Spyware/Adware

The Quest for Consumer Desktops & How it Went Wrong

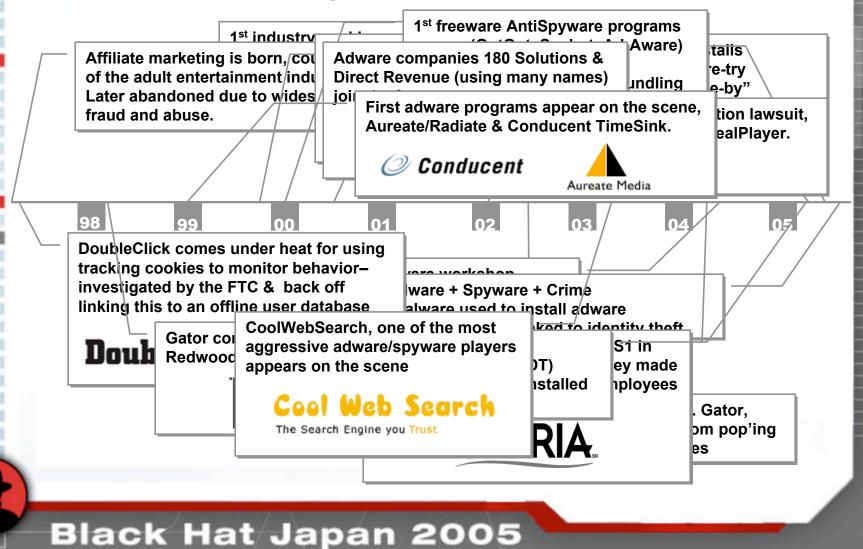
> Saumil Shah Dave Cole

Agenda

- The Adware & Spyware Business
- Disputes, Lawyers & Legislation

- The Technology
- Looking Ahead

How'd we get in this mess?





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

| Rank | Program name |
|------|-----------------|
| 1 | ShopAtHomeAgent |
| 2 | lstbar |
| 3 | CoolWebSearch |
| 4 | SearchAssistant |
| 5 | lefeats |
| 6 | Gain |
| 7 | BetterInternet |
| 8 | VirtuMonde |
| 9 | EliteBar |
| 10 | NdotNet |

Source: Symantec Internet Security Threat Report, 9/05

吕는

Adware Business Model – In Theory

Advertisers

Per-click commissions

Ad design

- ⊕



Distributors

7,256 K

bouncing benenas mpg 8,546 K bubbling bananas.mp3 5,862 K1 boling bananas.wav

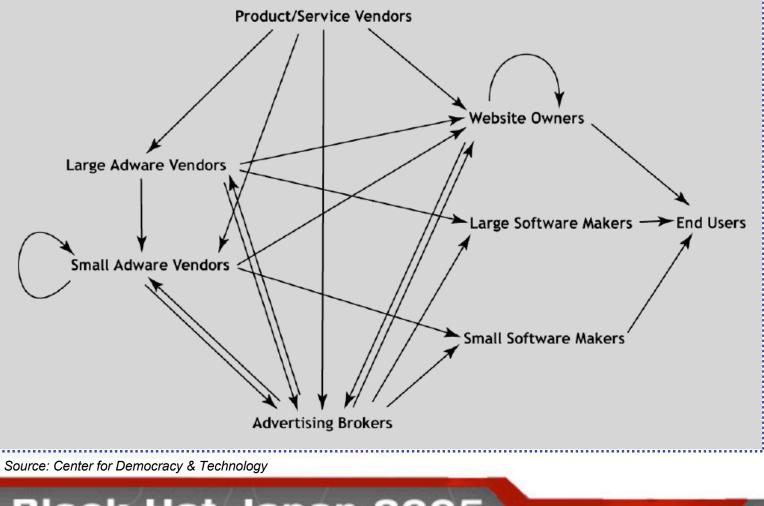
Free software bundle

Consumer

t Offer

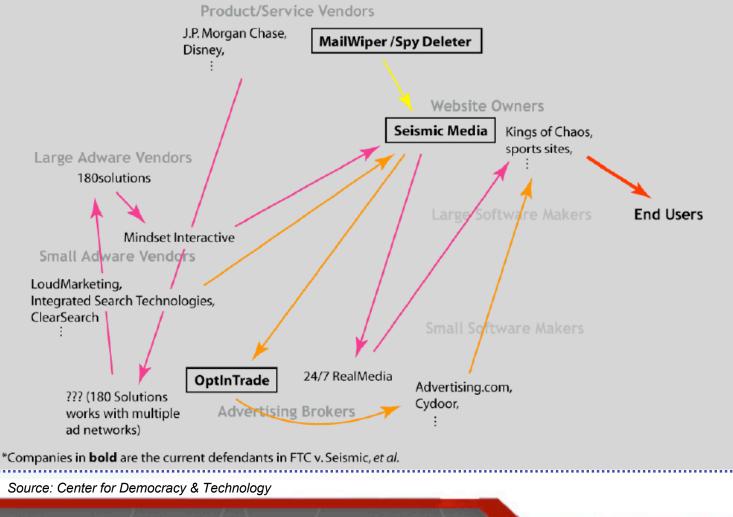
Source: Center for Democracy & Technology





Adware Business Model – Example

片는



Seismic Media Email Correspondence

From:

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.

From:

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.

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

| Rank | Program name |
|------|--------------|
| 1 | Webhancer |
| 2 | Apropos |
| 3 | Marketscore |
| 4 | CometCursor |
| 5 | e2give |
| 6 | Perfect |
| 7 | ISearch |
| 8 | Goidr |
| 9 | ISpynow |
| 10 | KeyTick |

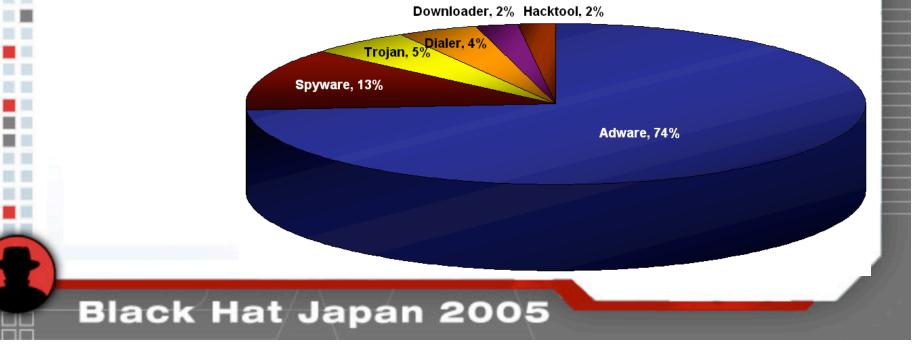
Source: Symantec Internet Security Threat Report, 9/05

Quick Look: Commercial Keyloggers

| Navigate | Time | | og Type Log Content | | Wiew Keylog | File Edit View Favorites Tools Help |
|-------------|------------|-------------|--|------------------------------|--------------------|--|
| | 11/03/2002 | 21:40:41 K | eystrokes [CTRL][ALT] | | | Search 🔶 💽 📓 🚮 🔎 Search 👷 Favorite |
| 1 | 11/03/2002 | | SpyActions Autostart Monitoring SpyActions Protect XPCSpy | | Archive Files | Links 🛅 AD 🙋 2CheckOut 👸 2CO Sellers Area — Login 👸 Barchart |
| General | 11/03/2002 | 21:40:38 K | eystrokes images[ENTER][ENTER][A SpyActions Close XPCSpy | LT] | Clear Capture | You are in 30's:7(for all the thirty-something Logging 14cbin9 (localhost/127.0.0.1) into the chat system |
| | 11/03/2002 | 21:39:26 X | SpyActions Send mail failed | | | You are in 30's:7 (for all the thirty-somethings out there.) |
| - I | 11/03/2002 | | creenshots 浏览文件夹 evstrokes | | Capture Folder | toungeslasher2000 joined the room. epsteinb123 : If anyone else wants to see, her name is heather 19pi |
| Logs View | 11/03/2002 | 21:37:51 K | eystrokes [ALT] | | mmddyy_hhmmss user | thomasforrest5002 : No, just raised the possibility ccc824 left the room. |
| | 11/03/2002 | 🚖 123 XPCSp | y 1.35 (unregistered) | | | mommynooooooooo : that hurt blueeyedchimchim : implying is same as raised thomas |
| | 11/03/2002 | Advanced | | | 📕 Apply | halos_kiss : Iol cathys0917 left the room. |
| Settings | 11/03/2002 | Navigate | Password Settings | | | d_spieg@sbcglobal.net joined the room. carebear412345 is back |
| settings | 11/03/2002 | | Enable password | Password setting Pa | assword | wgolyas left the room. thomasforrest5002 : one is saying, the other is identifying a possibili |
| ~~ . | 11/03/2002 | 2 | | | 10011010 | mommynooooooooooooooooooooooooooooooooo |
| 0 | 11/03/2002 | General | Start Monitoring Option | | | thomasforrest5002 : a subtle difference |
| Advanced | Refrest | | Enable scheduling. | Autostart Monitoring with ru | | blueeyedchimchim : battery cables on body parts would hurt sherlegalgiri joined the room. |
| a., | | 🔶 | Autostart XPCSpy when <u>O</u> S start. | C Start Monitoing by Schedul | | peter_peat2001 : peter blueeyedchimchim : i dont agree thomas |
| <u>8</u> | | Logs View | Start monitoring at: 00:00:00 | Stop monitoring at: 23:59:59 | | Aaddboddbr 🔗 🔪 Hide the user list |
| About | | | Send Logs Report Via EMail | | | |
| | | 1 | Enable sending logs report via email | C Send <u>I</u> ext Report | | |
| | | Settings | ✓ Send Keystorkes Log | Send Html Report | | |
| | | | ✓ Send Website Log | Send Mail To: test@share | -ware.us | |
| | | 1 | Send Application Log | Mail Subject: XPCSpy Ma | | |
| | | Advanced | Send 🛛 PCSpy Log | Send Mail Every 10 📩 | minute(s). | |
| | | | | | | |
| | | 1 | Start | S <u>t</u> op <u>H</u> ide | Exit | |
| | | About | | | | |

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



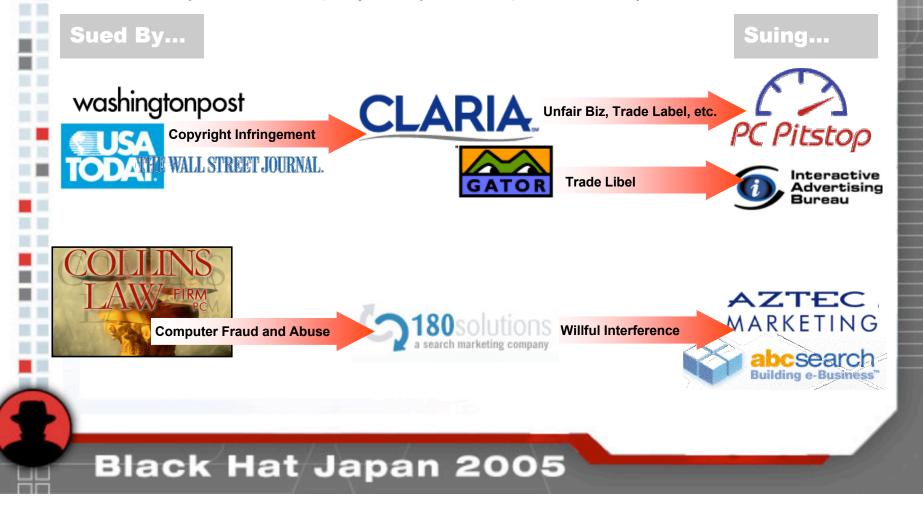
Adware & AntiSpyware Disputes

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)



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 Min defines spyware and | nistry of Information and Communica d sets penalties for those who create to 5 years in prison or fines of up to V 0,000). | or |
| | Australia Bill introduced in May of 2005 fine companies \$10,000 AUD for spreading spyware. | |
| Black Ha | t Japan 2005 | |

Spyware Taxonomy

- Spyware/snoopware/keyloggers
- Adware
- Backdoors
- Dialers
- Hijackers

Case Study - HotBar



Black Hat Japan 2005

片는

HotBar

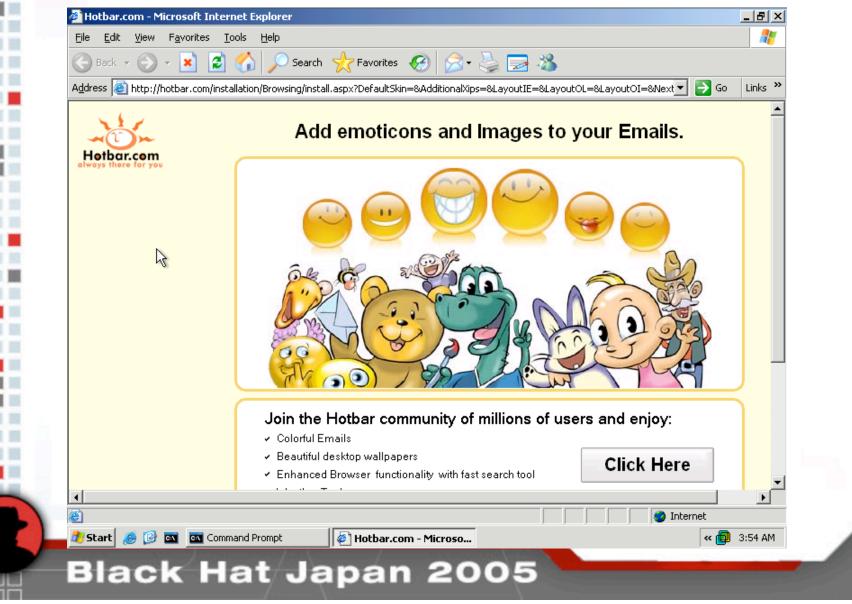
- Fancy toolbars for IE and Outlook.
- Skins, smileys, weather, games and other gimmicks.
- Hijacks Browser searches, URLs and displays advertisements.
- Ads are pop-unders, browser frames, DHTML overlays, tool buttons, etc.

HotBar

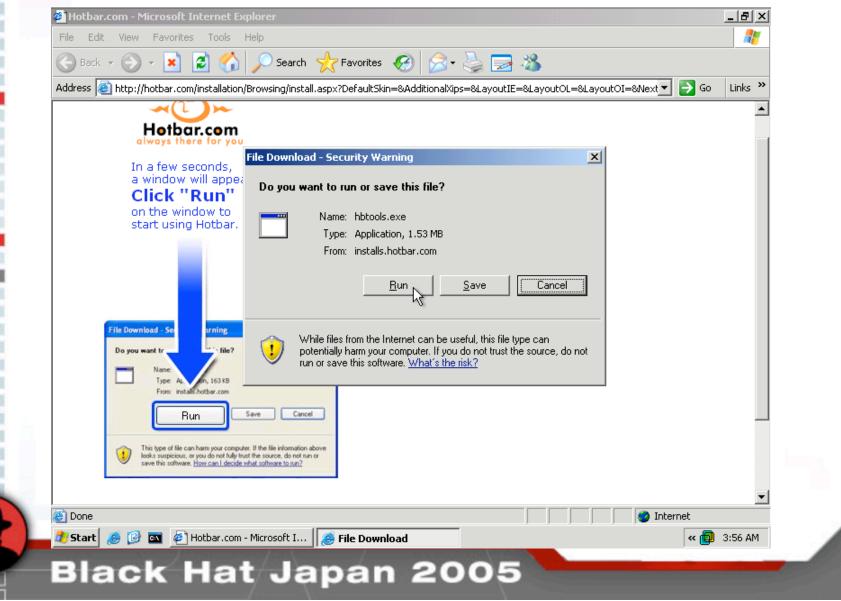
- Genuinely claims to be ad-supported software.
- Slight level of "social engineering" when it comes to installation.

hotbar.com site

井는



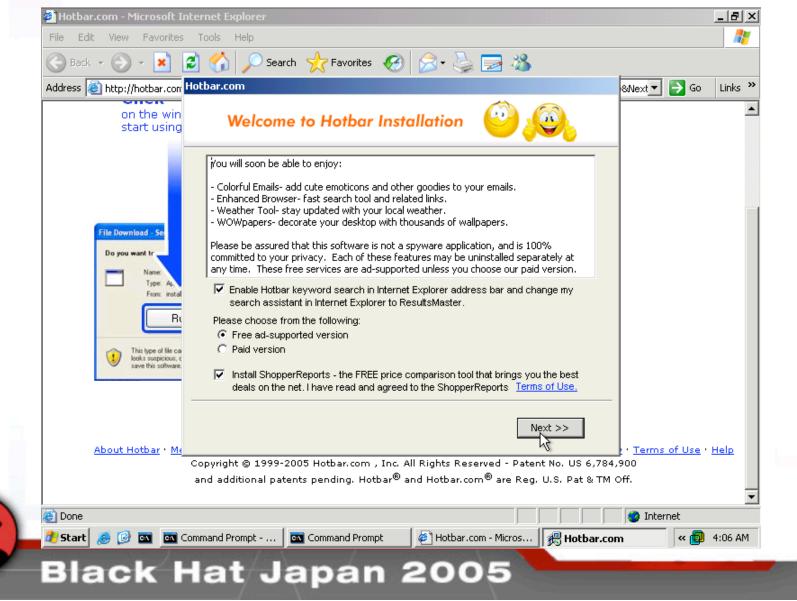
Instructions on how to "install"



Publisher: "a Microsoft Certified Partner"

| | net Explorer @ X Iols Help |
|--|--|
| 🕞 Back 👻 🕥 👻 🛃 | 🏠 🔎 Search 🤺 Favorites 🥝 🔗 🎍 🔜 🔏 |
| Address 🙆 http://hotbar.com/insta | llation/Browsing/install.aspx?Default5kin=&AdditionalXips=&LayoutIE=&LayoutOL=&LayoutOI=&Next 🗾 🎅 Go 🛛 Links 🌺 |
| on the window start using Hot | |
| In | ternet Explorer - Security Warning |
| File Download - Se Do you want tr Name: Type 44 Form installed Run With type of file can harm you fools surpticious, or you do save this software. How can About Hotbar - Media Cop | Do you want to run this software? Name: Hotbar.com, a Microsoft Certified Partner, and do Publisher: HOTBAR.COM Inc. More options Rup 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? Rup 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? Rup 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? Rup 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? Rup Harding and Harding above the file type can potentially harm your computer to only run software from publishers you trust. What's the risk? Rup Harding and Harding above the file type can potentially harm your computer to only run software from publishers you trust. What's the risk? Rup Harding and Harding above the file type can potentially harm your computer to only run software from publishers you trust. What's the risk? Rup Harding and Harding above the file type can potentially harm your computer to only file the file type can be above the fi |
| | |
| Done | 📄 📄 👘 🛃 🛃 🛃 |

Disclosure of Intention



Hotbar installed

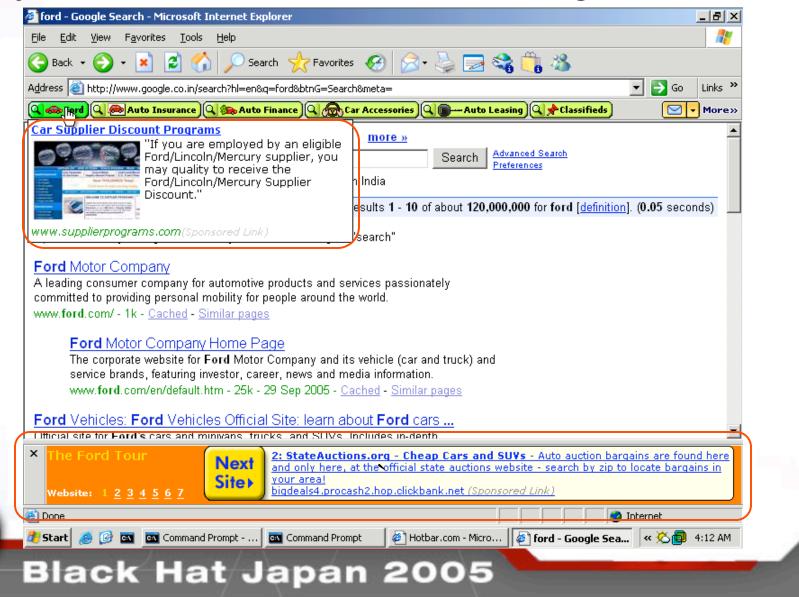


Hotbar Browser Helper Objects

10.0

| | with the operation might prevent son | rams that extend the capabilities of your browser. You can disab ne Web pages from working. re been used by Internet Explore | le, enable, o | | | Version=4%2e7%: So Links |
|--------------|---|---|---|---|--|---|
| N | ame 🔺 | Publisher | Status | Type | File | |
| | HbtMain Hotbar Hotbar Shockwave Flash Object ShopperReports - Com | (Not verified) Hotbar.com (Not verified) Hotbar.com (Not verified) Hotbar.com Macromedia, Inc. | Enabled Enabled Enabled Enabled Enabled | ActiveX Control Toolbar Browser Helper Object ActiveX Control Browser Extension | HbtHostIE HbtHostIE HbtHostIE flash.ocx | |
| | ShopperReports - Com | (Not verified) ShopperRep | Enabled Enabled | Browser Extension | ShprRprt.c | |
| | لم ا | 8 | | | P | |
| Sel | | bove to perform the following ac | ions: pdate | | | |
| 5 | o disable an add-on, click it hen click Disable. To update | an <u>Enable</u> (| lick here to dd-on | update this Update | ActiveX | uto auction bargains are found her search by zip to locate bargains in |
| T th A | ctiveX control, click it and th lick Update ActiveX. | | | | | |

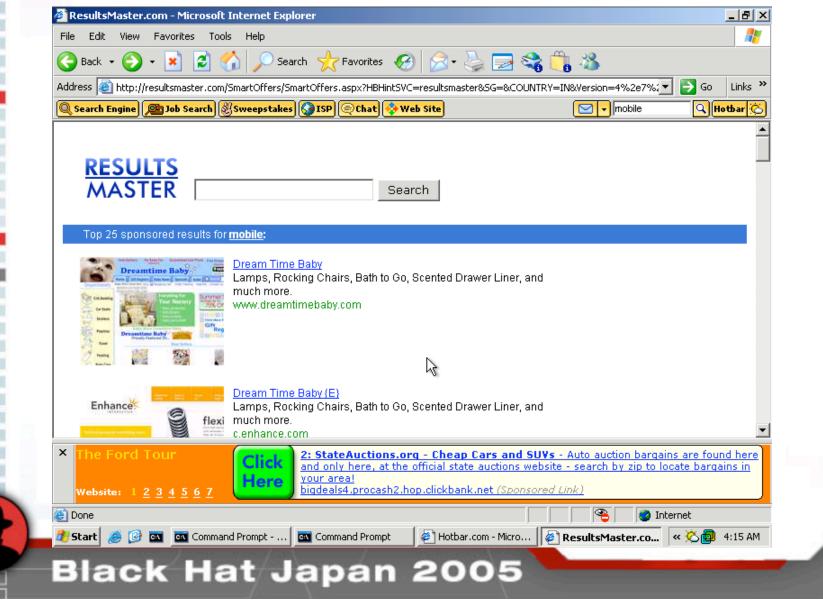
Dynamic tool buttons from Google search



Pop-under advertisements



Searching within hotbar



Hijacking the "404 not found" page

| dress 🧃 http://page-not-found.net/SmartOffers/Smart Classifieds 🙍 People Search 👰 Job Search 🕅 Sv | | | | o Links » |
|--|--|------------------------------|-------------------|-----------|
| Cassineas (Streake search) (Streake search) (Streake search) | | | | <u></u> |
| Search cannot be found - saumil.net. Please try typing a search query in the search box | below: | | Brought to you by | Hotbar |
| | | | | |
| | Search | | | |
| | | | | |
| erhaps you may find the links below helpful: | | | | |
| Block Pop-up ads | | | | |
| Stop Email Spam | | | | |
| Keep your PC private | | | | |
| | | | | |
| | R | | | |
| lease try one of the followings: | 0. | | | |
| Check your keywords spelling Try different keywords | | | | |
| Try unerent keywords Try more general keywords | | | | |
| | | | | |
| | | | | |
| | <u>lotbar</u> · <u>Advertise with Us</u> · <u>Contact</u> Hotbar.com Inc. All Rights Reserv | | | |
| copyright o reservoid | notbal.com nic. An Aights Aesero | eu. notbal is patent penung. | | |
| | | | | • |
| one | | | 🥑 Internet | |

Case Study - A Better Internet

a better †nternet



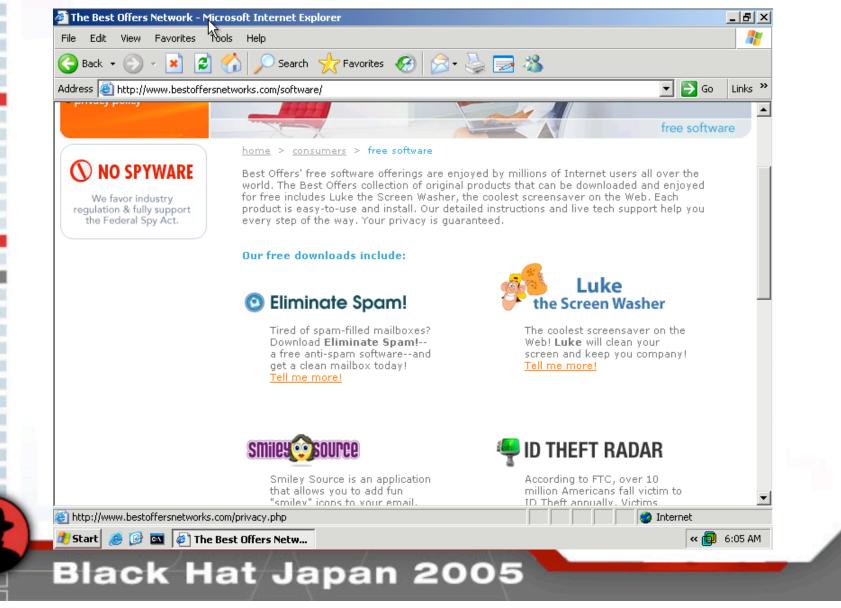
A Better Internet

- "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



Download free software - Screensaver

片는

| Address 🙆 http://bestoffersnetwo | orks.com/software/luke/ | 💌 🄁 Go |
|--|---|--|
| bestoffers | File Download - Security Warning | consumers partners |
| free software support eula privacy policy | Do you want to run or save this file? Name: BO_LUK1000.exe Type: Application, 179 KB From: st.bestoffersnetworks.com | free software |
| NO SPYWARE We favor industry regulation & fully support the Federal Spy Act. | <u>Run</u> Save Can While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source run or save this software. What's the risk? | en Requirements: ows XP, NT, 2000 or 98 |
| | 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? | How to install Luke the Screen Washer: Click the "download" button above to download the installation package. You will be asked whether you wish to Save the file locally or to Run the file. |
| | Luke the Screen Washer is provided to you free of charge because it is supported by advertising from | If you choose to Save the file: 1. Your computer will now ask |

"Free software" installing itself

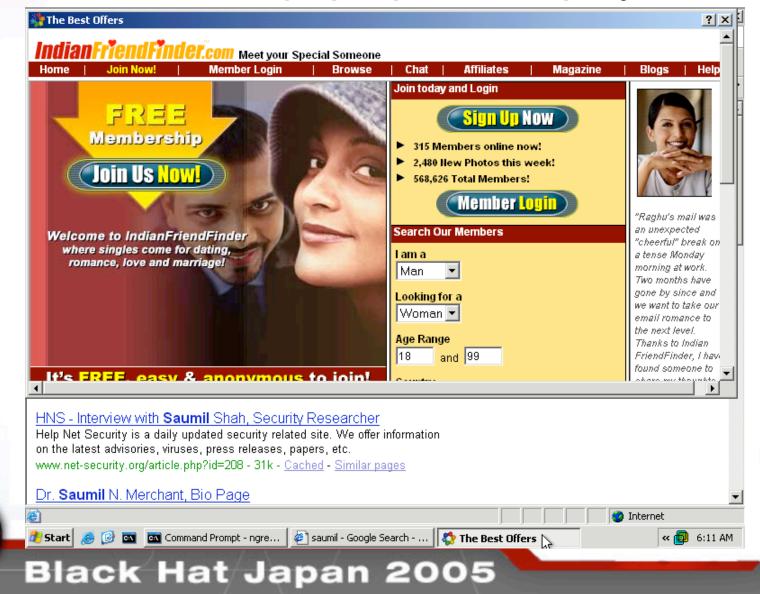
| Nddeoco 🦚 Like / VL L- Mana - Lu | under ander Genuere Ander A | 🔻 🔁 Go |
|--|---|--|
| Address 🙋 http://bestoffersnetv | vorks.com/sortware/luke/ | <u> </u> |
| bestoffers | Internet Explorer - Security Warning | isers consumers partner |
| free software support | Do you want to run this software? Name: Luke Installation Publisher: the best offers network, llc. | |
| eula privacy policy | More options | Don't Run |
| | | |
| () NO SPYWARE | While files from the Internet can be useful, this file type can puyour computer. Only run software from publishers you trust. | |
| NO SPYWARE We favor industry regulation & fully support the Federal Spy Act. | your computer. Only run software from publishers you trust. | What's the risk? |
| We favor industry regulation & fully support | your computer. Only run software from publishers you trust. | Ad Now! System Requirements: Windows XP, NT, 2000 or 98 How to install Luke the Screen Washer: Click the "download" button above to download the installation package. You will be |
| We favor industry regulation & fully support | your computer. Only run software from publishers you trust. You the Screen Washer Free Screensaver that cleans your screen 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 | Ad Now! System Requirements: Windows XP, NT, 2000 or 98 How to install Luke the Screen Washer: Click the "download" button above to download the |
| We favor industry regulation & fully support | your computer. Only run software from publishers you trust. You the Screen Washer Free Screensaver that cleans your screen 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. | Ad Now! System Requirements: Windows XP, NT, 2000 or 98 How to install Luke the Screen Washer: Click the "download" button above to download the installation package. You will be asked whether you wish to Sav |

Pop-under when using search engines

片

| 🖥 saumil - Google Search - M | licrosoft Internet Explorer | _ B × |
|--|--|--|
| <u>File E</u> dit <u>V</u> iew F <u>a</u> vorites | <u>T</u> ools <u>H</u> elp | A. |
| 🌏 Back 🝷 💮 🚽 🚺 | 💈 🏠 🔎 Search 🦙 Favorites 🛛 🔗 😓 🍡 | • |
| A <u>d</u> dress 🙋 http://www.google. | co.in/search?hl=en&q=saumil&meta= | 💌 ラ Go 🛛 Links 🌺 |
| 0 1 | Web Images Groups News more » | - |
| Google | Leaumil Dearth and a search and a search a searc | anced Search erences |
| 000010 | Search: 💿 the web 🔿 pages from India | |
| Web | Results 1 - 10 of a | bout 33,100 for saumil. (0.07 seconds) |
| | - 12k - <u>Cached</u> - <u>Similar pages</u> | |
| net-square.com/saumil/ - Saumil Merchant Saumil Merchant. Graduat University of Tennessee Kr web.utk.edu/~smerchan/ - <u>HNS - Interview with Sa</u> Help Net Security is a daily on the latest advisories, vir | tographs, publications, interests and poems. 14k - <u>Cached</u> - <u>Similar pages</u> the Student Department of Electrical and Computer Engineering toxville, TN 37996 3k - <u>Cached</u> - <u>Similar pages</u> aumil Shah, Security Researcher of updated security related site. We offer information uses, press releases, papers, etc. a.php?id=208 - 31k - <u>Cached</u> - <u>Similar pages</u> | |
| Family, friends, scenic pho net-square.com/saumil/ - 1 Saumil Merchant Saumil Merchant. Graduat University of Tennessee Kr web.utk.edu/~smerchan/ - <u>HNS - Interview with Sa</u> Help Net Security is a daily on the latest advisories, vir www.net-security.org/article Dr. Saumil N. Merchan | tographs, publications, interests and poems. 14k - <u>Cached</u> - <u>Similar pages</u> the Student Department of Electrical and Computer Engineering toxville, TN 37996 3k - <u>Cached</u> - <u>Similar pages</u> aumil Shah, Security Researcher of updated security related site. We offer information uses, press releases, papers, etc. a.php?id=208 - 31k - <u>Cached</u> - <u>Similar pages</u> | Titernet ers 6:10 AM |

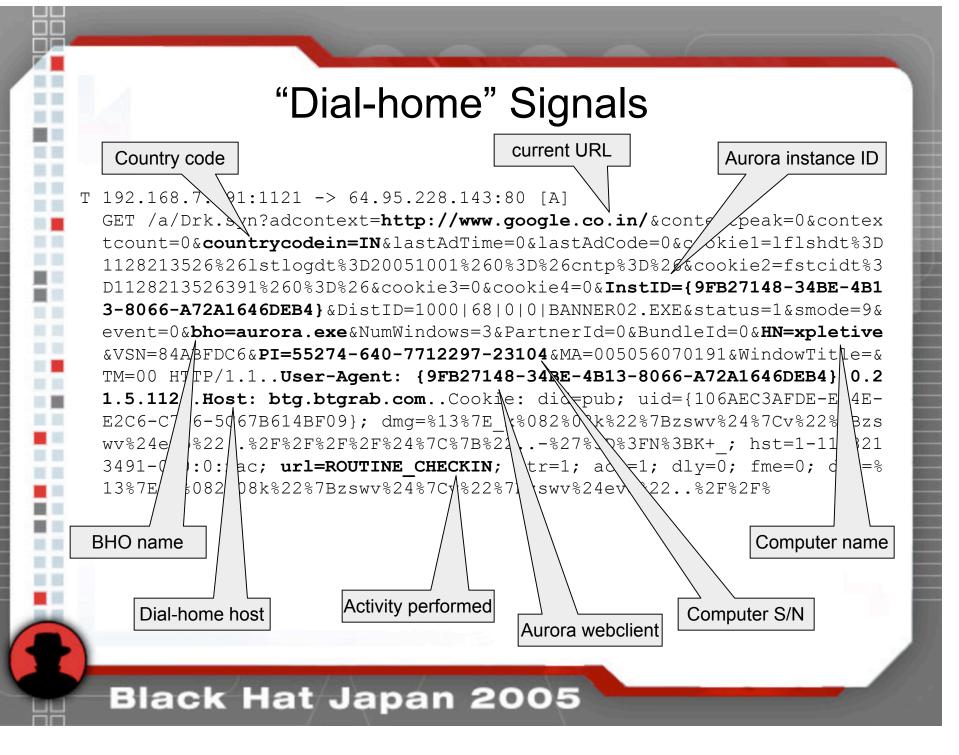
Contextual pop-up ads displayed



"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/&contextpeak=0&contex tcount=0&countrycodein=IN&lastAdTime=0&lastAdCode=0&cookie1=lflshdt%3D 1128213526%26lstlogdt%3D20051001%260%3D%26cntp%3D%26&cookie2=fstcidt%3 D1128213526391%260%3D%26&cookie3=0&cookie4=0&InstID={9FB27148-34BE-4B1 3-8066-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 1.5.112..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%24%7C%7B%22..-%27%5D%3FN%3BK+_; hst=1-112821 3491-0:0:0:nac; url=ROUTINE_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%



Advertisement Polling

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%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-Lan guage: 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=1-112821 3491-0:0:0:nac; url=http%3A%2F%2Fwww.google.co.in%2F; ctr=2; acl=1; dl y=1-1128213610-14486:259200-70912:259200; fme=1....

| Ad engine 7 CC V C | current URL Aurora instan | |
|---|--|---------------------------------------|
| т 192.168.7 191:1123 -> | 64.124.153.143:80 [AP] | country coo |
| | rve?urlContext=http%3A%2F%2Fw / .google | |
| domainContext=co.in&dia | stID=1000%7C68%7C0%7C0%7CBAN1/ER02.EXE& | |
| _ | 48-34BE-4B13-8066-A72A1646DEB4 } &build= | |
| s=136310&c=/0912&ca=1 | 4486&s0=136310 HTTP/1.1Accept: */* | - |
| | <pre>ncoding: gzip, deflateUser-Agent: Mo Windows NT 5.1; SV1)Host: xadsj.off</pre> | |
| 2C6-C7D6-5C67B614BF09 v%24evo%22%2F%2F%2F 191-0:0:0:nac; url=ht 1-1128213610-14486:2 | <pre>p-Alive; ookie: did=pub; uid={106AEC3. }; dmg=%1 7E_x%082%08k%22%7Bzswv%24%7 %2F%24%7C% %22%27%5D%3FN%3BK+_; hs tp%3A%2F%2F w.google.co.in%2F; ctr=2; 59200-70912 9200; fme=1 Request made through IE</pre> | Cv%22% Bzs t=1-11: 821 acl=1 dl |
| domain context | | Ad server |
| | | |
| | | |

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|
thnall1z.exe|2, 0, 3, 2|{88D61A6A-BDE5-4D95-B6F1-B9045DC6B03F}|84ABFDC
6|55274-640-7712297-23104|005056070191|0|0,0|0|1 ..Host: thinstall.abe
tterinternet.com..Content-Length: 164..Cache-Control: no-cache....Poke
Number=1..Computer Name=xpletive..ThinsId={88D61A6A-BDE5-4D95-B6F1-B9
045DC6B03F}..Disk Space=Total:2043 Mbytes, Free:802 Mbytes..XML Versio
n=XML Version 3.0...

Aurora.exe's registry entries

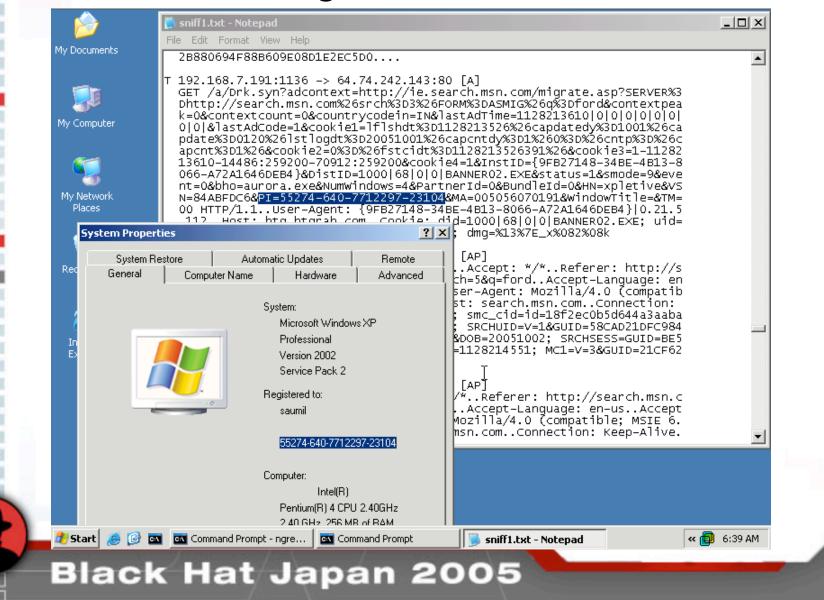
💣 Registry Editor

10.0

_ 8 ×

| 🖃 💻 My Computer | Name | Туре | Data | |
|--------------------------------------|---------------------|--|--|-------------|
| 🗄 🚞 HKEY_CLASSES_ROOT | (Default) | REG_SZ | (value not set) | |
| | AU3N5a7tionSCode | REG_SZ | IN | |
| 🗄 🧰 AppEvents | AUB3D5om | REG_SZ | ~Š'+•‰"—^œŒ—Ž~□€'œÌ'•ž'-†‰□Ô€□• | |
| Console | AUC1o3d5eOfSFi | REG SZ | 1 | |
| 🗄 🛄 Control Panel | AUC3n5tFyl | REG_DWORD | 0×00000000 (0) | |
| Environment | AUC3n5trMsgSDisp | - | 0x00000030 (48) | |
| | AUC3u5rrentSMode | | 0×00000001 (1) | |
| 🗄 🦲 Keyboard Layout | AUD3s5tSSEnd | REG SZ | `~_ÀÀÍ□Ž^Ì□Ž^□`~Ă□□—ÀƒÝ¾□%ሠœ>œ | |
| Network | AUE3v5nt | REG_SZ | 0 | - |
| | ab AUI3d5OfSDist | REG SZ | - 1000 68 0 0 BANNER02.EXE | |
| SessionInformation | ab AUI3d5OfSInst | REG SZ | {9FB27148-34BE-4B13-8066-A72A1646DEB4} | |
| ⊡ 📴 Software | AUI3g5nore5 | REG_SZ | ™f<™‰Á□€□*f,ÿ□—→Á□□—*†□□□Ž- | _™ f<"Å |
| Ca aurora ∓Casses | B AUI3n5ProgSCab | REG_DWORD | 0x00000000 (0) | |
| E Classes | AUI3n5ProgSEx | REG_DWORD | 0×00000000 (0) | |
| ⊡ ⊂ygnas solutions ⊕ _ Intel | AUI3n5ProgSLstest | — | 0×00000000 (0) | |
| | AUL3a5stSSChckin | REG_DWORD | 0x000001d2 (466) | |
| | AUL3n5Title | REG DWORD | 0x0000003c (60) | N |
| | AUM3o5deSSync | REG_DWORD | 0x00000009 (9) | 2 |
| 🗄 🧰 Sysinternals | AUP3D5om | REG_DWORD | •‰"—^€́4″×́^Ÿ□Ì'□Ÿ | |
| - DIVICODE Program Groups | AUs3t5icky15 | REG_SZ | IfIshdt%3D1128213526%26capdatedy%3D100 | 1194.266 |
| | AUs3t5icky25 | REG_SZ | 0%3D%26fstcidt%3D1128213526391%26 | 11 70200 |
| 표 🚞 Windows 3.1 Migration Stat | AUs3t5icky35 | REG_SZ | 1-1128213610-14486:259200-70912:259200 | |
| 🗄 🚞 HKEY_LOCAL_MACHINE | AUs3t5icky45 | REG_52 REG_5Z | 1 | |
| 🗄 🧰 HKEY_USERS | AUT3h5rsh5Bath | REG_DWORD | 1 0×00002710 (10000) | |
| | AUT3h5rsh5Chec | — | 0x00002710 (10000) 0x0000002d (45) | |
| | | _ | | |
| | AUT3h5rsh5Mots | REG_DWORD | 0x00000064 (100) | |
| | AUT3h5rshSysSInf | | 0x000007d0 (2000) | |
| | | REG_SZ | 1128213610 0 0 0 0 0 0 0 0 | |
| | J | | | |
| My Computer\HKEY_CURRENT_USER\Softwa | re\aurora | | | |
| 🏄 Start 🛛 🥭 🞯 🔤 🔤 Command Pr | ompt - ngre 🛛 🍻 Reg | istry Editor | | « 📵 6:13 Al |
| | [] <u></u> (reg | 1 | | |
| Black Hat | | And and a second se | | |

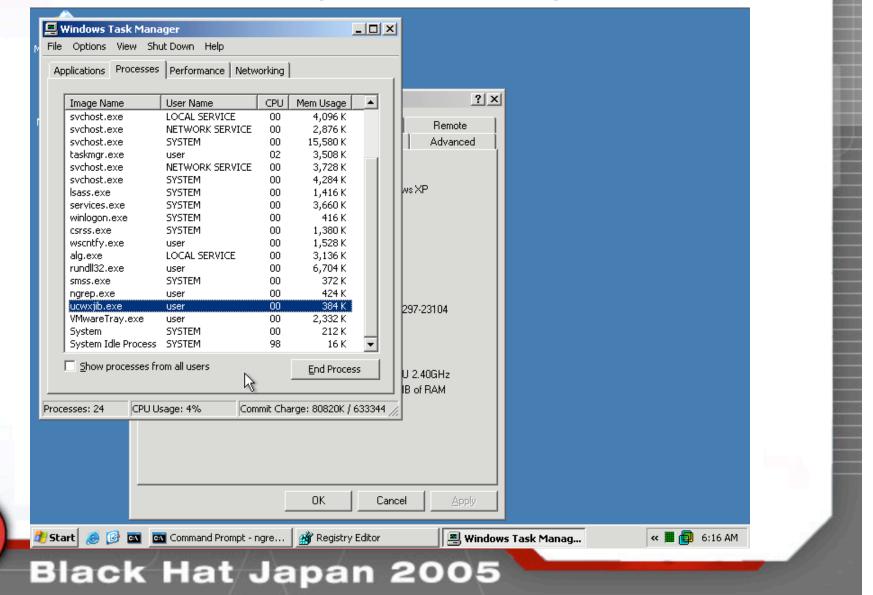
Dial-home string contains Windows S/N



Random registry key and program name

| | | Name | Туре | Data | |
|-----------------|-----------------------------|----------------------|---------------------|-------------------------------------|-----------------------|
| | | ab)(Default) | REG_SZ | (value not set) | |
| | 🕀 🧰 App Path | ab)pzdgavk | REG_SZ | C:\WINDOWS\system32\ucwxjib.e> | ker 🛛 |
| | 🕀 🧰 Applets 🧧 | Toois | REG_SZ | C:(Program Files(VMware)(VMware) | ray.exe |
| | 🕀 🧰 Control P | | | | |
| | 🕀 🧰 Controls | | | | |
| | CSCSettii | | | | |
| | 🕀 🧰 DateTime | | | | |
| | ⊕ 📄 Dynamic ⊕ 📄 Explorer | | | | |
| | | | | | |
| | | | | | |
| | H323TSP | | | | |
| | ⊞ ⊡ Hints | | | | |
| | ⊕ 🧰 Installer | | | | |
| | 🕀 🦲 Internet | | | | |
| | IPConfTS | | | | |
| | 🕀 🧰 MS-DOS I | | | | |
| | - 📄 NetCache | | | | |
| | 🗄 🧰 Nis | N | | | |
| | - OptimalLi | R. | | | |
| | 🕀 🚞 policies | | | | |
| | Reliability | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | SharedDl | | | | |
| | | | | | |
| | 🗄 🦲 ShellCom 💻 | | | | |
| | 🕀 🧰 ShellScra 💌 | | | | |
| • | | | | | |
| My Computer\HKE | Y_LOCAL_MACHINE\SOFTWA | ARE\Microsoft\Window | vs\CurrentVersion\P | Run | |
| | 🎯 💽 🔤 Command Prom | (| | 📧 Command Prompt 🛛 🚺 sniff1.txt - f | Notepad 🛛 < 👼 6:20 AM |
| <u> </u> | | | | | |

If killed, the process re-spawns



A Better Internet - BHO

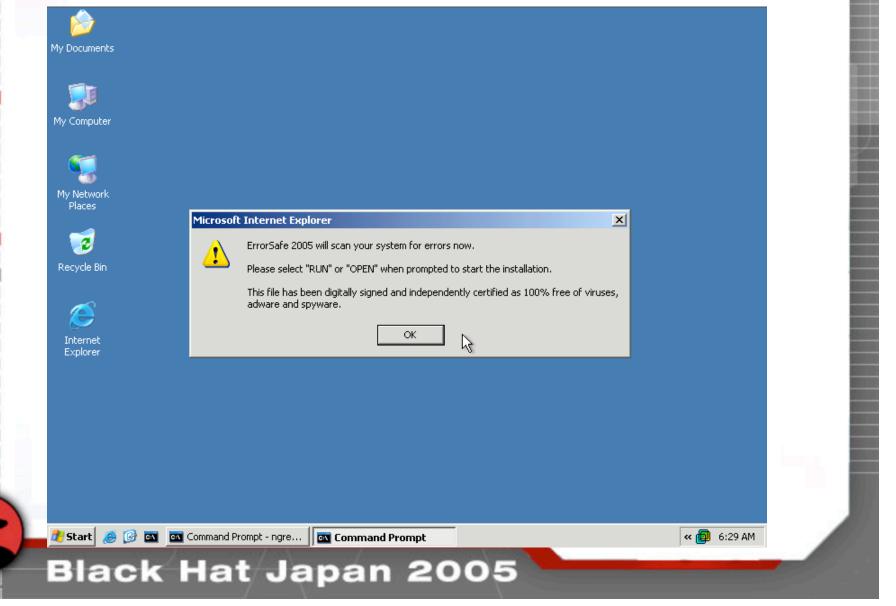
10.1

| ЧÇ | with the operation | rams that extend the capabiliti nof your browser. You can dis ne Web pages from working. | es of your Web able, enable, o | o browser. Some add-on or update add-ons. Disab | s can interfere bling an add-on | → Go L |
|---|---|--|---|--|------------------------------------|---|
| Sh <u>o</u> w: | Add-ons that hav | ve been used by Internet Expl | orer 💌 | | | <u>earch</u> |
| 🚺 🛐 Shockwa | ssistantOC ive Flash Object | Publisher Microsoft Corporation Macromedia, Inc. | Status Enabled Enabled | Type ActiveX Control ActiveX Control | File shdocvw.c flash.ocx | 100 for spyware. (0.06 second |
| Nindow: | s Messenger | | Enabled | Browser Extension | | Sponsored Links |
| | | | | | | ng <u>Slow?</u> i. Remove harmful adware, and popup ads. /areAlert.com |
| | | | | | Þ | pyware & Adware? ted? How Can I Remove It? Fo Common Spyware Questio ervoir |
| Settings To disable a then click D ActiveX cor | an add-on, click it Iisable. To update htrol, click it and th | an 💌 <u>E</u> nable | actions: Update Click here to add-on | update this | te ActiveX | Remover downloads yware Removers of 2005! on chart & software reviews areReport.com Could Be Infected |
| click Updat | bout add-ons | | | [| ОК | lidden & Harmful Software Vorms & Adware Now ! dware.com |

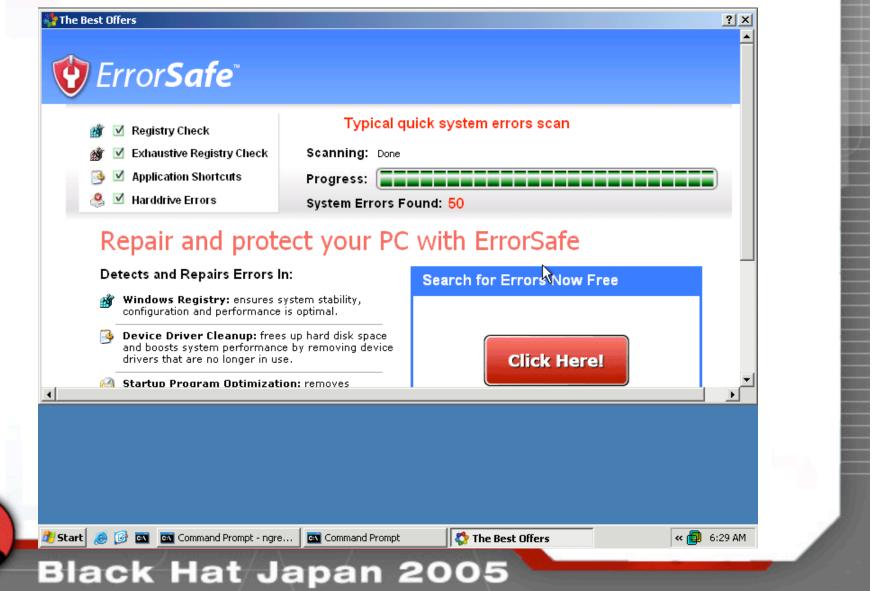
Socially Engineered software installs

| Snapin.CertTempMgr.1 | Name | Туре | Data | 1 | |
|---------------------------------------|--------------------------|---------------------------|-------------------------------------|--------------|-------------|
| Snapin.PolicySettings | (Default) | REG_SZ | (value not set) | | |
| Snapin.PolicySettings.1 | | _ | | | |
| Snapin.PolicySettingsAbout | | | | | |
| Snapin.PolicySettingsAbout.1 | | | | | |
| Snapins.FolderSnapin | | | | | |
| Snapins.FolderSnapin.1 | | | | | |
| Snapins.HTMLSnapin | | | | | |
| Snapins.HTMLSnapin.1 | | | | | |
| Snapins.OCXSnapin | | | | | |
| Snapins.OCXSnapin.1 | | | | | |
| snews | | | | | |
| SnmpSnapin.About Micro | soft Internet Explore | r | | × | |
| SnmpSnapin.About.1 | NOTICE: If your o | omputer bas errors in th | ne registry database or file system | a it could | |
| SnmpSnapin.SnmpSnapin | | le or erratic behavior, f | | ily ic coald | |
| SnmpSnapin.SnmpSnapin.1 🛛 🔍 | | | puter's performance and prevent | data loss. | |
| SnmpSnapinExtension.SnmpSn | | | | | |
| SnmpSnapinExtension.SnmpSn | (Recommended) | nstall ErrorSafe 2005 to | check your computer for free? | | |
| soap | (Recommended) | | | | |
| SoapAct.SoapAct | | | const. | | |
| SoapAct.SoapAct.1 | | <u>ок</u> | Cancel | | |
| Software | | | | | |
| a Microsoft | | | | | |
| 🖻 🧰 MediaPlayer | | | | | |
| Preferences | | | | | |
| SoftwareDistribution.WebControl | | | | | |
| SoftwareDistribution.WebControl.1 | | | | | |
| SoftwareDistribution.WUClientUIPlugin | | | | | |
| SoftwareDistribution.WUClientUIPlugin | | | | | |
| SoundRec | | | | | |
| SPCFile | 21 | | | | |
| | | | | | |
| ly Computer\HKEY_CLASSES_ROOT\Sol | tware\Microsoft | | | | |
| 🌮 Start 🛛 🥶 🚱 🔤 🔤 Comman | d Prompt - pare | Registry Editor | Command Prompt | | « 📵 6:27 AM |
| 🦲 scarej 📨 😰 🔤 comman | a Frompe - ngre | Registry Eultor | Command Prompt | | 1 0:27 AM |

It doesn't matter if you "Cancel"



Installation via IE ActiveX as well



Installation via IE ActiveX as well

10.0

12 1

| | ErrorSafe 2005 - Microsoft Internet Explorer | |
|----------------------|---|--|
| | File Edit View Favorites Tools Help | |
| My Network Places | 🕒 Back 👻 🕑 👻 📓 🏠 🔎 Search 🤺 Favorites 🤣 🔗 嫀 🔜 🖓 | |
| | Address 🕘 http://www.errorsafe.com/pages/scanner_in/download2.php?resize=1&aid=c 💽 🕞 Go 🛛 Links 🎽 | |
| 2 | To help protect your security, Internet Explorer blocked this site from downloading files to your computer. | |
| Recycle Bin | | |
| Internet | If automated download doesn't start, please Click Here | |
| Explorer | and select ''Run'' or ''Open'' when prompted. | |
| | Downloading from site: http://www.errorsafe.com/pages/ Downloading from site: http://www.errorsafe.com/pages/ | |
| | | |

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 omnious sounding words and jargon.
 - The average user has very little hope to survive the psychological battle.

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

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

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

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

