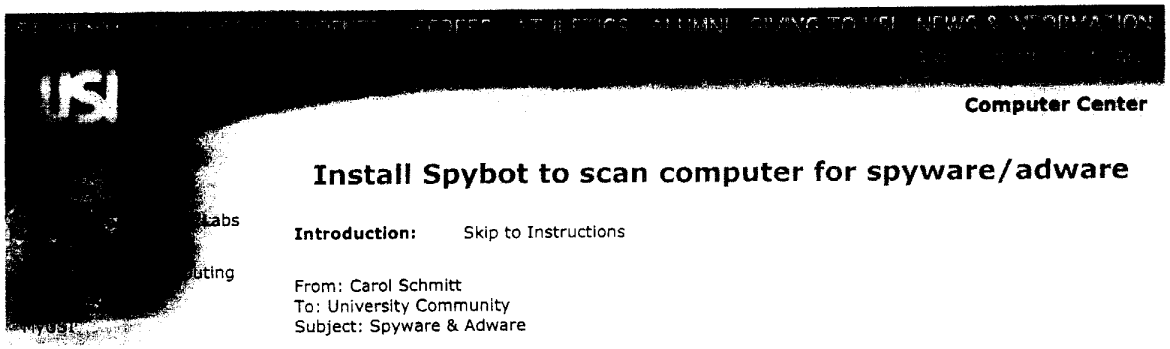
EXHIBIT O



Computer Center

Install Spybot to scan computer for spyware/adware

Labs

uting

Library Computing

Microcomputer Services

Network Services

Telecommunications

Web Services

Staff

Feedback

Sitemap

Computer Center Home

Introduction: Skip to Instructions

From: Carol Schmitt
To: University Community
Subject: Spyware & Adware

I have received several email messages recently that have the "Upgrade Outlook – Add icons to your email 'click here'" link at the bottom – along with the smiley face graphics.

This add-in is NOT a Microsoft product.

This is a marketing gimmick to trick you into thinking you are actually downloading a legitimate Outlook upgrade or enhancement. In reality, it is actually placing SPYWARE code on your computer from a marketing group called HOTBAR. Once installed, it has the ability to silently download and execute arbitrary code from the Hotbar site without your knowledge, along with tracking every website you visit.

It is strongly recommended that you do not install this onto your system. If it is already installed, it should be uninstalled. If you have already installed this, you may have noticed that you have more pop-ups, more junk e-mail, and a slow down in system performance. This is because in the background, this spyware is communicating your surfing habits to the Hotbar team so they can 'better' market advertisements to you.

If you would like to install software to scan your computer for adware/spyware, see the instructions at THIS PAGE.

If you want assistance in uninstalling spyware/adware– contact the Computer Center Help Desk at x1080.

Other products that are spyware (or unnecessary software) are Gator, Comet Cursor, BonziBuddy, Huntbar...

Adware, also known as an Adbot, can do a number of things, from profile your online surfing and spending habits, to popping up annoying ad windows as you surf. In some cases, Adware has been bundled with other software (i.e. peer-to-peer file swapping products) without the user's knowledge, or slipped in the fine print of a EULA (End User License Agreement). Not all adware is bad, but often users are annoyed by adware's intrusive behavior. Keep in mind that by removing Adware sometimes the program it came bundled with may stop functioning. Some Adware, dubbed a "BackDoor Santa", may not perform any activity other then profile a user's surfing activity for study.

AdWare can be obnoxious in that it performs "drive-by downloads". Drive-by downloads are

accomplished by providing a misleading dialogue box or other methods of stealth installation. Many times users have no idea they have installed the application. Often Adware makers make their application difficult to uninstall.

A "EULA" or End User License Agreement is the agreement you accept when you click "OK" or "Continue" when you are installing software. Most users never bother to read the EULA.

It is imperative to actually read this agreement before you install any software. No matter how tedious the EULA, you should be able to find out the intent BEFORE you install the software. If you have questions about the EULA, e-mail the company and ask them for clarification.

Spyware is potentially a more dangerous beast than Adware because it can record your keystrokes, history, passwords, and other confidential and private information. Spyware is often sold as a spouse monitor, child monitor, a surveillance tool or simply as a tool to spy on users to gain unauthorized access. Spyware is also known as: snoopware, PC surveillance, key logger, system recorders, Parental control software, PC recorder, Detective software and Internet monitoring software.

Spyware covertly gathers user information and activity without the user's knowledge. Spy software can record your keystrokes as you type them, passwords, credit card numbers, sensitive information, where you surf, chat logs, and can even take random screenshots of your activity. Basically whatever you do on the computer is completely viewable by the spy. You do not have to be connected to the Internet to be spied upon.

Instructions:

Click My Computer
Double click the O drive - if you don't have an O drive mapped go here
Double click Spybot folder
Double click Spybotsd12
Click NEXT
Read the License Agreement
Accept the Agreement, NEXT
It should default to: c:\program files\ - Click NEXT
At "Select Components" window click NEXT
Accept default Spybot Search & Destroy, NEXT
Accept the default again, NEXT
Click INSTALL
Click FINISH
Close Window

Start Internet Explorer
Click Tools (at top)
Select Internet Options
~~Under Temporary Internet Files, Delete Cookies, OK~~
Under Temporary Internet Files, Delete Files, OK - wait for hourglass to go away- this may take a while
Click OK
Close Internet Explorer

Find and double click Spybot icon on Desktop

Choose ENGLISH - ignore flag
Click Search for Updates
Click DOWNLOAD UPDATES, OK
Click Search and Destroy (in top left)
Choose "Check for Problems"
This scan will take 3-10 minutes...
When finished, Click "Fix selected Problems", OK

You can decide if you want Spybot to run on next system startup. I always like to reboot, and scan again - just to see the number of items found drop!

Download from web site -

Only do this if you don't have an 'O' drive mapped - see above where it says "Instructions"

To download the spybot software from the website go HERE. Find English download button. Download and install - then go to instructions above.

Revision Date:4/18/2005 10:40:36 AM

EXHIBIT P

[Skip To Content]

Information Resources

Information Security Tips

Protecting Data While Using Wireless Networks

As wireless networks increase, it is possible to check e-mail, surf the Internet, or conduct research from your laptop virtually anywhere. The university offers Wildcat Wireless service in and around the library, the BMU, Café by the Creek, Kendall Hall, Colusa Hall, Continuing Education Building, as well as some residence halls, with more locations coming soon.

With the convenience of using wireless, it is vital to protect your data as it moves through the networks. Hackers can "sniff" (or intercept) confidential information transmitted over wireless connections. It is extremely important to make sure your computer has current virus software and your operating system and software applications have the latest security patches.

In order to use the campus network you must pay a low monthly (or yearly) fee for a subscription. To connect to Wildcat Wireless, you need to download the VPN (Virtual Private Network) client. This software verifies that you are an authorized user, and insures that only authenticated users are on the network.

See CNS Wildcat Wireless http://www.csuchico.edu/cns/wireless.htm or call at 898-6868.
For information on downloading VPN, http://sandbox.net.csuchico.edu/index.shtml
A map showing wireless availability, http://www.csuchico.edu/cns/wireless%20map.pdf
Current Microsoft operating system updates, http://www.windowsupdate.com

Policy for Acceptable Use of Campus Computing and Communications Technology

Assuring that our campus computing and communications resources are used appropriately and legally is important to all of us. Access to these university facilities and resources is a privilege granted for educational use and legitimate university-related business.

Acceptable use of computing and communications resources at CSU, Chico includes

- Respect for the legal protections provided by copyright and license to programs and data as well as by university contractual agreements.
- Respect for the rights of others by complying with all university policies regarding intellectual property.
- Using accurate identification in all electronic communications to avoid deliberately misrepresenting any user's identity.

All users should be aware of and have read the official university "Policy on Use of Computing and Communications Technology", EM 97-18, http://www.csuchico.edu/prs/EMs/EM97/em97_18.htm, as well as the California State University System 4CNet Acceptable Use Policy, http://www.4c.net/documents/4cnet_policy.html. 4CNet provides the network for all CSU campuses to connect to each other and to the Internet. If you have any questions contact Information Resources, x6212.

Information Security Tip--Beware of Hotbar

Hotbar, a shareware program for PCs that provides smiley faces and other icons, can shut down your computer or make it vulnerable to outside intrusion. Hotbar is being pushed through unsolicited (spam) e-mail purporting to be an upgrade to Microsoft Outlook. Once installed on your system, Hotbar records the address of every Web site you visit. It then sends that information back to its controlling server along with a unique ID that allows your Internet use to be tracked and sold to advertisers. Hotbar also records network information so it can punch a hole though network security systems which can make the entire network open to virus or other attack.

E-mail you send to anyone else can also be affected. The recipients can be tracked, and hidden code within the mail may also retrieve information from our servers (such as text and/or banner promotions) which will, in such case, also appear in the e-mail sent.

For information on removing Hotbar see http://www.csuchico.edu/usrv/security/spybot.htm.
For other security information see http://www.csuchico.edu/inf/security.

Information Security Tip—Avoid Spam

To help prevent spam (unsolicited, commercial e-mail):

- Never respond to spam or click “remove me” from large, unknown sites. This confirms your e-mail address and you're likely to get

more.
- Use a second e-mail address to sign up for non-university newsgroups, chat rooms, and mailing lists, or for purchases. Free e-mail service is available through Hotmail and Yahoo.
- Check the privacy policy when you submit your address to a Web site.
- Use an e-mail filter. Attend User Services' workshops on the use of Microsoft Outlook and ways to filter some spam messages.
- Let the Federal Trade Commission know if a "remove me" request is not honored or if a removal link doesn't work; www.ftc.gov.

Avoid these common scam offers:

- Chain letters that involve money or valuable items and promise big returns
- Work at home opportunities
- Products that promote effortless, long term weight loss
- Offers to erase accurate, negative information from your credit record
- Promises to provide a loan for a fee
- Adult entertainment sites offering "free" content which may reconnect to international long distance phone numbers, at rates up to $7/minute

To file a complaint or for information on consumer issues visit www.ftc.gov, the Federal Trade Commission.

Protect Your Credit Card Information Online

When shopping online, protect your credit card information from being stolen and abused.

- Consider using only one credit card online, perhaps one with a low limit.
- Use a credit card that has a good liability policy if the number has been stolen. Most major credit cards limit your liability to $50.
- Never use a debit card online.
- Where possible, have your vendor NOT store your credit card number for use next time. This may keep your card number off of their Web server.
- Make certain the site is encrypting your credit card number. Your Web browser will have a small picture of a lock that is closed at the top or bottom of the page when using encryption. Also, check the URL of the page to see if it starts with "https://", which means the page is encrypted.
- Finally, some credit card companies offer one-time use credit card numbers that are tied to your main account and any subsequent attempts to use it will be denied. American Express and the Discover Card both offer this service.

For more information see the Information Resources Web site: http://www.csuchico.edu/inf/security(Some information courtesy of Duke University).

Avoid Identity Theft

Identity theft is one of the fastest growing crimes in the nation, accounting for 43 percent of all complaints received by the Federal Trade Commission in 2002—that's 161,800 complaints, up 88 percent. The average victim spends 175 hours and $800 resolving identity theft problems, and it can take two to four years.

To lower your risk:

- Don't carry your Social Security card or SSN on other cards.
- Tear up or shred papers with personal information, including credit card offers and "convenience checks" you don't use.
- Don't give out personal information on the phone - unless you made the call or know the caller. The same goes for mail and the Internet.
- To limit the sharing of financial information, write to your bank, credit card, insurance, and securities companies to "opt-out."
- Check credit card bills for unauthorized charges and report any to your card issuer. Call if bills don't arrive on time.
- Stop pre-approved credit card offers by calling toll-free 888-5OPTOUT.
- Get your credit reports at least once a year. Check for changed addresses or fraudulent information. Costs about $8.

For more information http://www.privacyprotection.ca.gov/identitytheft.htm or http://www.csuchico.edu/inf/security, Information from California Office of Privacy Protection.

Legal Music Downloading

One recent national survey shows the number of illegal music downloaders fell from 35 million last spring to 18 million last fall. But other measurements say illegal file sharing is still going strong. Downloading free music can violate copyright laws and make your computer vulnerable to hackers and viruses. A legal and safe option is now available through numerous online locations which sell individual music tracks typically for 99 cents or less. Some sell albums for $9.95 or have a monthly fee. The digital tunes can legally be played on the computer, transferred to portable music players, and burned onto CDs.

Apple iTunes, the forerunner in this market for both Macs and Windows platforms, sold more than 30 million songs since April. Wal-Mart, RealNetworks, Sony, Rhapsody, MusicMatch, EMusic Napster, Walmart, MP3University, and BuyMusic. have launched music downloading services. These can be found on the Internet by doing a search or typing in www, followed by the service name, then .com.

E-mail is not secure

Sending information through e-mail is not secure, and hackers could intercept your information. The university e-mail system and most other e-mail programs are not encrypted and can be vulnerable to outsiders who use sniffers to hack into our network and allow your messages and

attachments to be read. Be aware personal or confidential information such as social security numbers, bank account numbers, grades, etc. could be compromised.

In addition, to protect your computer from e-mail viruses, delete messages and attachments from unknown sources. By not opening these attachments and keeping your anti-virus software up-to-date, you minimize the chances of a virus infecting your computer. Current virus software can help handle these threats. PC users still using McAfee 4.5.1 should upgrade to version 7. Mac users should use Virex. For information see: http://www.csuchico.edu/usrv/security/.

For information contact User Services: x6000 or see the Information Security Web site: http://www.csuchico.edu/inf/security.

Protect Copyrighted Works

Copyright is a protection provided by U.S. laws (title 17, U.S. Code) to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and other works. Campus information is available at http://www.csuchico.edu/lcmt/copyright/. This protection extends to both published and unpublished works and generally gives the owner exclusive right to do and to authorize others to do the following:

- To reproduce the work in copies or phonorecords;
- To prepare derivative work;
- To distribute copies or phonorecords to the public by sale or transfer of ownership, by rental, lease, or lending;
- To perform the work publicly, for literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works;
- To display the copyrighted work publicly, for literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work; and
- In the case of sound recordings, to perform the work publicly through digital audio transmission.

It is illegal for anyone to violate any of the rights. These rights, however, are not unlimited in scope. One major exception is "fair use," section 107 of the 1976 Copyright Act which provides for use of parts of copyrighted works under defined and specific circumstances. From U.S. Copyright Office, http://www.copyright.gov/.

Kazaa Spreading Viruses

A study from TruSecure showed that nearly half of all software traded over the Kazaa file-sharing network was infected with malicious code. The findings apply not to music and video files but to executable files, including programs designed to circumvent digital copyright protections. Some of the malware infected files on a user's computer; other code would steal user passwords or allow hackers to control an infected machine. Most infected files have .exe extensions, but could be disguised with a .wav or .jpg extension. Current antivirus software would be able to identify 85 to 90 percent of the problematic code found in Kazaa files.

Current virus software can help handle these threats. PC users still using McAfee 4.5.1 should upgrade to version 7. Mac users should use Virex. For information see: http://www.csuchico.edu/usrv/security/.
For information contact User Services: x6000 or see the Information Security Web site: http://www.csuchico.edu/inf/security/.

Web Information for Students to Avoid Identify Theft

The U.S. Department of Education has launched a Web site (http://www.ed.gov/misused/) designed to educate students about the dangers of identity theft. College students are reminded to shred unused credit card applications, or any documents with account numbers, social security numbers, addresses, etc. to prevent identity theft. Students should carefully check credit card and bank statements for fraudulent charges or activity. The new Web site offers tips on how to prevent having personal information compromised and provides information on contacting various agencies to report identity theft. Other information security information is available at http://www.csuchico.edu/inf/security/.

Back to Information Security main page

For more information see

- Protecting your credit card online - Calif. Office of Consumer Affairs
- Protecting your Social Security number - Privacy Rights Clearinghouse
- Identity theft - Calif Office of Attorney General
- Protecting Your Personal Information - Federal Trade Commission

Back to Security 7

EXHIBIT Q

symantec.

security response

Adware.Hotbar

Last Updated on: May 31, 2005 09:31:26 AM

print document

Type:	**Adware**
Name:	Not available
Version:	Not available
Publisher:	Hotbar.com
Systems Affected:	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Serve 2003, Windows XP
Risk Impact:	Low

• Intelligent Updater Definitions*	August 18, 2003
• LiveUpdate™ Definitions **	August 18, 2003

* Intelligent Updater definitions are released daily, but require manual download and installation. Click here to download manually.

** LiveUpdate definitions are usually released every Wednesday. Click here for instructions on using LiveUpdate.

This risk can be detected only by Symantec products that support security risks. For more information on security risks, please go here.

summary

Behavior

Adware.Hotbar adds graphical skins to Internet Explorer, Microsoft Outlook, and Outlook Express toolbars and also adds its own toolbar and search button. These custom toolbars have keyword-targeted advertisements built into them.

Adware.Hotbar can send information on browsing habits to various servers, which may be used for targeted marketing.

Symptoms
The files are detected as Adware.Hotbar.

Transmission
Adware.Hotbar needs to be manually installed on the computer via ActiveX or an installer.

technical details

File names:
HbInstIE.dll
hotbar.exe
HBCORESRV.DLL
HBINST.EXE
HbToolbar.dll
HBHOSTOE.DLL
HBHOSTOL.DLL
HBHOSTIE.DLL
HBSRV.EXE
HbGuard.exe
ShprRprt.exe
ShprRpt.dll.

When Adware.Hotbar is installed, it does the following:

1. Creates files in the following folders:

   - %Program Files%\Hotbar
   - %ProgramFiles%\ShopperReports
   - %UserProfile%\Application Data\Hotbar.
   - %UserProfile%\Application Data\ShopperReports.

   Notes:
   - %UserProfile% is a variable that refers to the current user's profile folder. By default, this is C:\Documents and Settings\[Current User] (Windows NT/2000/XP).
   - %ProgramFiles% is a variable that refers to the program files folder. By default, this is C:\Program Files.

2. Creates the following files during the install:

   - %Windir%\Downloaded Program Files\HbInstIE.dll
   - %Windir%\Downloaded Program Files\hotbar.inf

   Note: %Windir% is a variable that refers to the Windows installation folder. By default, this is C:\Windows or

C:\Winnt.

3. Creates copys of Hbinst.exe and HbGuard.exe and installs [random name].exe in %System%.

   Note: %System% is a variable that refers to the System folder. By default this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

4. Creates following links on the desktop:

   - %UserProfile%\Desktop\Games.lnk
   - %UserProfile%\Desktop\WOWPapers.lnk

5. Creates the following registry subkeys:

```
HKEY_CLASSES_ROOT\CLSID\{69FD62B1-0216-4C31-8D55-840ED86B7C8F}
HKEY_CLASSES_ROOT\CLSID\{013A482E-1893-4F49-8D41-AC89156A6955}
HKEY_CLASSES_ROOT\CLSID\{0774F696-D801-4C18-81A7-A3A32B8BEF19}
HKEY_CLASSES_ROOT\CLSID\{1038DD23-8AE8-451B-A134-4DB8A49AA519}
HKEY_CLASSES_ROOT\CLSID\{1E0004EC-5DF0-48C7-A8F0-FBB0488A3D94}
HKEY_CLASSES_ROOT\CLSID\{1E6AC766-9094-4BCF-ABD3-39E2EAEA5FCD}
HKEY_CLASSES_ROOT\CLSID\{2178C864-B8BC-41AE-A1FB-EB6A32F87EB1}
HKEY_CLASSES_ROOT\CLSID\{2A8A997F-BB9F-48F6-AA2B-2762D50F9289}
HKEY_CLASSES_ROOT\CLSID\{31D0C6FF-5897-4A57-8005-A50FCE4CE159}
HKEY_CLASSES_ROOT\CLSID\{354382DB-DF55-4DA9-85A3-41696A0F510F}
HKEY_CLASSES_ROOT\CLSID\{3CEB882D-6B2B-4D81-A544-9D9B1D6FA945}
HKEY_CLASSES_ROOT\CLSID\{454B4812-E572-4703-A1BB-63490809EAC0}
HKEY_CLASSES_ROOT\CLSID\{4DBCFAF7-62E1-4811-8ACC-6511E7192CB4}
HKEY_CLASSES_ROOT\CLSID\{580A1F3F-89B4-433B-BBDB-B97AEB13F3FC}
HKEY_CLASSES_ROOT\CLSID\{60F630A2-41EC-11D5-B558-00D0B77F0A6D}
HKEY_CLASSES_ROOT\CLSID\{6FB2639A-4BA3-4531-8DB8-FAB03E0A8FFD}
HKEY_CLASSES_ROOT\CLSID\{6FE00B71-7251-4E00-9186-ED89BBB946B8}
HKEY_CLASSES_ROOT\CLSID\{75D2080B-4857-4B96-9B7D-732634FBD01F}
HKEY_CLASSES_ROOT\CLSID\{A798E2B4-B6A0-4B96-8C53-8EC7A3B0895A}
HKEY_CLASSES_ROOT\CLSID\{A80347E0-F757-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\CLSID\{B195B3B3-8A05-11D3-97A4-0004ACA6948E}
HKEY_CLASSES_ROOT\CLSID\{BECAFC17-BAF9-11D4-B492-00D0B77F0A6D}
HKEY_CLASSES_ROOT\CLSID\{FF6B2FD5-093C-4D4F-BB98-5641130A9DE6}
HKEY_CLASSES_ROOT\Interface\{17719B53-FAD1-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\Interface\{17719B54-FAD1-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\Interface\{3103E312-E1BB-49AB-80EB-0A92FCA78746}
HKEY_CLASSES_ROOT\Interface\{31321312-E1BB-49AB-80EB-13212CA78746}
HKEY_CLASSES_ROOT\Interface\{340D8791-0E2C-43CF-9671-7E90AAFBF0DA}
HKEY_CLASSES_ROOT\Interface\{34F4D917-31E4-464C-B8B3-84C1CE76B395}
```

HKEY_CLASSES_ROOT\Interface\{3F04CBF7-CD62-4403-B090-B432DEDCB159}
HKEY_CLASSES_ROOT\Interface\{3F6DA8BB-3E45-44E2-B494-C55BEAF3B41E}
HKEY_CLASSES_ROOT\Interface\{46417AFD-7A15-4ED1-B764-CB72CD4D904F}
HKEY_CLASSES_ROOT\Interface\{4BF4FAFA-186E-4E36-8F74-525290438D7B}
HKEY_CLASSES_ROOT\Interface\{6A6EBAE8-8C66-4675-B423-95B3BA530940}
HKEY_CLASSES_ROOT\Interface\{6F885F52-B45F-45BC-8642-FE3D56155A3A}
HKEY_CLASSES_ROOT\Interface\{7138714C-9819-4AB1-9A86-E7C413C9A99E}
HKEY_CLASSES_ROOT\Interface\{7E33BC81-0818-11D5-B50D-00D0B77F0A6D}
HKEY_CLASSES_ROOT\Interface\{8578D35E-C6C0-4808-9A80-0F6C29A2C423}
HKEY_CLASSES_ROOT\Interface\{8F59F897-6923-4B3B-8156-4E55D19DE99A}
HKEY_CLASSES_ROOT\Interface\{918E4B7A-4D80-43A4-83A7-39ADCC11841F}
HKEY_CLASSES_ROOT\Interface\{927420A3-7259-4A74-B402-9329177EC3FC}
HKEY_CLASSES_ROOT\Interface\{9DD19D39-2CDC-465B-BB21-1D433590BA3D}
HKEY_CLASSES_ROOT\Interface\{9EE87A26-B2C8-4130-83F6-E8511D939976}
HKEY_CLASSES_ROOT\Interface\{A1772E14-9291-454E-AEDE-02161FBC3E59}
HKEY_CLASSES_ROOT\Interface\{A80347DF-F757-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\Interface\{AD9A7B03-BE12-11D4-B493-00D0B77F0A6D}
HKEY_CLASSES_ROOT\Interface\{B00609A6-82AF-4C55-BBB8-ADC8593CEB86}
HKEY_CLASSES_ROOT\Interface\{B195B3B2-8A05-11D3-97A4-0004ACA6948E}
HKEY_CLASSES_ROOT\Interface\{BC190DA5-0187-4D99-B3AC-6C45EA1B9324}
HKEY_CLASSES_ROOT\Interface\{BC2025DC-136B-492F-AEFF-31D0BA8B98DA}
HKEY_CLASSES_ROOT\Interface\{C8539BFE-8FD7-405C-8EEF-D9AF48DC6BA4}
HKEY_CLASSES_ROOT\Interface\{DA603411-0593-11D5-A46B-00508B5BA2DF}
HKEY_CLASSES_ROOT\Interface\{DA603411-0593-11D5-A46B-10101B1B1111}
HKEY_CLASSES_ROOT\Interface\{DA603411-0593-11D5-A46B-10101DDD1111}
HKEY_CLASSES_ROOT\Interface\{F4132B7B-1576-41B6-ABD8-39C6C53047F7}
HKEY_CLASSES_ROOT\Interface\{F64B26C1-07DE-11D5-B50D-00D0B77F0A6D}
HKEY_CLASSES_ROOT\Interface\{F7A1BF21-1D7D-4F5F-A201-0CA35A5CD68F}
HKEY_CLASSES_ROOT\TypeLib\{522985F4-BA43-45A0-9B20-AB5F82C0FF7E}
HKEY_CLASSES_ROOT\TypeLib\{94BEB7A2-36B7-46DC-8AD1-81A8332409C0}
HKEY_CLASSES_ROOT\TypeLib\{60F63095-41EC-11D5-B558-00D0B77F0A6D}
HKEY_CLASSES_ROOT\TypeLib\{6D6D1580-5B74-40EA-97F4-3C2B46C5ABDD}
HKEY_CLASSES_ROOT\TypeLib\{842D315A-7E1E-448B-96E8-9E76D1820BE2}
HKEY_CLASSES_ROOT\TypeLib\{A80347D3-F757-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\TypeLib\{AB357854-7A72-4FBE-9382-CC74B45A3ADD}
HKEY_CLASSES_ROOT\TypeLib\{B195B3A5-8A05-11D3-97A4-0004ACA6948E}
HKEY_CLASSES_ROOT\TypeLib\{B5901229-25CC-43C9-B604-3BB6AC2B48A5}
HKEY_CLASSES_ROOT\TypeLib\{B701A704-F828-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\TypeLib\{C83DAED4-0611-4F7A-978E-7FEAFCB2F91B}
HKEY_CLASSES_ROOT\HBInstIE.HbInstObj.1
HKEY_CLASSES_ROOT\HBInstIE.HbInstObj
HKEY_CLASSES_ROOT\HbCoreSrv.DynamicProp

HKEY_CLASSES_ROOT\HbCoreSrv.DynamicProp.1
HKEY_CLASSES_ROOT\HbCoreSrv.HbCoreServices
HKEY_CLASSES_ROOT\HbCoreSrv.HbCoreServices.1
HKEY_CLASSES_ROOT\HbCoreSrv.LfgAx
HKEY_CLASSES_ROOT\HbCoreSrv.LfgAx.1
HKEY_CLASSES_ROOT\HbHostIE.Bho
HKEY_CLASSES_ROOT\HbHostIE.Bho.1
HKEY_CLASSES_ROOT\HbHostOL.HbElementFocus
HKEY_CLASSES_ROOT\HbHostOL.HbElementFocus.1
HKEY_CLASSES_ROOT\HbHostOL.HbMailAnim
HKEY_CLASSES_ROOT\HbHostOL.HbMailAnim.1
HKEY_CLASSES_ROOT\HbHostOL.HbWebmailSend
HKEY_CLASSES_ROOT\HbHostOL.HbWebmailSend.1
HKEY_CLASSES_ROOT\HbSrv.HbCoreServices
HKEY_CLASSES_ROOT\HbSrv.HbCoreServices.1
HKEY_CLASSES_ROOT\HbToolbar.HbHtmlMenuUI
HKEY_CLASSES_ROOT\HbToolbar.HbHtmlMenuUI.1
HKEY_CLASSES_ROOT\HbToolbar.HbToolbarCtl
HKEY_CLASSES_ROOT\HbToolbar.HbToolbarCtl.1
HKEY_CLASSES_ROOT\Hotbar.HbCommBand
HKEY_CLASSES_ROOT\Hotbar.HbCommBand.1
HKEY_CLASSES_ROOT\Hotbar.HbMain
HKEY_CLASSES_ROOT\Hotbar.HbMain.1
HKEY_CLASSES_ROOT\Hotbar.HbTravelCompareBar
HKEY_CLASSES_ROOT\Hotbar.HbTravelCompareBar.1
HKEY_CLASSES_ROOT\RprtsPSClient.PSExecuter
HKEY_CLASSES_ROOT\RprtsPSClient.PSExecuter.1
HKEY_CLASSES_ROOT\ShprRprts.HbAx
HKEY_CLASSES_ROOT\ShprRprts.HbAx.1
HKEY_CLASSES_ROOT\ShprRprts.HbCommBand
HKEY_CLASSES_ROOT\ShprRprts.HbCommBand.1
HKEY_CLASSES_ROOT\ShprRprts.HbInfoBand
HKEY_CLASSES_ROOT\ShprRprts.HbInfoBand.1
HKEY_CLASSES_ROOT\ShprRprts.IEButton
HKEY_CLASSES_ROOT\ShprRprts.IEButton.1
HKEY_CLASSES_ROOT\ShprRprts.IEButtonA
HKEY_CLASSES_ROOT\ShprRprts.IEButtonA.1
HKEY_CLASSES_ROOT\ShprRprts.SmrtShprCtl
HKEY_CLASSES_ROOT\ShprRprts.SmrtShprCtl.1
HKEY_CLASSES_ROOT\Wallpaper.WallpaperManager
HKEY_CLASSES_ROOT\Wallpaper.WallpaperManager.1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\HbSrv.EXE

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\WeatherOnTray.EXE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions\{946B3E9E-E21A-49c8-
9F63-900533FAFE14}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions\{E77EDA01-3C56-4a96-
8D08-02B42891C169}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{2A8A997F-BB9F-48F6-AA2B-2762D50F9289}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{B195B3B3-8A05-11D3-97A4-0004ACA6948E}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\HotbarOutlookTool
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\HotbarWebTools
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Shopper Reports b
Hotbar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\HbHostOL.HbMailAnim
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{2178C864-B8BC-41AE
A1FB-EB6A32F87EB1}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{B195B3B3-8A05-11D3
97A4-0004ACA6948E}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{A798E2B4-B6A0-4B96
8C53-8EC7A3B0895A}
KEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{BECAFC17-BAF9-11D4-
B492-00D0B77F0A6D}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{FF6B2FD5-093C-4D4F
BB98-5641130A9DE6}
HKEY_CLASSES_ROOT\AppID\{0507FDDE-F3B7-49F5-9E8F-C557E991F39B}
HKEY_CLASSES_ROOT\AppID\{B701A705-F828-11D4-A466-00508B5BA2DF}
HKEY_CURRENT_USER\Software\Hotbar
HKEY_LOCAL_MACHINE\Software\Hotbar
HKEY_USERS\.DEFAULT\Software\Hotbar
```

6. Adds the value:

   ```
   {B195B3B3-8A05-11D3-97A4-0004ACA6948E}
   ```

   to the regsistry subkeys:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar
   HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser
   HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser
   ```

7. Adds the values:

```
"WeatherOnTray" = "C:\Program Files\Hotbar\Bin\4.6.1.0\WeatherOnTray.exe
"Hotbar" = "C:\Program Files\Hotbar\Bin\4.6.1.0\HbOEAddOn.exe"
"[random value]" = "C:\WINDOWS\System32\[random name].exe"
```

to the registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

to ensure these programs run on startup.

removal instructions

Removal using the Adware.Hotbar Removal Tool
Symantec Security Response has developed a removal tool for Adware.Hotbar. Use this removal tool first, as it is the easiest way to remove this threat.

The tool can be found here:

http://securityresponse.symantec.com/avcenter/FxHotbar.exe

The current version of the tool is version 1.0.5.0. It will have a digital signature timestamp of Tuesday November 26, 2004 9:31 AM (PST).

Note: The date and time displayed will be adjusted to your time zone, if your computer is not set to the Pacific time zone.

The removal tool may terminate any instances of Microsoft Internet Explorer or Microsoft Windows Explorer currently running on the computer.

Some harmless Temporary Internet files created by the threat may remain on the system after using the removal tool. It is recommended that the Temporary Internet files be deleted by completing the following steps:

1. Open **Internet Explorer**
2. Select **Tools > Internet Options**
3. In the Temporary Internet Files section, click the **Delete Files** button
4. Check **Delete all offline content**, and then click **OK**

Some harmless registry entries created by the threat may remain on the system after using the removal tool. As a result of this some security products may still claim to detect Adware.Hotbar on the system.

Manual Removal

1. Update the virus definitions.
2. **Uninstall Hotbar and/or Web Tools from Hotbar using the Add/Remove Programs utility.**
3. *Run a full system scan and delete all the files detected as Adware.Hotbar.*
4. Delete the keys that were added to the registry.

The following instructions pertain to all Symantec antivirus products that support security risk detection.

1. To update the definitions
To obtain the most recent definitions, start your Symantec program and run LiveUpdate.

2. To uninstall the Security Risk

a. Do one of the following:
   a. On the Windows 98 taskbar:
      a. Click **Start > Settings > Control Panel**.
      b. In the Control Panel window, double-click **Add/Remove Programs**.

   b. On the Windows Me taskbar:
      a. Click **Start > Settings > Control Panel**.
      b. In the Control Panel window, double-click **Add/Remove Programs**.
      If you do not see the Add/Remove Programs icon, click "...**view all Control Panel options**."

   c. On the Windows 2000 taskbar:
      By default, Windows 2000 is set up the same as Windows 98, so follow the instructions for Windows 98. If otherwise, click **Start**, point to **Settings > Control Panel**, and then click **Add/Remove Programs**.

   d. On the Windows XP taskbar:
      a. Click **Start > Control Panel**.
      b. In the Control Panel window, double-click **Add or Remove Programs**.

b. Click Hotbar and/or "Web Tools from Hotbar."

Note: You may need to use the scroll bar to view the whole list.

c. Click **Add/Remove**, **Change/Remove**, or **Remove** (this varies with the operating system). Follow the prompts.

Note: After running the Add/Remove programs applet, all the files may have been removed. You will want to run a full system scan to ensure that this is the case. However, it is possible that no files will be detected after using Add/Remove programs.

3. To run the scan

a. Start your Symantec antivirus program, and then run a full system scan.
b. If any files are detected, and depending on which software version you are using, you may see one or more of the following options:

Note: This applies only to versions of Norton AntiVirus that support security risk detection. If you are running a version o Symantec AntiVirus Corporate Edition that supports security risk detection, and security risk detection has been enabled you will only see a message box that gives the results of the scan. If you have questions in this situation, contact your network administrator.

- Exclude (Not recommended): If you click this button, it will set the risk so that it is no longer detectable. That is, the antivirus program will keep the security risk on your computer and will no longer detect it to remove from your computer.

- Ignore or Skip: This option tells the scanner to ignore the risk for this scan only. It will be detected again the next time that you run a scan.

- Cancel: This option is new to Norton Antivirus 2005. It is used when Norton Antivirus 2005 has determined that it cannot delete a security risk. This Cancel option tells the scanner to ignore the risk for this scan only, and thus, the risk will be detected again the next time that you run a scan.

  To actually delete the security risk:
  - Click its file name (under the Filename column).
  - In the Item Information box that displays, write down the full path and file name.
  - Then use Windows Explorer to locate and delete the file.

    If Windows reports that it cannot delete the file, this indicates that the file is in use. In this situation, complete the rest of the instructions on this page, restart the computer in Safe mode, and then delete the file using Windows Explorer. Restart the computer in Normal mode.

- Delete: This option will attempt to delete the detected files. In some cases, the scanner will not be able to do this.
  - If you see a message, "Delete Failed" (or similar message), manually delete the file.
  - Click the file name of the risk that is under the Filename column.
  - In the Item Information box that displays, write down the full path and file name.
  - Then use Windows Explorer to locate and delete the file.

    If Windows reports that it cannot delete the file, this indicates that the file is in use. In this situation,

complete the rest of the instructions on this page, restart the computer in Safe mode, and then delete the file using Windows Explorer. Restart the computer in Normal mode.

Important: If your Symantec antivirus product reports that it cannot delete a detected file, Windows may be using the file. To fi this, run the scan in Safe mode. For instructions, read the document: How to start the computer in Safe Mode. Once you have restarted in Safe mode, run the scan again.

After the files are deleted, restart the computer in Normal mode and proceed with the next section.

Warning messages may be displayed when the computer is restarted, since the risk may not be fully removed at this point. You can ignore these messages and click OK. These messages will not appear when the computer is restarted after the removal instructions have been fully completed. The messages displayed may be similar to the following:

Title: `[File path]`
Message body: `Windows cannot find [file name]. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.`

4. To delete the value from the registry

Important: Symantec strongly recommends that you back up the registry before making any changes to it. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify the specified subkeys only. Read the document: How to make a backup of the Windows registry.

a. Click **Start > Run**.
b. Type **`regedit`**

   Then click **OK**.

   Note: If the registry editor fails to open the risk may have modified the registry to prevent access to the registry editor. Security Response has developed a tool to resolve this problem. Download and run this tool, and then continue with the removal.

c. Navigate to and delete the subkeys:

```
HKEY_CLASSES_ROOT\CLSID\{69FD62B1-0216-4C31-8D55-840ED86B7C8F}
HKEY_CLASSES_ROOT\CLSID\{013A482E-1893-4F49-8D41-AC89156A6955}
HKEY_CLASSES_ROOT\CLSID\{0774F696-D801-4C18-81A7-A3A32B8BEF19}
HKEY_CLASSES_ROOT\CLSID\{1038DD23-8AE8-451B-A134-4DB8A49AA519}
HKEY_CLASSES_ROOT\CLSID\{1E0004EC-5DF0-48C7-A8F0-FBB0488A3D94}
HKEY_CLASSES_ROOT\CLSID\{1E6AC766-9094-4BCF-ABD3-39E2EAEA5FCD}
HKEY_CLASSES_ROOT\CLSID\{2178C864-B8BC-41AE-A1FB-EB6A32F87EB1}
```

HKEY_CLASSES_ROOT\CLSID\{2A8A997F-BB9F-48F6-AA2B-2762D50F9289}
HKEY_CLASSES_ROOT\CLSID\{31D0C6FF-5897-4A57-8005-A50FCE4CE159}
HKEY_CLASSES_ROOT\CLSID\{354382DB-DF55-4DA9-85A3-41696A0F510F}
HKEY_CLASSES_ROOT\CLSID\{3CEB882D-6B2B-4D81-A544-9D9B1D6FA945}
HKEY_CLASSES_ROOT\CLSID\{454B4812-E572-4703-A1BB-63490809EAC0}
HKEY_CLASSES_ROOT\CLSID\{4DBCFAF7-62E1-4811-8ACC-6511E7192CB4}
HKEY_CLASSES_ROOT\CLSID\{580A1F3F-89B4-433B-BBDB-B97AEB13F3FC}
HKEY_CLASSES_ROOT\CLSID\{60F630A2-41EC-11D5-B558-00D0B77F0A6D}
HKEY_CLASSES_ROOT\CLSID\{6FB2639A-4BA3-4531-8DB8-FAB03E0A8FFD}
HKEY_CLASSES_ROOT\CLSID\{6FE00B71-7251-4E00-9186-ED89BBB946B8}
HKEY_CLASSES_ROOT\CLSID\{75D2080B-4857-4B96-9B7D-732634FBD01F}
HKEY_CLASSES_ROOT\CLSID\{A798E2B4-B6A0-4B96-8C53-8EC7A3B0895A}
HKEY_CLASSES_ROOT\CLSID\{A80347E0-F757-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\CLSID\{B195B3B3-8A05-11D3-97A4-0004ACA6948E}
HKEY_CLASSES_ROOT\CLSID\{BECAFC17-BAF9-11D4-B492-00D0B77F0A6D}
HKEY_CLASSES_ROOT\CLSID\{FF6B2FD5-093C-4D4F-BB98-5641130A9DE6}
HKEY_CLASSES_ROOT\Interface\{17719B53-FAD1-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\Interface\{3103E312-E1BB-49AB-80EB-0A92FCA78746}
HKEY_CLASSES_ROOT\Interface\{31321312-E1BB-49AB-80EB-13212CA78746}
HKEY_CLASSES_ROOT\Interface\{340D8791-0E2C-43CF-9671-7E90AAFBF0DA}
HKEY_CLASSES_ROOT\Interface\{34F4D917-31E4-464C-B8B3-84C1CE76B395}
HKEY_CLASSES_ROOT\Interface\{3F04CBF7-CD62-4403-B090-B432DEDCB159}
HKEY_CLASSES_ROOT\Interface\{3F6DA8BB-3E45-44E2-B494-C55BEAF3B41E}
HKEY_CLASSES_ROOT\Interface\{46417AFD-7A15-4ED1-B764-CB72CD4D904F}
HKEY_CLASSES_ROOT\Interface\{4BF4FAFA-186E-4E36-8F74-525290438D7B}
HKEY_CLASSES_ROOT\Interface\{6A6EBAE8-8C66-4675-B423-95B3BA530940}
HKEY_CLASSES_ROOT\Interface\{6F885F52-B45F-45BC-8642-FE3D56155A3A}
HKEY_CLASSES_ROOT\Interface\{7138714C-9819-4AB1-9A86-E7C413C9A99E}
HKEY_CLASSES_ROOT\Interface\{7E33BC81-0818-11D5-B50D-00D0B77F0A6D}
HKEY_CLASSES_ROOT\Interface\{8578D35E-C6C0-4808-9A80-0F6C29A2C423}
HKEY_CLASSES_ROOT\Interface\{8F59F897-6923-4B3B-8156-4E55D19DE99A}
HKEY_CLASSES_ROOT\Interface\{918E4B7A-4D80-43A4-83A7-39ADCC11841F}
HKEY_CLASSES_ROOT\Interface\{927420A3-7259-4A74-B402-9329177EC3FC}
HKEY_CLASSES_ROOT\Interface\{9DD19D39-2CDC-465B-BB21-1D433590BA3D}
HKEY_CLASSES_ROOT\Interface\{9EE87A26-B2C8-4130-83F6-E8511D939976}
HKEY_CLASSES_ROOT\Interface\{A1772E14-9291-454E-AEDE-02161FBC3E59}
HKEY_CLASSES_ROOT\Interface\{A80347DF-F757-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\Interface\{AD9A7B03-BE12-11D4-B493-00D0B77F0A6D}
HKEY_CLASSES_ROOT\Interface\{B00609A6-82AF-4C55-BBB8-ADC8593CEB86}
HKEY_CLASSES_ROOT\Interface\{B195B3B2-8A05-11D3-97A4-0004ACA6948E}
HKEY_CLASSES_ROOT\Interface\{BC190DA5-0187-4D99-B3AC-6C45EA1B9324}
HKEY_CLASSES_ROOT\Interface\{BC2025DC-136B-492F-AEFF-31D0BA8B98DA}

HKEY_CLASSES_ROOT\Interface\{C8539BFE-8FD7-405C-8EEF-D9AF48DC6BA4}
HKEY_CLASSES_ROOT\Interface\{DA603411-0593-11D5-A46B-00508B5BA2DF}
HKEY_CLASSES_ROOT\Interface\{DA603411-0593-11D5-A46B-10101B1B1111}
HKEY_CLASSES_ROOT\Interface\{DA603411-0593-11D5-A46B-10101DDD1111}
HKEY_CLASSES_ROOT\Interface\{F4132B7B-1576-41B6-ABD8-39C6C53047F7}
HKEY_CLASSES_ROOT\Interface\{F64B26C1-07DE-11D5-B50D-00D0B77F0A6D}
HKEY_CLASSES_ROOT\Interface\{F7A1BF21-1D7D-4F5F-A201-0CA35A5CD68F}
HKEY_CLASSES_ROOT\TypeLib\{522985F4-BA43-45A0-9B20-AB5F82C0FF7E}
HKEY_CLASSES_ROOT\TypeLib\{94BEB7A2-36B7-46DC-8AD1-81A8332409C0}
HKEY_CLASSES_ROOT\TypeLib\{60F63095-41EC-11D5-B558-00D0B77F0A6D}
HKEY_CLASSES_ROOT\TypeLib\{6D6D1580-5B74-40EA-97F4-3C2B46C5ABDD}
HKEY_CLASSES_ROOT\TypeLib\{842D315A-7E1E-448B-96E8-9E76D1820BE2}
HKEY_CLASSES_ROOT\TypeLib\{A80347D3-F757-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\TypeLib\{AB357854-7A72-4FBE-9382-CC74B45A3ADD}
HKEY_CLASSES_ROOT\TypeLib\{B195B3A5-8A05-11D3-97A4-0004ACA6948E}
HKEY_CLASSES_ROOT\TypeLib\{B5901229-25CC-43C9-B604-3BB6AC2B48A5}
HKEY_CLASSES_ROOT\TypeLib\{B701A704-F828-11D4-A466-00508B5BA2DF}
HKEY_CLASSES_ROOT\TypeLib\{C83DAED4-0611-4F7A-978E-7FEAFCB2F91B}
HKEY_CLASSES_ROOT\HBInstIE.HbInstObj.1
HKEY_CLASSES_ROOT\HBInstIE.HbInstObj
HKEY_CLASSES_ROOT\HbCoreSrv.DynamicProp
HKEY_CLASSES_ROOT\HbCoreSrv.DynamicProp.1
HKEY_CLASSES_ROOT\HbCoreSrv.HbCoreServices
HKEY_CLASSES_ROOT\HbCoreSrv.HbCoreServices.1
HKEY_CLASSES_ROOT\HbCoreSrv.LfgAx
HKEY_CLASSES_ROOT\HbCoreSrv.LfgAx.1
HKEY_CLASSES_ROOT\HbHostIE.Bho
HKEY_CLASSES_ROOT\HbHostIE.Bho.1
HKEY_CLASSES_ROOT\HbHostOL.HbElementFocus
HKEY_CLASSES_ROOT\HbHostOL.HbElementFocus.1
HKEY_CLASSES_ROOT\HbHostOL.HbMailAnim
HKEY_CLASSES_ROOT\HbHostOL.HbMailAnim.1
HKEY_CLASSES_ROOT\HbHostOL.HbWebmailSend
HKEY_CLASSES_ROOT\HbHostOL.HbWebmailSend.1
HKEY_CLASSES_ROOT\HbSrv.HbCoreServices
HKEY_CLASSES_ROOT\HbSrv.HbCoreServices.1
HKEY_CLASSES_ROOT\HbToolbar.HbHtmlMenuUI
HKEY_CLASSES_ROOT\HbToolbar.HbHtmlMenuUI.1
HKEY_CLASSES_ROOT\HbToolbar.HbToolbarCtl
HKEY_CLASSES_ROOT\HbToolbar.HbToolbarCtl.1
HKEY_CLASSES_ROOT\Hotbar.HbCommBand
HKEY_CLASSES_ROOT\Hotbar.HbCommBand.1

HKEY_CLASSES_ROOT\Hotbar.HbMain
HKEY_CLASSES_ROOT\Hotbar.HbMain.1
HKEY_CLASSES_ROOT\Hotbar.HbTravelCompareBar
HKEY_CLASSES_ROOT\Hotbar.HbTravelCompareBar.1
HKEY_CLASSES_ROOT\RprtsPSClient.PSExecuter
HKEY_CLASSES_ROOT\RprtsPSClient.PSExecuter.1
HKEY_CLASSES_ROOT\ShprRprts.HbAx
HKEY_CLASSES_ROOT\ShprRprts.HbAx.1
HKEY_CLASSES_ROOT\ShprRprts.HbCommBand
HKEY_CLASSES_ROOT\ShprRprts.HbCommBand.1
HKEY_CLASSES_ROOT\ShprRprts.HbInfoBand
HKEY_CLASSES_ROOT\ShprRprts.HbInfoBand.1
HKEY_CLASSES_ROOT\ShprRprts.IEButton
HKEY_CLASSES_ROOT\ShprRprts.IEButton.1
HKEY_CLASSES_ROOT\ShprRprts.IEButtonA
HKEY_CLASSES_ROOT\ShprRprts.IEButtonA.1
HKEY_CLASSES_ROOT\ShprRprts.SmrtShprCtl
HKEY_CLASSES_ROOT\ShprRprts.SmrtShprCtl.1
HKEY_CLASSES_ROOT\Wallpaper.WallpaperManager
HKEY_CLASSES_ROOT\Wallpaper.WallpaperManager.1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\HbSrv.EXE
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\WeatherOnTray.EXE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions\{946B3E9E-E21A-49c8-9F63-900533FAFE14}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions\{E77EDA01-3C56-4a96-8D08-02B42891C169}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{2A8A997F-BB9F-48F6-AA2B-2762D50F9289}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{B195B3B3-8A05-11D3-97A4-0004ACA6948E}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\HotbarOutlookTool
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\HotbarWebTools
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Shopper Reports by Hotbar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\HbHostOL.HbMailAnim
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{2178C864-B8BC-41AE-A1FB-EB6A32F87EB1}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{B195B3B3-8A05-11D3-97A4-0004ACA6948E}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{A798E2B4-B6A0-4B96-8C53-8EC7A3B0895A}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{BECAFC17-BAF9-11D4-

B492-00D0B77F0A6D}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Explorer Bars\{FF6B2FD5-093C-4D4F
BB98-5641130A9DE6}
HKEY_CLASSES_ROOT\AppID\{0507FDDE-F3B7-49F5-9E8F-C557E991F39B}
HKEY_CLASSES_ROOT\AppID\{B701A705-F828-11D4-A466-00508B5BA2DF}
HKEY_CURRENT_USER\Software\Hotbar
HKEY_LOCAL_MACHINE\Software\Hotbar
HKEY_USERS\.DEFAULT\Software\Hotbar

d. Navigate to and delete the value:

{B195B3B3-8A05-11D3-97A4-0004ACA6948E}

from the registry subkeys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser

e. Navigate to and delete the values:

"WeatherOnTray" = "C:\Program Files\Hotbar\Bin\4.6.1.0\WeatherOnTray.exe
"Hotbar" = "C:\Program Files\Hotbar\Bin\4.6.1.0\HbOEAddOn.exe"
"[random value]" = "C:\WINDOWS\System32\<randomname>.exe"

Note: <randomvalue>/<randomname> may appear like this kvmsvzfm: "C:\WINDOWS\System32\hkbveqrv.exe"

from the registry subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

f. Exit the Registry Editor.