehersteller in Sachen Security nachziehen werden. «Derzeit treffen sie zwar nicht einmal die trivialsten Sicherheitsvorkehrungen, doch in Kürze werden die ersten Hersteller damit beginnen, einschlägige Sicherheitsfunktionen einzubauen. Damit ist jenen Firmen ein massiver Wettbewerbsvorteil gewiss», so Baumgartner. Dasselbe dürfte seiner Meinung nach auch auf die Mobilfunkbetreiber zutreffen. «Diese könnten mit relativ geringem Aufwand adäquate Filtertechniken einsetzen und sich gegenüber der Konkurrenz einen Vorsprung herausholen. Baumgartner will wissen, dass sich auch das helvetische Providerumfeld bereits entsprechende Gedanken macht und «die eine oder andere Betreiberin» bereits den Evaluationsprozess für ein Intrusion-Detection-System eingeleitet hat.

Impressum

Computerworld
Wiltikonerstrasse 15, Postfach 253,8030 Zürich
http://www.computerworld.ch

Tel. Verlag und Redaktion 01 387 44 44
Tel.Anzeigen 01 387 45 55
Tel. Veranstaltungskalender 01 387 45 34
Tel.Abonnemente 071 314 04 49
Fax Verlag und Redaktion 01 387 45 80
Fax Anzeigen 01 387 45 83
Fax Abonnemente 071 314 04 08
ISSN 1420-5009
«Computerworld» ist offizielles Organ des VIW.

Redaktion
Chefredaktion:Karlheinz Pichler (kapi)
karlheinz.pichler@computerworld.ch
Diese Woche:
Leitung:Jens Stark (jst) und Beat Hochuli (hoc)
jens.stark@computerworld.ch
beat.hochuli@computerworld.ch
Claudia Bardola (bac)
claudia.bardola@computerworld.ch
Catharina Bujnoch (cb)
catharina.bujnoch@computerworld.ch
Fredy Haag (fha),fred y.haag@computerworld.ch
Michael Keller (mk)
michael.keller@computerworld.ch
Volker Richert (vr), volker.richert@computerworld.ch

Dossier:
Fredy Haag (fha),fred y.haag@computerworld.ch
Corinne Schmidt (cs)
corinne.schmidt@computerworld.ch
Produkte und Lösungen:
Volker Richert (vr), volker.richert@computerworld.ch
Fredy Haag (fha),fred y.haag@computerworld.ch
Test und Produkte:Andreas Heer (ahe)
andreas.heer@computerworld.ch
Regelmässige Mitarbeit:
Christian Fichter (cf),Gregor Henger (gh)
Dirk Pelzer (dp),Josef Wetzel (jw)
Markus Zitt (mz),René Uhlmann (ruh)
Thomas Hürlimann (thü),thu@ecliptic.ch
Computerworld Online:
Karlheinz Pichler (kapi)
karlheinz.pichler@computerworld.ch
Michael Keller (mk)
michael.keller@computerworld.ch
Fokus und Specials:
Catharina Bujnoch (cb)
catharina.bujnoch@computerworld.ch
Beat Hochuli (hoc), beat.hochuli@computerworld.ch
Redaktionsassistenz:
Gaby Kirschbaum
gaby.kirschbaum@computerworld.ch

Bild,Grafik & Layout:
Ernst Tanner (eta),ernst.tanner@computerworld.ch
Gilles Steinmann (gis),gis@computerworld.ch
Nina Osterwalder (nos),nos@computerworld.ch

Anzeigen
Gesamtleitung Anzeigen IDG:
Kurt Strebel,kurt.strebel@idg.ch
Lokaler Verkauf:
Rolf Fischer, rolf.fischer@idg.ch
Esther Majoleth,esther.majoleth@idg.ch
Internationaler Verkauf/Online:
Urs Flückiger, urs.flueckiger@idg.ch
Administration/Disposition:
Natalie Rickli,natalie.rickli@idg.ch (Leitung)
Madeleine Meyer, madeleine.meyer@idg.ch

Grundpreise
Empfehlungsanzeigen: Fr. 3.10/mm
Stellenanzeigen: Fr. 3.45/mm
Rubrikanzeigen:Schulen/Kurse Fr. 2.75/mm
Dienstleistungen, Verschiedenes Fr. 2.65/mm
Stellengesuche,Kaufgesuche, Occasionen,freie Kapazität: Fr. 2.35/mm
Mindestmasse aller Inserate: 2 Spalten = Breite 55 mm,Höhe 20 mm

Marketing und Vertrieb
Nicole Ehrat,nicole.ehrat@idg.ch

Buchhaltung:
Anton Müller, anton.mueller@idg.ch

Verlagsleitung
Gebhard Osterwalder, gebhard.osterwalder@idg.ch

Abonnemente
Adressänderungen:
CW-Leserservice, Postfach, 9026 St.Gallen
Tel.071 314 04 49, Fax 071 314 04 08
abo@computerworld.ch
Bezugspreise:
Computerworld erscheint 50-mal im Jahr, jeweils am Freitag.Einzelverkaufspreis Fr.5.80, Jahresabonnement Fr. 259.–

Druck
St.Galler Tagblatt AG

Gesamtleitung IDG Schweiz
Gebhard Osterwalder, gebhard.osterwalder@idg.ch

Im Verlag IDG Communications AG erscheinen folgende drei Schweizer Publikationen:

Computerworld PCtipp
Computerworld magazin