Ouroboros

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

- Used to symbolise cyclicality – 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 antispyware 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 antispyware 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
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

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, binkx Deal.
- Custom Installation with FREEzeFrog View EULAs and Privacy Policy

By clicking “Start”, I represent that I (1) am at least 15, (2) agree to the terms and conditions and (3) to install selected programs.

Click "Start" to install FREEzeFrog and access this website for free.
Surveys: (from ‘08 to) April 2012

2012 DOOMSDAY CONFIRMED: NASA WARNS BE PREPARED!!

Please complete a survey
Please fill out one of the following surveys. You will not be allowed to continue until you have completed a survey.

Free Starbucks gift card!
Win an iPad 2!

Complete
Survey Installers - May 2013

To prevent automated leechers from stealing our movies, please complete a quick survey to prove you are human!

Download LightSpark Player Pro

Movie Hosted by:
Survey DIY kit - July 2013
## Bundles – 2005 to 2008

<table>
<thead>
<tr>
<th>Filename</th>
<th>Size</th>
<th>Type</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyboard25.exe</td>
<td>32 KB</td>
<td>Application</td>
<td>6/12/2006 3:23 AM</td>
</tr>
<tr>
<td>defender23a.exe</td>
<td>36 KB</td>
<td>Application</td>
<td>6/12/2006 3:23 AM</td>
</tr>
<tr>
<td>drsmartload849a.exe</td>
<td>28 KB</td>
<td>Application</td>
<td>6/12/2006 3:23 AM</td>
</tr>
<tr>
<td>newname25.exe</td>
<td>56 KB</td>
<td>Application</td>
<td>6/12/2006 3:23 AM</td>
</tr>
<tr>
<td>Trelew.exe</td>
<td>303 KB</td>
<td>Application</td>
<td>6/12/2006 3:23 AM</td>
</tr>
<tr>
<td>MTE3NDI6ODoxNg.exe</td>
<td>25 KB</td>
<td>Application</td>
<td>6/12/2006 3:23 AM</td>
</tr>
<tr>
<td>S51001.exe</td>
<td>30 KB</td>
<td>Application</td>
<td>6/12/2006 3:24 AM</td>
</tr>
<tr>
<td>stub_113_4_0_4_0.exe</td>
<td>15 KB</td>
<td>Application</td>
<td>6/12/2006 3:24 AM</td>
</tr>
<tr>
<td>warebundle.exe</td>
<td>565 KB</td>
<td>Application</td>
<td>6/12/2006 3:24 AM</td>
</tr>
<tr>
<td>WHCC2.exe</td>
<td>293 KB</td>
<td>Application</td>
<td>6/12/2006 3:24 AM</td>
</tr>
<tr>
<td>mc-110-12-0000228.exe</td>
<td>29 KB</td>
<td>Application</td>
<td>6/12/2006 3:24 AM</td>
</tr>
<tr>
<td>drsmartload45a.exe</td>
<td>28 KB</td>
<td>Application</td>
<td>6/12/2006 3:24 AM</td>
</tr>
<tr>
<td>drsmartload46a.exe</td>
<td>28 KB</td>
<td>Application</td>
<td>6/12/2006 3:24 AM</td>
</tr>
<tr>
<td>drsmartload1.exe</td>
<td>60 KB</td>
<td>Application</td>
<td>6/12/2006 3:27 AM</td>
</tr>
</tbody>
</table>
Welcome to the xvid Setup Wizard

Xvid is the world's best video codec library allowing outstanding quality and performance for video playback and encoding. This distribution of xvid 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 xvid from ClickPotato's servers also requires installation of the ClickPotato software, described below, which is subject to the ClickPotato End User License Agreement (EULA).

This Distribution is sponsored by ClickPotato

The ClickPotato add-on gives you FREE and unlimited access to all of the most popular TV shows and films online! Based on keywords from your browsing, ClickPotato will show you labeled advertising in a separate browser or a temporary slider.

View ClickPotato EULA  Privacy Policy  FAQ

- Yes, I want free ShopperReports too
- Make QuestBrowse your address bar search provider
- Install blinkx Beat
- Make blinkx Beat my screensaver

By clicking "Next", I represent that I (1) am at least 18, (2) agree to the xvid Privacy Policy and the ClickPotato EULA and Privacy Policy terms and (3) consent to install xvid, ClickPotato, if selected ShopperReports, QuestBrowse, blinkx Beat.
Bundles – June 2011

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

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 TOS
☐ 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.
INFECTION CHANNELS
Social Networks – May 2006

From: LIFE ON MYSPACE

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.
Social Networks: Fake Codecs Nov 06

GET ALL THREE FOR JUST £30 A MONTH
DIRECT DEBIT PAYMENT, FOR 12 MONTHS

THIS PROFILE IS SECURELY PROTECTED

CLICK HERE TO DOWNLOAD FREE MYSPACE VIEWER

http://www.myviewersoft.com/myspace.php
Fake AV on Social Networks – June 07
Profile Stalkers – Jan to May 2007

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 assigns, 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.
Profile Stalkers – Nov 2006

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
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 Acess Anywhere!
- Get A Subscription To Biz Mag!
- Get Rewards Towards Shell Fuel!
Botnet Installs – May 2006

This application is FREE, thanks to Zango. Why? Because it's paid for by advertising.

Zango Search Assistant shows advertisements relevant to what you search or shop for online; the number of ads you receive is based on how often you use your browser. When running, you can access Zango Search Assistant from your system tray. Your download is managed by Media Gateway and includes Zango Toolbar, which lets you search the Internet from any webpage, and Zango SiteFinder, which directs your browser to search results when you are unable to locate a website. You can uninstall these applications anytime by using Add or Remove Programs.

Get Zango and get full access to free entertainment! For more information, see our Privacy Policy and visit Zango.com for more free content.

End User License Agreement ("EULA")
(Revised June 13, 2005)

NOTICE TO USER: THIS END USER LICENSE AGREEMENT ("AGREEMENT") APPLIES WITH RESPECT TO SOFTWARE APPLICATIONS PROVIDED BY 180SOLUTIONS, INC. AND ITS AFFILIATES (REFERRED TO IN THIS AGREEMENT AS "WE" OR "180"). PLEASE READ THIS AGREEMENT.

I am 18 or older and agree to the terms of the End User License Agreement.

Finish
Botnet Installs – July 2008

Stream Content

botsMINOFMINOFkimya_bots

AIM IM with Chunkylover53 from

chunkylover53 is away
The link is now fixed everyone. CHECK OUT THE NEW SIMPSONS EPISODE THAT WE'RE ONLY RELEASING TO THE INTERNET AIM FANS! BE THE FIRST TO EXPERIENCE THE MAGIC BY CLICKING THE FOLLOWING LINK:
http://[REDACTED].exe SELECT...

ExitProcess
capCreateCaptureWindowA
acmStreamSize
SysFreeString
ShellExecuteA
waveInOpen
DENEME
DVCLAL
PACKAGEINFO
ROOTKIT
MAINICON
Botnet Installs – February 2009
Botnet Installs – May 2010
Ad Networks and Affiliates
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

Make Skype part of your everyday life!

Features!
- Free video calling - Why just talk when you can see each other?

More Features:
- IM with your friends
- Call anyone, even if they're not on Skype

Download it now!!!

Skype is Free
Skype is free 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 aren't on Skype.

Opening Skype_5.3.0.111.exe
You have chosen to open

| File: | skype_5.3.0.111.exe
Which is an .exe file
From: http://skype.on-software.net

Would you like to save this file?

Save File
Cancel

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

Download Skype Now

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

ThreatTrack Security
Ads in Search Results: July 2013

- **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

- **Coupandropdown**: 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

- **Strongvaut**: 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

- **Infotomes**: Highlight any word or phrase and Wikipedia, Bing, and other results appear in page. Learn more | Uninstall instructions

- **Translategenius**: 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
(l-r) Appendix Opt-Out, Big Truck, Fast Points, Pontiflex
Use the app on your phone to recognize the QR code and download the QIP_mobile.apk
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.
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 page cannot be displayed

The page you are looking for is currently unavailable. The website might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or...
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?
Thank you for listening!