Google Hacking
Making Competitive Intelligence Work for You

Tom Bowers
President Philadelphia InfraGard
Managing Director, Security Constructs, LLC
Competitive Intelligence

1. What is it?
2. How is it done?
3. Is it legal?
4. How do we prevent it?
### Asking Questions

#### Basics
- Who
- What
- When
- Why
- Where
- How

#### “Godiva Chocolatier Inc”
- What business is it in?
- How big is it?
- Where are they located?
- Is it publicly traded?
- What are the annual sales and growth?
- Pending legal issues?
- Who are the decision makers?
Refining the Search

1. Use “intitle” versus “inurl” (looking for dirt)
2. Scour news sites and newsgroups
3. Check financial filings
4. Check security analyst reports
5. Use Google Groups and Blogs
Google Tools

Google Answers (retired)  answers.google.com
Google Scholar          scholar.google.com
Google Earth            earth.google.com
Google Patent Search    www.google.com/patents
Google Blog Search      blogsearch.google.com
Google Alerts           www.google.com/alerts
Google Maps             maps.google.com
Google Maps – Satellite

Wyeth Pharmaceuticals - Collegeville, PA

550 Arvida Rd, Collegeville, PA
Ph: (610) 902-1000

*.. On Tuesday, April 22, 2008, Wyeth announced 2008 First Quarter Financial Results and held a conference call to discuss earnings. Click here for further information... wyeth.com
Google Earth – 3D Satellite

3 Levels:
Free
Plus - $20
Pro - $400
1. Auto traffic
   1. Manufacturing schedules
   2. Production cycles

2. Parking lot analysis – personnel
   1. Executives – dedicated parking
   2. Department Heads – early arrivals

3. Security arrangements

4. Plant expansion
View Operationally:
- Type of Equipment
- OS used / vulnerabilities
- Personnel traffic
- Business Operations
Google Alerts
Constant Information Leakage Monitoring (counter-intelligence)

Note that some search terms are “explicit” and others are not.
Additional Google Related Tools

• Open Directory Project
dmoz.org

• ResearchBuzz
www.researchbuzz.org

• TouchGraph GoogleBrowser
www.touchgraph.com/TGGoogleBrowser.html
ResearchBuzz

News about search engines, databases, and other information collections.

2007 03 13

Time to Search, Search With Time

Hey, this is pretty neat. Time Search is designed to allow you to search for information based on time with location or a theme. Check it out at http://www.timesearch.info.

Make sure you have JavaScript turned on because this site doesn’t work well without it. Click on the buttons to pick an area if you like (broken down by continent, with sub-areas available, you can also choose World) and pick a theme if you like (technology, war, politics, religion, society, etc.)

If you’re REALLY feeling specific, choose which timelines sites to search (click on the Timeline Sites button at the bottom of the query box) then choose the year you want to search and BC or AD.

I chose 78 AD, worldwide, no themes, no restrictions on site. I got a timeline as a search result. The timeline starts at 78 AD (Titus is emperor) and goes as far as 175 (Constantine takes on emperor). These are the simple listings. Extended listings cover about a paragraph and as you might imagine are much more extensive. Sometimes the listings leave out a fact or two, the first entry says “Titus becomes emperor” but even the extended listing doesn’t say OF WHERE.

Now you know and I know, but does everybody know?

Each listing has several icons to the right and left. One set of icons are blue and will take you to text-based search results for several different resources based on keywords in the timeline listing. (For example, the first entry in my search result might have text search links for Titan, Vesuvius, “Roman Empire”, etc.) The other set of icons links directly to Google Image search results for selected words in the timeline entry.
Notice that this is a spreadsheet. With the search terms highlighted.
Metadata analysis
Using Metadata Assistant

Author
Creation dates...

Hidden Hyperlinks
Additional points of data leakage
1. Conduct CI on yourself – your competitors are
   1. Build a competitive profile
   2. Who are the movers and shakers
   3. Lines of business……..
2. What type of information is leaking and from where?
3. Can a business process be modified?
4. Active disinformation? (running equipment at odd times…)
5. Will a new policy help? (business or security)
6. Can I leverage existing security technologies?
7. Are there new technologies?
1. **Los Alamos and Oak Ridge Spear Phishing attack**
   1. Visitor database only
   2. 12 different attackers, 7 emails to 1000's of employees
   3. Which scientist visited, how often and what is their expertise.
   4. Allows us to build a competitive profile of the type of research being done at these facilities and by extension what type of research these facilities are capable of.

2. **What about your business?**
   1. Whaling Attack – phishing your executives
   2. Specific companies
   3. Specific groups within a company
      1. Who are the movers and shakers
      2. Email addressing schema (look and feel)
      3. Who do these people normally talk to
      4. Detailed contact information
      5. Similar to Executive Recruiters today
What Can I Learn?

**Tariff Rates**

<table>
<thead>
<tr>
<th>Daily plans</th>
<th>Per Use plans</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Price</strong></td>
<td><strong>Price</strong></td>
</tr>
<tr>
<td>Daily</td>
<td>Monthly</td>
</tr>
<tr>
<td><strong>0.55€</strong></td>
<td><strong>0.29€</strong></td>
</tr>
<tr>
<td><strong>0.15€</strong></td>
<td><strong>0.07€</strong></td>
</tr>
<tr>
<td><strong>0.08€</strong></td>
<td><strong>0.04€</strong></td>
</tr>
<tr>
<td><strong>0.05€</strong></td>
<td><strong>0.02€</strong></td>
</tr>
<tr>
<td><strong>0.03€</strong></td>
<td><strong>0.02€</strong></td>
</tr>
<tr>
<td><strong>0.02€</strong></td>
<td><strong>0.01€</strong></td>
</tr>
<tr>
<td><strong>0.01€</strong></td>
<td><strong>0.00€</strong></td>
</tr>
</tbody>
</table>

*Quantity of proxies involved in monthly payment.
**Quantity restriction on proxies which you can use for a day
***Tariffs have a refund system implied to a proxy that goes dead while work

**PAYMENT IS ACCEPTED VIA:** Webmoney, Egold

**Support (only in English) & demo accounts:** ICQ : 555019, 990100

**Terms of Service**

**Peculiar Properties of Tariff Rates:**

**per use:**
The *Per Use Tariff Rate* includes one month payment; the payment involves a certain amount of proxy servers which you can take from the base as many as you wish without any restrictions. If you have not used the proxies included in the monthly payment, these proxies are not extended to the next month. In these Tariffs you can see all proxies which are online at a moment.

**Daily:**
The *Daily Tariff Rate* includes one month payment; the amount of proxy servers which you can take from the base within 24 hours is limited in your Tariff Rate-related quantity. With these Tariff Rates, you can see all proxy servers which are online at a moment. If the system finds out for the first 10 minutes of using a proxy that the proxy has stopped responding, this proxy will not be billed, and the system will automatically refund you.

*Typically, this time is enough to see if a proxy can go on working.

**At present the system is working in a test mode.

**Information about Proxy Helper:**
Proxy Helper manual (ENGLISH VERSION)

**PROHIBITED:**
1. Account may not be used by more than 1 person (Daily Tariff Rates)
2. Proxy Helper may not be used by more than 1 person (All Tariffs)
3. A proxy server may not be used for mass mailing (not only in terms of spam)
4. A proxy may not be taken from the base by using programs other than your browser (Daily Tariff Rates)
Interpretation

- Investors
  - Organized Criminal Activity
  - Other Groups
    - Business Plan Ideas
    - Project Managers
    - Malware Consultants (Specialists)
      (same sub boxes as before)
    - Distribution Mechanisms (Conduits)
      (same sub boxes as before)
    - Victim’s Data
      (same sub boxes as before)
    - Data Conversion into Cash
    - Money Mules
- Guarantors
Flexible Protection Architecture

1. Policies
2. Procedures
3. Contracts
4. Vendor selection
5. Auditing
6. Active Protections
7. Passive Protections
Conclusions

• If its on Google its probably public information
• Google has many tools built in
• Many tools are built on Google APIs
• Always start with "the question."

Then refine, research, refine...
• Don't forget the documents themselves
• Build a profile, use it to improve your security
Questions?

Tom.Bowers@securityconstructs.com