

# ***Web Browsers: A History of Rogues***

*Chris Boyd, Senior Threat Researcher – GFI Software*

## *2006/07: Interesting Times*

Adware industry VS the FTC, NYAG, rest of the World

Slowly moving away from desktop fireworks

Rogue browsers: an attempt at stealth

Many tactics shared by Fake AV groups

## February 2006: RedBrowser

Downloaded from the net or via bluetooth

Claims to send free SMS

Sends SMS in an infinite loop

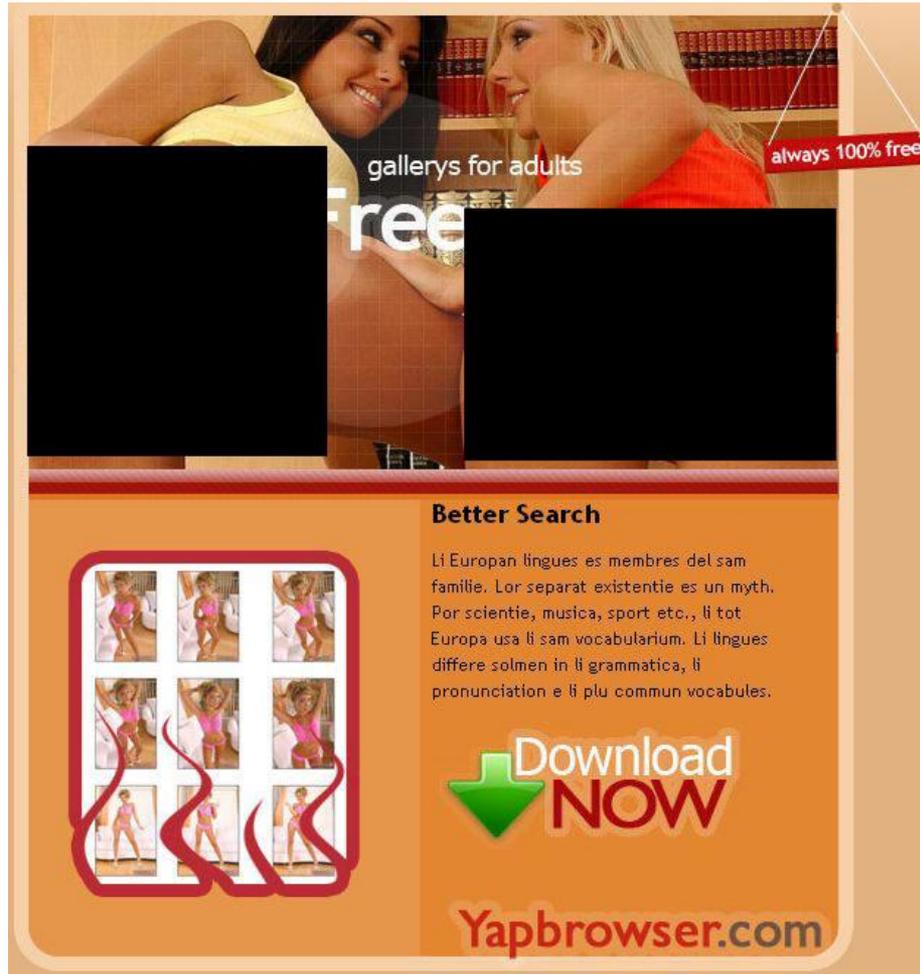
Phone owner charged for each message



# April 2006: YapBrowser

The advertisement features a blue background. At the top left is a large green checkmark icon. To its right, the word "Yap" is written in a large white font, with "browser.com" in a smaller yellow font. Below this, two links are visible: "Download yapbrowser" and "Adult ersion". The central part of the ad is split into two panels. The left panel shows three ice cubes melting on a reflective surface. The right panel shows a white clock face with black numbers and hands, with a red "free" sticker on it. At the bottom, the slogan "Don't Waste your time" is written in a large, light blue font.

## April 2006: YapBrowser



galleries for adults  
free

always 100% free

### Better Search

Li European lingues es membres del sam familie. Lor separat existentie es un myth. Por scientie, musica, sport etc., li tot Europa usa li sam vocabularium. Li lingues differe solmen in li grammatica, li prononciation e li plu commun vocabules.

Download  
NOW

Yapbrowser.com

## April 2006: YapBrowser



**YapBrowser is a browser** which will make searching for any information online much simpler. Download YapBrowser for free and forget about getting to sites containing harmful exploits. Your computer will be free from viruses breeding online. Attention! You can download a 100% free [adult version of YapBrowser](#). There is a 100% guarantee no system infection will occur when using our software. YapBrowser is the only browser which gives you safe search and browsing capabilities. Now you can download free!

# April 2006: YapBrowser

## FAQ

### What is PPC and how does the YapSearch.com affiliate program work?

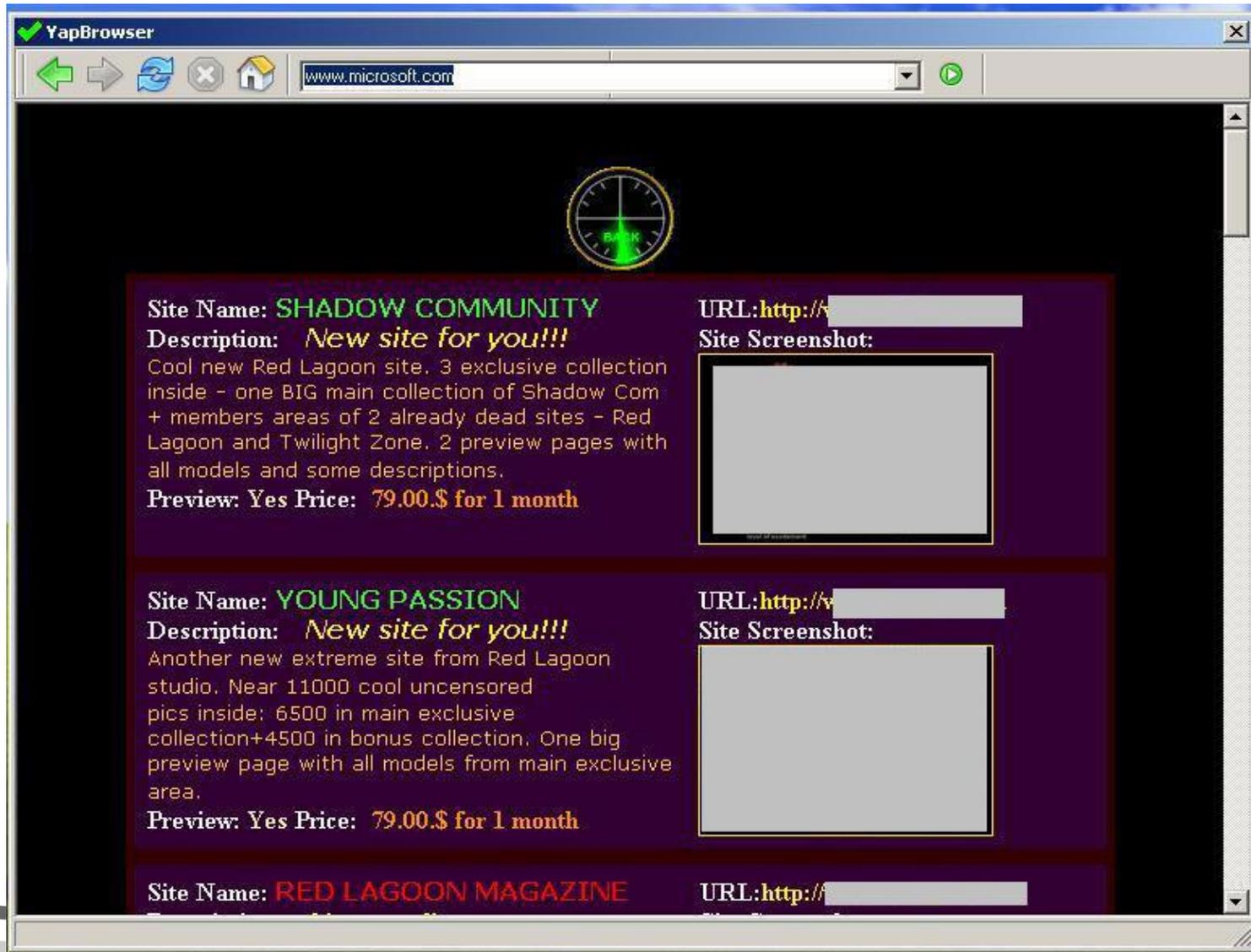
Pay-Per-Click search engine means that every search result has money value, and results appear according to the bid value set by corresponding advertisers. We pay you, our partner, a 70% share from the bid price. You also receive 20% of the earnings of your referrals. This simple and powerful scheme is guaranteed to provide regular and increasing incomes for our webmasters!

### What is needed to join the YapSearch.com affiliate program? Do I have to pay anything?

Joining with YapSearch.com is absolutely free, you just have to own a working email address. Please read our Terms before joining with us!

[home](#)[SignUp](#)[About](#)[FAQ](#)[Terms](#)[Contact Us](#)[Webmaster Login](#)Username: Password:

# April 2006: YapBrowser



# April 2006: YapBrowser

[Larges Lolitas Photos and Video Archive LOLITA THUMBNAIL GALLERY ...](#)

Real Lola

21k - [Cached](#) - [Similar pages](#)

[Pass Board Teen Preteen lolitas](#)

members : [http://](#)

- 20k - 24 Apr 2007 - [Cached](#) - [Similar pages](#)

[LOLITAS BBS](#)

20k - 24 Apr 2007 - [Cached](#) - [Similar pages](#)

[LOLITAS BBS](#)

- 20k - 24 Apr 2007 - [Cached](#) - [Similar pages](#)

*In response to a legal request submitted to Google, we have removed 9 result(s) from this page. If you wish, you may [read more about the request at ChillingEffects.org](#).*

## April 2006: YapBrowser

# Don't Waste your time



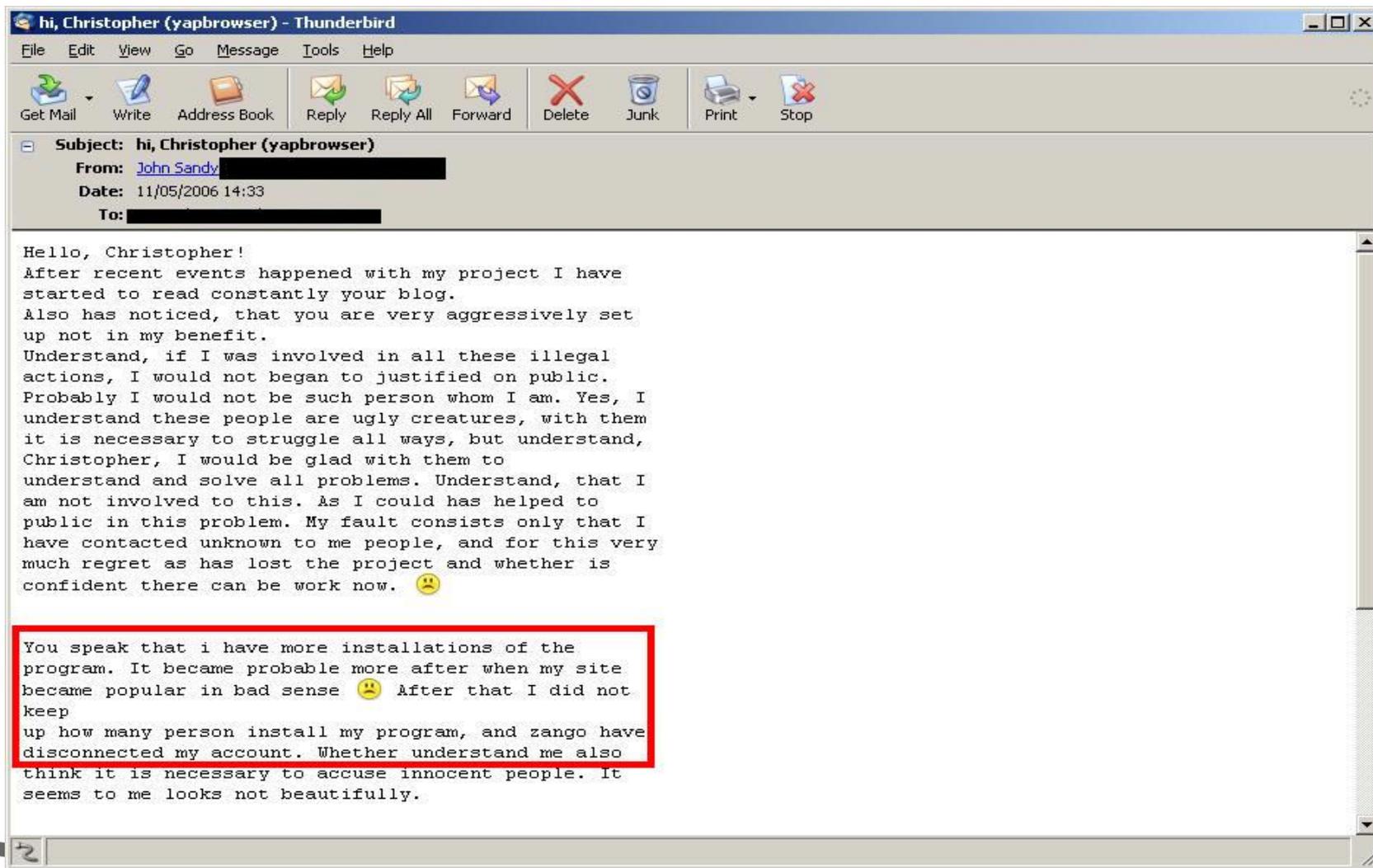
**Hello dear visitors! Recently there were events which have spoiled reputation of our site and our program not on our fault.**

**Some links of our browser direct on 404 page on which our hosting provider promoted an illegal content. At present time we solve the given situation and we apologize before all victims. Including our partners which sponsored to us installation of a browser, have suffered most of all. Separate apology to them. We promise that will not repeat such thing.**

**Download NOW**

apcash.com contact: support@yapbrowser.com

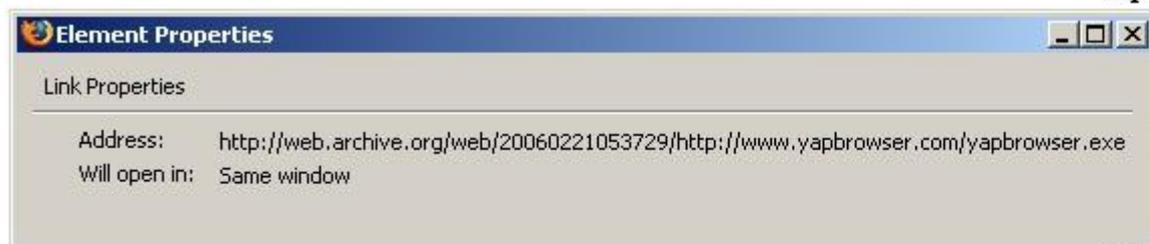
# April 2006: YapBrowser



# April 2006: YapBrowser

2006
3 pages
<a href="#">Feb 21, 2006</a> *
<a href="#">Apr 23, 2006</a> *
<a href="#">Apr 23, 2006</a>

[Download yapbrowser](#) [Adult ersion](#)



**YapBrowser is a browser** which will make finding for any information online much easier. Download YapBrowser for free and without any risk about getting to sites containing harmful contents. Your computer will be free from viruses and malware. You can download a free [adult version](#) of YapBrowser. Using it you will be able to search for and browse adult content for free. There is a 100% guarantee no system infection will occur when using our software. YapBrowser is the only browser which gives you safe search and browsing capabilities. Now you can download it for no cost at all.

©2006 Klass Media. Design by Artelectrons

## April 2006: YapBrowser

5 - при вводе адреса в address bar и нажатии enter юзер попадает на [урл]

**5 – When user types web address and presses enter he will be redirected to certain URL**

6 - при вводе адреса в address bar и нажатии enter проверяется наличие кейвордов (опционально) - если один из кейвордов найден, то вместо введенного адреса показывается [урл]

**6 – When user types the web address and presses enter then application checks if there are keywords in user’s input (optional) and if so then the browser shows some URL instead of the original web address**

бй способ - допустим надо фильтровать только по teen В кейвордах указываем **\*\*teen,young\*\***

Если юзер ввел <website removed> то он попадет на maturepics.com Если он ввел <website removed> или <website removed> то он попадет на твой урл»

(PS такой консольный софт уже есть. Его только лишь надо немного доработать-улучшить)

**6 – Example: say we want to filter all users’ input by a keyword “teen”. In this case the keyword list would contain words “\*\*teen,young\*\*”. If user typed maturepics.com then he’ll be directed to maturepics.com. However if he entered the exact full domain name then he will be redirected to that URL that we need.**

## April 2006: YapBrowser

б) Замена 404 , home page/ search page и Локальный фид.

Замена будет происходить на локальную html страницу (локальный фид) Первоначально он будет загружена на комп юзера в нескольких вариантах дизайнов. Допустим 5 видов. Дизайны будут такого плана как тут [www.yapsearch\(dot\)com](http://www.yapsearch(dot)com)

Локальный фид нужен для того что бы не грузить лишний раз комп юзера. Т.е. допустим если бы мы ставили на home page какой-то урл, то при каждом открытии браузера грузился бы какой-то сайт, а это очень напрягает юзера. Намного удобнее если грузится локальная страничка. А на этой странице просто будет список кейвордов, со ссылками на PPC.

Естественно при желании наш адверт может попросить заменять домашнюю страничку на нужный ему сайт. Следовательно локальный фид уже не будет нужен.

**Replace 404 error page, home page, search page and local page.**

**Replacement will be done with local html page (local feed). Local pages will be loaded to user's PC in multiple forms and different designs. They might look like this:**

**[www.yapsearch\(dot\)com](http://www.yapsearch(dot)com)**

## *April 2006: YapBrowser*

All Yap domains registered to John Malkovich

Same details used for sites at Eltel (a Russian ISP) including paradise dialer.com which pushes exploits and Trojans

Paradise Dialers Whois info links it to the CWS group Dimpy AKA BigBuks

BigBuks and Yap domains share the same whois details (Mix-click)

## May 2006: The Safety Browser



## *May 2006: The Safety Browser*

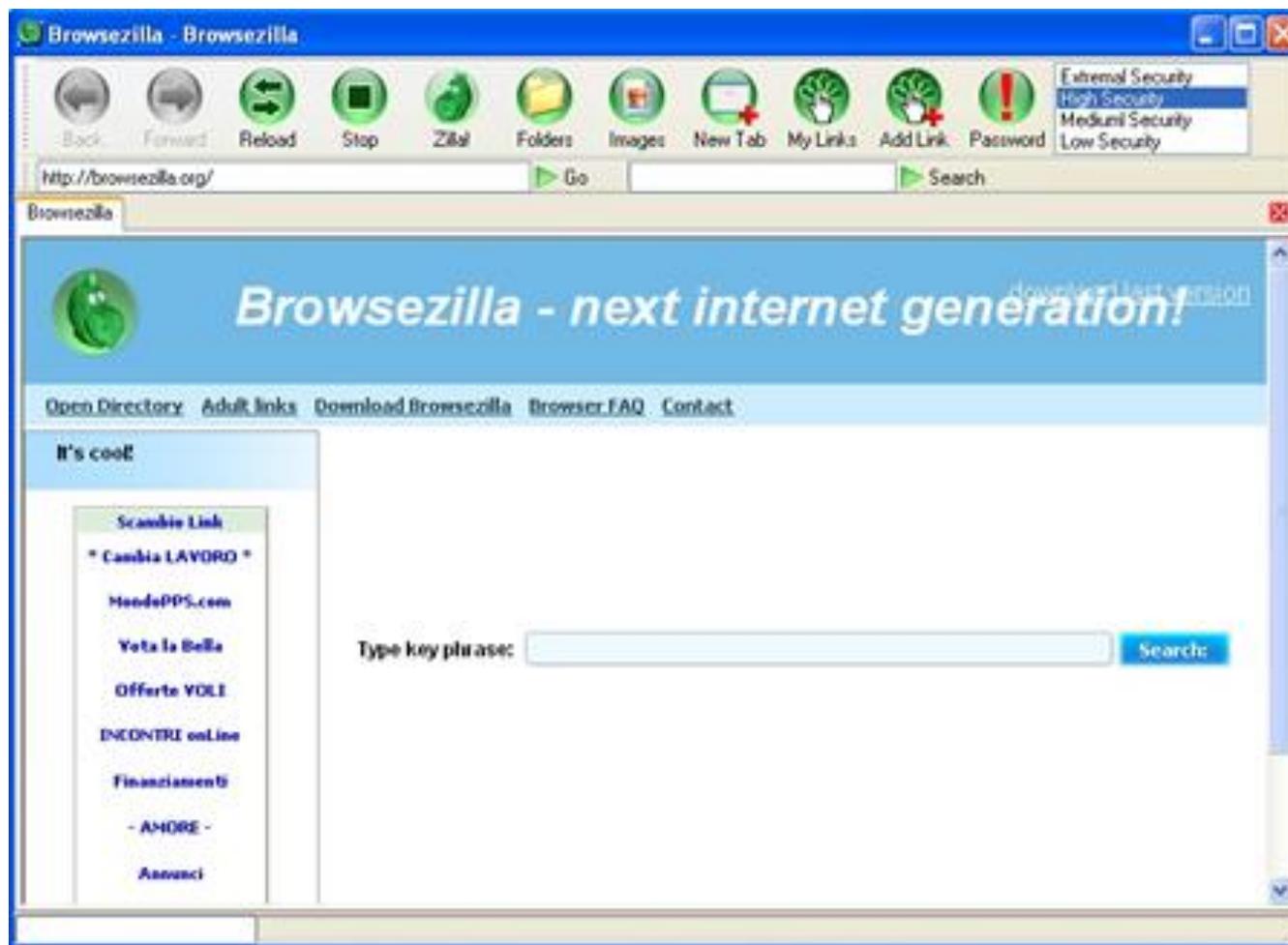
File on PC contacts a URL providing ever changing instructions for IM, IRC.

Geolocational technology ensures affiliate adverts served to victim

Safety Browser occasionally redirected users to “free gift” virus payload URLs

Desktop hijacked with looped 10 second thrash metal guitar riff

## June 2006: Browsezilla



## *June 2006: Browsezilla*

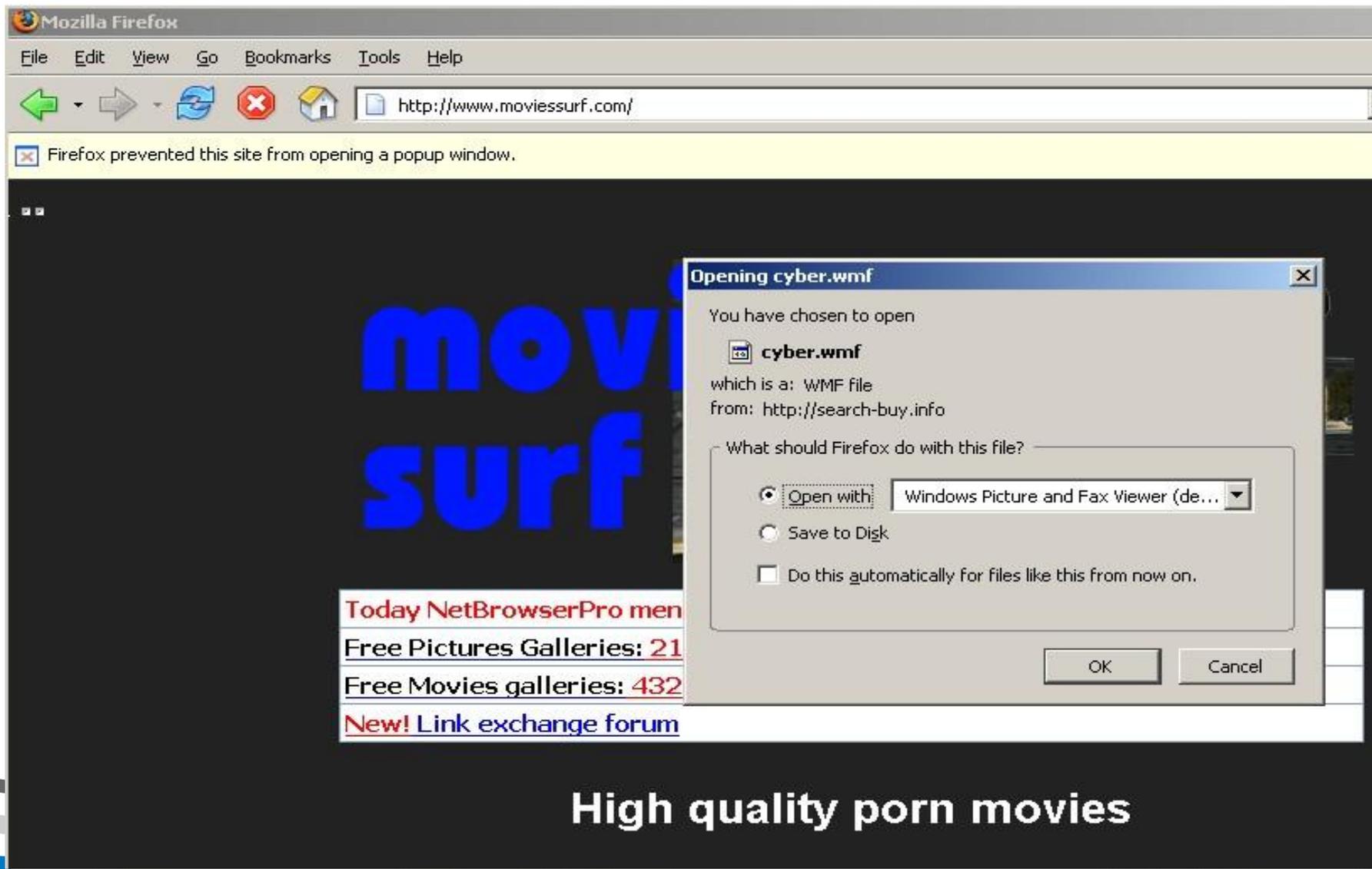
Name, lizard logo similar to Mozilla

Claimed to help stay hidden on porn sites, store bookmarks remotely

“Security level” features, no tracking

Installed adware that clicked hidden pornographic content

## March 2007: NetBrowserPro



## *March 2007: NetBrowserPro*

Website shared same IP as Browsezilla (216.255.178.220)

“All bookmarks are being kept on the remote server”

Common theme: promises of security (website lists Firefox vulnerability stats)

“NetBrowserPro uses only features, which are necessary to surf porn, it switch everything except this off. So there is absolutely no gap for the virus.”

## *No money, Mo problems*

Adware industry fired into the heart of the Sun

Traditional installs lose ground to survey scams

Fake AV: your new favourite band

Rogue browsers gone, mostly forgotten

As the Adware model died out, so too did the rogue browser

# March 2009: The Myspace Lottery

Lottery

Previous Next GroupID  Go  Skip all Invalid Groups

Topics Lottery previous URL:

by millions of buyers

**myspace.com**  
UK

Home Browse Find People Forums Music MySpaceTV More ▾

Groups »  Group

Listing 15901-15911 of 15911 1 << 1061 of 1061 < Previous

Forum Topic	Posts	Last Post	Topic Starter
 <input type="text"/>	9	<input type="text"/>	<input type="text"/>
 <input type="text"/>	16	<input type="text"/> 1	<input type="text"/>
 <input type="text"/>	2	<input type="text"/> 0	<input type="text"/>

**Pimp Your**  
Free- Layout  
Profile Gen  
Free  
[webfetti.sm](http://webfetti.sm)

**Local UK P**  
Postcode M  
Partner.  
Find and Ch  
Join!  
[www.single](http://www.single)

**Pimp Your**  
Download t

## *The future of fake web browsers?*

A move to mobile: Fake Opera Mini browsers, update sites

Fake AV still a better business model

Difficult to encourage downloads

# *Thank You!*

GFI Software

[www.gfi.com](http://www.gfi.com)

GFI Labs Blog:

[Sunbeltblog.blogspot.com](http://Sunbeltblog.blogspot.com)

Twitter (Personal account):

[@paperghost](https://twitter.com/paperghost)