Peer-to-Peer Botnets

Security & Communication

65963 – David Dias
68208 – Artur Balanuta
68210 – Dário Nascimento

Basic Concepts:

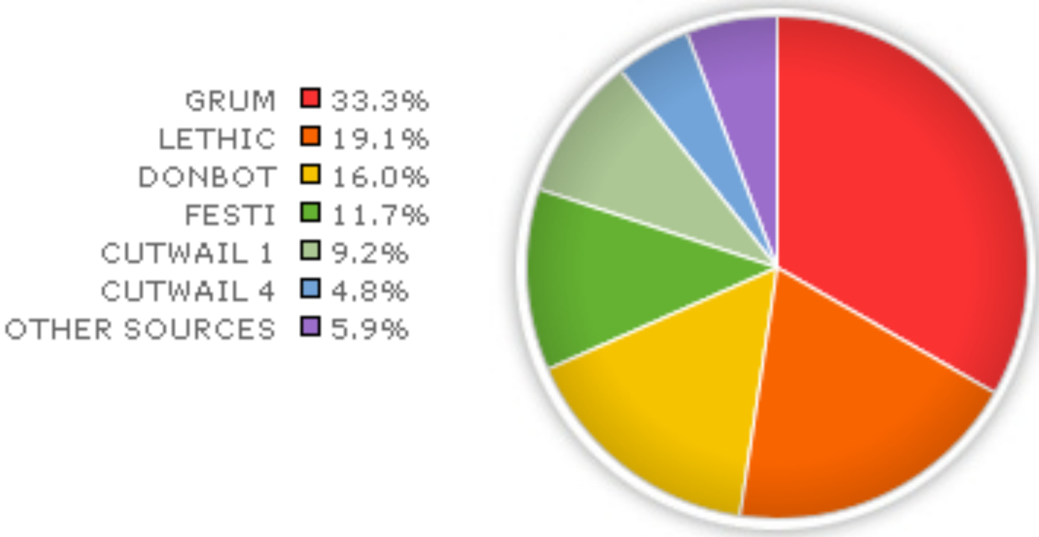
- Bot/Zombie
- Botnet
- Bot Master

Can be used for:

- DDoS
- Spam
- Phishing Emails
- Click-fraud
- Stealing Personal Data

Facts and Figures

Statistics for Week ending January 22, 2012



Spam by Spambot Type

This chart is a percentage breakdown of spam received at our spam traps for each spambot type. Typically a small number of major botnets are responsible for the bulk of all spam.

“1 trilion monthly spam messages by the end of March 2012”

Source: Annual McAffee Threats Report, First Quarter 2012

Facts and Figures

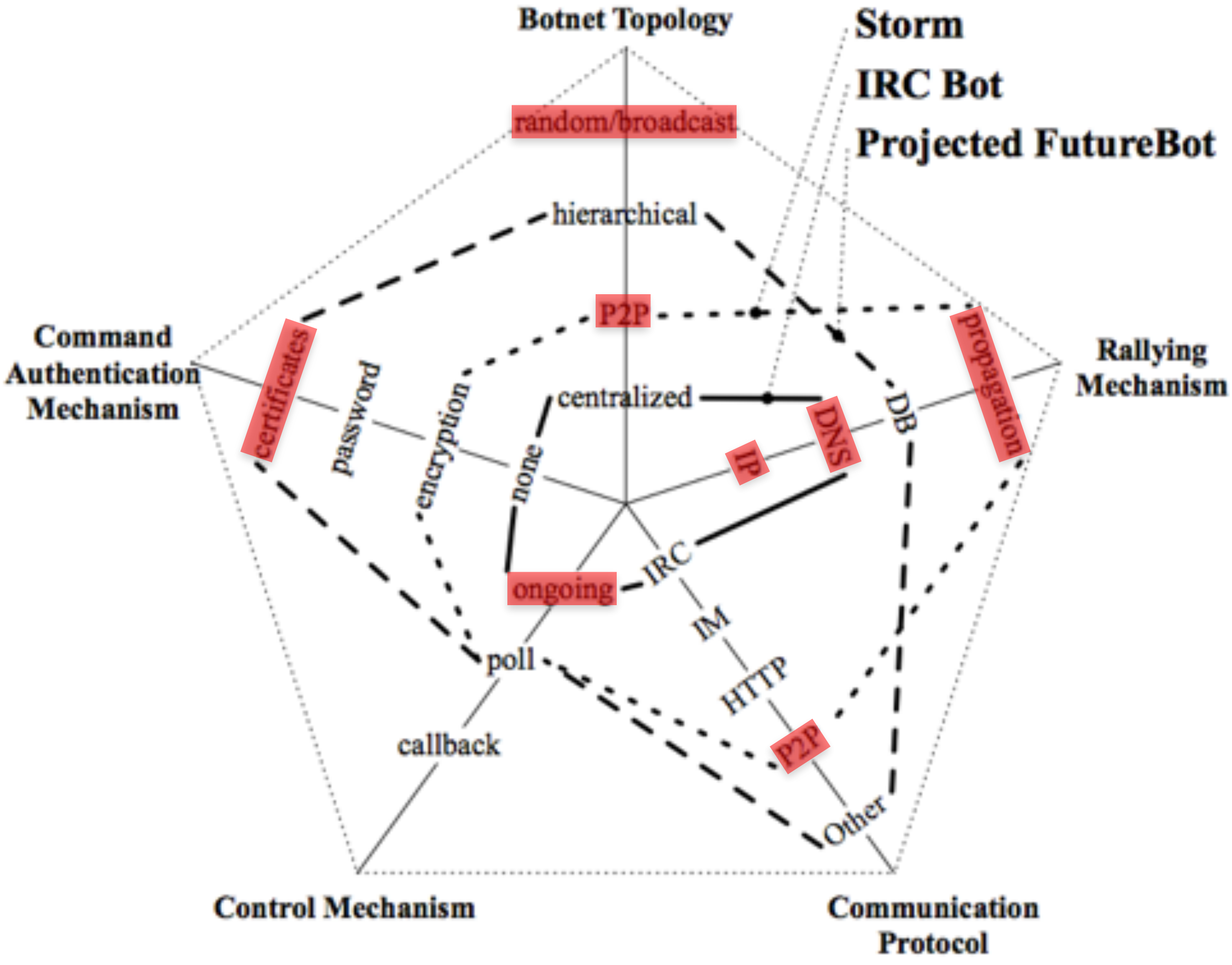
More 5 Million Infections during Q1 2012

Cutwail Botnet: 2 million new infections

Grum botnet: 18% of spam (18 billion/day) sent out across the world

Columbia, Japan, Poland, Spain and USA have the largest botnet increase

Indonesia, Portugal and South Korea continued to decline

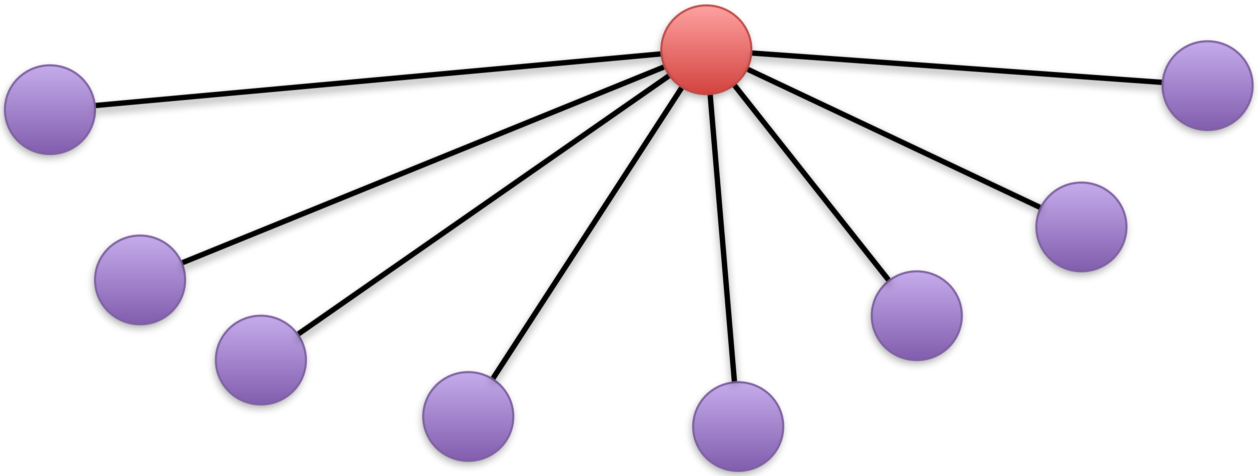

Botnet Topology
Storm
IRC Bot
Projected FutureBot
random/broadcast
hierarchical
P2P
centralized
Command Authentication Mechanism
certificates
password
encryption
none
Rallying Mechanism
propagation
DB
DNS
IP
IRC
IM
HTTP
P2P
Other
ongoing
poll
callback
Control Mechanism
Communication Protocol

Propagation

- **Phishing Scams (Ex. SPAM)**
- **Social Engineering (Ex. Facebook)**
- **DNS Poisoning**
- **Infected Mobile Storage (Ex. USB Flashdrives)**
- **App Infection (Ex. Android/IOS)**
- **Polluted Files (Ex. Infected Torrents)**
- **Etc**

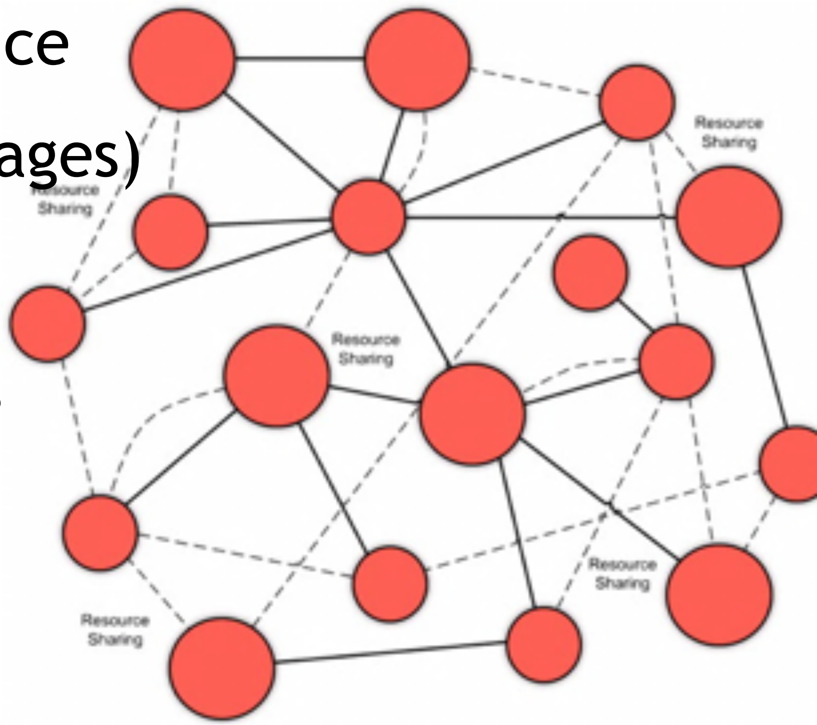
Centralized Command and Control

- Single point of control
- Direct control of zombies
  - Easy to detect using traffic analysis



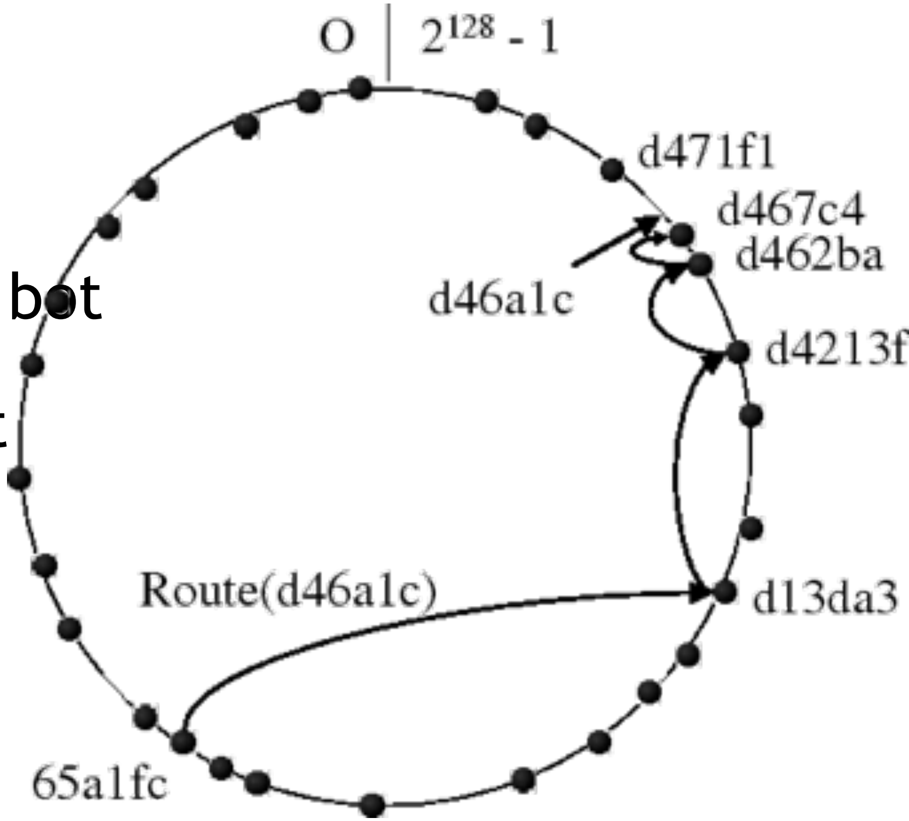
Unstructured Control

- Unknown botnet size
- Bots disseminate commands between themselves
- Huge latency => poor performance
- Small eficiency (Broadcast messages)
- Parts of the network may be unreachable without us knowing



P2P Overlay Network

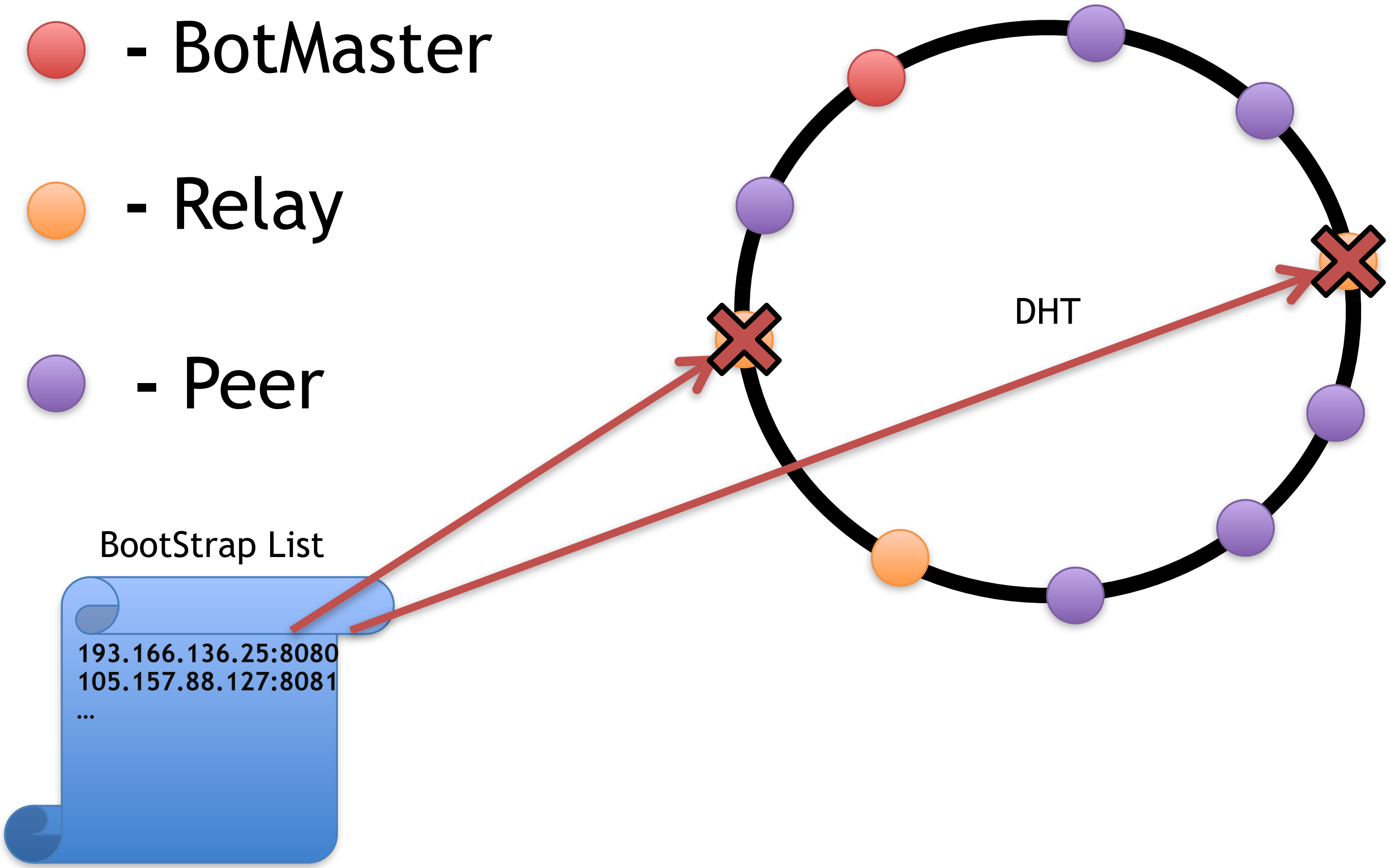
- Bots join a P2P Network
- Communicate through DHT
- Botmaster can act as normal bot
- Botmaster can enter and exit from several points



Our solution?

- P2P - DHT Pastry
- Secure communication
- Safe Peer Entry
- Renting Model
- Avoid Crawlers and Sybil Attacks

Peer entry



🔴 - BotMaster

🟠 - Relay

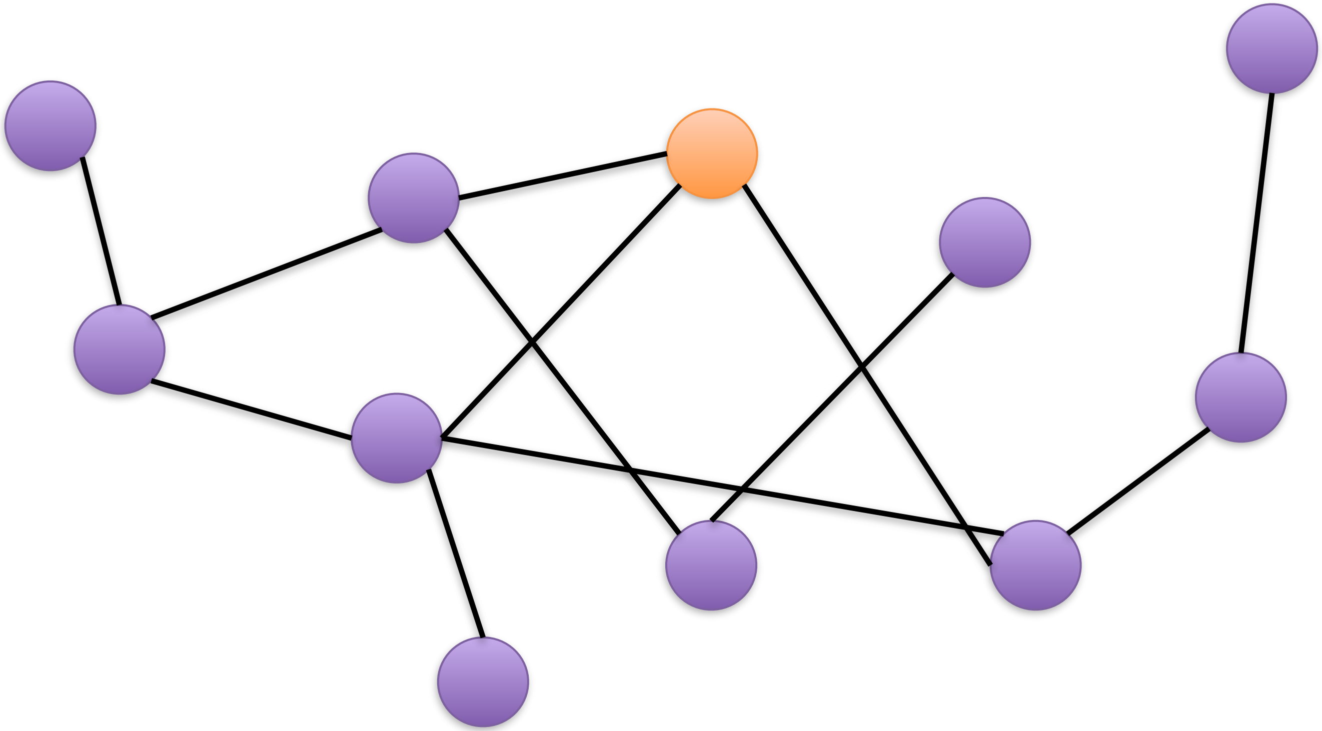
🟣 - Peer

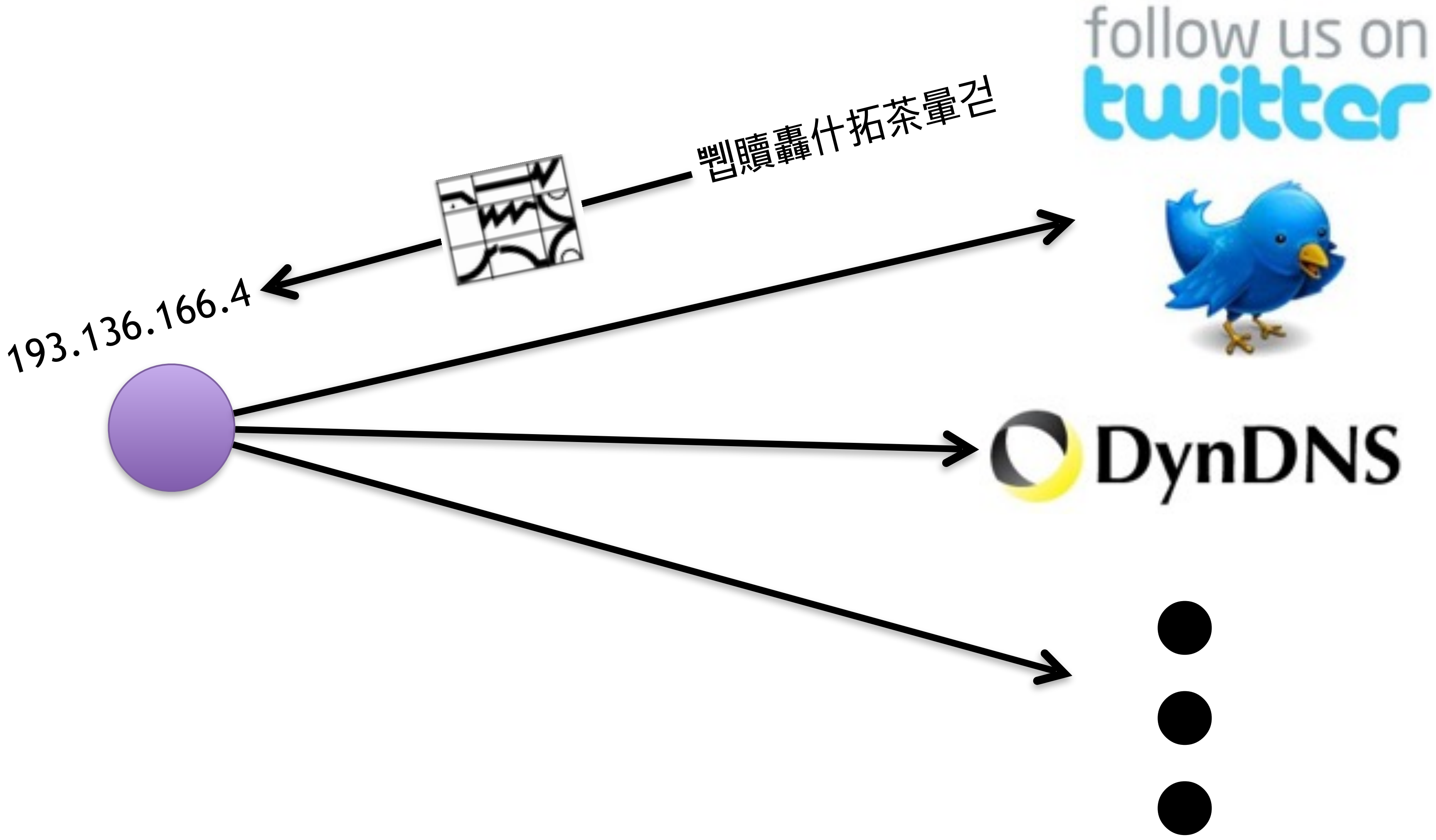
DHT

BootStrap List

```
193.166.136.25:8080
105.157.88.127:8081
…
```

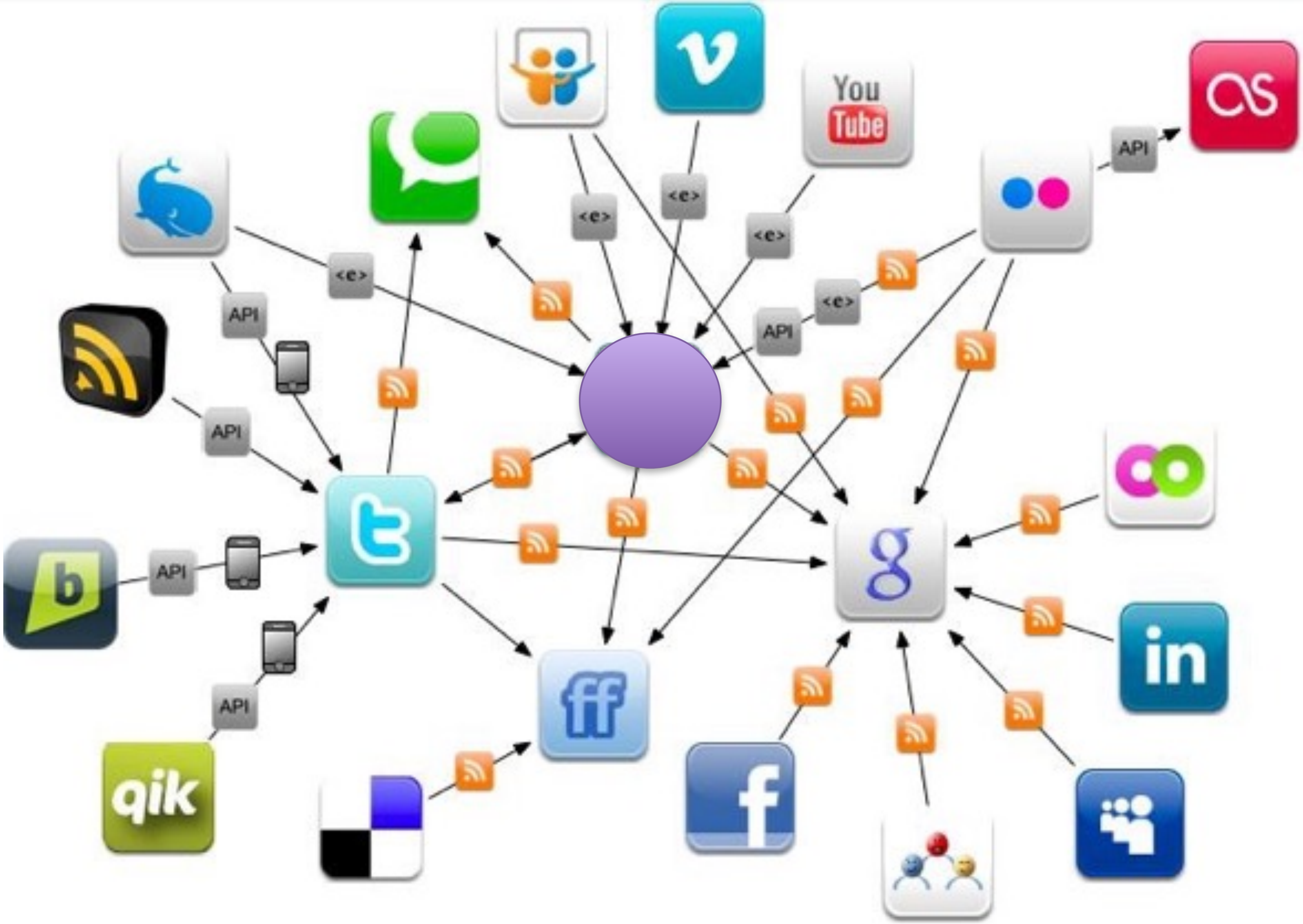
Unstructured Network



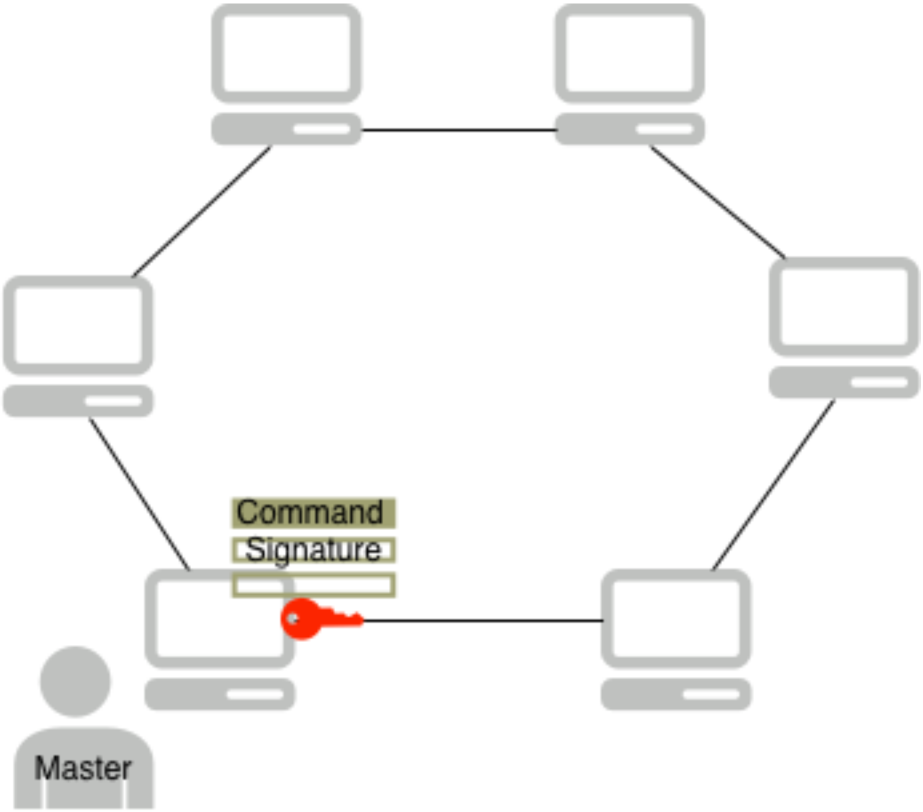


193.136.166.4

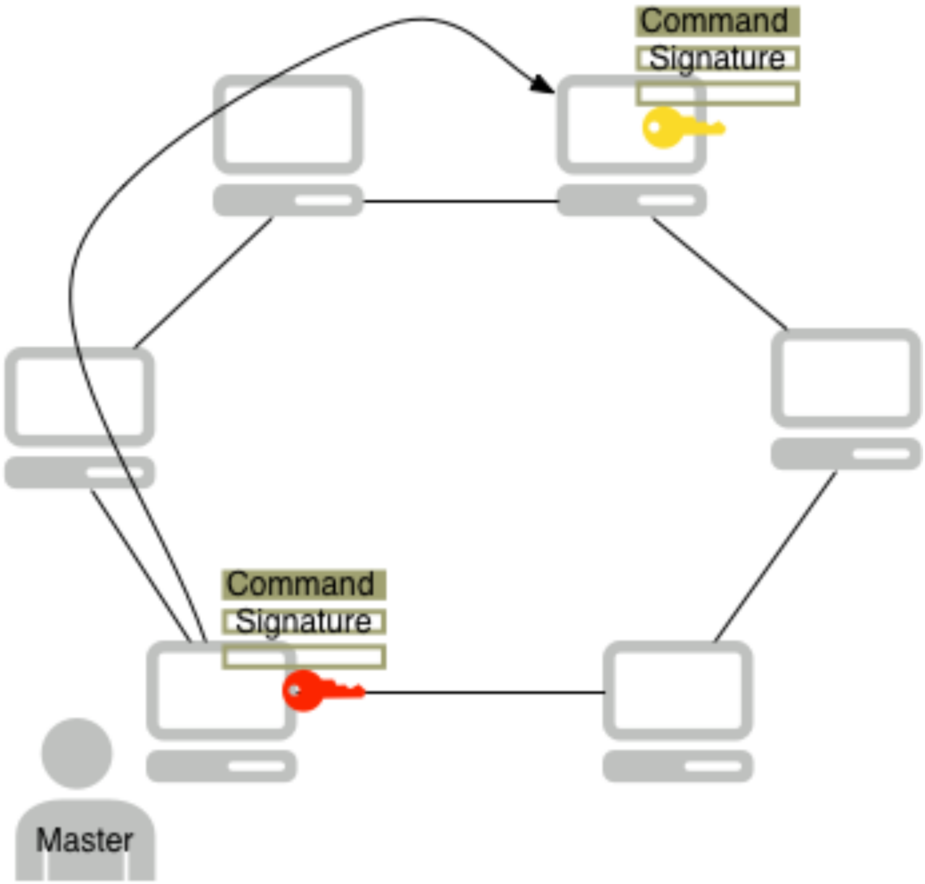
뻡贖轟什拓茶暈건


<e>
API

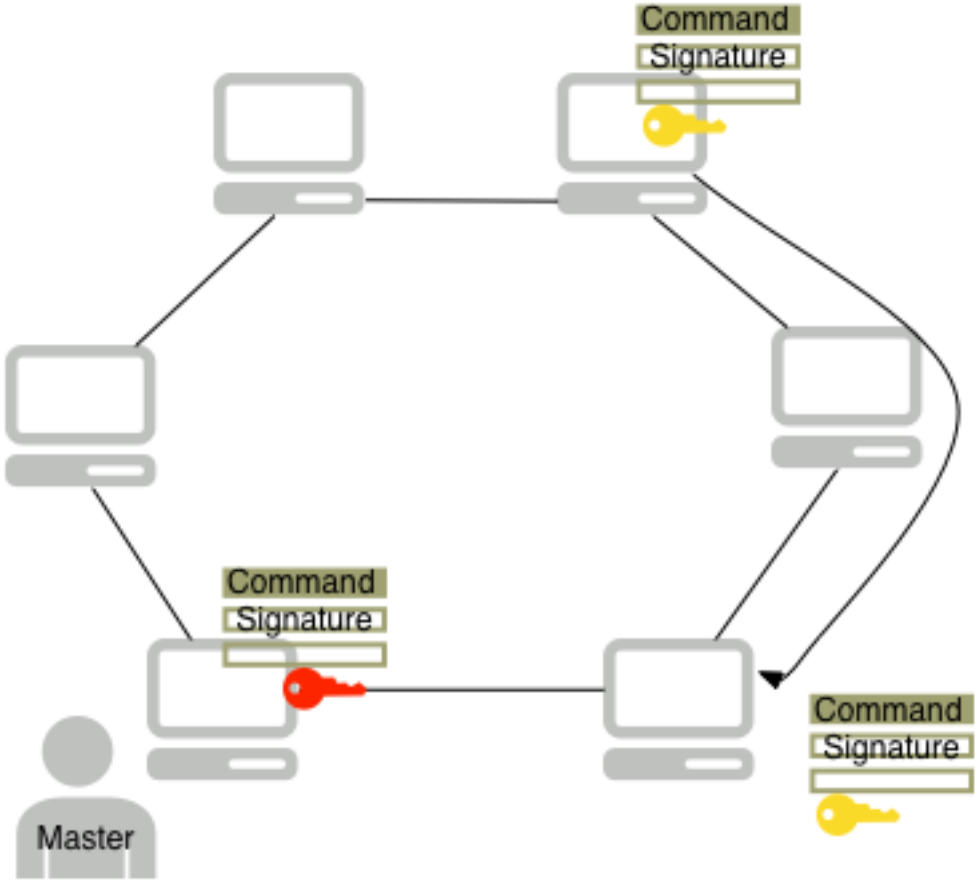
Secure dissemination of orders



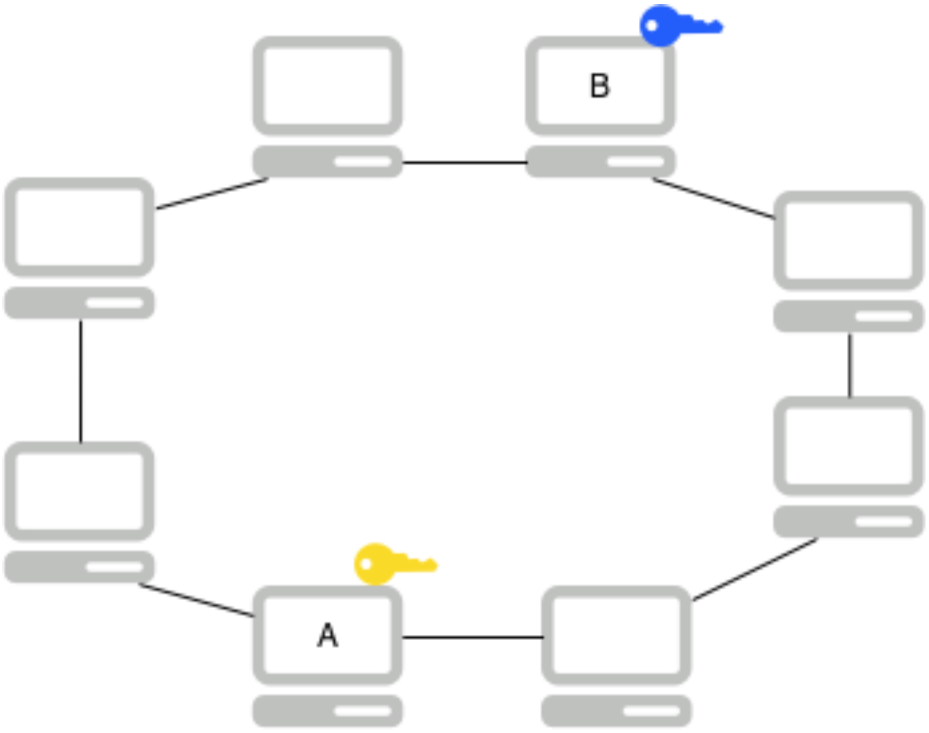
Secure dissemination of orders



Secure dissemination of orders



Peer-to-peer traffic obfuscation

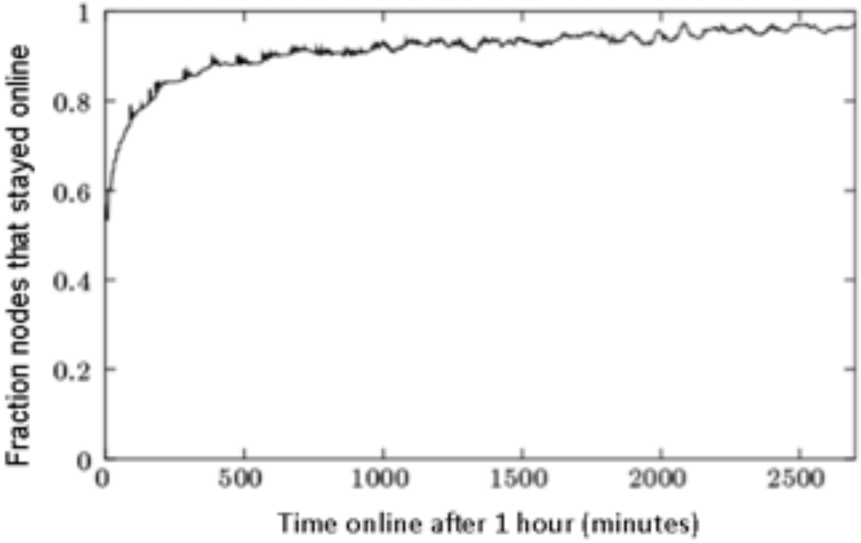


Peer-to-Peer Trust

Accomplice List

<NodeID,K_{pub},Credits,LastMsgReceived>

- Limited Size
- Sorted by Credits



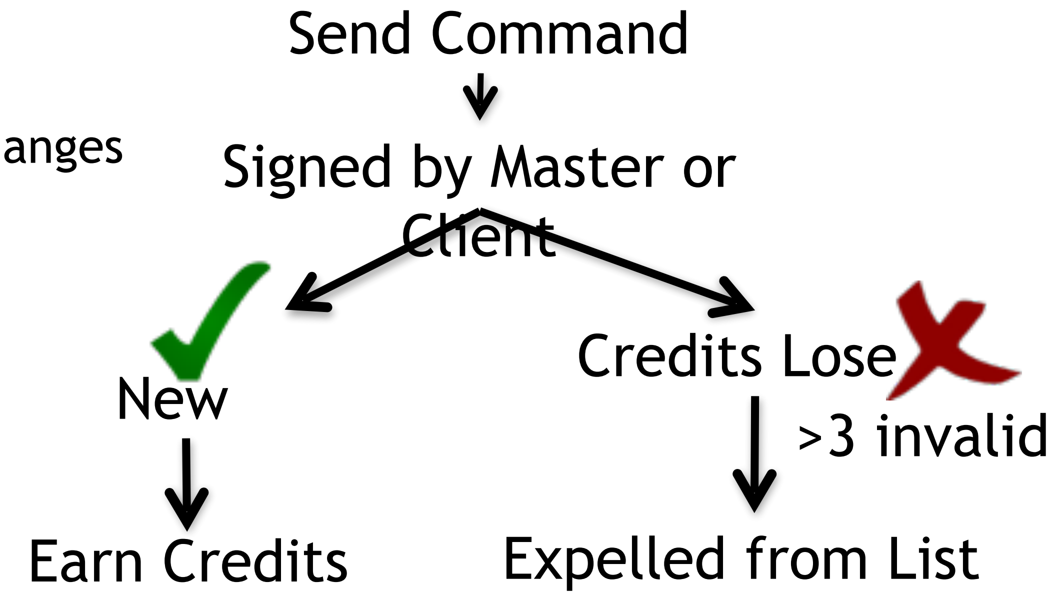
Old peers have priority

Difficult to crawl older bots

Peer-to-Peer Trust

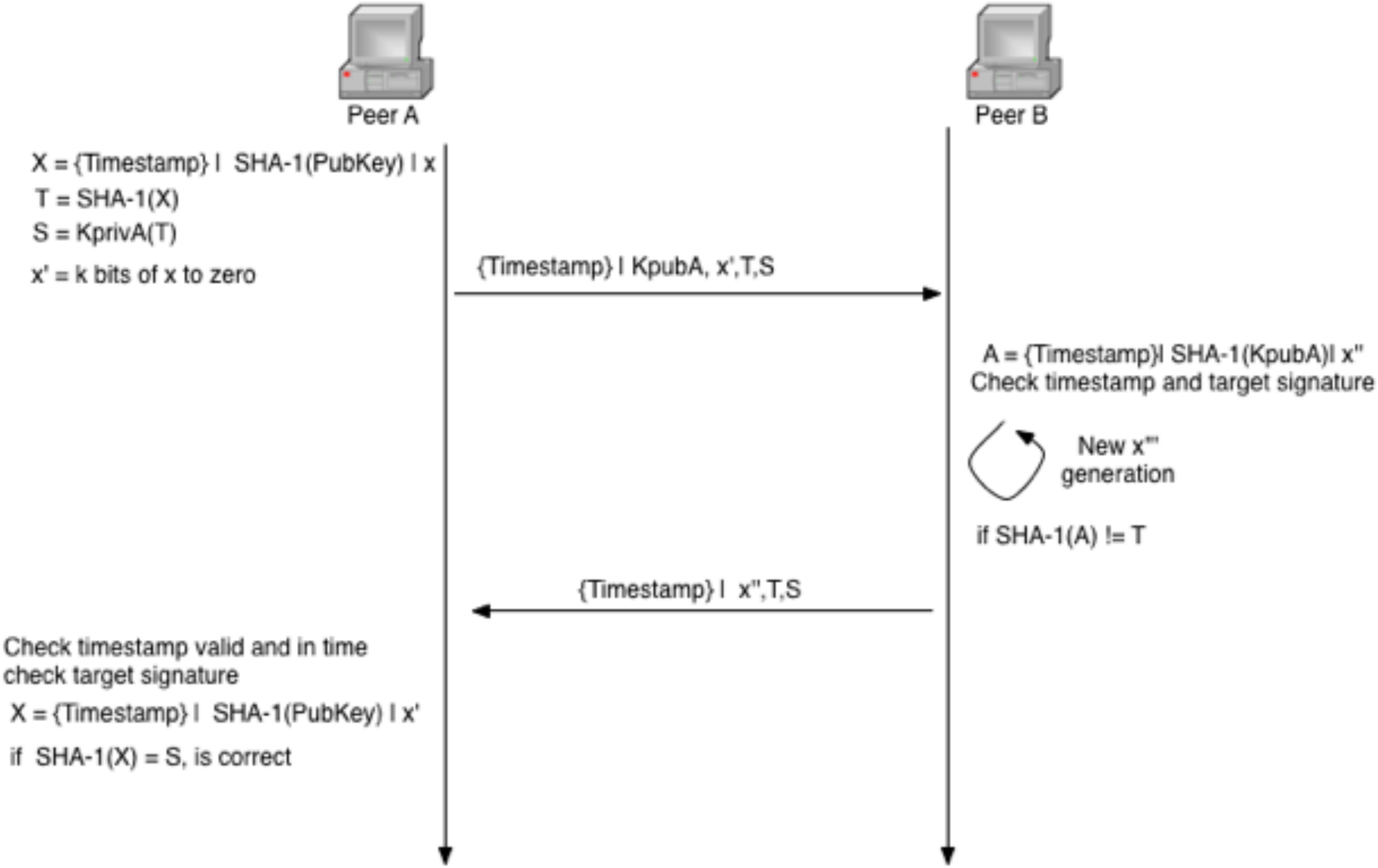
Send Commands

- Preference to avoid key Exchanges
- Random Send



It doesn’t avoid Sybil Attacks

Proof-of-Work



X = {Timestamp} I SHA-1(PubKey) I x
T = SHA-1(X)
S = KprivA(T)
x' = k bits of x to zero

{Timestamp} I KpubA, x',T,S

A = {Timestamp}I SHA-1(KpubA)I x"
Check timestamp and target signature

New x'''
generation

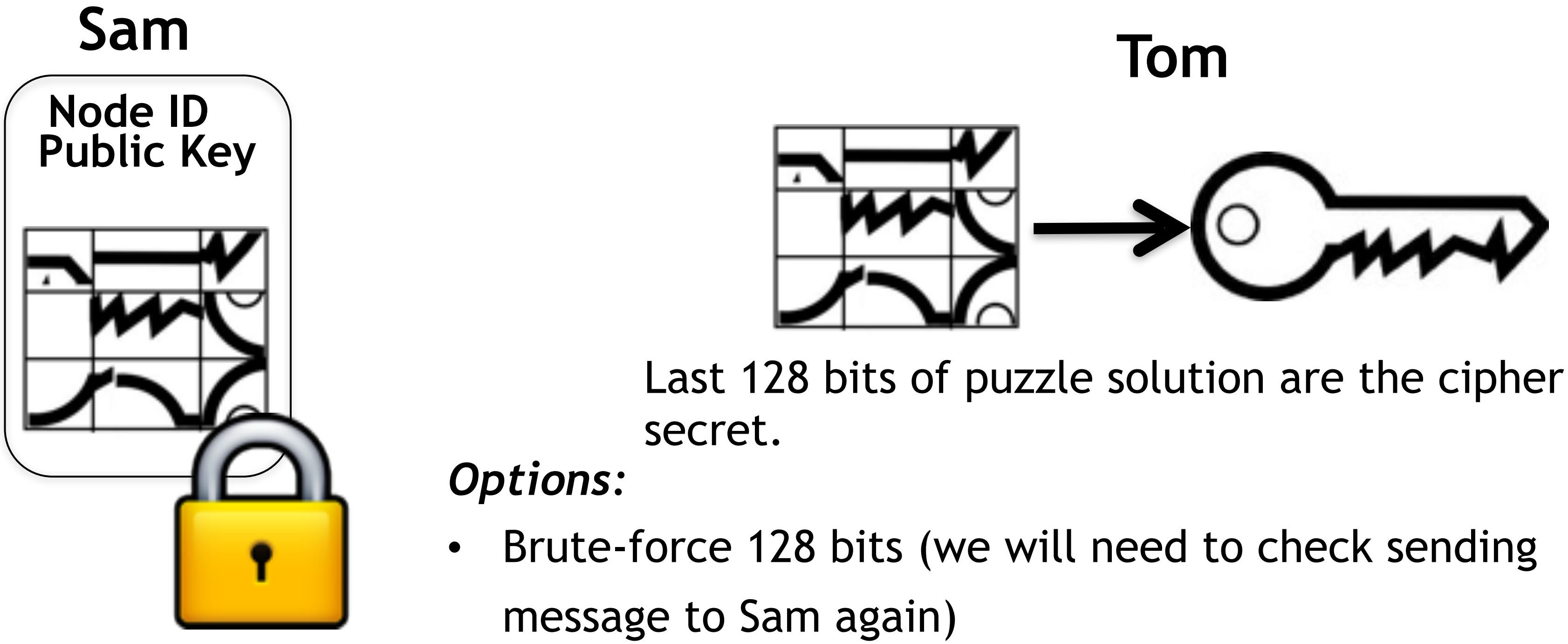
if SHA-1(A) != T

{Timestamp} I x",T,S

Check timestamp valid and in time
check target signature
X = {Timestamp} I SHA-1(PubKey) I x'
if SHA-1(X) = S, is correct

Mafia Proof-of-Work

Sam wants add Tom to his Accomplice List, they must show that they work to Mafia

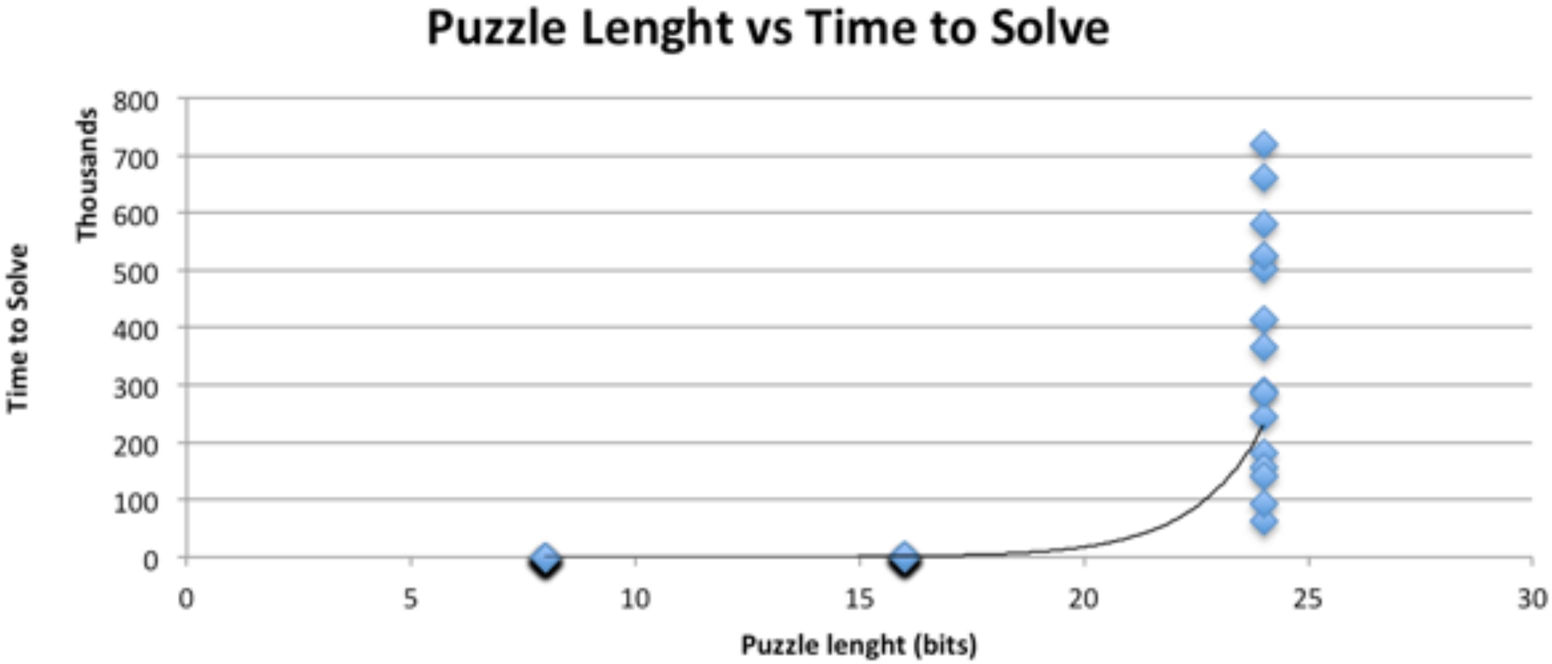


Last 128 bits of puzzle solution are the cipher secret.

Options:

- Brute-force 128 bits (we will need to check sending message to Sam again)
- Solve the puzzle 16 bits

Proof-of-Work



Bit	Attemps	% Total	Time Avg
8	122	47.65	22 ms
16	29 486	44.99	1 sec
24	8 327 669	49.63	6 min
32	2 147 milion	49.98	25 hours
64	9.22337×10^{18}	50%	12 306 411 years

Average key difficulty is half of size

23.75 attemps / mili secound - Java is slow

Prices on Darknet

Citadel (Zeus variant, financial botnet):

US$2,399

$125 for “rent” botnet builder and administration panel

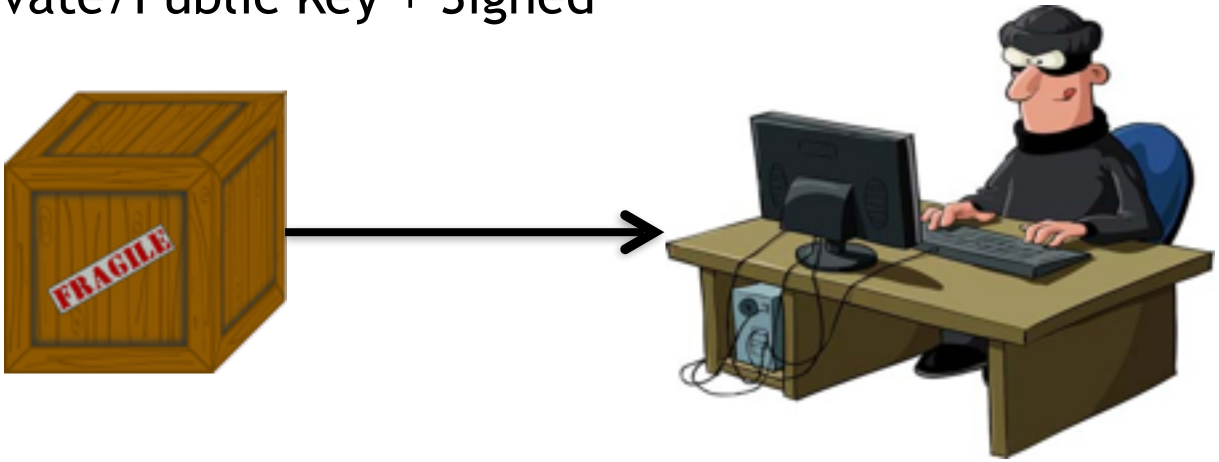
$395 for automatic updates for antivirus evasion

Darkness (DDoS)

From $450 until $1.000

Monetization Model

Botmaster Generate Private/Public Key + Signed Certificate



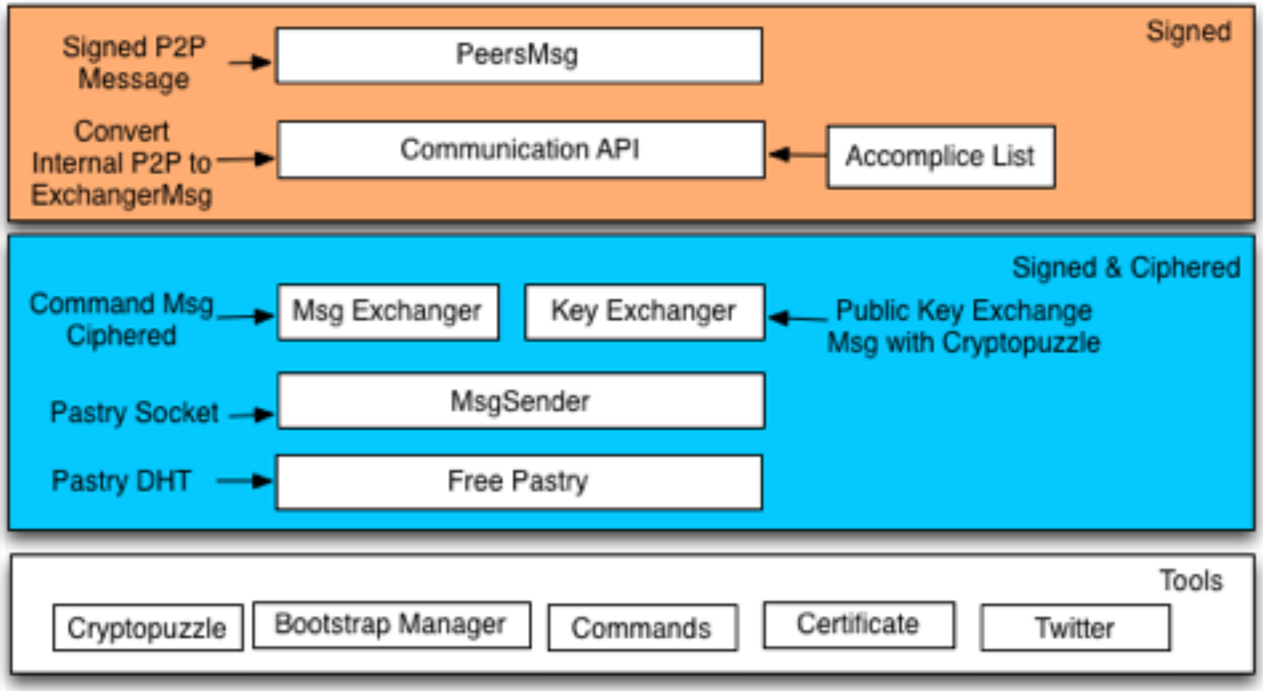
Attacker sign the command with his private key

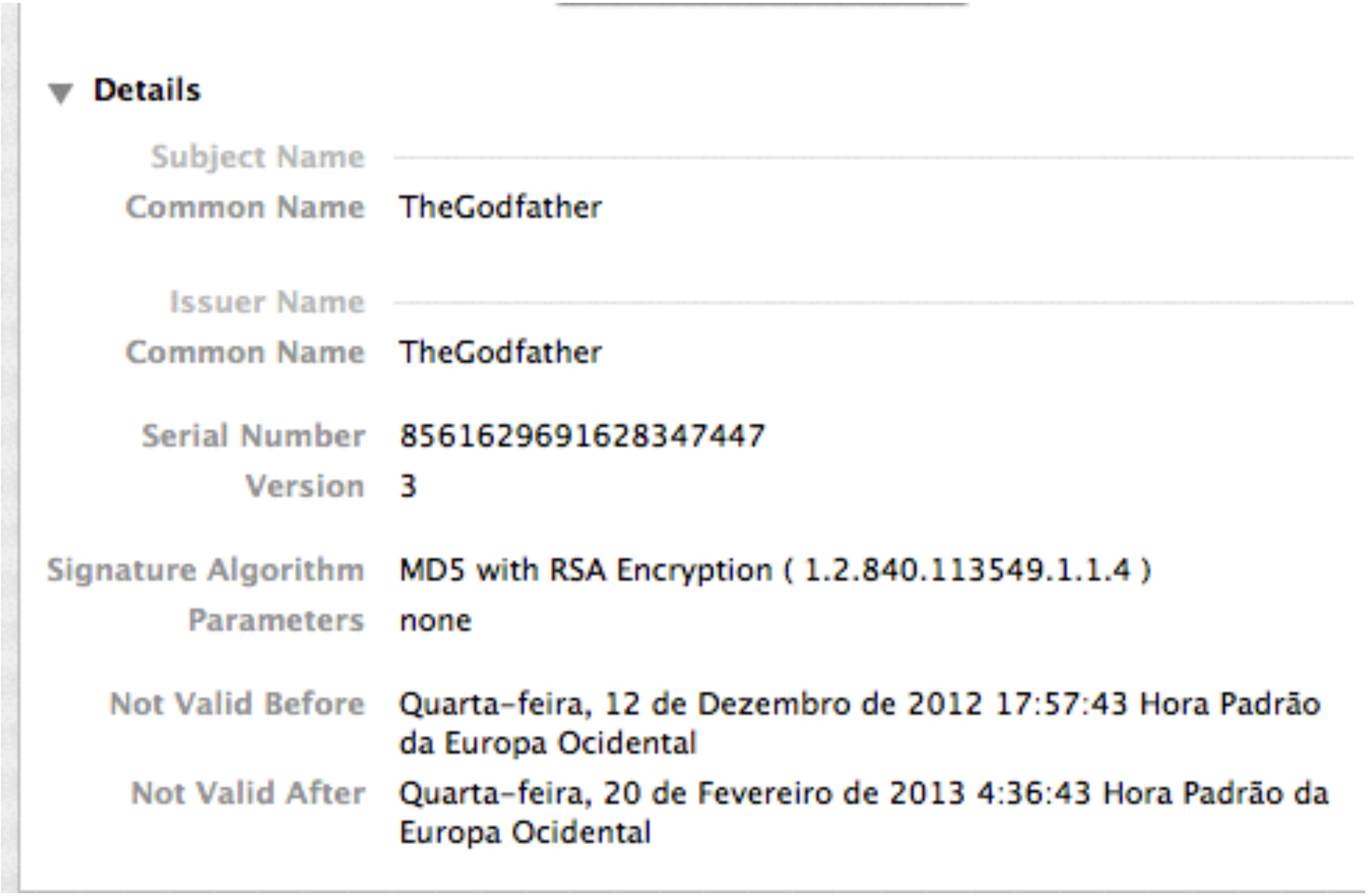
Send the signed command + signature

Bot check the certificate signature, attack and forward the message

Solution Architecture

- Peer-to-Peer DHT with signed commands
- Cipher messages transfer
- Cryptopuzzle generator and solver
- Certificate generator
- Twitter Bootstrapper
- Reputation Accomplice List





▼ **Details**

Subject Name	
Common Name	TheGodfather
Issuer Name	
Common Name	TheGodfather
Serial Number	8561629691628347447
Version	3
Signature Algorithm	MD5 with RSA Encryption (1.2.840.113549.1.1.4)
Parameters	none
Not Valid Before	Quarta-feira, 12 de Dezembro de 2012 17:57:43 Hora Padrão da Europa Ocidental
Not Valid After	Quarta-feira, 20 de Fevereiro de 2013 4:36:43 Hora Padrão da Europa Ocidental

Demo Time!

Conclusions

- Keeping both low level of traffic and guarantee secure connections it’s hard in botnets
- Attacks such as DoS are easy to perform
- Botnet detection systems evolved, trust mechanisms are required
- All will be released with researching purpose in mind

Thank you!

Q&A