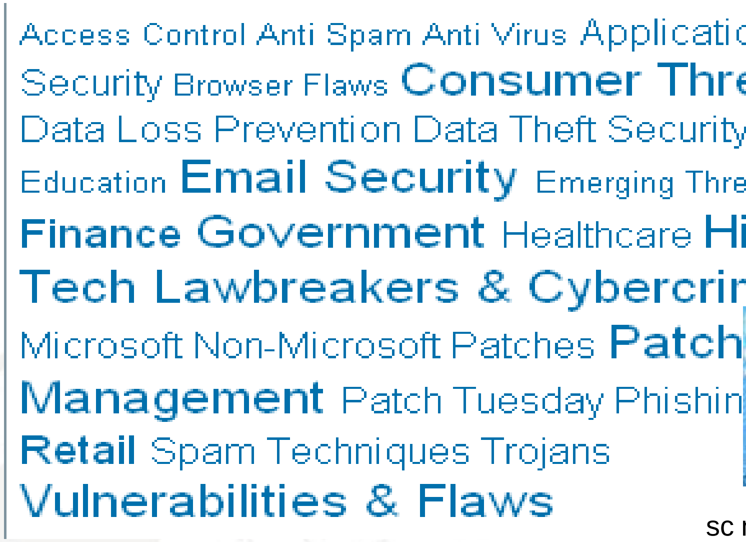
The future of DNS Security & IDNs

By Ram Mohan
EVP & Chief Technology Officer
Afilias

APRICOT Plenary Meeting
Kuala Lumpur
March 1, 2010

© Afilias Limited

What does Online Crime look Like?



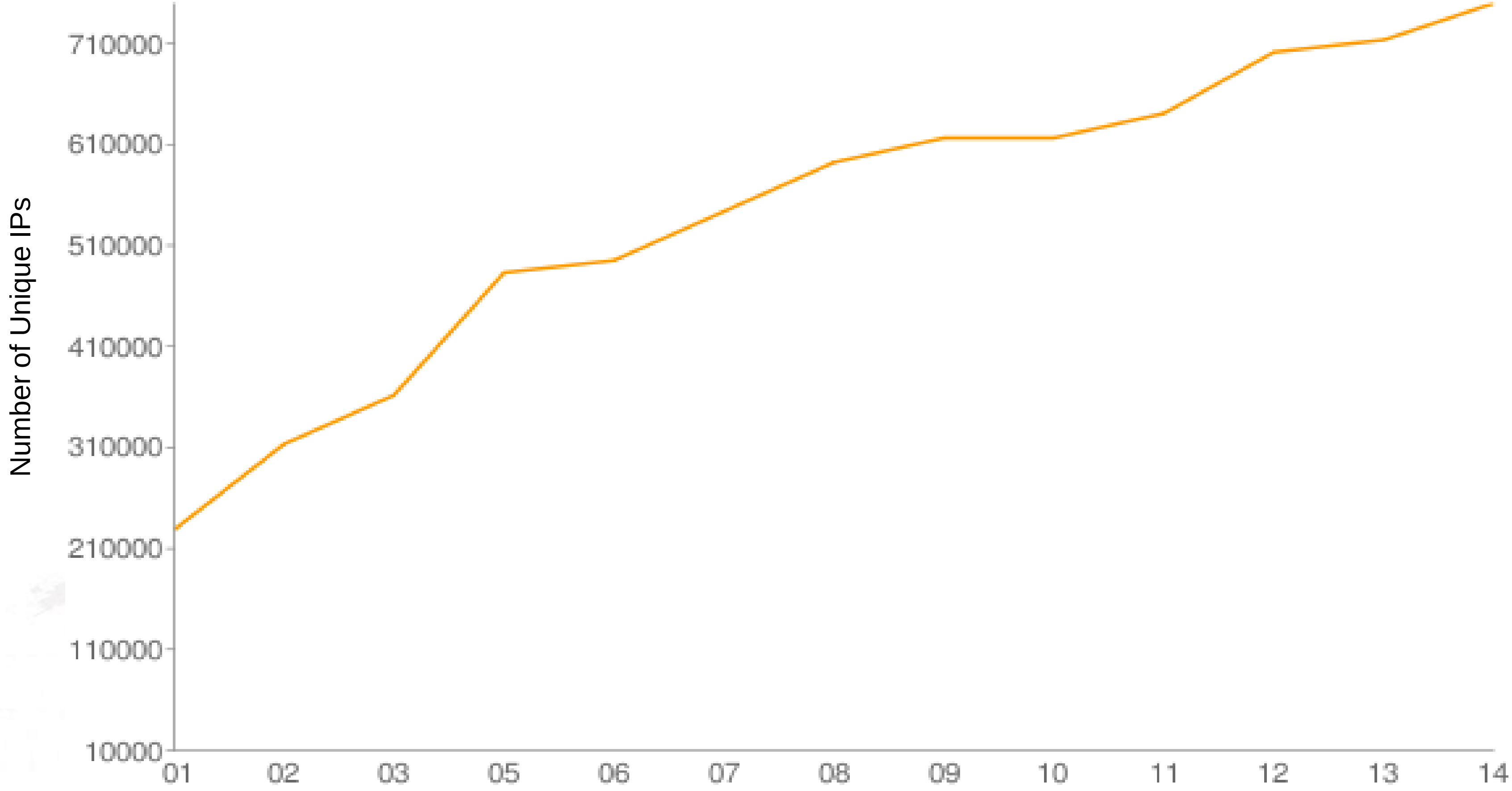
Access Control Anti Spam Anti Virus Application Security Browser Flaws Consumer Threats Data Loss Prevention Data Theft Security Education Email Security Emerging Threats Finance Government Healthcare High Tech Lawbreakers & Cybercrime Microsoft Non-Microsoft Patches Patch Management Patch Tuesday Phishin Retail Spam Techniques Trojans Vulnerabilities & Flaws

sc magazine

Why Attack You?

- Money
  - Lot of money waiting to be made (stolen) when ecommerce and banking is compromised
- Power
  - ISPs, Network operators and Internet users can be hijacked and forcibly redirected
  - Reduce credibility and erode trust
- Control
  - Spy on your customers without their knowledge or control

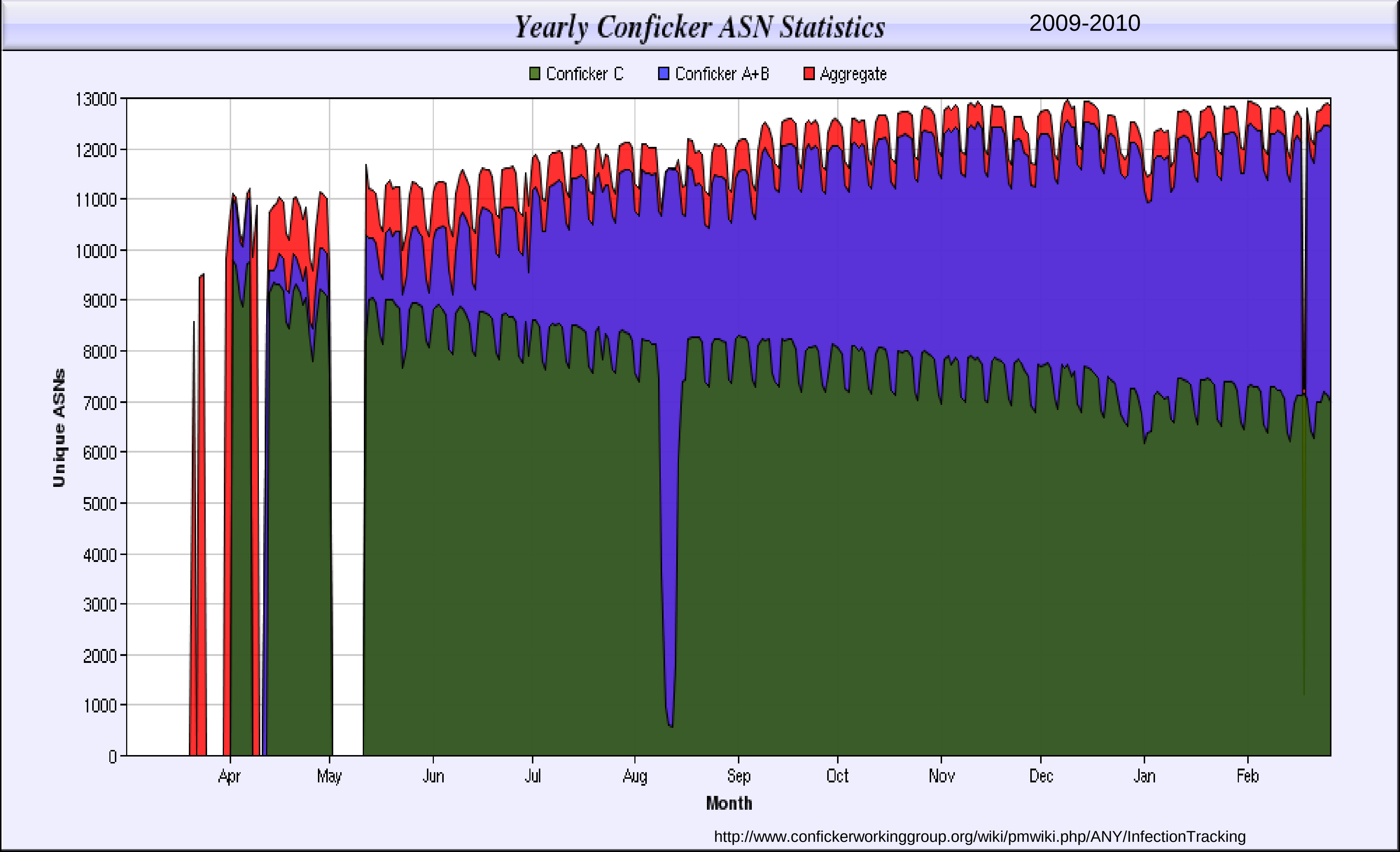
Criminals are infecting systems faster than ever



Conficker Botnet Spread: More than12 million hosts

Source: Arbor Networks, Jan30, 2009

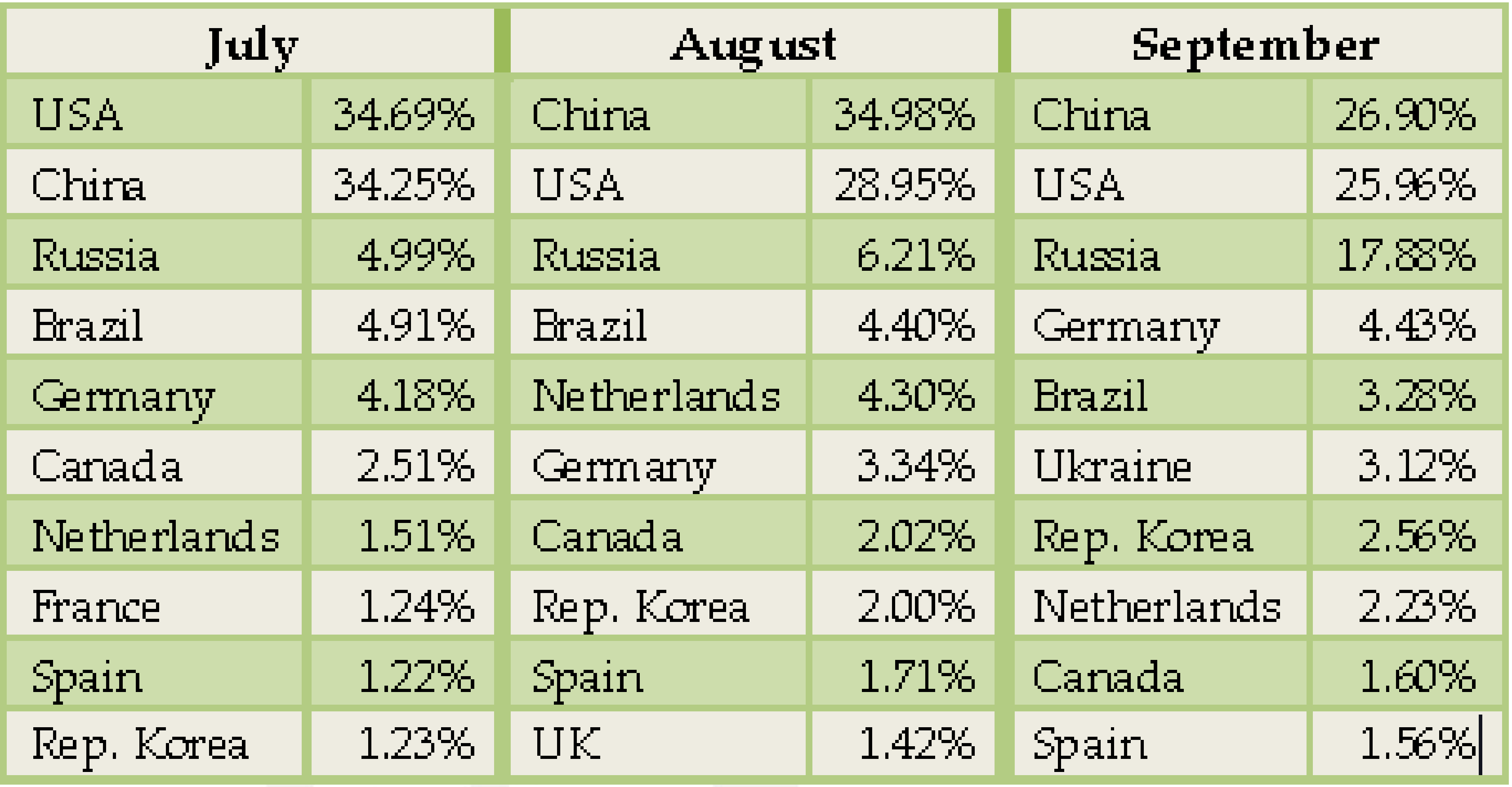
… and they are targeting YOUR networks



2009-2010

http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking

They are using sophisticated techniques

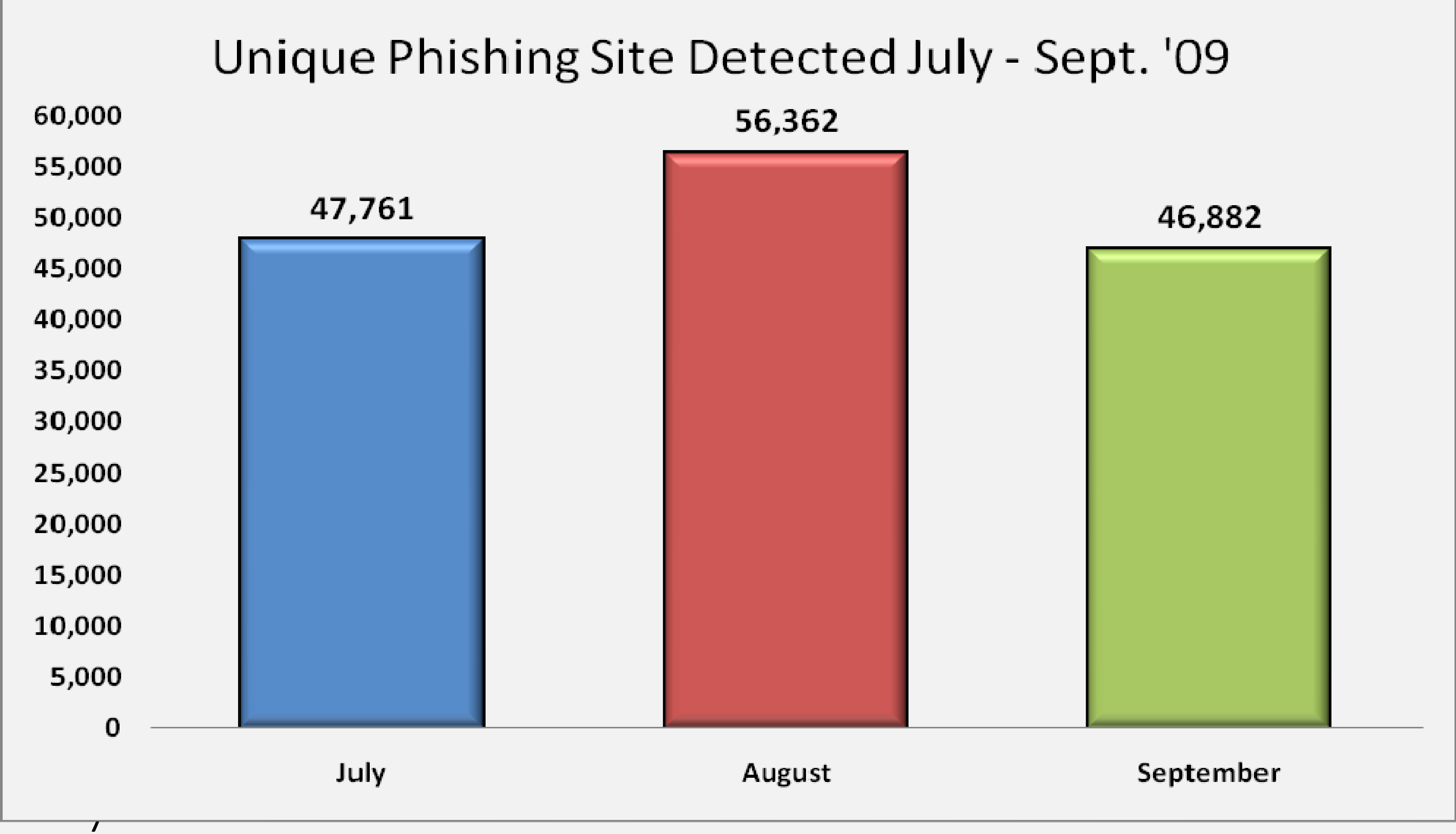


July		August		September	
USA	34.69%	China	34.98%	China	26.90%
China	34.25%	USA	28.95%	USA	25.96%
Russia	4.99%	Russia	6.21%	Russia	17.88%
Brazil	4.91%	Brazil	4.40%	Germany	4.43%
Germany	4.18%	Netherlands	4.30%	Brazil	3.28%
Canada	2.51%	Germany	3.34%	Ukraine	3.12%
Netherlands	1.51%	Canada	2.02%	Rep. Korea	2.56%
France	1.24%	Rep. Korea	2.00%	Netherlands	2.23%
Spain	1.22%	Spain	1.71%	Canada	1.60%
Rep. Korea	1.23%	UK	1.42%	Spain	1.56%

Phishing-based Trojans and Downloader's Hosting Countries (by IP address), 2009

Source: APWG

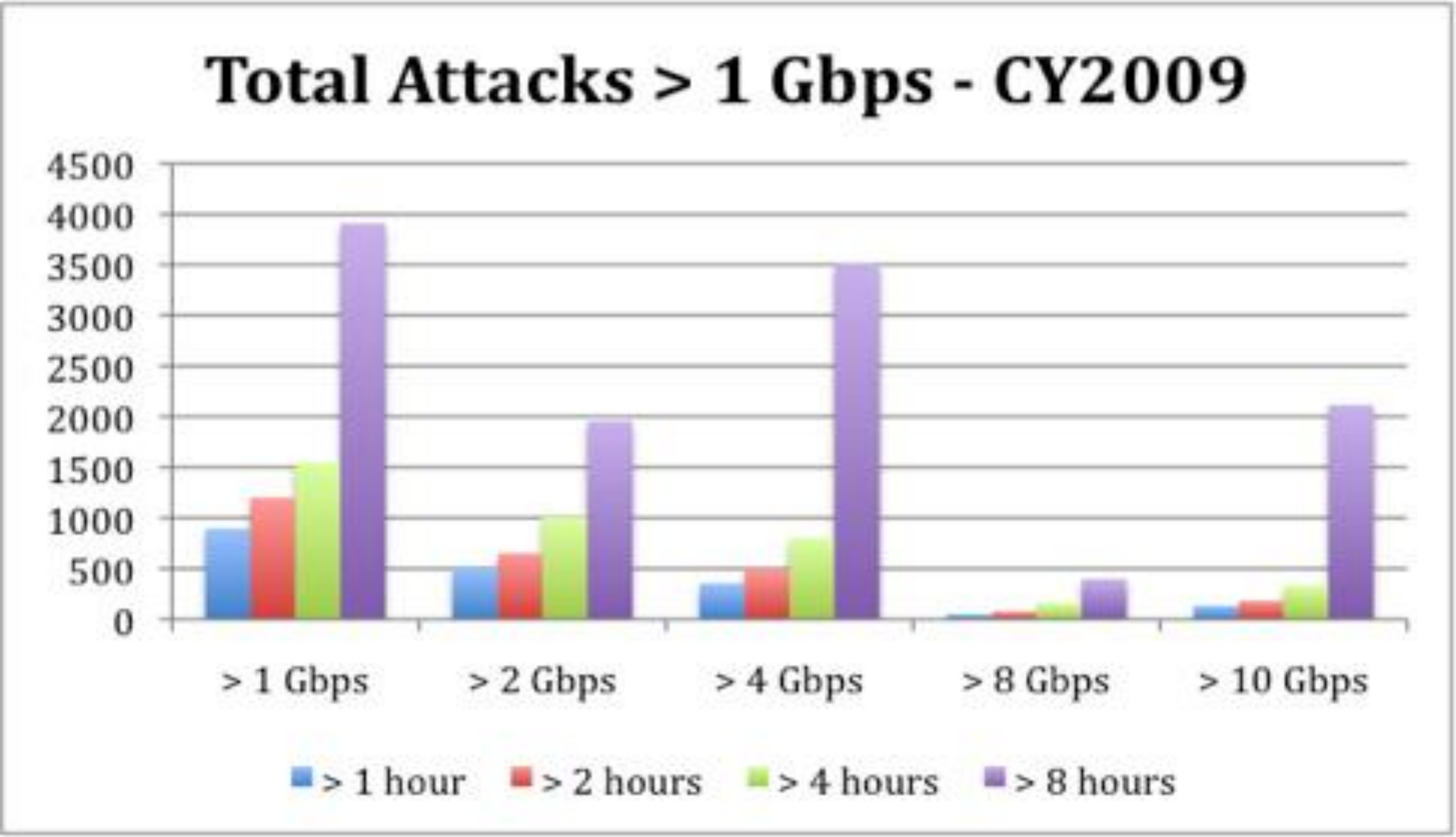
… and increasing their capacity


Unique Phishing Site Detected July - Sept. '09

© Afilias Limited

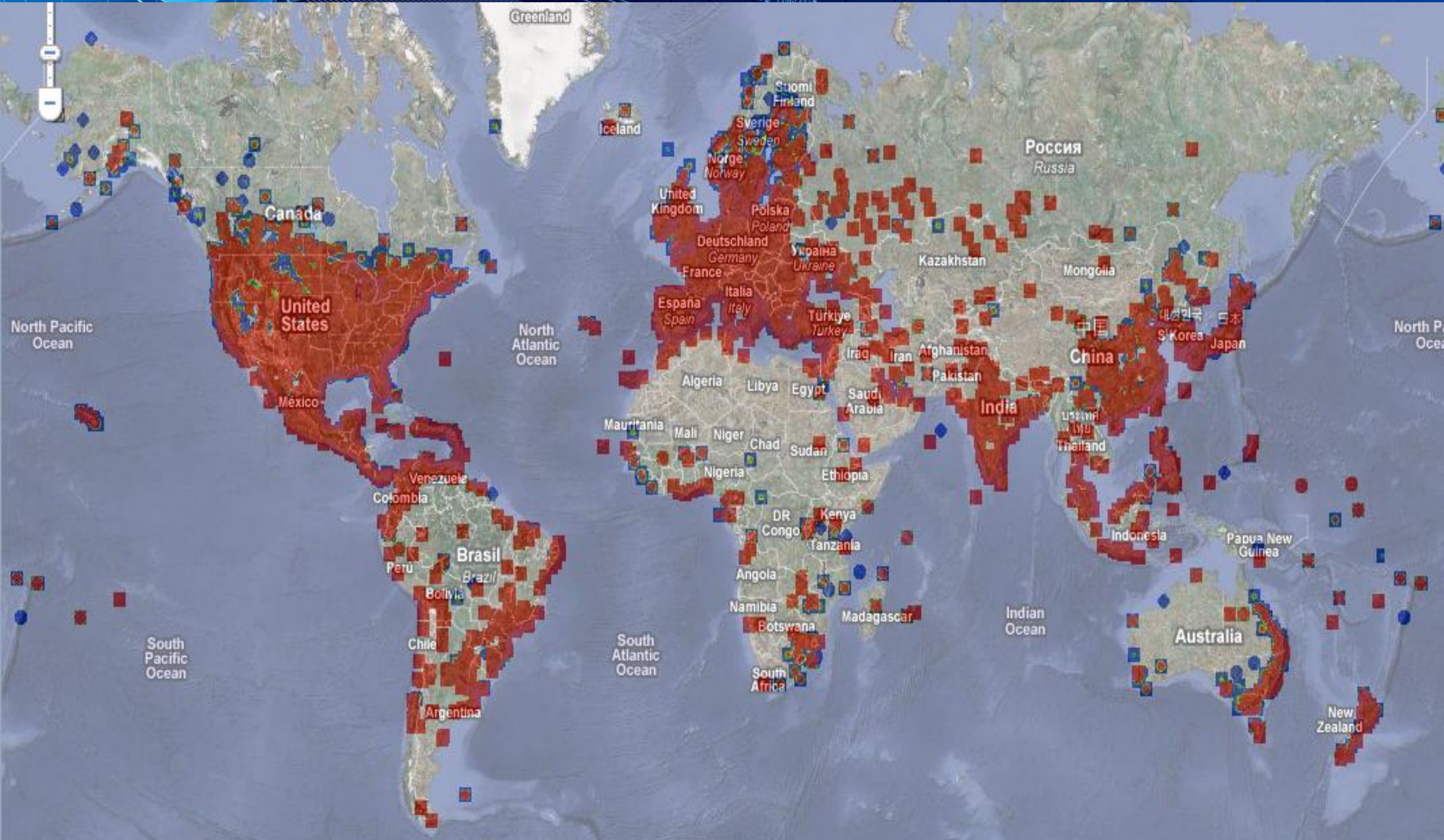
Source: APWG

Varying their frequency of attacks



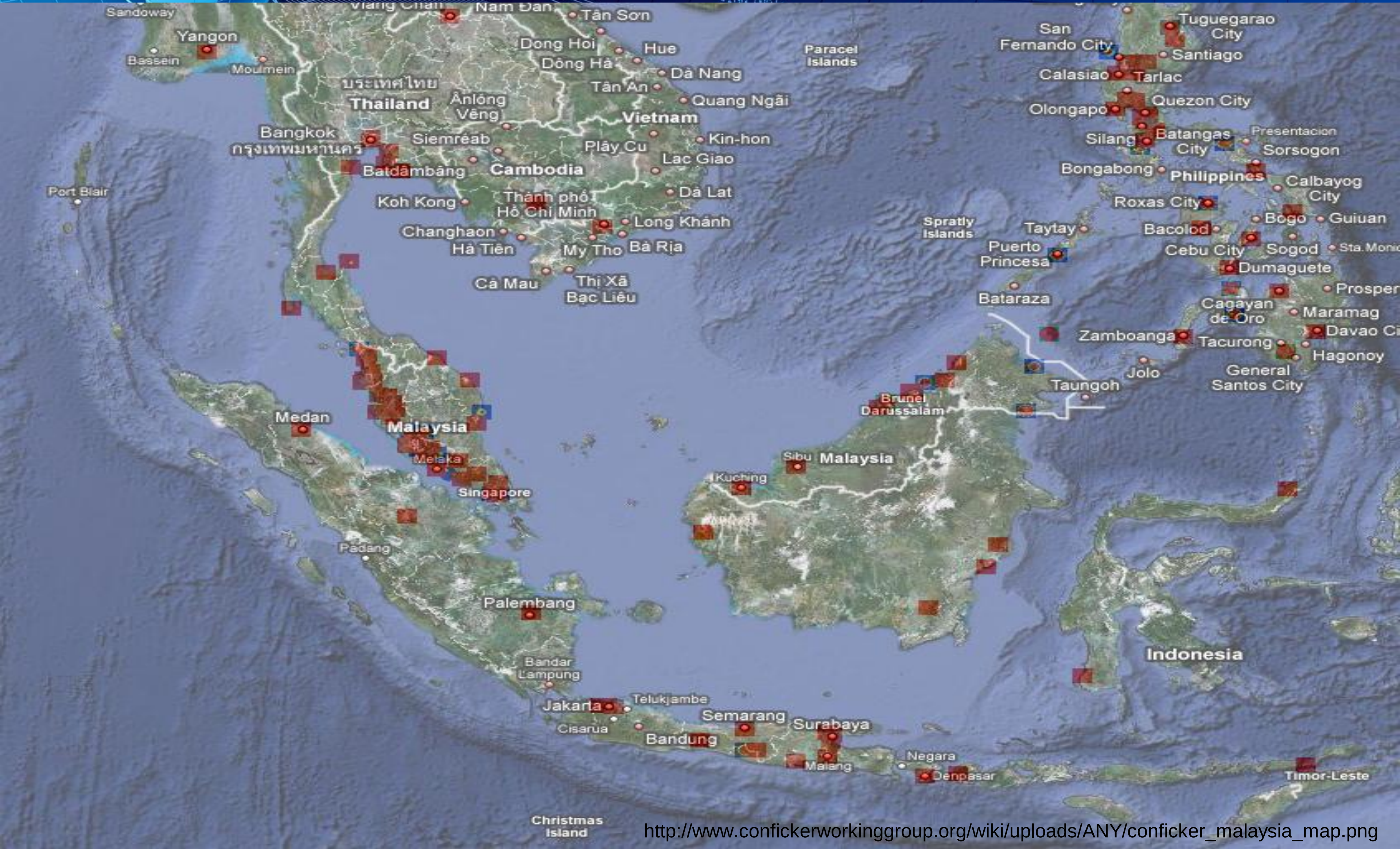
Source: Arbor Networks

And it works…



http://www.confickerworkinggroup.org/wiki/uploads/ANY/conficker_world_map.png

Including in Malaysia…



http://www.confickerworkinggroup.org/wiki/uploads/ANY/conficker_malaysia_map.png

What can you learn from online criminals?

Access Control Anti Spam Anti Virus Application Security Browser Flaws **Consumer Threats** Data Loss Prevention Data Theft Security Education **Email Security** Emerging Threats **Finance Government** Healthcare **High Tech Lawbreakers & Cybercrime** Microsoft Non-Microsoft Patches **Patch Management** Patch Tuesday Phishin **Retail** Spam Techniques Trojans **Vulnerabilities & Flaws**

sc magazine

© Afilias Limited

They operate like you do!

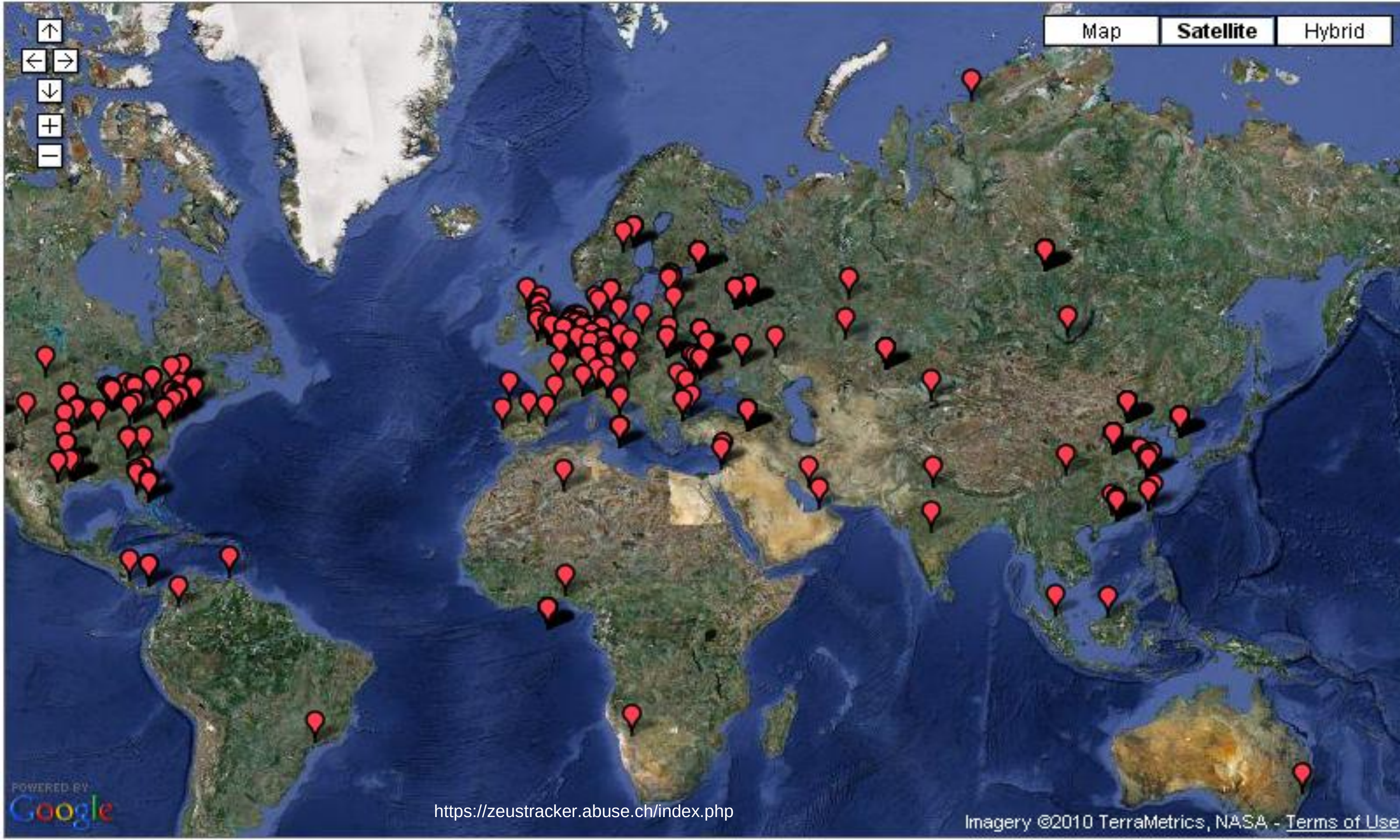
- **Specialized Services**
  - Spammers, Phishers, Kit Builders, Site Builders, Command & Control hoster, Money Launderer…
    - One will do the spamming via his botnet, another will do the phishing kit or phishing sites, another will do the cash-out or money-laundering via online gambling sites
- **Outsourced Operations**
  - They outsource specialty work where appropriate
  - Concentrate on what they do best
- **Bundle related services and create strategic partnerships**
  - Managed spamming services
  - Publish stolen credit cards to buy online ID theft kits
  - Phishing networks that share resources

They operate like you do!

- **Infrastructure and R&D investment**
  - Build scalability, increasing security, leveraging economies of scale
  - Extending infrastructure into new businesses, or for new uses
- **Hardened and secure infrastructure**
  - Use Peer-to-peer botnets, with no centralized command-and-control system

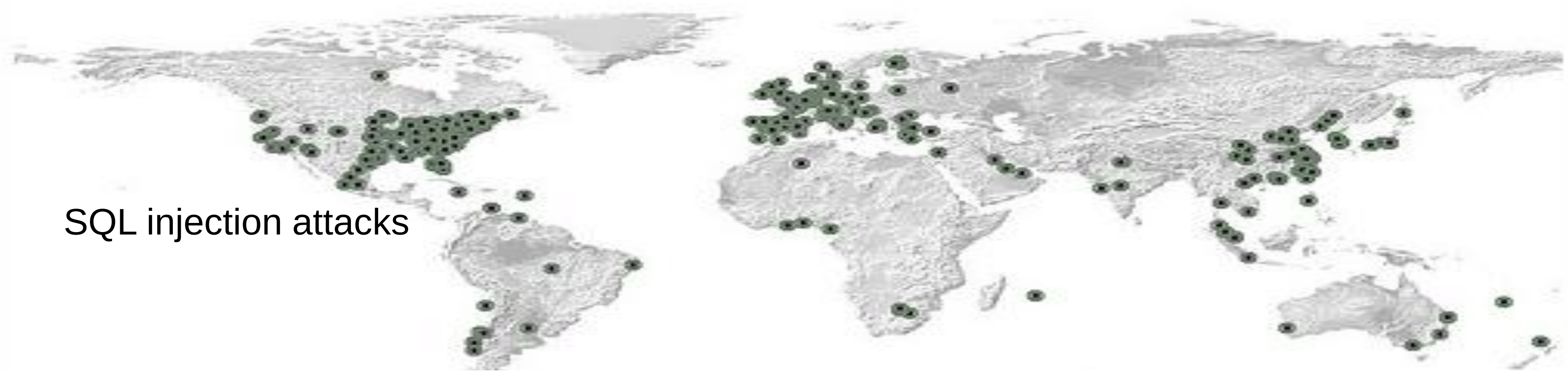
© Afilias Limited

Using Distributed Infrastructure

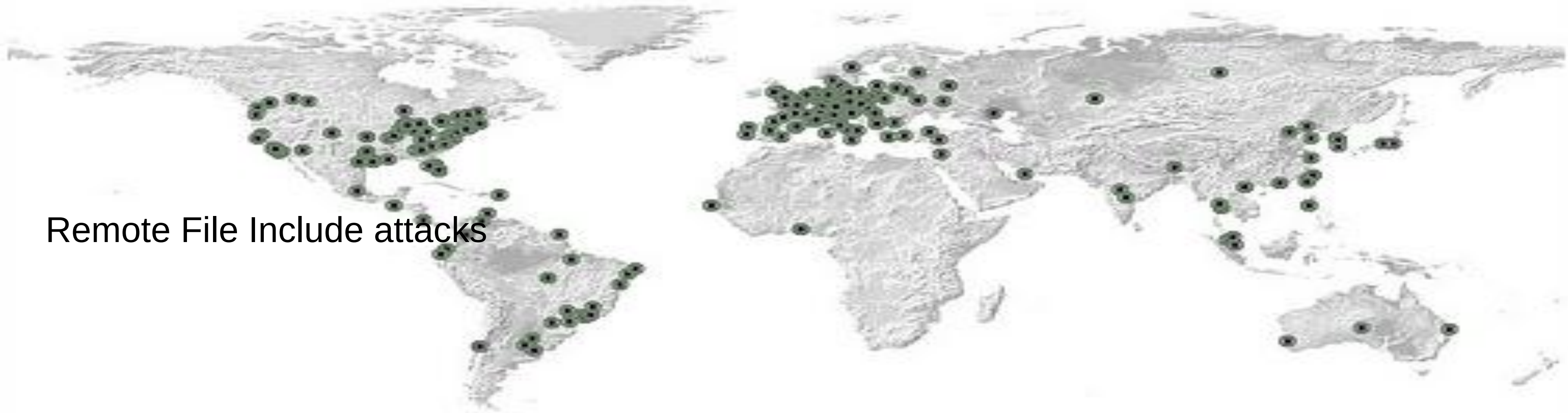


https://zeustracker.abuse.ch/index.php

With Global Points of Presence



SQL injection attacks



Remote File Include attacks

http://asert.arbornetworks.com/2008/10/botnet-visualizations-rfi-and-sql-injections/

Leveraging economies of Scale

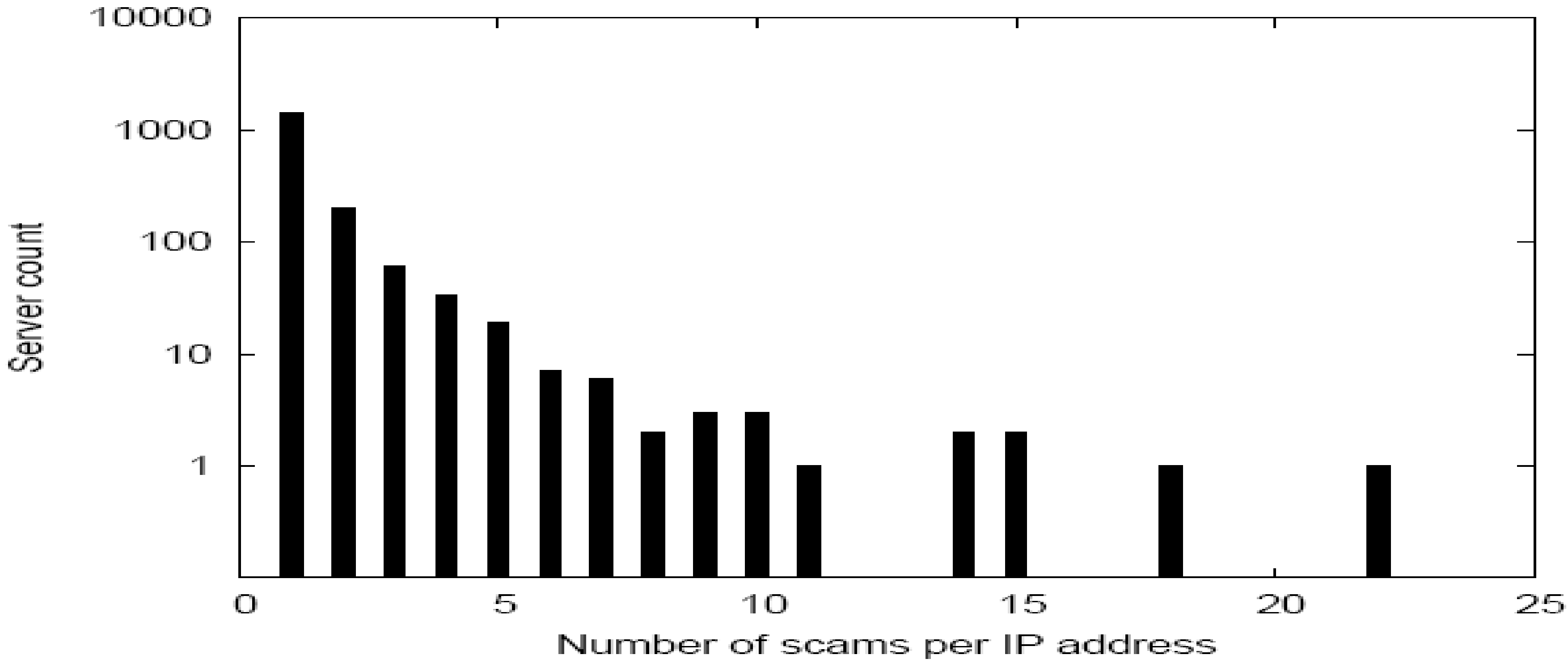
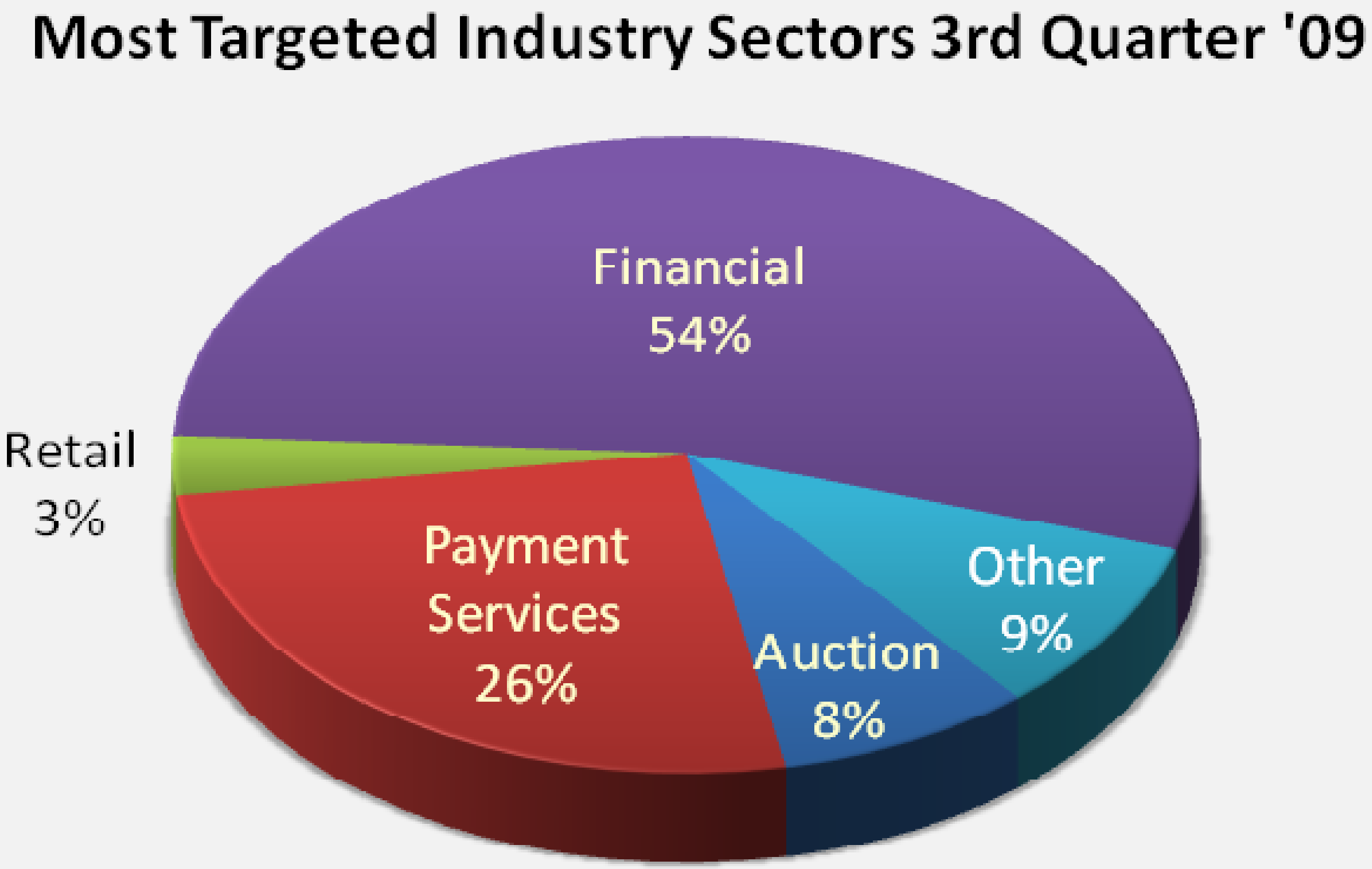


Figure : The number of scams found on a server IP address.

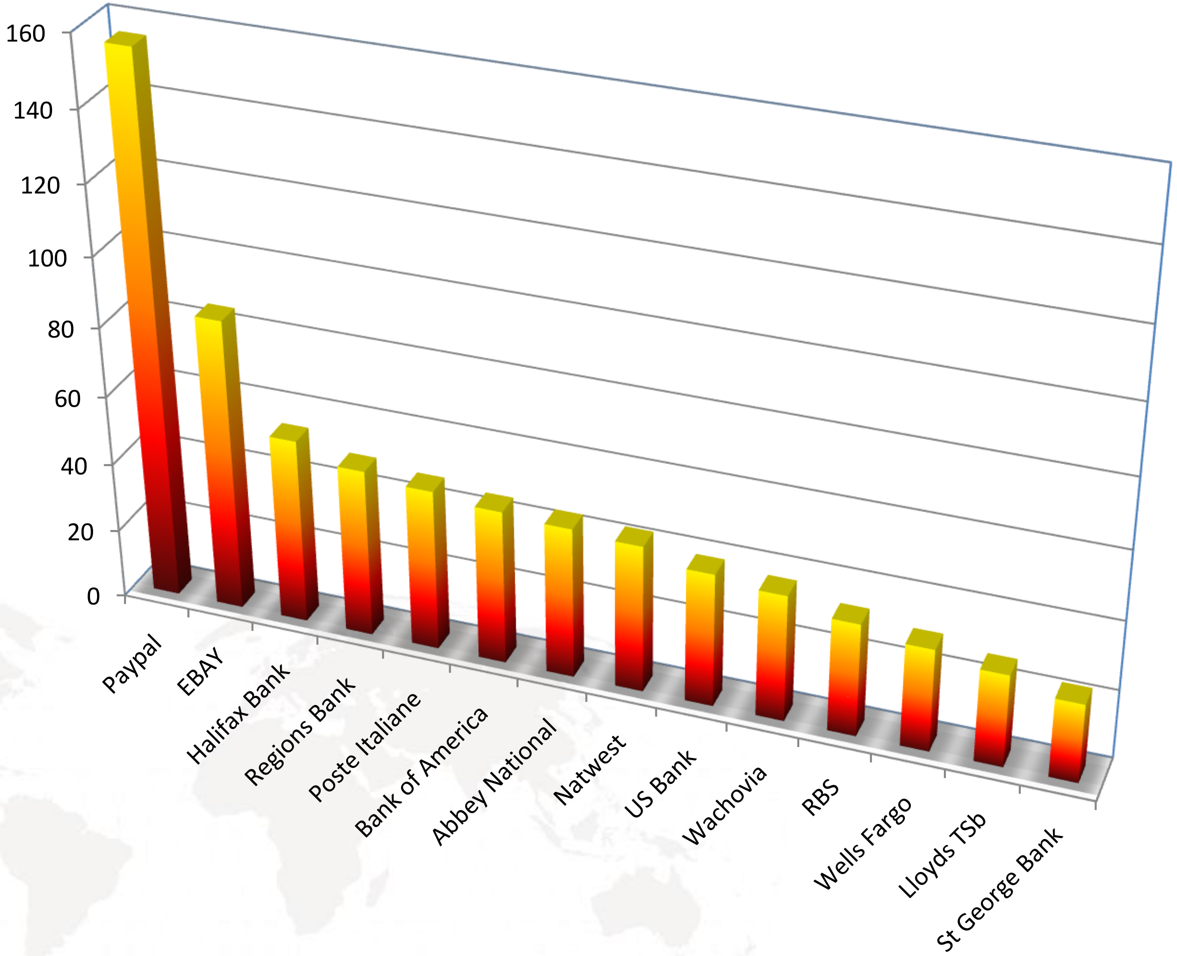
40% of scams were hosted on the same infrastructure as spam

Focused on profitable segments



Source: APWG

Targeting specific “customers”



Afilias Phishing Study, Jan-Oct 2008

© Afilias Limited

With High Speed & High Performance

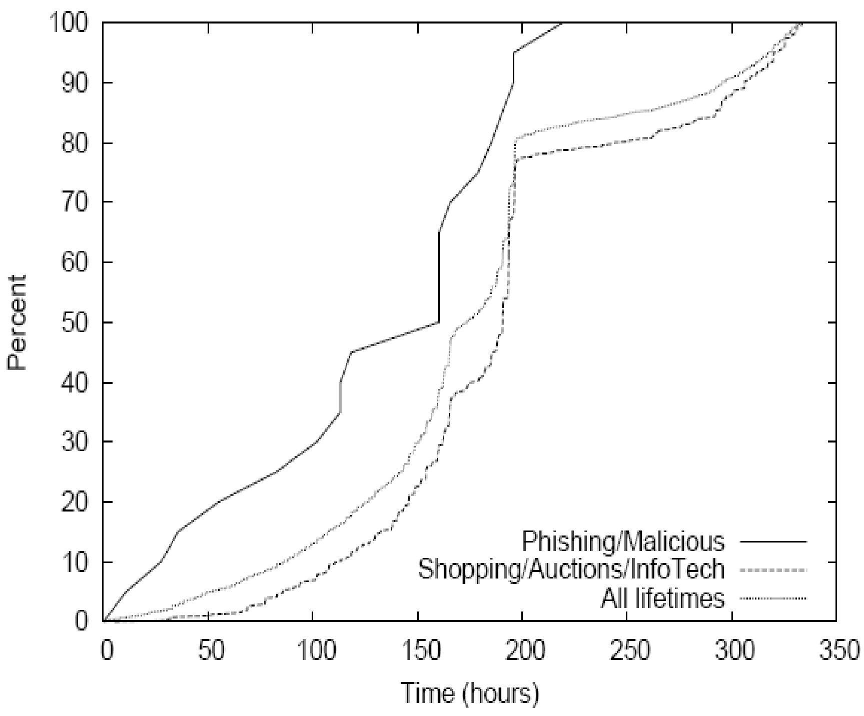


Figure : Scam lifetime distributions for malicious and shopping scams.

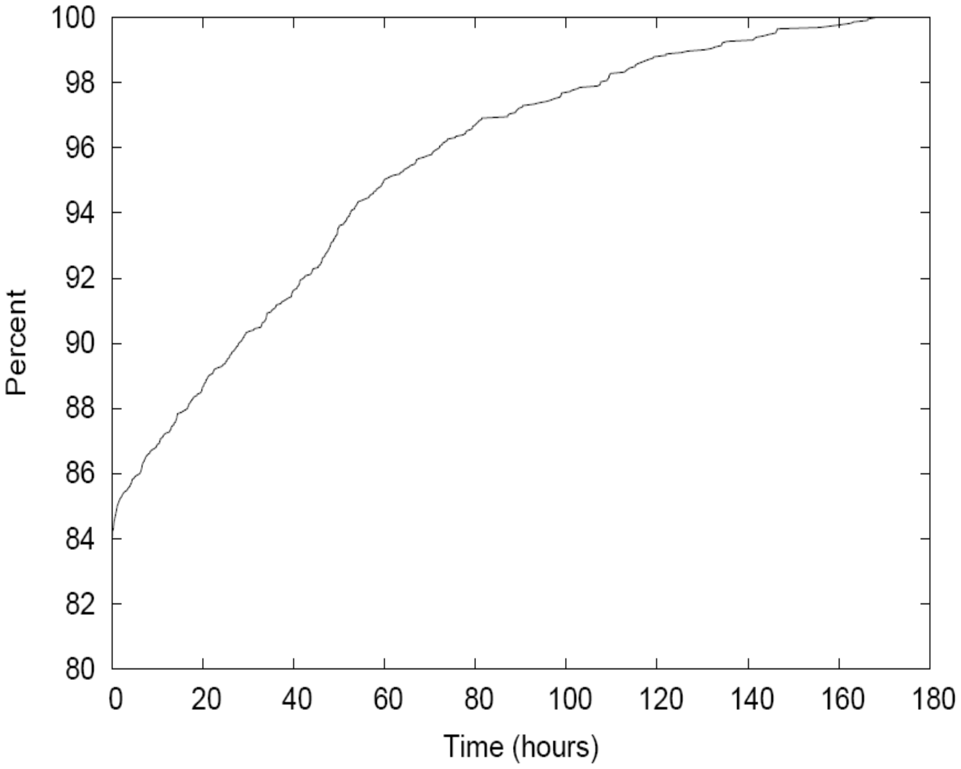


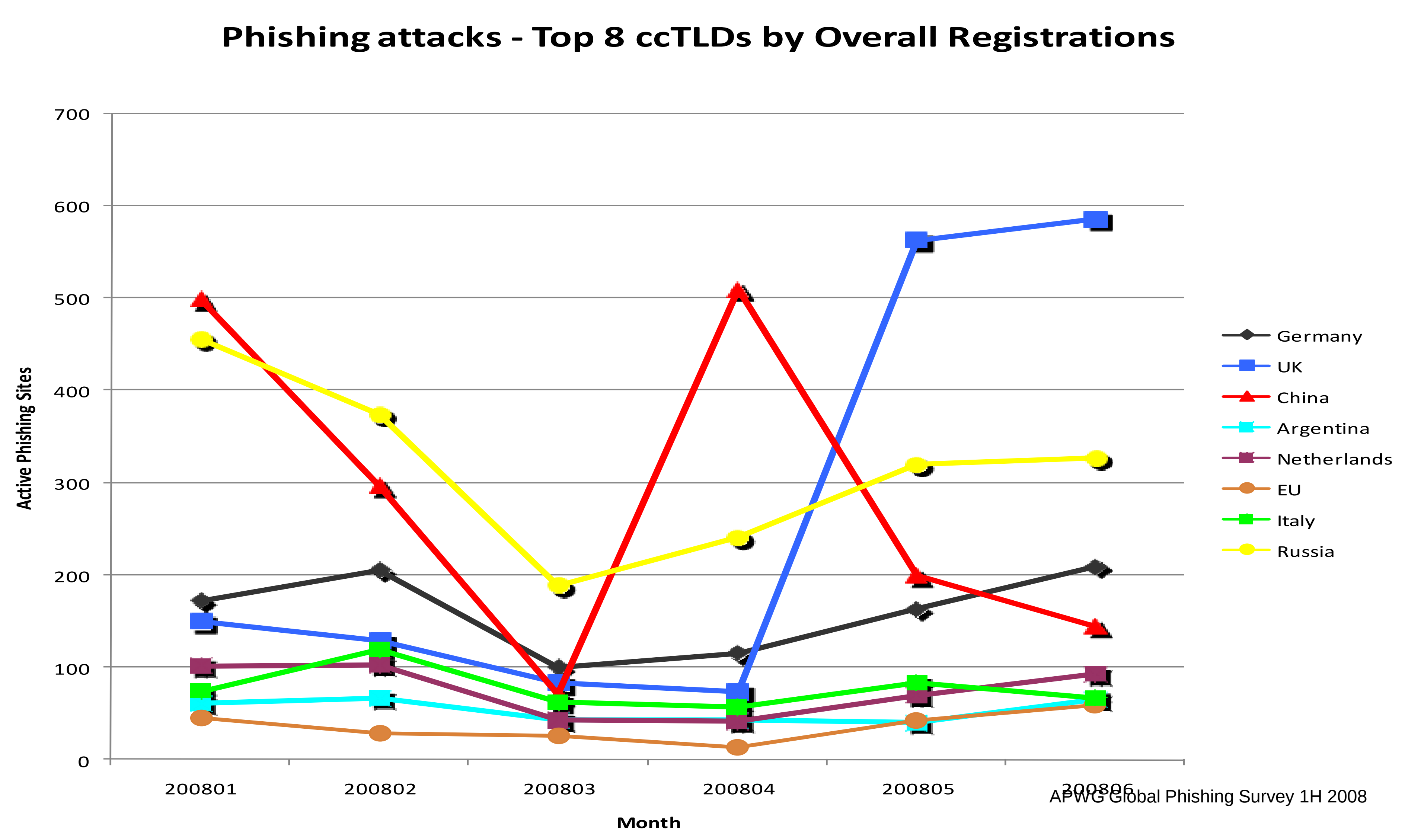
Figure : The duration of a spam campaign.

Spam and phishing sites – come up within minutes and go down within days

Avg. time online for phishing site: 3.8 days
Max. time online for phishing site: 30 days

Spamscatter study, Andeson et al.

Using local supply chains



APWG Global Phishing Survey 1H 2008

Resulting in Strong RoI

The average Revenue per user (RPU) was approximately $1,244 in 2006, up from $257 in 2005 (380% increase in revenue)

Phishing initiatives resulted in **~$2.8 billion** in revenue in 2006

Strong business model combined with first-mover technology resulted in largest group making at least $150 million in 2006

The average consumer victim lost approximately $1,244 in 2006. Up from $257 in 2005. (Source: Gartner Group)

Cumulative losses stemming from phishing attacks rose to more than $2.8 billion in 2006. (Source: Gartner)

VeriSign estimates that the Rock Phish gang alone made $150 million in 2006.

The future of DNS security

- DNS is the technology that underpins the development and functionality of the Internet
- Since DNS was developed, the use and effect of the Internet has fundamentally shifted
  - The Internet is now mission critical to everyone and permeates all communications

Future looking:

DNS and DNS networks need to be based on:

1. **a stable, reliable security model to thwart criminal attacks**
2. **a diverse, scalable network with no single points of failure**

Will the DNS and the root be stable?

Several deployments, more or less in parallel:

- IPv6 (and IPv4 depletion)
- New TLDs
- IDN TLDs (iTLDs)
- DNSSEC deployment

Not a technical scaling question alone

DNSSEC: A new security model for DNS

- DNS Security Extensions (DNSSEC)
  - Best way to protect from a man-in-the-middle attacks and cache poisoning (a.k.a. “the Kaminsky bug”)
- DNSSEC introduces digital signatures to the DNS infrastructure, allowing end users to more securely navigate the Internet.
- Provides effective verification that applications, such as Web or email, are using the correct addresses for servers they want to reach.

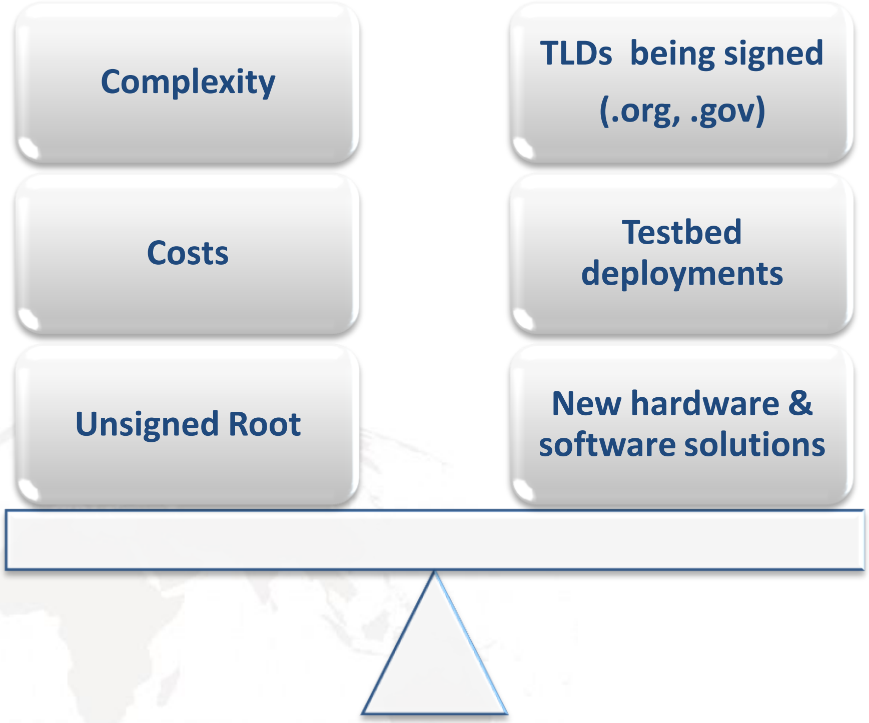
Current state of implementation

- 25-35 TLDs are signed
- .ORG signed, 2009
  - Largest TLD signed to date
- Root to be signed mid-2010
- .COM expected to be signed 2011
- Top of the DNS hierarchy being signed … work remains to be done in spreading this through the DNS resolver infrastructure

What's the tipping point for DNSEC adoption?

Stagnation

Adoption



Complexity

Costs

Unsigned Root

TLDs being signed (.org, .gov)

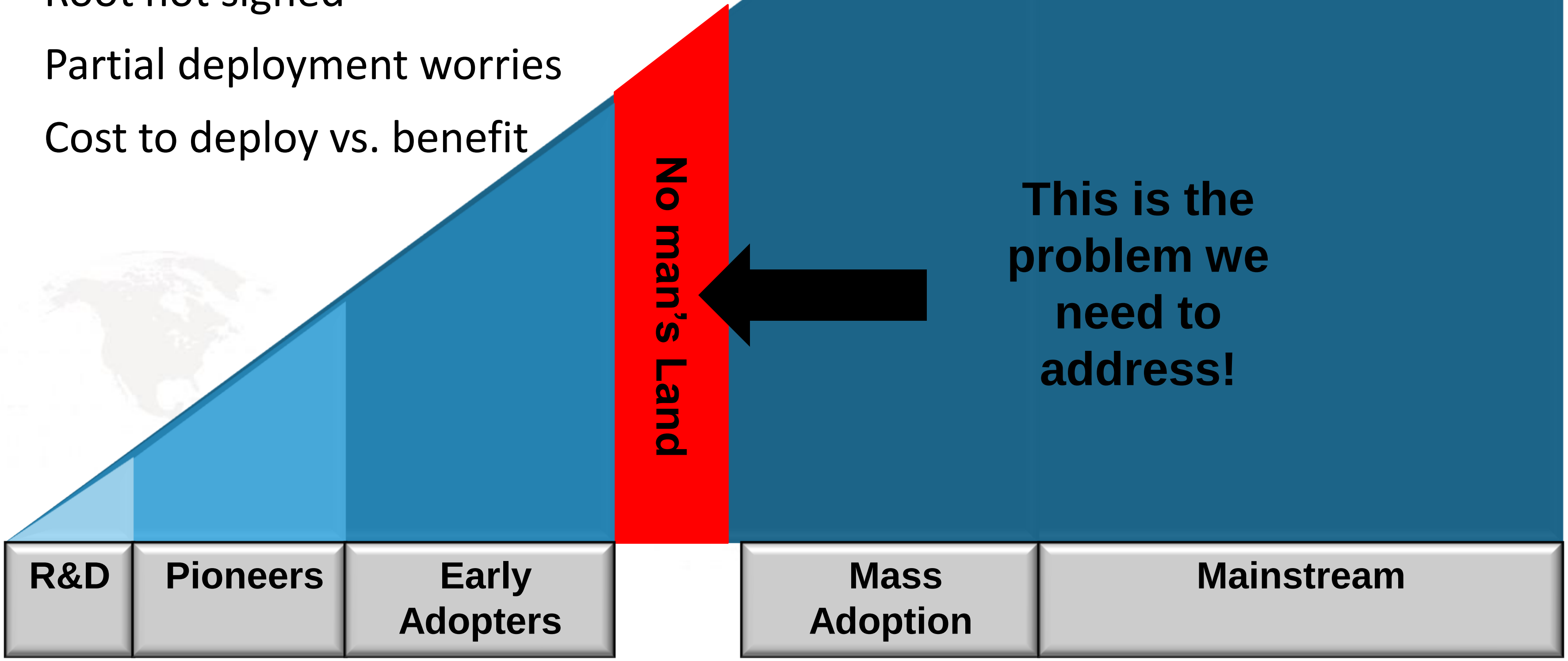
Testbed deployments

New hardware & software solutions

Getting DNSSEC to the mainstream

What are the problems with getting to mass adoption?

- Not enough early adopters
- Complex to implement
- Root not signed
- Partial deployment worries
- Cost to deploy vs. benefit



No man’s Land

This is the problem we need to address!

R&D

Pioneers

Early Adopters

Mass Adoption

Mainstream

Choices to adopt DNSSEC

- Option 1: Do it yourself requires:
  - Hardware and software costs
  - Overcome complexities of key distribution
  - In-house expertise, typically not mission critical
  - Risks of website being inaccessible , if done incorrectly

If a site owner selects this they will have to manage:

•New DNSSEC software

•New DNSSEC hardware

•Generating keys – KSKs, ZSKs

•Loading keys for each zone

• Generating and storing DS records at the registrar

• Key rollover

This is NOT a core business function for most organizations!

Choices to adopt DNSSEC

- Option 2: Outsource
  - Fixed cost
  - No expertise needed
  - Complete end- to-end solution

Requires:

- Known provider with global DNS infrastructure and experience in DNSSEC
- Simple interface for signing and management
- Relationships with Trust Anchors and DNSSEC industry leaders
- Service Level Agreement and Contract

Need for an easy solution

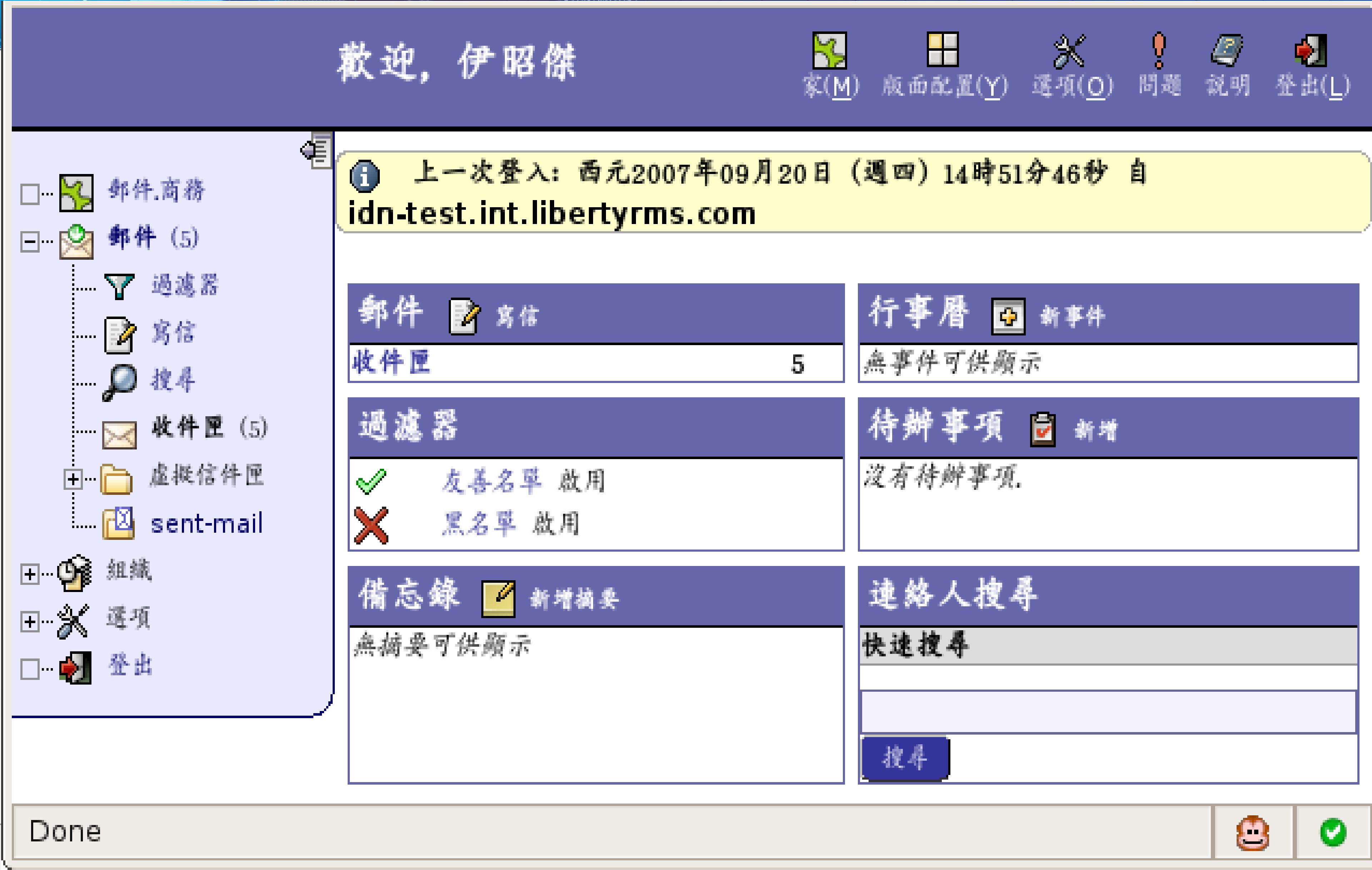
To get DNSSEC to the mainstream DNSSEC needs to be **made easy** with managed services and deployment down the chain of trust

- Afilias beta testing 1-Click DNSSEC^{TM}
  - Security of DNSSEC and the convenience of effortless management, in one solution.
- Opportunity for new DNSSEC products to
  - Securing Email
  - E-Commerce applications
  - RFID networks, etc.

DNSSEC SECURED by Afilias

A future where all domains and all content is in your local language…

Your mailbox in Chinese



歡迎, 伊昭傑

家(M) 版面配置(Y) 選項(O) 問題 說明 登出(L)

- 郵件.商務
- 郵件 (5)
  - 過濾器
  - 寫信
  - 搜尋
  - 收件匣 (5)
  - 虛擬信件匣
  - sent-mail
- 組織
- 選項
- 登出

上一次登入: 西元2007年09月20日 (週四) 14時51分46秒 自 idn-test.int.libertyrms.com

郵件 寫信

收件匣	5

行事曆 新事件

無事件可供顯示

過濾器

✓	友善名單	啟用
✗	黑名單	啟用

待辦事項 新增

沒有待辦事項.

備忘錄 新增摘要

無摘要可供顯示

連絡人搜尋

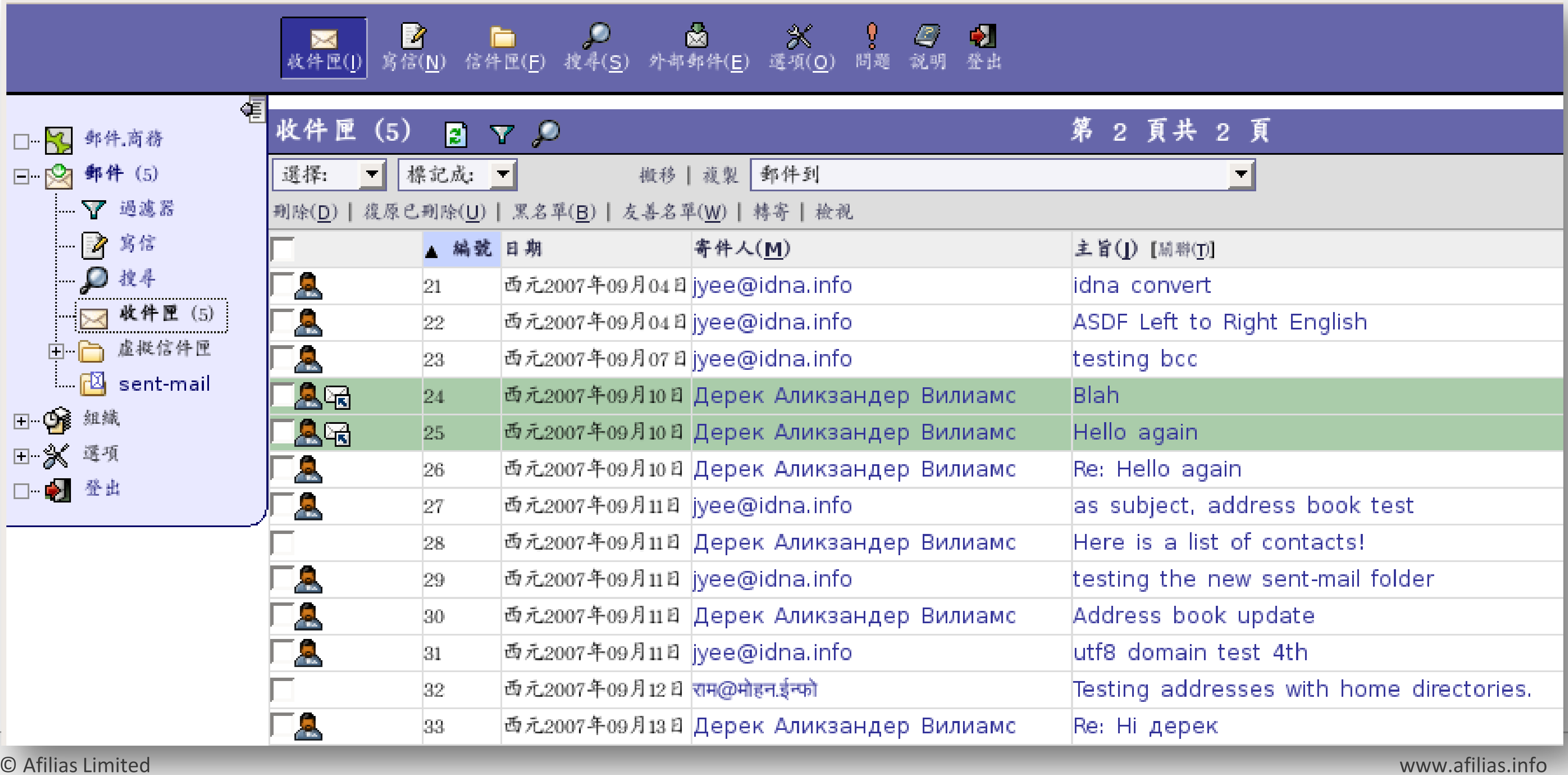
快速搜尋

搜尋

Done

How Do You Know Who Is Writing To You?

- Internet applications must handle messages in multiple languages

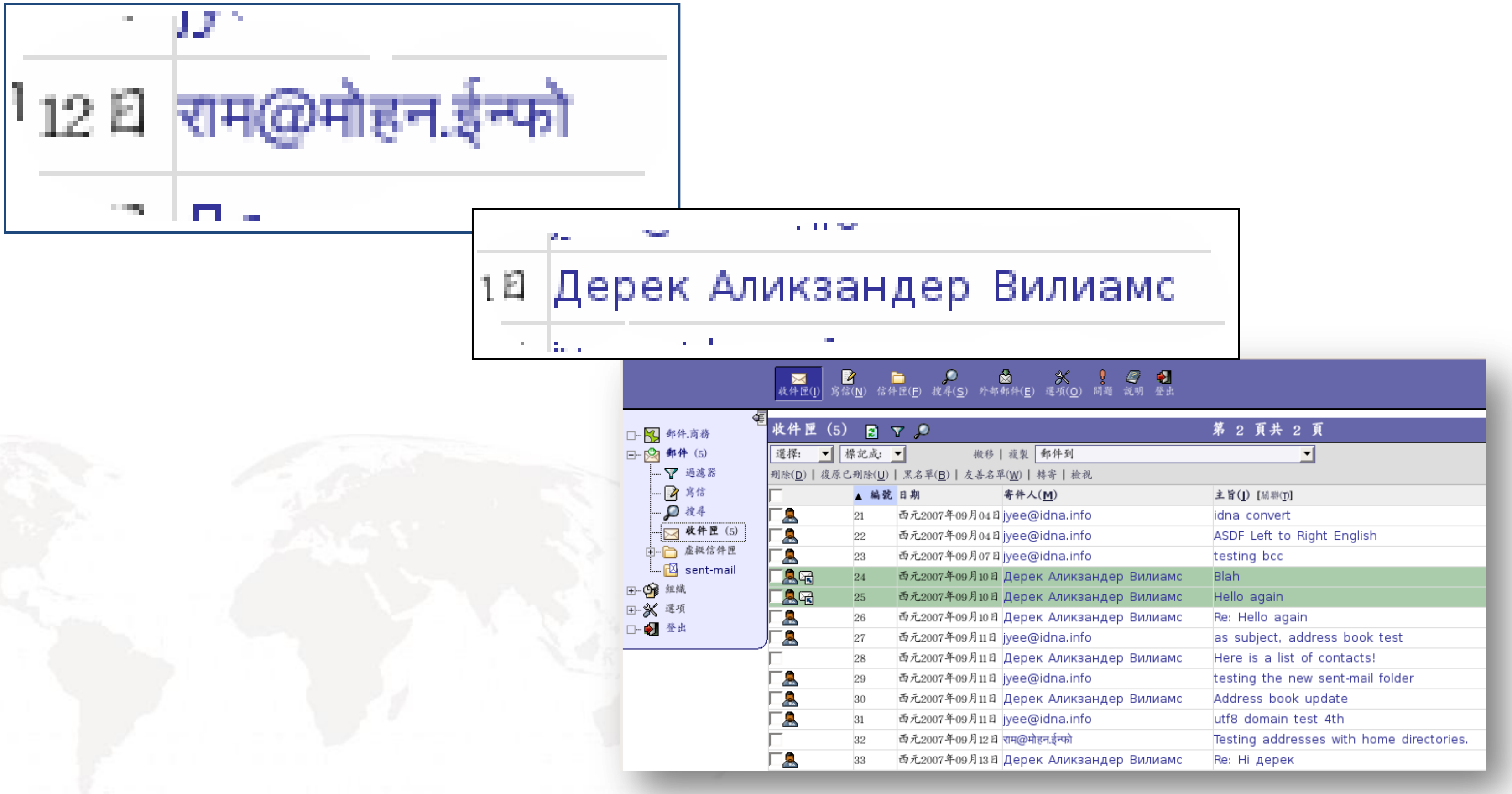


□	▲ 編號	日期	寄件人(M)	主旨(J) [關聯(T)]
□	21	西元2007年09月04日	jyee@idna.info	idna convert
□	22	西元2007年09月04日	jyee@idna.info	ASDF Left to Right English
□	23	西元2007年09月07日	jyee@idna.info	testing bcc
□	24	西元2007年09月10日	Дерек Аликзандер Вилиамс	Blah
□	25	西元2007年09月10日	Дерек Аликзандер Вилиамс	Hello again
□	26	西元2007年09月10日	Дерек Аликзандер Вилиамс	Re: Hello again
□	27	西元2007年09月11日	jyee@idna.info	as subject, address book test
□	28	西元2007年09月11日	Дерек Аликзандер Вилиамс	Here is a list of contacts!
□	29	西元2007年09月11日	jyee@idna.info	testing the new sent-mail folder
□	30	西元2007年09月11日	Дерек Аликзандер Вилиамс	Address book update
□	31	西元2007年09月11日	jyee@idna.info	utf8 domain test 4th
□	32	西元2007年09月12日	राम@मोहन.इन्फो	Testing addresses with home directories.
□	33	西元2007年09月13日	Дерек Аликзандер Вилиамс	Re: Hi дерек

© Afilias Limited

Can You Write To Someone In Another Language?

Applications must allow users to enter text in multiple languages



12 日 राम@मोहन.इन्फो

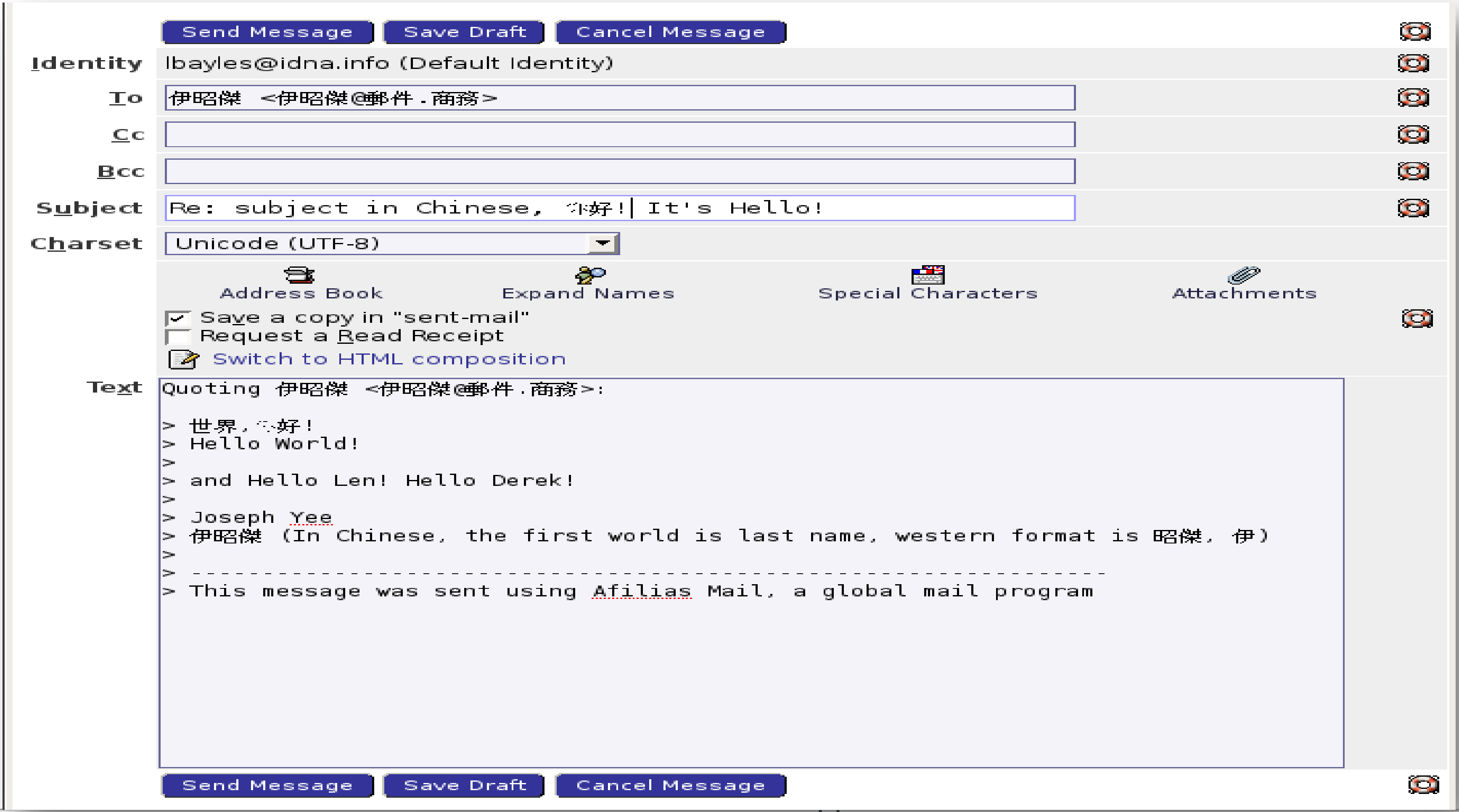
1 日 Дерек Аликзандер Вилиамс

☐	▲ 編號	日期	寄件人(M)	主旨(J) [關聯(T)]
☐	21	西元2007年09月04日	jyee@idna.info	idna convert
☐	22	西元2007年09月04日	jyee@idna.info	ASDF Left to Right English
☐	23	西元2007年09月07日	jyee@idna.info	testing bcc
☐	24	西元2007年09月10日	Дерек Аликзандер Вилиамс	Blah
☐	25	西元2007年09月10日	Дерек Аликзандер Вилиамс	Hello again
☐	26	西元2007年09月10日	Дерек Аликзандер Вилиамс	Re: Hello again
☐	27	西元2007年09月11日	jyee@idna.info	as subject, address book test
☐	28	西元2007年09月11日	Дерек Аликзандер Вилиамс	Here is a list of contacts!
☐	29	西元2007年09月11日	jyee@idna.info	testing the new sent-mail folder
☐	30	西元2007年09月11日	Дерек Аликзандер Вилиамс	Address book update
☐	31	西元2007年09月11日	jyee@idna.info	utf8 domain test 4th
☐	32	西元2007年09月12日	राम@मोहन.इन्फो	Testing addresses with home directories.
☐	33	西元2007年09月13日	Дерек Аликзандер Вилиамс	Re: Hi дерек

© Afilias Limited

What About Content?

Applications must handle content in multiple languages



Identity	lbayles@idna.info (Default Identity)
To	伊昭傑 <伊昭傑@郵件.商務>
Cc	
Bcc	
Subject	Re: subject in Chinese, 你好! It's Hello!
Charset	Unicode (UTF-8)

☑ Save a copy in "sent-mail"
□ Request a Read Receipt

Text

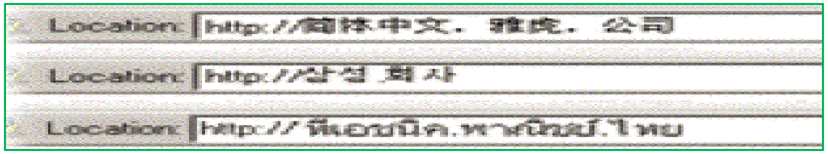
```
Quoting 伊昭傑 <伊昭傑@郵件.商務>:

> 世界，你好！
> Hello World!
>
> and Hello Len! Hello Derek!
>
> Joseph Yee
> 伊昭傑 (In Chinese, the first world is last name, western format is 昭傑, 伊)
>
> ----------------------------------------------------------------
> This message was sent using Afilias Mail, a global mail program
```

© Afilias Limited

IDN Utility – 2010 & Beyond

- Will work in all major browsers (incl mobile phones)
- IDN Email is already working
- Will it affect SEO? (local content with local language URLs)
- Applications will start adopting/using IDNs

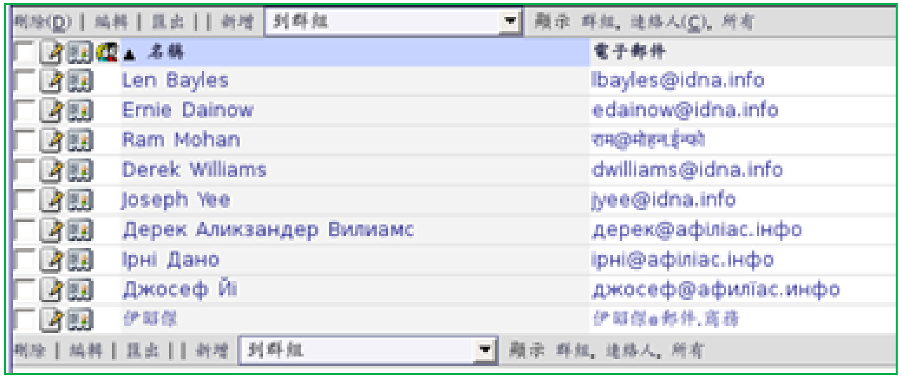


Location: http://網絡中文. 雅虎. 公司

Location: http://삼성 회사

Location: http://ทีเอชนิค.พาณิชย์.ไทย

IDNs in browsers, 2008



刪除(D) | 編輯 | 匯出 | | 新增 列郵組 顯示 郵組, 連絡人(C), 所有

名稱	電子郵件
Len Bayles	lbayles@idna.info
Ernie Dainow	edainow@idna.info
Ram Mohan	राम@मोहन.इंफो
Derek Williams	dwilliams@idna.info
Joseph Yee	jyee@idna.info
Дерек Аликзандер Вилиамс	дерек@афіліас.інфо
Ірні Дано	ірні@афіліас.інфо
Джосеф Йі	джосеф@афилïас.инфо
伊麗莎	伊麗莎@郵件.商務

刪除 | 編輯 | 匯出 | | 新增 列郵組 顯示 郵組, 連絡人, 所有

IDNs in email, 2008

IDN TLDs on-the-go, 2009?

Designing a diverse, scalable network with no single points of failure…

TLD Security Readiness plan

1. Become a member of industry research and action groups such as
   - RISG (Registry Internet Security Group) registrysafety.org
   - OARC (DNS Operations, Analysis & Research Center) dns-oarc.org
   - APWG (Anti Phishing Working Group) 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

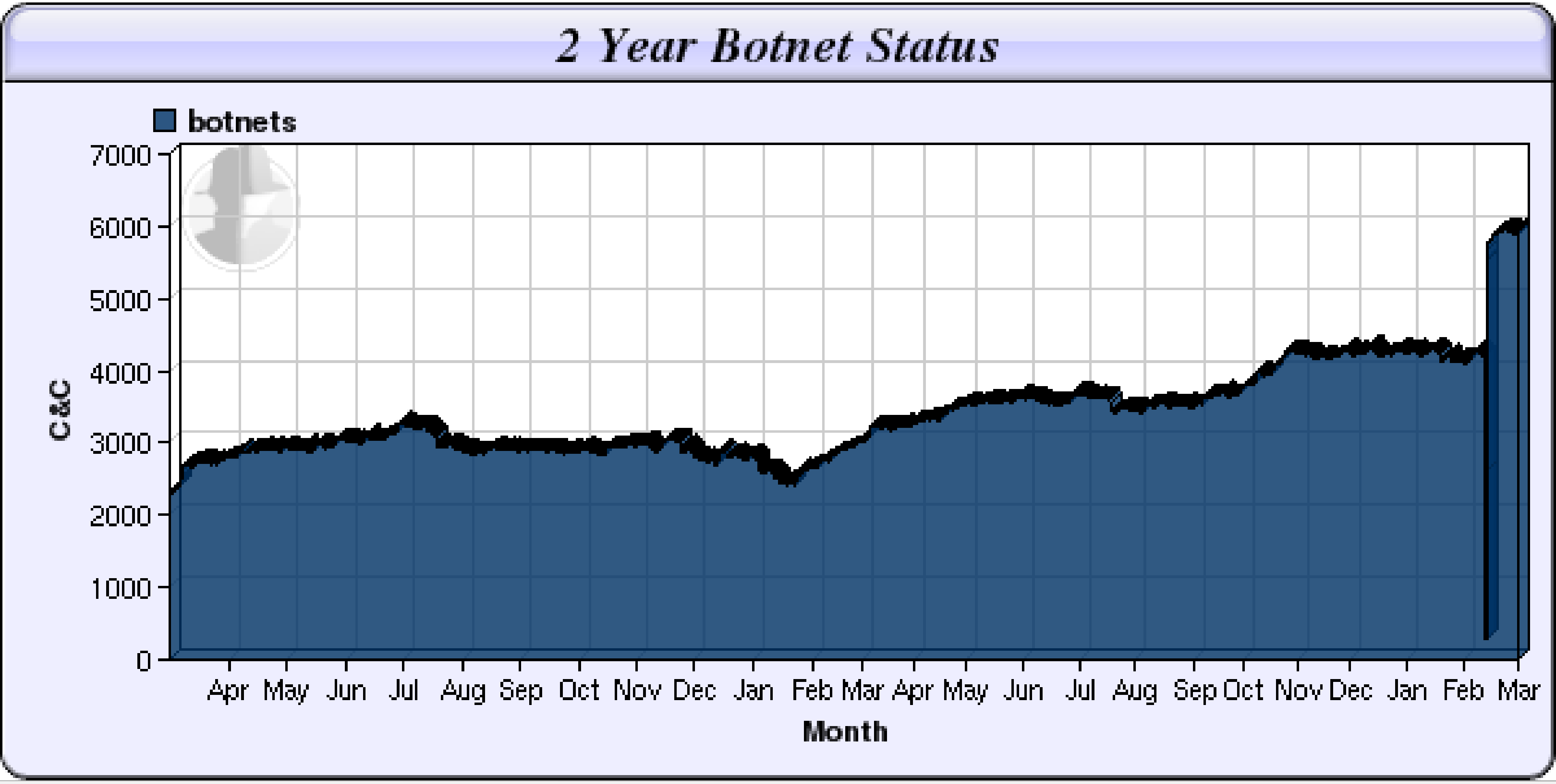
3. Proactive Monitoring
   - A NOC is not enough!
   - Track external research to ID new trends and threats
4. Institute a Domain Anti-Abuse Policy
   - Enables you to work with registrars to take down sites within your existing registration policies
5. Operate on a secure, diverse DNS architecture
   - Redundant architecture able to withstand attack
   - Diversity to ensure that no single point of failure can bring down your network

Why you need to consider DNS Security more seriously

- It's not just companies being targeted anymore!
- The DNS is growing more and more susceptible to attack through
  - Continued and larger scale DDoS attacks aimed at the Root and TLD operators
  - Regionalized attacks focusing on countries or specific governments / government agencies
- DNS is being victimized by new malicious activity (e.g.: Worms like Conficker)
- Small DNS networks being tasked with heavy load from new services (e.g.: URL shortening)

Botnets are here to stay

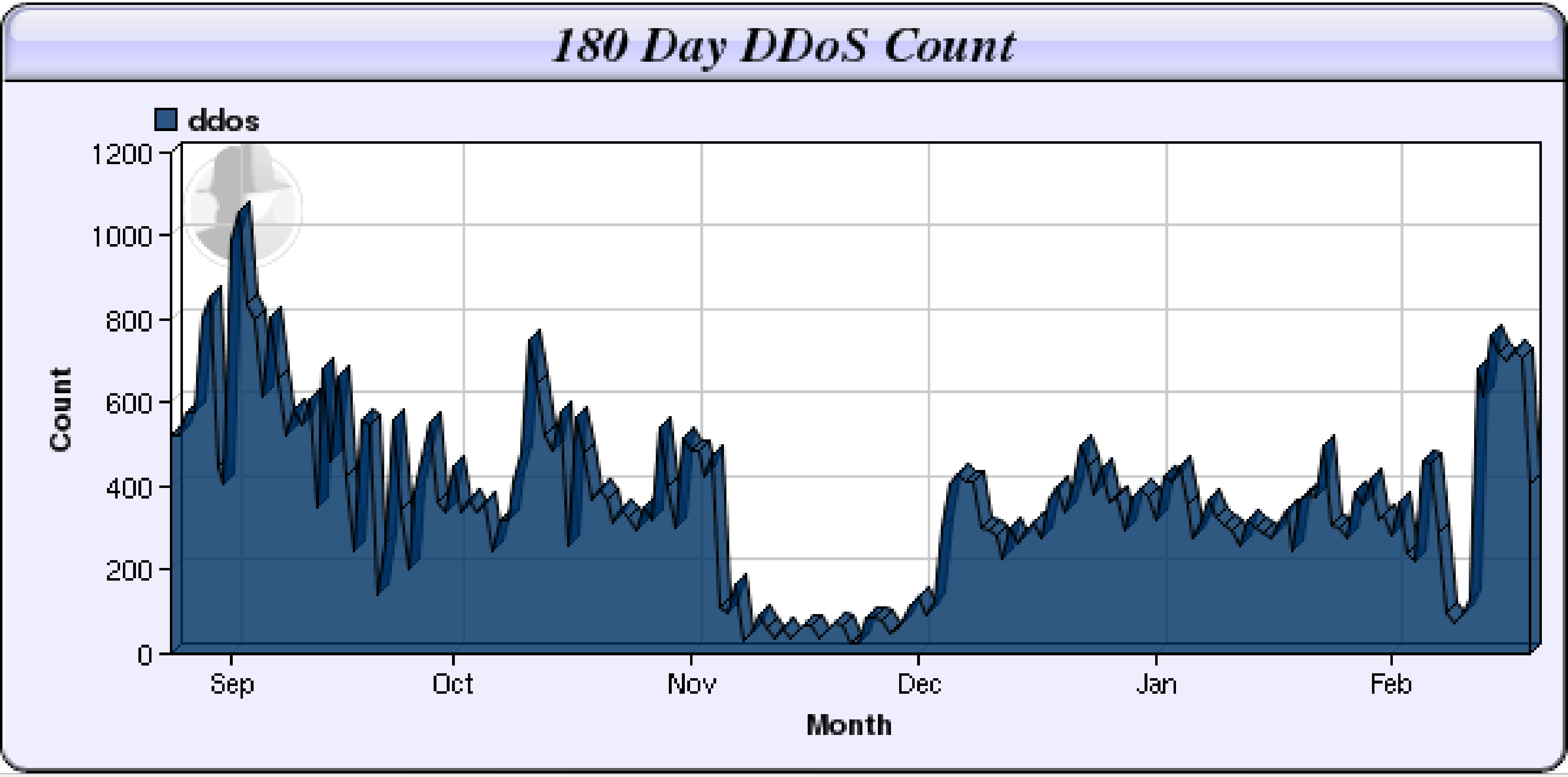
- Larger attacks, more sophistication



Source: http://www.shadowserver.org

DDOS Remains Serious Threat

- Increasing frequency and sustained activity



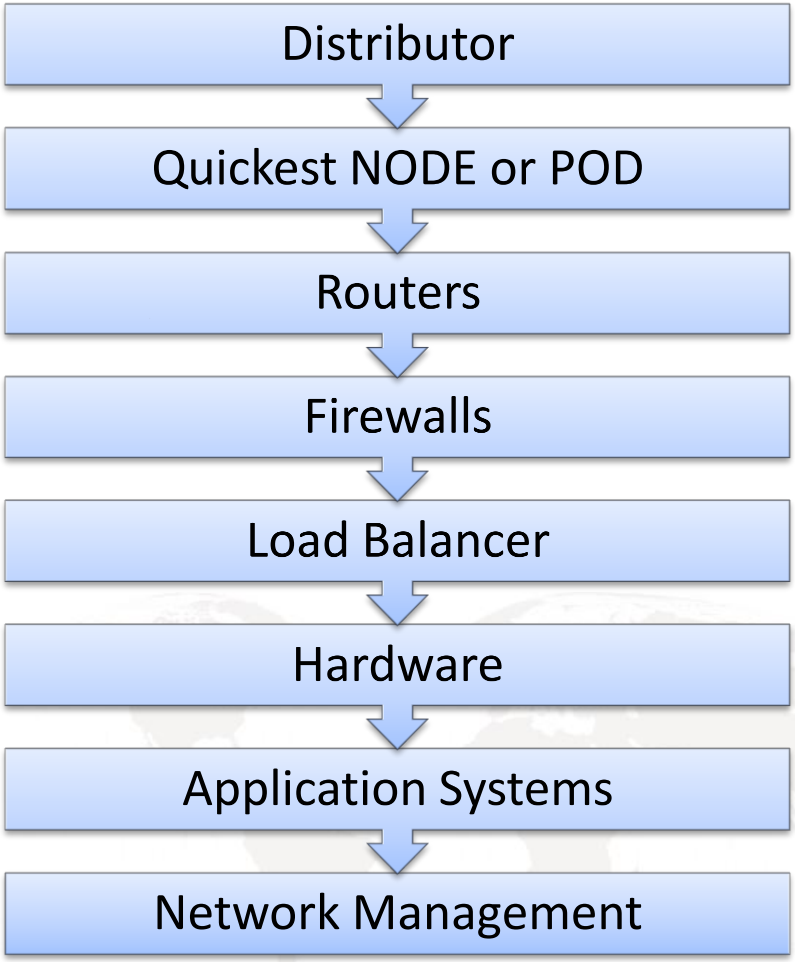
© Afilias Limited

Source: http://www.shadowserver.org

Build your network with diversity

- No other Internet technology matters if users can not get to the Web site, or the e-mail can not be delivered.
- Treat your DNS like you do any other technology – **build it with redundancy, scalability and ensure no single points of failure**
- To deploy diversity across your DNS your options include:
  1. Internal development
  2. Adding an outsourced provider

Implementing DNS Diversity



Distributor

Quickest NODE or POD

Routers

Firewalls

Load Balancer

Hardware

Application Systems

Network Management

Diversity at all levels

- Multiple DNS providers
- Multiple types of DNS software (e.g. : Bind + NSD)
- Geographically diverse datacenters and NOCs
- Geographically diverse DNS node constellation on multiple continents
- Nodes configured with Anycast technology
- Multiple bandwidth providers w/ min. 1 gbps
- Multiple brands of hardware (e.g: both Cisco and Juniper Routers)
- No single OS or other software
- Diversity in Personnel and expertise

Thank You!

Ram Mohan
Afilias
rmohan@afilias.info
www.afilias.info

.info Where the World Goes for Information.

.org advance your mission

.mobi Internet Made Mobile

.Asia

.aero the domain of aviation

.bz NIC HN NicAG domain registration .GI .in .VC .LC .MN Domain Registry .SC Me