


A horizontal blue banner with a globe on the left and binary code (0s and 1s) scattered across the background. The text "2009 Cyber Security Outlook for TLD operators" is written in white, bold, sans-serif font across the center of the banner.

2009 Cyber Security Outlook for TLD operators

A large, faint, light-colored world map is visible in the background of the lower half of the slide, centered behind the text.

*February 23, 2009
APTLD Meeting*

Ram Mohan
Executive Vice President &
Chief Technology Officer
rmohan@afilias.info



Agenda

- Current Cyber Security Threats
- What are cyber criminals doing?
- How does this affect TLDs?
- Effective TLD response to threats
- Preparing a Readiness Plan
- The road ahead

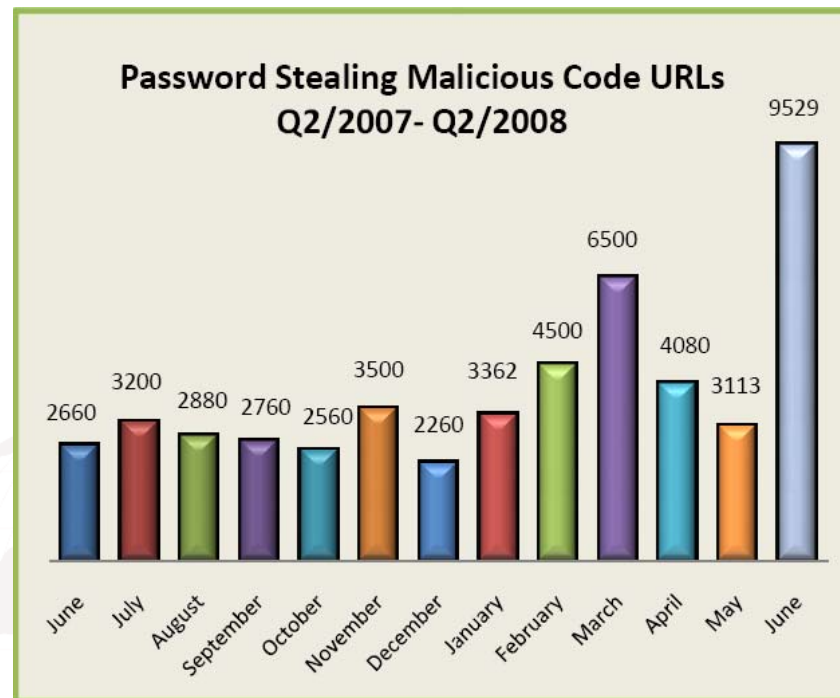


Current Cyber Security Threats

- DDOS/aDDOS
- Cache poisoning (Kaminsky Bug)
- Fast flux networks
- Phishing
- Worms/C&C Botnets

Phishing Statistics

Number of sites infecting PCs with password-stealing crimeware rose 47%



Source: APWG 2Q 08 Phishing Study

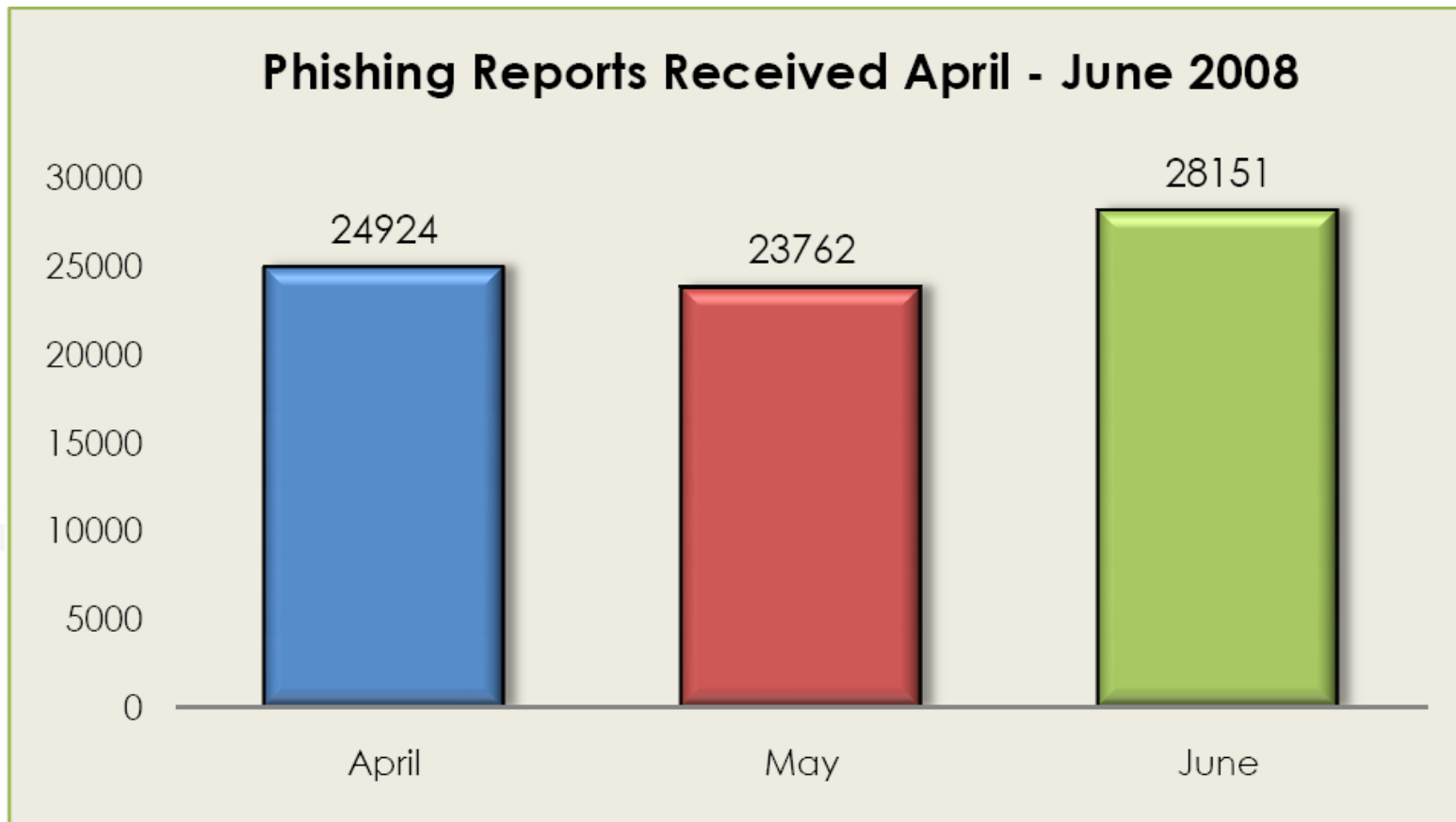
Phishing Statistics

	April	May	June
Number of unique phishing email reports received by APWG from consumers	24,924	23,762	28,151
Number of unique phishing web sites detected	20,410	20,317	18,509
Number of brands hijacked by phishing campaigns	276	294	227
Country hosting the most phishing websites	China	Turkey	US
Contain some form of target name in URL	28.3%	23.2%	26.1%
No hostname; just IP address	5.5%	13.2%	4%
Percentage of sites not using port 80	.81%	.45%	.49%
Longest time online for website	30 days	31 days	30 days

Source: APWG 2Q 08 Phishing Study

Phishing Statistics

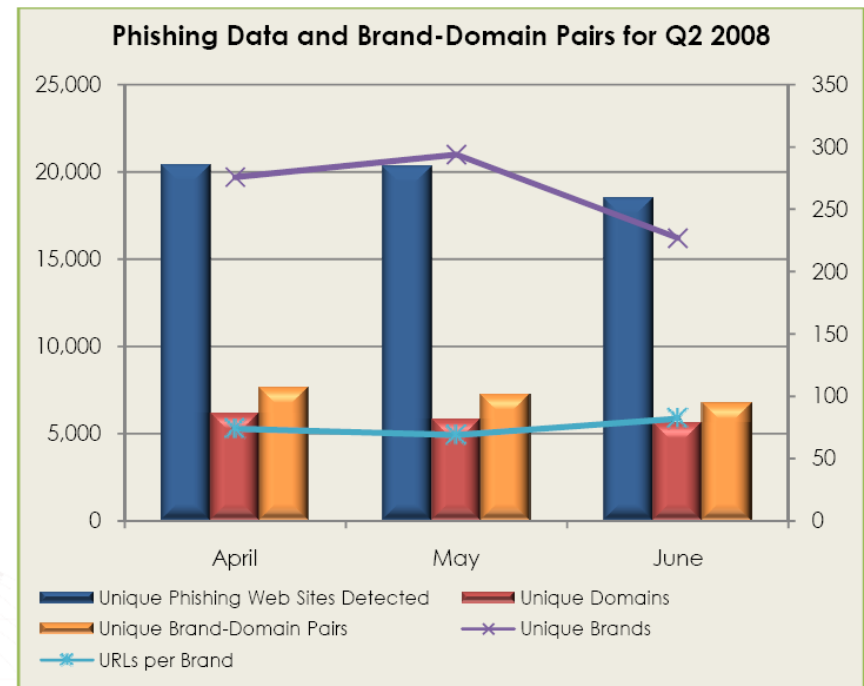
Email phishing reports are up 13%



Source: APWG 2Q 08 Phishing Study

Phishing Statistics

- Number of brands targeted by Phishing continues to rise
- Phishers are investing in sophisticated marketing tools and IT infrastructure



Source: APWG 2Q 08 Phishing Study

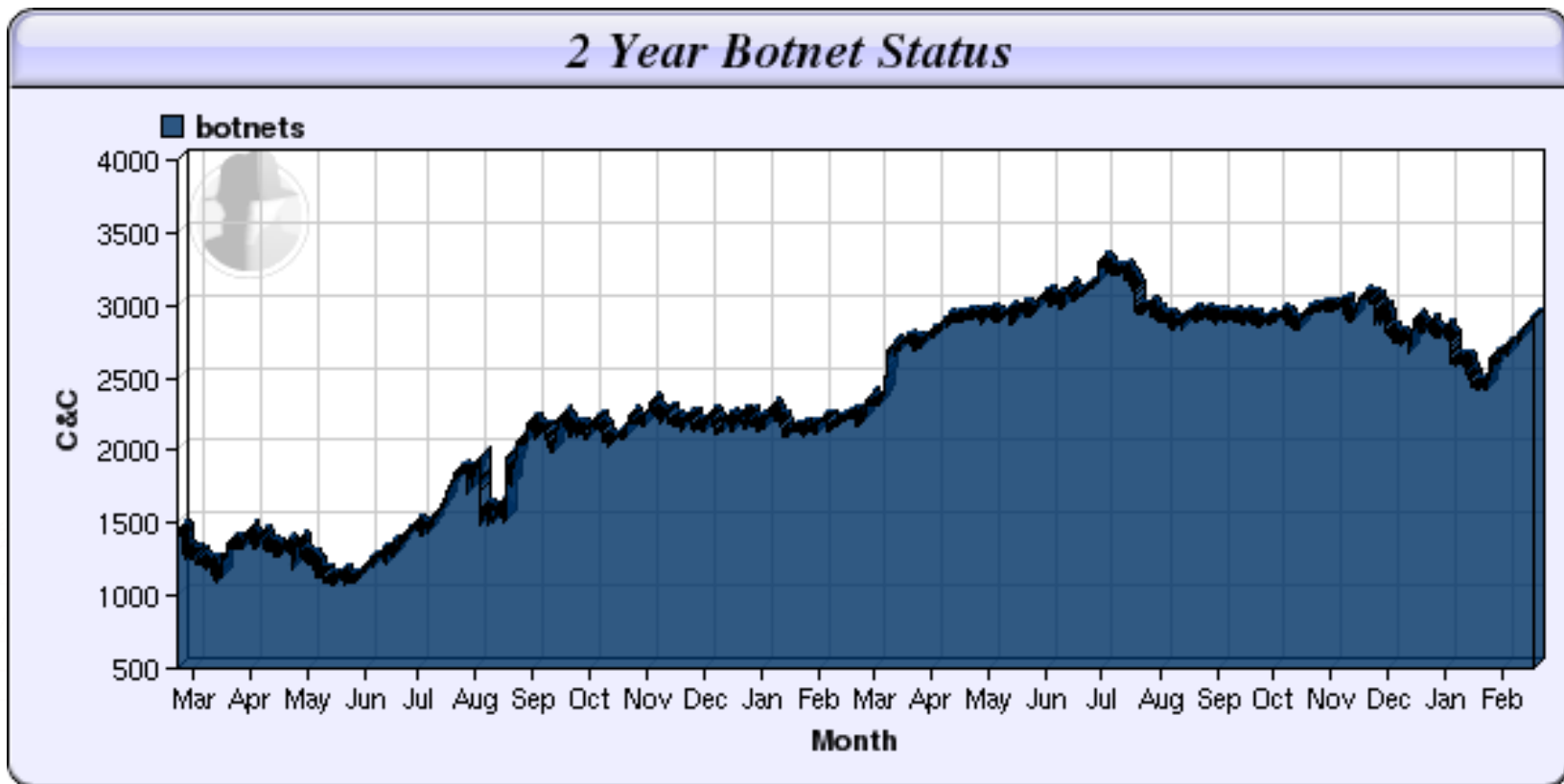
Overall Phishing Stats

	1H2008	2H2007
Phishing domain names:	29,073 ↑	28,818
IP-based phish (unique IPs):	3,389 ↓	5,217
TLDs phished on:	102	104
“Attacks”:	>47,342	
IDN domains:	52	10

Source: APWG 1H 2008 Global Phishing Survey: Domain Trends and Use

Botnet Data

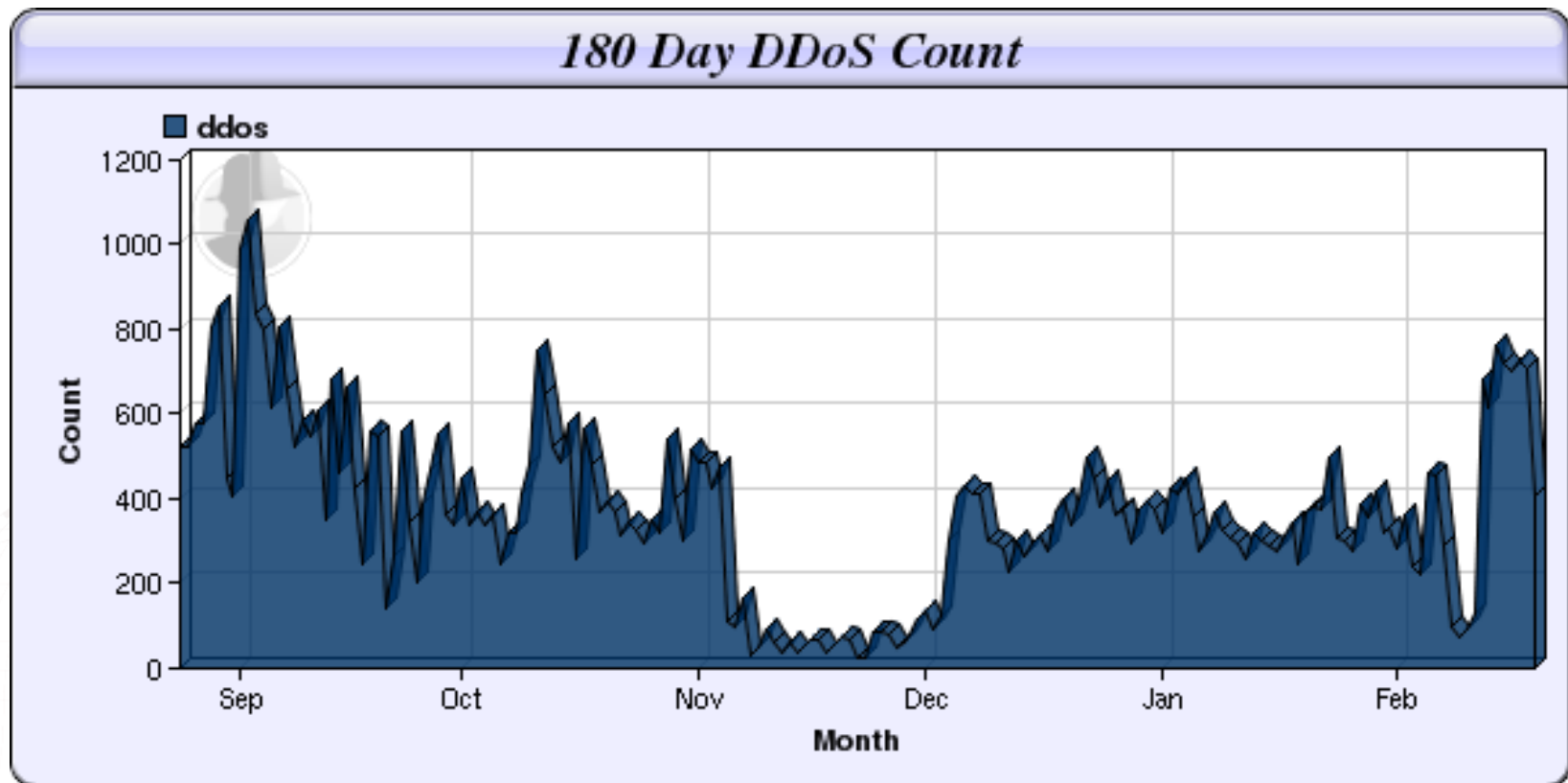
- Increasing attacks



Source: <http://www.shadowserver.org>

DDoS Data


- Increasing frequency and sustained activity



Source: <http://www.shadowserver.org>



What are cyber criminals doing?

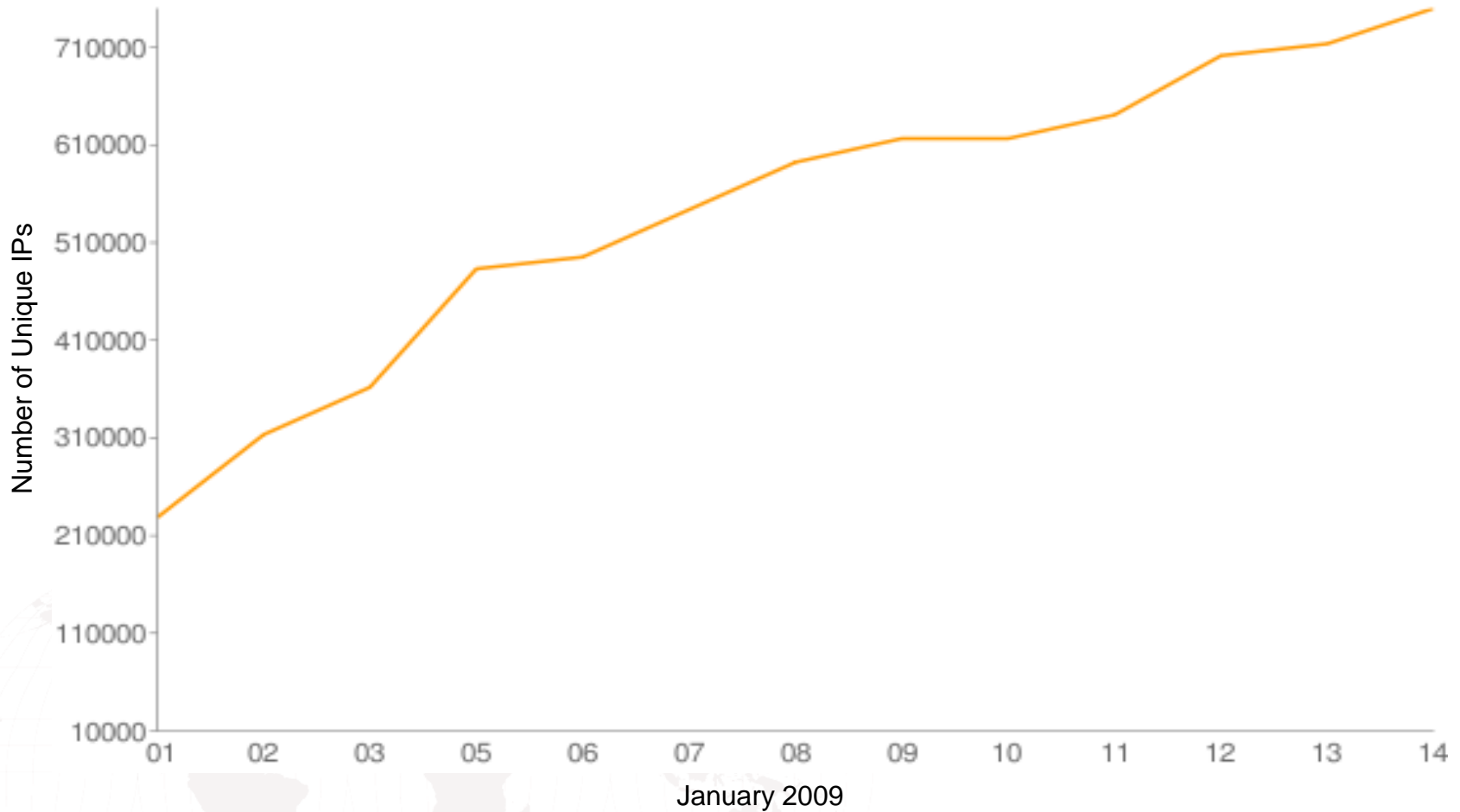
- Sustaining their momentum and becoming more sophisticated
 - Innovating
 - Investing in R&D and infrastructure
 - Utilizing new techniques and marketing
 - Leverage economies of scale and scope
 - Building international networks
- 



Security Threats to TLDs

- Registries and domain names are an increasing focus of cyber security
- Registries/ TLD nameservers continue to experience DDoS attacks
- Specific TLDs are targeted for phishing
 - Registration policies, popularity, or geographic jurisdiction have an effect
- Increasing in use by worms and botnets
 - Conficker is a recent example of using the domain name registration process to spread

Growth of Conficker – Jan 1 – Jan 14, 2009



~ 12 million hosts as of Jan 14, 2009

Source: Arbor Networks, Jan30, 2009



Why is this important?

If your TLD has a reputation as a cyber security risk, consumers will turn elsewhere.

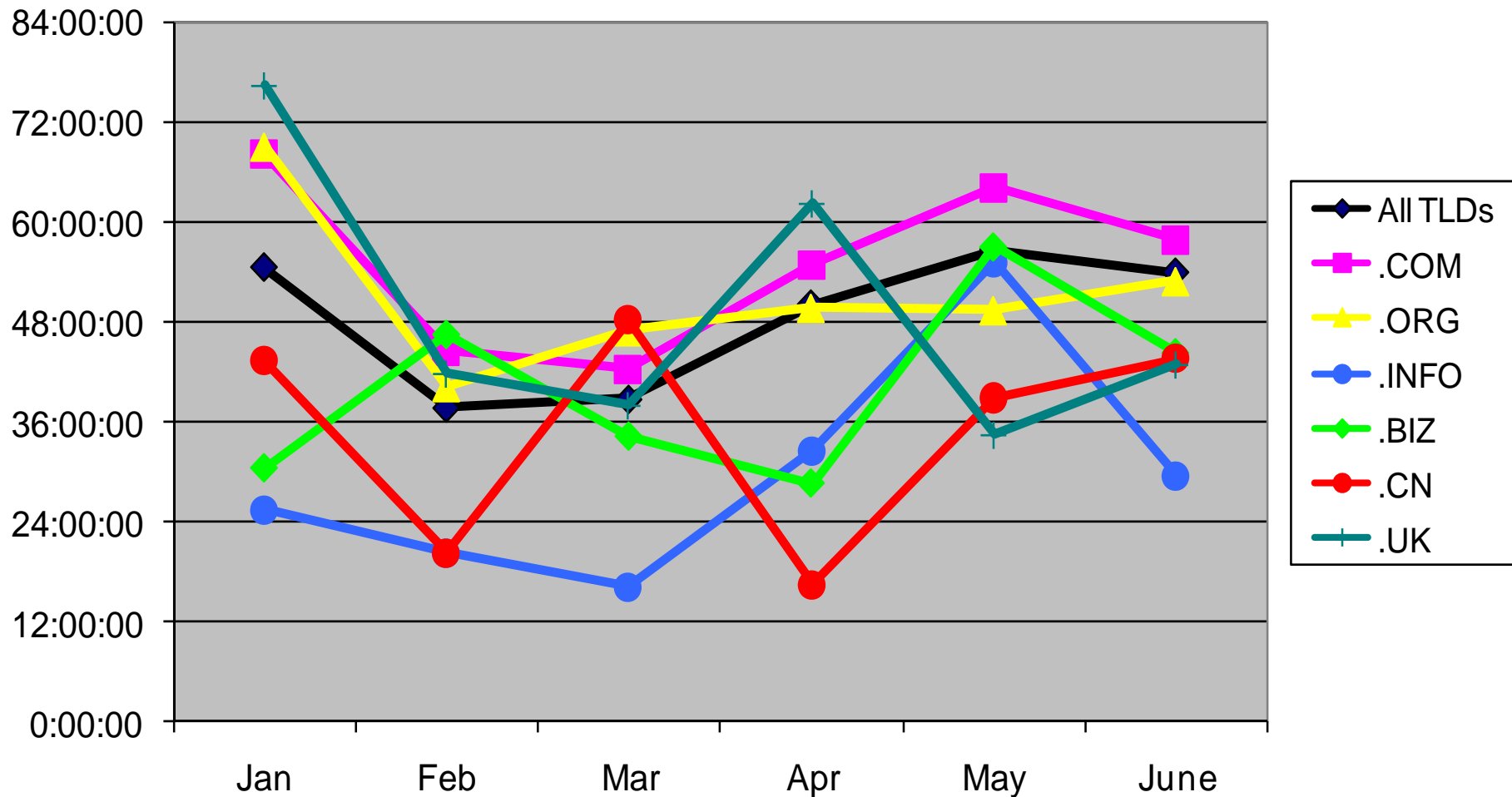


TLD response to threats

- Case Study: 
Where the World Goes for Information.
 - Fast Flux automated monitoring
 - Afilias Phishing Lab
 - Botnet detection mechanisms
 - Alliances with CERTs worldwide for data sharing
 - .INFO Anti-Abuse Policy
 - Collaboration with Microsoft and industry leaders to stop Conficker
- Results
 - Suspended over 100,000 domains to date
 - .INFO has lowest phish uptime among gTLDs

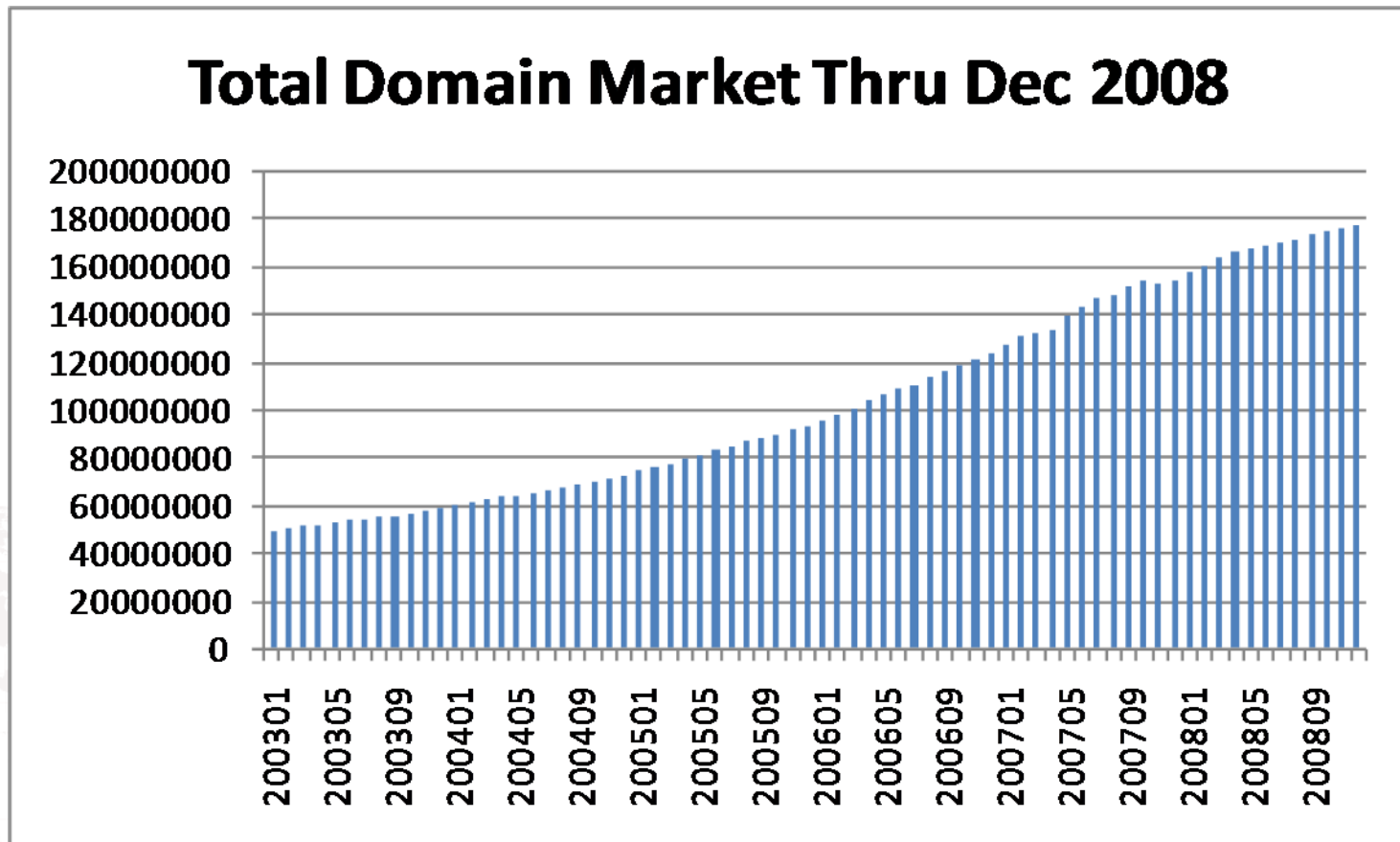
.INFO Phishing success

Average Phishing Uptimes 1H2008



Market growth flattening out

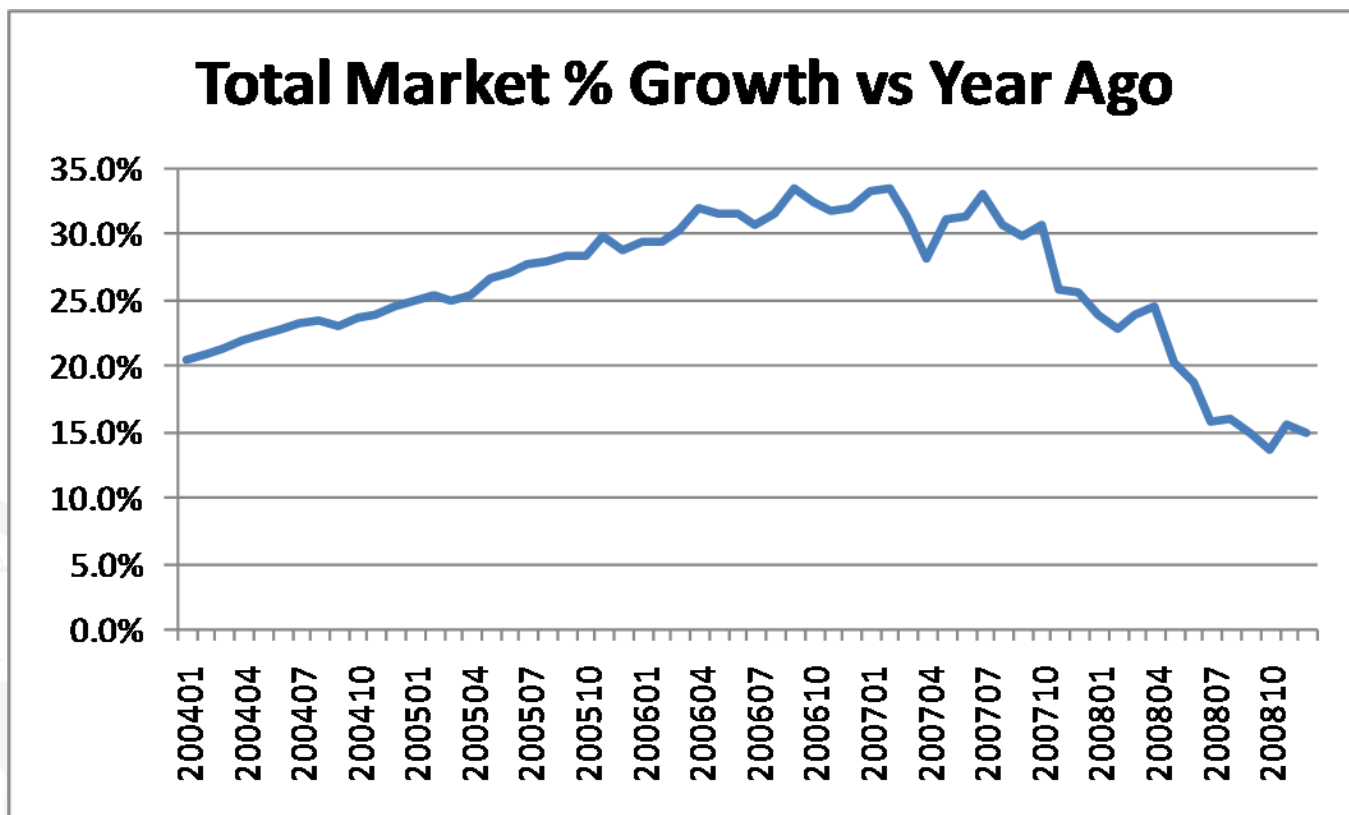
- Total now nearly 180,000,000 registrations



Source: zooknic.com

Current growth rate is half what it was last year

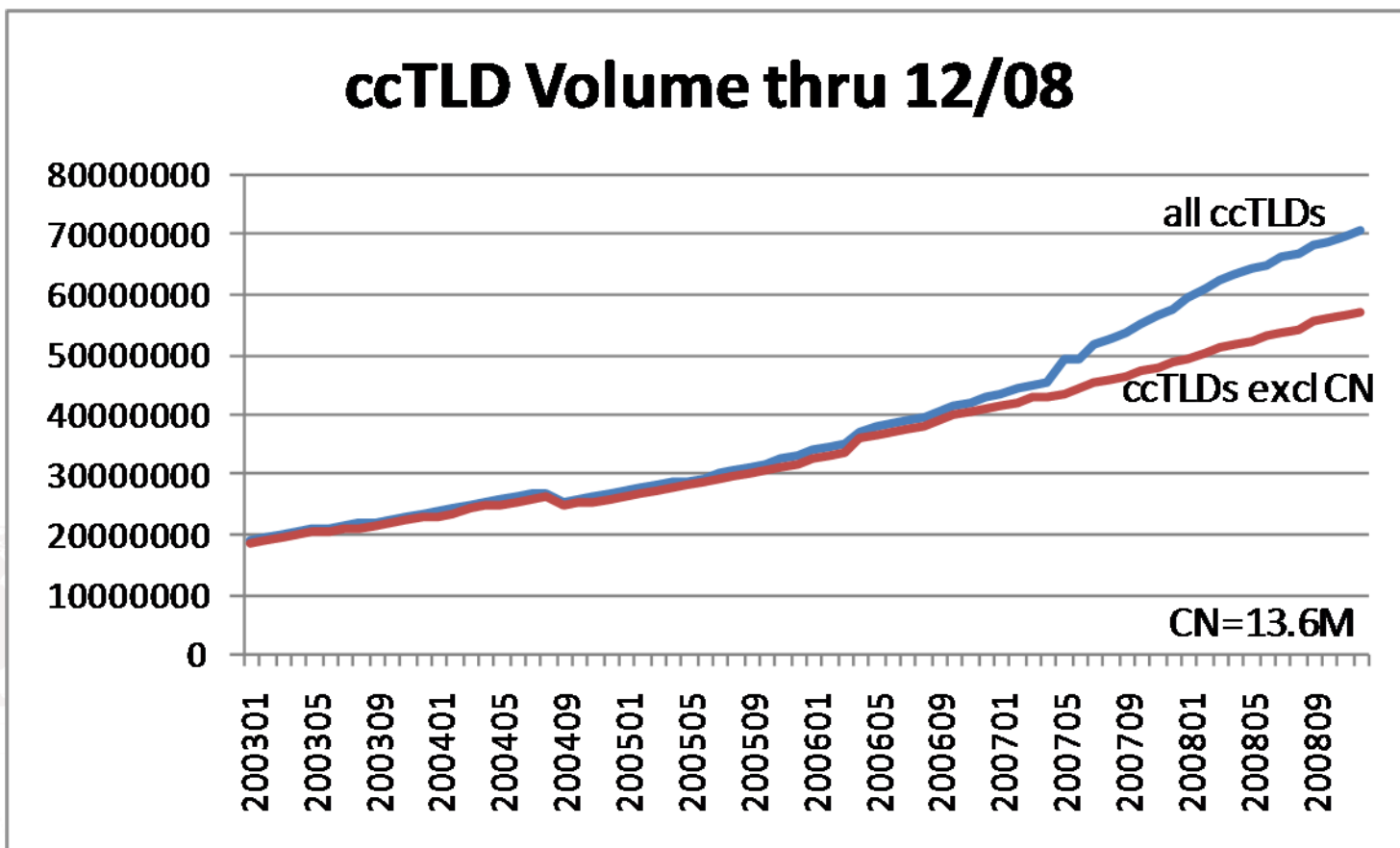
- Industry growth peaked at 33% in early 2007
- December growth was <+15% vs year ago



Source: zooknic.com

ccTLD registrations are now 40% of market

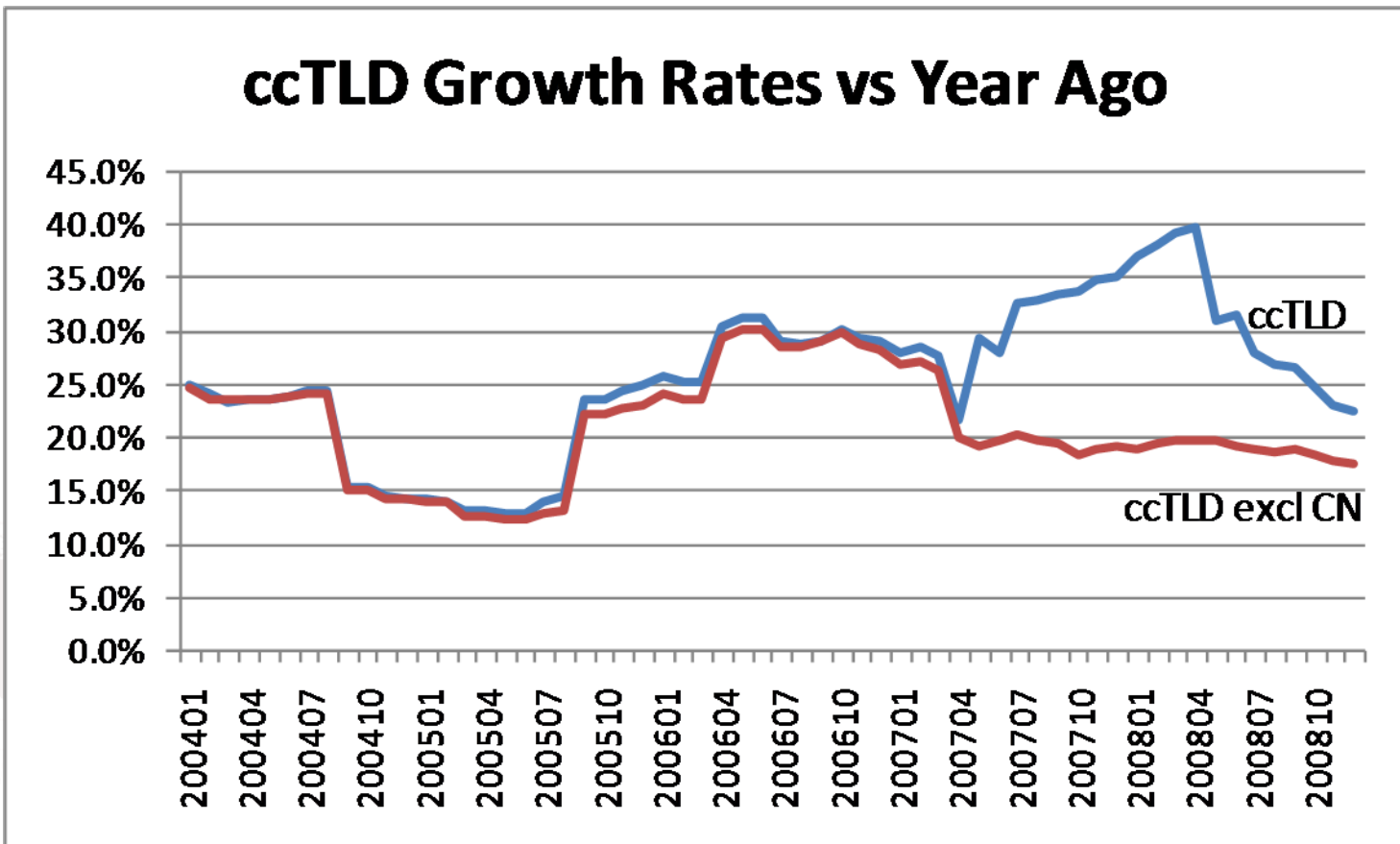
- ccTLD 's are now over 70,000,000 registrations



Source: zooknic.com

ccTLD growth declining

Without CN, growth is 17%



Source: zooknic.com



So how can your TLD be prepared?





TLD Security Readiness plan

1. Become a member of industry research and action groups such as
 - RISG (Registry Internet Security Group) [registrysafety.org](https://www.registrysafety.org)
 - OARC (DNS Operations, Analysis & Research Center) [dns-oarc.org](https://www.dns-oarc.org)
 - APWG (Anti Phishing Working Group) [apwg.org](https://www.apwg.org)
2. Prepare an escalation plan
 - Internal process to report threats and problems
 - External processes to work with registrars and law enforcement to take down sites



TLD Security readiness plan

3. Proactive Monitoring

- A NOC is not enough!
- Track external research to ID new trends and threats

4. Institute a Domain Anti-Abuse Policy

- Enables you to work with registrars to take down sites within your existing registration policies

5. Operate on a secure, diverse DNS architecture

- Redundant architecture able to withstand attack
- Diversity to ensure that no single point of failure can bring down your network



The road ahead

- Registration policies need to be reviewed to allow for security actions
 - Registration prices and fees are a key consideration for non-registry partners
 - Registration grace period policies need to be reviewed
 - AGP reform going on in ICANN with gTLDs
- Registry Anti-abuse policies are working
 - ICANN is considering support for registries enacting anti-abuse measures



The road ahead

- Preserve the value of your TLD
 - Important to continue to ensure the value of your TLD
 - Don't reduce your domain's value with programs that may attract cyber criminals
 - Investigate opportunities to expand the security of your registrar and DNS network
 - New opportunities like DNSSEC are on the horizon



Security can differentiate your TLD



rmohan@afiliast.info