Google Toolbar: The NARC Within

“The” Google
What would we do without them/it?
Google Toolbar: The NARC Within

The problem: URLs are the geek tool? URLs, URLs everywhere... Home, work, on the go?
Google Toolbar: The NARC Within

Google Toolbar is the Solution?
Google Toolbar: The NARC Within

Or just a tease?
Google Toolbar: The NARC Within

Of course it's good, it's free!
Google Toolbar: 
The NARC Within

Installs easy..
Stores URLs..
Access them wherever, whenever you need it
No more lost URLs!
Happy!

~SOME DAYS~
they just start better than others
Google Toolbar: 
The NARC Within

Time passes....

You bookmark your discoveries

Happy!
Google Toolbar: The NARC Within

bookmark any pr0n?
Next day at work…

You log in to google and of course use the toolbar with all your handy bookmarked urls.
Corporate Security

You probably have a corporate security department?

They probably watch you?
Corporate Security

Maybe they watch you closely?
Web proxies?
Web filtering?
Web reporting?
What happens when you access the toolbar?

Let's untangle...
Demonstration
What we saw

For every url, google attempts a hit to the favicon.gif or favicon.ico url.
<xml>
  <xml_api_reply>
    <version>1.0</version>
  </xml_api_reply>
  <bookmarks>
    <bookmark>
      <title>
        DEF CON 302/256 Hacking Conference - The Hacker Commun...
      </title>
    </bookmark>
    <bookmark>
      <title>
        Freaky Midgets - We Know How To Get Our Freak On!
      </title>
      <attribute>
        <name>favicon_url</name>
        <value>
          http://www.freakymidgets.com/favicon.ico
        </value>
      </attribute>
    </bookmark>
  </bookmarks>
</xml>
So?

Fascinating!
Corporate Security

Remember they watch you?

Top 10 porn viewers now likely includes you?

Even though you didn't do anything.
Forensics

When they investigate you, what will they see?
Bluecoat

Bluecoat one liner to watch traffic in realtime:

```
```

Pipe it through grep to narrow the target

```
| grep "10.2.2.2" | grep favicon
```
Forensics

index.dat files?

Nope..the toolbar generated the traffic, not IE.
Workarounds

Firefox Plugins to the rescue?:
Places pack from Andy Halford:
SyncPlaces:
CheckPlaces:
SortPlaces:
WebDav or file=rsync
favicon.ico?

Stored in the .json file generated by syncplaces:

{"iconData": [
{"uri":"http://s.com/", "faviconuri":"http://s.com/favicon.ico",
"mimeType": {"value": "image/png"}, "data": [137, 80, 78, 71, 13, 10, 26, 10, 0, 0, 0, 13, 73, 72, .........}
Not so fast…

Retrieve, import bookmarks via syncplaces also triggers Firefox to attempt favicon hits just like Google toolbar.
What to do?

Duh...
quit
looking
at porn!
What else to do?

Or, write some code to straighten up the .json and remove bookmarks that you don't want ending up at work.
Toolbar p0wnage?

So what else can we do with this toolbar information?

Normal user agent:
Toolbar p0wnage?

Quite detailed client version info from google:
Profiling/Dating? (aka stalking)

IP/Bookmark tag cloud from coffee shop wifi?

http://tagcrowd.com/
http://www.wordle.net/create

Python/regex= new tool gtoolbarsnoop.py?
tcpdump -i eth0 -s0 -w - port 80| ./gtoolbarsnoop.py --icons --titles -f -
Demonstration
What else?

Deleted

Bookmarks?!
Allocated bookmark:

```xml
<bookmark>
  <title>Yahoo!</title>
  <url>http://www.yahoo.com/?r0=1277010878</url>
  <timestamp>1277012340477390</timestamp>
  <id>17266698985382022972</id>
  <attributes>
    <attribute>
      <name>favicon_url</name>
      <value>http://www.yahoo.com/favicon.ico</value>
    </attribute>
  </attributes>
</bookmark>
```
Bookmark forensics

Deleted bookmark:

```xml
<Bookmark>
  <Title>BP Global | BP</Title>
  <Url>http://www.bp.com/bodycopyarticle.do?categoryId=1&contentId=7052055</Url>
  <Timestamp>1277010823575646</Timestamp>
  <Id>17521067242763822402</Id>
  <Labels>
    <Label>^k</Label>
  </Labels>
  <Attributes>
    <Attribute>
      <Name>favicon_url</Name>
      <Value/>
    </Attribute>
    <Attribute>
      <Name>favicon_timestamp</Name>
      <Value>1277006535</Value>
    </Attribute>
  </Attributes>
</Bookmark>
```
Shocking
Sad
What to do?
Questions?