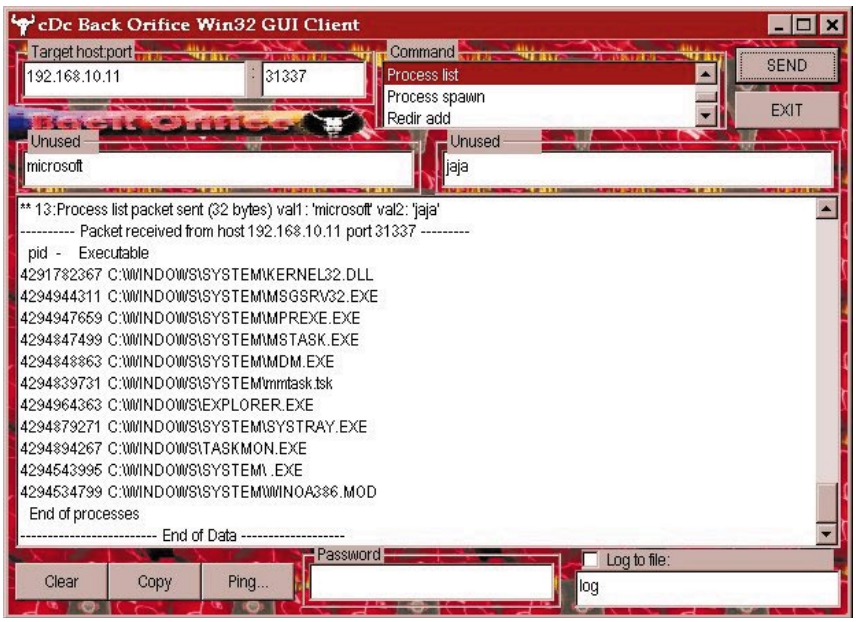
Windows: Hacker-Tool schafft den gläsernen PC

Spion im Netz

In Hackerkreisen kursiert ein kleines Programm, mit dem sich Windows-95/98-Systeme kinderleicht über das Internet ausspionieren lassen. Microsoft spielt die Gefahr herunter; die Anwender müßten eben selber aufpassen



Das Hacker-Tool Back Orifice in Aktion: Die Abbildung zeigt die Liste der laufenden Anwendungen auf einem ausspionierten Rechner

Ein Hacker-Tool mit dem Namen „Back Orifice“ (BO) sorgt derzeit bei Systemverwaltern und Online-Anwendern für Unruhe. Das Programm, das als Trojanisches Pferd in ein Windows-95/98-System eingeschleust wird, erlaubt die absolute Kontrolle des infizierten Systems über eine aktive IP-Verbindung – also beispielsweise über das DFÜ-Netzwerk von Windows. Zusatz-Tools erlauben es, Back Orifice ohne großen Aufwand an beliebige Programme anzuhängen.

Wird das Trägerprogramm einmal gestartet, installiert sich BO selbst so, daß es bei jedem folgenden Systemstart zu den standardmäßig geladenen Services gehört. Dabei verbraucht Back Orifice im Betrieb so wenig Ressourcen, daß es dem Benutzer nicht weiter auffällt.

BO ist seit Anfang August 1998 verfügbar, und inzwischen sollen bereits über 100.000 Kopien direkt von der Website der Hacker heruntergeladen worden sein. Über den Programmaustausch zwischen nichtsahnenden Anwendern dürfte es sich inzwischen weit verbreitet haben.

Sie können sich BO über jede ausführbare Datei einfangen, die Sie irgendwo herunterladen oder von jemandem bekommen – also auch über selbstextrahierende komprimierte Dateien.

HINTEREINGANG

Back Orifice steuert Ihr System

Ende Juli 1998 zeigte die in Hacker-Kreisen bekannte Gruppe „Cult of Dead Cow“ (CdC) ihr neuestes Tool erstmals auf der Hacker-Konferenz Dev-con 6 in Las Vegas. Bereits der Name „Back Orifice“ (dezent übersetzt „Hintereingang“) macht deutlich, daß es sich um ein Hacker-Tool handelt – die gewisse Namensähnlichkeit zu Microsofts „Back Office“ ist wohl auch beabsichtigt.

BO ist mit nur 124 KB ein äußerst effizientes Stück Programmierkunst. Über einen wählbaren TCP/IP-Port kann ein Hacker unbemerkt die Kontrolle über das System erlangen, wenn eine Verbindung ins Internet oder Intranet steht. Die Möglichkeiten, die sich ihm jetzt bieten, übersteigen sogar die, die dem eigentlichen Benutzer ohne Zusatzprogramme auf seinem System zur Verfügung stehen. Der Hacker kann per Fernsteuerung Kommandos starten, Datei-Up- und -Downloads initiieren, Einträge in der Registry manipulieren oder die Systemfreigaben (Drucker, Netzlaufwerke) für sich nutzen und erweitern. Um den Anwender zu irritieren oder bestimmte Handlungen auszulösen, lassen sich beliebige Systemmeldungen auf dem Bildschirm ausgeben oder Sounddateien abspielen.

Eine Spitzel-Funktion sucht an den bekannten Stellen nach Paßwörtern und gibt diese als Liste aus. Um einfacher an diese Daten zu gelangen, besteht die Möglichkeit, alle Tastatureingaben zu protokollieren oder Bildschirminhalte in einer Datei zu speichern. Ist an dem überwachten PC eine Videokamera aktiv, so kann der Beobachter von dieser Quelle AVI-Dateien mitschneiden. Alle auf diese Weise lokal erstellten Dateien lassen sich dann schnell zu einem beliebigen System übertragen. Über die Online-Verbindung kann man neue Programme unauffällig installieren und auch wieder unbemerkt aus dem System entfernen.

SPIONAGETECHNIK

So arbeitet Back Orifice

Der infizierte PC übernimmt die Rolle des „Servers“, der zur verschlüsselten Kommunikation über das Netz mit UDP (User Datagram Protocol) arbeitet, um vom angeschlossenen „Client“ Kommandos entgegenzunehmen und auszuführen. Die Kommunikation zwischen den beiden BO-Komponenten selbst startet erst nach der Eingabe eines vorher definierten Benutzernamens mit Paßwort. Danach stehen alle Tore auf dem Zielrechner offen. Der BO-Client ist sowohl für Windows (als grafisches Front-End oder kommandozeilenorientiert) als auch als „Open Source“-Variante (also mit Quelltext) für Unix verfügbar.

Die Kommunikation per UDP verlangt neben der aktiven Verbindung auch eine genau definierte IP-Adresse des angeschlossenen PCs. Die Tatsache, daß speziell in Unternehmen IP-Nummern oft fest vergeben werden, erleichtert Hacker-Angriffe ungemein. Doch auch dynamische IP-Adressen sind keine unüberwindliche Hürde. Wer eine IP-Adresse kennt, kann von dort aus das gesamte Subnetz – etwa den Adreßpool eines Internet-Providers oder ein Unternehmensnetz untersuchen („sweepen“), um infizierte Rechner oder Sicherheitslücken (etwa freigegebene Verzeichnisse) zu finden. Auf diesem Weg werden dann auch weitere Rechner mit BO angesteckt.

RISIKO ANTI-TOOLS

Trojaner in Virenscannern

Inzwischen finden Sie auf Hacker-Seiten im Internet Erweiterungen, die aus Back Orifice eine noch gefährlichere Waffe machen können. Mit diesen Programmen läßt sich beispielsweise die IP-Adresse des überwachten Systems automatisch an einen weltweit offenen IRC-Kanal (Internet Relay Chat) oder per E-Mail an beliebige Adressaten weitergeben.

Immerhin hinterläßt BO doch einige Spuren, die Sie gezielt suchen können, um Gegenmaßnahmen zu ergreifen. Erste BO-Scanner (→ Kasten „Back Orifice: So erkennen und entfernen Sie es“) sind ebenfalls verfügbar, und auch die meisten aktuellen Antiviren-Programme sollen BO erkennen und entfernen können.

Doch unvorsichtige Anwender könnten sich über das Internet genau den Beelzebub auf den PC holen, den sie eigentlich austreiben wollen. Unter dem Namen „BOSniffer“ ist ein als Anti-Tool getarntes waschechtes BO-Programm im Umlauf. Der angebliche Schnüffler gaukelt mit einer hübschen Oberfläche Such-Aktivitäten vor, während er Back Orifice ins System einschleust!

UNGESCHÜTZTES WINDOWS

Laut Microsoft „kein Handlungsbedarf“

CdC entwickelte BO nach eigenen Angaben, um zu zeigen, wie wenig sicher Windows im Netz ist. Microsoft zieht sich in einer offiziellen Reaktion auf die Position zurück, jeder Anwender trage selbst die Verantwortung für alle installierten Programme. Das Betriebssystem selbst könne an dieser Stelle nur wenig helfen. Es seien also entweder die Anwender oder die Administratoren in den Unternehmen gefordert, für die entsprechende Kontrolle zu sorgen.

Übrigens gilt BO in der Hardcore-Hackerszene nicht unbedingt als das Mittel der Wahl. Echte Hacker vertrauen auf die schon bislang bewährten Mittel, Bugs, Buffer Overflows oder schlichte Fehlkonfigurationen auszunutzen. Das Hauptproblem an BO ist daher ein quantitatives: Es lädt Tausende von Hobby-Hackern zum Schnüffeln ein, die ohne das Tool dazu technisch nicht in der Lage gewesen wären.

JÜRGEN FEY / TE

BACK ORIFICE: SO ERKENNEN UND ENTFERNEN SIE ES

Bereits kurz nach dem Auftauchen von Back Orifice stellten sich die Anbieter von Antiviren-Software darauf ein. Viele bieten inzwischen Schutz vor BO. Gut ist, wenn das Tool wie Antivir/95 direkt nach BO-Code sucht statt nur nach den Spuren der Urversion von BO. Nur so ist man derzeit sicher (Antivir/95, H+B EDV, Tettnang, Tel. 07542/93040, Fax 52510; ***http://www.antivir.de***, 149 Mark).

Wer mit dem Windows-System vertraut ist, kann BO auch selbst aufspüren. Das Original-BO installiert sich in der Registry unter „Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\RunServices“, wobei der dort angegebene Dateiname meist „ .exe“ lautet (Leerzeichen vor dem Punkt). Die entsprechende Datei findet sich im Windows-Verzeichnis – löschen Sie sie. Wenn Sie diesen Dateinamen nicht finden, sollten Sie nach einer EXE-Datei mit 124.928 Bytes Größe suchen (kleine Abweichungen nach oben oder unten sind möglich). BO-Varianten nutzen den Registry-Schlüssel \Run, den direkten Aufruf in AUTOEXEC.BAT, WIN.INI (Load=, Run=) oder im Autostart-Ordner von Windows. Erfahrene Anwender sollten hier eingetragene Programme überprüfen und verdächtige Kandidaten beseitigen.

Auf den in unserer Übersicht verzeichneten Web-Seiten finden Sie eine Menge Informationen und aktuelle Tools, mit denen Sie BO erkennen und aus dem System entfernen.

Internet-Adresse *(http://www.)*	Hier gibt's . . .
technotronic.com/microsoft.htm	Infos über Windows-Sicherheitsmängel
nwi.net/~pchelp/bo/bo.html	Hintergründe und Links auf BO-Detektoren
nwi.net/~pchelp/bo/morefindBO.htm	Anleitungen zum Finden von BO
nwi.net/~pchelp/bo/removingBO.htm	Anleitungen zum Entfernen von BO
spiritone.com/~cbenson/	ein Tool zum Finden von BO
bardon.com/boelimdl.htm	ein Tool zum Entfernen von BO