



Take Back Command-and-Control

VB2010, Vancouver

Size Matters

Measuring a Botnet Operator's Pinkie

Gunter Ollmann, VP Research
gollmann@damballa.com

- **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/>

The image features two globes constructed from interlocking puzzle pieces. The globe on the left is dark grey with white puzzle pieces, some of which are missing, revealing a black interior. The globe on the right is colorful, with puzzle pieces in shades of blue, green, orange, and pink, representing different continents. A semi-transparent blue rounded rectangle is overlaid in the center, containing white text. Below the text, several loose puzzle pieces are scattered on a light surface.

Worldwide Threat Statistics

Different vendor, different numbers...

An aerial photograph showing a vast, dense field of yellow taxis, likely in a rural or undeveloped area. The cars are packed closely together, filling most of the frame. The scene is viewed from a high angle, showing the tops and sides of the vehicles. The ground is a mix of dirt, grass, and some sparse vegetation. The overall impression is one of a massive, unorganized collection of vehicles.

How was the number derived?

Calculated and extrapolated...

An aerial photograph showing a city street with a large, deep sinkhole in the center. The sinkhole is filled with brown, muddy water. The surrounding buildings are in various states of disrepair, with some roofs missing and walls crumbling. Debris is scattered on the street. A semi-transparent white box with rounded corners is overlaid on the image, containing text.

How was the number derived?

Sinkholes, spam traps and honeypots...

A black and white photograph of an elderly man with glasses, wearing a dark sweater, sitting at a desk and typing on a keyboard. He is looking down at the keyboard. In the background, there is a computer monitor, a mouse, and a mug. The scene is dimly lit, suggesting an office or home workspace.

How was the number derived?

Infiltration and interpretation...

A large group of dark-colored fish, likely catfish, with their mouths open, gathered around a person's hand holding a piece of yellow fruit. The fish are densely packed, and their long whiskers are visible. The background is dark, and the overall scene suggests a feeding or market activity.

How was the number derived?

Victim counts from customers...

A satellite image of Earth showing a tropical storm over the ocean. The storm is a large, circular cloud system with a distinct eye and spiral bands of clouds. The surrounding ocean is dark blue, and the landmasses are green and yellow. The text is overlaid on a semi-transparent white box in the center of the image.

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

A hand is shown reaching towards a row of green glass bottles, likely in a laboratory or factory setting. The bottles are arranged in a line, and the lighting is dramatic, highlighting the green color and the liquid inside. The background is dark, making the bottles stand out.

New bot agent for every victim

...Frequent updates of agents (<24hrs)

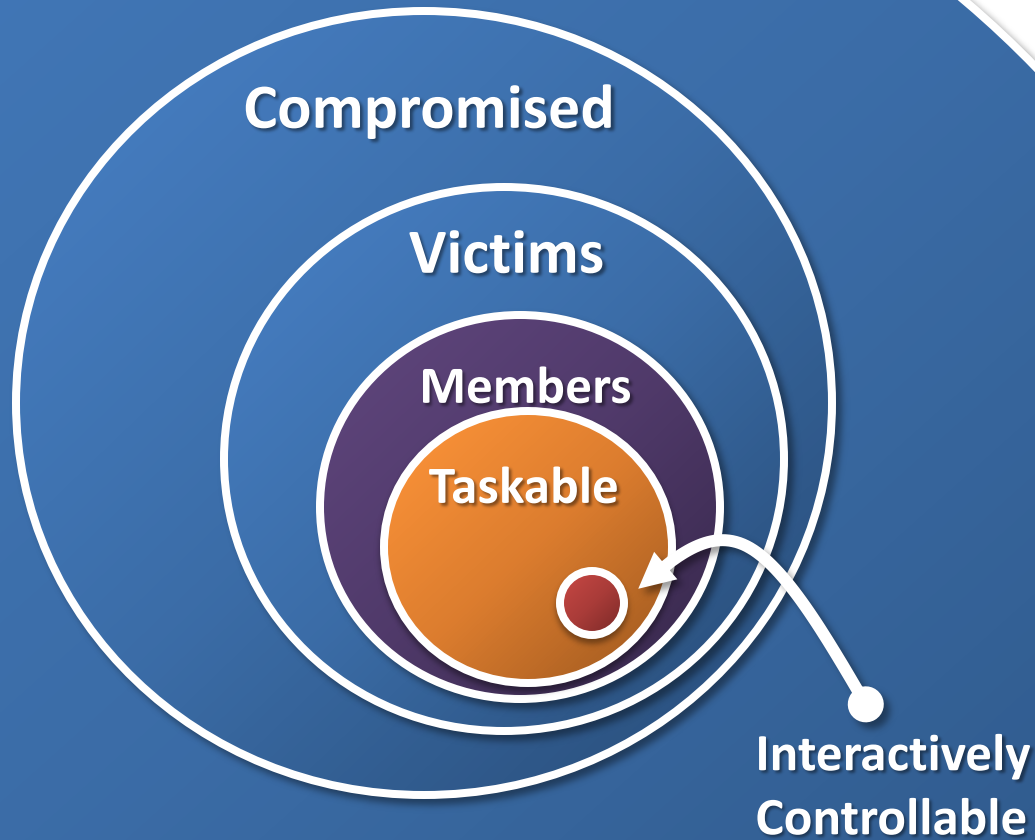
...QA tested and designed to evade

- **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)



Detections

Typical "Internet" botnets



- **Characteristics of Enterprise botnets**

- Detections happen at the pace of compromise and victimization
- All members are taskable





Best way to measure size?

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

A vintage wooden measuring tape is coiled around a brown leather measuring tool. The tape has numbers and the word 'Inch' printed on it. The leather tool has a metal hook and a small knob. The background is a plain, light-colored surface.

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*

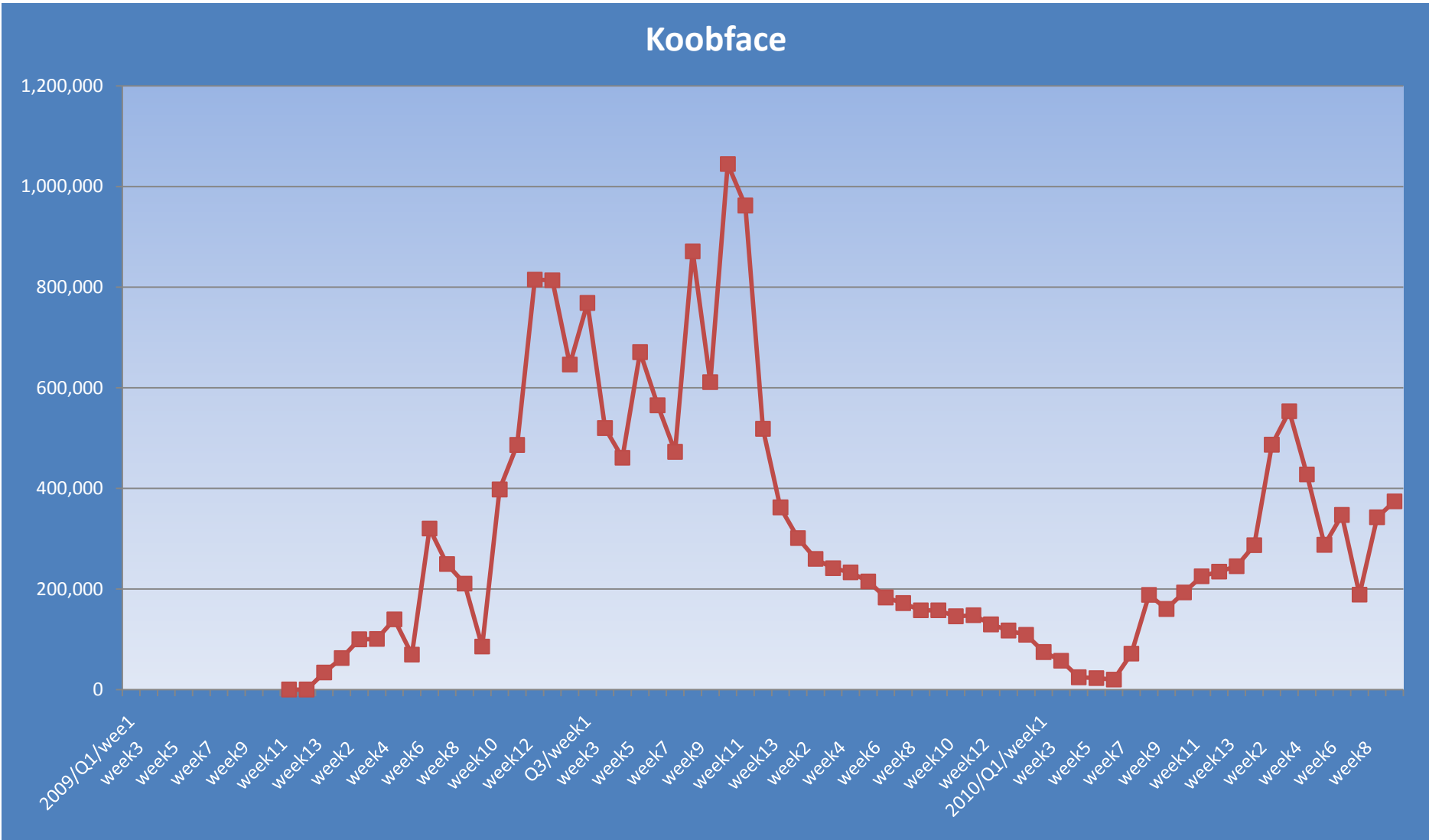
Keeping track is difficult

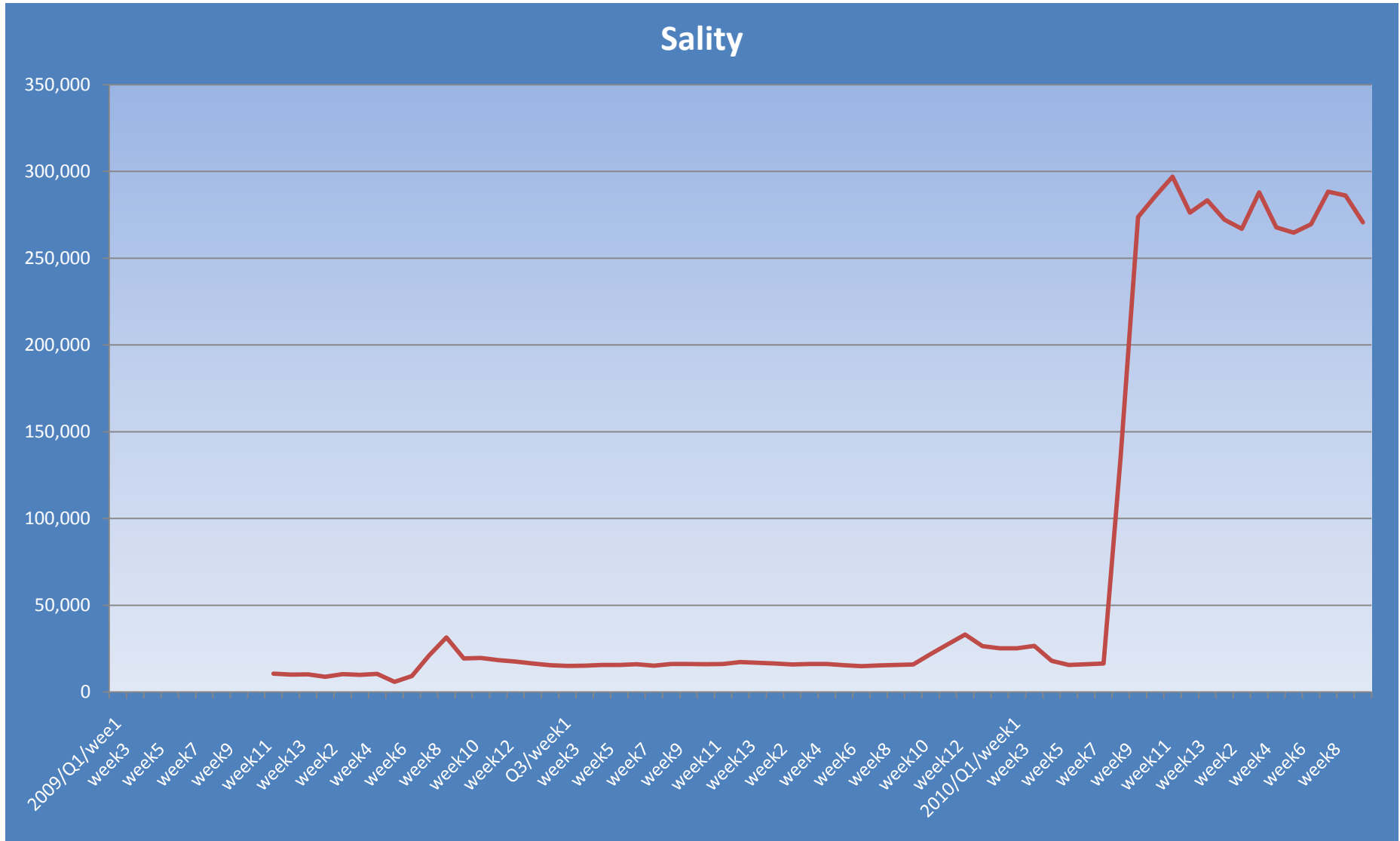
Singling out a unique “victim”



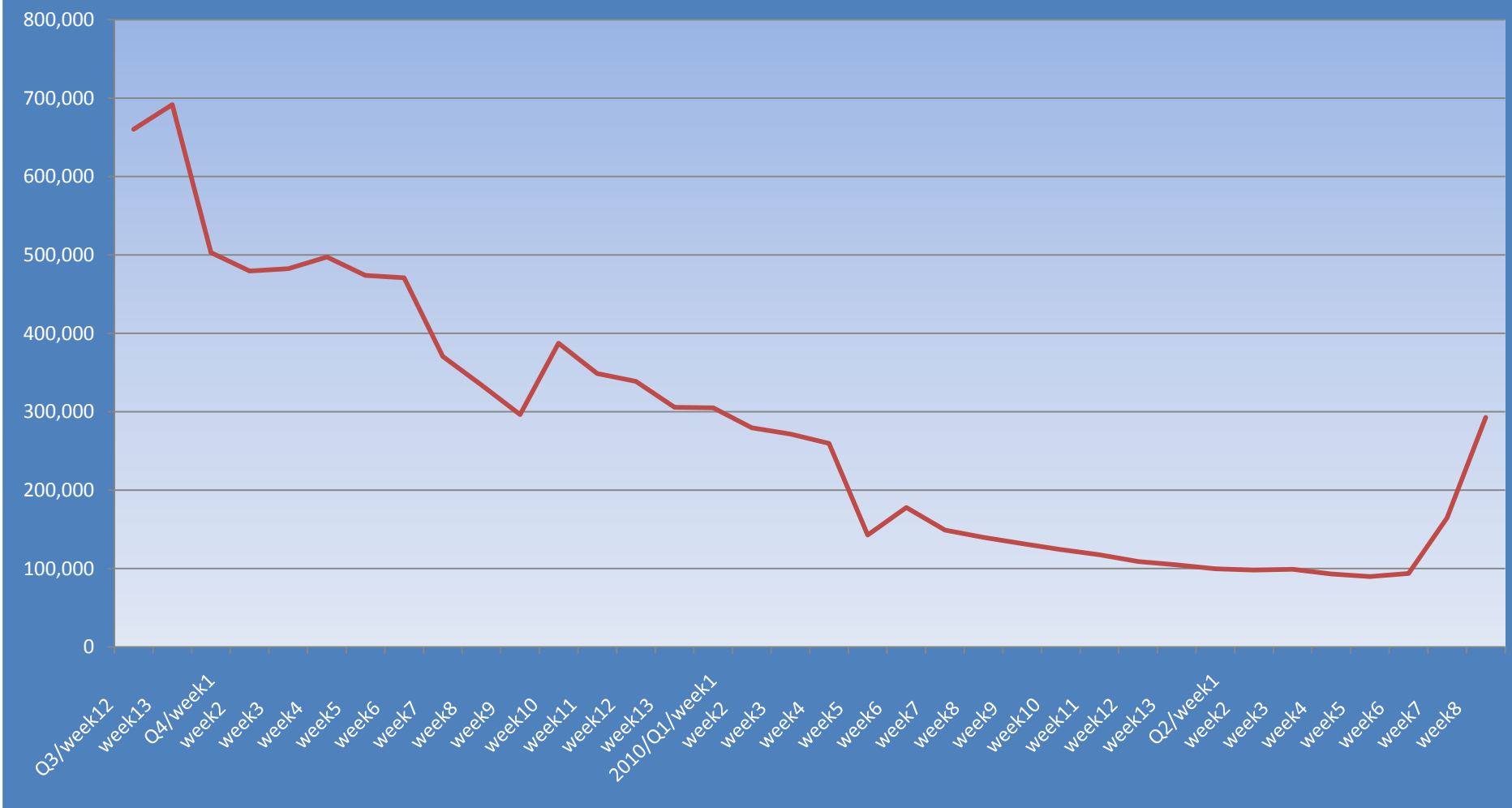
- **CnC traffic appears to be an ideal way of measuring size of the botnet...**
- **Look at three large/common botnets**
 - Koobface, Sality, Monkif
- **Count number of successful connections to botnet CnC (unique IP per week)**







Monkif



A large flock of sheep is gathered on a dirt field, forming a dense, irregular shape. The sheep are light-colored and their heads are visible, creating a textured, organic form. The background is a plain, light-brown dirt surface.

“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

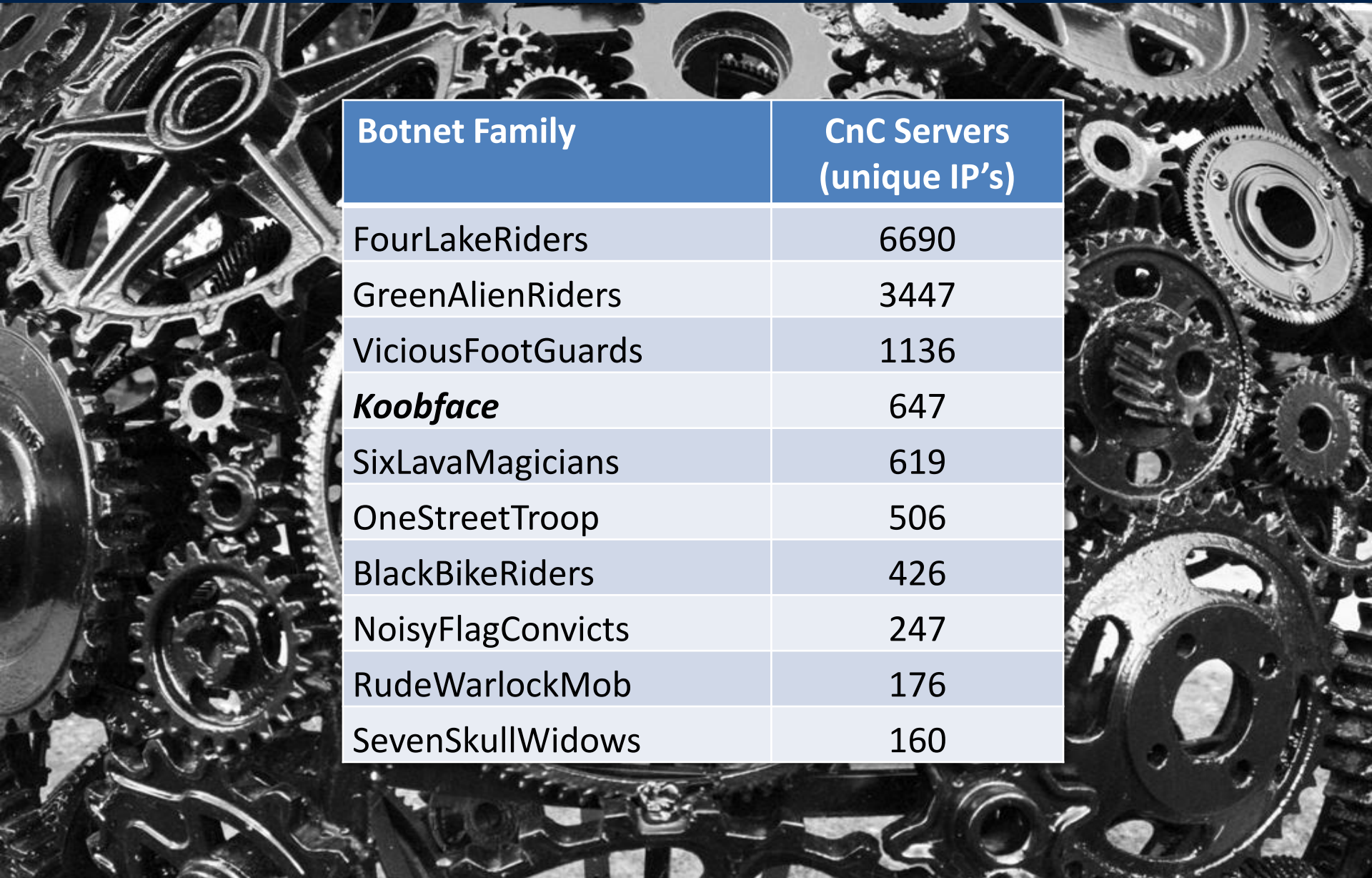
A man in a dark shirt is seen from the side, cleaning a large, illuminated clock face with a white cloth. The clock face is white with black Roman numerals and hands. In the background, another large clock face is visible, and the scene is set in a museum or gallery with other clock faces and a person's silhouette in the distance.

When to stop counting?

...Period of monitoring (weekly unique)

...Period since "last seen"

Top-10 Server Ratios (4 months)



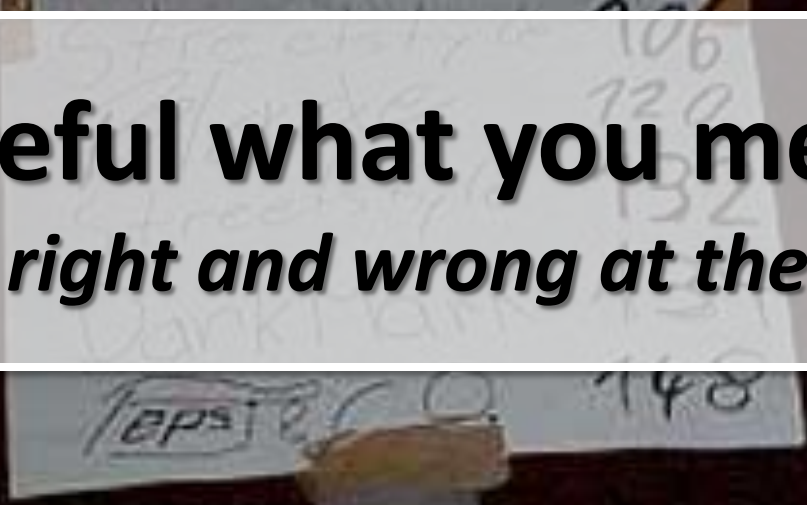
Botnet Family	CnC Servers (unique IP's)
FourLakeRiders	6690
GreenAlienRiders	3447
ViciousFootGuards	1136
<i>Koobface</i>	647
SixLavaMagicians	619
OneStreetTroop	506
BlackBikeRiders	426
NoisyFlagConvicts	247
RudeWarlockMob	176
SevenSkullWidows	160

- **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





Questions?

Gunter Ollmann

email: gollmann@damballa.com Twitter: [@gollmann](https://twitter.com/gollmann)
Web: <http://www.damballa.com> Blog: <http://blog.damballa.com>