Perpetual Beta = Live Testing = Trouble

Airline Terminals using Active Script
Wait, the Web has version numbers?

Web Two Dot UH-OH or Exploit 2.0

An introduction to HoneyJax
- Definitions
- Reasons for deploying them
- Types: Passive, Active HoneyJax, Passive Aggressive
- Reporting data from Accounts
- Disclosure for web site vulnerabilities
- Legal Aspects / Grab Bag

Conclusion
One of these things is not like the other

- It's a bird, is it a plane, no it's Web 2.0: 80% top 20 Web sites have Web 2.0 “philosophies”
XML HTTP Request

- When Microsoft created XMLHttpRequest in Internet Explorer 5, which let browser-side JavaScript communicate with the web server in the background without requiring the browser to display a new web page. That made it possible to develop more fluid and responsive web applications. Mozilla soon implemented XMLHttpRequest in its browsers, as did Apple (in the Safari browser) and Opera.

- Several dozen *very* loosely defined standards mashed together

- At the heart of it all are JavaScript and XML
Web “Two Dot Uh-Oh”

- Losing control of your destiny: User Created Content
- Who do you trust: Social Networks
- Unattended Installs and Code Injection: R.S.S
- Mushy Peas: Mash-ups
- ANY ANY PORT 80: Security is often the last ones to know
- But I have a firewall: Its about the information not the network
- If I told you to jump of a bridge…: Its just sooooo easy and being web 2.0 is cool
Threats → User-created content

- Property owner gives / leases space to user
- 400 Million + pages change dramatically close real-time
- Content stripping done but very difficult to enforce (JavaScript obfuscation deluxe)
- Easy to test for vulnerabilities, little disclosure: Can you say “Web borne Worms”
- Allow dynamic/graphic content (jscript, qt, mov)
- Trust within user-networks
- Used a many-to-many communication platform
User-created Content → Hidden IFRAME w/WMF, CSS auth page phish, Wikipedia Trojan
Social Networks (1 account: 70M views ~2 M “friends”)

- Interlinking of hundreds of millions of users
- Communication platform not just content “Email is so yr 2000”
- More contacts = better site / success
- One “friend” can infect millions through their network
- One account compromise can be used to gain user trust

1991623

www.tilashotspot.com

myspace.com/tilatequila
Social Networks → “My network is bigger than yours”

- It's not just about entertainment. Business colleagues, networking with associates, recruiting, etc., gaining popularity.
SideBar: Un-attended installations (can they happen?)
- RSS: Meta-Feeds
- RSS: Pulling data every X seconds
Introduction to HoneyJax

- **HoneyPots → HoneyClients → HoneyJax**

- **HoneyPots:**
  *Emulate OS and Applications behavior*

- **HoneyClients:**
  *Emulate client applications behavior*

- **HoneyJax:**
  *Emulate user accounts, profiles, and web social networks.*
  *Can also emulate user behavior*
Reasons for deploying HoneyJax

- 95% of all BLOG comments are SPAM (src: Akismet)
- SPAM -> P0RN -> Phishing -> Malicious Code
- One new weapon in arsenal to help research Web 2.0 threats
- The threat playing field is changing and research needs to evolve with it
- Can be used by web property-owners also

Assist in:
- Tracking and trending attacks, attackers, predators
- Escalation to abuse or security department of property owners
- Track common techniques
- Collect samples of binary code for detection / protection
- Collect URL’s and script code for detection / protection
- Monitor outbreaks (yes more Web worms are coming)
Types of HoneyJax

- **Passive HoneyJax:**
  Accounts in web 2.0 space that are not luring users to add them to their network in any way.

- **Active HoneyJax:**
  Accounts and BOT’s in web 2.0 space that are designed to join networks actively and solicit users to join theirs and reply to requests.

- **Passive Aggressive HoneyJax:**
  Accounts that are designed to lure users to visit them through their characteristics. Eg: p0rn, baby boomers looking for friends, music band, common interest groups, popular merchandise, contests
I want the bike, give me number account bank and tomorrow i solicite deposit to you in the morning, please i want the bike, thank you.
# Passive HoneyJax: Spam first!

## My Account / General Messages

Your Inbox is the central place to keep track of messages and videos from other people on YouTube. You can view and delete messages and invites sent to you, manage comments and video responses, and send messages to others.

### General Messages

<table>
<thead>
<tr>
<th>From</th>
<th>Subject</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>blogvideo</strong></td>
<td>Hi, please upload all your videos to Noid97.com</td>
<td>Jun 08, 2007, 12:55 AM</td>
</tr>
<tr>
<td><strong>rene970</strong></td>
<td>Hi, what's up? That's a sweet video page you've got there. You should check out my other site. I'm usually online there: view now 970 video next <em>for</em> com. But umm, ignore the pics!</td>
<td>Jan 25, 2007, 11:10 AM</td>
</tr>
</tbody>
</table>
Passive Aggressive HoneyJax: Luring $$ $$

![Image of MySpace homepage]

---

**New MySpace Profile Editor**
Now powered by Fantastic Fireflow of the Silver Surfer

- Pick your MySpace Name/URL
- Click Here

**My Mail**
- Inbox
- Friend Requests
- Sent
- Post Bulletin

**My Bulletin Board**
You don’t have any bulletins yet.

- Subscribe to alert your friends about a party, things for sale, job hunts, etc.
- (Post a Bulletin Here)

**Get New Videos**
- American rapper #1
- Alabama Toomer Board Classes
- Make MySpace my home page

**Featured Profiles**
- No one deals like we do
- Negotiator

**Sponsored Links**
- No Handle Callouses Loans

---

**GerryAttric’s Profile**
- Your profile has been viewed 4 times
- View all comments
- Edit my photos
- Add a video
- Post a blog entry
- Add a widget

**History**
- Edit my history

**About Me**
- Add a comment

**LifeMap**
- You haven’t created a Lifemap yet!
- Start my Lifemap!

**Interests and Activities**
- Add my interests and activities

---

**WEBSENSE® Security Labs**

---

**Eons: My Financial Partner**
- We'll help you with the financial part.
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Status</th>
<th>Sender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 12, 2007</td>
<td>2:59 PM</td>
<td>Read</td>
<td>No Subject</td>
</tr>
<tr>
<td>Jan 10, 2007</td>
<td>9:06 AM</td>
<td>Unread</td>
<td>This Profile No Longer Exists</td>
</tr>
<tr>
<td>Jan 6, 2007</td>
<td>1:32 AM</td>
<td>Read</td>
<td>This Profile No Longer Exists</td>
</tr>
<tr>
<td>Dec 20, 2006</td>
<td>11:46 PM</td>
<td>Unread</td>
<td>This Profile No Longer Exists</td>
</tr>
<tr>
<td>Dec 19, 2006</td>
<td>7:58 PM</td>
<td>Unread</td>
<td>This Profile No Longer Exists</td>
</tr>
<tr>
<td>Dec 11, 2006</td>
<td>1:17 PM</td>
<td>Read</td>
<td>This Profile No Longer Exists</td>
</tr>
<tr>
<td>Dec 9, 2006</td>
<td>1:59 PM</td>
<td>Read</td>
<td>GET $1500 BY TOMORROW - IT'S SO EASY - CLICK HERE</td>
</tr>
</tbody>
</table>

Note: The image contains a security alert from Websense Security Labs.
Active HoneyJax : 4 Types

- Open Source
- Commercial
- Proof-of-Concept (i.e. copy-code)
- Do your own
Active HoneyJax : Open Source

FacebookBot

Description

Hello from FacebookBot!

FacebookBot allows for completely automated control of your Facebook profile.

- Posting Profile Pictures
- Tagging Pictures
- Changing your Status
- Posting Wall Comments
- Changing Personal Profile Information
- Sending and Reading Private Messages
- Joining Groups
- Adding Friends
- A system for generating random sentences (rather simply)
- And much more...

Downloading

You can obtain the hot-off-the-press-brand-sparkling-new FacebookBot and loads of pretty examples from rubyforge.org/frs/?group_id=3643
Active HoneyJax: Commercial

Welcome to the home of the FriendBot!

FriendBot Suite now has captcha bypass!

Auto accept pending friend requests!
- Auto message, comment, or just approve!
- Get more myspace friends with adding.
- Sends real friend requests!
- Import users from comments, friends and more
- Comment on all of your friends with auto commenter
- Event and Group inviter
- Send event invites to everyone on your list!
- Invite all your friends to groups.

The best messaging features:
- Search by any demographic on myspace.com!
- Allows you to search bands
- Message only online users
- Import friends from the page you are on
- Send messages to users with pictures only
- Import the friends of someone else!
- Keeps track of who it has sent to

Unique timed bulletin features
- All features have:
  - Filter out bands and/or people
  - Global age and gender filter
  - Free updates for life!

More Info

$55.50

Popular Links
- Free Download
- Help me choose a bot!
- A Guide for Mac users
- Microsoft .NET Runtime
- Affiliate signup 50% commission

Windows and Mac!
We now have both windows and mac version of our software. Look for these icons:

Get more Friends!
With FriendBot you are guaranteed to gain more friends in a matter of minutes.

Promote your band!
There is no better place to promote your band than Myspace.com. Do it the right way.
Active HoneyJax: POC
Active HoneyJax: DYO

SpiderMonkey (JavaScript-C) Engine
What is SpiderMonkey?
SpiderMonkey is the code-name for the Mozilla's C implementation of JavaScript.

Where do I get it?
The core SpiderMonkey engine can be found in mozilla/src. The standalone interpreter can be built using Makefile, files mozilla/pkgrc/README.html for the nitty gritty. Some projects embedding the JavaScript engine (in addition to Mozilla itself) are listed in the projects page.

You can get the engine via CVS and build it yourself, or look for recent tarballs at (please check the mirrors first). http://ftp.mozilla.org/pub/mozilla.org/js/. Release notes are available at http://www.mozilla.org/js/spidermonkey/release-notes/

Where do I find out more?

<table>
<thead>
<tr>
<th>Site</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JS Embedder's Guide</td>
<td>A guide to embedding the JavaScript C engine in applications.</td>
</tr>
<tr>
<td>JS Embedder's Reference in the following formats:</td>
<td>A function by function reference to the public JavaScript API.</td>
</tr>
<tr>
<td>HTML, CSS only</td>
<td></td>
</tr>
<tr>
<td>HTML, CSS, JavaScript only</td>
<td></td>
</tr>
<tr>
<td>HTML, CSS, JavaScript, XML</td>
<td></td>
</tr>
<tr>
<td>Source XML file</td>
<td></td>
</tr>
<tr>
<td>Source HTML file</td>
<td></td>
</tr>
<tr>
<td>Source CSS file</td>
<td></td>
</tr>
</tbody>
</table>

Tools

Roadmap

Projects

Coding

- Module Owners
- Hacking

Get the Source

- Build it

Testing

- Releases
- Nightly Builds

Report A Problem

FAQs

Mozilla.org

Products Support Store Developers About

Security Labs
Reporting and Forensics

- HoneyJax accounts should be setup to send email or SMS when new attempts to access the account are added
- Spider/Bot should connect to HoneyJax accounts and fingerprint content looking for changes. Make sure that dynamic content changes by the host are accounted for. All changes should be kept and stored
- Data should be mined for URL’s that are dropped
- Content should be analyzed from data mined
- Binaries should be sandboxed, etc…
- JavaScript should be run through decoder and tested
- HTML code should be tested for candidates to send to sandbox
- Report information to vendor, web property owner, etc..
The LAW and the T&C’s

- As with any honey technologies check with your legal team before you deploy these
- Check Acceptable Use Policies / Terms and Conditions
- Be weary of “commercial” software that allows you to manage profiles, add friends, etc.

The following is a partial list of the kind of activity that is illegal or prohibited on the MySpace Website and through your use of the MySpace Services. MySpace.com reserves the right to investigate and take appropriate legal action against anyone who, in MySpace.com’s sole discretion, violates this provision, including without limitation, reporting you to law enforcement authorities. Prohibited activity includes, but is not limited to:

1. criminal or tortious activity, including child pornography, fraud, trafficking in obscene material, drug dealing, gambling, harassment, stalking, spamming, sending of viruses or other harmful files, copyright infringement, patent infringement, or theft of trade secrets;
2. advertising to, or solicitation of, any Member to buy or sell any products or services through the MySpace Services. You may not transmit any chain letters or junk email to other Members. It is also a violation of these rules to use any information obtained from the MySpace Services in order to contact, advertise to, solicit, or sell to any Member without their prior explicit consent. In order to protect our Members from such advertising or solicitation, MySpace.com reserves the right to restrict the number of emails which a Member may send to other Members in any 24-hour period to a number which MySpace.com deems appropriate in its sole discretion. If you breach this Agreement and send unsolicited bulk email, instant messages or other unsolicited communications of any kind through the MySpace Services, you acknowledge that you will have caused substantial harm to MySpace.com, but that the amount of such harm would be extremely difficult to ascertain. As a reasonable estimation of such harm, you agree to pay MySpace.com $50 for each such unsolicited email or other unsolicited communication you send through the MySpace Services;
3. covering or obscuring the banner advertisements on your personal profile page, or any MySpace.com page via HTML CSS or any other method;
4. any automated use of the system, such as using scripts to add friends or send comments or messages;
5. including, without limitation, hacking or attempting to gain unauthorized access to the MySpace Services or the networks or services connected to the MySpace Services;
6. attempting to impersonate another Member or person;
Disclosure of Website Vulnerabilities: It's not just about the browser!

- Website Security has to be taken more seriously!
- Massive amounts of problems with sites not being patched, configured incorrectly, allowing bad data, conduit for others
- Website security or lack thereof is a HUGE problem
- Cross site scripting, open redirectors, allowing binary file posts, not scanning upload files, poor script filtering are all big problems
- PHP BB, SQL, old Web servers, old OS all too common
- Problem with tracking?
  - No version numbers: how about time-stamp + example + hash
  - No reporting: security departments must field reports on websites and do more testing, re-testing
  - Change controls: force security into the process
  - No public credit: MS and Google started doing this, others should start
  - Property owners: get to know who is in your backyard
  - How about a web owner area on OSVDB?
Grab Bag

- What if there is a reference in one of my HoneyJax but the site is down?
  - A: Is there a reputation for it?
    - Query search engines for link references and cached pages
    - What is the age of the domain
    - History the site hosted malcode/phishing in the past
    - Who registered it
    - Where is the IP located
    - Who are its neighbors

- My boss told me that I need to make our website “Web 2.0”, should I?
  - A: Get the security team involved. Make sure they buy-off on all design, implementation, and have a reproducible security testing process, mitigation techniques, and incident reporting and handling
Conclusion

- Don’t run with Scissors
  - Before you deploy Web 2.0 be educated on the risks

- If you must have user-created content…
  - Filter, Filter, Filter, Pen-test, Pen-Test, report, update

- If you are a security researcher..
  - Advanced JavaScript may not be as cool as ASM but its powerful. Live it, learn it, you don’t have to love it

- The good, the bad, and the ugly
  - There is a lot of good, productive, useful Web 2.0 functionalities. But with functionality comes security risk. Security standards, policies, and practices must balance the scales with functionality. Its not too late!
Questions are guaranteed in life; Answers aren't.

dhubbard /AT/ websense /DOT/ com