vol. 2006.1
ver. 1.0

# Badware Report

March 21, 2006

stopBADware.org *Regaining Control of Our Computers*

Kazaa
MediaPipe
SpySheriff
Waterfalls 3


Berkman
The Berkman Center for Internet & Socie
at Harvard Law School

oxford internet institute
university of oxford

**SPONSORS**
Google
Lenovo
Sun Microsystems

**SPECIAL ADVISOR**
Consumer Reports WebWatch

# Executive Summary

**Badware** is more than just an annoyance to millions of Americans; the problem of badware represents a fundamental threat to the Internet's continued growth and potential. Today, an estimated 59 million Americans have some form of badware on their computers, according to the Pew Internet & American Life Project, and are paying more than $1 billion a year to fix their computers and protect their identities online. As the badware scourge continues to grow, there exists the danger of a consumer backlash against software in general. Consumers' skepticism toward badware may cause people to hesitate to download or run legitimate software from the Internet on their computers. Such a backlash would reduce the Internet's openness.

The Internet has the extraordinary capacity to allow anyone, anywhere, to develop software, and to instantly distribute it, without cost, throughout the world. **StopBadware.org** was established in an effort to preserve this positive ability to generate and share information by exploring ways to solve the badware problem.

By educating computer users about badware — what it is, how to identify it, and who manufactures and distributes it — **StopBadware.org** aims to curb the future need for Internet gatekeepers or regulators by empowering people to protect themselves.

The **StopBadware.org** website launched on January 25, 2006. As word spread through media outlets and the online community, story submissions and technical reports by computer users quickly poured in to our research team. In the short time that **StopBadware.org** has been active, the website has drawn over 300,000 visits and over 1,000 individual submissions.

Submissions to the **StopBadware.org** website served as the base data for this report. Before we could aggregate and qualitatively analyze peoples' submissions, we first needed to define the parameters and essential traits of badware. With the advice and input of a panel of Internet experts, we isolated seven categories of behaviors that many users reported as unwanted in software they download: deceptive installations, unclear identification, causing harm to other computers, modifying other software, transmitting user data, interfering with computer use, and being difficult to uninstall completely. Badware (represented by a red "X" in this report) is software that engages in these behaviors without adequately disclosing that fact to the user and without seeking the user's consent. In addition, there are some classes of behavior which cause irreversible harm to a user's computer — software which does these things also constitutes badware, regardless of whether the behavior was disclosed to the user.

A second category of software (represented by a yellow triangle) consists of software that engages in one of the seven categories of potentially objectionable behavior, but adequately discloses those behaviors to the user, so that the user can make an informed judgment about whether or not to install the software. The final category of software (represented by a green check mark) is free of the potentially objectionable behaviors we have defined above.

In our first Badware Report, we decided to apply these guidelines to four applications that visitors to **StopBadware.org** had reported as badware. The first, **Kazaa**, is a well-known peer-to-peer file-sharing program. The next application we examined, **SpyAxe**, advertises itself as a

spyware removal program. **MediaPipe**, the third application, identifies itself as a "Download Manager" that will give users access to media content. The final application, **Waterfalls 3**, is a typical screensaver found on Screensaver.com.

To determine whether these applications constituted badware, we downloaded and installed each application into a controlled environment. During the installation process, we analyzed and recorded the disclosures the program made to the user and the files it installed. We then tested the program's effect on our computer's performance, noting anything it did that fell under our badware guidelines. Our findings are summarized in the following chart. As explained above, potentially objectionable behaviors that are sufficiently disclosed to the user are represented by a yellow triangle, while behaviors that are not disclosed to the user, or that cause irreversible damage, are represented by a red "X". Green checkmarks represent categories of bad behavior that are not found in the application.

| Score | Program name | Deceptive installation | Unclear identification | Hurts other computers | Modifies other software | Transmits private info | Interferes w/ computer use | Hard to uninstall completely |
|---|---|---|---|---|---|---|---|---|
| ✗ | Kazaa | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |
| ✗ | MediaPipe | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ |
| ✗ | SpyAxe | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| ✗ | Waterfalls 3 from Screensaver.com | ✗ | ✓ | ✓ | ✗ | ✗ | ▲ | ✓ |

**KEY**

- ✓ Engages in no objectionable behaviors
- ▲ Engages in behaviors that users should be aware of
- ✗ Badware

As our efforts continue, **StopBadware.org** will publish short, user-friendly reports on downloads identified as badware, as well as more detailed academic studies on the problem of badware. At the same time, we will continue to seek stories from Internet users who have been adversely affected by badware.

This consumer-driven online community is meant to serve as a central resource to help educate users on badware and to spotlight those companies who embed these programs into downloadable software applications. We believe this first report helps us move toward that goal.

# Kazaa

We find that Kazaa is badware because it misleadingly advertises itself as spyware-free, does not completely remove all components during the uninstall process, interferes with computer use, and makes undisclosed modifications to other software. **We currently recommend that users do not install the version of Kazaa that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

OVERALL RATING

## Badware Behavior

| |
|---|
| Claims "no spyware," but bundled software is considered spyware (Deceptive installation) |
| Bundled application cannot be closed (Interferes with computer use) |
| Fails to uninstall executables and system components (Unacceptable uninstallation) |

## Behavior to Be Aware of

| | Properly disclosed? |
|---|---|
| Adds links to Windows Desktop (Modifies other software) | ✗ |
| Changes default 404 and DNS error pages in Internet Explorer (Modifies other software) | ✗ |
| Installs adware (Potentially deceptive installation) | YES |
| Installs file-sharing anti-virus software (Potentially deceptive installation) | YES |
| Installs programs that modify Internet Explorer (Potentially deceptive installation, Modifies other software) | ✗ |

## Bad or Undisclosed Behavior

**Claims "no spyware," but bundled software is considered spyware**

Sharman Networks claims that Kazaa has "NO SPYWARE," based on a highly restricted definition of spyware (namely, that no personally identifiable information is sent by the program). However, Kazaa's installation includes several bundled programs that are considered spyware under the common definition of spyware as software that subverts the computer's operation for the benefit of a third party (see Anti-Spyware Coalition and Wikipedia's article on "Spyware").

**Bundled application cannot be closed**

The Best Offers Network, one of the bundled applications included with Kazaa, cannot be closed at all by a typical user. It must be closed by killing the process from within the Windows Task Manager.

**SELF-IDENTIFICATION**

Kazaa's full name is "Kazaa." It advertises itself as a peer-to-peer file-sharing agent.

**PRODUCER**

Kazaa is produced by Sharman Networks, **www.sharmannetworks.com**.

**OBTAINED**

We obtained a free version of Kazaa 3.0 from **http://download.kazaa.com/kazaa_setup.exe** on 3/14/06.

**BUNDLING**

The version of Kazaa we downloaded from the above URL comes bundled with TopSearch (**www.altnet.com**), AltNet Peer Points Manager (**www.altnet.com**), BullGuard P2P (**www.bull-guard.com**), Cydoor (**www.cydoor.com**), The Best Offers (**www.bestoffersnetworks.com**), InstaFinder (**www.vista-interactive.com** and **www.instafinder.com**), and RX Toolbar (**www.vista-interactive.com**).

# Kazaa *(cont'd.)*

**Fails to uninstall executables and system components**

The uninstallation process does not eliminate all components related to Kazaa and its bundled programs. Executables and system components still remain, including the Kazaa Plus Installer.

**Adds links to Windows Desktop**

Kazaa and its bundled applications add two new links to the Windows Desktop: "Your Free Casino Chips!" and "Play Poker Now!" The addition of these links is not disclosed to the user during the installation process.

**Changes default 404 and DNS error pages in Internet Explorer**

InstaFinder, one of the applications bundled with Kazaa, changes the default 404 page and DNS error pages in Internet Explorer. This modification is not disclosed to the user during the installation process.

## Disclosed Behavior

**Installs adware**

Kazaa requires the installation of various adware programs, including TopSearch, AltNet Peer Points Manager, Cydoor, and The Best Offers. The bundling of these applications is disclosed to the user during the installation process, and the user has the option of proceeding with the installation or canceling it.

**Installs file-sharing anti-virus software**

Kazaa requires the installation of file-sharing anti-virus software (BullGuard P2P). The bundling of this application is disclosed to the user during the installation process, and the user has the option of proceeding with the installation or canceling it.

**Installs programs that modify Internet Explorer**

Kazaa requires the installation of programs that modify Internet Explorer, including AltNet's Need2Find Bar, InstaFinder, and RXToolbar. These programs add several new toolbars to Internet Explorer. The bundling of these applications and the addition of these toolbars is disclosed to the user during the installation process, and the user has the option of proceeding with the installation or canceling it.

## Recommendations

**We recommend that Sharman Networks, the producer of Kazaa, do the following:**

- Stop claiming that Kazaa is spyware-free.
- Ensure that Kazaa is not bundled with programs that cannot be closed by the user.
- Remove all executables, system components, and registry keys during the uninstall process.
- Disclose to the user during installation that links that will be added to the Windows Desktop.
- Disclose to the user during installation that the bundled software will change the default 404 and DNS error pages in Internet Explorer.

**We currently recommend that users do not install the version of Kazaa that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

For more information, visit **www.stopbadware.org**.

# MediaPipe

We find that MediaPipe is badware because it does not fully disclose what it is installing, does not completely remove all components and "obligations" during the uninstall process, and modifies other software without disclosure.
**We currently recommend that users do not install the version of MediaPipe that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

OVERALL RATING

## Badware Behavior

| |
|---|
| Reserves right to continue charging user after uninstallation (Unacceptable uninstallation) |
| Fails to uninstall components, links, and executable (Unacceptable uninstallation) |

## Behavior to Be Aware of

| | Properly disclosed? |
|---|---|
| Installs peer-to-peer file-sharing client (Deceptive installation) | |
| Installs payment system (Deceptive installation) | |
| Bundled software runs at Windows startup (Modifies other software) | |

## Bad or Undisclosed Behavior

**Reserves right to continue charging user after uninstallation**

According to Movieland's website and MediaPipe's EULA (End User License Agreement), Movieland reserves the right to continue to charge the user even if he has uninstalled the software. MediaPipe requires the user to visit a website to cancel the "trial obligation."

**Fails to uninstall components, links, and executable**

After uninstallation of the MediaPipe Download Manager, an executable remains which can be used to reinstall the application. The bundled components itbill.exe (a payment system) and mpp2pl.exe (a peer-to-peer file-sharing client) are also are not removed. These components have no stand-alone value apart from the Download Manager. Finally, links to the Movieland website and Movieland terms of service are left on the desktop.

**Installs peer-to-peer file-sharing client**

MediaPipe is bundled with mpp2pl.exe, a peer-to-peer file-sharing client, which is capable of using the user's bandwidth without notification. This executable's configuration files point at p2pnetworks.net, which is currently shut down, so we could not verify whether or not bandwidth is actually used. This bundling is mentioned in the EULA, but is not clearly disclosed to the user during the installation process.

**SELF-IDENTIFICATION**
MediaPipe identifies itself in its license as "MediaPipe"; it identifies itself in the main window and uninstall window of the application only as "Download Manager." The version we obtained reported itself as "Version: 3 Build: _" (sic). It is advertised on Movieland.com as the "Movieland Download Manager," and an apparently similar application is advertised on **moviepass.tv**.

**PRODUCER**
MediaPipe is produced by Net Publican, Ltd., registered in Great Britain.

**OBTAINED**
We obtained MediaPipe from **http://movieland.com/getaccess.html**, which installed **http://download.movieland.com/install/US/movieland_access_g.exe**. The server **download.movieland.com** is apparently also a server for **mediapipe.tv**, so we believe the two services are linked.

**BUNDLING**
MediaPipe is bundled with a payment system, ITBill.exe, and a peer-to-peer file-sharing system, mpp2pl.exe.

# MediaPipe *(cont'd.)*

**Installs payment system**

MediaPipe is bundled with itbill.exe, a payment system, which appears to be responsible for popping up requests for payment. This is disclosed in the EULA, and the behavior is mentioned on the website, but is not clearly disclosed to the user during the installation process.

**Bundled software runs at Windows startup**

MediaPipe automatically adds bundled software (itbill.exe, a payment system, and mpp2pl.exe, a peer-to-peer file-sharing client) to the Windows startup. These additions are not disclosed to the user during the installation process.

## Recommendations

**We recommend that Net Publican, the producer of MediaPipe, do the following:**

- Terminate any "trial obligation" automatically when the Download Manager is uninstalled.
- Remove bundled applications with no stand-alone value (itbill.exe and mpp2pl.exe) when the Download Manager is uninstalled.
- Remove all executables and links when the Download Manager is uninstalled.
- Clearly disclose to the user during installation that MediaPipe is bundled with software that may create popups and use excessive bandwidth.
- Disclose to the user during installation that bundled software will automatically launch at Windows startup.

**We currently recommend that users do not install the version of MediaPipe that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

For more information, visit **www.stopbadware.org**.

# SpyAxe

We find that SpyAxe is badware because it fails to uninstall completely, is difficult to exit without purchasing the full version of the product, and because it interferes with computer use and modifies other software without disclosure.
**We currently recommend that users do not install the version of SpyAxe that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

OVERALL RATING

## Badware Behavior

| |
|---|
| Exiting application requires multiple, non-obvious steps (Interferes with computer use) |
| Fails to uninstall executable (Unacceptable uninstallation) |

## Behavior to Be Aware of

| | Properly disclosed? |
|---|---|
| Launches automatically after reboot and scans computer (Interferes with computer use) | ✗ |

## Bad or Undisclosed Behavior

**Exiting application requires multiple, non-obvious steps**

The main application window for SpyAxe contains no "Exit" or "Quit" button. Moreover, the "Delete Spyware" button that appears after a scan (and which a user might reasonably expect would allow one to delete spyware and exit the application when done) asks the user to register and pay, and does not allow the user to exit the application without doing so. The only way to exit SpyAxe without paying for it to click the "X" button in the right-hand corner of the application window. When the "X" is clicked, the program minimizes to the system tray. The user must then right-click the icon, and choose "Exit." The user is then prompted with a final "Are you sure?" alert box before he can completely quit the application. SpyAxe automatically runs again after the computer is restarted.

**Fails to uninstall executable**

When removing SpyAxe via the bundled uninstaller or the Windows uninstaller, an executable remains which can be used to reinstall the application.

**Launches automatically after reboot and scans computer**

SpyAxe launches automatically after every reboot and then scans the user's computer. Each scan leads to a nag screen which prompts the user to purchase the full version. This automatic launching and scanning is not disclosed to the user during the installation process.

**SELF-IDENTIFICATION**

SpyAxe's full name is "SpyAxe." It claims to be "the latest and one of the most technologically advanced applications on the Internet for detection and removal of potentially undesired items."

**PRODUCER**

SpyAxe claims that it is "a Cyprus based developer of software and Internet-based systems." No address can currently be found on their website.

**OBTAINED**

We obtained SpyAxe from **http://www.spyaxe.com/download.php**. SpyAxe also runs a paid affiliate program that allows third parties to distribute the software.

**BUNDLING**

The version of SpyAxe we downloaded from the above URL is not bundled with other software.

# SpyAxe *(cont'd.)*

## Other

**Trial nature of software**

All actions within the SpyAxe application lead to an alert that directs the user to a purchase screen for the software. The "trial" nature of this software is not disclosed to the user during the installation process.

## Recommendations

**We recommend that the producers of SpyAxe do the following:**

- Provide an "Exit" or "Quit" function from the main application window, so that a user can quit the application normally without being constantly nagged to buy the program.
- Completely remove all executables during uninstallation.
- Disclose to the user that the program will launch automatically after each reboot and scan the user's computer.
- Disclose to the user that the program will be added to the Windows startup folder.
- At download and installation time, clearly label both the trial and full versions of the software as such and define what functions are disabled in the trial version (e.g. that it does not remove badware).

**We currently recommend that users do not install the version of SpyAxe that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

For more information, visit **www.stopbadware.org**.

# Waterfalls 3 from Screensaver.com

We find that Waterfalls 3 from Screensaver.com is badware because it includes components that are generally considered spyware, is bundled with a Trojan horse-like program, and modifies other software without disclosure.
**We currently recommend that users do not install the version of Waterfalls 3 that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**

OVERALL RATING

## Behavior to Be Aware of

| | Properly disclosed? |
|---|---|
| Spyware components found within product (Transmits private info) | ✗ |
| Bundles Trojan horse (Deceptive installation) | ✗ |
| Changes default DNS error page (Modifies other software) | ✗ |
| Adds programs to Windows startup folder (Modifies other software) | ✗ |
| Installs browser modification (Modifies other software) | YES |
| Installs adware programs (Potentially deceptive installation) | YES |
| Overlays ads on Internet Explorer window (Interferes with computer use) | YES |

## Bad or Undisclosed Behavior

### Spyware components found within product

The Waterfalls 3 product includes components by Webhancer, which is commonly considered spyware (see Symantec, DoxDesk, and Spyware Guide). Webhancer monitors websites visited by the user and reports this information to a remote server. This potential transmission of personal information is not disclosed to the user during the installation process.

### Bundles Trojan horse

The New.net EULA (End User License Agreement) reserves to New.net the right to arbitrarily install software on a user's computer as New.net sees fit. Software that uses such EULAs may effectively act as Trojan horses, installing additional programs without disclosing to the user that any installation is occurring. This behavior is not disclosed to the user during the installation process.

### Changes default DNS error page

The default DNS error page for Internet Explorer is changed to a search page that is provided by the New.Net software. This action is not disclosed to the user during the installation process.

**SELF-IDENTIFICATION**
Waterfalls 3 calls itself "Living Waterfalls 3 Screen Saver." It advertises itself as 3D screen saver.

**PRODUCER**
Waterfalls 3 is produced by Freeze.com, **www.freeze.com**. Freeze.com's End User License Agreement, or EULA, (available at **http://www.freeze.com/Policies/License.aspx**) states that Freeze.com content is available at a network of websites: **www.freeze.com, www.screensaver.com, www.wallpapers.com, www.ringtone.com,** and **www.risoftsystems.com**.

**OBTAINED**
We obtained a free version of Waterfalls 3 from Screensaver.com at **http://register.screensaver.com/(cqayce45omswo3vxqa0j2b55)/download/index.aspx**.

**BUNDLING**
The version of Waterfalls 3 we downloaded from the above URL came bundled with Yahoo Toolbar, **www.yahoo.com**, SaveNow, **www.whenu.com**, New.net, **www.new.net**, Yak Community Client, **www.yak.com**, the Crunch Bar, **www.crunchgames.com**, and Desktop Weather, **www.weather.com**.

# Waterfalls 3 from Screensaver.com *(cont'd.)*

**Adds programs to Windows startup folder**

Yak Community Client, the Crunch Bar, and Desktop Weather are automatically added to the Windows startup folder without notifying the user during the installation process. At launch, and after each reboot, Yak Community Client requests user input, the Crunch Bar modifies the Windows desktop, and Desktop Weather displays a large application window containing advertising.

## Disclosed Behavior

**Installs browser modification**

Included in the installation of Waterfalls 3 is the installation of a browser modification (Yahoo Toolbar). The bundling of this application is disclosed to the user during the installation process, and the user has the option of proceeding with the installation or canceling it.

**Installs adware programs**

Waterfalls 3 gives users the option to install several adware programs (SaveNow, New.net, Yak Community Client, the Crunch Bar, and Desktop Weather). Although the Waterfalls 3 installer defaults to installing these applications, the user can choose not to install any individual component of this bundled software.

**Overlays ads on Internet Explorer window**

WhenU displays pop-up windows or overlay ads based on search terms on top of the Internet Explorer window. These overlays sometimes obscure the user's view of the Internet Explorer window; however, these advertisements are disclosed to the user during the installation process and the user has the option of proceeding with the installation or canceling it.

## Other

**Other screensavers**

We observed badware behavior similar to that described above when we downloaded and installed other screensavers from Screensavers.com.

## Recommendations

**We recommend that Freeze.com, the producer of Waterfalls 3, do the following:**

- Remove or properly disclose the inclusion of the WebHancer components, and disclose that personal information will be sent via these components.
- Stop bundling potential Trojan horses such as New.net, or disclose that this application will enable the installation of additional applications without the user's knowledge or consent.
- Disclose to the user that the default DNS error page will be changed by the bundled applications.
- Disclose the addition of bundled applications to the Windows startup folder.

**We currently recommend that users do not install the version of Waterfalls 3 that we tested, unless the user is comfortable with the level of risk we identify or until the application is updated consistent with the recommendations in this report.**