DAMBALLA

Take Back Command-and-Control

VB2010, Vancouver

Size Matters

Measuring a Botnet Operator’s Pinkie

Gunter Ollmann, VP Research

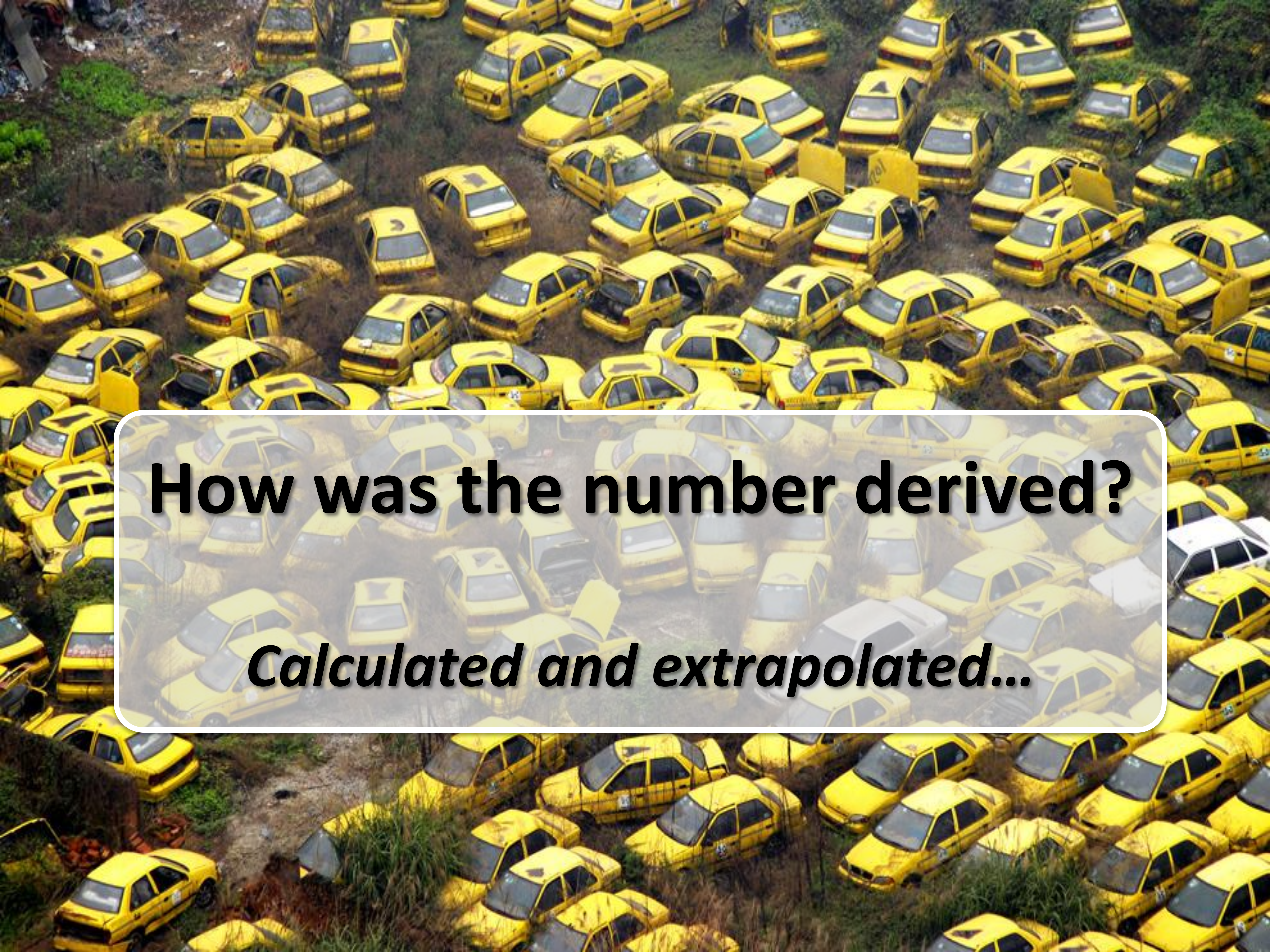
gollmann@damballa.com

About

- **Gunter Ollmann**
  - VP of Research, Damballa Inc.
  - Board of Advisors, IOActive Inc.
- **Brief Bio:**
  - Formerly Chief Security Strategist for IBM, Director of X-Force for ISS, Professional Services Director for NGS Software, Head of Attack Services EMEA, etc.
  - Frequent writer, columnist and blogger with lots of whitepapers…
    - http://blog.damballa.com & http://technicalinfodotnet.blogspot.com/

Worldwide Threat Statistics

Different vendor, different numbers…

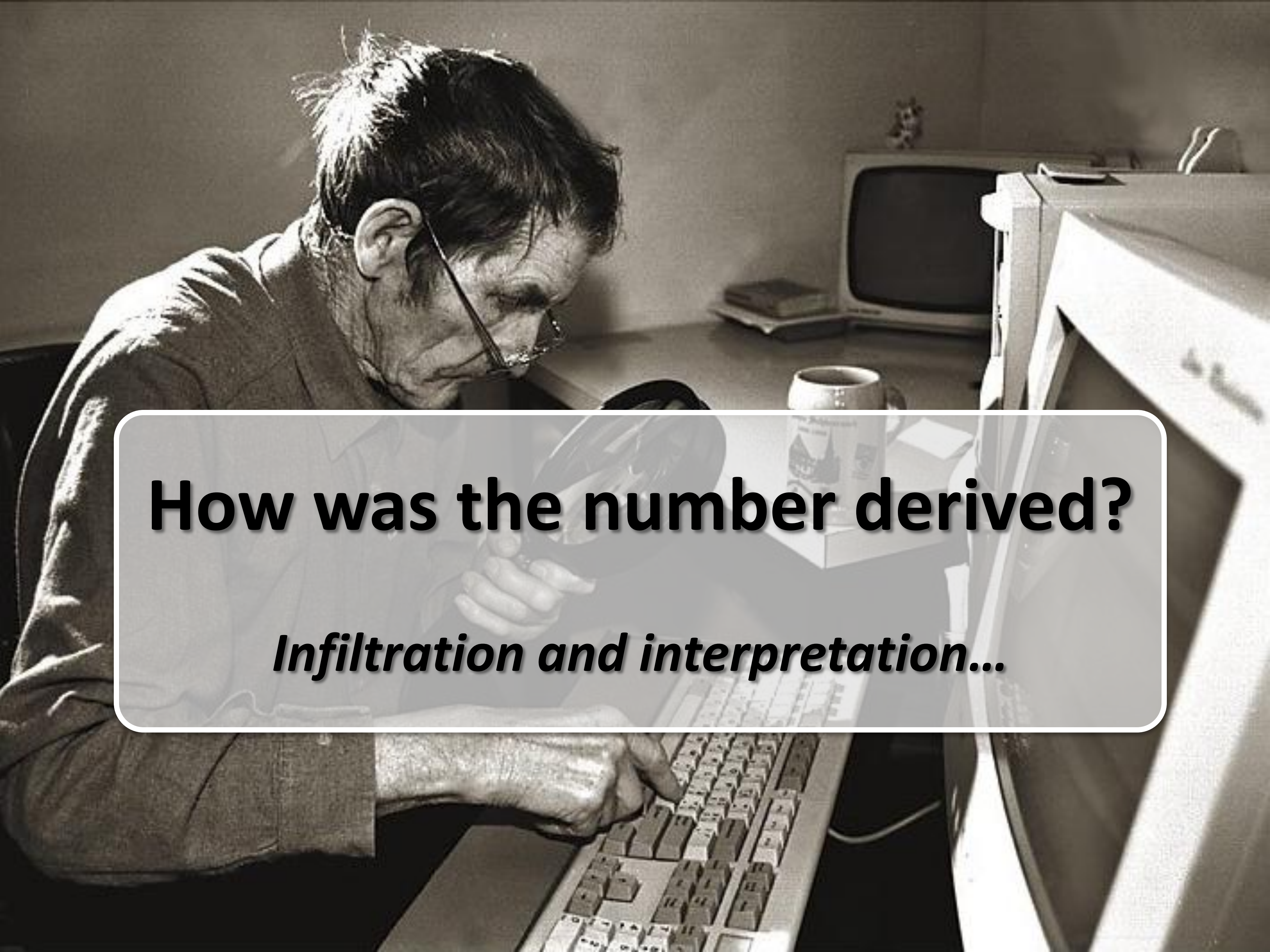


How was the number derived?

Calculated and extrapolated…

How was the number derived?

Sinkholes, spam traps and honeypots…

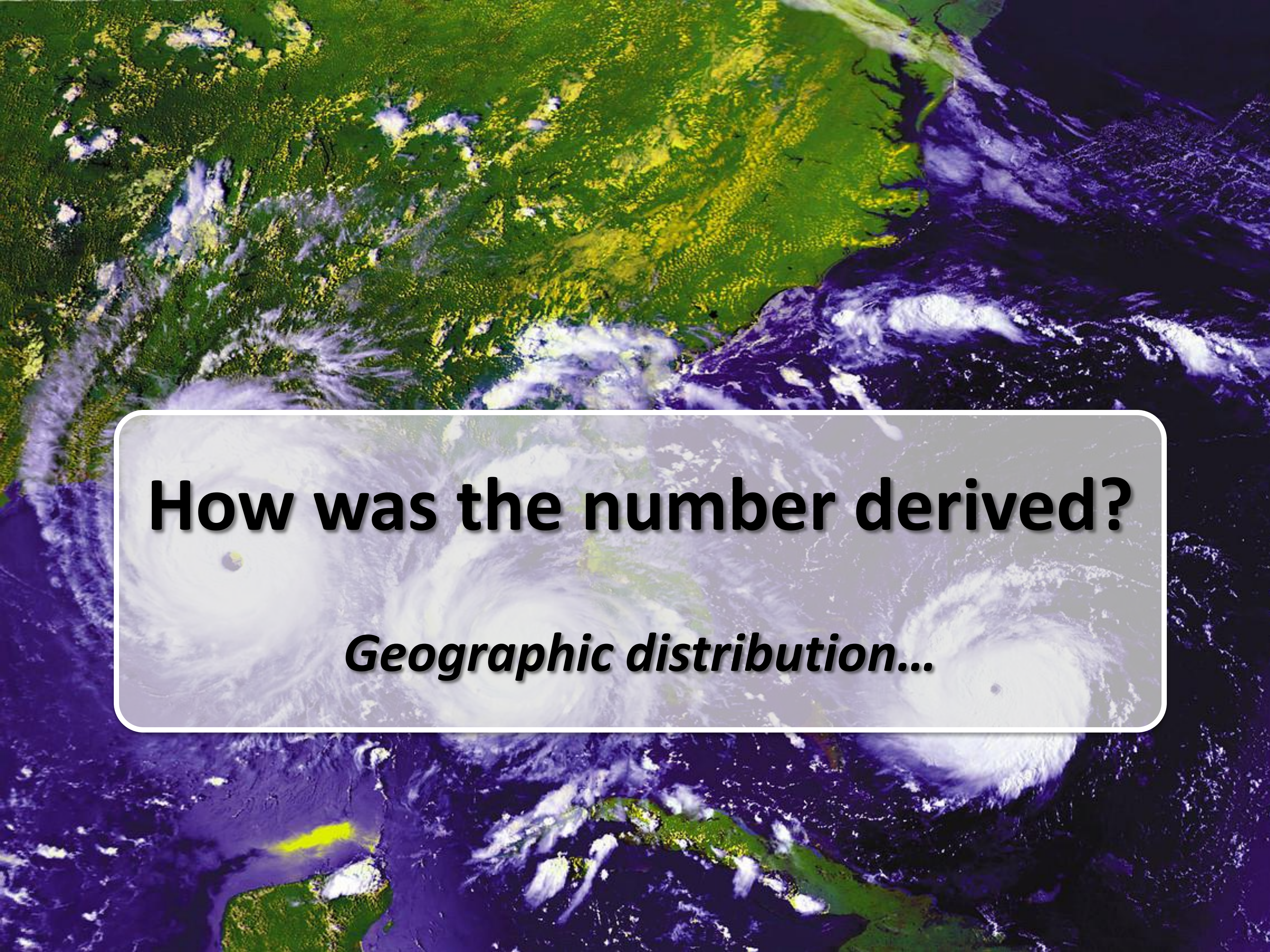


How was the number derived?

Infiltration and interpretation…

How was the number derived?

Victim counts from customers…



How was the number derived?

Geographic distribution…

Who’s right?

Trust me, I’m a professional

Serial variant production

…New & unique piece of malware

…"on the fly" creation of malware

New bot agent for every victim

…Frequent updates of agents (<24hrs)

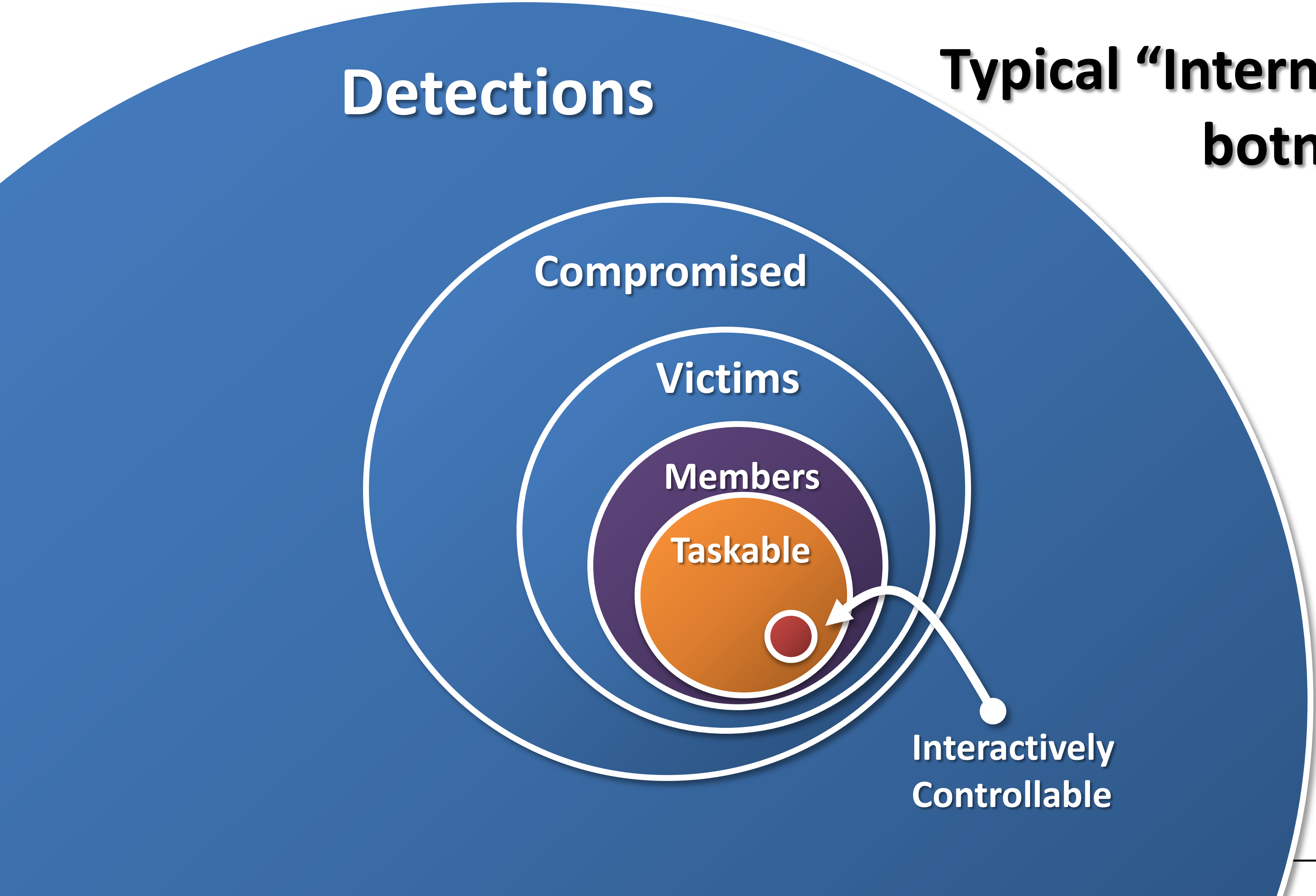
…QA tested and designed to evade

Threat Measurements

- **Differences between the numbers:**
  - – Detections (malicious files in circulation)
  - – Compromises (Malware making it to the host)
  - – Victims (actually infected with the malware)
  - – Botnet members (victim hosts that can connect)
  - – Taskable Bots (capable of being assigned tasks)
  - – Controllable Bots (can be interactively controlled)

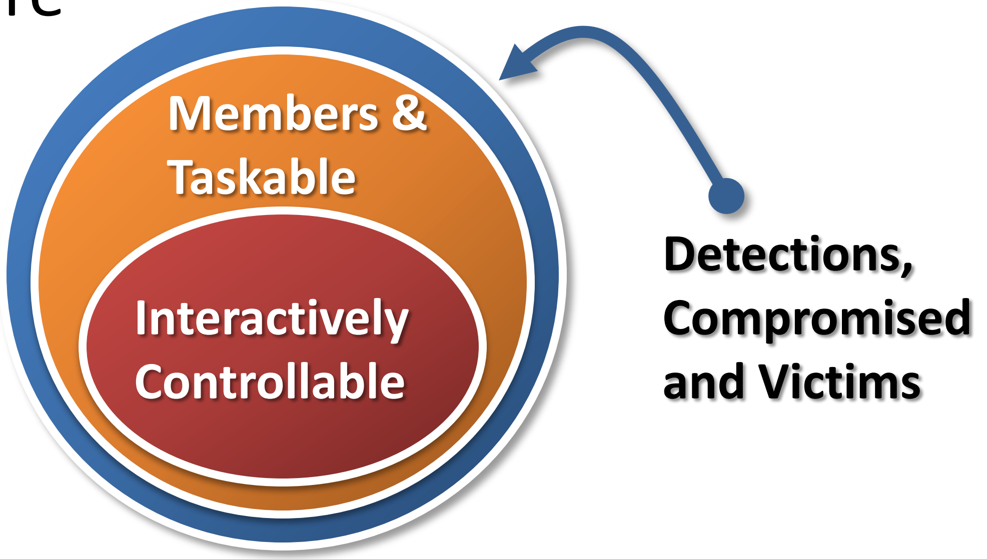
Threat Measurements

Typical "Internet" botnets



Threat Measurements

- **Characteristics of Enterprise botnets**
  - Detections happen at the pace of compromise and victimization
  - All members are taskable


Members & Taskable
Interactively Controllable
Detections, Compromised and Victims

Best way to measure size?

Sinkholed CnC Domains…
…got to capture all the domains and correlate between them

Best way to measure size?

Authoritative DNS Server…
…counting all DNS resolutions
and location diversity

Best way to measure size?

Spanning ports…
…observing bi-directional CnC traffic

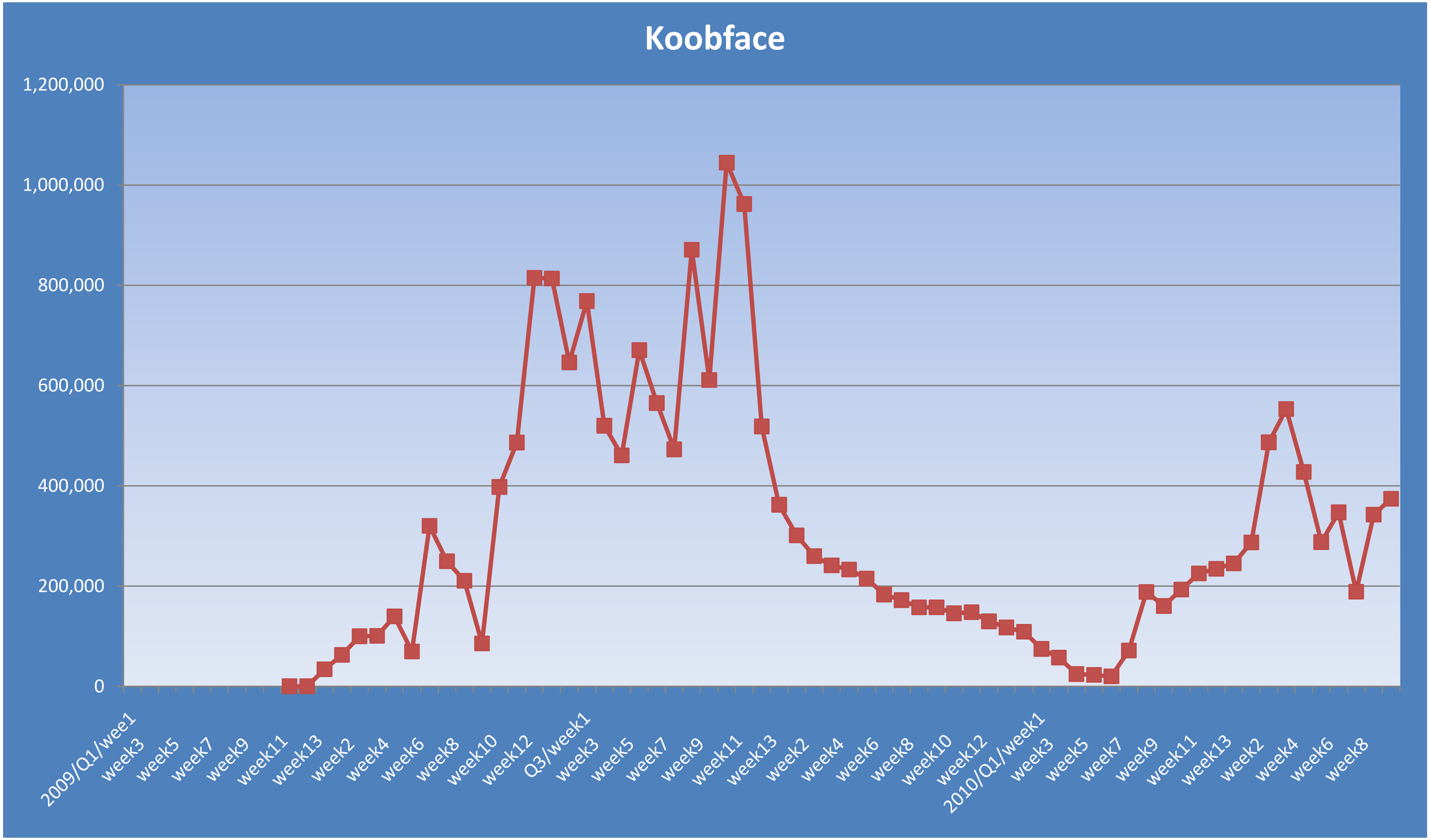
Keeping track is difficult

Singling out a unique "victim"

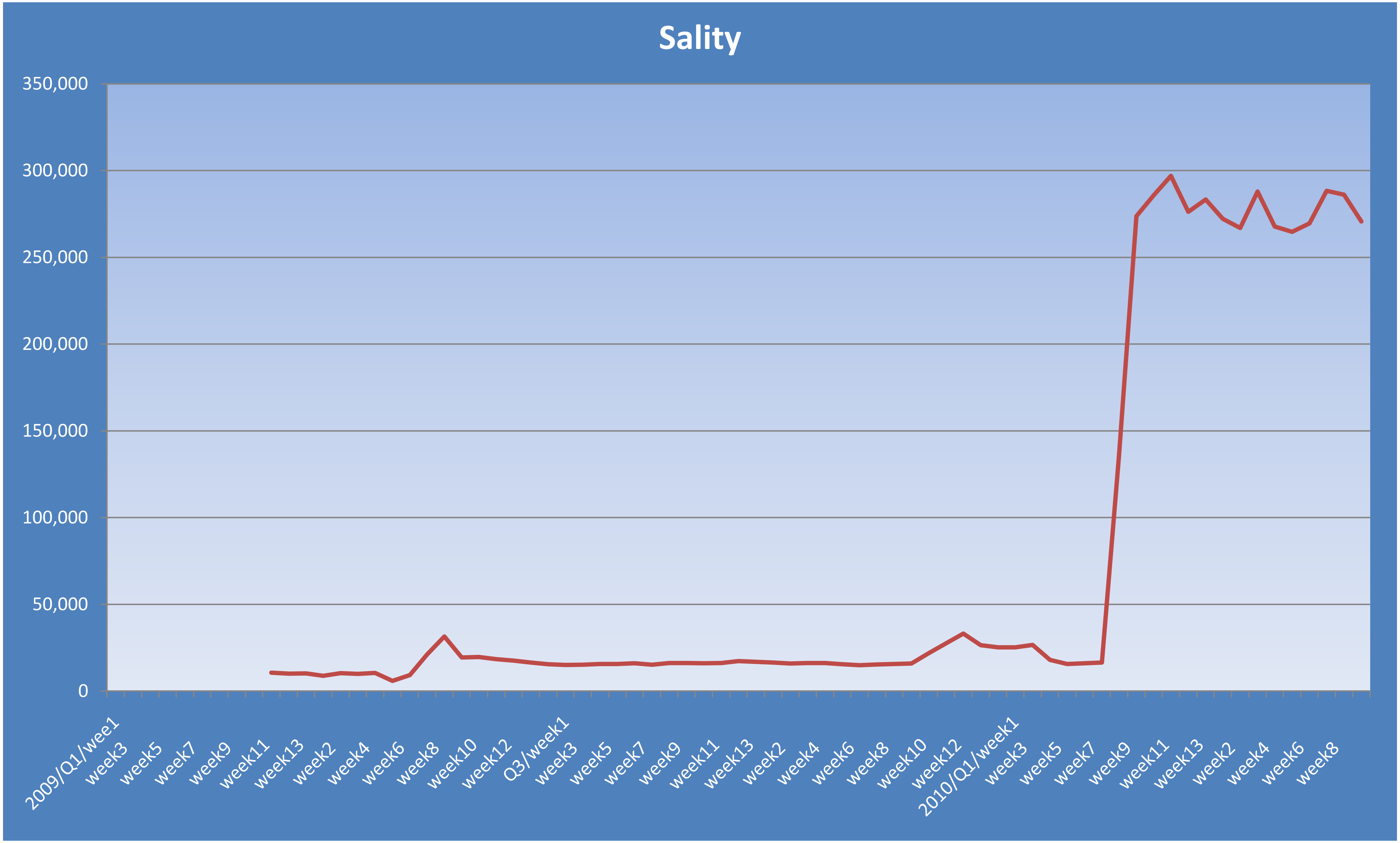
Large Internet Botnets

- **CnC traffic appears to be an ideal way of measuring size of the botnet…**
- **Look at three large/common botnets**
  - Koobface, Sality, Monkif
- **Count number of successful connections to botnet CnC (unique IP per week)**

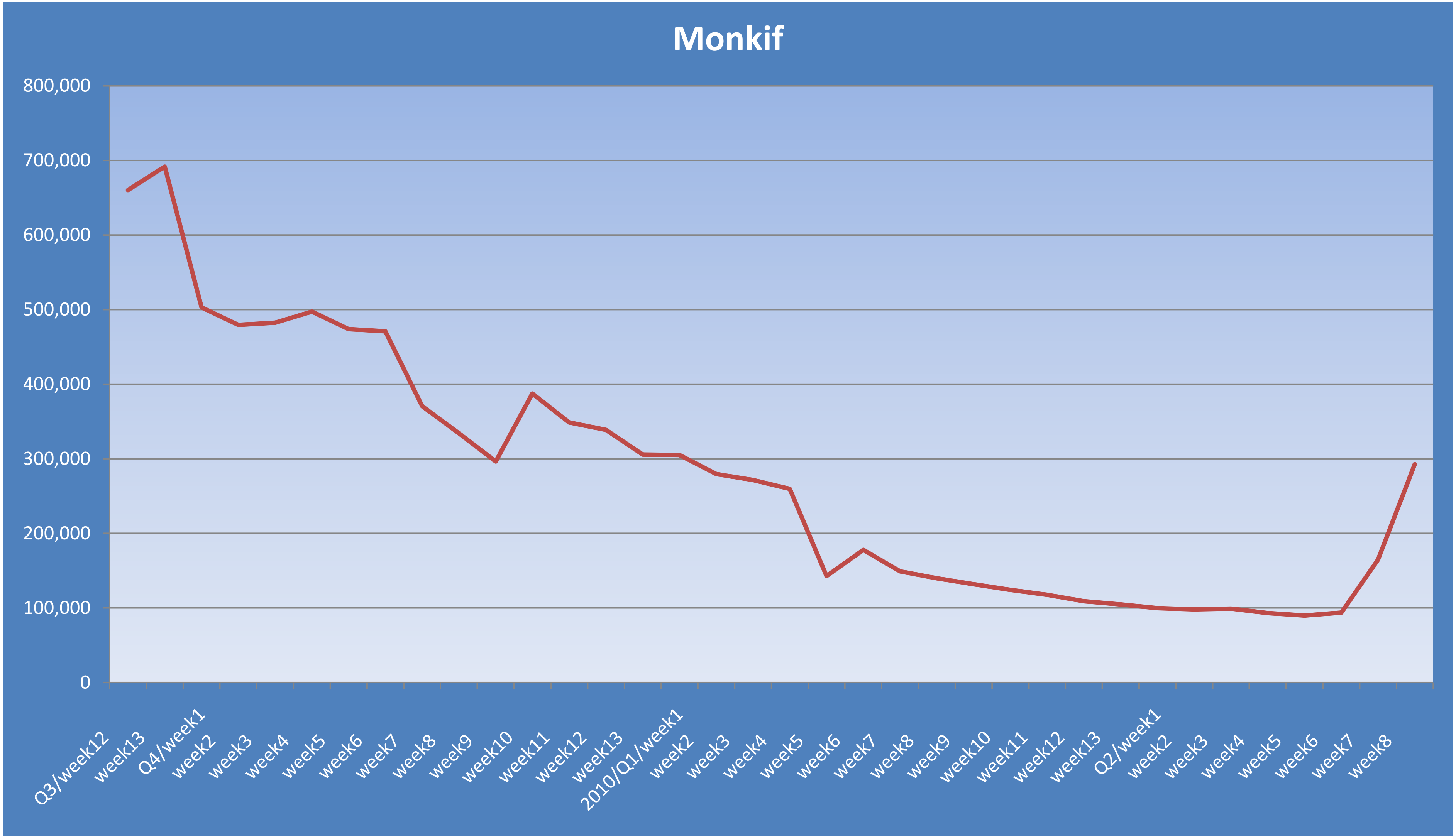
Koobface

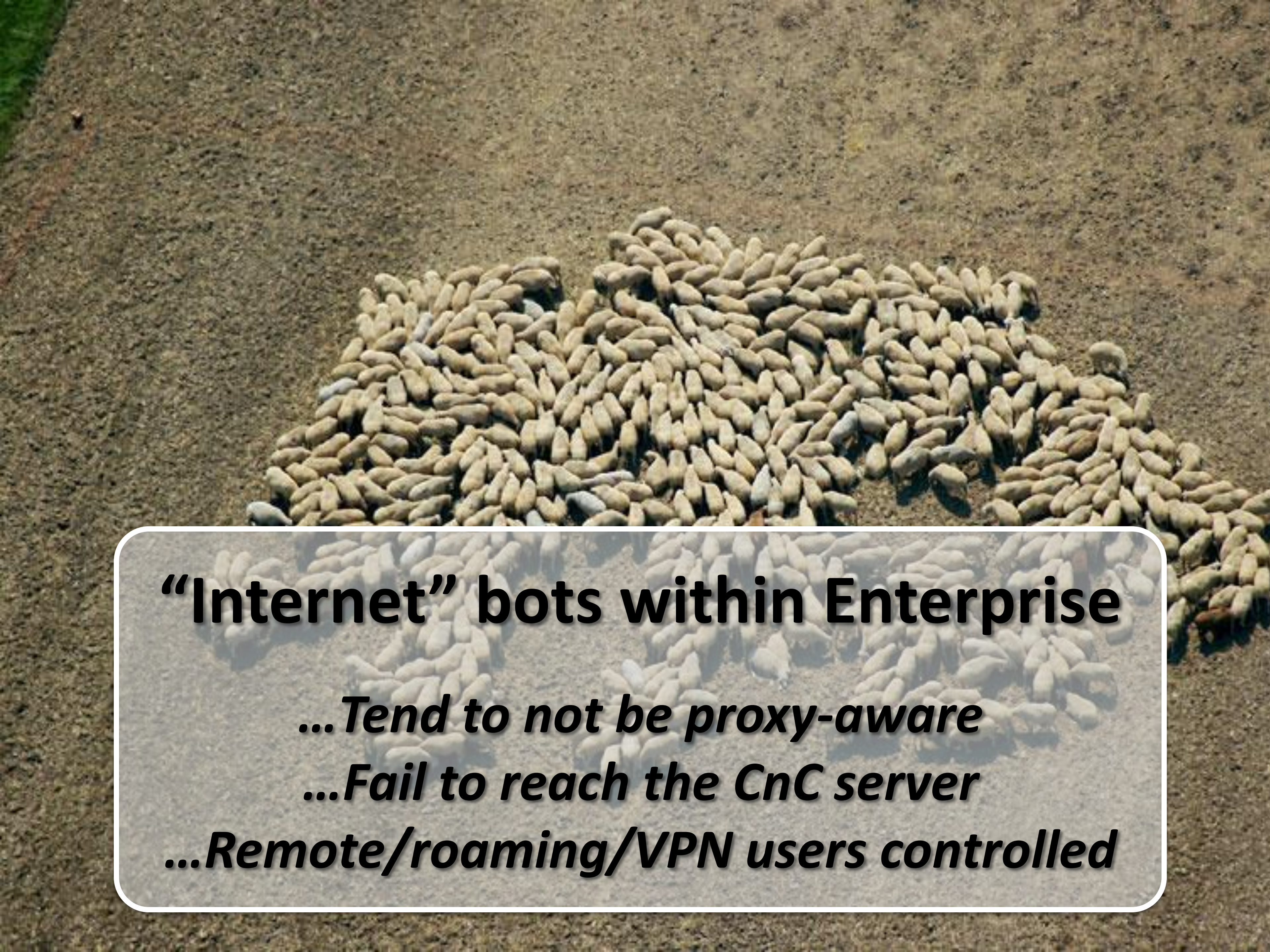

Koobface
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
2009/Q1/wee1
week3
week5
week7
week9
week11
week13
week2
week4
week6
week8
week10
week12
Q3/week1
week3
week5
week7
week9
week11
week13
week2
week4
week6
week8
week10
week12
2010/Q1/week1
week3
week5
week7
week9
week11
week13
week2
week4
week6
week8

Sality


Sality
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
2009/Q1/wee1
week3
week5
week7
week9
week11
week13
week2
week4
week6
week8
week10
week12
Q3/week1
week3
week5
week7
week9
week11
week13
week2
week4
week6
week8
week10
week12
2010/Q1/week1
week3
week5
week7
week9
week11
week13
week2
week4
week6
week8

Monkif


Monkif
800,000
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
Q3/week12
week13
Q4/week1
week2
week3
week4
week5
week6
week7
week8
week9
week10
week11
week12
week13
2010/Q1/week1
week2
week3
week4
week5
week6
week7
week8
week9
week10
week11
week12
week13
Q2/week1
week2
week3
week4
week5
week6
week7
week8

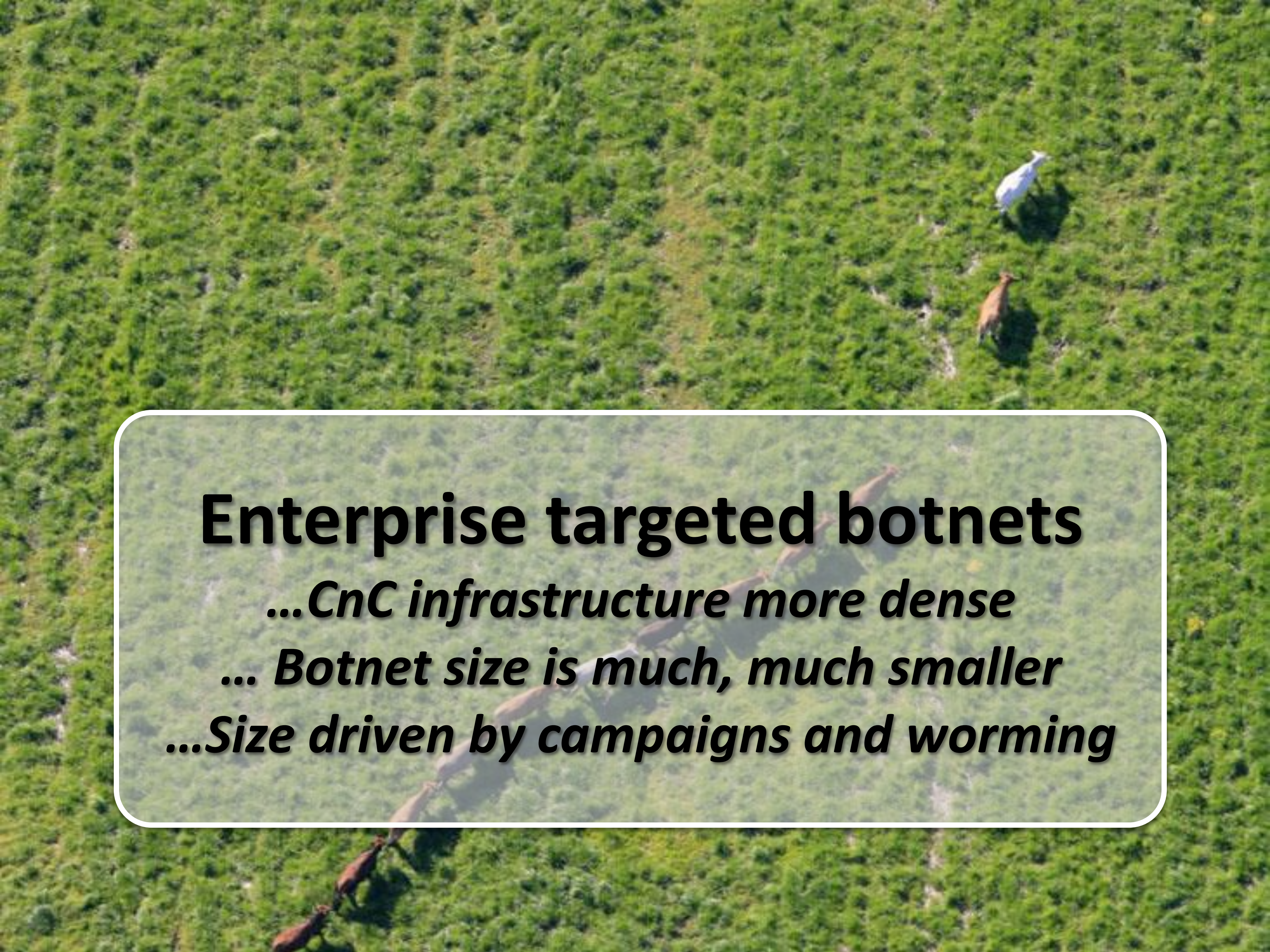


“Internet” bots within Enterprise

…Tend to not be proxy-aware

…Fail to reach the CnC server

…Remote/roaming/VPN users controlled

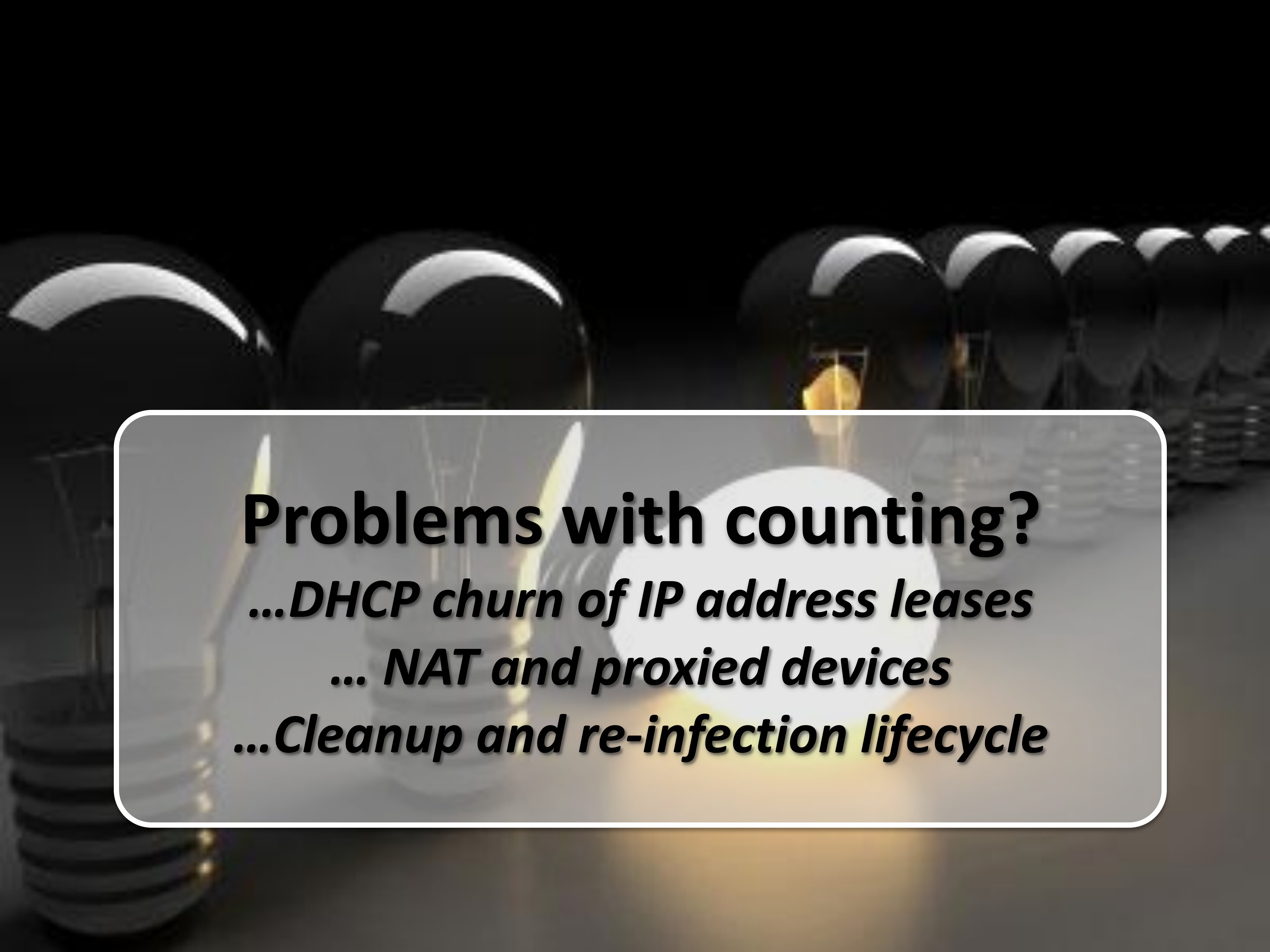


Enterprise targeted botnets

…CnC infrastructure more dense

… Botnet size is much, much smaller

…Size driven by campaigns and worming



Problems with counting?

…DHCP churn of IP address leases

… NAT and proxied devices

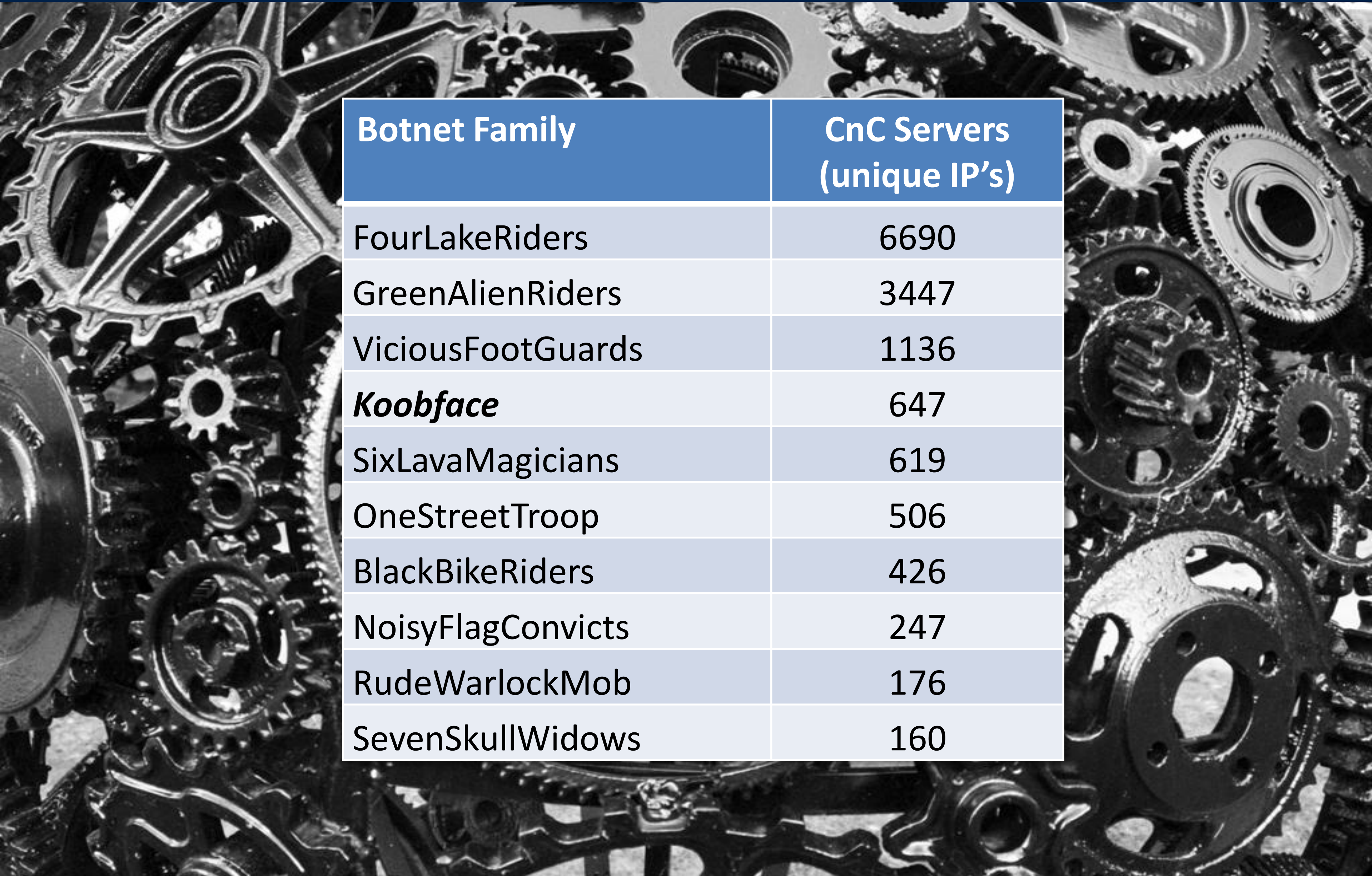
…Cleanup and re-infection lifecycle

When to stop counting?

…Period of monitoring (weekly unique)

…Period since "last seen"

Top-10 Server Ratios (4 months)



Botnet Family	CnC Servers (unique IP’s)
FourLakeRiders	6690
GreenAlienRiders	3447
ViciousFootGuards	1136
Koobface	647
SixLavaMagicians	619
OneStreetTroop	506
BlackBikeRiders	426
NoisyFlagConvicts	247
RudeWarlockMob	176
SevenSkullWidows	160

12 Month Analysis

- **56,524 different pieces of malware (single bot)**
- **18,424 different TLD's for a single botnet**
- **Interactively controllable**
  - – 1%-10% of Internet bot infections
  - – 25%-75% of enterprise bot infections

Be careful what you measure

You can be right and wrong at the same time

DAMBALLA

Take Back Command-and-Control

Questions?

Gunter Ollmann

email: gollmann@damballa.com Twitter: @gollmann
Web: http://www.damballa.com Blog: http://blog.damballa.com