Dialer

Was sie sind, wie sie funktionieren und wie man sich dagegen schützen kann

Jan Manuel Tosses

12. September 2004

Zusammenfassung

Gegenwärtig zählen neben Viren und Würmern vor allem "Dialer" zu den größten Schwächen des Internets, von denen vor allem das Windows Betriebssystem betroffen ist. Während die meisten Viren und Würmer bei Privaten nur geringen wirtschaftlichen Schaden verursachen, weil sie meist nur vorübergehend die Funktion von Netzwerken und PCs einschränken, greifen Dialer immer direkt in den Geldbeutel der Betroffenen.

1 Was sind Dialer?

Dialer sind Anwahl Programme, die dem Nutzer Zugang zu gebührenpflichtigen Diensten ermöglichen, die mit den Telefongebühren abgerechnet werden. Diese Programme werden zunehmend auch in betrügerischer Absicht verwendet, indem sie sich ohne Kenntnis des Nutzers in seine EDV einschleichen. Seit der Freigabe der 0190er Mehrwert Dienste Rufnummern sind den Verbindungskosten praktisch keine Grenzen mehr gesetzt.

2 So funktioniert ein Dialer

Dialer finden sich überwiegend auf Internetseiten, manchmal aber auch auf CD-ROMs und in Emails. Zumeist verbergen sie sich hinter einem harmlos klingenden Link, der mit der zu erreichenden Adresse dann wenig oder nichts zu tun hat. Nach dem Klick auf den Link in Internetseite oder Email öffnet sich ein Programm, das sich als Teil der Internetseite oder des Email Programms tarnt. Nach einer verwirrenden Zustimmungsabfrage installiert sich ein Programm fest im Betriebssystem, das das betriebssystemeigene Wahlprogramm durch ein Programm ersetzt, das nun gebührenpflichtige und meist sehr teure Nummern für telefonische Mehrwert Dienste im In- und Ausland anwählt. Diese Einwahl ins Internet kann zu Gebühren im mehrstelligen Eurobereich führen.

Betroffen sind hierbei vor allem Nutzer von digitalen ISDN- und analogen Modem-Telefonverbindungen auf der Microsoft Windows Plattform.

3 Beispiele für Dialer

Dialer kommen in unterschiedlichen Gewändern daher. Nachfolgend eine Liste der gebräuchlichsten Typen: Der Dialer tarnt sich als preiswerte Dienstleistung,

Nachschlagewerk oder ähnliches und wird per Klick herunter geladen und sofort ausgeführt. Die Kosten für einen Verbindungsaufbau der telefonischen Mehrwert Dienste Nummer werden meist ebenso verschleiert, wie die Verbindung selbst. Der Dialer stellt sich als nützliches und meist kostenloses Werkzeug vor und ist als solches auch benutzbar. Beispiele hierfür sind Gebührenrechner, Virenschutz Software, Dialer Entferner, Spam Schutz Programme und dergleichen. Der Dialer installiert sich tief im System und leitet alle künftigen Internet Anwahlen auf seine vordefinierten Mehrwert Dienste Nummern um. Der Dialer wird per Email versendet und nach einem Klick ausgeführt. Der Dialer tarnt sich als witzige Animation oder Warnhinweis und verrät nichts über seine tatsächliche Funktion. Nach seiner Installation ist er nur von Experten zu entfernen.

4 Wie man sich vor Dialern schützen kann

Einen absoluten Schutz gegen Dialer gibt es nicht. Allerdings kann man es Betrügern deutlich schwerer machen. Hierzu stehen dem Nutzer verschiedene Möglichkeiten offen.

4.1 Schutz beim Telekommunikationsdienstleister

Bestimmte Rufnummern zu sperren, hilft nur kurzfristig, da auch Kriminelle die verfügbaren Sperrlisten einsehen können und jede gesperrte Vorwahl eben auch die Anwahl zu legalen Diensten in diesem Vorwahlbereich verhindert. Manche Telekommunikationsdienstleister bieten auch die automatische Berücksichtigung eines vom Kunden gewünschten Gebührenlimits an. Das ist aber meist nur bei konstanten Gebührenrechnungen sinnvoll. Dann kann das Limit vor zu unangenehmen Überraschungen schützen.

4.2 Schutz durch Software und Hardware

Computer mit dem Microsoft Windows System sollten nicht direkt mit dem Internet verbunden sein. Alle Systeme sollten auf dem aktuellen Stand sein. Antiviren Software kann es Betrügern schwerer machen, ist oftmals aber leicht zu umgehen. Antiviren Software muss laufend aktualisiert werden, sonst täuscht sie eine falsche Sicherheit vor: Es ist das Spiel von Igel und Hase. Es gibt Software, die dem Schutz vor Dialern und auch deren Löschung dienen. Solche Software sollte von Experten heruntergeladen und installiert werden, da sich Dialer gern als Schutzprogramme tarnen. Wird ein Windows NT, 2000 oder XP System eingesetzt, sollte der Benutzer nicht im Administrator Modus angemeldet sein, der bekanntlich alle Schutzmechanismen aus hebelt. Firewalls nützen grundsätzlich nicht gegen Dialer. Sicher schützen derzeit nur Einwahl Router, die zwischen Computer und Telefonsystem geschaltet werden. Dialer können solche Router weder umgehen, noch umkonfigurieren. Solche Router können wahlweise angepasste Linux Systeme sein oder beim PC Händler günstig gekauft werden. Linux- und Mac OS X Systeme sind als Unix Systeme gegen Dialer resistent. Tief implementierte Schutzmechanismen machen hier die unerkannte Installation von Dialern unmöglich.

5 Was tun bei Verdacht auf Dialer

Vermuten Sie einen installierten Dialer in Ihrem System, so trennen Sie den Rechner umgehend vom Telefonnetz und fordern sie eine ungekürzte Einzelaufstellung von ihrem Telekommunikationsdienstleister an.

Bestimmte Dateien des Rechners sollten zur Beweissicherung auf Diskette oder CD gespeichert werden. Bitten Sie Ihren Systemadministrator oder ihren Computerservice darum, die entsprechenden Daten zu sichern.

Erst nach einer Beweissicherung sollten die entsprechenden Programmteile von Experten entfernt werden. Besonders hartnäckige und trickreiche Dialer sind selbst von Experten erst nach Stunden sicher aus dem System entfernt.

6 Hinweise und Tipps

Speichern Sie Programme und Dokumente in Internet und Email immer erst auf die Festplatte und führen Sie diese nur nach einem Virencheck aus. Was hier umständlich wirkt mag Ihnen viel Geld sparen.

Vergewissern Sie sich erst, ob ein Dokument auch von demjenigen versendet wurde, dessen Name im "Von"-Feld steht. Seien Sie misstrauisch! Löschen Sie fragwürdige Emails.

Dialer können auch über ein mobiles Internet oder im Hotel via Notebook funktionieren. Einen Dialer auf dem Notebook nimmt man überall hin mit.

7 Glossar der verwendeten Fachbegriffe

7.1 DSL

Auf Netzwerkprotokollen basiertes Verfahren, sich mit dem Internet zu verbinden. Die Verbindungsgebühren werden vom Dienstleister in Rechnung gestellt. Das DSL ist derzeit nicht durch Dialer angreifbar.

7.2 Firewall

Eine Firewall schützt in erster Linie vor unerwünschten Verbindungen aus dem Internet oder in das Internet, aber nicht vor Dialern.

7.3 ISDN

Auslaufendes digitales, telefonbasiertes Verfahren, sich mit dem Internet zu verbinden. Ebenso wie bei analogen Modem Verbindungen werden die Verbindungsgebühren über die Telefonrechnung gezahlt. Alle bekannten Dialer nutzen ISDN oder analoge Modem Verbindungen.

7.4 Modem

Der Modem (Modulator/Demodulator) wandelt analoge Signale in digitale Informationen um und umgekehrt.

7.5 Router

Ein Router ist ein kleiner Computer, der sich bei Bedarf automatisch ins Internet einwählt und die Verbindung freigibt. Router haben feste Einwahl Daten zum Verbindungsaufbau, die nur mit entsprechenden Kennworten änderbar sind.

7.6 Trojaner

Trojaner sind Programme, die neben einer scheinbaren Hauptfunktion (witzige Animation, kleines Werkzeug) eine weitere verdeckte Funktion beinhalten. Solche Funktionen können die Installation von Dialern, Viren und Würmern sein. Andere Trojaner veranlassen beispielsweise den eigenen Rechner, Massenwerbung aus dem Internet zu versenden.

7.7 Viren

Viren sind Programme, die sich meist, aber nicht nur über das Internet verbreiten und eine Interaktion mit dem Nutzer voraussetzen (Zum Beispiel "Speichern", "Öffnen" oder Ähnliches). Sie können über Makros in Microsoft Office Produkten, über Emails, den Internet Explorer, über CD-Roms, Software-DVDs und Disketten eingeschleppt werden. In vielen Fällen enthalten sie Schadenroutinen, die beim Aufruf bestimmter Daten oder nach einer vordefinierten Anzahl von Benutzeraktionen gestartet werden. Schadenroutinen können beispielsweise die Löschung bestimmter Dateien oder Bibliotheken sein. Praktisch sind hiervon nur Microsoft Windows Systeme betroffen.

7.8 Würmer

Würmer sind Programme, die sich ohne weitere Interaktion mit dem Benutzer verbreiten. Würmer benutzen Sicherheitslücken in Programmen, um sich fortzupflanzen. Würmer sind fast ausschliesslich auf Microsoft Windows Systeme spezialisiert. Würmer breiten sich verstärkt über Emails, aber auch zwischen Servern aus, die auf anderen Betriebssysteme beruhen.