Exposing Snooping in Tor by HSDir Relays

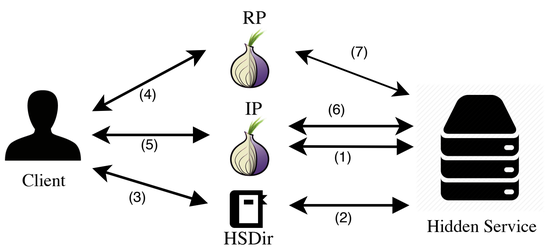
Motivation

- Tor's security relies on the honest behavior of relays
- Tor clearly states HSDirs should not snoop on onion services
- The behavior of HSDirs has not been studied

Question: How to detect the snooping HSDirs and estimate a lower bound on them?

Tor

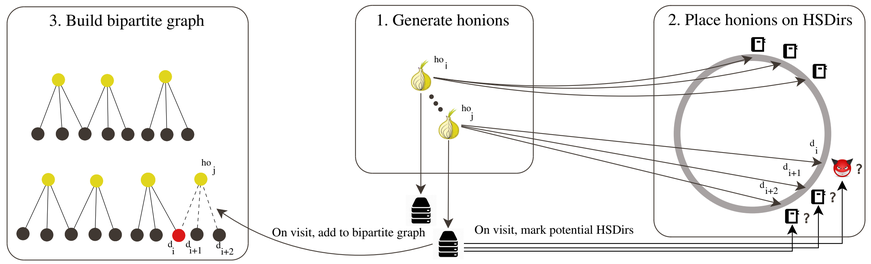
- Provides anonymity and privacy for users
- Hidden Services protect the anonymity of the servers



Hidden Services architecture.

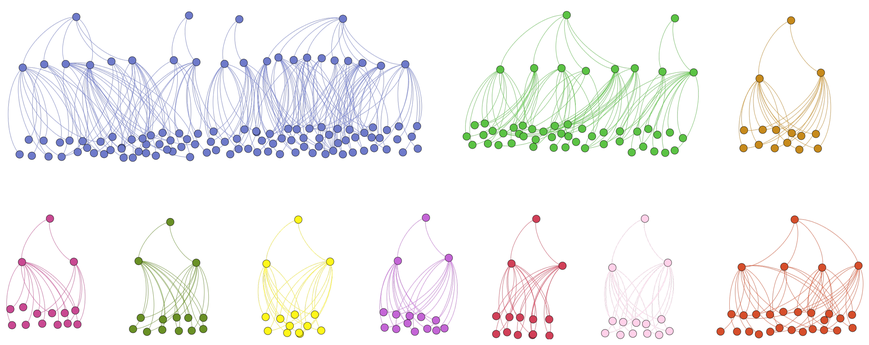
Honey Onions (HOnions)

- A framework to detect misbehaving Tor HSDir relays
- Each honion is a server program that logs visits
- Three schedules; daily, weekly, monthly (1500 per batch)
- Generate the bipartite graph of HSDirs and visited honions
- Identify the snooping HSDirs using the set cover problem
- NP- Complete problem
- Integer Linear Programming (ILP)



Flow diagram of the honion system. When a visit happens to one of the honions, after identifying the potential suspicious HSDirs, we add them to the bipartite graph.

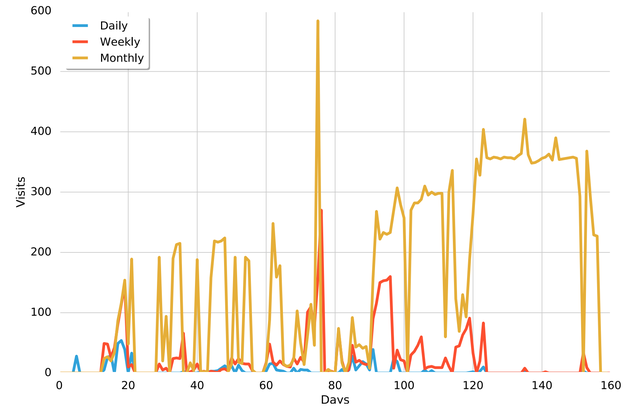
The global map of detected misbehaving HSDirs and their most likely geographic origin.



A typical graph representation of the visited honions, and the hosting HSDirs.

Results

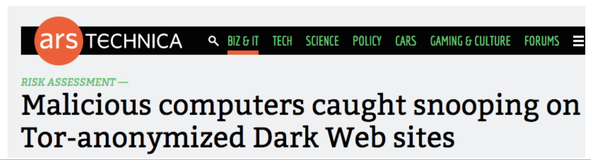
- Identified more than 100 snooping HSDirs over the period of 72 days
- Logged about 40000 visits to the honions
- Wide range of probing, SQL injection, XSS, user enumeration, etc.
- More than 70% of the snoopers hosted on cloud, 25% were also exit nodes
- Top countries: USA, Germany, France, United Kingdom, and Netherlands
- The snoopers have adapted their techniques and increased their sophistication



The new trend of visits. The snoopers are delaying their visits to avoid identification.

Conclusion and Future Work

- Malicious HSDirs have different level of sophistication
- Some delay visits to avoid detection as a tradeoff
- More than half of the misbehaving relays are hosted on cloud
- Some cloud providers accept bitcoins as payment
- These privacy infrastructures make the tracking more difficult



Amirali Sanatinia, Guevara Noubir
Northeastern University

References

1) A. Sanatinia, G. Noubir, "Honey Onions: a Framework for Characterizing and Identifying Misbehaving Tor HSDirs", IEEE Conference on Communications and Network Security (CNS), 2016

2) P. Winter, R. Kower, M. Mulazzani, M. Huber, S. Schrittwieser, S. Lindskog, E. Weippl, "Spoiled Onions: Exposing Malicious Tor Exit Relays", Privacy Enhancing Technologies Symposium (PETS), 2015