



***ThreatTrack**TM* *Security*

Ouroboros

Christopher Boyd - Senior Threat Researcher

Jovi Umawing - Communications & Research Analyst

Ouroboros

An ancient symbol depicting a serpent or dragon eating its own tail

- ◆ Used to symbolise cyclicity – it is never ending
- ◆ Eats its own tail, destroying itself to create life
- ◆ Now you don't need to Google it

Old is the New “New”

“Printers contain hardcoded backdoor account” - 2012

“Laser printers encode pages with identifying information” – 2005

“Street gangs use Twitter to trash talk rivals” - 2009

“Netbangers” use web services to communicate – 2006

“Google files facial password patent” – 2013

“Passwords may be thing of the past” – 2007

“PRISM scours the web” – 2013

“Government spyware” – 2005

“Charlatans exaggerate mobile malware threat” – 2011

“Mobile viruses greatly exaggerated” - 2005

Way Back When...

The Problem

- ◆ Adware / Spyware wasn't being addressed by traditional AV
- ◆ Threat of legal action – all of a sudden, the “bad guys” had lawyers
- ◆ Numerous attempts to combat the antispware industry

The Solution

- ◆ An explosion of support forums training grassroots infection removal
- ◆ Numerous independent researchers and their blogs
- ◆ Smaller firms / programs dedicated to tackling Ad/Spyware

The Problem

- ◆ Nobody understood what we were doing

THE KEY PLAYERS

The Key Players

Zango (1999 - 2009)

- ◆ Adware applications, gateways display advertisements to view or access content online
- ◆ Notification issues, affiliate problems, gave up \$3 million in 2006 for ill gotten gains via an FTC settlement
- ◆ Numerous attempts to combat the antispymware industry

Direct Revenue (2002 - 2007)

- ◆ Notorious pieces of Adware, including Nail.exe and Aurora
- ◆ A “Department of the Dark Arts” responsible for new types of Adware
- ◆ Aggressively pursued researchers: legal threats, private detectives
- ◆ Settled with the FTC for \$1.5 million in 2007

Main Areas of Concern: 2005 -2008

Adware Installs

- ◆ Standalone executables / Browser Plugins / Active-X
- ◆ Bundles (some legit, some blackhat)
- ◆ Content Gateways

Infection Channels

- ◆ Social Networks (Myspace & similar) (Standalones, plugins, gateways)
- ◆ Ad Networks and affiliates (Drive-by, exploits, scam sites)
- ◆ P2P, IM worms, Botnets (Bundles, cracked / tampered standalones)

Main Areas of Concern: 2009 -2013

Adware Installs

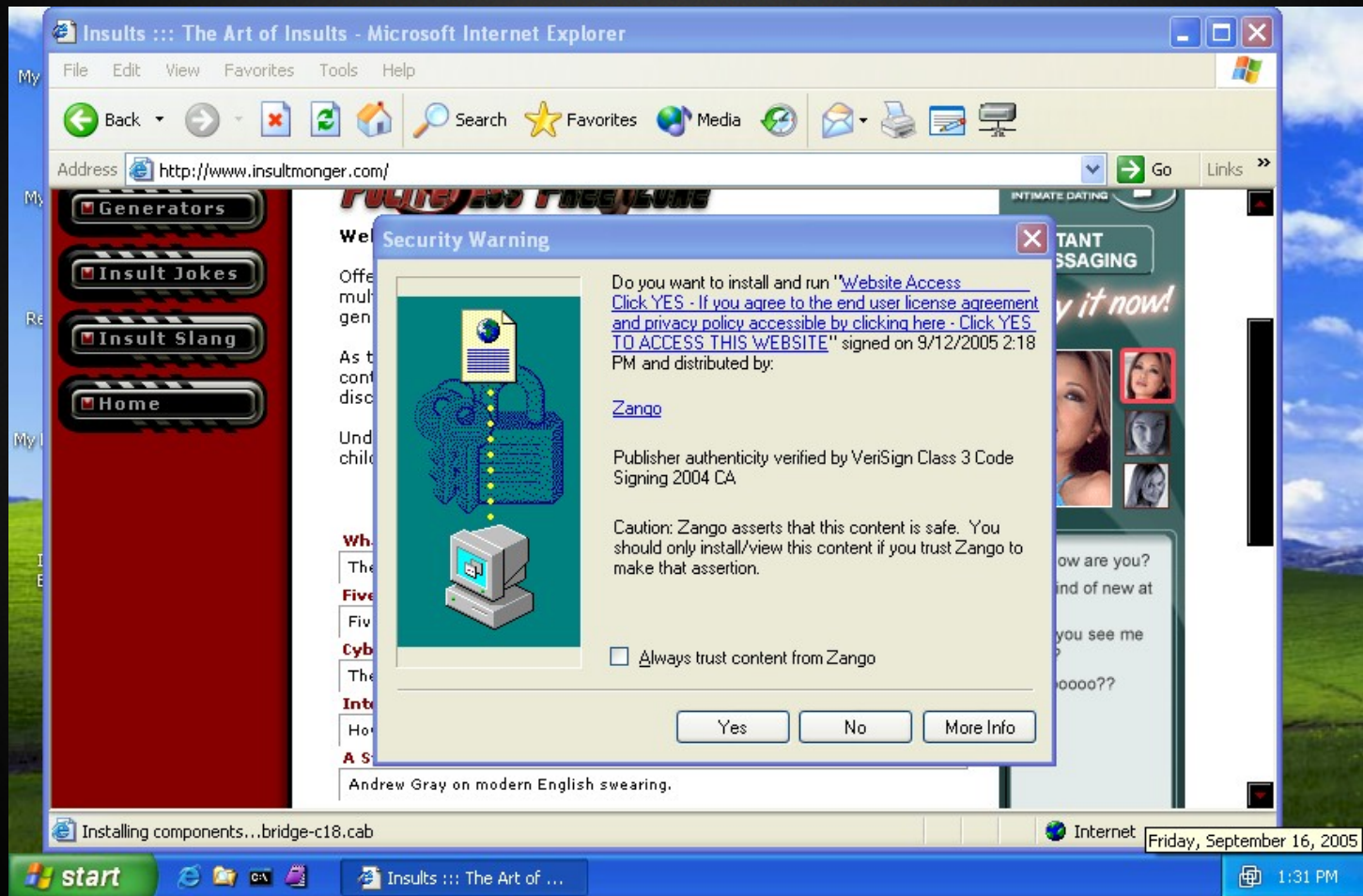
- ◆ Standalone executables / Browser Plugins / Surveys
- ◆ Bundles (mostly legit, some blackhat)
- ◆ Content Gateways

Infection Channels

- ◆ Social Networks (YouTube, Twitter, Facebook etc)
- ◆ Ad Networks and affiliates, Search engine adverts
- ◆ Mobile (SMS scam, survey scam, fake / rogue apps)

ADWARE INSTALLS

ActiveX (Gateway Evolution) - Sept 05



Content Gateways – August 2008

The screenshot shows the MovieTvOnline.com website. At the top, there is a navigation bar with links for HOME, TRAILERS, and MOVIES. A Zango advertisement is prominently displayed in the center, featuring the Zango logo and the text "You're Good to Go". Below the logo, it states "movietvonline.com is sponsored by Zango" and provides a detailed explanation of Zango's services as a free, premium-content access tool. To the left of the ad, there is a movie poster for "The Dark Knight (2008)" with a description of the plot. To the right, there is a list of movies, including "5. Shine a Light (2008)". A dialog box for the "Zango, Inc. End User License Agreement" is open in the foreground, containing a "NOTICE TO USER" and a checkbox for agreeing to the terms. The dialog box has "Cancel" and "Start" buttons.

MovieTvOnline.com

HOME TRAILERS MOVIES

Welcome to MovieTvOnline.com, have a nice day! BOOKMARK

Watch Movies Online for

zango™ You're Good to Go

movietvonline.com is sponsored by Zango

Zango is a free, premium-content access tool, paid for by advertising. Once installed and while online, using keywords sent to Zango from your Internet browsing, Zango software (with Weather) shows ads in a Zango Toolbar; a temporary Slider, on (e.g.) the bottom corner of your screen; and a separate browser window that pops up on your screen. If you search for or view Adult websites, you may receive Adult-oriented ads. Depending on your browser version, Zango may become the default search provider. Additionally, Zango may redirect a search resulting in an error to a list of sites similar to your search terms. Zango's Internet Explorer, Outlook/Outlook Express and Word Toolbars give access to free emoticons (and more) within those applications, when online. Zango runs continuously and upgrades automatically. Uninstallation is easy via Add/Remove Programs.

For more information: [Best Practices](#), [Privacy Policy](#), [FAQ](#) [View EULA](#) | [Print EULA](#)

Zango, Inc.
End User License Agreement
(June 3, 2008)

NOTICE TO USER: THIS END USER LICENSE AGREEMENT ("EULA" or "AGREEMENT") APPLIES WITH RESPECT TO SOFTWARE APPLICATIONS AND DIGITAL CONTENT OWNED AND PROVIDED BY ZANGO, INC. AND ITS SUBSIDIARIES

☒ By clicking "Start," I represent that I (1) am at least 18, (2) agree to the EULA and Privacy Policy terms and (3) consent to install Zango and access movietvonline.com.

Cancel Click "Start" to install Zango and access this website for free Start

The Dark Knight (2008)
Batman and Attorney, Ha Joker, whils and more d
TRAILER (0
FULL MOVIE (



Vers
PAR
Vers
PAR
6 P
Vers
PAR
Vers
PAR

5. Shine a Light (2008)
[View complete list >>>](#)

Content Gateways - July 2011

The screenshot shows the Fox News website interface. At the top, there are navigation links for Fox News, Fox Business, Small Business Center, Fox News Latino, Fox News Radio, and Fox Nation. A search bar is visible. Below the navigation, there are sections for 'ON AIR NOW' featuring Glenn Beck and a 'Special Report w/ Bret Baier'. A large overlay window titled 'Get FREE access to Videos' is centered on the screen. The overlay contains the Fox News logo, a description of the FREEzeFrog offer, and two installation options: 'Express Installation (recommended)' and 'Custom Installation with FREEzeFrog'. At the bottom of the overlay are 'Cancel' and 'Start' buttons. The background of the website shows various news headlines and a video player.

Get FREE access to Videos

 Fox News is Now in HD Watch uninterrupted live coverage of news and latest videos on your pc. [Download](#) & install the utility  News HQ here

Get free access to this site with FREEzeFrog.

How does it work?

The FREEzeFrog offer engine provides you FREE and unlimited downloads of handy, popular software. Based on keywords from your browser, FREEzeFrog will show you labeled advertisements in a separate browser window or a temporary slider. [Click here for more details...](#)

Choose Installation Type

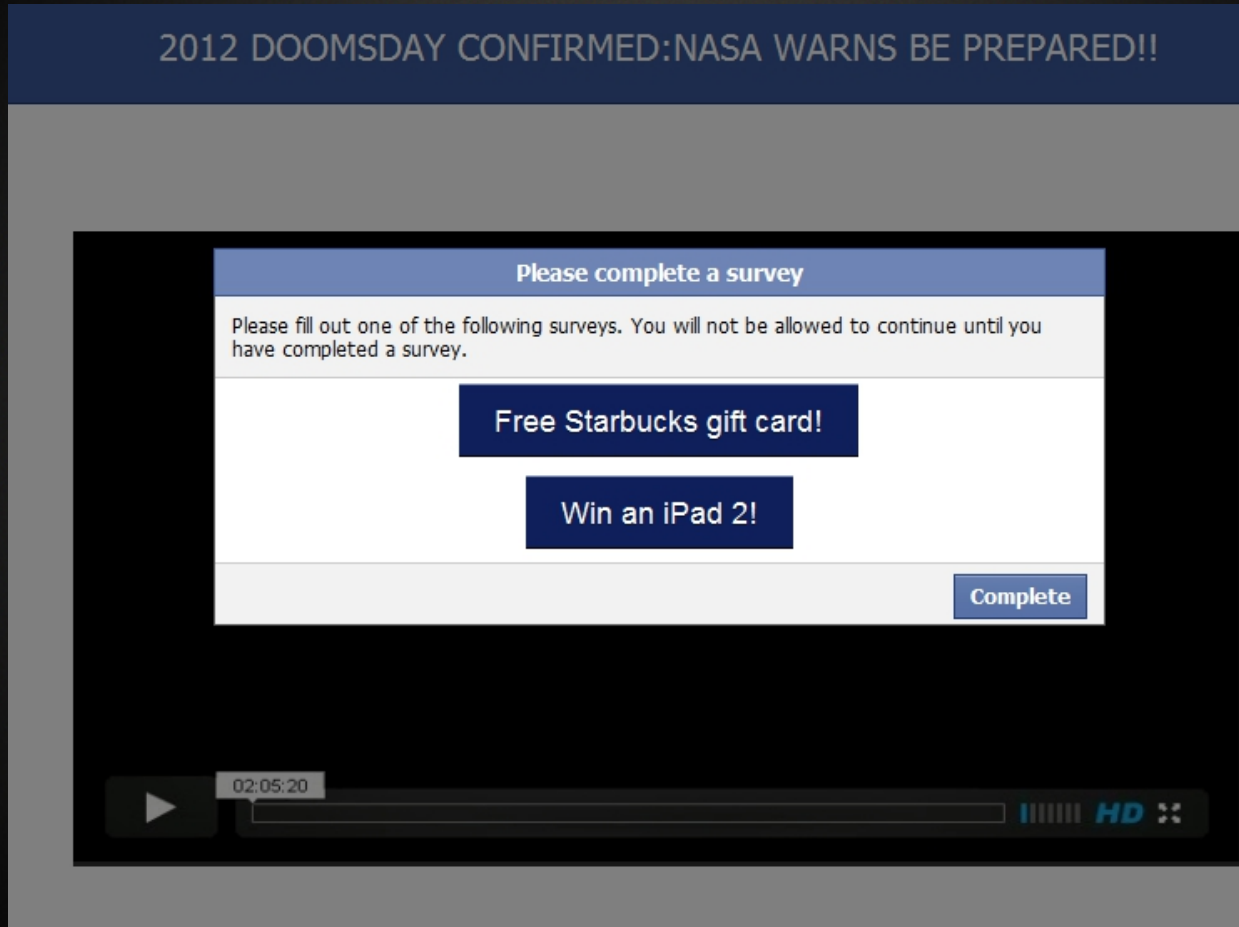
☒ **Express Installation (recommended)** [View EULAs and Privacy Policy](#)
Fast and Secure installation of FREEzeFrog, ShopperReports, QuestScan address bar search provider, blinkx Beat.

☐ **Custom Installation with FREEzeFrog** [View EULAs and Privacy Policy](#)

By clicking "Start", I represent that I (1) am at least 18, (2) agree to the [terms and conditions](#) and (3) to install selected programs.

Cancel **Click "Start" to install FREEzeFrog and access this website for free.** **Start**

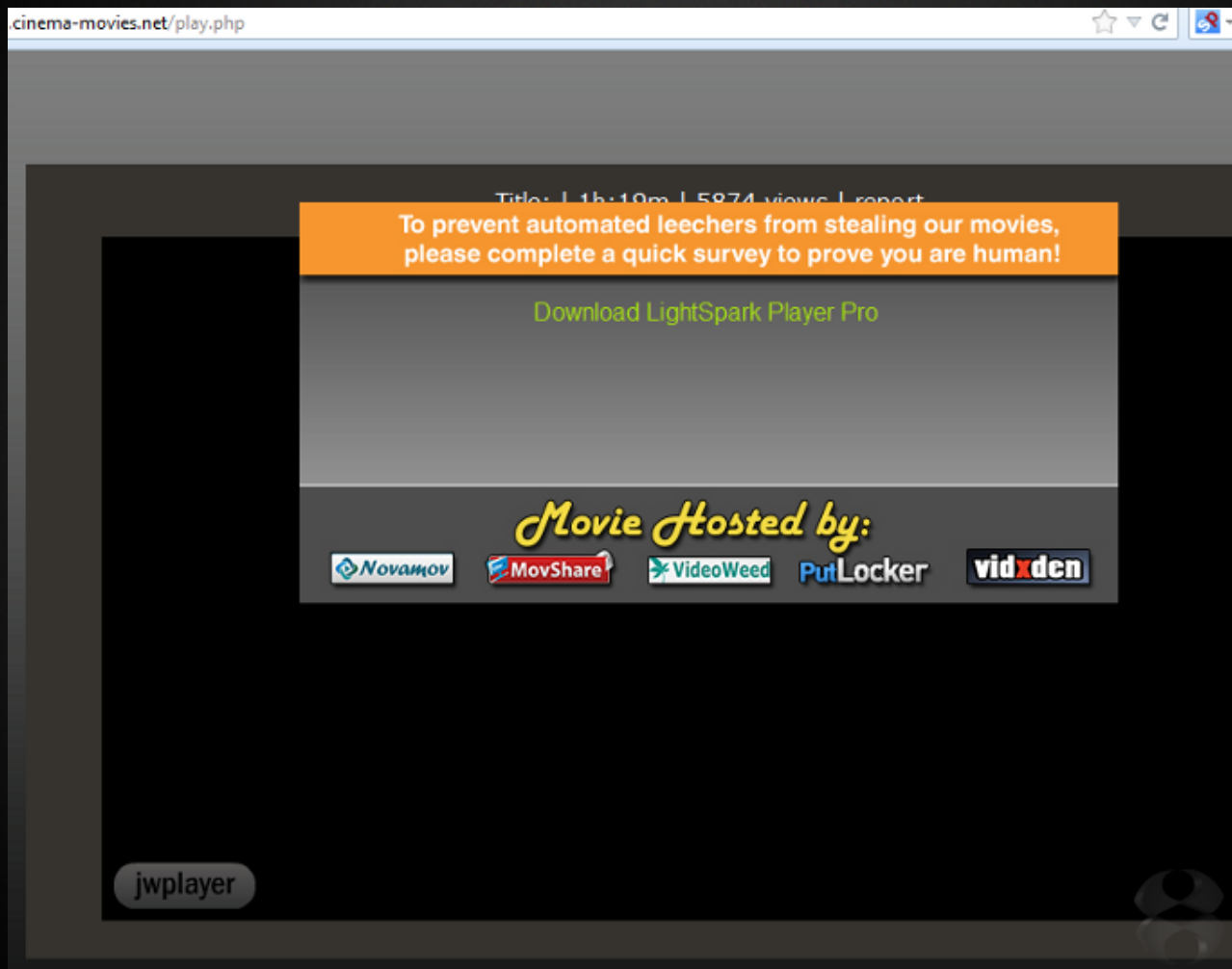
Surveys: (from '08 to) April 2012



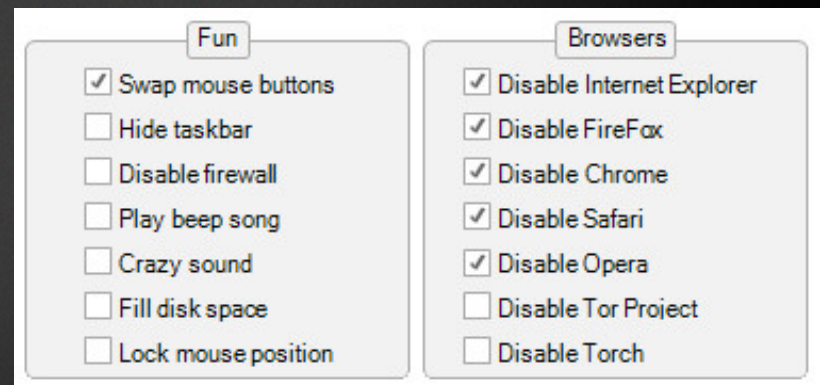
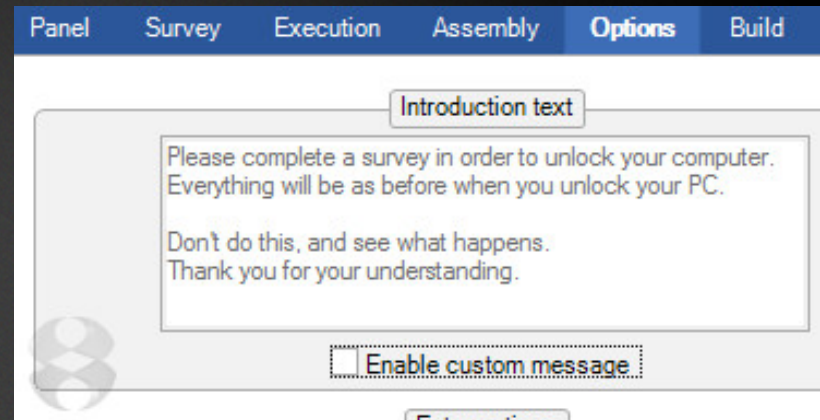
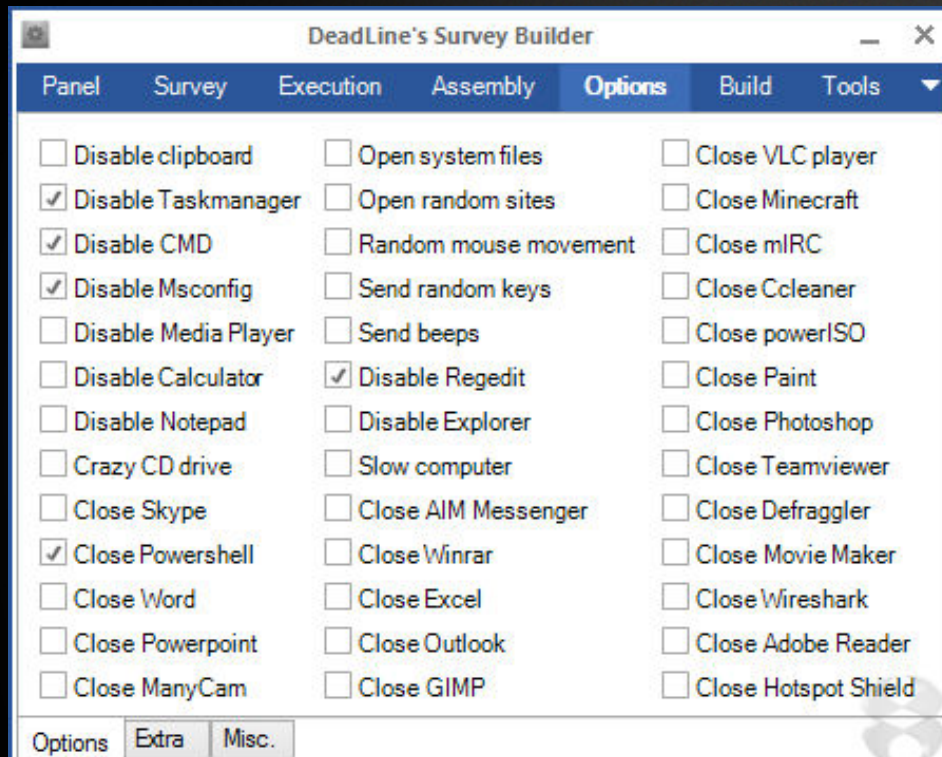
Ransomware Survey Lock - Dec 2012

















Survey Installers - May 2013



Survey DIY kit - July 2013



Bundles – 2005 to 2008

 keyboard25.exe	32 KB	Application	6/12/2006 3:23 AM
 defender23a.exe	36 KB	Application	6/12/2006 3:23 AM
 drsmartload849a.exe	28 KB	Application	6/12/2006 3:23 AM
 newname25.exe	56 KB	Application	6/12/2006 3:23 AM
 Trelew.exe	303 KB	Application	6/12/2006 3:23 AM
 MTE3NDI6ODoxNg.exe	25 KB	Application	6/12/2006 3:23 AM
 SS1001.exe	30 KB	Application	6/12/2006 3:24 AM
 stub_113_4_0_4_0.exe	15 KB	Application	6/12/2006 3:24 AM
 warebundle.exe	565 KB	Application	6/12/2006 3:24 AM
 WHCC2.exe	293 KB	Application	6/12/2006 3:24 AM
 mc-110-12-0000228.exe	29 KB	Application	6/12/2006 3:24 AM
 drsmartload45a.exe	28 KB	Application	6/12/2006 3:24 AM
 drsmartload46a.exe	28 KB	Application	6/12/2006 3:24 AM
 drsmartload1.exe	60 KB	Application	6/12/2006 3:27 AM

Bundles – Jan 2011



Bundles – June 2011

Open Office Installation

Welcome to the Open Office Setup Wizard

OpenOffice.org 3 is the leading open-source office software suite for word processing, spreadsheets, presentations, graphics, databases and more. This distribution of Open Office is provided free of charge and is governed by the [General Public License v2.0](#). Its source code is available [here](#). Downloading this version of Open Office from FREEzeFrog's servers also requires installation of the FREEzeFrog software, described below, which is subject to the FREEzeFrog End User License Agreement (EULA).

This Distribution is sponsored by FREEzeFrog **FREEzeFrog**

The FREEzeFrog offer engine provides you FREE and unlimited downloads of handy, popular software. Based on keywords from your browser, FREEzeFrog will show you labeled advertisements in a separate browser window or a temporary slider.

[View FREEzeFrog EULA](#) [Privacy Policy](#)

☒ Yes, I want free ShopperReports too [View TOU](#)


☒ Make QuestScan your address bar search provider [View EULA](#)

☒ Install blinkx Beat ☒ Make blinkx Beat my screensaver [View EULA](#)

By clicking "Next", I represent that I (1) am at least 18, (2) agree to the Open Office Privacy Policy and the FREEzeFrog EULA and Privacy Policy terms and (3) consent to install Open Office, FREEzeFrog, if selected ShopperReports, QuestScan address bar search provider, blinkx Beat.

Cancel

Next »



INFECTION CHANNELS

Social Networks – May 2006

Find Your Old School [Here](#):


[Your High School](#)


Jefferson High School


Ridgemont High School



From:  `MySpaceLife`

Date: May 15, 2006 6:25 PM

Subject: Cool New MySpace Feature - check it out!

Body:

CHANGE YOUR DISPLAY NAME COLOR NOW!

 *Be one of the first people to have it! Change your display name to color or image!*

Your display name will show in color on bulletins, messages, friend requests and on your page!

Get rid of the boring blue display name on a bulletin - Change your color today!

This is not a hoax! It really works and is a new cool thing to do on MySpace.

My Bulletin Space		
From	Date	Bulletin
Mia	May 13 11:32 AM	hey
Jake	May 13 11:30 AM	get your name in color!
♥LoSiNg muH iNhiBiTiOnS♥	May 13 11:03 AM	IMPORTANT BROOKS AND DUNN CONCERT TODAY!!! READ!!!
!fgt	May 13 10:16 AM	r e a d.

Social Networks – July 2006

The screenshot shows a MySpace profile page from July 2006. The browser's address bar displays "UK.Myspace.com". The page header includes navigation links: "Home", "The Web", "MySpace", a search bar, and "International | Help | SignOut". A banner at the top features a gorilla and the text "so his bile can be drained twice".

The main content area displays a Zango advertisement. The ad text reads: "Friends play a hilarious practical ioke. This content is FREE thanks to Zango." It describes the Zango Search Assistant and Zango Toolbar. A "Play Now" button is visible. Below the ad, a section titled "View My: Pics | Videos" is partially visible.

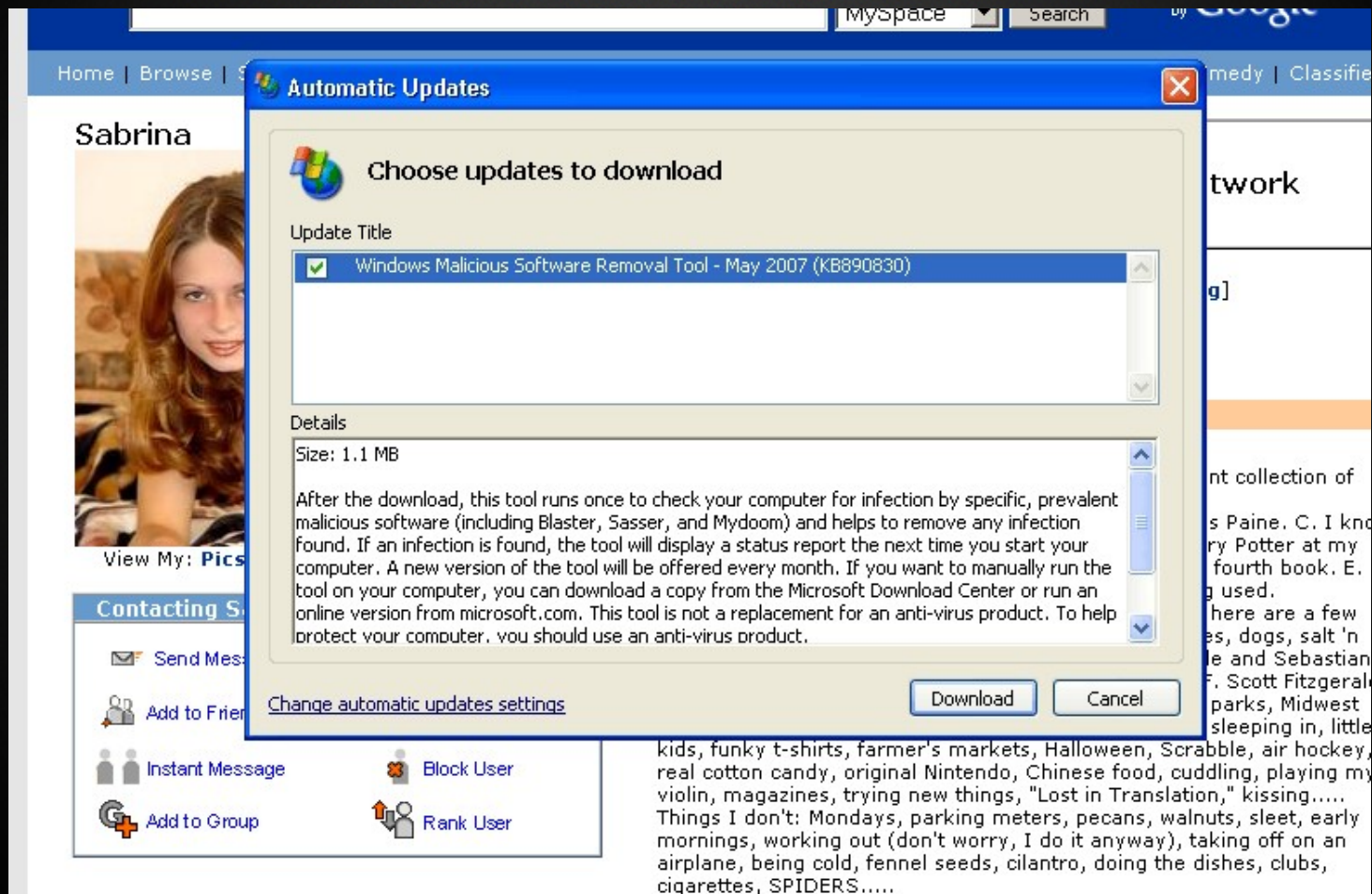
An "End User License Agreement (EULA)" pop-up window is overlaid on the advertisement. The window title is "End User License Agreement (EULA)" with a subtitle "(Last Revised April 19, 2006)". The text inside the window states: "NOTICE TO USER: THIS END USER LICENSE AGREEMENT ('AGREEMENT') APPLIES WITH RESPECT TO SOFTWARE APPLICATIONS PROVIDED BY 180SOLUTIONS, INC. AND ITS". A checkbox is checked, with the text: "By clicking 'Play Now', I am at least 18 and I agree to the terms of the License Agreement above." The window has "Play" and "Cancel" buttons at the bottom.

On the left side of the page, there is a "Contacting Zango" section with links: "Send Message", "Add to Friends", "Instant Message", and "Add to Group". Below this is a "MySpace URL:" field containing "http://www.myspace.com/zangocash". At the bottom, a "Zango's Details" section shows "Status: Single".

Social Networks: Fake Codecs Nov 06



Fake AV on Social Networks – June 07



Profile Stalkers – Jan to May 2007

The screenshot shows a Windows XP desktop with two windows. The top window is WordPad, editing a file named 'license.rtf'. It contains two paragraphs of text. The bottom window is File Explorer, showing the directory 'C:\Program Files\ProfileWatcher'. It lists several files, including 'pj.exe'. An error dialog box titled 'Error Deleting File or Folder' is open, displaying the message: 'Cannot delete pj: Access is denied. Make sure the disk is not full or write-protected and that the file is not currently in use.' A red rectangle highlights a paragraph in the WordPad document.

4.2 ZeroPoint may from time to time present programming fixes, updates and upgrades to you, including version updates to the Software. You must accept such programming fixes, updates and upgrades, including version updates.

4.3 Recommendation Engine. You understand, accept, and agree that as a condition of installing the Software at no cost, you possess the express desire and intent to communicate with others about the Software and other products and services offered by ZeroPoint and/or its assignees, now or in the future. As a convenience to fulfill said desire and intent, you hereby authorize the Software to automatically send messages, bulletins, comments, create groups, and carry out any other types of actions and/or communications on your behalf and through any accounts you may hold at various online social networking sites without further notification to you. You understand and agree that these communications may appear to have been written by you, and for legal purposes are being sent by you. You understand that you may opt out of your use of the recommendation engine at any time by deleting the file "pj.exe" from the directory to which you installed the Software, and that deleting this file will not have any adverse effects on the operation of the Software.

Error Deleting File or Folder

Cannot delete pj: Access is denied.

Make sure the disk is not full or write-protected and that the file is not currently in use.

OK

Name	Size	Type	Date Created
cool.dat	10 KB	DAT File	1/2/2007
license.rtf	26 KB	Rich Text Document	3/25/2007
pj.exe	598 KB	Application	4/26/2007
profilewatch.exe	1,599 KB	Application	5/16/2007
unins000.dat	2 KB	DAT File	5/16/2007
unins000.exe	663 KB	Application	5/16/2007

Date Created: 5/16/2007 8:51 AM Size: 598 KB

Profile Stalkers – Nov 2006

http://musicvideocodes.powered-by.zango.com/?a074a075/ga275a9&s=http%3A//www.musicvideocodes.info/clip_11_Ronaldinho_Soccer_Tricks.htm

Profile Tracker Friends Generator Profile Editor Profile Layouts Music Codes Profile Tools

MUSIC VIDEO CODES.info

Without lime... There would be nothing.

Music Video Codes Movie Trailer Codes Short Clip Codes Your PlayList Request Codes Help with Codes

MUSIC VIDEO CODES

UPDATED DAILY

ADD MUSIC VIDEOS TO YOUR WEBSITE FOR FREE

MORE ABOUT ZANGO



James Blunt
Sean Paul Black Eye Peas
FREE Music Videos
Notorious B.I.G Jack Johnson

Powered by **zan**

The content on this website is FREE, thanks to Zango. Why? Because it's paid for by advertising.

The following is included in the Zango installation:

Zango Search Assistant (Zango SA) provides free access to this website and all Zango-supported content across the Internet and, in exchange, may display to you several ads per day based upon keywords from your Internet browsing. These ads will pop up on your computer screen in a separate browser window. [Learn more about Zango SA.](#)



Profile Stalkers – April 2012

The screenshot shows a web browser window displaying a Facebook profile viewer. At the top, a user's profile picture is visible next to the text "and 6 other people are Currently Watching Your Profile". Below this is a blue header with the text "facebook profile viewer" and a magnifying glass icon. A central overlay box titled "Verify your account" contains the message: "This is a private content. To verify your identity, please complete one of these fun offers below:". Inside the box, there is a link "Your Chance to Win an Iphone 4!". Below the link, there are two options: "Restricted access" (with a red minus icon) and "Secured content" (with a lock icon). A green checkmark icon and the text "This is your current setting." are also present. To the right of the overlay, there is a notification bell icon with a red "1" and the text "Account notification". Below the overlay, a list of stalkers is visible, each with a profile picture, a name, and a "Click To See" button. The list includes entries for "Viewed your profile 26 times in the last 7 days", "Viewed your profile 25 times in the last 7 days", and "Viewed your profile 23 times in the last 7 days".

and 6 other people are Currently Watching Your Profile

facebook profile viewer

Verify your account Account notification

This is a private content. To verify your identity, please complete one of these fun offers below:

[Your Chance to Win an Iphone 4!](#)

Restricted access This is your current setting.

Secured content

Viewed your profile 26 times in the last 7 days **Click To See**

Viewed your profile 25 times in the last 7 days **Click To See**

Viewed your profile 23 times in the last 7 days **Click To See**







Profile Stalkers – October 2012

Your Tumblr Stalkers Have Been Found!...

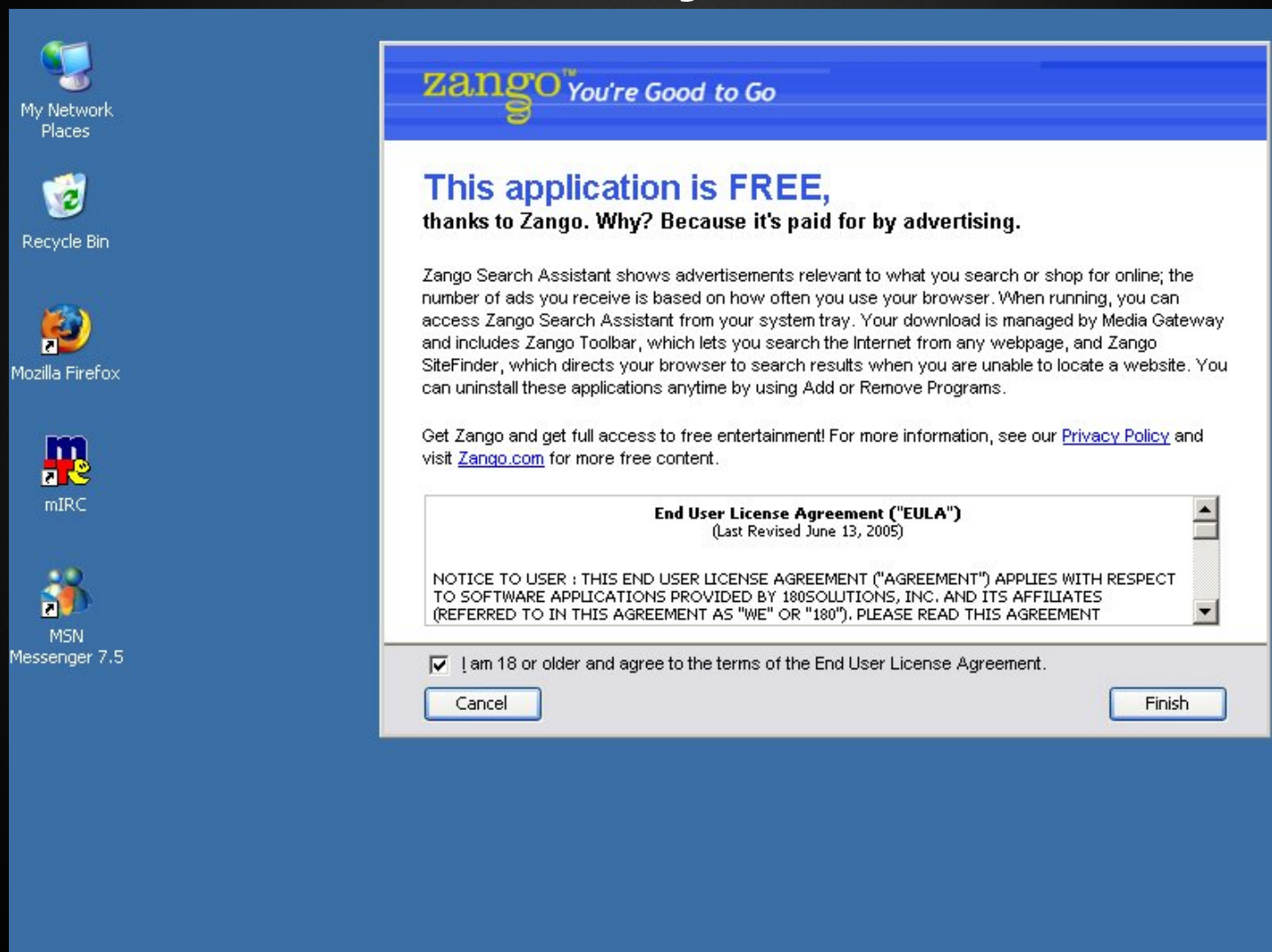
Now just verify you are human and not a spam-bot.



To verify you are HUMAN and not a SPAM-BOT
Please complete a free, 30 second survey below.

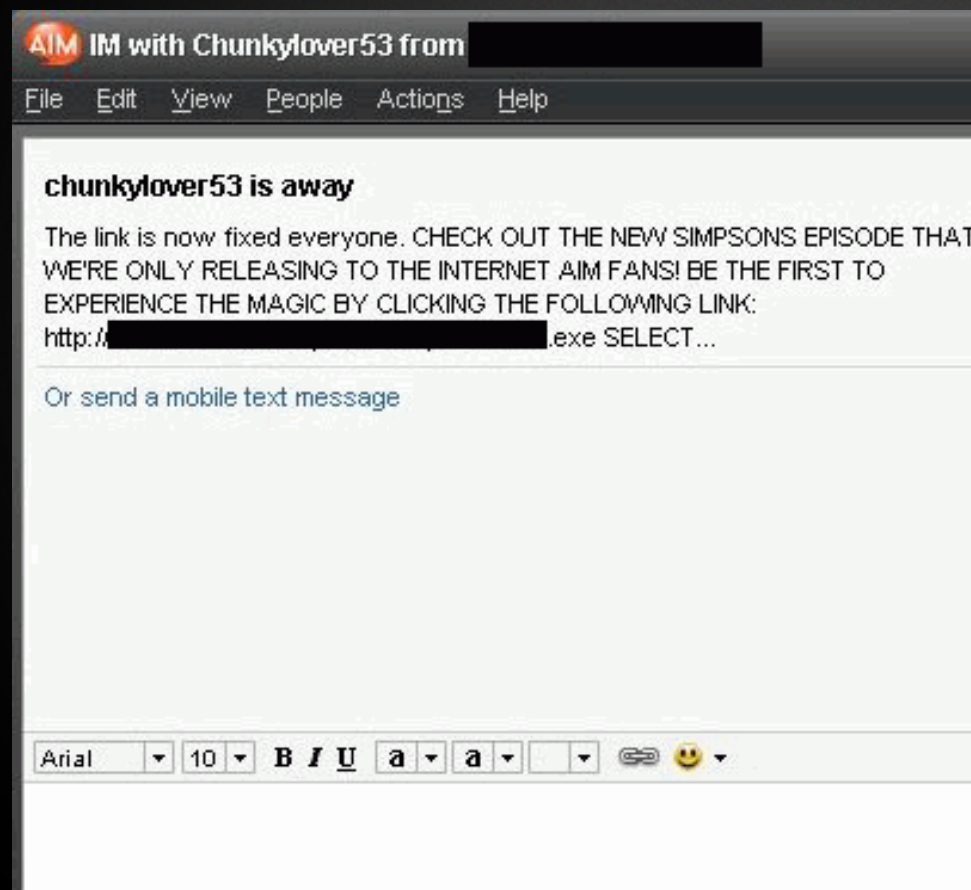
-  WIN \$50,000 Dollars! Enter Today!
-  Get Amazing Emoticons and Smileys!
-  Learn How To Save Money On Gas!
-  Get Remote PC Access Anywhere!
-  Get A Subscription To Biz Mag!
-  Get Rewards Towards Shell Fuel!

Botnet Installs – May 2006



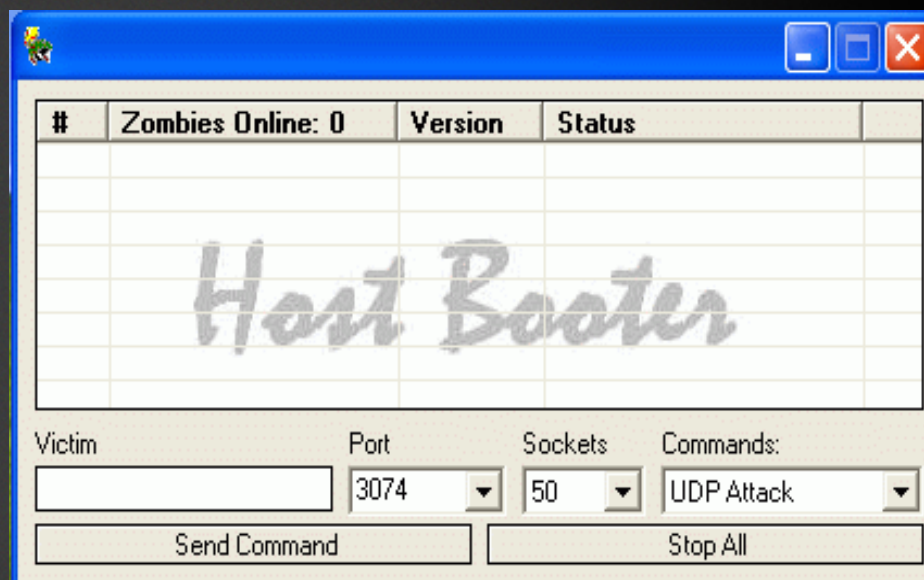
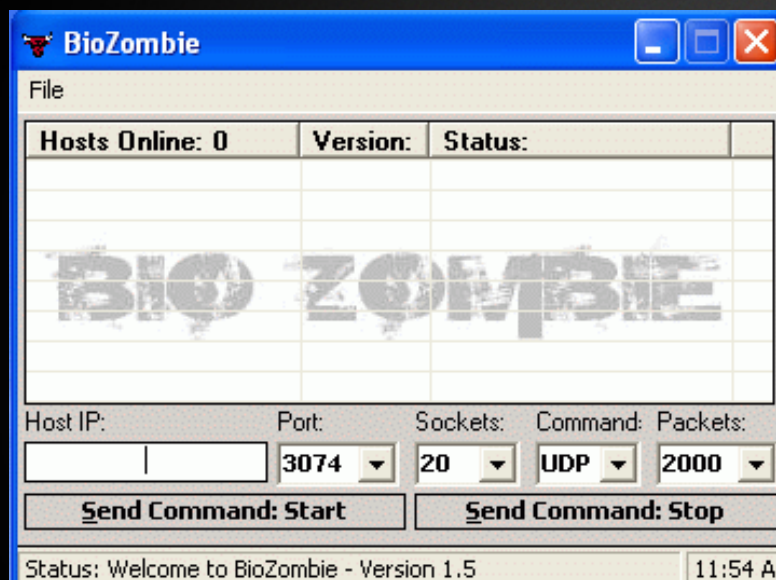
Botnet Installs – July 2008

Stream Content
amsMINFOMINFO | kimya_bots | | | WinXP | ENU

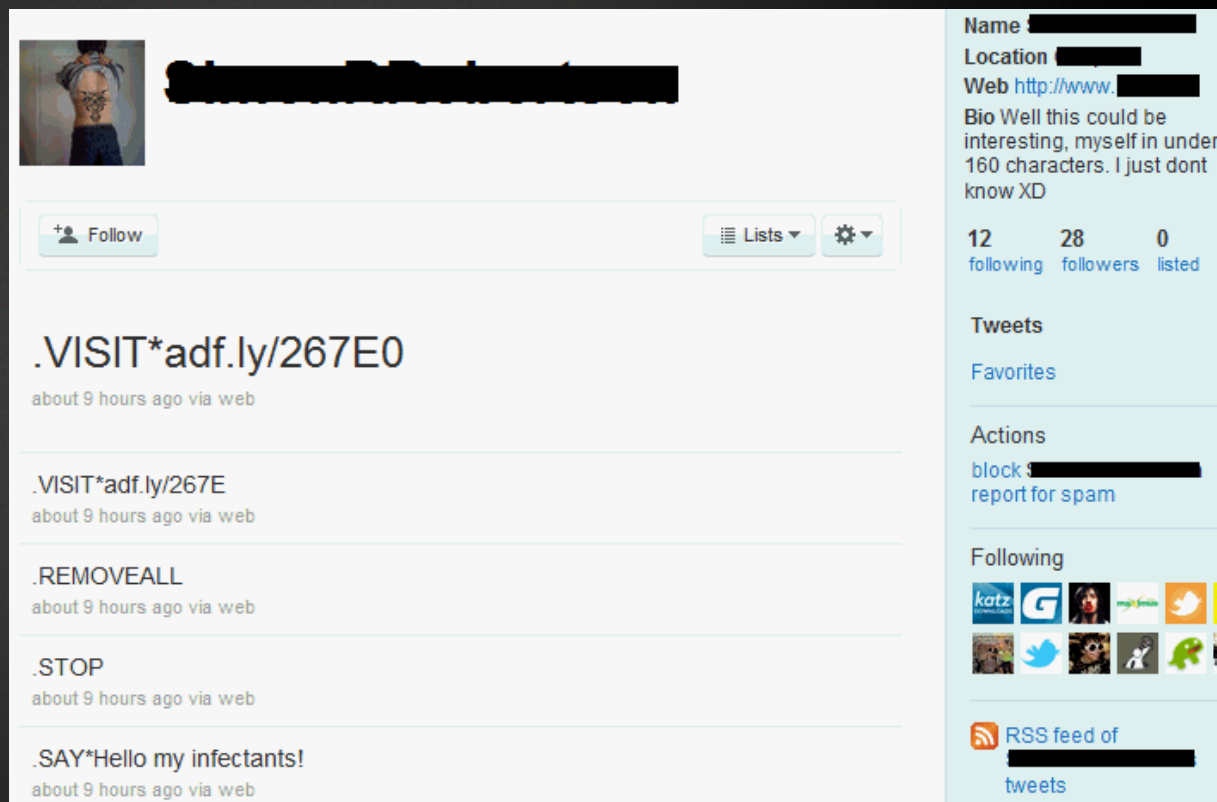
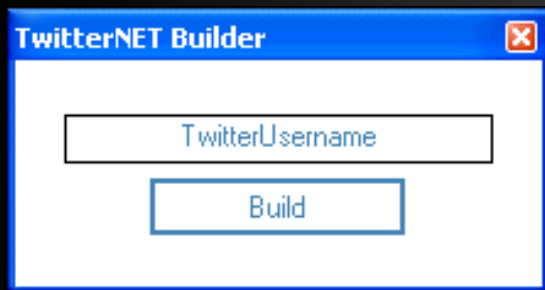


ExitProcess
capCreateCaptureWindowA
acmStreamSize
SysFreeString
ShellExecuteA
waveInOpen
DENEME
DVCLAL
PACKAGEINFO
ROOTKIT
MAINICON

Botnet Installs – February 2009



Botnet Installs – May 2010



Ad Networks and Affiliates

The screenshot displays a desktop environment with several overlapping windows, illustrating the presence of various advertisements and security warnings:

- Microsoft Internet Explorer:** The top window shows the URL `http://txt2d8.com/txtme/`. The page features a large image of a woman and a mobile phone with the text "WAN2TLK? U R QT". To the right, there is a section titled "MOBILE SMS DATING - FIRST MATCH FREE" with a form for "Mobile No", "Postcode", "I am a" (set to "Man"), and "Looking for a" (set to "Woman").
- Mozilla Firefox:** The middle window shows the URL `http://www.broadcast-ing.com/tau.html`. It displays a security warning from Zango, stating: "Thank you for installing Zango search tools! Now you also have unlimited access to free entertainment at Zango.com. Have questions? Visit Zango customer support." Below this, there is a section titled "Your system needs to DOWNLOAD one of these security software programs to prevent malware infections". It mentions the "Backtera Virus" and states: "Attention! Security Center has detected potential security vulnerabilities on your PC that may send private information documents to a remote computer. One of the processes (Win32res.exe) has just sent this information:". There are fields for "IP address:" and "Browser:". A "Close" button is visible.
- Command Desktop Advertising:** A small window at the bottom right contains a public service announcement: "This public service announcement is brought to you by Command desktop advertising. Future advertisements will not display the Command logo and are not endorsed or delivered by the sites that you visit. Command can be automatically removed at any time through your control panel." The Command logo is visible in the bottom right corner.
- Other Elements:** A "Messenger 7.5" status bar is visible at the bottom left. A "This Ad is from Zango" message is partially visible on the left side of the Firefox window.

Ad Networks and Affiliates

Desktop is problematic for advertisers

- ◆ Proliferation of blockers: Adblock Plus, NoScript, Ghostery, FlashBlock, Disconnect
- ◆ Web filtering / online blacklists / AV tools / threat detection
- ◆ Large selection of infosec blogs / researchers / privacy groups
- ◆ Easier to litigate as clear and understandable precedent

Ads in Search Results: Sept 2011

Get Skype - Download for free - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Get Skype - Download for free

http://river-park.net/sf/

Google



Get Skype - Download for free

Make Skype part of your everyday life!

[Download Skype Now](#)

It's free and installs in seconds.
for Windows 2000/XP/Vista/7

Skype is Free

skype is free a software. Skype is released under the GNU General Public License.

On your computer

Install Skype, add your friends as contacts, then call, video call and instant message with them for free. Call people who arent on Skype

Opening skype_5.3.0.111.exe

You have chosen to open

 **skype_5.3.0.111.exe**
which is a: Binary File
from: http://skype.en-sofonic.net

Would you like to save this file?

[Save File](#) [Cancel](#)

comfort of your living room with a new Skype-ready high definition TV from LG, Panasonic or Samsung.

Features!

- Free video calling - Why just talk when you can see each other face-to-face?

More Features:

- **Voicemail.** Let Skype take a message.

Download it now!!!

- Free **skype** software
- **Skype Access.** Get online with public



Ads in Search Results: July 2013

These offers will be displayed depending on the user's location as well as the configuration of Internet Explorer, considered normal to display these offers. You also have the chance to reject all the offers at the start and during the process. Compatibility: Windows 2000/XP/Vista/7/8 and Mozilla Firefox, Google Chrome and Internet Explorer.

Delta Toolbar



The toolbar adds cool content to your browser. You can add your favorite emoticons & other cool stuff to various web mails & social networks. [Learn more](#) | [Uninstall instructions](#)

Iminent Toolbar



Free emoticons, animations and games for your browser. Personalize your homepage's background with Iminent SearchTheWeb. [Learn more](#) | [Uninstall instructions](#)

Whitesmoke Toolbar



Helps you to translate words from a language to another. It support multiple languages and also can pronounce the desired words. [Learn more](#) | [Uninstall instructions](#)

Addlyrics

With this application you will have the lyrics of your favorite artists' songs available. [Learn more](#) | [Uninstall instructions](#)

PCSpeedUp

Use this application to analyze and repair your PC. [Learn more](#) | [Uninstall instructions](#)

Coupondropdown

Receive the best offers for different products with this browser add-on. [Learn more](#) | [Uninstall instructions](#)

Boxore

Receive personalized recommendations for videos, games, music and more thanks to this application. [Learn more](#) | [Uninstall instructions](#)

Speedupmypc

With this application you will get a quick system scan and a detailed report of possible problems with your internet connection speed. [Learn more](#) | [Uninstall instructions](#)

Strongvault

Have you ever lost information from your PC and haven't had a backup? Thanks to this application you will have a backup of your PC. [Learn more](#) | [Uninstall instructions](#)

Dealcabby

Receive the best offers from your favorite online shopping sites. [Learn more](#) | [Uninstall instructions](#)

Infoatoms

Highlight any word or phrase and Wikipedia, Bing, and other results appear in page. [Learn more](#) | [Uninstall instructions](#)

Translatengenius

Learn a second language for free in minutes a day all by just surfing the web! [Learn more](#) | [Uninstall instructions](#)

Ads in the Mobile Ecosystem

Advantages of mobile / tablet

- ◆ Device owners not used to desktop ad tech in their phones
- ◆ EULAs range from difficult to impossible to read
- ◆ “Freemium” in return for ads similar to desktop “value proposition”
- ◆ Security tech / research playing catch-up to traditional approaches
- ◆ Porn advertising is allowed on many major networks

Key Ad Players in the Mobile Ecosystem

- ◆ **Airpush**

- 2nd largest mobile ad network
- Places ads on the toolbar of the Android device

- ◆ **LeadBolt**

- Displays ads over pages, can overwrite ads on pages
- Can collect lots of user data

Other Notable Ad Players

- ◆ Appenda
- ◆ Pontiflex
- ◆ Plankton / Counterclank / Apperhand
- ◆ Sellaring

Mobile Ads: Samples

The image displays four mobile app screenshots, each showing a different type of mobile advertisement. The first screenshot, titled 'Appenda Opt-out', shows an app listing with a description and a 'Description' section. The second screenshot, titled 'Big truck race', shows a 'Top Apps/Offer of the Day' section with three offers: '1. Ace Top Gunner. Play for Free', '2. Play Chimp Tac Toe', and '3. Get the Latest APPs for FREE Now!'. The third screenshot, titled 'Fast Points', shows an 'App permissions' dialog box with a list of permissions: 'Your messages', 'Phone calls', 'Network communication', and 'See all'. The fourth screenshot, titled 'Sponsored Offers From Pontiflex Deals', shows a list of sponsored offers from Priceline.com and RetailMeNot, including a 10% discount on hotel bookings and a newsletter subscription offer.

Appenda Opt-out
APPENDA
INSTALL
★ ★ ★ ★ ★ 36
1,000+ downloads
Dec 20, 2011
141KB
5 people +1'd this.
Description
You are receiving Appenda ads because you installed an app which uses Appenda. If you choose to not support the developer's use of Appenda ads, you can remove Appenda ads in three different ways as listed below.
1) Install this app to opt-out, which can be immediately uninstalled once your opt-out is complete.

Big truck race
Top Apps/Offer of the Day
Choose one of these great offers now!
1. Ace Top Gunner. Play for Free
Download the app now
2. Play Chimp Tac Toe
Download now
3. Get the Latest APPs for FREE Now!
Tap to Download
Ads by LeadBolt

Fast Points
App permissions
Fast Points needs access to:
Your messages
Receive SMS
Phone calls
Read phone status and ID
Network communication
Full Internet access
See all
ACCEPT
Description
Earn points shopping for music, games, flowers

Sponsored Offers From Pontiflex Deals
Sign up today and save!
Save 10% off your next hotel booking with Priceline.com
Looking for a better way to save?
Subscribe to the RetailMeNot newsletter! The best deals from your favorite stores straight to your inbox. Sign up today!
?? ????!
No Thanks Sign Up
Privacy Center

(l-r) Appenda Opt-Out, Big Truck, Fast Points, Pontiflex

Mobile Rogues – May 2013

Use the app on your phone to recognize the QR code and download the QIP_mobile.apk



Mobile Rogues – May 2013

INTERNET: For Sending and receiving data from the C&C.

SEND_SMS: Sends hidden Premium text messages. The number and the amount are controlled by the C&C.

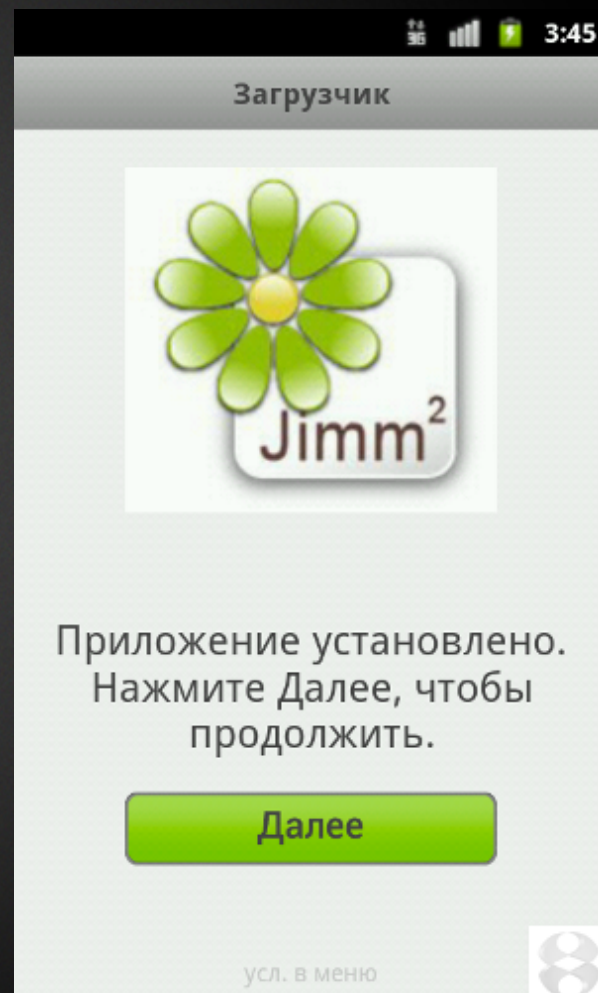
RECEIVE_SMS: Can receive commands through SMS as well as the C&C.

INSTALL_SHORTCUT and CREATE_SHORTCUT: Installs shortcuts to itself and websites.

CALL_PHONE: This permission would grant the app the ability to send phone calls without the users knowledge

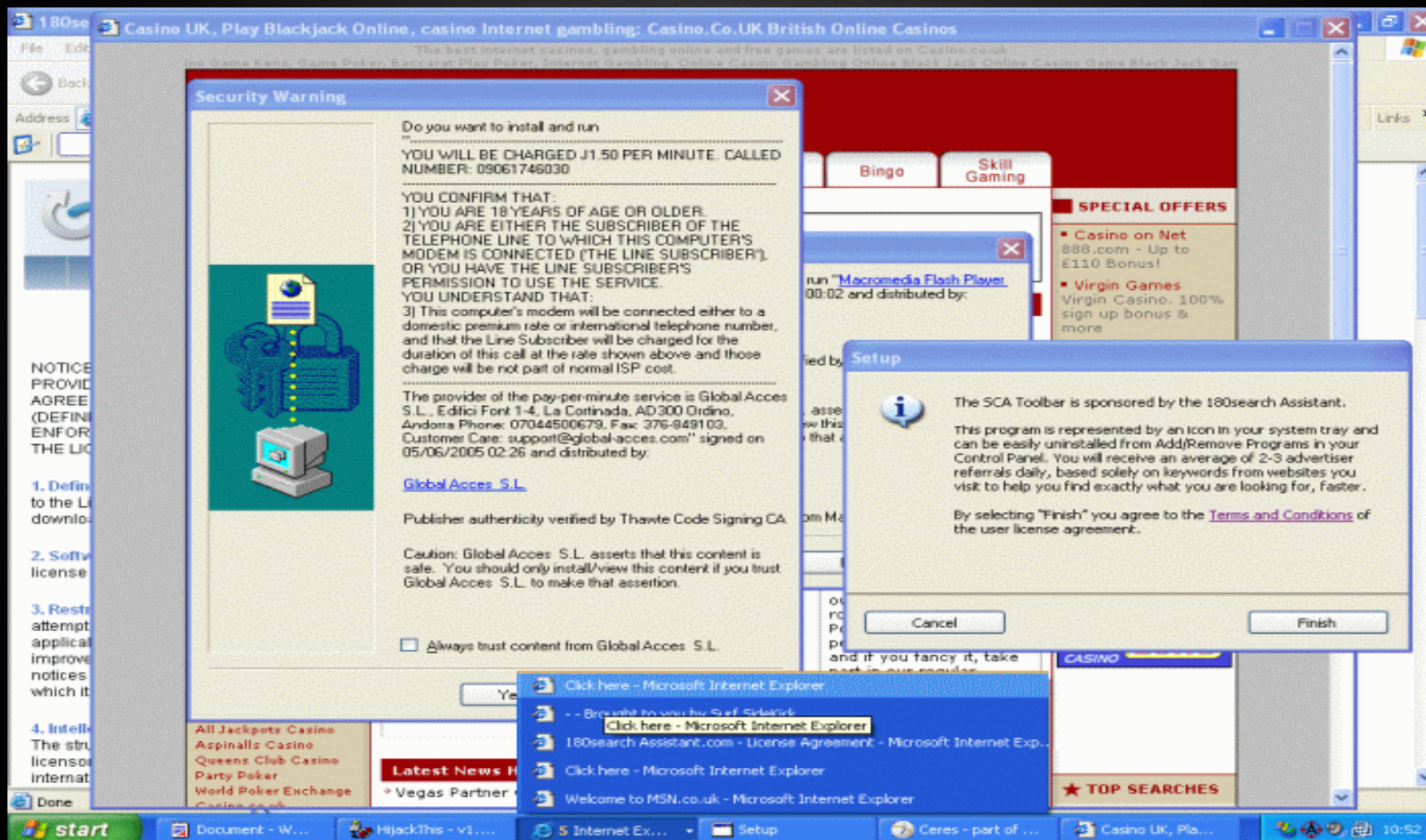
BOOT_COMPLETED: Turns on upon Restart.

QUICKBOOT_POWERON: Turns on before other apps.



TRICKY TECH

Typical Install – July 05



“At Least we’re not Ebola”

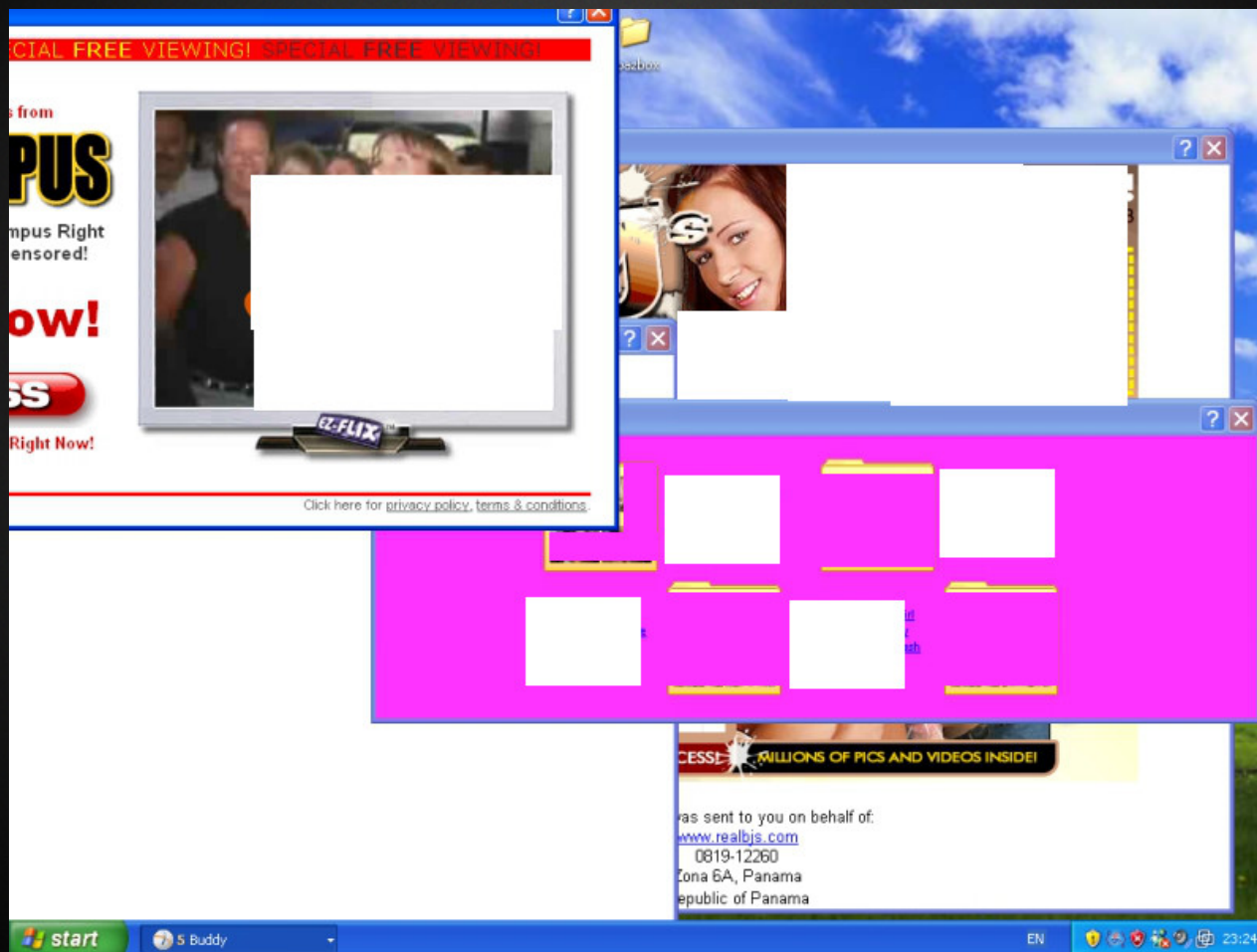
An actual Department of the Dark Arts

- ◆ A division of Direct Revenue
- ◆ “This has nothing to do with us” disclaimers
- ◆ Death threat comment watch (Document 5)

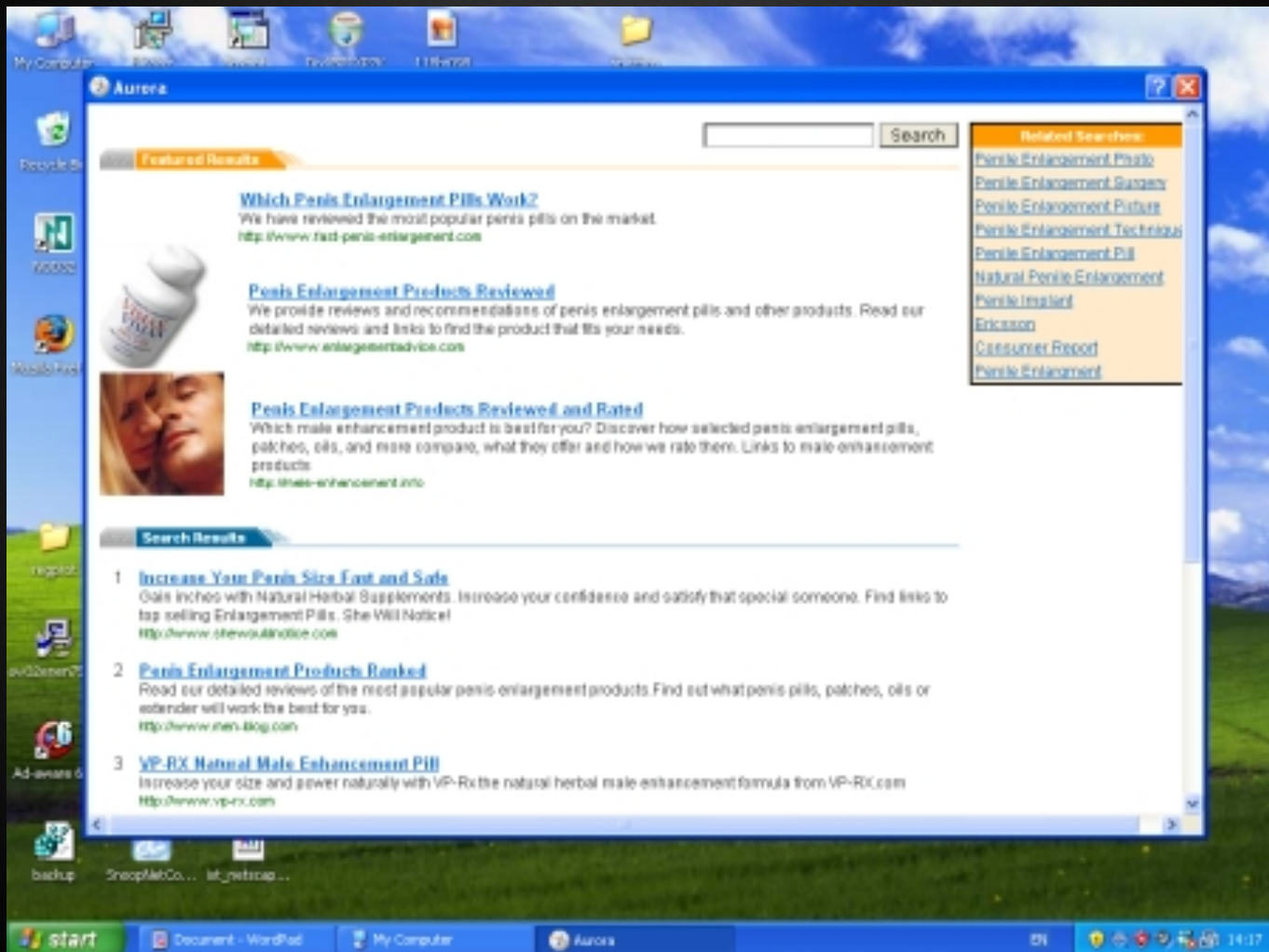
Living in Interesting Times

- ◆ “...perhaps a letter to his true home address showing that we know more about him will have results...”
- ◆ “..we are very interested in learning from your experience in dodging SP2 and Antivirus programs”
- ◆ “Very stealthy version...if we do a deal, we will not be caught”
- ◆ “It’s not spyware, it’s advertising software (teethy grin)”

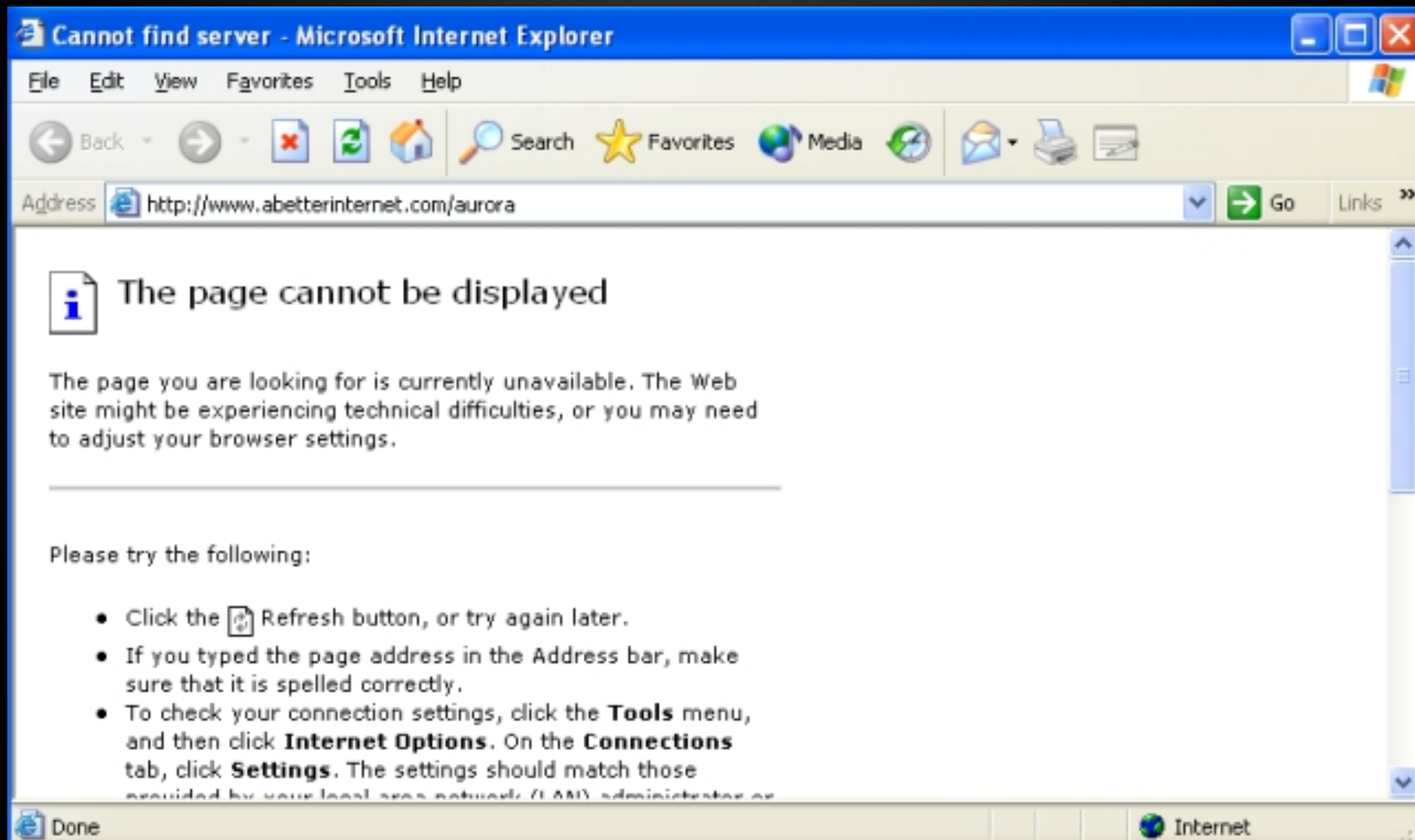
Aurora infected PC left for 5 minutes



Aurora – May 05



Dark Arts and Death Threats



The Adware Collapse Fallout

Security Researchers

- ◆ Burn Out: Taking a Toll
- ◆ Narrowing of focus and lack of content
- ◆ Skillset adjustment: more anonymity = less accountability - moneytrail

Adware Vendors

- ◆ Tech rolled up into other entities and industries
- ◆ Return to spender: reformation
- ◆ Platform creep

DID WE WIN?



ThreatTrackTM Security

Thank you for listening!