NAME	NUISANCE/ DANGER LEVEL	WHAT IT DOES	COMMON SOURCES
Alexa/ ZBubbles	Moderate to severe	Collects and catalogs information on Web browsing and shopping habits. May collect personal information (including credit card numbers and passwords) transmitted via URLs.	Referral from Microsoft site. Direct download from Alexa or Amazon.com. Preinstalled on some computers.
Aureate/ Radiate	Moderate	Monitors browsing and media downloads. Collects demographics. Delivers advertising to users of ad-sponsored software. May continue to operate even if host software is registered and paid for. Causes system instability and crashes.	Many ad-sponsored freeware products (for specifics see http://accs-net.com/smallfish/aur-list.txt). Also Qualcomm's Eudora.
Aveo/ HelpExpress	Moderate	Displays targeted advertising at regular intervals. Continues to run after software with which it was bundled is uninstalled. May try to reinstall itself if not properly removed.	Many commercial products from Canon, Corel, Hewlett-Packard, McAfee, U.S. Robotics, and others.
BackOrifice client	Severe	Trojan horse; can control PCs and monitor their activities.	Usually installed via physical access but can be injected via other malware or security holes.
BDE/ BrilliantDigital	Moderate	Shows 3-D ads. Causes instability and crashes with some graphics cards. May also install the company's AltNet software without warning.	Kazaa.
BonziBuddy	Moderate	Gathers information on browsing habits. Talking purple gorilla recommends sites similar to ones the user is browsing. Slows some systems; can cause a blue screen of death.	May be intentionally downloaded or silently installed with other software. Ads masquerade as alarming error messages.
CommonName/ common.com/ CNBabe	Moderate to severe	Toolbar lets users type site names rather than URLs—but also tracks Web browsing and identifies users via cookies. Pops up ads, changes search settings, causes malfunctions, and blocks access to some sites. Tricky to remove.	Gator, iMesh, Kazaa, NetSonic Internet Accelerator, others.
Cydoor	Moderate	Serves advertising within ad-sponsored software. Attempts to collect demographic information. Profiles users according to ads clicked. Identifies users with unique ID numbers.	Kazaa, Opera.
DownloadWare/ ClipGenie	Moderate	Runs on Windows start-up. Connects to servers and downloads advertising software. It or the software it downloads can crash or take over the system.	ActiveX drive-by downloads, Grokster, Kazaa.
DSSAgent/ Brodcast	Moderate	Discontinued product of Broderbund. Pulls advertising from a central server. May create serious network congestion with legions of DNS queries.	Broderbund Family Archive Viewer; some Mattel software, including Where in the World Is Carmen Sandiego?
eAcceleration	Low to moderate	Periodically downloads advertising for ad-sponsored software.	AudioGalaxy, DIrect Connect, Webcelerator.
EasyInstall	Moderate	Appears to track browsing habits and use this information to download targeted ads.	NetSonic.
eZula/TopText	Moderate to severe	Alters Web pages to add new links from selected phrases to sponsors' sites. Queries a central server; information leakage likely.	Kazaa, drive-by downloads.
Gator/GAIN	Moderate	Ostensibly just fills out forms and remembers passwords. Collects info on browsing habits. Steals sites' advertising revenue by replacing Web page ads—sometimes with those of competitors. The subject of a pending lawsuit.	Usually installed by other products such as Grokster and Morpheus or as a drive-by download. The installer is designed to trickle Gator software onto PCs in the background, unnoticed, while users are online.
HotBar	Moderate	Toolbar monitors browsing and adds sponsored links based on browsing history.	iMesh and other freeware; spam purporting to upgrade Outlook.
Lop	Moderate to severe	Hijacks start page and default search engine; alters bookmarks to add links to advertisers; pops up ads; triggers spontaneous dial-up connections.	Drive-by downloads, pop-up ads.
NetBus	Severe	A remote-control Trojan horse, similar to BackOrifice.	Installed via IM, IRC, malware, security holes, or physical access to machine.
NetObserve	Severe	Key logger; captures screens, monitors browsing.	Suspicious spouse, boss, or parents.
Network Essentials	Moderate	Monitors browsing; displays targeted pop-up ads. URLs visited may be sent to a central server. Employs Web bugs to gather statistics.	DownloadWare (which has its own row above).
New.net	Low to moderate	Lets a browser resolve names from an alternative Domain Name System. Not spyware, but reported to cause problems with some browsers.	BearShare, Go!Zilla, Grokster, Kazaa.
OnFlow	Moderate	Like BDE, a 3-D animation player for advertising. Phones home with a unique ID to indicate that ads have been played.	Kazaa, other applications.
PromulGate/ DelFin	Moderate	Plays targeted multimedia advertising during Internet connect time. Runs continuously in the background; sometimes displays error messages at system start-up.	Kazaa.
SaveNow	Moderate	Monitors browsing, collects demographic info, pops up windows with ads related to sites visited. Runs continuously in the background.	BearShare.
SideStep	Moderate	Travel-related search engine watches searches, sends info to SideStep, and pitches travel options from the SideStep site.	Grokster, iMesh.
Spyagent	Severe	Key logger; captures screens, monitors browsing.	Suspicious spouse, boss, or parents.
Sub7 client	Severe	Trojan horse; can control PCs and monitor activities. May use machines in DDoS attacks.	Installed via security holes or pushed to users via IM or IRC.
TimeSink/ Conducent	Moderate to severe	Gathers data on browsing habits and attempts to transmit it to Conducent (now out of business). Tries to reinstall itself if partially removed. May slow systems by repeatedly trying to connect to defunct servers.	Formerly bundled with ad-sponsored freeware from PKware.
TwistedHumor/ Winad.exe	Moderate to severe	Hijacks browsers to display large Flash ads. May gather personal information for sale to third parties.	Programs (such as "Yo Mama, Osama") downloaded from TwistedHumor.com and affiliated sites.
VX2/ Transponder	Moderate to severe	Gathers personal data, including name, e-mail address, browser history, entries from Web forms filled out, and detailed computer configuration info. Uses tracking cookies. Can install additional software at will.	AudioGalaxy.
webHancer	Moderate	Tracks Web browsing, watching for customer acquisition, conversion, and retention. Feeds statistics to the vendor. Can disrupt networking, especially if removal is attempted.	Many free products, including AudioGalaxy and other file-sharing programs.
Web3000	Moderate	Serves ads in freeware, as Aureate and TimeSink do. Collects demographics. Uses tracking cookies.	NetSonic.
WinWhatWhere	Severe	Key logger; captures screens, monitors browsing.	Suspicious spouse, boss, or parents.
WurldMedia	Severe	Hijacks e-commerce sessions, steals referral commissions, and may capture personal data.	Morpheus.
Xupiter Toolbar	Severe	Tracks and hijacks browsing; deploys pop-ups; diverts browsers to its own site.	Drive-by downloads, spam.