Spoiled Onions:
Exposing Malicious Tor Exit Relays

Philipp Winter, Richard Köwer, *Martin Mulazzani*, Markus Huber, Sebastian Schrittwieser, Stefan Lindskog, Edgar Weippl

KARLSTADS UNIVERSITET

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

secure
sba-research.org

Outline

This talk is about:

- Detecting malicious Tor exit relays
- Two new exit relay scanners: *exitmap* and *HoneyConnector*
- Several months runtime on the Tor network
- Identified 65 *spoiled onions*

Problem Description

We define a malicious relay to:

- injects or modifys HTML
- conducts MitM (TLS & SSH, ...)
- modifies DNS responses
- credentials reusage (FTP, IMAP, SMTP)

Our solution:

- lightweight and modular exit scanners
- focus: opportunity, impact and history
- open source

Problem Description

We define a malicious relay to:

- injects or modifys HTML
- conducts MitM (TLS & SSH, ...)
- modifies DNS responses
- credentials reusage (FTP, IMAP, SMTP)

Our solution:

- lightweight and modular exit scanners
- focus: opportunity, impact and history
- open source

Related Work

Previous work:

- PETS 2008, "Shining light into dark places": 1 relay
- RAID 2011, "Detecting Traffic Snooping in Tor Using Decoys": 10 relays
- "Snakes on a Tor" (Mike Perry), "tortunnel" (Moxie Marlinspike), numerous others

However, so far:

- Tor network (and the world) has changed since 2011
- no systematic framework to detect active attacks

Related Work

Previous work:

- PETS 2008, "Shining light into dark places“: 1 relay
- RAID 2011, "Detecting Traffic Snooping in Tor Using Decoys“: 10 relays
- “Snakes on a Tor” (Mike Perry), “tortunnel” (Moxie Marlinspike), numerous others

However, so far:

- Tor network (and the world) has changed since 2011
- no systematic framework to detect active attacks

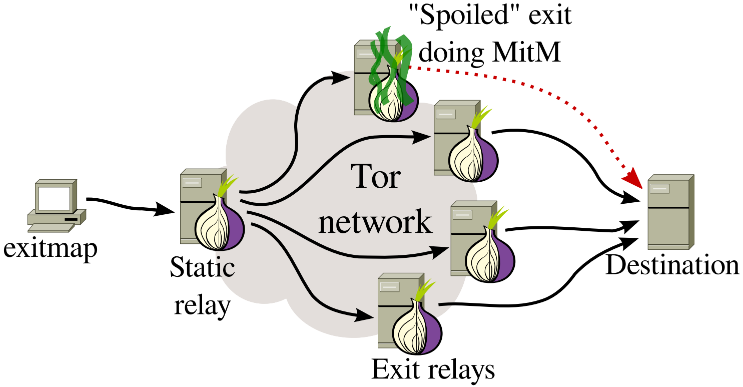
exitmap

Design of *exitmap*:

- detect MitM attacks
- two-hop Tor circuits
- asynchronous & event-driven

Implemented modules:

- HTTPS, SSH, XMPP, IMAPS, DNS, *sslstrip*
- Python & Stem library



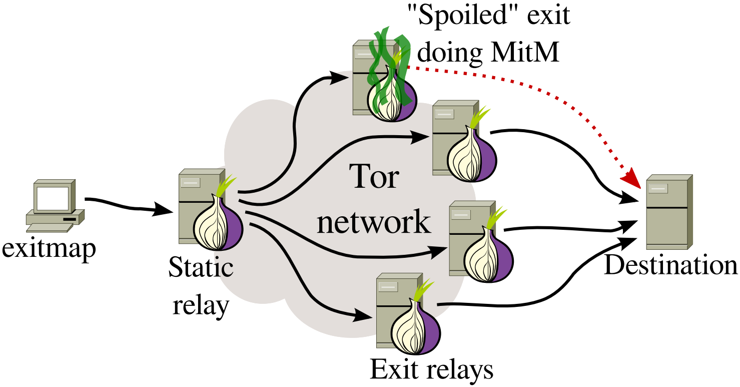
exitmap

Design of *exitmap*:

- detect MitM attacks
- two-hop Tor circuits
- asynchronous & event-driven

Implemented modules:

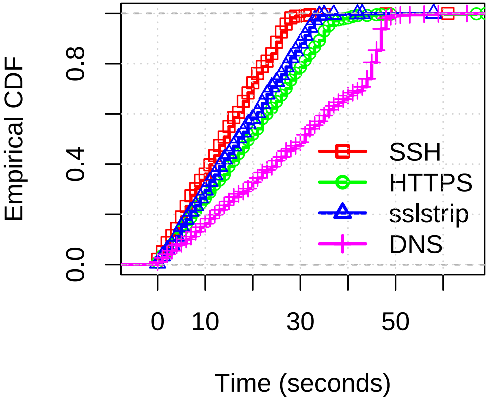
- HTTPS, SSH, XMPP, IMAPS, DNS, *sslstrip*
- Python & Stem library



Performance *exitmap*

Really fast!

- can be configured to spread over time
- on average: 84%-88% of circuits suceeded



exitmap scans

Evaluation:

- September 2013, running 7 months
- several scans per week

Detected **40** malicious relays:

- mostly HTTPS MitM (18)
- some additionally SSH MitM (5)
- many *sslstrip* (9)
- some DNS modifications:
  - DNS censorship (4) in Hong Kong, Malaysia and Turkey
  - OpenDNS (4)

HoneyConnector

Design:

- unique credentials per relay and connection
- full connections
- dummy content
- log inspection for reconnections

Implemented modules:

- FTP (pyFTPdlib)
- IMAP (Dovecot)

HoneyConnector scans

Evaluation:

- October 2013, running 4 months
- popular hosting providers
  - one each for FTP and IMAP
- 54.000 bait connections

Detected **27** malicious relays:

- 255 login attempts, with 128 sniffed credentials
- credentials reused: 97 (FTP), 31 (IMAP)
- many reconnection attempts in bulks

HoneyConnector scans

Evaluation:

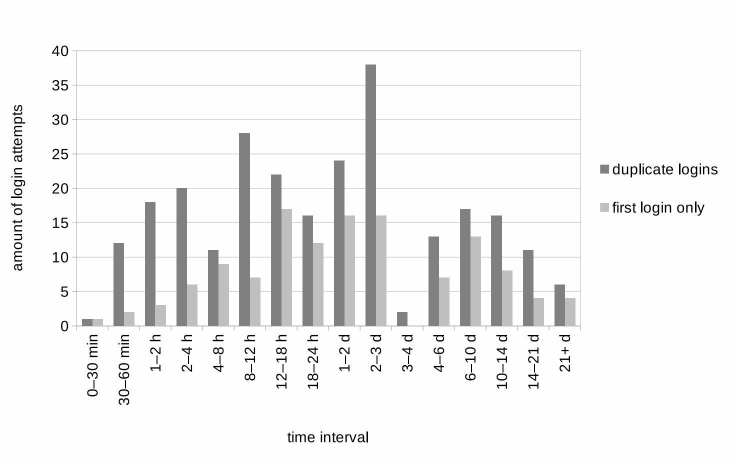
- October 2013, running 4 months
- popular hosting providers
  - one each for FTP and IMAP
- 54.000 bait connections

Detected **27** malicious relays:

- 255 login attempts, with 128 sniffed credentials
- credentials reused: 97 (FTP), 31 (IMAP)
- many reconnection attempts in bulks

Timely distribution

Timely distribution of login attempts:



Reconnection attempts

Details of login attempts:

- majority (57%, or 145) used Tor
- 18% (45) came from the same IP as exit relay
- 16% (41) used Mail2Web
- 9% (22) used IP from consumer lines, UMTS or hosting providers

Software used for some cases:

- Firefox and Internet Explorer for FTP (mozilla@example.com)
- Thunderbird for IMAP (autoconf XML file)

Reconnection attempts

Details of login attempts:

- majority (57%, or 145) used Tor
- 18% (45) came from the same IP as exit relay
- 16% (41) used Mail2Web
- 9% (22) used IP from consumer lines, UMTS or hosting providers

Software used for some cases:

- Firefox and Internet Explorer for FTP (mozilla@example.com)
- Thunderbird for IMAP (autoconf XML file)

Fun facts

Using credentials is harder than it seems, for 12% (31):

- copy-paste errors
- manual typos (username, passwords)
- IMAP credentials for FTP, and vice-versa
- mixing passwords for usernames
- one completely unrelated password
- pasting connection URL in wrong browser (Chrome vs. TBB)

Groups of relays

Multiple relays worked in groups:

- relay operators can cooperate
- multiple relays per operator
- 3 different groups identified

Russian nodes, HTTPS MitM:

- 20 relays
- same, self-signed certificate
- all but one relay located in Russia
- one VPS provider / netblock
- rather high bandwidth (up to 7 MB/s)

Groups of relays

Multiple relays worked in groups:

- relay operators can cooperate
- multiple relays per operator
- 3 different groups identified

Russian nodes, HTTPS MitM:

- 20 relays
- same, self-signed certificate
- all but one relay located in Russia
- one VPS provider / netblock
- rather high bandwidth (up to 7 MB/s)

Groups of relays

Indian relays:

- 7 relays
- distinguishable reconnect patterns
- same ISP, new IP every 6 hours
- low bandwidth (50-80 KB/s)

International group:

- 5 relays
- sniffed credentials tested in batches
- medium bandwidth (2-3 MB/s)

Groups of relays

Indian relays:

- 7 relays
- distinguishable reconnect patterns
- same ISP, new IP every 6 hours
- low bandwidth (50-80 KB/s)

International group:

- 5 relays
- sniffed credentials tested in batches
- medium bandwidth (2-3 MB/s)

Discussion

Spoiled onions:

- two nodes were found using both scanners
- overall: diverse set of attacks
- protection:
  - end-to-end encryption
  - user education
  - pinning, HSTS, DANE

Effects on Tor users:

- propability to use malicious relay is tricky to calculate
- influenced by churn rate and bandwidth
- in total 6835 exit relays
- around 2700 <= 50 hours or less

Discussion

Spoiled onions:

- two nodes were found using both scanners
- overall: diverse set of attacks
- protection:
  - end-to-end encryption
  - user education
  - pinning, HSTS, DANE

Effects on Tor users:

- propability to use malicious relay is tricky to calculate
- influenced by churn rate and bandwidth
- in total 6835 exit relays
- around 2700 $<=$ 50 hours or less

Firefox Extension

HTTPS MitM protection:

- self-signed certificates
- fetches certificate over second Tor circuit
- triggered on *about:certerror*

Does not protect against:

- malicious (and trusted) CA
- large number of relays/bandwidth

Limitations

- not all HTTPS connections targeted (sampling)!
- performance vs. detectability?
- attacker may be upstream?
- only snapshot in time

Aftermath

- notified Tor
- (reproduction of attacks)
- BadExit flag assigned
- as of yesterday:
  - one relay still in consensus, with BadExit

Conclusions

To conclude:

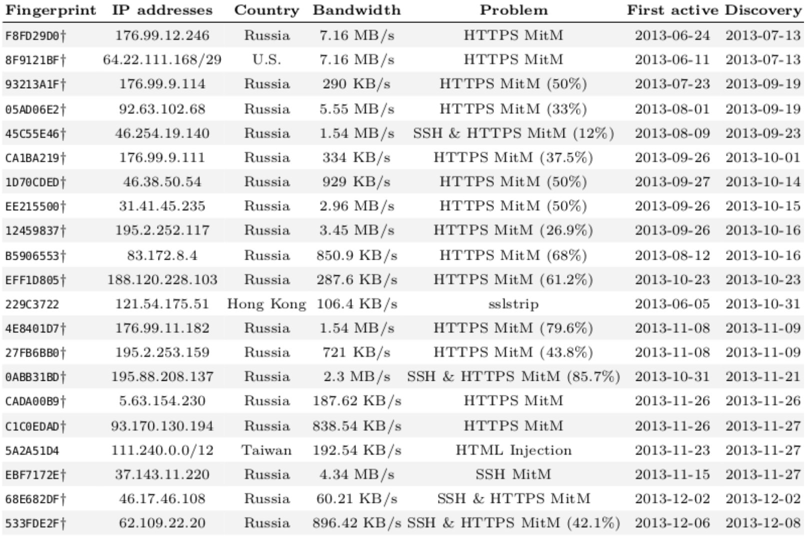
- get the source here: `http://www.cs.kau.se/philwint/spoiled_onions`
- run your own scans
- identified 65 *spoiled onions*, maybe more?

Thank you for your time!

Questions?

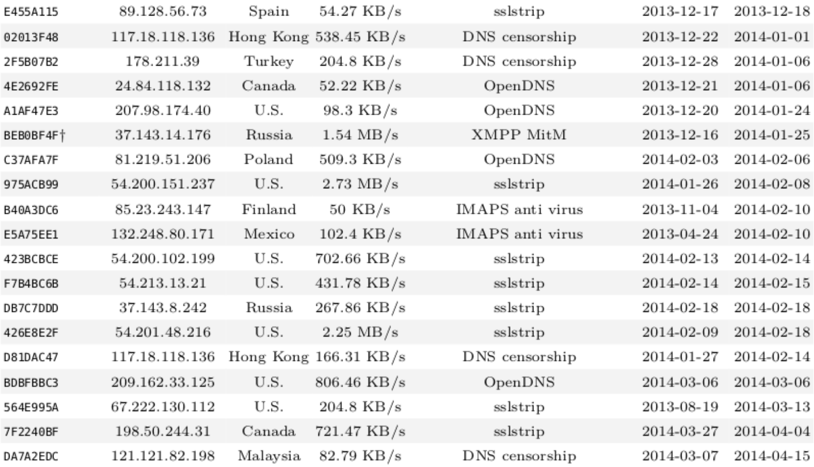
mmulazzani@sba-research.org

Full table *exitmap*



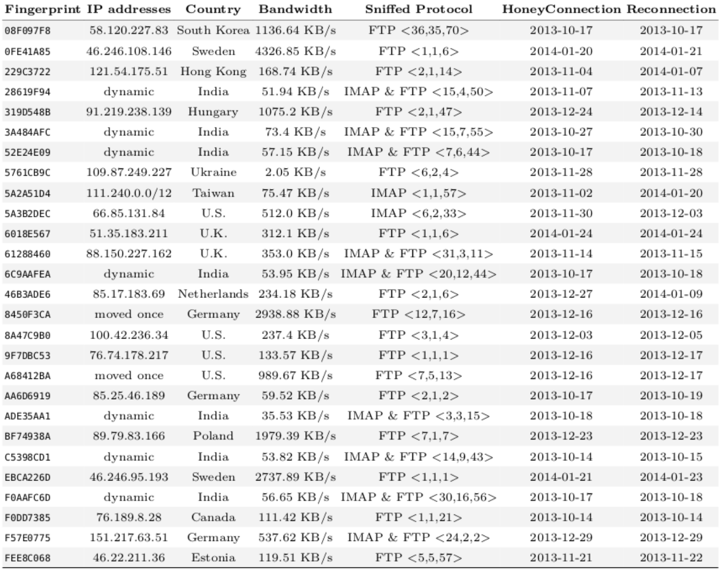
Fingerprint	IP addresses	Country	Bandwidth	Problem	First active	Discovery
F8FD29D0†	176.99.12.246	Russia	7.16 MB/s	HTTPS MitM	2013-06-24	2013-07-13
8F9121BF†	64.22.111.168/29	U.S.	7.16 MB/s	HTTPS MitM	2013-06-11	2013-07-13
93213A1F†	176.99.9.114	Russia	290 KB/s	HTTPS MitM (50%)	2013-07-23	2013-09-19
05AD06E2†	92.63.102.68	Russia	5.55 MB/s	HTTPS MitM (33%)	2013-08-01	2013-09-19
45C55E46†	46.254.19.140	Russia	1.54 MB/s	SSH & HTTPS MitM (12%)	2013-08-09	2013-09-23
CA1BA219†	176.99.9.111	Russia	334 KB/s	HTTPS MitM (37.5%)	2013-09-26	2013-10-01
1D70CDED†	46.38.50.54	Russia	929 KB/s	HTTPS MitM (50%)	2013-09-27	2013-10-14
EE215500†	31.41.45.235	Russia	2.96 MB/s	HTTPS MitM (50%)	2013-09-26	2013-10-15
12459837†	195.2.252.117	Russia	3.45 MB/s	HTTPS MitM (26.9%)	2013-09-26	2013-10-16
B5906553†	83.172.8.4	Russia	850.9 KB/s	HTTPS MitM (68%)	2013-08-12	2013-10-16
EFF1D805†	188.120.228.103	Russia	287.6 KB/s	HTTPS MitM (61.2%)	2013-10-23	2013-10-23
229C3722	121.54.175.51	Hong Kong	106.4 KB/s	sslstrip	2013-06-05	2013-10-31
4E8401D7†	176.99.11.182	Russia	1.54 MB/s	HTTPS MitM (79.6%)	2013-11-08	2013-11-09
27FB6BB0†	195.2.253.159	Russia	721 KB/s	HTTPS MitM (43.8%)	2013-11-08	2013-11-09
0ABB31BD†	195.88.208.137	Russia	2.3 MB/s	SSH & HTTPS MitM (85.7%)	2013-10-31	2013-11-21
CADA00B9†	5.63.154.230	Russia	187.62 KB/s	HTTPS MitM	2013-11-26	2013-11-26
C1C0EDAD†	93.170.130.194	Russia	838.54 KB/s	HTTPS MitM	2013-11-26	2013-11-27
5A2A51D4	111.240.0.0/12	Taiwan	192.54 KB/s	HTML Injection	2013-11-23	2013-11-27
EBF7172E†	37.143.11.220	Russia	4.34 MB/s	SSH MitM	2013-11-15	2013-11-27
68E682DF†	46.17.46.108	Russia	60.21 KB/s	SSH & HTTPS MitM	2013-12-02	2013-12-02
533FDE2F†	62.109.22.20	Russia	896.42 KB/s	SSH & HTTPS MitM (42.1%)	2013-12-06	2013-12-08

Full table *exitmap*



E455A115	89.128.56.73	Spain	54.27 KB/s	sslstrip	2013-12-17	2013-12-18
02013F48	117.18.118.136	Hong Kong	538.45 KB/s	DNS censorship	2013-12-22	2014-01-01
2F5B07B2	178.211.39	Turkey	204.8 KB/s	DNS censorship	2013-12-28	2014-01-06
4E2692FE	24.84.118.132	Canada	52.22 KB/s	OpenDNS	2013-12-21	2014-01-06
A1AF47E3	207.98.174.40	U.S.	98.3 KB/s	OpenDNS	2013-12-20	2014-01-24
BEB0BF4F†	37.143.14.176	Russia	1.54 MB/s	XMPP MitM	2013-12-16	2014-01-25
C37AFA7F	81.219.51.206	Poland	509.3 KB/s	OpenDNS	2014-02-03	2014-02-06
975ACB99	54.200.151.237	U.S.	2.73 MB/s	sslstrip	2014-01-26	2014-02-08
B40A3DC6	85.23.243.147	Finland	50 KB/s	IMAPS anti virus	2013-11-04	2014-02-10
E5A75EE1	132.248.80.171	Mexico	102.4 KB/s	IMAPS anti virus	2013-04-24	2014-02-10
423BCBCE	54.200.102.199	U.S.	702.66 KB/s	sslstrip	2014-02-13	2014-02-14
F7B4BC6B	54.213.13.21	U.S.	431.78 KB/s	sslstrip	2014-02-14	2014-02-15
DB7C7DDD	37.143.8.242	Russia	267.86 KB/s	sslstrip	2014-02-18	2014-02-18
426E8E2F	54.201.48.216	U.S.	2.25 MB/s	sslstrip	2014-02-09	2014-02-18
D81DAC47	117.18.118.136	Hong Kong	166.31 KB/s	DNS censorship	2014-01-27	2014-02-14
BDBFBBC3	209.162.33.125	U.S.	806.46 KB/s	OpenDNS	2014-03-06	2014-03-06
564E995A	67.222.130.112	U.S.	204.8 KB/s	sslstrip	2013-08-19	2014-03-13
7F2240BF	198.50.244.31	Canada	721.47 KB/s	sslstrip	2014-03-27	2014-04-04
DA7A2EDC	121.121.82.198	Malaysia	82.79 KB/s	DNS censorship	2014-03-07	2014-04-15

Full table *HoneyConnector*



Fingerprint	IP addresses	Country	Bandwidth	Sniffed Protocol	HoneyConnection	Reconnection
08F097F8	58.120.227.83	South Korea	1136.64 KB/s	FTP <36,35,70>	2013-10-17	2013-10-17
0FE41A85	46.246.108.146	Sweden	4326.85 KB/s	FTP <1,1,6>	2014-01-20	2014-01-21
229C3722	121.54.175.51	Hong Kong	168.74 KB/s	FTP <2,1,14>	2013-11-04	2014-01-07
28619F94	dynamic	India	51.94 KB/s	IMAP & FTP <15,4,50>	2013-11-07	2013-11-13
319D548B	91.219.238.139	Hungary	1075.2 KB/s	FTP <2,1,47>	2013-12-24	2013-12-14
3A484AFC	dynamic	India	73.4 KB/s	IMAP & FTP <15,7,55>	2013-10-27	2013-10-30
52E24E09	dynamic	India	57.15 KB/s	IMAP & FTP <7,6,44>	2013-10-17	2013-10-18
5761CB9C	109.87.249.227	Ukraine	2.05 KB/s	FTP <6,2,4>	2013-11-28	2013-11-28
5A2A51D4	111.240.0.0/12	Taiwan	75.47 KB/s	IMAP <1,1,57>	2013-11-02	2014-01-20
5A3B2DEC	66.85.131.84	U.S.	512.0 KB/s	IMAP <6,2,33>	2013-11-30	2013-12-03
6018E567	51.35.183.211	U.K.	312.1 KB/s	FTP <1,1,6>	2014-01-24	2014-01-24
61288460	88.150.227.162	U.K.	353.0 KB/s	IMAP & FTP <31,3,11>	2013-11-14	2013-11-15
6C9AAFEA	dynamic	India	53.95 KB/s	IMAP & FTP <20,12,44>	2013-10-17	2013-10-18
46B3ADE6	85.17.183.69	Netherlands	234.18 KB/s	FTP <2,1,6>	2013-12-27	2014-01-09
8450F3CA	moved once	Germany	2938.88 KB/s	FTP <12,7,16>	2013-12-16	2013-12-16
8A47C9B0	100.42.236.34	U.S.	237.4 KB/s	FTP <3,1,4>	2013-12-03	2013-12-05
9F7DBC53	76.74.178.217	U.S.	133.57 KB/s	FTP <1,1,1>	2013-12-16	2013-12-17
A68412BA	moved once	U.S.	989.67 KB/s	FTP <7,5,13>	2013-12-16	2013-12-17
AA6D6919	85.25.46.189	Germany	59.52 KB/s	FTP <2,1,2>	2013-10-17	2013-10-19
ADE35AA1	dynamic	India	35.53 KB/s	IMAP & FTP <3,3,15>	2013-10-18	2013-10-18
BF74938A	89.79.83.166	Poland	1979.39 KB/s	FTP <7,1,7>	2013-12-23	2013-12-23
C5398CD1	dynamic	India	53.82 KB/s	IMAP & FTP <14,9,43>	2013-10-14	2013-10-15
EBCA226D	46.246.95.193	Sweden	2737.89 KB/s	FTP <1,1,1>	2014-01-21	2014-01-23
F0AAFC6D	dynamic	India	56.65 KB/s	IMAP & FTP <30,16,56>	2013-10-17	2013-10-18
F0DD7385	76.189.8.28	Canada	111.42 KB/s	FTP <1,1,21>	2013-10-14	2013-10-14
F57E0775	151.217.63.51	Germany	537.62 KB/s	IMAP & FTP <24,2,2>	2013-12-29	2013-12-29
FEE8C068	46.22.211.36	Estonia	119.51 KB/s	FTP <5,5,57>	2013-11-21	2013-11-22