Xploiting Google Gadgets: Gmalware and Beyond

Robert Hansen

Tom Stracener

DRAFT: Complete slides will be made available after our talk.

The **Dark Side** of Gadgets

Xploiting Google Gadgets: Gmalware and Beyond
Tom Stracener & Robert Hansen (Rsnake)

Complete slides will be made available after the our talk on August 8th.

If today’s malware mostly runs on Windows because it’s the commonest executable platform, tomorrow’s will likely run on the Web, for the very same reason. Because, like it or not, Web is already a huge executable platform, and we should start thinking at it this way, from a security perspective.

PDP, Architect, GNUCITIZEN, quoting Giorgio Maone

XSS hole in gmodules.com

Vulnerability documented by Rsnake in 2007

“http://ha.ckers.org/blog/20070817/xss-hole-in-google-apps-is-expected-behavior/””

XSS was never fixed and is never going to be fixed

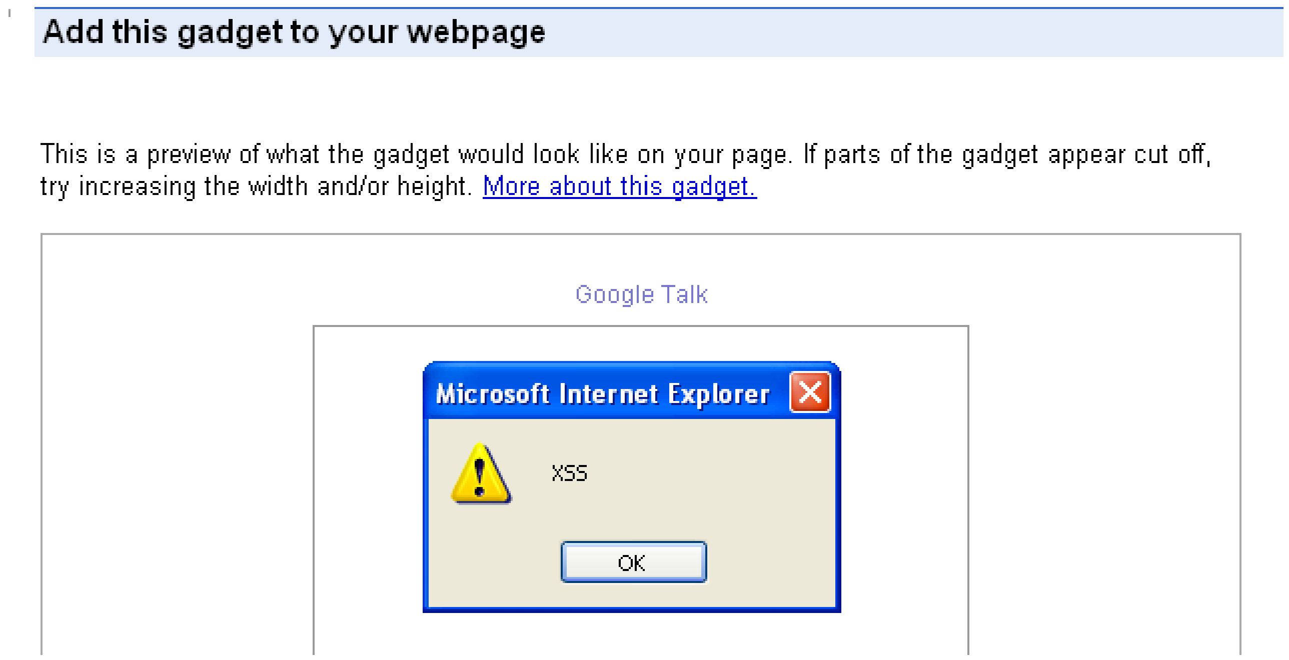
***Rsnake** reported the vulnerability to Google and finally Disclosed its existence to the public after dialog with google*

Those of you that havent read Rnsake’s blog are probably wondering why?

Cross-Site Scripting is a serious vulnerability, so why was it ignored?

XSS So what?

- Execute arbitrary code
  “Use javascript and HTML to craft custom payloads”
- Content Spoofing
  “Make users believe that content is legitimate when in fact it is controlled by an attacker with malicious intent.”
- Phishing
  “Steal user passwords by faking login portals to web-based services, devices, or web sites.”


Add this gadget to your webpage

This is a preview of what the gadget would look like on your page. If parts of the gadget appear cut off, try increasing the width and/or height. More about this gadget.

Arbitrary Javascript executes whenever the user follows a link to the gadget or if the gadget is embedded within a web page.

XSS is Expected Behavior…

Google's Argument (one line)

We need javascript, we can't turn it off, so arbitrary execution of javascript is part of the expected behavior

On further review, it turns out that this is not a bug, but instead the expected behavior of this domain. Javascript is a supported part of Google modules, as seen, for example, here: http://www.google.com/apis/maps/documentation/mapplets/#Hello_World_of_Mapplets. Since these modules reside on the gmodules.com domain instead of the Google domain, cross-domain protection stops them from being used to steal Google-specific cookies, etc. If you do find a way of executing this code from the context of a google.com domain, though, please let us know.

Google’s Argument

Google’s Reasoning is as flawed…

We are going to spend a few minutes and take their reasoning apart piece by piece and then show you why they are wrong.

Google's Argument

Our Format is designed to help you follow the logic flow (shown below)

Premise (Source): Content

We have done our best to faithfully summarize Google's position from the dozens of emails we we have exchanged.

Google's Reasoning about the XSS Vuln (Domain Argument)

<u>Premise(Google):</u> Gmodules is a different domain
From Google or Gmail.

<u>Premise (Google):</u> You can only attack Gmodules
with this vulnerability

<u>Conclusion (Google):</u> The vulnerability is insignificant

Response: This begs the questions *that there is nothing worth exploiting on gmodules*, and *that phishing attacks should not be a concern.*

Google's Reasoning about the XSS Vuln (Resemblance Argument)

Premise(Google): Gmodules does not look like a Google domain

Premise(Google): Users who would follow a link to Gmodules (a google domain) would be just as likely to follow a link to BadGmodules (not a Google domain).

Conclusion(Google): Fixing the vulnerability would not reduce risk to the user

Response: *Does Gmail look like a Google domain?*

Google's Reasoning about the XSS Vuln (Expected Behavior)

Premise(Google): Gmodules needs javascript to serve and cache Gadgets

Premise(Google): There is no harm in using javascript to host our Gadgets

Conclusion(Google): The XSS is expected behavior and should not be fixed.

Response: The issue is 1) not javascript, but javascript security.
2) Placing additional security measures could make the hosted code more Secure. 3) The current architecture creates an environment of significant risk.

Impact of Gmodules XSS

1. Attackers can exploit the Gmodules XSS to attack Google Gadgets and potentially the users desktop

2. Attackers can use Gmodules as a place to host their malware

This makes it virtually impossible to tell bad or dangerous gmodules code from good or safe code.

3. Attackers can use gmodules as a host for Phishing sites

Understanding Google™ Gadgets

Part of a new world view of *how the web* should operate…

Gadgets are often talked about in ideological terms

Google Seed Money!

Google Gadgets Overview

1. Simple to build

“” create gadgets that include tabs, Flash content, persistent storage, dynamic resizing, and more”

2. Access and Run on Multiple Sites

“Your gadget can run on multiple sites and products including iGoogle, Google Maps, Orkut, or any webpage.”

3. Reach Millions of Users

“Gadgets are viewed millions of times per week and generate significant traffic”

Google Gadgets Social Design

“OpenSocial is built upon gadgets,so you can build a great viral social app with little to no serving costs.”

- Viral Spread via ‘Social Graph’

  Gadget-as-a-Meme

2. Decentralized Architecture Distributed Processing

   Gadget-as-an-Agent

3. Content Rich, Self-Expression

   Gadget-as-Expression

http://code.google.com/apis/opensocial/articles/bestprac.html

Google Gadgets Social Design

4. Dynamic, Organic Change

   Gadget-as-an-Organism

5. Expose the Activity Stream

   Gadget-as-'Social Information'

   Gadget-as-a-'Record of Activity'

6. Browse the Social Graph

   Gadget-as-Graph

   - *Monitoring without centralization*

http://code.google.com/apis/opensocial/articles/bestprac.html

Google Gadgets Social Design

7. Drive Interactions and Communication

    Gadget-as-Communication

8. Build Relationships and Communities

    Gadget-as-a-Community

9. Solve Real World Tasks

    Gadget-as-Tool

    - *Problem Solving*
    - *Revenue Generating*

http://code.google.com/apis/opensocial/articles/bestprac.html

Types of Google Gadgets

1. Gadgets for iGoogle

3. Gadgets for the web

5. OpenSocial API

7. Desktop Gadgets

http://code.google.com/apis/gadgets/

High Level Security Concerns

Gadgets can be easily weaponized into attack tools or payloads

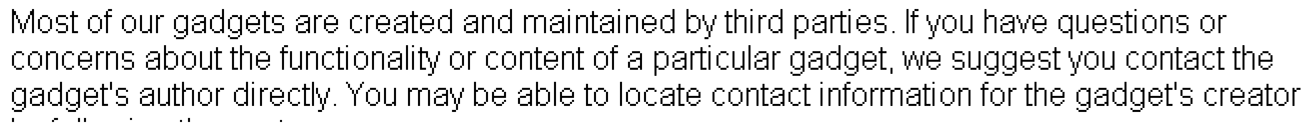
Gadgets are largely 3rd party code and potentially malicious

Gadgets can attack other gadgets, the desktop, or web sites

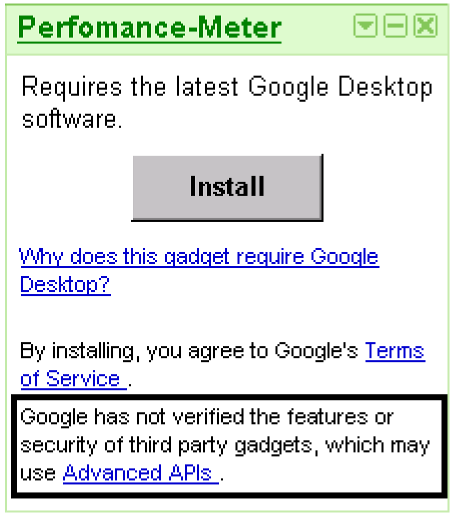
Gadgets can have (most of) the same vulnerabilities as web applications

Disturbing Disclaimers: Gadget FAQ

What if my Gadget is broken or displays offensive or inappropriate content?



Most of our gadgets are created and maintained by third parties. If you have questions or concerns about the functionality or content of a particular gadget, we suggest you contact the gadget's author directly. You may be able to locate contact information for the gadget's creator



Perfomance-Meter

Requires the latest Google Desktop software.

Install

Why does this gadget require Google Desktop?

By installing, you agree to Google's Terms of Service .

Google has not verified the features or security of third party gadgets, which may use Advanced APIs .

Gadgets Threat Model

- **Javascript/HTML/Script Injection**

  -Gadget-to-Gadget Vectors

  -Gadget-to-Desktop Vectors

2. **Defacement**

   -Content/Data Manipulation Attacks

3. **Poisoning**

   -Data Pollution

   -Social Graph Attacks

   -’click fraud’ correllaries

Gadgets Threat Model

4. **Content/Gateway Spoofing**

   -Masquerading, Redirection

   -Gateways to other apps

   -Phishing

5. **Surveillance/Spyware**

   -Spyware/Adaware

   -User tracking/monitoring

   -Unauthorized Data collection & Export

6. **Exposures**

   -Exposing "low-interaction" user data

   -Personal information theft + leaks

Gadgets Threat Model

7. **Malware "Gmalware"**

   -targeted attacks, DDOS

   -Cookie Theft, Zombies

   -Exploits, Wrappers

   -Browser attacks + Hijacking

8. **Worms**

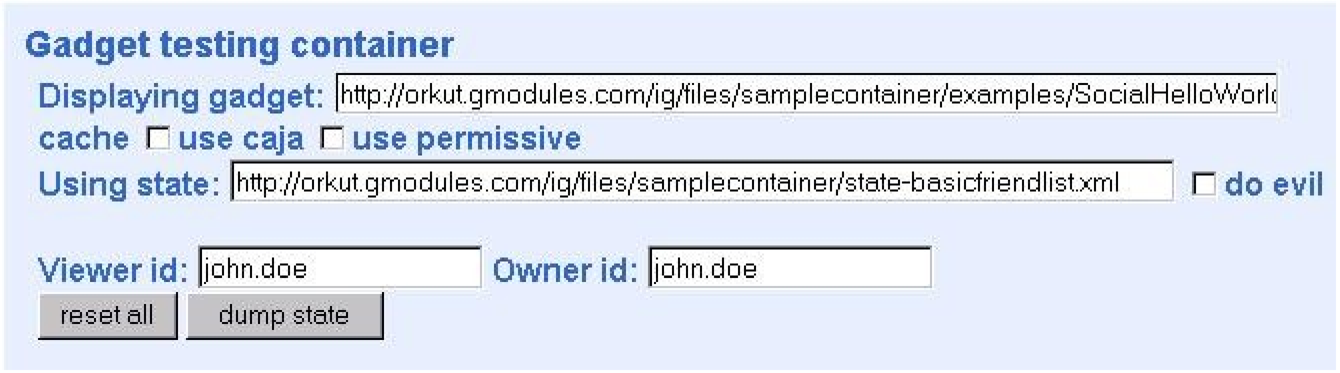
   -Social Networks

9. **Abusive/Coercive Functionality**

   -Tracking gadgets, privacy concerns, unfriendly gadgets

Developer Humor

Take a close look at the Gadget's *Options*. Someone at Google has a sense of humor…



Gadget testing container

Displaying gadget: http://orkut.gmodules.com/ig/files/samplecontainer/examples/SocialHelloWorl

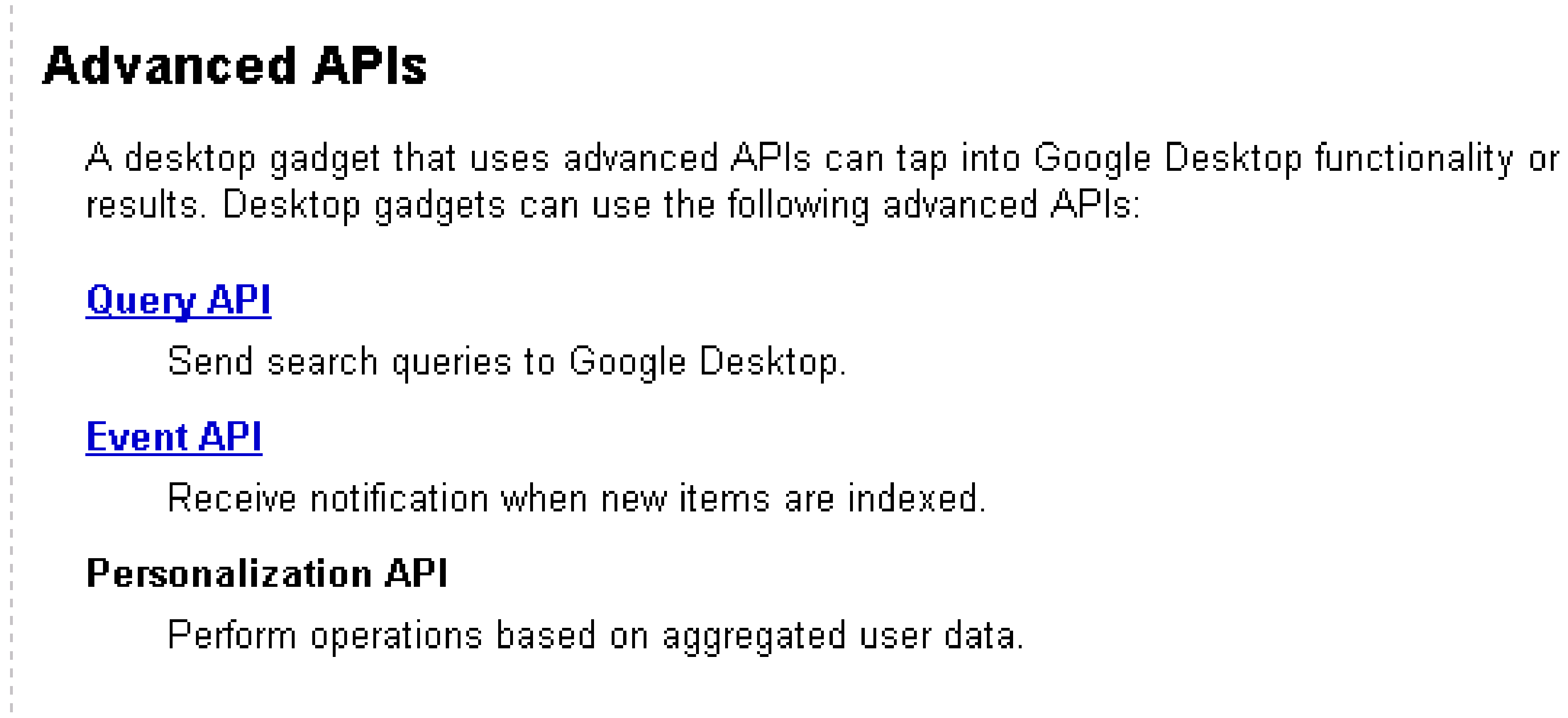
cache ☐ use caja ☐ use permissive

Using state: http://orkut.gmodules.com/ig/files/samplecontainer/state-basicfriendlist.xml ☐ do evil

Viewer id: john.doe Owner id: john.doe

Lets run this with the **"Do Evil"** Option…

Advanced API



Advanced APIs

A desktop gadget that uses advanced APIs can tap into Google Desktop functionality or results. Desktop gadgets can use the following advanced APIs:

Query API

Send search queries to Google Desktop.

Event API

Receive notification when new items are indexed.

Personalization API

Perform operations based on aggregated user data.

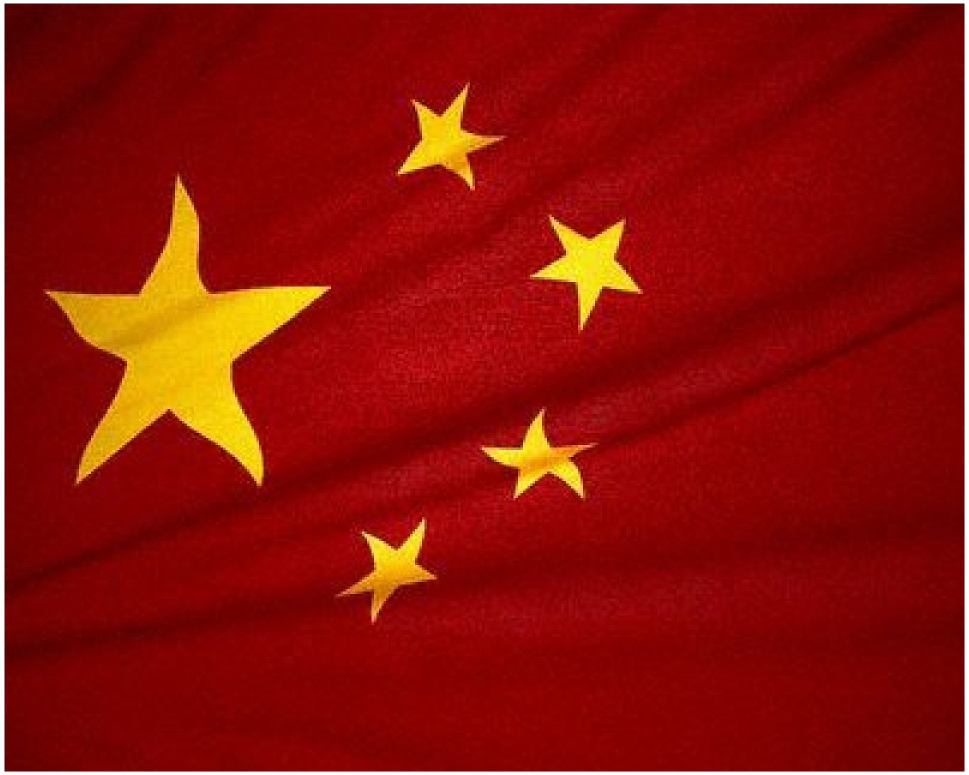
hxxp://desktop.google.com/en/dev/advancedapi.html

Example Gadgets and POCs

We will discuss example gadgets in several Categories.

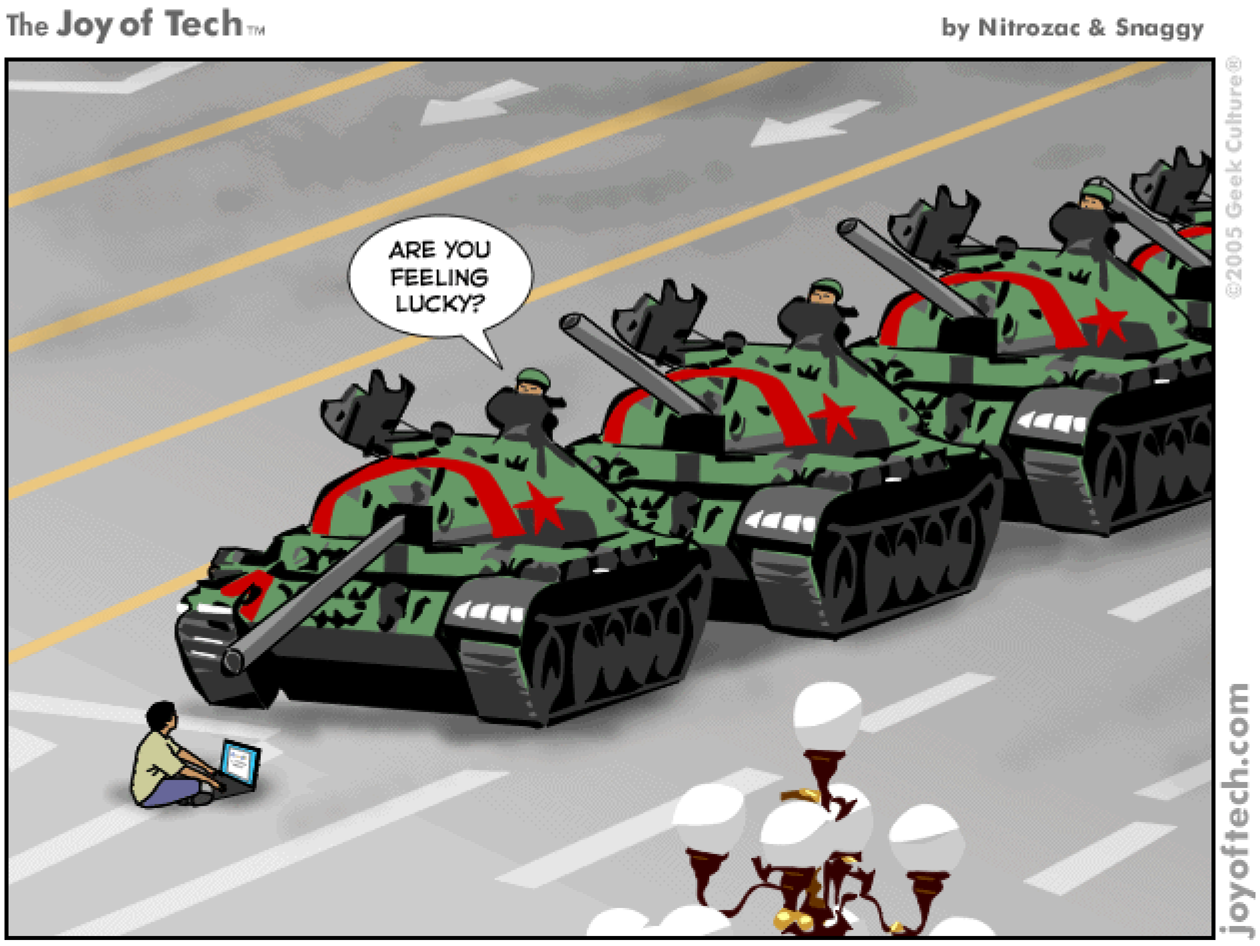
- Not every Gadget or Gmalware we will discuss has a POC
- Gadgets are introduced in no particular order
- Gadgets fall into general categories (e.g., Gmalware, WHGs)

The People’s Gadget…



Crackdown Gadget..

The People's Gadget…



Google in China... search no evil?

The People’s Gadget…

M.U.S.H.U!

- **Monitors** feeds/web sites for subversive content
- **Uploads** search terms and IP address to state server
- **Spiders** Web Sites from which content originates and determines how “Red” a domain is
- **Hinders** freedom movements and suppresses Anti-Communist rhetoric
- **Updates** state database with data from the “Social Grid”

Yahoo Site Explorer Spider Gadget

1. Port of PDPs Yahoo Spider Gadget

On this page you will find a small POC (Proof of Concept) of a client-side (only JavaScript) spider that is based on the top of Yahoo Site Explorer PageData service

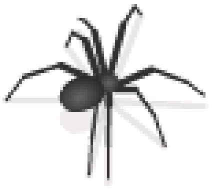
2. Gadget

We created a gadget for PDPs spider example

3. Client-Side JS Spider

The Page Data service allows you to retrieve information about the subpages in a domain or beneath a path that exist within the Yahoo! index.

Simple PHP Spider Gadget



1. Demonstrates ability to call an external PHP script to include functionality within a Gadget

2. One of a number of useful web hacking Gadgets we've ported

3. Gadget Code & Spider Code is available for download

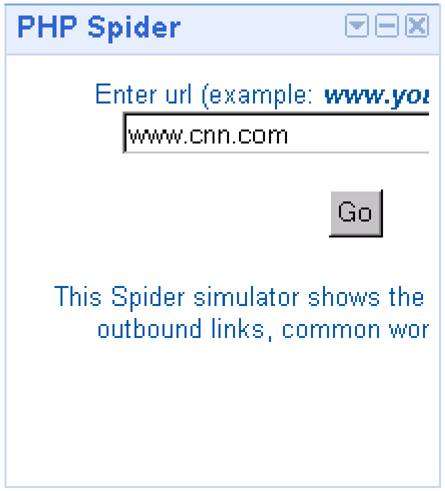
Gadget Spider

http://www.seoish.com/spider-simulator-google-gadget/

Simple PHP Spider

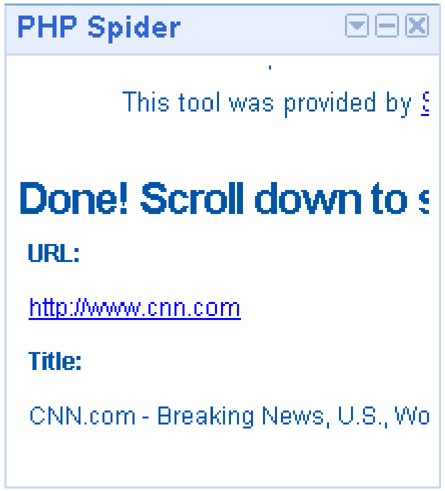
We fetch a PHP script within the Gadget

Configuration Results


PHP Spider

Enter url (example: ***www.yo***
www.cnn.com
Go

This Spider simulator shows the
outbound links, common wor


PHP Spider

This tool was provided by

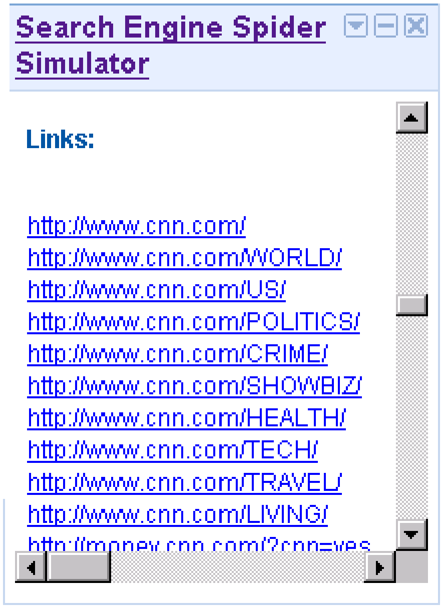
Done! Scroll down to s

URL:

http://www.cnn.com

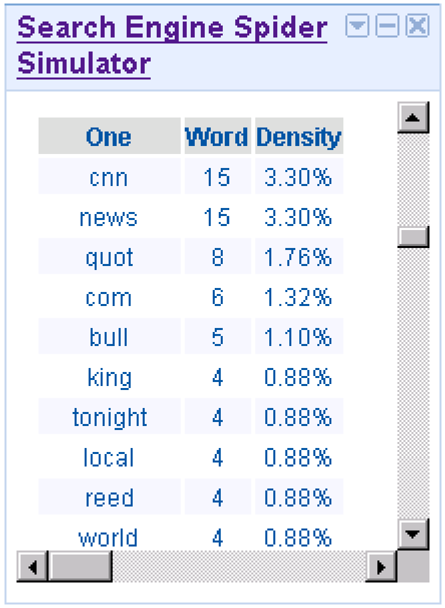
Title:

CNN.com - Breaking News, U.S., Wo


Search Engine Spider Simulator

Links:

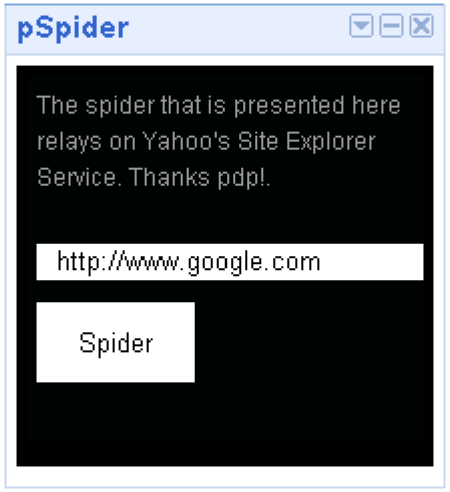
http://www.cnn.com/
http://www.cnn.com/WORLD/
http://www.cnn.com/US/
http://www.cnn.com/POLITICS/
http://www.cnn.com/CRIME/
http://www.cnn.com/SHOWBIZ/
http://www.cnn.com/HEALTH/
http://www.cnn.com/TECH/
http://www.cnn.com/TRAVEL/
http://www.cnn.com/LIVING/
http://money.cnn.com/?cnn=yes


Search Engine Spider Simulator

One	Word	Density
cnn	15	3.30%
news	15	3.30%
quot	8	1.76%
com	6	1.32%
bull	5	1.10%
king	4	0.88%
tonight	4	0.88%
local	4	0.88%
reed	4	0.88%
world	4	0.88%

Yahoo Site Explorer Spider Gadget (pSpider)

Configuration



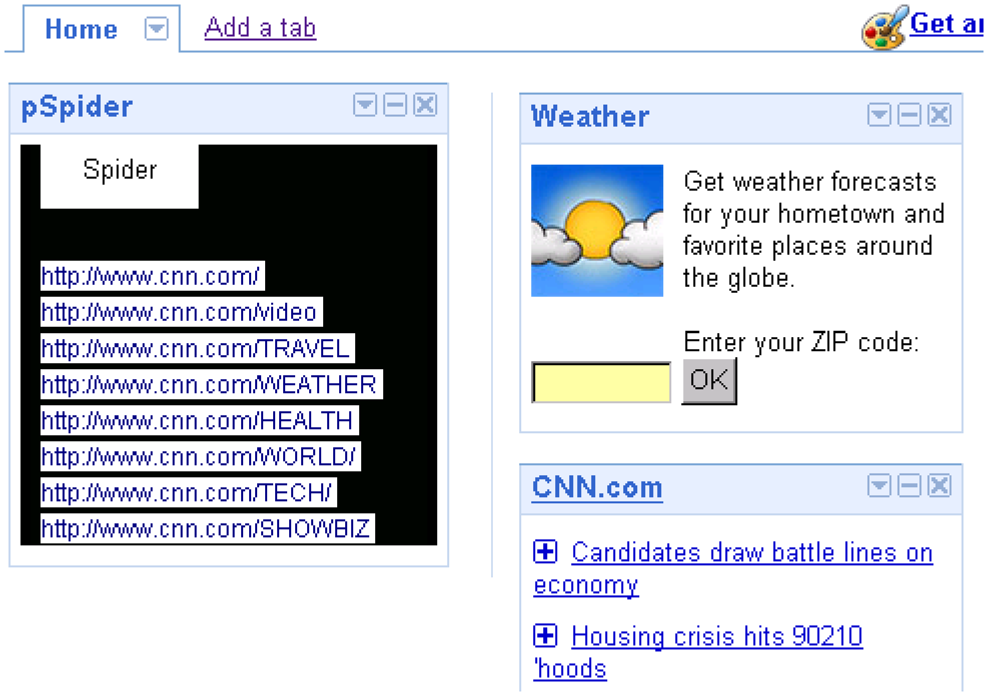
pSpider

The spider that is presented here relays on Yahoo's Site Explorer Service. Thanks pdp!.

http://www.google.com

Spider

Results



Home | Add a tab | Get a

pSpider

Spider

http://www.cnn.com/
http://www.cnn.com/video
http://www.cnn.com/TRAVEL
http://www.cnn.com/WEATHER
http://www.cnn.com/HEALTH
http://www.cnn.com/WORLD/
http://www.cnn.com/TECH/
http://www.cnn.com/SHOWBIZ

Weather

Get weather forecasts for your hometown and favorite places around the globe.

Enter your ZIP code: OK

CNN.com

Candidates draw battle lines on economy

Housing crisis hits 90210 'hoods

hxxp://exgenesis.com/wonderbread/pspider.xml

JS Port Scanner Gadget

1. Demonstrates port scanning via a javascript embedded within a gadget

2. We ported PDPs nice JS Scanner to a Gadget

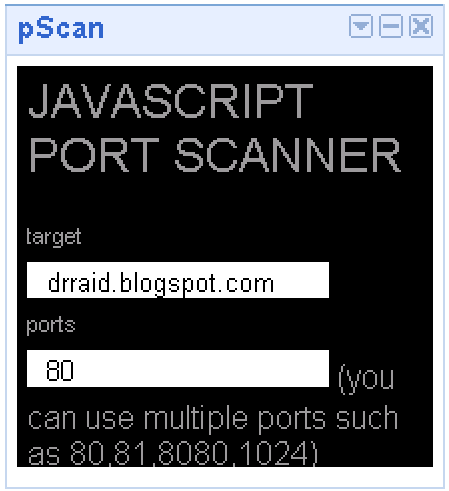
3. Port Scanner Gadget code is available for download

Gadget Port Scanner

JS Port Scanner Gadget

1. pScan Configuration

Results



pScan

JAVASCRIPT PORT SCANNER

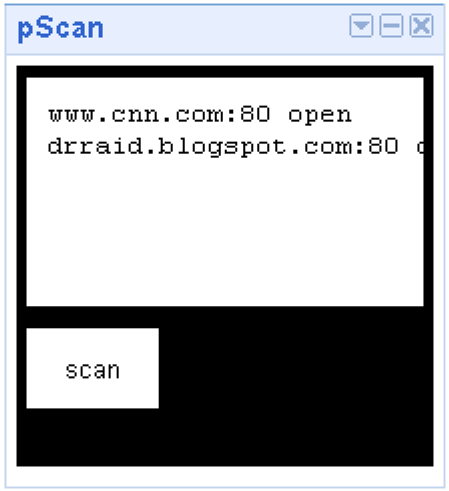
target

drraid.blogspot.com

ports

80

(you can use multiple ports such as 80,81,8080,1024)



pScan

```
www.cnn.com:80 open
drraid.blogspot.com:80 o
```

Gmodules Proxy Cache

hxxp://gmodules.com/ig/proxy?url=

- Vulnerabilities & Insecure Design
  - Proxy is linked to Gadgets functionality for caching purposes when a Gadget is hosted.
  - Can be used to cash arbitrary javascript/HTML rather than just gadgets. Caches code from any domain.
  - Allows ‘one click’ JS execution
  - JS malware persistence

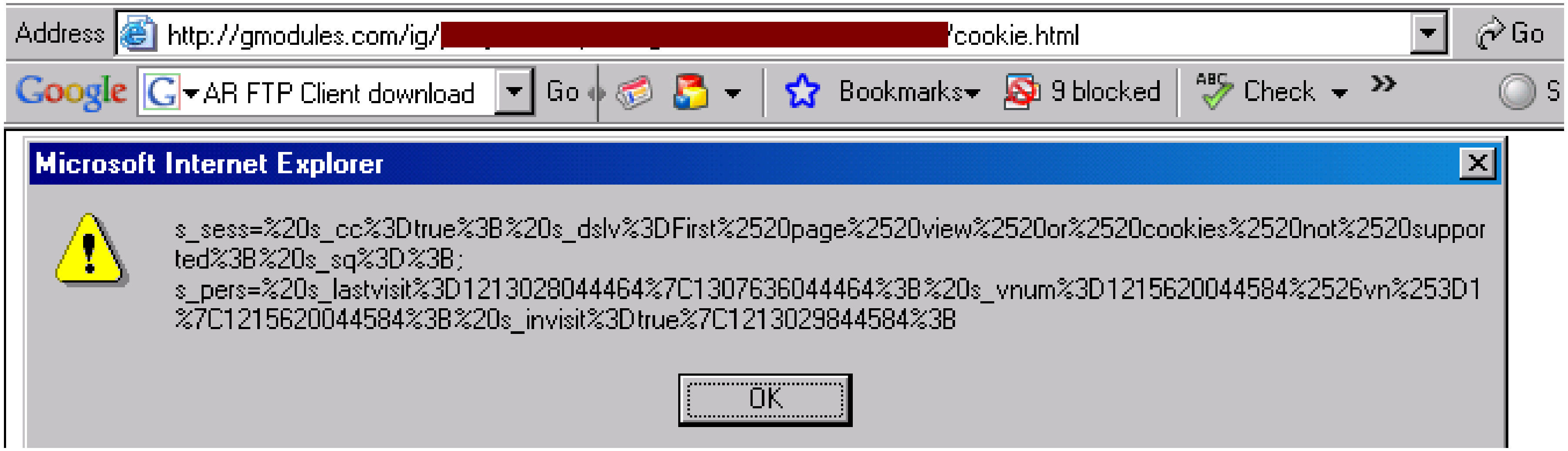
What is the gmodules Proxy Cache?

hxxp://gmodules.com/ig/proxy?url=www.evil.org

- Use of Public Gmodules proxy results in the caching of content on the users machine
- Arbitrary javsascript executes and is cached by the proxy on the local machine
- Locally cached content can be accessed by the originating URL
- Designed for use by Gadgets but can be misused in the payload of any XSS or Phishing attack to give persistence to the payload

Implications of the gmodules Proxy Cache for Gmalware?

- Any javascript construct on the proxied page executes
- Javascript can re-open a connection to the proxy cache and content will be reactivated



Address http://gmodules.com/ig/[redacted]/cookie.html

Microsoft Internet Explorer

```
s_sess=%20s_cc%3Dtrue%3B%20s_dslv%3DFirst%2520page%2520view%2520or%2520cookies%2520not%2520suppor
ted%3B%20s_sq%3D%3B;
s_pers=%20s_lastvisit%3D1213028044464%7C1307636044464%3B%20s_vnum%3D1215620044584%2526vn%253D1
%7C1215620044584%3B%20s_invisit%3Dtrue%7C1213029844584%3B
```

- Persistence: Malicious javascript can remain active indefinitely until reboot.

Cross-Gadget Attacks

1. Gadgets can attack one another, steal cookies and/or data, manipulate the content of other gadgets.

We have recorded a movie of Robert’s attack