RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

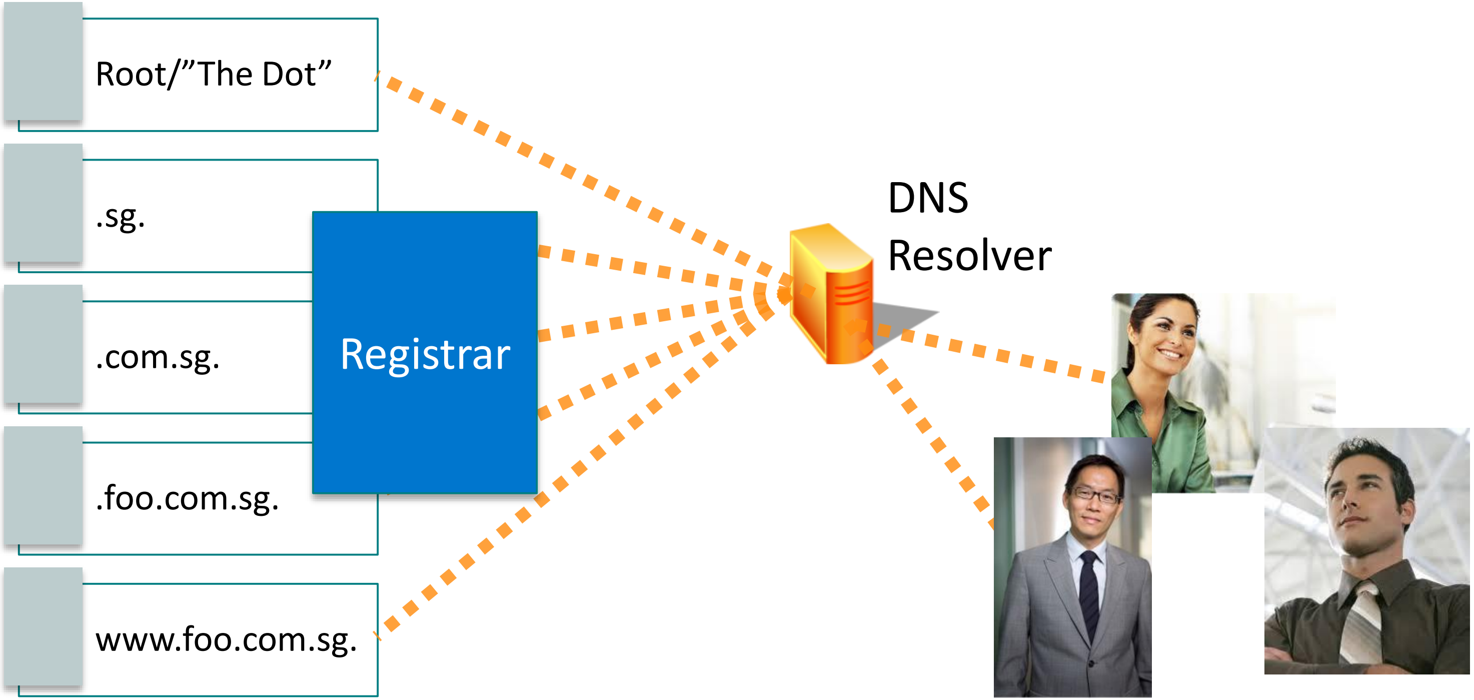
SESSION ID: CLE-F01

DNS in the Crossfire: 2 Years of Hijacks and Defacements

Michael Smith

APJ Security CTO
Akamai Technologies
@rybolov

DNS Hierarchy



Root/"The Dot"

.sg.

.com.sg.

.foo.com.sg.

www.foo.com.sg.

Registrar

DNS Resolver

Whois akamai.com

```
$ whois akamai.com | grep ’^Name Server'
Name Server: A1-66.AKAM.NET
Name Server: A11-66.AKAM.NET
Name Server: A13-66.AKAM.NET
Name Server: A28-66.AKAM.NET
Name Server: A16-66.AKAM.NET
Name Server: A7-66.AKAM.NET
……
```

These are
all glue
records

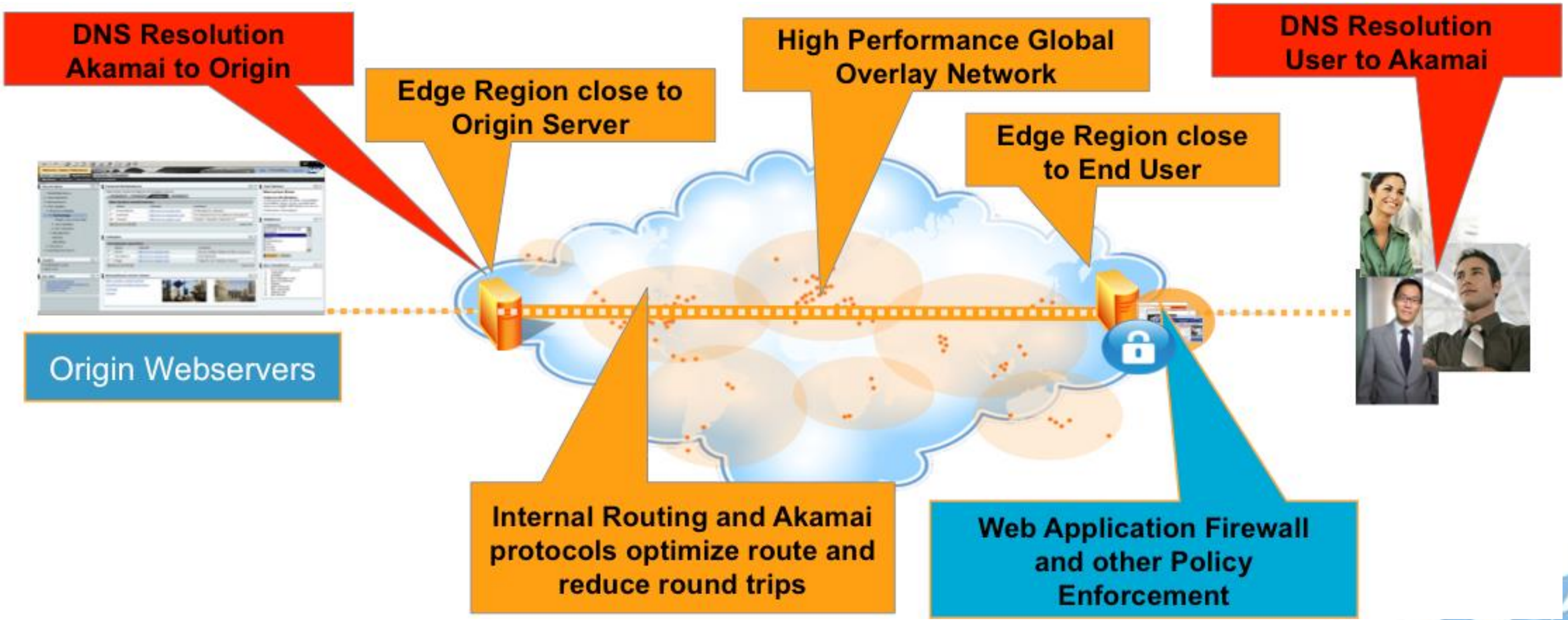
Glue Record TTL

```
$dig +trace www.akamai.com

.              56955    IN    NS    f.root-servers.net.

com.           172800   IN    NS    e.gtld-servers.net.

akamai.com.    172800   IN    NS    a5-66.akam.net.
```

Case Study 1: Oops, Premature Expiration

- Catch expired domains and kite them
- Registrar expires domains early
- ~1500 Domains hijacked
- Chaos ensues
- Multiple mitigation streams

Basic CDN and DNS Operation



DNS Resolution Akamai to Origin

Edge Region close to Origin Server

High Performance Global Overlay Network

DNS Resolution User to Akamai

Edge Region close to End User

Origin Webservers

Internal Routing and Akamai protocols optimize route and reduce round trips

Web Application Firewall and other Policy Enforcement

The Magic of DNS CNAMEs and TTLs

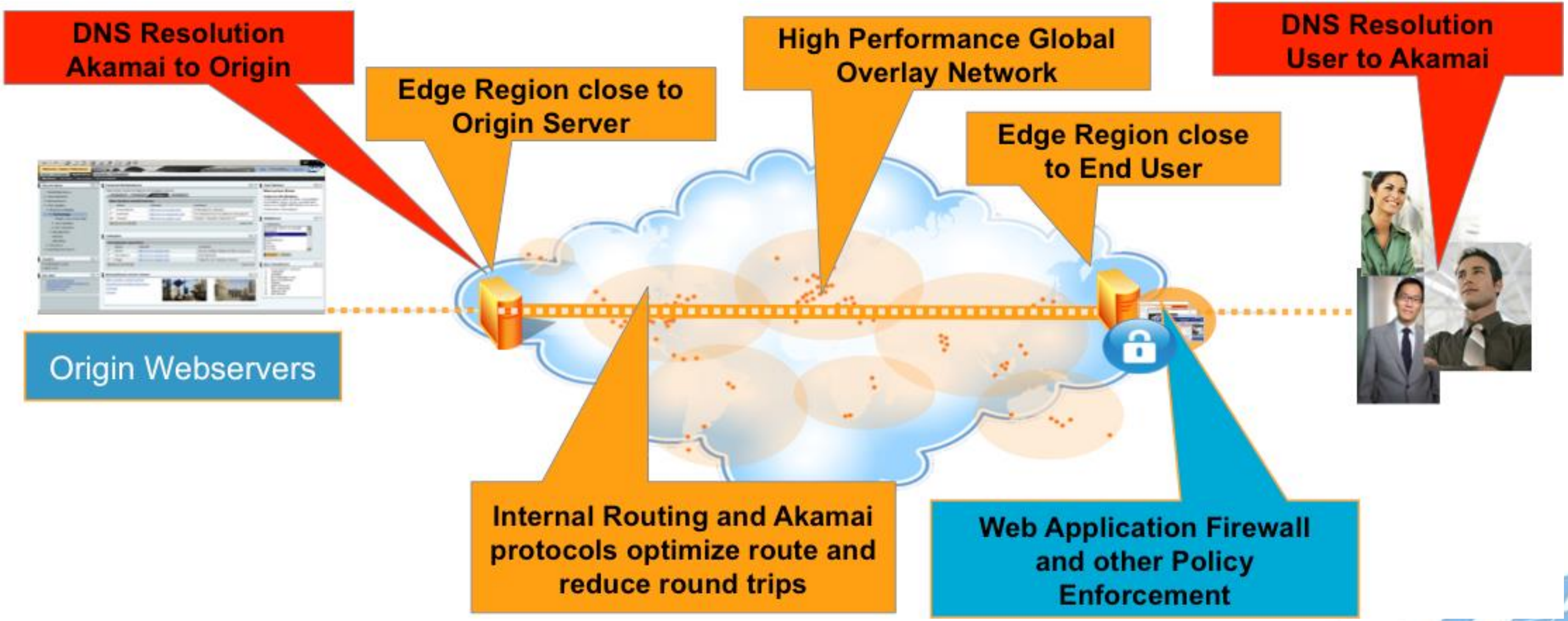
```
$ dig www.akamai.com


;; ANSWER SECTION:

www.akamai.com.        20  IN  CNAME
     wwwsecure2.akamai.com.edgekey.net.

wwwsecure2.akamai.com.edgekey.net. 1576  IN CNAME
e8921.dscx.akamaiedge.net.

e8921.dscx.akamaiedge.net. 6 IN  A   23.74.224.166
```

Case 2: SEA Brings us “Hacksgiving”

Hacksgiving Details

- Hijack of “monetization service”
- Served JavaScript with url rewrite
- Services delivered from the SEA webservers
- 40+ Sites impacted
- 2 Incident workflows
  - Restore hijacked domain
  - Disable content on customer’s sites and republish

Basic CDN and DNS Operation



DNS Resolution Akamai to Origin
Edge Region close to Origin Server
High Performance Global Overlay Network
DNS Resolution User to Akamai
Edge Region close to End User
Origin Webservers
Internal Routing and Akamai protocols optimize route and reduce round trips
Web Application Firewall and other Policy Enforcement

Case 3: Lizard Squad

Lizard Squad Domain Hijacks

- Compromised registrar or phishing domain logins
- Change domain NS glue records
- Set up MX record and capture email
- Build infrastructure
  - DNS zone on service provider
  - Defacement page on CDN
  - Email server

Whois => Spear Phishing

```
$ whois akamai.com | grep \@
Registrar Abuse Contact Email: domainabuse@tucows.com
Reseller: hostmaster@akamai.com
Registrant Email: hostmaster-billing@akamai.com
Admin Email: hostmaster-billing@akamai.com
Tech Email: hostmaster-billing@akamai.com
Akamai Technologies, hostmaster@akamai.com
```

The Phish

Akamai Technologies

Your domain, akamai.com is due to expire. Please <a href=www.wecaptureyourlogin.net>login to renew this domain</a>

Thank you

--Your Registrar

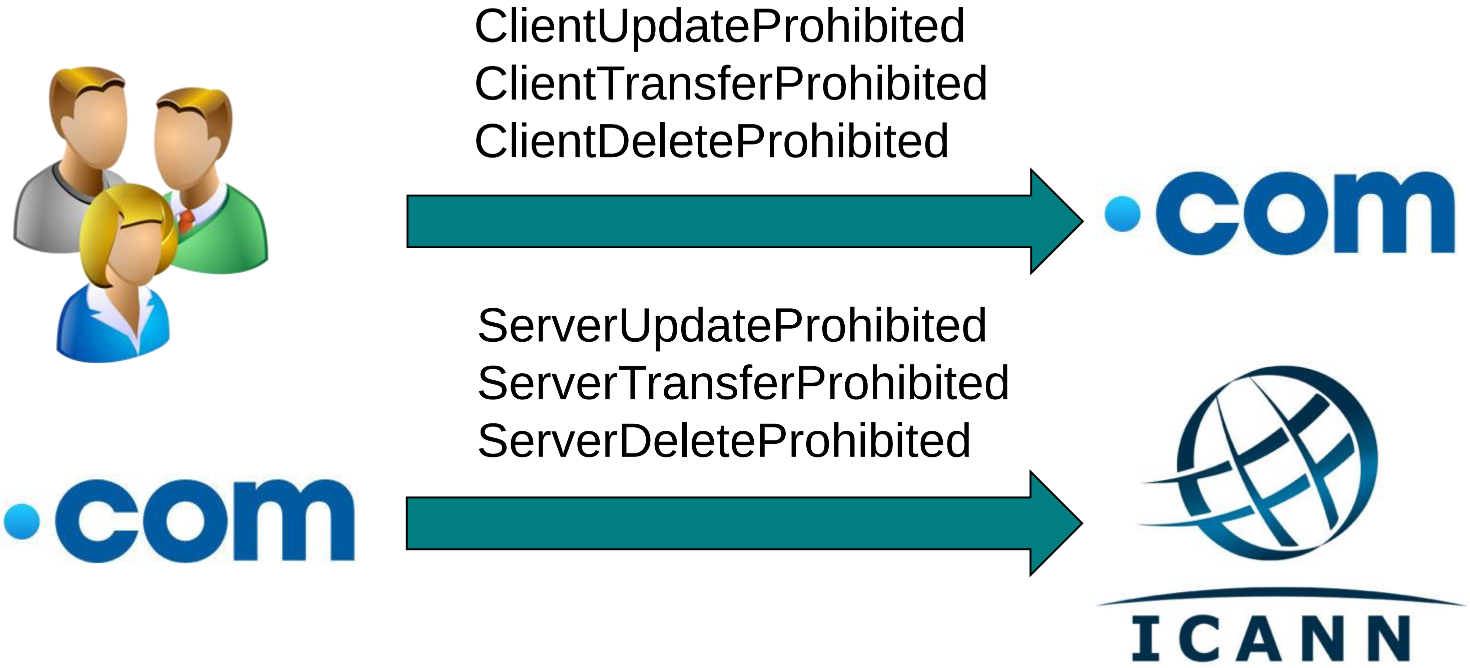
How Akamai Changed Their Operations

- Forward to Origin SSL
- Alerts for minimum traffic level
- Edge server DNS purge
- Content purging
- AkaRegistrar
- Portal 2-factor/SAML/ACL access control

Prevention and Application

- Lock your domains, lock your domains, lock your domains
- Whois privacy
- site:github.com dns monitoring
- 2FA on registrars and other providers
- Anti-phishing training for IT admins
- Ready to disable third-party content
- 2FA on email, VPN

Domain Hijacking Countermeasures



ClientUpdateProhibited
ClientTransferProhibited
ClientDeleteProhibited

ServerUpdateProhibited
ServerTransferProhibited
ServerDeleteProhibited

Thank You