Impostor

Polluting Tor Metadata

Mike Larsen
Charlie Vedaa

tl;dr

example Snort rule-

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 9030:9031
(msg:"POLICY-OTHER TOR traffic anonymizer server
request"; flow:established,to_server; content:"GET
/tor/server"; fast_pattern:only; classtype:policy-violation;
sid:9324; rev:5;)
```

code can be found here-

https://impostor.io

about us

the issue

https://www.torproject.org/download/download.html#warning

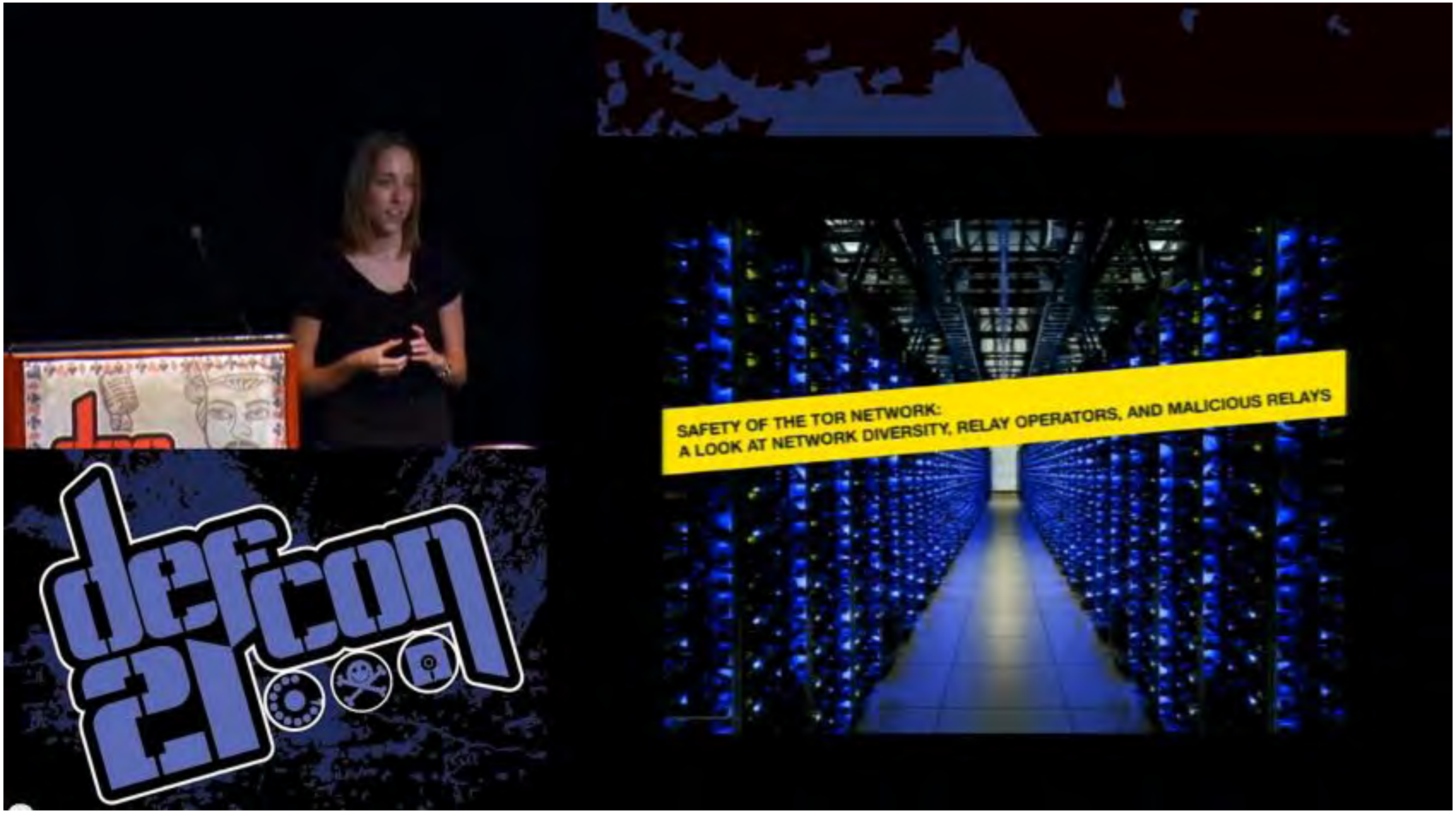
f. **Use bridges and/or find company**

Tor tries to prevent attackers from learning what destination websites you connect to. However, by default, it does not prevent somebody watching your Internet traffic from learning that you're using Tor. If this matters to you, you can reduce this risk by configuring Tor to use a Tor bridge relay rather than connecting directly to the public Tor network. Ultimately the best protection is a social approach: the more Tor users there are near you and the more diverse their interests, the less dangerous it will be that you are one of them. Convince other people to use Tor, too!

the impact

- AFFIDAVIT OF SPECIAL AGENT THOMAS M. DALTON 835 1682 (Harvard bomb threat case)
  - December 16 2013 ~08:30 – Harvard officials receive bomb threat via email
  - “Specifically, Harvard received the e-mail messages from a service called Guerrilla Mail, an Internet application that creates temporary and anonymous e-mail addresses available free of charge. Further investigation yielded information that the person who sent the e-mail messages accessed Guerrilla Mail by using a product called TOR [sic]”
  - “Harvard University was able to determine that, in the several hours leading up to the receipt of the e-mail messages described above, [kid] accessed TOR using Harvard’s wireless network.”

is Tor safe?



SAFETY OF THE TOR NETWORK:
A LOOK AT NETWORK DIVERSITY, RELAY OPERATORS, AND MALICIOUS RELAYS

@runasand

other considerations

- implementations
  - Onion Browser
    https://cure53.de/pentest-report_onion-browser.pdf
    (@0x6D6172696F, @7a_, @insertScript)
- endpoints
  - CVE-2013-1690
    https://community.rapid7.com/community/metasploit/blog/2013/08/07/heres-that-fbi-firefox-exploit-for-you-cve-2013-1690
    (@_sinn3r)

PORTAL

- blocks egress except via Tor
- managed out of band
- https://github.com/grugq/ (@thegrugq)

obfsproxy and FTE

- defaults matter
- https://trac.torproject.org/projects/tor/wiki/doc/AChildsGardenOfPluggableTransports

Tor overview

“”””

- Tor relays publish to directory authorities
- Directory authorities create a consensus of relays
- Clients bootstrap by downloading the consensus
- Clients choose their own network path

“”””

from ‘Anonymity and Censorship: The Tor Network’ (@ln4711 and @ioerror)

detection models

- connections to the Tor network
- connections from the Tor network
- leaking Tor clients

Snort VRT

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 9030:9031
(msg:"POLICY-OTHER TOR traffic anonymizer server request";
flow:established,to_server; content:"GET /tor/server";
fast_pattern:only; classtype:policy-violation; sid:9324; rev:5;)
```

https://gitweb.torproject.org/torspec.git/blob_plain/HEAD:/dir-spec.txt

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 9001:9030
(msg:"POLICY-OTHER TOR proxy connection initiation";
flow:to_server,established; content:"TOR"; content:"client ";
classtype:policy-violation; sid:13696; rev:3;)
```

https://lists.torproject.org/pipermail/tor-talk/2008-November/015471.html (@nickm_tor)

False positives- https://impostor.io/snort_vrt.js

Snort ETOpen

```
alert udp $HOME_NET any -> any 53 (msg:"ET POLICY DNS Query for TOR Hidden
Domain .onion Accessible Via TOR"; content:"|01 00 00 01 00 00 00 00 00 00|";
depth:10; offset:2; content:"|05|onion|00|"; fast_pattern; distance:0;
reference:url,en.wikipedia.org/wiki/.onion; classtype:policy-violation; sid:2014939;
rev:1;)
```

```
alert udp $HOME_NET any -> any 53 (msg:"ET POLICY TOR .exit Pseudo TLD DNS
Query"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|04|exit|00|"; fast_pattern; distance:0;
reference:url,en.wikipedia.org/wiki/.onion; classtype:policy-violation; sid:2014941;
rev:3;)
```

http://www.ietf.org/rfc/rfc1035.txt

10 bytes- flags, questions, anwser RRs, authority RRs, additional RRs
QNAME - each label consists of a length octet followed by that number of octets

Snort ETOpen

```
alert tcp [101.109.17.96,101.55.12.75,103.10.197.50,103.4.19.125,106.186.21.31,
106.187.45.156,106.187.90.158,107.161.153.170,107.161.158.146,107.161.81.187]
any -> $HOME_NET any (msg:"ET TOR Known Tor Exit Node TCP Traffic group 1";
flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; threshold:
type limit, track by_src, seconds 60, count 1; classtype:misc-attack;
flowbits:set,ET.TorIP; sid:2520000; rev:1815;)
```

```
alert udp [101.109.17.96,101.55.12.75,103.10.197.50,103.4.19.125,106.186.21.31,
106.187.45.156,106.187.90.158,107.161.153.170,107.161.158.146,107.161.81.187]
any -> $HOME_NET any (msg:"ET TOR Known Tor Exit Node UDP Traffic group 1";
reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; threshold: type limit,
track by_src, seconds 60, count 1; classtype:misc-attack; flowbits:set,ET.TorIP;
sid:2520001; rev:1815;)
```

False positives- https://impostor.io/snort_et.js

JavaScript pros

- low impact
- easy to opt out
- easy to publish
  - XSS
  - ad networks https://media.blackhat.com/us-13/us-13-Grossman-Million-Browser-Botnet.pdf (@jeremiahg and @mattjay)
  - <script src=“https://impostor.io/all.js" async></script>

JavaScript cons

- XHR limitations
  - http://xhr.spec.whatwg.org/
    “certain headers cannot be set and are left up to the user agent”
- browser prohibited ports
  - prevents cross-protocol scripting
  - ‘The Tangled Web’ pages 190-192 (@lcamtuf)
- little ability to generate UDP traffic

Bro

```
event ssl_established(c: connection )
        {
        if ( c$ssl?$subject && /^CN=[^=,]*$/ == c$ssl$subject && c$ssl?$issuer &&
/^CN=[^=,]*$/ == c$ssl$issuer )
                {
                SumStats::observe("ssl.tor-looking-cert", [$host=c$id$orig_h],
[$str=c$ssl$subject]);
                }
        }
```

https://github.com/sethhall/bro-junk-drawer/blob/master/detect-tor.bro

https://gitweb.torproject.org/torspec.git/blob_plain/HEAD:/proposals/195-TLS-normalization-for-024.txt

False positives- https://impostor.io/bro.js

other detection techniques?

- time synchronization https://tails.boum.org/contribute/design/Time_syncing/
- TBB user-agent https://www.torproject.org/projects/torbrowser/design/#fingerprinting-linkability
- 512 bytes cells https://gitweb.torproject.org/torspec.git/blob_plain/HEAD:/tor-spec.txt

endgame

- is it possible to write rules that cannot be spoofed by a browser?

testing your tools

- verify https://impostor.io doesn’t work
- verify detection does work (e.g. boot Tails)
- .pcap yourself, and identify alerting flow(s)
- look for clues in alert description/details
- just ask

how you can help

- visit https://impostor.io
- test against your security tools
- support the Tor Project https://www.torproject.org/donate/donate

supporting anonymity ain’t easy

- "If your secure communications platform isn’t being used by terrorists and pedophiles, you’re probably doing it wrong. – [REDACTED]“ http://grugq.github.io/blog/2013/12/01/yardbirds-effective-usenet-tradecraft/

summary

- Tor traffic is easy to detect
- detection is easy to fool
- you can help make Tor safer

questions? comments?

https://impostor.io

thanks!

https://impostor.io

@charlievedaa