GlobaLeaks

A brief analysis of whistleblowing and GlobaLeaks
What we want to do

• **Develop** a platform for interaction between whistleblowers, editors and node maintainers

• **Easy** setup and maintenance
  – Allows a diversification of leak sites based on geography and areas of expertise

• Build a knowledgebase on setup, maintenance and promotion of the local leak sites for the **node maintainer**

• Knowledgebase for **whistleblower** support

• We are all **random GlobaLeaks contributors**.
Different kinds of Leak Sites

- Editing & publishing leak site
- Raw data publishing leak sites
- Leak amplification leak sites

Different leak sites have different risk levels

It is a collective effort to create an analysis of the different existing:
- leak sites
- whistleblowing organizations
- whistleblowing activities
- whistleblowing laws
GlobaLeaks: Disclaimer

• We do not receive leaks and we do not publish leaks

• We are developing a software and designing a leaking methodology

• PLEASE DO NOT SEND US YOUR LEAKS!
WikiLeaks workflow

- leaker protection
- leak filtering (ham/spam)
- leak management
- leak validation
- information rationalization
- leak publishing
- leak resilience
- media coordination

- Reduced risks and resources
- The organization takes responsibility
- Can be easily taken down by authorities (or censored)
- Does not scale up to a regional level

The organization assumes responsibility for what is published and how it is organized.

Requires costly IT infrastructure and resources.

Requires human resources.
qualified and professional targets will work together to classify and organize leaks. GlobaLeaks leak filtering (ham/spam) resources are provided by volunteers. leak amplification by sending the leak to targets. leak validation qualified and professional targets will work together to classify and organize leaks. Information rationalization will be handled by the interested media. based on the leak importance/type the interested target will be contacted. leak publishing will be handled by the interested media. Will be handled by the interested media. based on the leak importance/type the interested target will be contacted. leak acquisition resources are provided by volunteers. NGOs, journalists, activists, bloggers will be handled by the interested media. Democratic tool for democracy. Secure bridge between leaker and target. Does not take responsibility. Scale up to regional leak level. Takedown resistant. Crowdsourcing leak acquisition by sending the leak to targets. Democratic tool for democracy. Secure bridge between leaker and target. Does not take responsibility. Scale up to regional leak level. Takedown resistant.
GlobaLeaks: goals

- Develop a platform for interaction between whistleblowers, editors and node maintainers
- Easy setup and maintenance
  - Allows a diversification of leak sites based on geography and areas of expertise
- Knowledgebase on setup maintenance and promotion of the local leak site
- Knowledgebase on leaker support
GlobaLeaks: information flow

- Leaker
  - Leak Submission
  - Vidalia
  - Leak node
  - Leak download
  - Vidalia
  - Leak notification
  - Leak publication

- Node Maintainer
  - the node maintainer selects a list of targets
  - A Leak is created
  - Targets are notified via mail

- Media
  - the target is a journalist, NGO, or Blogger
  - he reviews the leak content and analyses it
GlobaLeaks: The whistleblower

- Leaker education

- If the leaker is smart he will be given all the information and technologies to stay safe

- Ideally a leaker will connect via a tor client
  - Or simply with tor2web
GlobaLeaks: The Leak Node

- Easy Setup even for a non-technical crowd
- No payment, or domain names
- Running as Tor Hidden service
- A web interface
GlobaLeaks: The Leak Node

- Knowledgebase for the leaker
-Leaks are tagged
-Each leak node contains a target list with associated tags
- Based on the tags that are selected by leaker, the node will notify the required targets
- The targets are notified with a leank
GlobaLeaks: Node maintainer

- Customize leak site presentation (graphical appearance and some content)
- Selects the target list based on the leak nodes interests and crowd
- He can also be in the list of the targets
- He will also carry on publicity campaigns to promote his leak site
GlobaLeaks: Leanks

• Leak Link

• The method through which a target perceives a leak

• A bit.ly style URL unique for each target

• They are dispatched via email (in a future possibly with other methods)
  – Random delay between each dispatch

• They expire after a fixed or customizable amount of clicks and amount of time
  – To avoid leak link sharing
  – Once expired a blank page is returned
GlobaLeaks: Leanks

- A target can add a password to his leak page, but this is disabled by default

- Two types of leak pages, one containing the actual material the other containing a status page

- The status pages is:
  - used to monitor the impact of the leak
  - useful for a leaker, who can see how many people have downloaded the leak (the risk is higher)

- The actual leak (can be multiple files) is distributed in a packaged format (.zip)
# GlobaLeaks: Leanks

**GlobaLeaks**
Gotham City leak router

<table>
<thead>
<tr>
<th>Gotham City Police department corruption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>tags:</strong> Gotham City, Corruption, Police, Commissioner Gillian B. Loeb, James Gordon</td>
</tr>
<tr>
<td><strong>leak description:</strong> This leak provides evidence that Commissioner Gillian B. Loeb is conspiring. It also contains hard proof of corruption at various levels of the department.</td>
</tr>
<tr>
<td><strong>leak urgency:</strong> Medium-High</td>
</tr>
<tr>
<td><strong>support type:</strong> CD-ROM</td>
</tr>
<tr>
<td><strong>status page:</strong> <a href="http://y/sypaircja/buwwl/onlinen/87438f522803d31065e7bce3c03fe475099631e5607b4d7a09a60c4df5c7">http://y/sypaircja/buwwl/onlinen/87438f522803d31065e7bce3c03fe475099631e5607b4d7a09a60c4df5c7</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Leank status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>leak id:</strong> 87438f522803d31065e7bce3c03fe475099631e5607b4d7a09a60c4df5c7</td>
</tr>
<tr>
<td><strong>Comments:</strong></td>
</tr>
<tr>
<td>618672: I have reason to believe this leak is in fact true. Could the leaker provide details regarding the label on the cd-rom?</td>
</tr>
<tr>
<td>1676827: &quot;classified material 1234&quot;</td>
</tr>
<tr>
<td>8912897: Excellent, just as I suspected! It’s authentic.</td>
</tr>
</tbody>
</table>

this leak was downloaded **42** times
GlobaLeaks: Leanks

- It also provides a channel through which targets can communicate
  - Integrated comment functionality
  - A leaker can also visit the status page and, knowing the risks he will face by doing so, talk with the target and give more details on the leak
  - Discussion channel for leak targets
GlobalLeaks: Organisation

• Being part of the leak process will bring some sort of problems

• By splitting responsibility we demotivate attackers to plan an attack strategy

• There are no specific roles (we are all Random GlobalLeaks contributors)
  – Spokespeople are randomly rotated
  – Code produced is Free Software
  – All encryption and security technology are community produced and tested free software
Conclusions