Northeastern University

OnionBots: Subverting Privacy Infrastructure for Cyber Attacks

Amirali Sanatinia Guevara Noubir

College of Computer and Information Science
Northeastern University, Boston, MA

Motivation

- Abusing privacy infrastructure
  - Tor Hidden Services
- Recent examples of abuse of privacy infrastructure and technology
  - Silk road, cryptolocker, Zeus 64, Chewbacca botnet
- Infected devices can setup a botnet through Tor Hidden Services
  - No nodes know the IP/location of others
  - C&C can be anywhere

Outline

- Evolution of botnets and their shortcomings
- Review of Tor and Hidden Services
- OnionBots
  - Life Cycle
  - C&C Communication
  - Dynamic Distributed Self Repairing (DDSR)
  - Sybil Onion Attack Protocol (SOAP)

Evolution of Botnets

- Popular for denial of service attacks, spam, click frauds, bitcoin mining, stealing sensitive information, and other malicious activities
- Communications between botmaster & bots (C&C)
  - Centralized -> P2P; HTTP or IRC;
  - Fast Flux, Double Flux to randomize the IP addresses
  - Domain Generation Algorithms (DGA)
- Various technical mitigations
  - Limited by problems of jurisdiction

Centralized

- Easy to build and maintain
- Single point of failure
- Does not scale
- Easy to detect and mitigate
- Analysis of traffic
- Clustering of the hosts

Fast-flux

- Mapping numerous IP addresses associated with a single fully qualified domain name (FQDN)
- Single-flux
  - multiple nodes registering and de-registering as the DNS A record
- Double-flux
  - More sophisticated
  - multiple nodes registering and de-registering as the DNS Name Server (NS) record
- Can be neutralized by taking over the domain

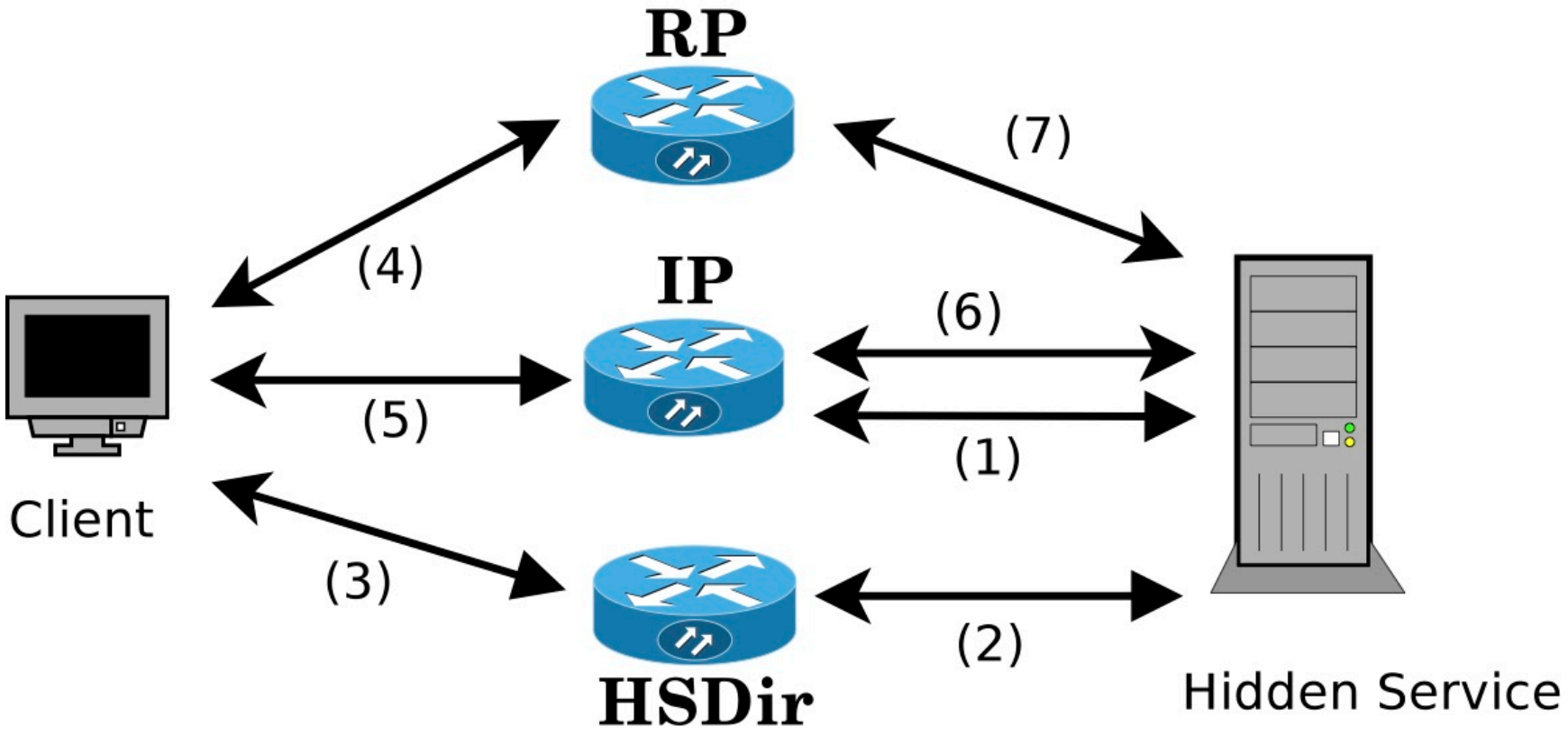
DGA

- Periodically generating domain names, used as rendezvous point
- Once a sample is obtained it becomes easier to block
- Conficker.a and .b are prime examples
- *E.g., zffezlkgfnox.net*
- Can be blocked using patterns in the domains

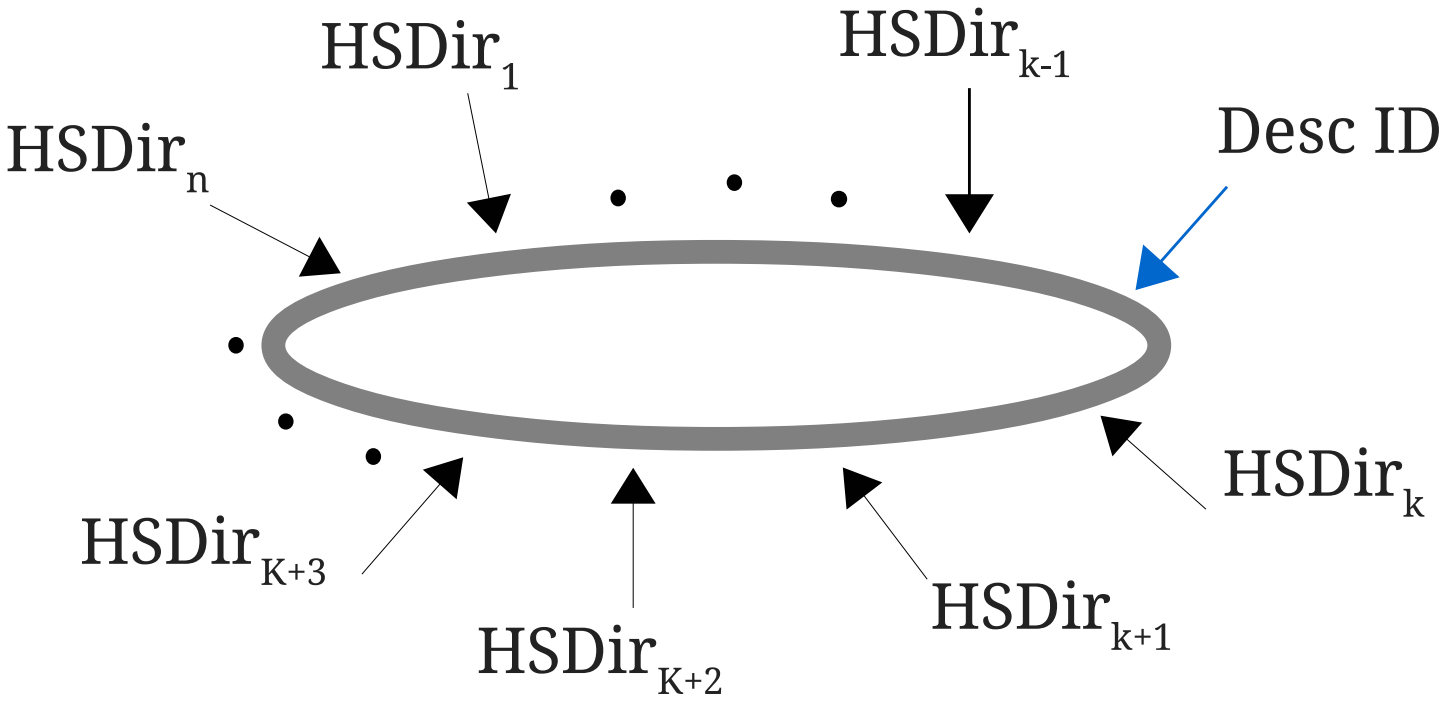
Tor

- Most widely used anonymity-network
- Based on onion routing of packets
- Hidden services (HS) provides anonymity for the servers
- Silkroad and Cryptolocker are prime examples
- It is possible to block access to a single HS with sufficient resources

Tor Hidden Services



Tor Hidden Services



OnionBot: a Crypto-based P2P Botnet

- Typical botnet lifecycle
  - Infection: phishing, spam, remote exploits, drive-by-download or zero-day vulnerabilities
  - Rally or bootstrapping: join the botnet
  - Wait for commands
  - Execution

- OnionBot key features
  - Similar lifecycle
  - Fully decoupled from IP addresses: only `.onion` addresses
  - Self-healing P2P network on top of Tor
  - Temporarily knowledge of neighbors `.onion` addresses
  - Indistinguishable traffic: control, data, src/dst, from random
  - Access for botmaster from any bot through hidden services

Botnet as a Service

- Provide a stealthy virtual machine
  - Time limited access tokens from botmaster
  - Accessible though HiddenServices
- Payment with Bitcoins + mixing

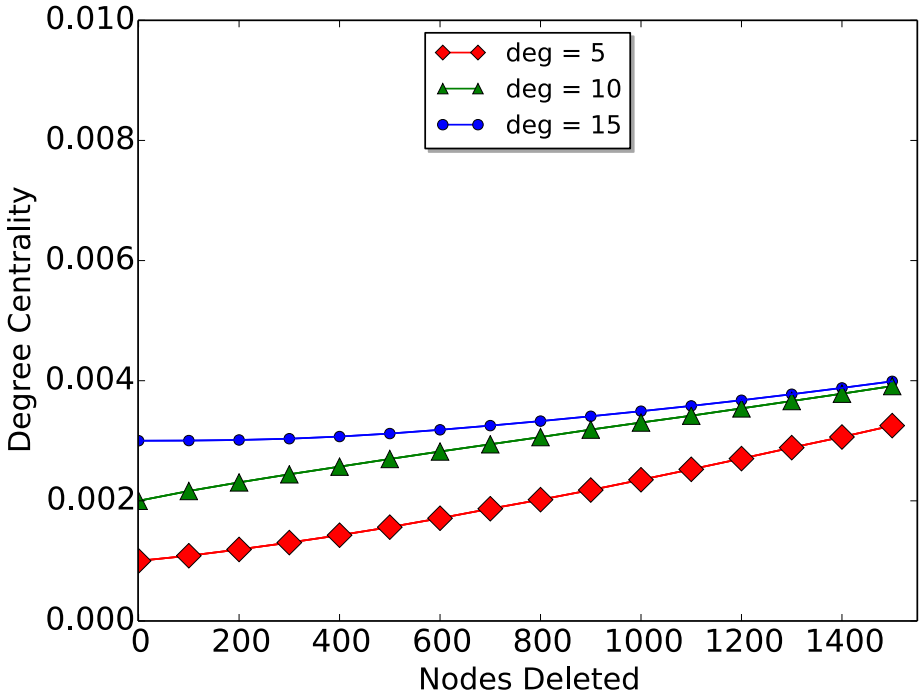
C&C Communications in OnionBot

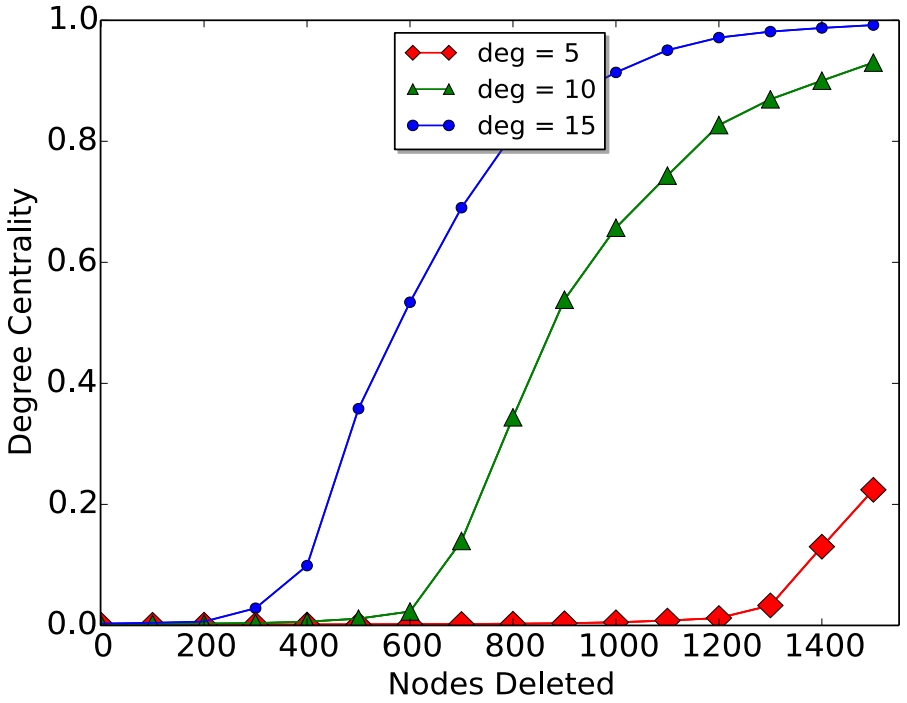
- All bots know OnionBot master's public key
- Communicate through flooding over P2P net
- Unicast communications are indistinguishable from random noise (Elligator crypto keys)
- Bots periodically change their .onion address
- Bots report .onion address key-seed to botmaster

Maintaining the OnionBot Graph

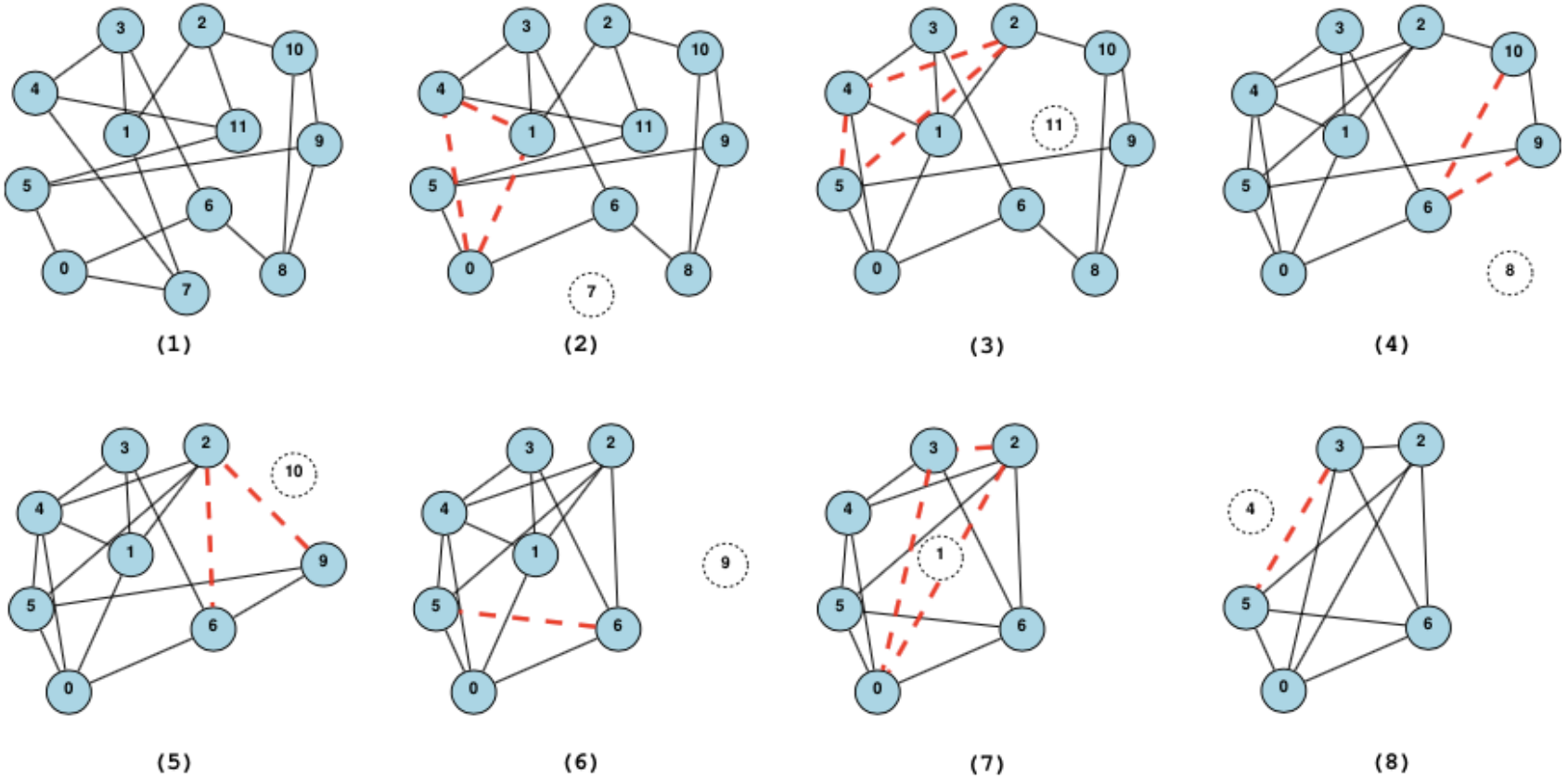
- Dynamic Distributed Self Repairing (DDSR)
  - Based on Neighbors of Neighbor technique + pruning + forgetting
  - When a node is deleted, each pair of its neighbors will form an edge
  - To maintain a low degree, a node deletes the highest degree node from its peer list
  - New .onion address is generated based on a secret key and time

Pruning vs No-Pruning



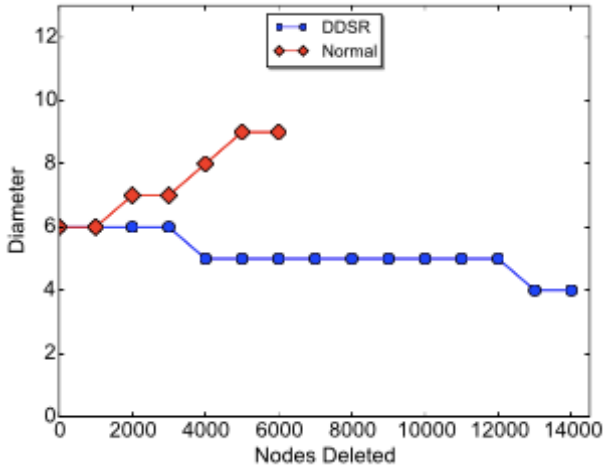


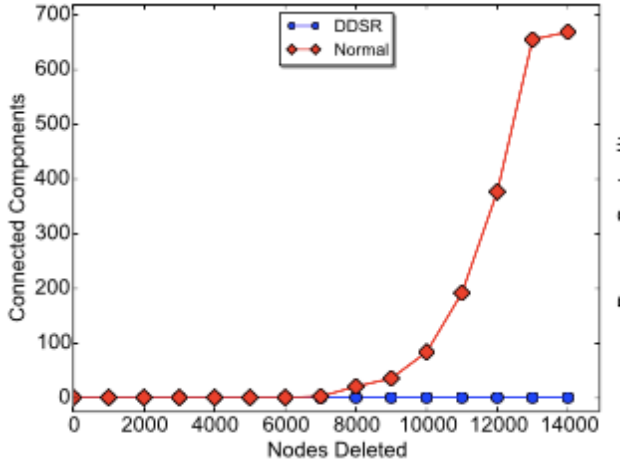
DDSR in Action

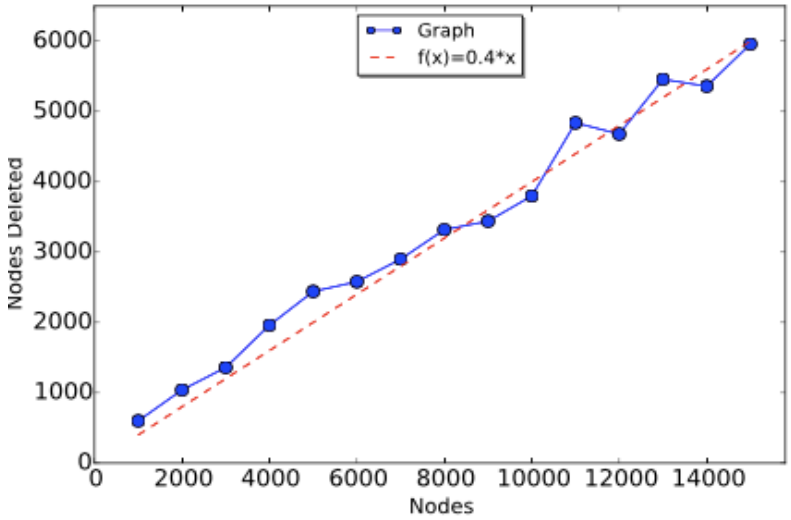


DDSR Properties

- Low diameter, degree, resiliency to nodes deletions,



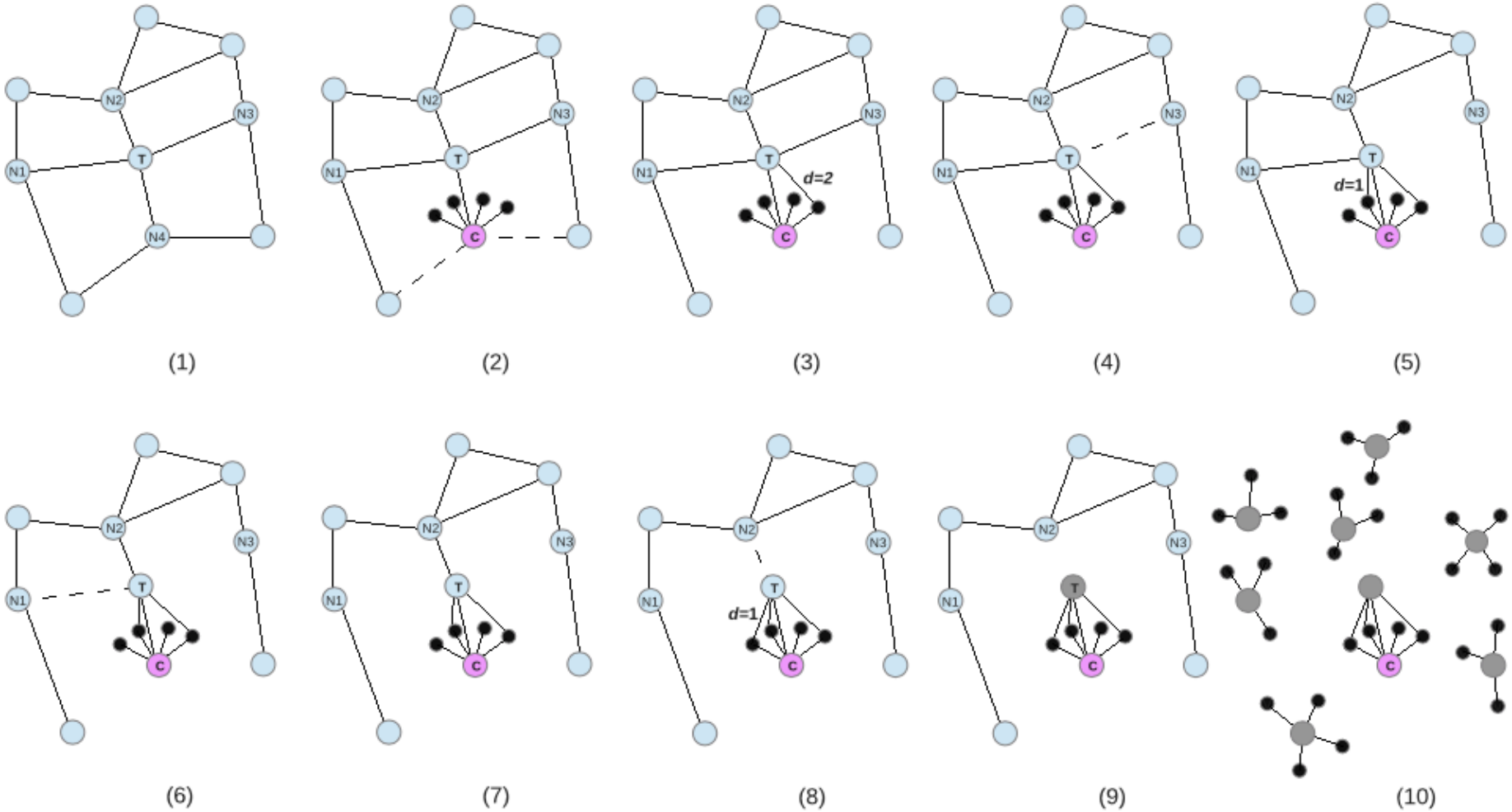




Targeting OnionBots

- Denial of Service attack against .onion addresses
- Does not scale
- Needs prior knowledge of the .onion domains
- More long term approaches:
  - CAPTCHAs
  - Throttling entry guards
  - Reusing failed partial circuits

Sybil Onion Attack Protocol (SOAP)



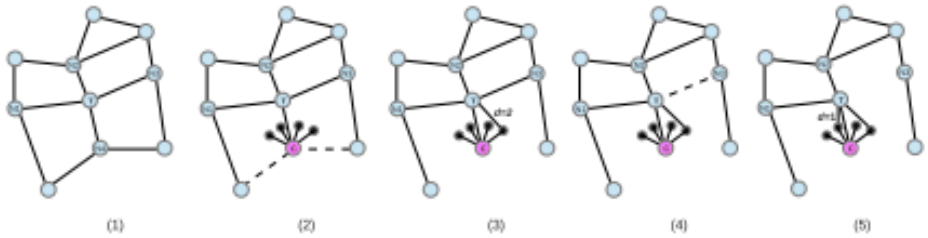
Conclusion

- Next Generation of Botnets:
  - Subvert privacy infrastructures
  - Strong cryptographic blocks
  - Resilient and dependable network formations and maintenance
  - Tor for hiding the traffic
  - Bitcoin for anonymous payments

MIT Technology Review

How the Next Generation of Botnets Will Exploit Anonymous Networks, and How to Beat Them

Computer scientists are already devising strategies for neutralizing the next generation of malicious botnets.



Interests in OnionBots

一场全球性的运动。第一代僵尸网络往往是由Web上面的单台计算机控制的，因此只需找到控制主机并将其干掉即可。
捣老巢。

。近年来这场猫捉老鼠的游戏开始变得非常复杂。僵尸网络现在开始不断地想方设法隐藏控制主机的位置。方法之一是
时指向同一个域名。而控制主机的实际IP地址可以是其中的任意一个，而且还会经常变换。哪怕你顺藤摸瓜好不容易追
。

利用Tor网络的匿名性来加大难度。再加上比特币这样不可跟踪的电子货币的出现，导致网上的勒索行为愈发的难以追溯

nirali Sanatinia和Guevara Noubir认为，僵尸网络最重要的的创新将会发生在匿名性的利用方面。而洋葱路由（onion routi
同的加密层当中，要想还原消息，就得一层层地进行解密，其过程就像剥洋葱一样。