For my next trick... hacking Web2.0

Petko D. Petkov (pdp)
GNUCITIZEN
http://www.gnucitizen.org

OWASP Day
September 2007

The OWASP Foundation
http://www.owasp.org/

POWERED BY

GNUCITIZEN

HTTP://WWW.GNUCITIZEN.ORG

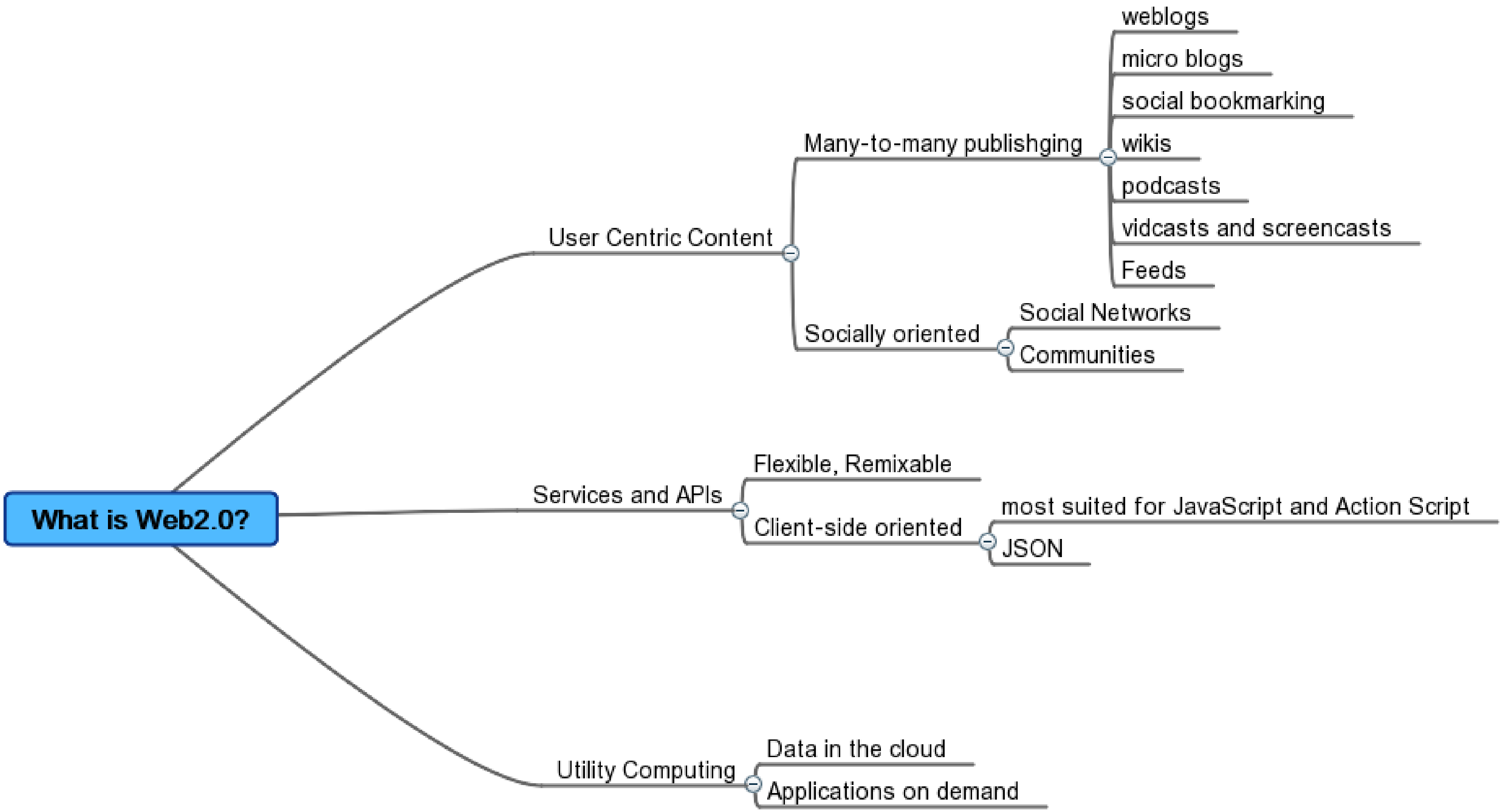
…before we start

- Feel free to ask questions
- Do ask questions
- Read the paper for getting better understandings

What is Web2.0?

- Marketing buzzword
- Invented by O'Reilly Media in 2003
- Wikis, Blogs, AJAX, Social Networks, Collaboration
- APIs, SOA (Service Oriented Architecture)
- Data in the Cloud
- Applications on Demand

...a Web2.0 Mindmap

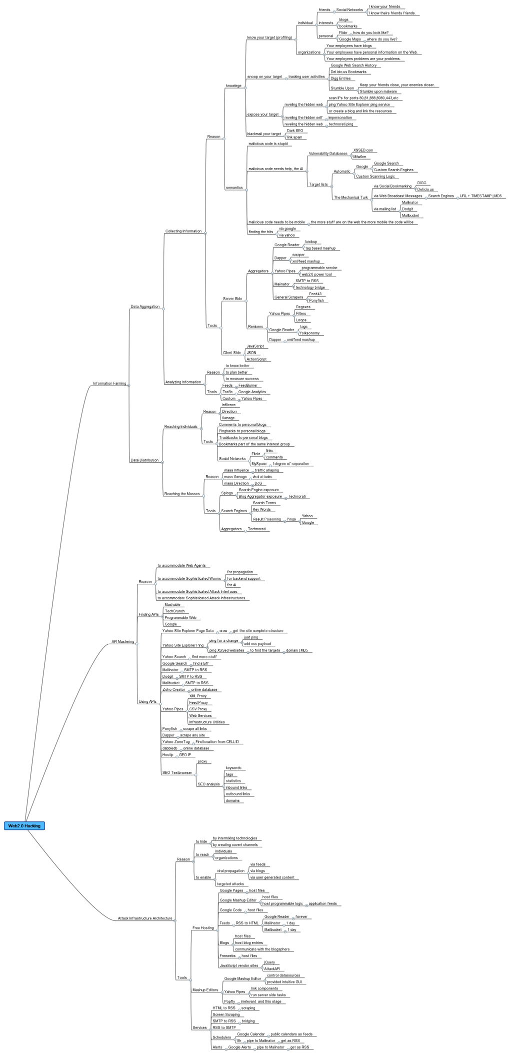


- What is Web2.0?
  - User Centric Content
    - Many-to-many publishging
      - weblogs
      - micro blogs
      - social bookmarking
      - wikis
      - podcasts
      - vidcasts and screencasts
      - Feeds
    - Socially oriented
      - Social Networks
      - Communities
  - Services and APIs
    - Flexible, Remixable
    - Client-side oriented
      - most suited for JavaScript and Action Script
      - JSON
  - Utility Computing
    - Data in the cloud
    - Applications on demand

Why Web2.0 hacking?

- Data Management
- Information Leaks
- Live Profiling
- Information Spamming
- Service Abuse
- Autonomous Agents
- Distribution
- Attack Infrastructures

...a Web2.0 Hacking Mindmap



- Web2.0 Hacking
  - Information Farming
    - Data Aggregation
      - Collecting Information
        - Reason
          - knowlege
            - know your target (profiling)
              - individual
                - friends
                  - Social Networks
                    - I know your friends.
                    - I know theirs friends friends.
                - interests
                  - blogs
                  - bookmarks
                - personal
                  - Flickr
                    - how do you look like?
                  - Google Maps
                    - where do you live?
              - organizations
                - Your employees have blogs
                - Your employees have personal information on the Web.
                - Your employees problems are your problems.
            - snoop on your target
              - tracking user activities
                - Google Web Search History
                - Del.icio.us Bookmarks
                - Digg Entries
                - Stumble Upon
                  - Keep your friends close, your enemies closer.
                  - Stumble upon malware
            - expose your target
              - reveling the hidden web
                - scan IPs for ports 80,81,888,8080,443,etc
                - ping Yahoo Site Explorer ping service
                - or create a blog and link the resources
              - reveling the hidden self
                - impersonation
              - reveling the hidden web
                - technorati ping
            - blackmail your target
              - Dark SEO
              - link spam
          - semantics
            - malicious code is stupid
            - malicious code needs help, the AI
              - Vulnerability Databases
                - XSSED.com
                - Milw0rm
              - Target lists
                - Automatic
                  - Google
                    - Google Search
                    - Custom Search Engines
                  - Custom Scanning Logic
                - The Mechanical Turk
                  - via Social Bookmarking
                    - DIGG
                    - Del.icio.us
                  - via Web Broadcast Messages
                    - Search Engines
                      - URL + TIMESTAMP | MD5
                  - via mailing list
                    - Mailinator
                    - Dodgit
                    - Mailbucket
            - malicious code needs to be mobile
              - the more stuff are on the web the more mobile the code will be
            - finding the hits
              - via google
              - via yahoo
        - Tools
          - Server Side
            - Aggregators
              - Google Reader
                - backup
                - tag based mashup
              - Dapper
                - scraper
                - xml/feed mashup
              - Yahoo Pipes
                - programmable service
                - web2.0 power tool
              - Mailinator
                - SMTP to RSS
                - technology bridge
              - General Scrapers
                - Feed43
                - Ponyfish
            - Remixers
              - Yahoo Pipes
                - Regexes
                - Filters
                - Loops
              - Google Reader
                - tags
                - folksonomy
              - Dapper
                - xml/feed mashup
          - Client Side
            - JavaScript
            - JSON
            - ActionScript
      - Analyzing Information
        - Reason
          - to know better
          - to plan better
          - to measure success
        - Tools
          - Feeds
            - FeedBurner
          - Trafic
            - Google Analytics
          - Custom
            - Yahoo Pipes
    - Data Distribution
      - Reaching Individuals
        - Reason
          - Inflience
          - Direction
          - 0wnage
        - Tools
          - Comments to personal blogs
          - Pingbacks to personal blogs
          - Trackbacks to personal blogs
          - Bookmarks part of the same interest group
          - Social Networks
            - Flickr
              - links
              - comments
            - MySpace
              - 1degree of separation
      - Reaching the Masses
        - Reason
          - mass Influence
            - traffic shaping
          - mass 0wnage
            - viral attacks
          - mass Direction
            - DoS
        - Tools
          - Splogs
            - Search Engine exposure
            - Blog Aggregator exposure
              - Technorati
          - Search Engines
            - Search Terms
            - Key Words
            - Result Poisoning
              - Pings
                - Yahoo
                - Google
          - Aggregators
            - Technorati
  - API Mastering
    - Reason
      - to accommodate Web Agents
      - to accommodate Sophisticated Worms
        - for propagation
        - for backend support
        - for AI
      - to accommodate Sophisticated Attack Interfaces
      - to accommodate Sophisticated Attack Infrastructures
    - Finding APIs
      - Mashable
      - TechCrunch
      - Programmable Web
      - Google
    - Using APIs
      - Yahoo Site Explorer Page Data
        - craw
          - get the site complete structure
      - Yahoo Site Explorer Ping
        - ping for a change
          - just ping
          - add xss payload
        - ping XSSed websites
          - to find the targets
            - domain | MD5
      - Yahoo Search
        - find more stuff
      - Google Search
        - find stuff
      - Mailinator
        - SMTP to RSS
      - Dodgit
        - SMTP to RSS
      - Mailbucket
        - SMTP to RSS
      - Zoho Creator
        - online database
      - Yahoo Pipes
        - XML Proxy
        - Feed Proxy
        - CSV Proxy
        - Web Services
        - Infrastructure Utilities
      - Ponyfish
        - scrape all links
      - Dapper
        - scrape any site
      - Yahoo ZoneTag
        - Find location from CELL ID
      - dabbledb
        - online database
      - Hostip
        - GEO IP
      - SEO Textbrowser
        - proxy
        - SEO analysis
          - keywords
          - tags
          - statistics
          - inbound links
          - outbound links
          - domains
  - Attack Infrastructure Architecture
    - Reason
      - to hide
        - by intermixing technologies
        - by creating covert channels
      - to reach
        - individuals
        - organizations
      - to enable
        - viral propagation
          - via feeds
          - via blogs
          - via user generated content
        - targeted attacks
    - Tools
      - Free Hosting
        - Google Pages
          - host files
        - Google Mashup Editor
          - host files
          - host programmable logic
            - application feeds
        - Google Code
          - host files
        - Feeds
          - RSS to HTML
            - Google Reader
              - forever
            - Mailinator
              - 1 day
            - Mailbucket
              - 1 day
        - Blogs
          - host files
          - host blog entries
          - communicate with the blogsphere
        - Freewebs
          - host files
        - JavaScript vendor sites
          - jQuery
          - AttackAPI
      - Mashup Editors
        - Google Mashup Editor
          - control datasources
          - provided intuitive GUI
        - Yahoo Pipes
          - link components
          - run server side tasks
        - Popfly
          - irrelevant and this stage
      - Services
        - HTML to RSS
          - scraping
        - Screen Scraping
        - SMTP to RSS
          - bridging
        - RSS to SMTP
        - Schedulers
          - Google Calendar
            - public calendars as feeds
          - l8r
            - pipe to Mailinator
              - get as RSS
        - Alerts
          - Google Alerts
            - pipe to Mailinator
              - get as RSS

The Paper

- 5 fictional stories with technology that is real
- Learn by example
- KISS (Keep it Simple Stupid)
- Problems with no solutions

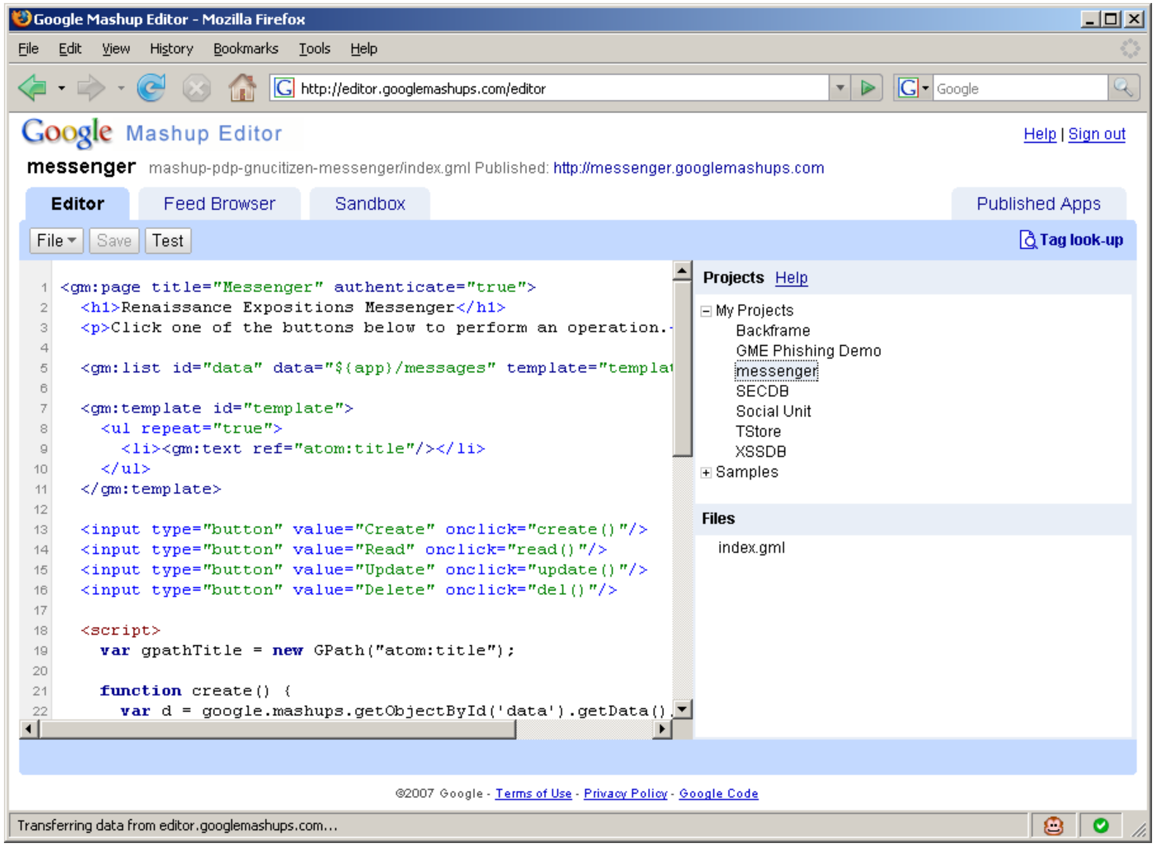
The Stories

- MPack2.0
  - Attack Infrastructures
- Wormoholic
  - Autonomous Agents
- Bookmarks Rider
  - Distribution
- RSS Kingpin
  - Information Spamming
- Revealing the hidden Web
  - Service Abuse

MPack2.0

- The Story:
  - Kr0nx runs a Malware Construction Kit
  - He constantly needs to find better ways to keep the Kit on-line
  - Google Mashup Editor to the rescue
- The Technology:
  - AJAX
  - ATOM Feeds
  - SVN (Subversion)

MPack2.0 :: The Tool


Google Mashup Editor - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://editor.googlemashups.com/editor
Google
Google Mashup Editor
Help | Sign out
Editor
Feed Browser
Sandbox
Published Apps
File
Save
Test
Tag look-up

messenger mashup-pdp-gnucitizen-messenger/index.gml Published: http://messenger.googlemashups.com

```
<gm:page title="Messenger" authenticate="true">
  <h1>Renaissance Expositions Messenger</h1>
  <p>Click one of the buttons below to perform an operation.

  <gm:list id="data" data="${app}/messages" template="templat

  <gm:template id="template">
    <ul repeat="true">
      <li><gm:text ref="atom:title"/></li>
    </ul>
  </gm:template>

  <input type="button" value="Create" onclick="create()"/>
  <input type="button" value="Read" onclick="read()"/>
  <input type="button" value="Update" onclick="update()"/>
  <input type="button" value="Delete" onclick="del()"/>

  <script>
    var gpathTitle = new GPath("atom:title");

    function create() {
      var d = google.mashups.getObjectById('data').getData().
```

Projects Help

- My Projects
  - Backframe
  - GME Phishing Demo
  - messenger
  - SECDB
  - Social Unit
  - TStore
  - XSSDB
- Samples

Files

index.gml

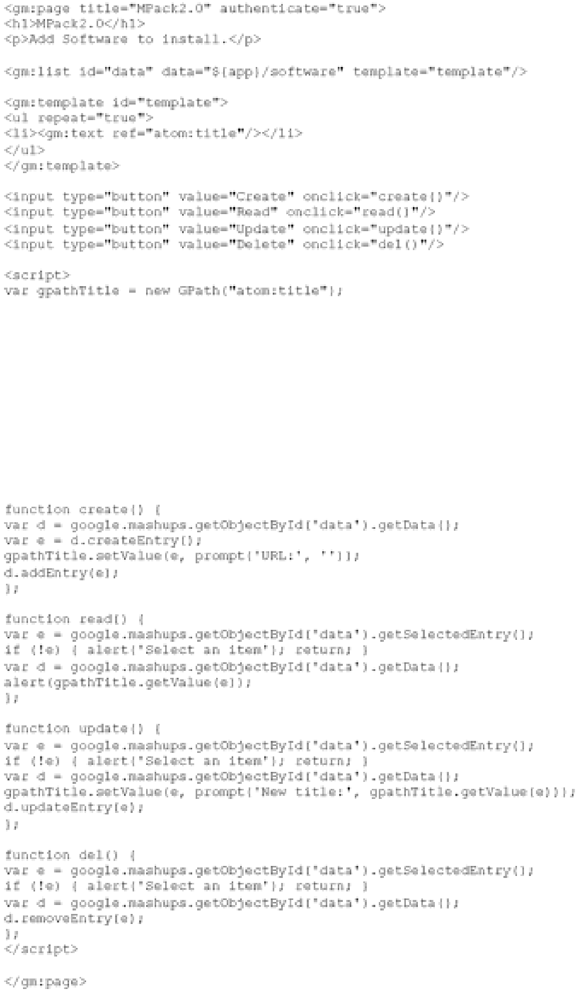
©2007 Google - Terms of Use - Privacy Policy - Google Code

Transferring data from editor.googlemashups.com...

MPack2.0 :: The Plan

- Write the client by using the CRUD example
- Link the member's feeds with the global application feed
- Upload the JavaScript attack libraries
- Link the libraries to the application feed
- Control via Subversion
- Instantiate the application as many times as you wish

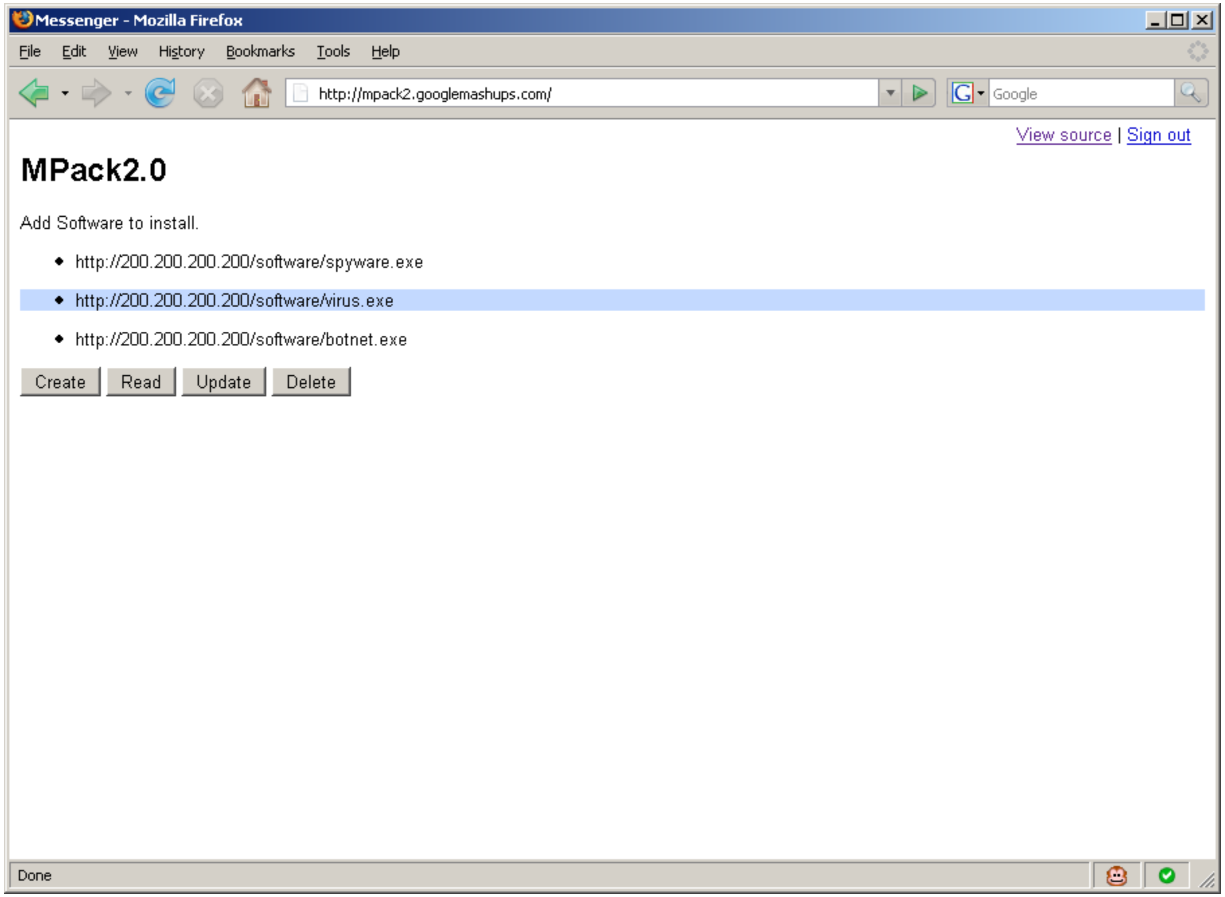
MPack2.0 :: The Code



```
<gm:page title="MPack2.0" authenticate="true">
<h1>MPack2.0</h1>
<p>Add Software to install.</p>

<gm:list id="data" data="${app}/software" template="template"/>

<gm:template id="template">
<ul repeat="true">
<li><gm:text ref="atom:title"/></li>
</ul>
</gm:template>

<input type="button" value="Create" onclick="create()"/>
<input type="button" value="Read" onclick="read()"/>
<input type="button" value="Update" onclick="update()"/>
<input type="button" value="Delete" onclick="del()"/>

<script>
var gpathTitle = new GPath("atom:title");
```

```
function create() {
var d = google.mashups.getObjectById('data').getData();
var e = d.createEntry();
gpathTitle.setValue(e, prompt('URL:', ''));
d.addEntry(e);
};

function read() {
var e = google.mashups.getObjectById('data').getSelectedEntry();
if (!e) { alert('Select an item'); return; }
var d = google.mashups.getObjectById('data').getData();
alert(gpathTitle.getValue(e));
};

function update() {
var e = google.mashups.getObjectById('data').getSelectedEntry();
if (!e) { alert('Select an item'); return; }
var d = google.mashups.getObjectById('data').getData();
gpathTitle.setValue(e, prompt('New title:', gpathTitle.getValue(e)));
d.updateEntry(e);
};

function del() {
var e = google.mashups.getObjectById('data').getSelectedEntry();
if (!e) { alert('Select an item'); return; }
var d = google.mashups.getObjectById('data').getData();
d.removeEntry(e);
};
</script>

</gm:page>
```

MPack2.0 :: The Result


Messenger - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://mpack2.googlemashups.com/
Google
View source | Sign out

MPack2.0

Add Software to install.

- http://200.200.200.200/software/spyware.exe
- http://200.200.200.200/software/virus.exe
- http://200.200.200.200/software/botnet.exe

Create
Read
Update
Delete
Done

MPack2.0 :: The Conclusion

- Malware Construction Kits such as MPack and WebAttacker are widely used to compromise hundreds of thousands machines per day.
- They require access to Web servers with support of server-side scripts
- We fight them by informing the ISPs about their presence and by blacklisting malicious IP blocks

MPack2.0 :: The Conclusion

- Google Mashup Editor is one of the most vivid Web2.0 technologies
- Developers can write complex Server-side/Client-side software by using only AJAX.
- Database like functionalities are ready to use
- Applications can be easily backed up and redeployed from local or remote source code repositories

MPack2.0 :: …therefore

- These types of services can be easily abused for malicious purposes
- They can host malicious software that can compromise client machines
- The can host software to control botnets
- Google cannot be blocked as it is one of the biggest service providers
- The platform is suitable for all kinds of malicious purposes

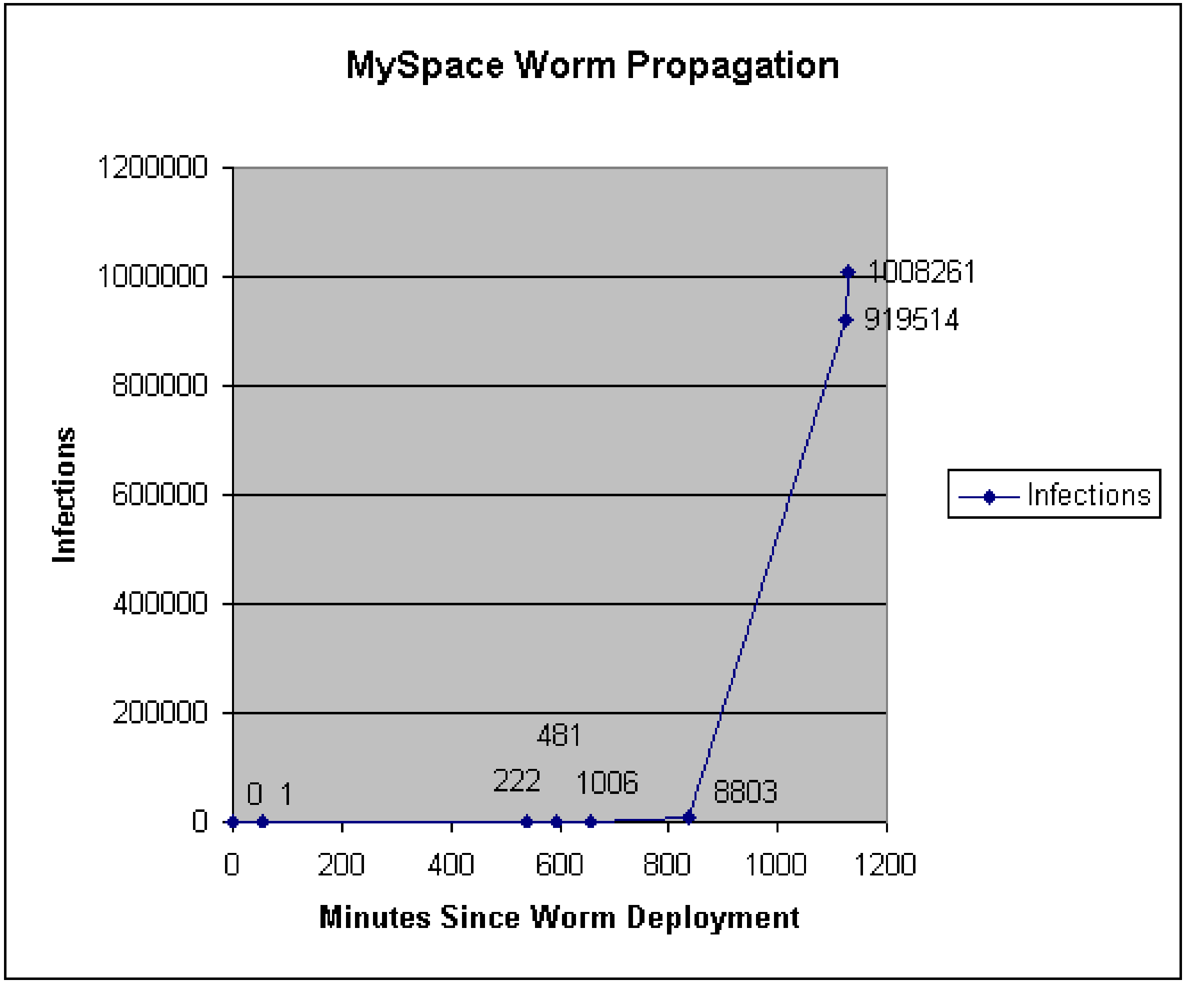
Wormoholic

- The Story:
  - Excerpts of a fictional presentation
- The Technology:
  - JavaScript
  - Feeds
  - Aggregators
  - Social Sites
  - Services
  - Search Engines

Wormoholic :: Why it matters?

- Samy is one of the fastest spreading worms over seen
- It could have been used for malicious purposes
- Software of this type can reach audience larder then traditional viral attacks
- Attackers can create botnets instantaneously

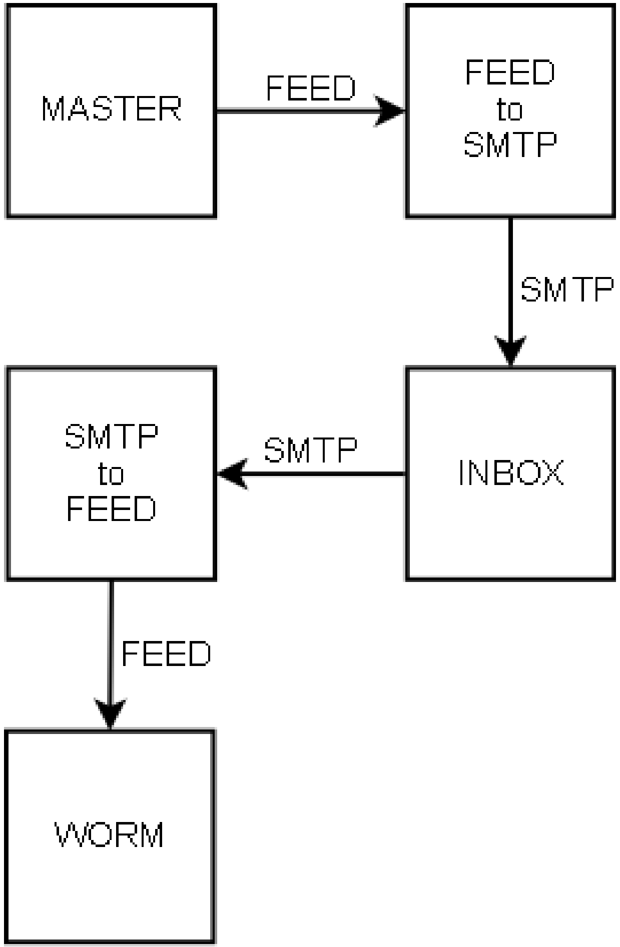
Wormoholic :: Samy



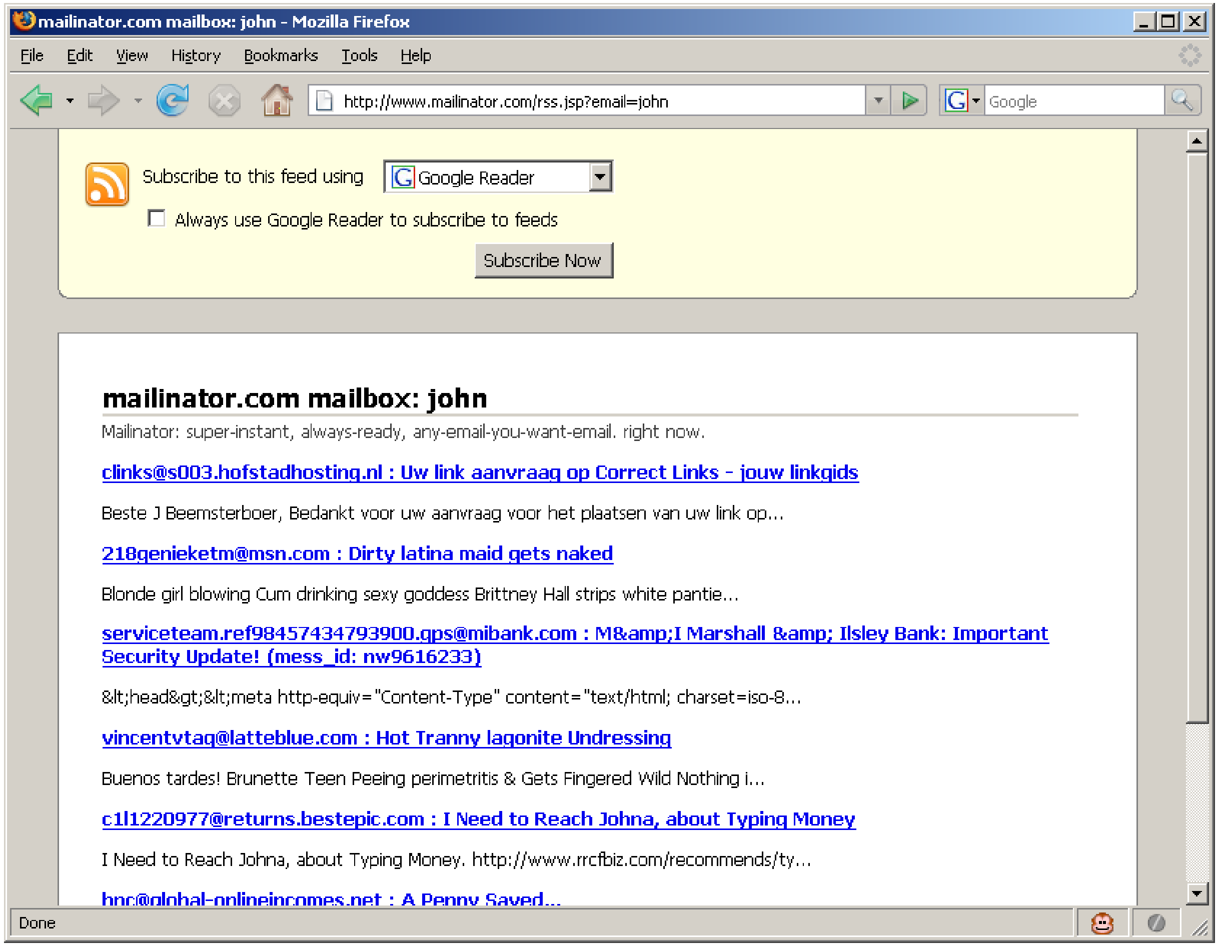
Wormoholic :: Covert Channels

- Obfuscate feed path
- Purpose:
  - To monitor
  - To hide worm control channel
  - To control
- Technology:
  - Feed Readers (Google Reader, etc)
  - Mixers (Google Reader, Yahoo Pipes, etc)
  - Forwarders (RSS to Mail, Mail to RSS)

Wormoholic :: The Covert Diagram



Wormoholic :: Mailinator Forwarder


mailinator.com mailbox: john - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.mailinator.com/rss.jsp?email=john
Google

Subscribe to this feed using Google Reader

□ Always use Google Reader to subscribe to feeds

Subscribe Now

mailinator.com mailbox: john

Mailinator: super-instant, always-ready, any-email-you-want-email. right now.

clinks@s003.hofstadhosting.nl : Uw link aanvraag op Correct Links - jouw linkgids

Beste J Beemsterboer, Bedankt voor uw aanvraag voor het plaatsen van uw link op...

218genieketm@msn.com : Dirty latina maid gets naked

Blonde girl blowing Cum drinking sexy goddess Brittney Hall strips white pantie...

serviceteam.ref98457434793900.gps@mibank.com : M&amp;I Marshall &amp; Ilsley Bank: Important Security Update! (mess_id: nw9616233)

&lt;head&gt;&lt;meta http-equiv="Content-Type" content="text/html; charset=iso-8...

vincentvtaq@latteblue.com : Hot Tranny lagonite Undressing

Buenos tardes! Brunette Teen Peeing perimetritis & Gets Fingered Wild Nothing i...

c1l1220977@returns.bestepic.com : I Need to Reach Johna, about Typing Money

I Need to Reach Johna, about Typing Money. http://www.rrcfbiz.com/recommends/ty...

hnc@global-onlineincomes.net : A Penny Saved...

Done

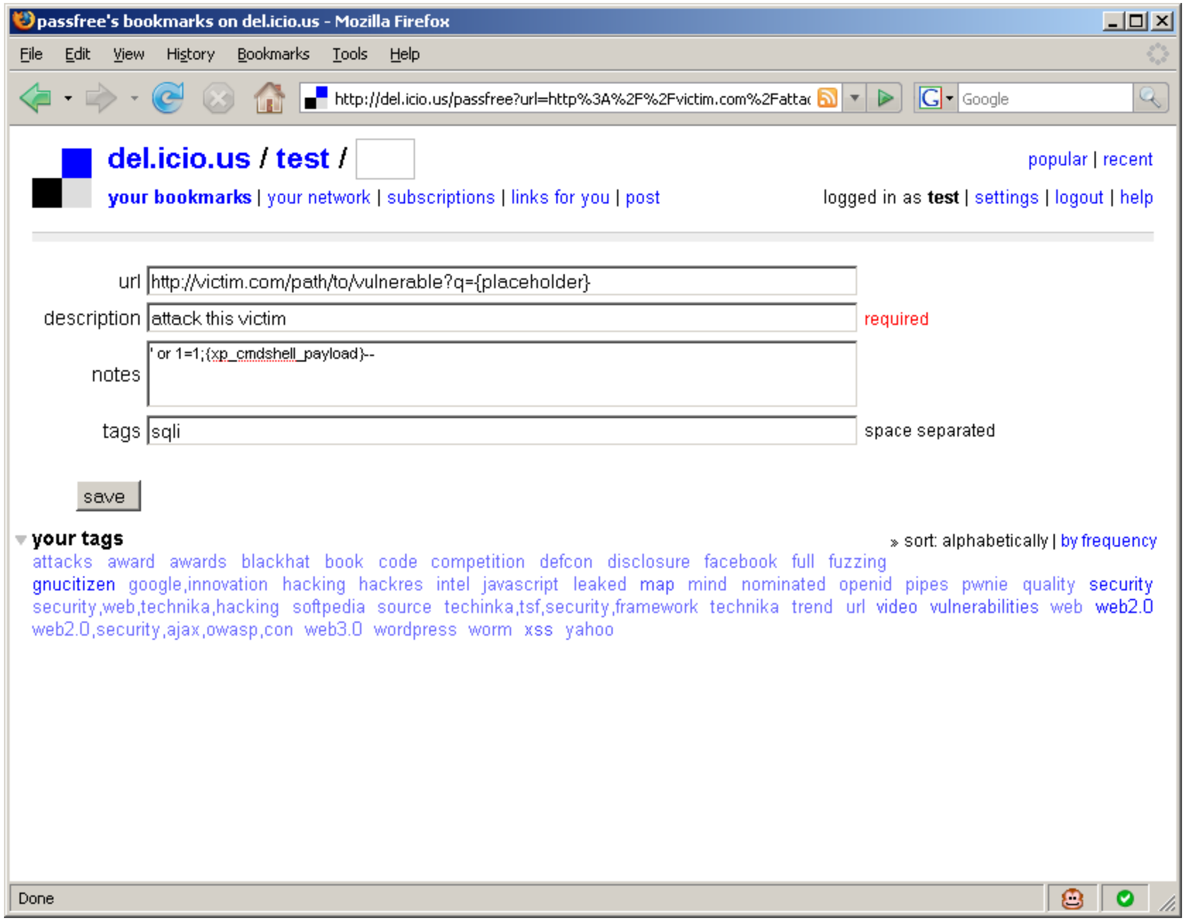
Wormoholic :: The Mechanical Turk

- What is it?
  - Dumb machine that looks smart
- Applied to malware!
  - Dumb viral code that looks smart
- What is the trick?
  - Syndication
  - Automatic Discovery

Wormoholic :: Syndication

- Bookmarking sites can hold the description of the attack
- The data can be contributed by multiple authors
- The data can be consumed as a feed or any other syndication mechanism

Wormoholic :: Syndication Example



passfree's bookmarks on del.icio.us - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Done

http://del.icio.us/passfree?url=http%3A%2F%2Fvictim.com%2Fattac

del.icio.us / test /

popular | recent

your bookmarks | your network | subscriptions | links for you | post

logged in as **test** | settings | logout | help

url	http://victim.com/path/to/vulnerable?q={placeholder}	
description	attack this victim	required
notes	' or 1=1;{xp_cmdshell_payload}--	
tags	sqli	space separated

save

your tags

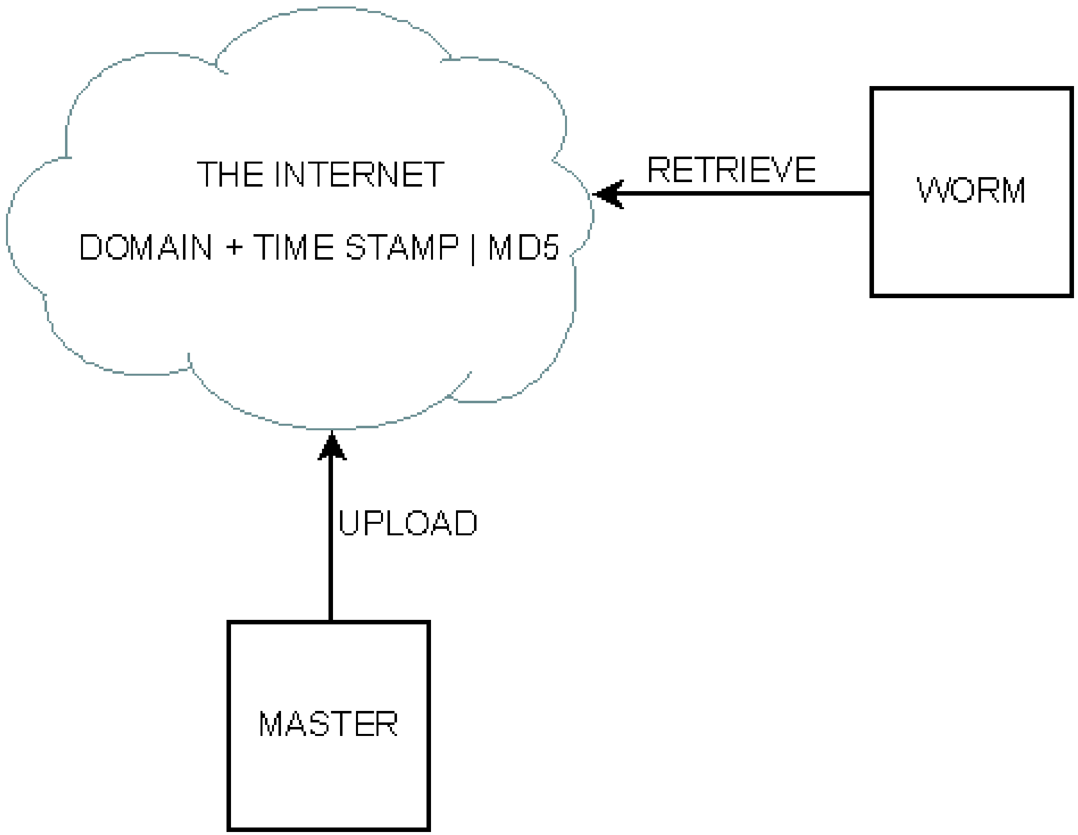
» sort: alphabetically | by frequency

attacks award awards blackhat book code competition defcon disclosure facebook full fuzzing gnucitizen google,innovation hacking hackres intel javascript leaked map mind nominated openid pipes pwnie quality security security,web,technika,hacking softpedia source techinka,tsf,security,framework technika trend url video vulnerabilities web web2.0 web2.0,security,ajax,owasp,con web3.0 wordpress worm xss yahoo

Wormoholic :: Automatic Discovery

- Search Engines can deliver messages to surface agents in a distributed manner
- Cannot be easily prevented
- AJAX Search APIs to the rescue
- Queries are sometimes very very very generic
- Example:
  - The master says: **WORM DOMAIN + FUTURE TIME STAMP | MD5**
  - The worm looks for: **CURRENT DOMAIN + CURRENT TIME STAMP | MD5**

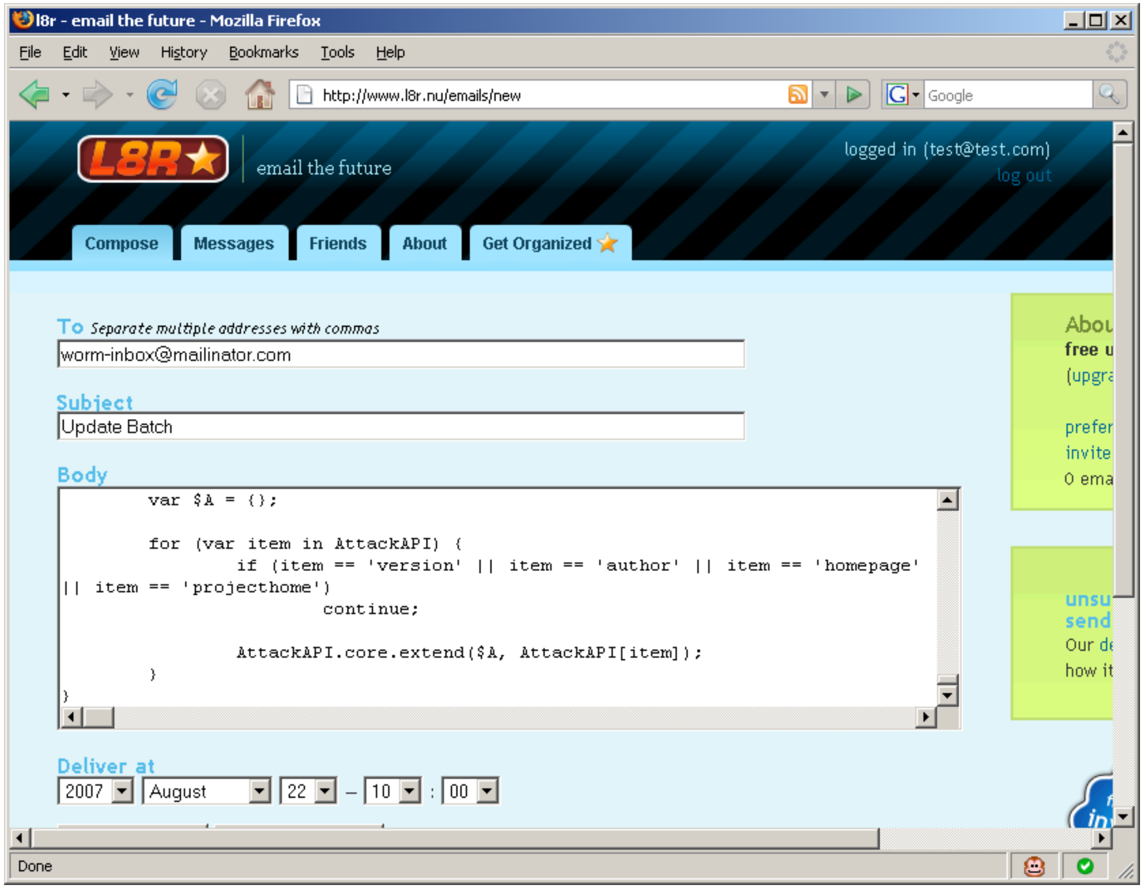
Wormoholic :: Message Broadcasting Diagram



Wormoholic :: Scheduling and Logical bombs

- Actions can be taken at given time
- Mimics traditional logical bombs but a lot more powerful when mixed with AJAX
- Time management services are freely available on the Web:
  - Google Calendar
    - Calendars are available as feed
  - L8R
    - Can schedule future e-mails
    - Messages can be taken out as a Feed

Wormoholic :: L8R


l8r - email the future - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.l8r.nu/emails/new
Google
L8R
email the future
logged in (test@test.com)
log out
Compose
Messages
Friends
About
Get Organized
Abou
free u
(upgra
prefer
invite
0 ema
unsu
send
Our de
how it
Done

To *Separate multiple addresses with commas*
worm-inbox@mailinator.com

Subject
Update Batch

Body

```
        var $A = {};

        for (var item in AttackAPI) {
                if (item == 'version' || item == 'author' || item == 'homepage'
|| item == 'projecthome')
                        continue;

                AttackAPI.core.extend($A, AttackAPI[item]);
        }
}
```

Deliver at
2007 August 22 – 10 : 00

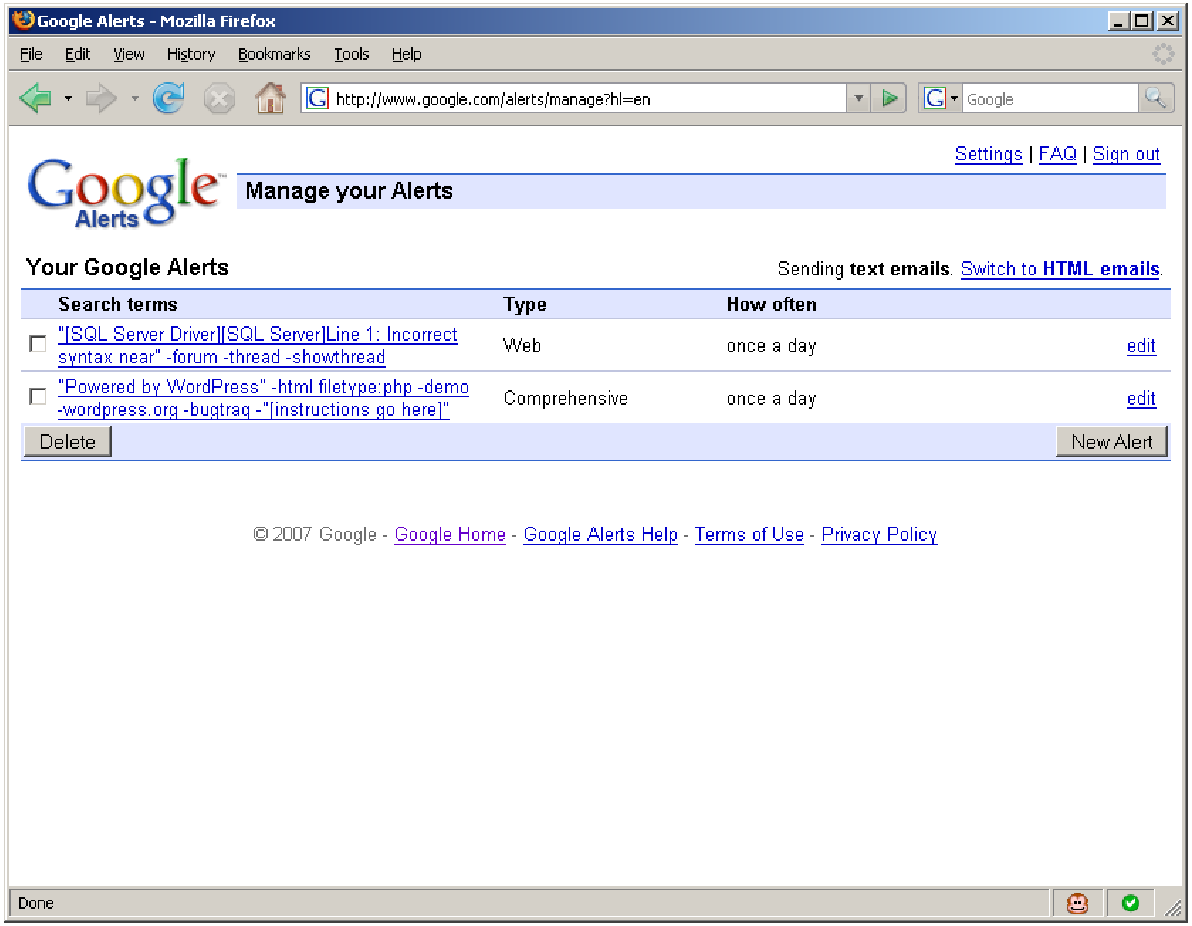
Wormoholic :: Push down target discovery

- Find patterns in targets
- Configure server to look for these targets
  - Use legitimate service like Google Search, Yahoo Search and the all mighty Google Alerts
- Push the results to worms

Wormoholic :: Google Alerts

- Place strategic Google Dorks into the alerting system
- Supply payload within the dork body:
  - "Powered by WordPress" -html filetype:php -demo -wordpress.org -bugtraq -"[instructions go here]"
- Forward Google Alert emails to any mail client that can export to feed, such as Malinator, DodgIt and Mailbucket
- Consume the result with the surface agent
- Hide

Wormoholic :: Google Alerts Interface


Google Alerts - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Settings | FAQ | Sign out
Google Alerts
Delete
New Alert
Done

http://www.google.com/alerts/manage?hl=en

Manage your Alerts

Your Google Alerts

Sending **text emails**. Switch to **HTML emails**.

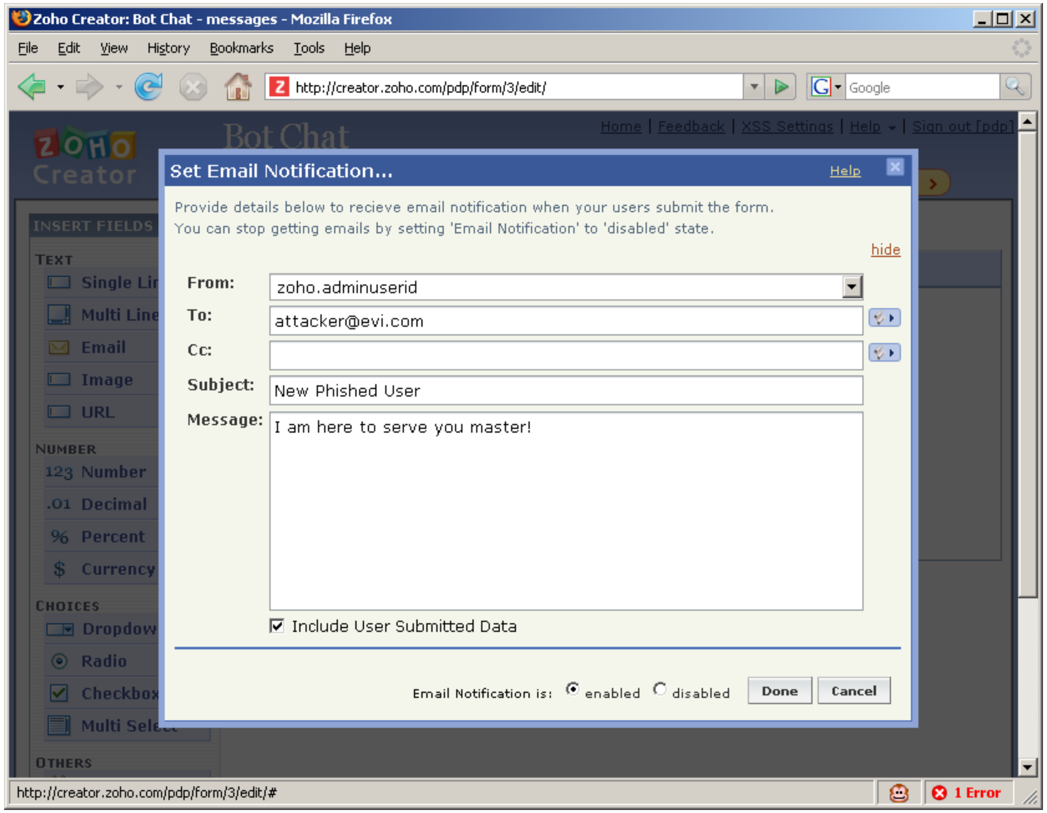
	Search terms	Type	How often	
□	"[SQL Server Driver][SQL Server]Line 1: Incorrect syntax near" -forum -thread -showthread	Web	once a day	edit
□	"Powered by WordPress" -html filetype:php -demo -wordpress.org -bugtraq -"[instructions go here]"	Comprehensive	once a day	edit

©2007 Google - Google Home - Google Alerts Help - Terms of Use - Privacy Policy

Wormoholic :: Data storage

- Web2.0 has many services (DabbleDB, Zoho Creator), which allow you to create AJAX applications powered by a backend database
- These services are completely legitimate but can be abused for malicious purposes
- Example:
  - Viral code communication systems
  - Easy phishing infrastructures
    - Phish credentials, Upload to database, Send confirmation e-mail, All via AJAX

Wormoholic :: Zoho Creator



Zoho Creator: Bot Chat - messages - Mozilla Firefox

http://creator.zoho.com/pdp/form/3/edit/

Set Email Notification...

Provide details below to recieve email notification when your users submit the form.
You can stop getting emails by setting 'Email Notification' to 'disabled' state.

From:	zoho.adminuserid
To:	attacker@evi.com
Cc:	
Subject:	New Phished User
Message:	I am here to serve you master!

☑ Include User Submitted Data

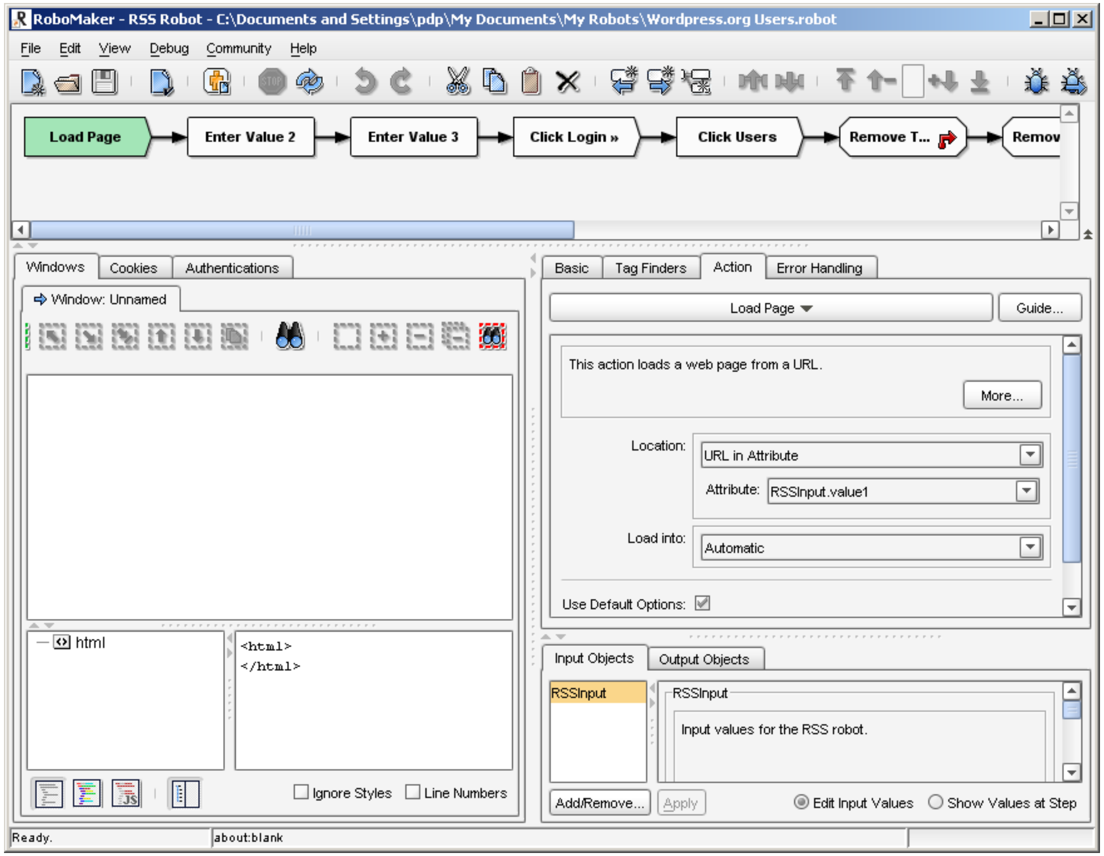
Email Notification is: ● enabled ○ disabled

http://creator.zoho.com/pdp/form/3/edit/#

Wormoholic :: Robots

- Web2.0 centric
- Work where JavaScript fails
- Most vivid members:
  - Dapper
    - Scrapper
  - Openkapow
    - Can scrape
    - Can spider
    - Can perform basic and form based authentication
    - Can call XML-RPC and SOAP services
    - Can execute JavaScript (server-side)

Wormoholic :: Openkapow



```
<html>
</html>
```

This action loads a web page from a URL.

Location: URL in Attribute

Attribute: RSSInput.value1

Load into: Automatic

Use Default Options: ☑

RSSInput

Input values for the RSS robot.

● Edit Input Values ○ Show Values at Step

Wormoholic :: Robot Exploits

- Services like Dapper and Openkapow allow attackers to write exploits and deploy them on-line
- Once a target is identified, attackers will ping the robot to do the dirty job
- Robots can be invoked from client-side JavaScript and ActionScript
- Examples:
  - Wrote one that exploits Wordpress SQL Injection
  - There is one at Openkapow that logs into any Wordpress and dumps account details

Wormoholic :: The Conclusion

- You've seen Samy?
- You've seen Yamaner?
- It could have been worse!

Bookmarks Rider

- The Story:
  - Tow ways to make money:
    - By Ad-jacking
    - By hooking users on a botnet
- The Technology:
  - Social Bookmarking Services
  - Javascript
  - XSS

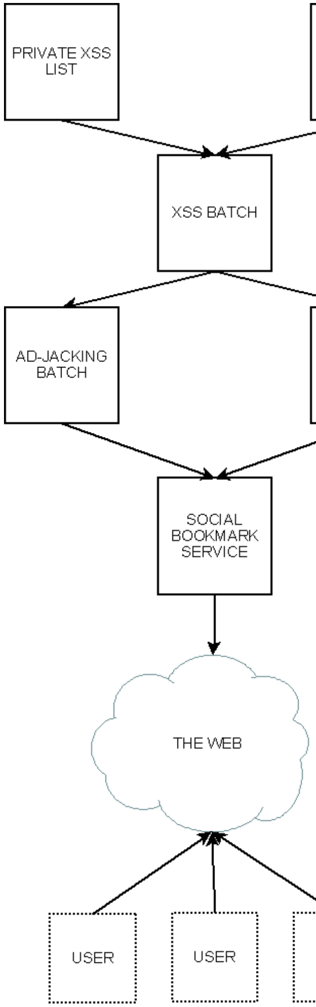
Bookmarks Rider :: State and Persistence

- What is state?
- What is persistence?
- How to use bookmarks to create semi-persistent state
- Why social bookmarks:
  - Because they are social
  - Because people like to click on them

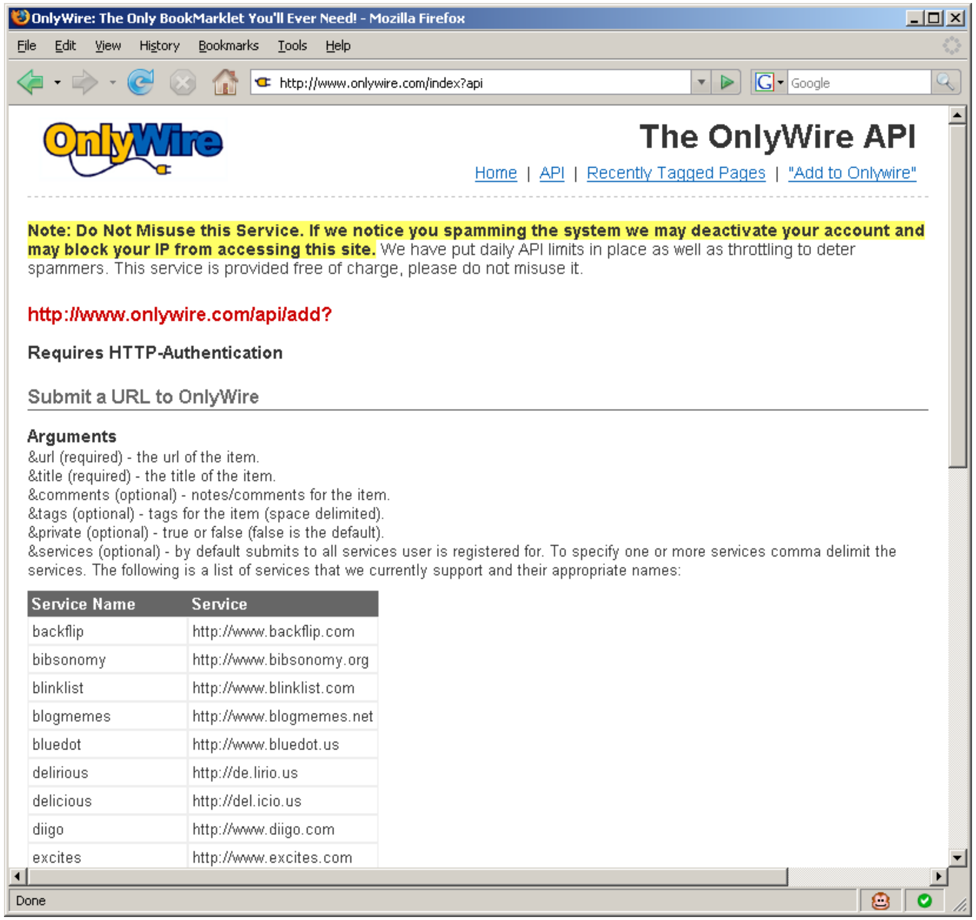
Bookmarks Rider :: The Trick

- Find a bunch of XSS vulnerabilities
- Get even more from database like XSSDB.com
- Write two types of payloads:
  - One to exploit Ad-Jacking
  - One to exploit the Client
- Send the bookmarks across all social bookmarking sites
- You can use services such as OnlyWire

Bookmarks Rider :: Process Diagram



Bookmarks Rider :: OnlyWire



OnlyWire: The Only BookMarklet You'll Ever Need! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.onlywire.com/index?api
Google
OnlyWire
Done

The OnlyWire API

Home | API | Recently Tagged Pages | "Add to Onlywire"

Note: Do Not Misuse this Service. If we notice you spamming the system we may deactivate your account and may block your IP from accessing this site. We have put daily API limits in place as well as throttling to deter spammers. This service is provided free of charge, please do not misuse it.

http://www.onlywire.com/api/add?

Requires HTTP-Authentication

Submit a URL to OnlyWire

Arguments
&url (required) - the url of the item.
&title (required) - the title of the item.
&comments (optional) - notes/comments for the item.
&tags (optional) - tags for the item (space delimited).
&private (optional) - true or false (false is the default).
&services (optional) - by default submits to all services user is registered for. To specify one or more services comma delimit the services. The following is a list of services that we currently support and their appropriate names:

Service Name	Service
backflip	http://www.backflip.com
bibsonomy	http://www.bibsonomy.org
blinklist	http://www.blinklist.com
blogmemes	http://www.blogmemes.net
bluedot	http://www.bluedot.us
delirious	http://de.lirio.us
delicious	http://del.icio.us
diigo	http://www.diigo.com
excites	http://www.excites.com

Bookmarks Rider :: Conclusion

- Attackers can steal vulnerable sites ad revenue
- Attackers can take advantage of the attacked site status and popularity in order to exploit unaware visitors
- Services such as OnlyWire can distribute hundreds of thousands of links a day
- Social sites and bookmarks are also listed in Google and Yahoo search index
  - Check GNUCITIZEN

RSS Kingpin

- The Story:
  - Is about splogging
- The Technology:
  - Blogs
  - Feeds
  - Trackbacks
  - Pingbacks
  - Aggregators

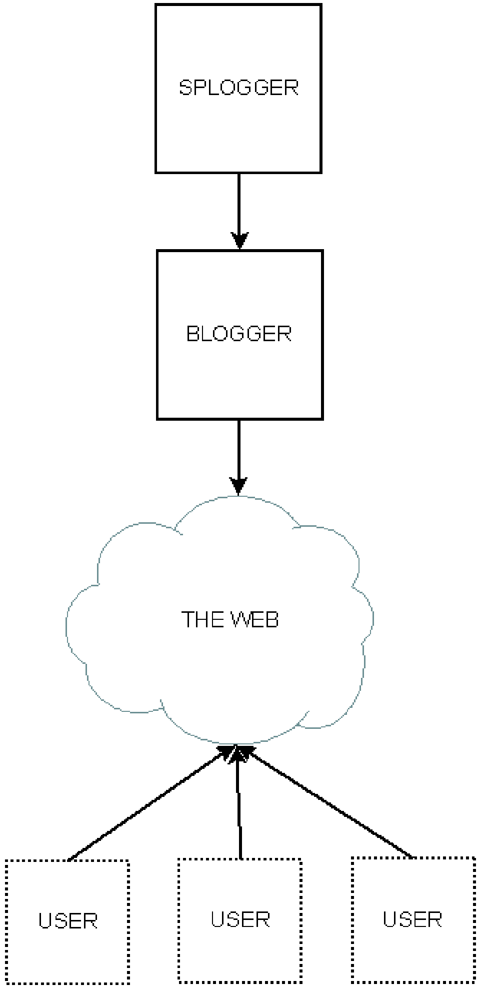
RSS Kingpin :: What is sploggin?

- Splogging is SPAM logging
- It is applicable to Blogs
- It is applicable to data aggregators
- Splogging is suitable to get a large user base
- The user base will subscribe to the splog feeds and redistribute the content even further

RSS Kingpin :: Why Splogging?

- To control
- To reach
- To distribute
- For magnitude

RSS Kingpin :: Splogging in Action



RSS Kingpin :: How to Splog?

- For Wordpress:
  - Learn python
  - Learn the XML-RPC python bindings
- For Blogger:
  - Learn python
  - Learn the GData python bidnings

RSS Kingpin :: Conclusion

- Attackers can easily distribute malware to millions of machines
- Attackers can easily control splog networks through RSS and ATOM
- Splogging is easy and really hard to fight against
- Splogging = Botnet

Revealing the hidden Web

- The Story:
  - John needs to penetrate Krenos Network
  - He has one week time to find as much as possible about the target
- The Technology:
  - XML
  - Yahoo My Web Search
  - Yahoo Site Explorer PageData
  - Yahoo Site Explorer Ping

Revealing the hidden Web :: The Trick

- Get the range of Ips
- Do light scan and discover Web services
- Make sure that you are looking for weird ports such as 8001, 8080, 8888, etc.
- Compile a list of URLs
- Use Yahoo Site Explorer service to ping each URL
- Wait for Yahoo Spider to craw the hidden resources

Revealing the hidden Web :: The Trick

- Bulk upload all URLs into Yahoo My Web search service
- Query for interesting data

Revealing the hidden Web :: Another trick

- Spam search engines by:
  - Making use of Dark SEO techniques with:
    - Blogger
    - Google Pages
- Spam social bookmarking sites
- Spam social sites
- Wait for search engines to spider
- Query

Revealing the hidden Web :: Conclusion

- Legit services can be abuse for malicious purposes
- Attackers can harvest data by making use of powerful infrastructures in undesired ways
- All it is required is a little bit of imagination from the attacker's side
- Everything else is free

…more

- Profiling targets by watching their Web activities
- Snoop onto targets
- GEO Position Mobile phones
- GEO Position individuals
- More service abuse
- More vulnerabilities
- More Insecure

Conclusions

- Web2.0 security is not only about AJAX
- In Web2.0, security problems are not necessarily data validation problems
- Sometimes, it is irrelevant whether servers are vulnerable or not. The data can be retrieved anyway
- Non-executable stacks and other types of software security features are only helpful when attackers want to compromise your computer. Your data is still on the Web

More Conclusions

- It is all about who has the information
- It is all about who can find the information
- Information is everything. It is the most valuable digital asset
- Web2.0 makes attackers lives a lot easer
- Web2.0 is not bad but new security problems will emerge
- When must learn how to see to the general picture