6cure
secure your business

Dec-18

How much should you pay for your own botnet?

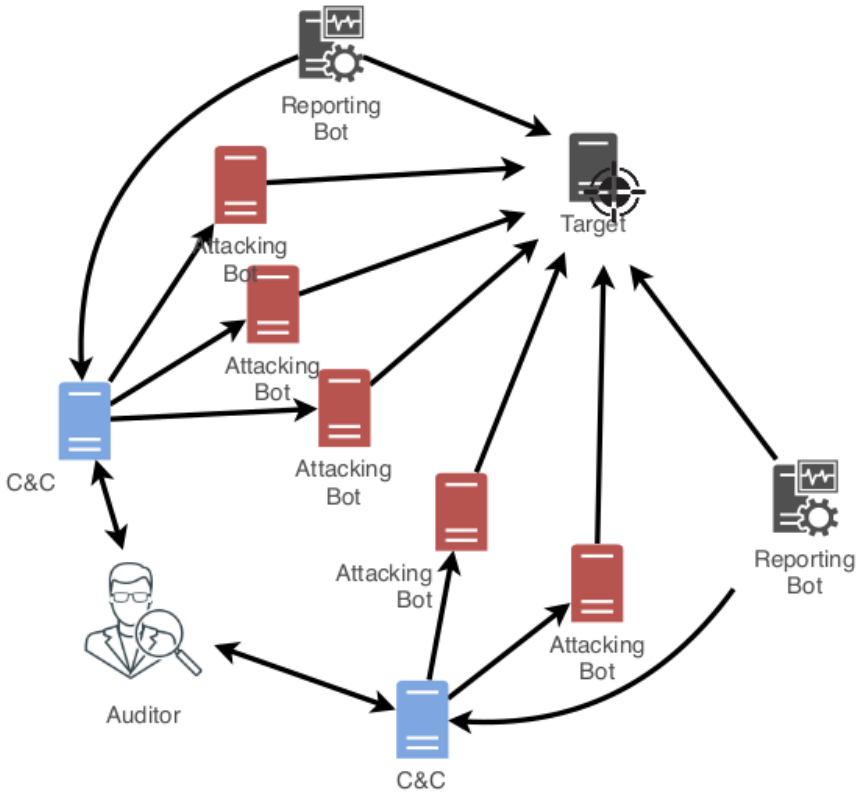
Antoine REBSTOCK, Pierre-Edouard FABRE, Emmanuel BESSON

who am I?

Antoine Rebstock

@AntoineRebstock

what is this talk about?



- **DDoS resilience tests**
  - **legal** audit
  - purposed-built, controlled & **cloud-based** botnet
- **how much does it costs?...**

sorry, we will not talk about...

- **legal & ethical issues**
  - DDoS law
  - authorizations

- **detailed technical how-to**
  - attack types
  - spoofing issues

agenda

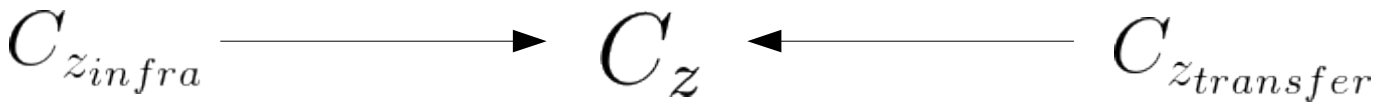
- **back to school**
  - botnet cost model
- **comparative survey**
  - infrastructure & data costs
- **use case**
- **discussion & further research**

How much should you pay for your own botnet?

back to school...

back to school...

- **theorical cost for audit z**
  - infrastructure
  - data transfer



- **cost variables**
  - infrastructure
    - a nb of attack bots
    - r nb of report bots
    - c nb of C&Cs
    - T instance operating time (mn)
    - x_1 unit price (€ per instance per mn)
  - data transfer
    - i index of price stage
    - d transferred volume (GB)
    - n nb of price stages (per month)
    - x_2 unit price (per GB)
    - S global throughput (Mbps)
    - s individual bot throughput (Mbps)
    - t_2 flood duration

back to school...

- **theorical audit cost**
  - infrastructure & data (transfer) costs

$$C_z = \overbrace{(a_z + r_z + c_z)x_1 T_z}^{C_{z_{infra}}} + \overbrace{\frac{\sum_{i=1}^{n} d_i x_{2_i}}{\sum_{i=1}^{n} d_i} d_z}^{C_{z_{transfer}}}$$

$$d_z = \frac{\frac{S_z}{8} \times 60}{1000} t_{2_z} = \frac{15}{2000} (\sum_{u=1}^{a_z} s_{z_u}) t_{2_z}$$

back to school...

- **theorical audit cost**
  - infrastructure & data (transfer) costs

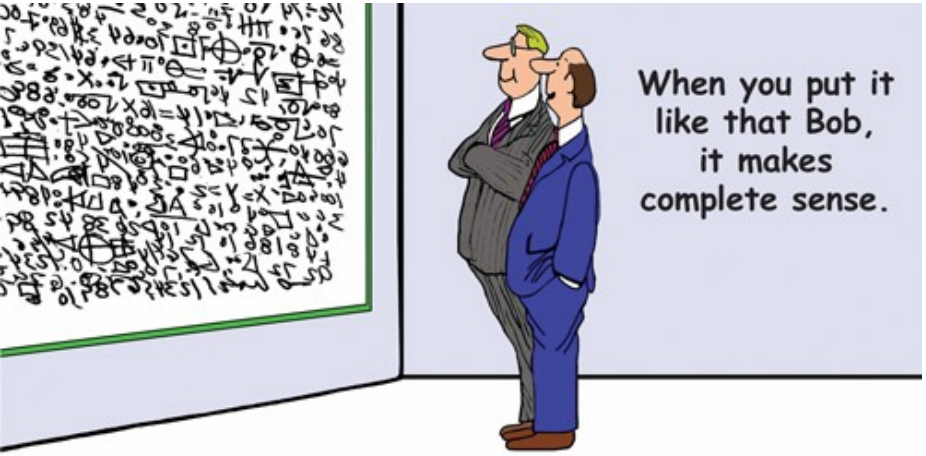
$$C_z = \underbrace{\sum_{l=1}^{k}\sum_{p=1}^{j}[(a_z + r_z + c_z)x_1 T_z]_{p_l}}_{C_{z_{infra}}} + \underbrace{\sum_{l=1}^{k}\sum_{p=1}^{j}[\frac{\sum_{i=1}^{n} d_i x_{2_i}}{\sum_{i=1}^{n} d_i} d_z]_{p_l}}_{C_{z_{transfer}}}$$

- **additional cost variables**
  - infrastructure
    - l nb of locations
    - p nb of cloud providers

$$d_z = \frac{\frac{S_z}{8} \times 60}{1000} t_{2_z} = \frac{15}{2000}(\sum_{u=1}^{a_z} s_{z_u}) t_{2_z}$$

theorical audit cost

$$C_z = \sum_{l=1}^{k} \sum_{p=1}^{j} [(a_z + r_z + c_z) x_1 T_z + \frac{\sum_{i=1}^{n} d_i x_{2_i}}{\sum_{i=1}^{n} d_i} d_z]_{p_l}$$



$$d_z = \frac{\frac{S_z}{8} \times 60}{1000} t_{2_z} = \frac{15}{2000} (\sum_{u=1}^{a_z} s_{z_u}) t_{2_z}$$

6cure
secure your business

How much should you pay for your own botnet?

comparative survey

infrastructure cost

- **assumptions**
  - instance size: 2vCPU – 4GB
  - geographical area: France

Providers	Areas	Instances	vCPU	RAM	ROM	Bandwidth (Mbps)	Price(€)/Instance/h (ET)
Microsoft	Paris	b2s	2	4	8	?	0.0440 €
Amazon	Paris	t2.medium	2	4	?	?	0.0450 €
Google	Belgique	customisée	2	4	?	?	0.0752 €
Orange	Paris	c2.large	2	4	?	?	0.0841 €
Amazon	Paris	c5.large	2	4	?	?	0.0862 €
Microsoft	Europe Ouest	F2v2	2	4	16	?	0.0870 €
Cloudwatt	Normandie	n1.cw.highcpu-2	2	4	50	400	0.0870 €
Microsoft	Paris	a2v2	2	4	20	?	0.0900 €
Orange	Paris	h1.large.2	2	4	?	?	0.1024 €

low

geographically variable

infrastructure cost

geographical multiplier factor

- **instance in same area**
  - reference: France/Western Europe

Providers	Areas			
X	North America	South America	Asia	Oceania
Orange	X	X	1.4	X
Microsoft	0.9	1.5	1.1	1.3
Amazon	0.9	1.5	1	1.2
Google	1	1.4	1.1	1.3

data transfer cost

France (Western Europe) area

significant

provider dependent

Providers	Price(€) / GB / month (ET)									
X	1st GB	< 5 GB	< 15GB	< 1TB	< 2TB	< 10TB	< 50TB	< 150TB	< 500TB	+ 500TB
Cloudwatt	0.000 €					0.014 €	Contact			
Orange	0.000 €			0.070 €			0.066 €	0.054 €	0.038 €	Contact
Microsoft	0.000 €		0.074 €				0.070 €	0.060 €	0.043 €	Contact
Amazon	0.000 €	0.077 €					0.073 €	0.060 €	0.043 €	Contact
Google	0.103 €				0.094 €		0.069 €			

data transfer cost

geographical multiplier factor

- **instance in same area**
  - reference: France/Western Europe

Providers	Areas			
X	North America	South America	Asia	Oceania
Orange	Irrelevant instances	X	2	X
Microsoft	1	3.2	1.6	1.6
Amazon	1	3.8	1.6	2.4
Google	1	1	1	1.9

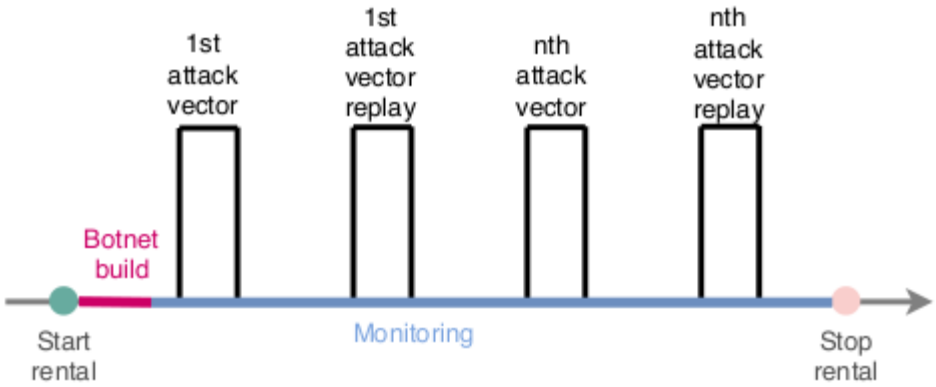
How much should you pay for your own botnet?

use case

use case
single audit

- **infrastructure**
  - France
  - 100 attack bots + 11 report bots + 6 C&Cs

- **duration**
  - 30mn botnet setup
  - 3 (volumetric) attacks
    - 2x 5mn-shots
    - 30mn inter-shots
  - 30mn post-attack



- **data transfer**
  - 400Mbps throughput per bot → 9TB data transferred

use case

infrastructure cost

Provider	Area	Instance	Price/instance/h (ET)
Orange	Paris	h1.large.2	0.1024 €

$$C_{z_{infra}} = (a_z + r_z + c_z) x_1 T_z$$

$$T_z = setup + \#attacks \times \#shots \times attack\_duration + (\#attacks \times \#shots - 1) \times inter\_attack\_duration + post\_attack$$

$$(100 + 11 + 6) \times \frac{0.1024}{60} \times (30 + 3 \times 2 \times 5 + (3 \times 2 - 1) \times 30 + 30) = 47.93$$

use case

data transfer cost

Provider	Price/GB/month (ET)					
X	15 GB	< 10TB	< 50TB	< 150TB	< 500TB	+ 500TB
Orange	0.000 €	0.070 €	0.066 €	0.054 €	0.038 €	Contact

$$C_{z_{transfer}} = \frac{\sum_{i=1}^{n} d_i x_{2_i}}{\sum_{i=1}^{n} d_i} \times \frac{\frac{S_z}{8} \times 60}{1000} t_{2_z}$$

$$t_{2_z} = \#attacks \times \#shots \times attack\_duration$$

$$\frac{0 \times 15 + 8985 \times 0.070}{9000} \times \frac{\frac{400 \times 100}{8} \times 60}{1000} \times (3 \times 2 \times 5) = 628.95$$

use case

provider comparision

- **equitability**
  - price/service ratio equivalence

X	Infrastructure	Data transfer	Total
Cloudwatt*	40.73 €	98.00 €	138.73 €
Orange	47.93 €	628.95 €	676.88 €
Microsoft	42.12 €	665.63 €	707.75 €
Amazon	40.34 €	692.92 €	733.26 €
Google	35.18 €	855.00 €	890.18 €

How much should you pay for your own botnet?

discussion & further research

discussion

- **approximations**
  - calculation of multiplier factor
  - single provider/location
  - only attack (flood) traffic considered
- **lack of information**
  - throughput limitations
  - detailed processor characteristics
- **to be confirmed**
  - preeminence of data transfer costs
  - provider detection schemes

conclusion

- **audit cost**
  - depends on multiple factors (approx. required)
  - affordable cost for (target) customer
- **how to choose?**
  - provider data costs
  - IP diversity
  - flexibility in instance management
- **further research**
  - technical how-to & assumptions

6cure
secure your business

How much should you pay for your own botnet?

see you later

thank you for your attention