Spyware/Adware
The Quest for Consumer Desktops & How it Went Wrong

Saumil Shah
Dave Cole
Agenda

- The Adware & Spyware Business
- Disputes, Lawyers & Legislation
- The Technology
- Looking Ahead
How’d we get in this mess?

Affiliate marketing is born, courtesy of the adult entertainment industry. Later abandoned due to widespread fraud and abuse.

DoubleClick comes under heat for using tracking cookies to monitor behavior—investigated by the FTC & back off linking this to an offline user database used to install adware.

Injunction ruled vs. Gator, preventing them from pop’ing ads over 16 websites.

1st freeware AntiSpyware programs appear (OptOut, Spybot, Ad-Aware) after FTC Spyware workshop.

Adware companies 180 Solutions & Direct Revenue (using many names) join the fray.

First adware programs appear on the scene, Aureate/Radiate & Conducent TimeSink.

CoolWebSearch, one of the most aggressive adware/spyware players appears on the scene.

First adware programs appear on the scene, Aureate/Radiate & Conducent TimeSink.
Who’s behind it all?

Mainstream Players

Working in the Shadows

Playing by their own rules

Black Hat Japan 2005
Adware Company Profile

- Major players founded in last 4-6 years
- 100-200 employees
- $50-$200 million USD in revenues
- Goals
  - Get as many eyeballs as possible (wide installed base)
  - Get a deep understanding of consumer behavior
  - Drive purchases for clients / show as many ads as possible
- Funded by mainstream venture capital firms
  - Greylock, US Venture Partners, Spectrum Equity Investors
- Boast the world’s top brands as their clients
  - Examples: Expedia, Buy.com, Travelocity, Sprint, Cendant…
# Latest Symantec Top 10

<table>
<thead>
<tr>
<th>Rank</th>
<th>Program name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ShopAtHomeAgent</td>
</tr>
<tr>
<td>2</td>
<td>Iстbar</td>
</tr>
<tr>
<td>3</td>
<td>CoolWebSearch</td>
</tr>
<tr>
<td>4</td>
<td>SearchAssistant</td>
</tr>
<tr>
<td>5</td>
<td>Iefeats</td>
</tr>
<tr>
<td>6</td>
<td>Gain</td>
</tr>
<tr>
<td>7</td>
<td>BetterInternet</td>
</tr>
<tr>
<td>8</td>
<td>VirtuMonde</td>
</tr>
<tr>
<td>9</td>
<td>EliteBar</td>
</tr>
<tr>
<td>10</td>
<td>NdotNet</td>
</tr>
</tbody>
</table>

*Source: Symantec Internet Security Threat Report, 9/05*
Adware Business Model – In Theory

Advertisers
- Ad design
- Per-click commissions

Adware Company
- Ad software
- Per-install commissions

Distributors
- Free software bundle

Source: Center for Democracy & Technology
Adware Business Model – In Practice

Source: Center for Democracy & Technology
Adware Business Model – Example

*Companies in bold are the current defendants in FTC v. Seismic, et al.*

Source: Center for Democracy & Technology
From: jared@optintrade.com
To: jared@optintrade.com
Date: Fri, Nov-28-2003 12:37 PM
Subject: strategy

I do my sneaky shit with adv.com today through Sunday -- everyone’s off anyway…. You then send an email to your contact early Monday AM saying the advertiser was unethical and pulled a switch and you are no longer doing business with them... Then we stop buying adv.com through you in any way.

From: jared@optintrade.com
To: jared@optintrade.com
Date: Sat, Mar-6-2004 4:51 PM
Subject: I DID IT

I figured out a way to install an exe without any user interaction. This is the time to make the $$$ while we can.
Spyware Company Profile

- Small companies (<50 employees) & individuals
- Less revenue & resources
  - No official backing or affiliations in most cases
  - Direct sales from their websites & distributors
- Surveillance software / keyloggers
  - Sold as parental/jealous spouse monitoring tool
- Free tool + aggressive behavior monitoring
  - Behavior tracking often hidden or poorly disclosed
- Walking a fine line with malware (e.g., LoverSpy)
# Latest Symantec Top 10

<table>
<thead>
<tr>
<th>Rank</th>
<th>Program name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Webhancer</td>
</tr>
<tr>
<td>2</td>
<td>Apropos</td>
</tr>
<tr>
<td>3</td>
<td>Marketscore</td>
</tr>
<tr>
<td>4</td>
<td>CometCursor</td>
</tr>
<tr>
<td>5</td>
<td>e2give</td>
</tr>
<tr>
<td>6</td>
<td>Perfect</td>
</tr>
<tr>
<td>7</td>
<td>ISearch</td>
</tr>
<tr>
<td>8</td>
<td>Goidr</td>
</tr>
<tr>
<td>9</td>
<td>ISpynow</td>
</tr>
<tr>
<td>10</td>
<td>KeyTick</td>
</tr>
</tbody>
</table>

Source: Symantec Internet Security Threat Report, 9/05
Quick Look: Commercial Keyloggers
What Symantec Sees…

…When performing weekly AntiSpyware testing

- Based on sampling of URLs & bundled software (e.g. P2P)
- Mostly adware from vendors “working in the shadows”
- Spyware: mostly keyloggers & some aggressive trackers
- Trojans are not uncommon
Adware & AntiSpyware Disputes

What adware/spyware cos. complain about

• “You’re killing my business!”
  – The emotional appeal
• “Adware is bad, we’re not adware”
  – We’re really *ad-supported* software
• “You’re breaking our EULA with our customers”
  – Our EULA provisions prohibit partial or complete removal by AntiSpyware
• “Everyone thinks we’re a virus because of you.”
  – There’s nothing you can do other than stop detecting us
• “You’re detecting our ad-free, paid version too”
  – There’s dolphins in your tuna net
• “What about my Acme corp., my competitor?”
  – You’re just picking on me
• “What about Google & Yahoo?”
  – You’re really just picking on the little guys
When Adware Goes Legal

Recent years have featured a large number of lawsuits among the major adware players (2 examples below)

Sued By…

- Washington Post
- USA Today
- The Wall Street Journal

Suing…

- CLARIA
- PC Pitstop
- Gator
- Interactive Advertising Bureau

- Copyright Infringement
- Unfair Biz, Trade Label, etc.
- Trade Libel
- Computer Fraud and Abuse
- Willful Interference
Call in the Feds

Lawmakers across the globe are beginning to step in & regulate as consumer complaints increase

Brazil
No specific legislation on spyware but a major bill covering cybercrime and internet applications is being debated in the upper chamber of congress after passing the lower.

United States
- 2 states have laws already in place (28 total in progress)
- 5 federal bills are at various stages of completion

Netherlands
Bill discussed to combat the use of dialers and spyware.

Korea
This August, the Ministry of Information and Communication defines spyware and sets penalties for those who create or spread spyware up to 5 years in prison or fines of up to W50 million (about US$50,000).

Australia
Bill introduced in May of 2005 to fine companies $10,000 AUD for spreading spyware.
Spyware Taxonomy

- Spyware/snoopware/keyloggers
- Adware
- Backdoors
- Dialers
- Hijacklers
Case Study - HotBar
HotBar

- Fancy toolbars for IE and Outlook.
- Skins, smileys, weather, games and other gimmicks.
- Hijacks Browser searches, URLs and displays advertisements.
- Ads are pop-unders, browser frames, DHTML overlays, tool buttons, etc.
HotBar

- Genuinely claims to be ad-supported software.
- Slight level of “social engineering” when it comes to installation.
hotbar.com site

Add emoticons and Images to your Emails.

Join the Hotbar community of millions of users and enjoy:
- Colorful Emails
- Beautiful desktop wallpapers
- Enhanced Browser functionality with fast search tool

Click Here
Instructions on how to “install”

In a few seconds, a window will appear. Click "Run" on the window to start using Hotbar.

File Download - Security Warning

Do you want to run or save this file?

- Name: hbttools.exe
- Type: Application, 1.53 KB
- From: Installs.hotbar.com

Run  Save  Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?
Publisher: “a Microsoft Certified Partner”

Internet Explorer - Security Warning

Do you want to run this software?

- Name: Hotbar, a Microsoft Certified Partner, and do...
- Publisher: HOTBAR.COM Inc.

- More options
- Run
- Don't Run

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

About Hotbar • Media Center • Advertise with Us • Report Copyright Infringement • Contact • Privacy Policy • Terms of Use • Help
Disclosure of Intention

Welcome to Hotbar Installation 😊😊

You will soon be able to enjoy:
- Colorful Emails - add cute emoticons and other goodies to your emails.
- Enhanced Browser - fast search tool and related links.
- Weather Tool - stay updated with your local weather.
- WOWpapers - decorate your desktop with thousands of wallpapers.

Please be assured that this software is not a spyware application and is 100% committed to your privacy. Each of these features may be uninstalled separately at any time. These free services are ad-supported unless you choose our paid version.

☑ Enable Hotbar keyword search in Internet Explorer address bar and change my search assistant in Internet Explorer to ResultsMaster.

Please choose from the following:
- Free ad-supported version
- Paid version

☑ Install ShopperReports - the FREE price comparison tool that brings you the best deals on the net. I have read and agreed to the ShopperReports Terms of Use.

Next >>

Copyright © 1999-2005 Hotbar.com, Inc. All Rights Reserved - Patent No. US 6,784,900
Hotbar installed
Hotbar Browser Helper Objects

Add-ons are programs that extend the capabilities of your Web browser. Some add-ons can interfere with the operation of your browser. You can disable, enable, or update add-ons. Disabling an add-on might prevent some Web pages from working.

Select an add-on from the list above to perform the following actions:

- Settings: To disable an add-on, click it and then click Disable. To update an ActiveX control, click it and then click Update ActiveX.

- Click here to update this add-on.
Dynamic tool buttons from Google search

Ford Motor Company
A leading consumer company for automotive products and services passionately committed to providing personal mobility for people around the world.

Ford Motor Company Home Page
The corporate website for Ford Motor Company and its vehicle (car and truck) and service brands, featuring investor, career, news and media information.

Ford Vehicles. Ford Vehicles Official Site. learn about Ford cars...

The Ford Tour
Website: 1 2 3 4 5 6 7
Pop-under advertisements

Search Results: mobile

Top 15 sponsored results

Dream Time Baby
Lamps, Rocking Chairs, Bath to Go, Scented Drawer Liner, and much more.
www.dreamtimebaby.com

Dream Time Baby {E}
Lamps, Rocking Chairs, Bath to Go, Scented Drawer Liner, and much more.
c.enhance.com

Info.com - Find Info on Mobile
Info.com gives you the best of the web, providing you with the best results from the biggest search engines. Click here now to find results for Mobile
web.info.com

Black Hat Japan 2005
Searching within hotbar

Top 25 sponsored results for **mobile**:

- **Dream Time Baby**
  - Lamps, Rocking Chairs, Bath to Go, Scented Drawer Liner, and much more.
  - [www.dreamtimebaby.com](http://www.dreamtimebaby.com)

- **Dream Time Baby**
  - Lamps, Rocking Chairs, Bath to Go, Scented Drawer Liner, and much more.

- **The Ford Tour**
  - Click Here

---

**2: StateAuctions.org - Cheap Cars and SUVs** - Auto auction bargains are found here and only here, at the official state auctions website - search by zip to locate bargains in your area.

[www.godisaist.pranch3.1hp.clickbank.net](http://www.godisaist.pranch3.1hp.clickbank.net) (Sponsored link)
Hijacking the “404 not found” page

Search cannot be found - saumil.net.
Please try typing a search query in the search box below:

Search

Perhaps you may find the links below helpful:

- Block Pop-up ads
- Stop Email Spam
- Keep your PC private

Please try one of the followings:

- Check your keywords spelling
- Try different keywords
- Try more general keywords

About Hotbar - Advertising with Us - Contact - Terms of Use
Copyright © 1999-2006 Hotbar.com Inc. All Rights Reserved. Hotbar® is a patent pending.
Case Study - A Better Internet
A Better Internet

- "Turbo" Adware - doesn’t stop at anything.
- Gathers a lot of private data and information.
- Multiple installation vectors.
- Employs stealth techniques.
- Hooks into multiple places.
A Better Internet

- Does not disclose its intentions.
- Heavy use of “social engineering”.
- Extremely hard to remove - keeps resurrecting.
- Random process names and registry entries.
- Malicious in nature.
A Better Internet - the website

NO SPYWARE
We favor industry regulation & fully support the Federal Spy Act.

Best Offers' free software offerings are enjoyed by millions of Internet users all over the world. The Best Offers collection of original products that can be downloaded and enjoyed for free includes Luke the Screen Washer, the coolest screensaver on the Web. Each product is easy-to-use and install. Our detailed instructions and live tech support help you every step of the way. Your privacy is guaranteed.

Our free downloads include:

Eliminate Spam!
Tired of spam-filled mailboxes? Download Eliminate Spam! - a free anti-spam software - and get a clean mailbox today!
Tell me more!

Luke the Screen Washer
The coolest screensaver on the Web! Luke will clean your screen and keep you company!
Tell me more!

Smiley Source
Smiley Source is an application that allows you to add fun "smiley" icons to your email.

ID Theft Radar
According to FTC, over 10 million Americans fall victim to ID Theft annually. Version...
Download free software - Screensaver

Do you want to run or save this file?

- Name: DO_LUK1000.exe
- Type: Application, 179 KB
- From: st.bestoffersnetworks.com

Run | Save | Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Luke the Screensaver will clean your computer screen - and keep you company. Luke is one of the coolest screensavers on the web today and will provide you with a clean computer screen at all times.

Why is Luke the Screen Washer Free?

Luke the Screen Washer is provided to you free of charge because it is supported by advertising from

Black Hat Japan 2005
“Free software” installing itself
Pop-under when using search engines
Contextual pop-up ads displayed
“Dial-home” Signals

T 192.168.7.191:1121 -> 64.95.228.143:80 [A]
GET /a/Drk.syn?adcontext=http://www.google.co.in/&contxtpeak=0&contxtcount=0&countrycodein=IN&lastAdTime=0&lastAdCode=0&cookie1=1flshdt%3D1128213526%261stlogdt%3D20051001%260%3D%26cntp%3D%26&cookie2=fstcidt%3D1128213526391%260%3D%26&cookie3=0&cookie4=0&InstID={9FB27148-34BE-4B13-8066-A72A1646DEB4}&DistID=0|0|0|0|BANNER02.EXE&status=1&smode=9&event=0&bho=aurora.exe&NumWindows=3&PartnerId=0&BundleId=0&HN=xpletive&VSN=84ABFDC6&PI=55274-640-7712297-23104&MA=005056070191&WindowTitle=&TM=00 HTTP/1.1..User-Agent: {9FB27148-34BE-4B13-8066-A72A1646DEB4}|0.21.5.112..Host: btg.btgrab.com..Cookie: did=pub; uid={106AEC3AFDE-E74E-E2C6-C7D6-5C67B614BF09}; dmg=%13%7E_x%082%08k%22%7Bzswv%24%7Cv%22%7Bzs%wv%24evo%22.%2F%2F%2F%2F%2F%24%7C%7B%7B%7B%7B+_; hst=1-1128213491-0:0:0:nac; url=ROUTEINE_CHECKIN; ctr=1; acl=1; dly=0; fme=0; dmg=%13%7E_x%082%08k%22%7Bzswv%24%7Cv%22%7Bzswv%24evo%22.%2F%2F%
“Dial-home” Signals

T 192.168.7.91:1121 -> 64.95.228.143:80 [A]
GET /a/Drk.syn?adcontext=http://www.google.co.in/&contextpeak=0&contextcount=0&countrycodein=IN&lastAdTime=0&lastAdCode=0&cookie1=lflshdt%3D1128213526%261stlogdt%3D20051001%2620%3D26cntp%3D26&cookie2=fstcidt%3D1128213526391%2620%3D%26cookie3=0&cookie4=0&InstID={9FB27148-34BE-4B13-8066-A72A1646DEB4}&DistID=1000|68|0|0|BANNER02.EXE&status=1&smode=9&event=0&bho=aurora.exe&NumWindows=3&PartnerId=0&BundleId=0&HN=xpletive&VSN=84ABFDC6&PI=55274-640-7712297-23104&MA=005056070191&WindowTitle=&TM=00 HTTP/1.1
User-Agent: {9FB27148-34BE-4B13-8066-A72A1646DEB4} 0.2
Host: btg.btgrab.com
Cookie: did=pub; uid={106AEC3AFDE-EB4E-E2C6-76-5067614BF09}; dmg=%13%7E%082%08k%22%7Bzswv%24%7C%22%Bzs wv%24evo%22%.2F%2F%2F%2F%24%7C%7B%22%-%27%5D%3FN%3BK+_; hst=1-1123491-0:0:0:0:ac; url=ROUTEINE_CHECKIN; tr=1; ac=1; dly=0; fme=0; c=%13%7E%082%08k%22%7Bzswv%24%7C%22%7Bsvv%24evo%22...%2F%2F%22

T 192.168.7.191:1123 -> 64.124.153.143:80 [AP]
GET /imp/servlet/ImpServe?urlContext=http%3A%2F%2Fwww.google.co.in%2F&domainContext=co.in&distID=1000%7C68%7C0%7C0%7CBANNER02.EXE&country=IN&transponderID={9FB27148-34BE-4B13-8066-A72A1646DEB4}&build=0.21.5.112&s=136310&c=70912&ca=14486&s0=136310 HTTP/1.1..Accept: */*
Accept-Language: en-us..Accept-Encoding: gzip, deflate..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)..Host: xadsj.offeroptimize.r.com..Connection: Keep-Alive..Cookie: did=pub; uid={106AEC3AFDE-E74E-E2C6-C7D6-5C67B614BF09}; dmg=%13%7E_x%082%08k%22%7Bzswv%24%7Cv%22%7Bzs wv%24evo%22..%2F%2F%2F%2F%24%7C%7B%22..-%27%5D%3FN%3BK+_; hst=1-1128213491-0:0:0:nac; url=http%3A%2F%2Fwww.google.co.in%2F; ctr=2; acl=1; d1 y=1-1128213610-14486:259200-70912:259200; fme=1....
T 192.168.7.191:1123 -> 64.124.153.143:80 [AP]
&domainContext=co.in&distID=1000%7C68%7C0%7C0%7C6BANER02.EXE&country=IN
&transponderID={9FB27148-34BE-4B13-8066-A72A1646DEB4}&build=0.21.5.112
&s=136310&c=70912&ca=14486&s0=136310 HTTP/1.1..Accept: */*
&country code
&Request made through IE
&Ad server
&current URL
&Aurora instance ID
&domain context
&Ad engine
Transmission of System data

T 192.168.7.191:1129 -> 64.192.114.141:80 [AP]

POST /bi/servlet/ThinstallPre HTTP/1.1..Accept: */*

User-Agent: POKE\nthnall1z.exe|2, 0, 3, 2|{88D61A6A-BDE5-4D95-B6F1-B9045DC6B03F}|84ABFDC6|55274-640-7712297-23104|005056070191|0|0,0|0|1 ..Host: thinstall.abe\ntterinternet.com..Content-Length: 164..Cache-Control: no-cache..Poke\nNumber=1..Computer Name=xpletive..ThinsId={88D61A6A-BDE5-4D95-B6F1-B9045DC6B03F}..Disk Space=Total:2043 Mbytes, Free:802 Mbytes..XML Versio\nn=XML Version 3.0...
Aurora.exe’s registry entries
Dial-home string contains Windows S/N
Random registry key and program name
If killed, the process re-spawns
A Better Internet - BHO
Socially Engineered software installs
It doesn’t matter if you “Cancel”
Installation via IE ActiveX as well
Installation via IE ActiveX as well

If automated download doesn't start, please Click Here and select "Run" or "Open" when prompted.
Removal Techniques

• Technological:
  – Spyware removers, much on the same lines as virus cleaners.
  – Browser protection toolbars, plugins.
  – Spybot, SpySweeper, Foxie, etc.
  – Firefox or non-IE browsers.
Removal Techniques

• Psychological:
  – Attacks made on our common sense and productivity.
  – We click to get rid of “annoyances”.
  – Bombarded with ominous sounding words and jargon.
  – The average user has very little hope to survive the psychological battle.
Looking Ahead

The shadows dissipate & the adware market polarizes

- The legitimate players become more visible
  - Forward-thinking adware cos. prove the behavioral model can work
  - Timely, very targeted ads (in small quantities) gain acceptance
  - Stigma shed over time and it begins to feel like a TV commercial, product placement in a movie, or just-in-time deal comparisons

- The illegitimate players retreat to malware
  - Increased media, advertiser & law enforcement scrutiny force them fully underground & to tolerant countries
Looking Ahead

The shadows dissipate & the adware market polarizes

- Winds of change are blowing
  - Some major advertisers (e.g. Major League Baseball) have stopped/condemned using adware
  - WhenU sets the bar high (& takes a revenue hit)
  - Claria shifting model away from pop-ups to search engine

- But…
  - The shake-out will not happen quickly
  - Solving the complex distribution/affiliate network problem is key and hits players in the bottom-line
Looking Ahead

From Chaos to Order

• Vendor consolidation
  – AntiVirus players catch up to AntiSpyware pure plays
  – Pure plays release full suites, die, or are acquired

• Market standardization sets in
  – Standards for definitions, classification and disputes already forming through AntiSpyware Coalition
  – 3rd party testing bodies emerge
  – Myriad of small “reviewers” fade as trustworthy tests emerge
Looking Ahead

From Chaos to Order

- Rogue AntiSpyware Programs Squashed
  - Programs that actually *install* spyware
  - Reached peak of 200+ bogus programs recently (SpywareWarrior.com)
  - FTC has taken action already vs. Spyware Assassin, SpywareKiller, and SpyBlast
  - Will be prosecuted or otherwise chased out of business