BOTCOIN
Bitcoin-Mining on Botnets

Danny Y. Huang
Hitesh Dharmdasani, Sarah Meiklejohn
Vacha Dave, Chris Grier, Damon McCoy
Stefan Savage, Nicholas Weaver
Alex C. Snoeren, Kirill Levchenko
Motivation

Unique IP address → Money

Spam → $$$

Click-fraud → $$$

Computational Power → Money

Mining Bitcoins → $$$
Motivation

Kevin
Loss in productivity
High electricity bill

Scale?
- Who?
- Operations?
- Profitable?

Implications?
- Bitcoin-mining in relation to spam/click-fraud?
Contributions

What we learned about botnets:

- Identities
- Modus Operandi
- Revenue
- Implications
How you can make bitcoins

Pick a different integer

P2P Network

Apply SHA-256 on integer

Mining App Takes 100+ years

Found hash collision

Get 25

5
Mining Pools

- Parallelizes hashing.
- Finds solution faster.
- Workers divide reward.

BUT:
- Hardware costs
- Energy costs

Free!

miner.exe my_wallet http://pool.com
Botnet Mining

Malware connects to pool

Victim  Victim  Victim

Pool pays botnet

We want to identify these botnets!

miner.exe botnet_wallet http://pool.com
Finding the Mining Malware

Malware Databases
   Threat Expert, Emerging Threats, ...

2,000 binaries
10 botnets

Bitcoin Malware
   Reports / Blogs

Leaked Data
   Interviews with Pools
Examples of Mining Botnets

- **ZeroAccess**
  - Spamming,
  - click-fraud
  - Bitcoin-mining

- **FeodalCash**
  - Affiliate program

- **BMControl**
  - bitcoin wallet addresses in public cloud

- Hitman
  - UK

- Dload asia

- Zenica

- Fareit

- gamers

- xfhp.ru

- misc
Outline

*What we learned about botnets:*

**Identities**
- 2,000 binaries
- 10 botnets

**Modus Operandi**
- e.g. affiliate program, wallet addresses in cloud

**Revenue**

**Implications**
Botnet Mining Revenue

ZeroAccess
486 bitcoins in 1 year

FeodalCash
168 bitcoins in 3 months

BMControl
3,000 bitcoins in 1 year

Lots of challenges!

Gather botnet wallet addresses

Look up in public ledger (i.e. blockchain)

Examine payments from mining pool (Meiklejohn et al)
Botnet Revenue in Bitcoins

![Graph showing Bitcoin Price in US Dollars and Mining Revenue (BTC/day)]

- **ZeroAccess**
- **BMControl**
- **FeodalCash**
Botnet Revenue in US Dollars

![Graph showing the revenue in US Dollars over time. The graph is divided into two sub-plots: one for Bitcoin Price in US Dollars, and another for Mining Revenue (USD/day). The x-axis represents months from May 2012 to July 2013.]
Mining Revenue
Litecoin Mining

- Different hash function
  - Bitcoin: SHA-256
  - Litecoin: Scrypt

Number of New Botnet Mining Operations

Litecoin Mining Revenue
Outline

What we learned about botnets:

**Identities**
- 2,000 binaries
- 10 botnets

**Modus Operandi**
- e.g. affiliate program, wallet addresses in cloud

**Revenue**
- 4,000 bitcoins
- in 2 years

**Implications**
Implication & Conclusion

Spam
Click-fraud
Bitcoin-mining
Litecoin-mining
*coin-mining
Outline

What we learned about botnets:

- Identities
- Modus Operandi
- Revenue
- Implications