

Internet Security:
Report from the ICANN
Security and Stability Advisory Committee

David Piscitello
Senior Security Technologist
ICANN

About SSAC

- SSAC advises the ICANN community on matters relating to the *security and stability of the Internet's unique systems of names, numbers and identifiers*
 - Not a policy-making body
- Committee of volunteers with expertise in, internetworking, security, DNS name server operations, domain name registry and registration services
- SSAC studies a wide range of matters
 - Technology and behavior that affect name, address (and routing) systems
 - Traditional security analysis (incidents, abuses)
 - Interactions between technology and market forces

Completed Projects

Domain Name Hijacking

Alternative TLD Name Systems and Roots

Renewal Considerations for Domain Name Registrants

DNS Distributed Denial of Service (DDoS) Attacks

Redirection in the COM and NET Domains

Adding IPv6 Resource Records at the Root of DNS

Commercial firewall support of IPv6 transport

Domain Name Front Running

Registrar Impersonation in Phishing Attacks

Fast flux attacks and DNS

DNS protocol vulnerabilities

DNS response modification

Today's topics

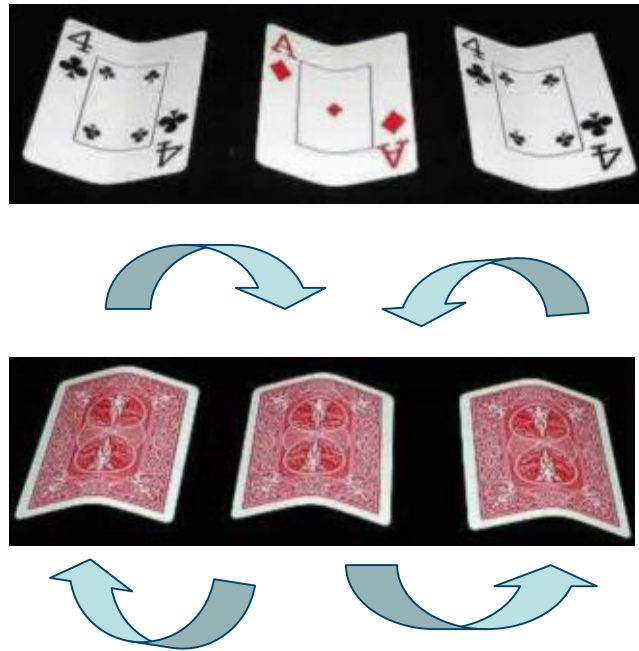
For complete list, visit <http://www.icann.org/committees/security>

What is Fast Flux Hosting?

- An evasion technique
- Goal of all fast flux variants
 - Avoid detection and take down of web sites used for illegal purposes
- Technique
 - Host illegal content at many web sites
 - Send phishing email with links to web site's domain name
 - Rapidly change the locations of the web site so that no one site is used long enough to isolate and shut down

e-version of age-old scam

- 3 card monte, a classic street corner scam



Bet on which card is the Ace of Diamonds!

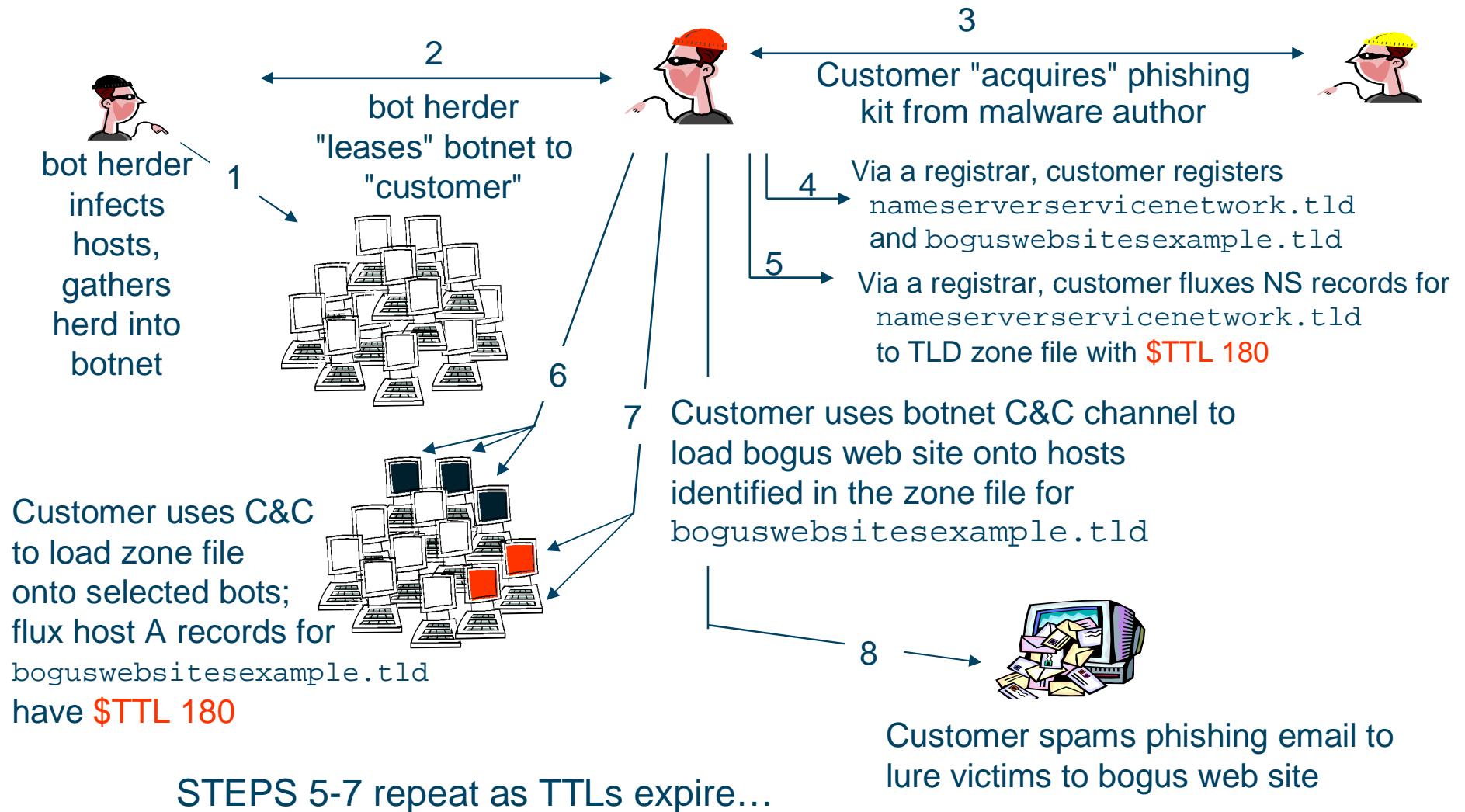
In *basic* fast flux attacks, the web site
is the Ace of Diamonds

Eluding the beat cop

- In the brick-and-mortar world, 3 card Monte is run on a street corner
- Lookouts warn the scam artist when the beat cop is approaching
- The scam artist packs up his game and moved to another corner
- In the e-world, scammers alter the DNS to "change corners"
 - This is called **Name Server Fluxing**
 - **Double flux** combines basic and name server fluxing



Anatomy of one form of fast flux attack



Can we shut down the bots?

- Bots number in the 100,000s or 1Ms



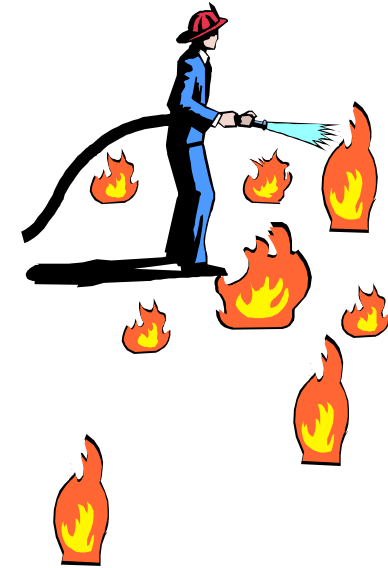
- Current mitigation techniques

- Anti-malware on desktops and at gateways
- Education and awareness
- Current efforts not close to stemming the tide



- Possible additional techniques include

- Process and executable white listing
- Network access/admission controls for private networks and public Internet service
- Inclusion of bot detection in “unified threat management” security



Can we shut down fast flux hosts?

- Today,
 - Responders and law enforcement collect information (and obtain court orders) to shut down fast flux hosts
 - The shut down process operates at a real world pace
 - Fast flux is designed to thwart these activities
 - Fast flux hosts remain operational well beyond the average illegal site lifetime of 4 days
- Possible additional measures
 - Accelerated domain name suspension procedures
 - Information sharing among responders, CERTS, LEAs
 - Accredited entities work directly with registrars and registries
 - Make additional data on zone activity available for use in detecting fast flux and other attacks that exploit DNS

Can we remove fast flux domains from service?

- Some domains are easier to delete than others
 - Conventional phishing and spam detection methods apply
- Other domains are **HARD** to take down
 - Illegal sites hosted on legitimate but compromised servers or on bulletproof hosts
- Overly simplistic detection methods may result in false positives
 - Flux hosting attacks are not simply “volatile networks that use NS records with short TTLs ”

Additional practices and study items

- Explicitly prohibit use of domains and hosting services to abet illegal activities in Universal Terms of Service agreements
- Enforce stronger controls over NS record changes
 - Authenticate contacts before allowing NS record changes
 - Require confirmation of or limit NS record changes or whitelist registrants with legitimate uses
 - Detect and block automated NS record changes
- Develop monitoring systems to detect flux activity
 - Combined presence of several factors “fingerprints” flux attacks
 - Multiple IPs per NS spanning multiple ASNs, frequent NS changes, in-addr of IPs lying within consumer broadband allocation blocks, domain name age, poor quality WHOIS, use of nginx to hide/proxy illegal web server are all “markers” of fast flux activity
 - What roles can registries and registrars play in making statistical data available for detection purposes

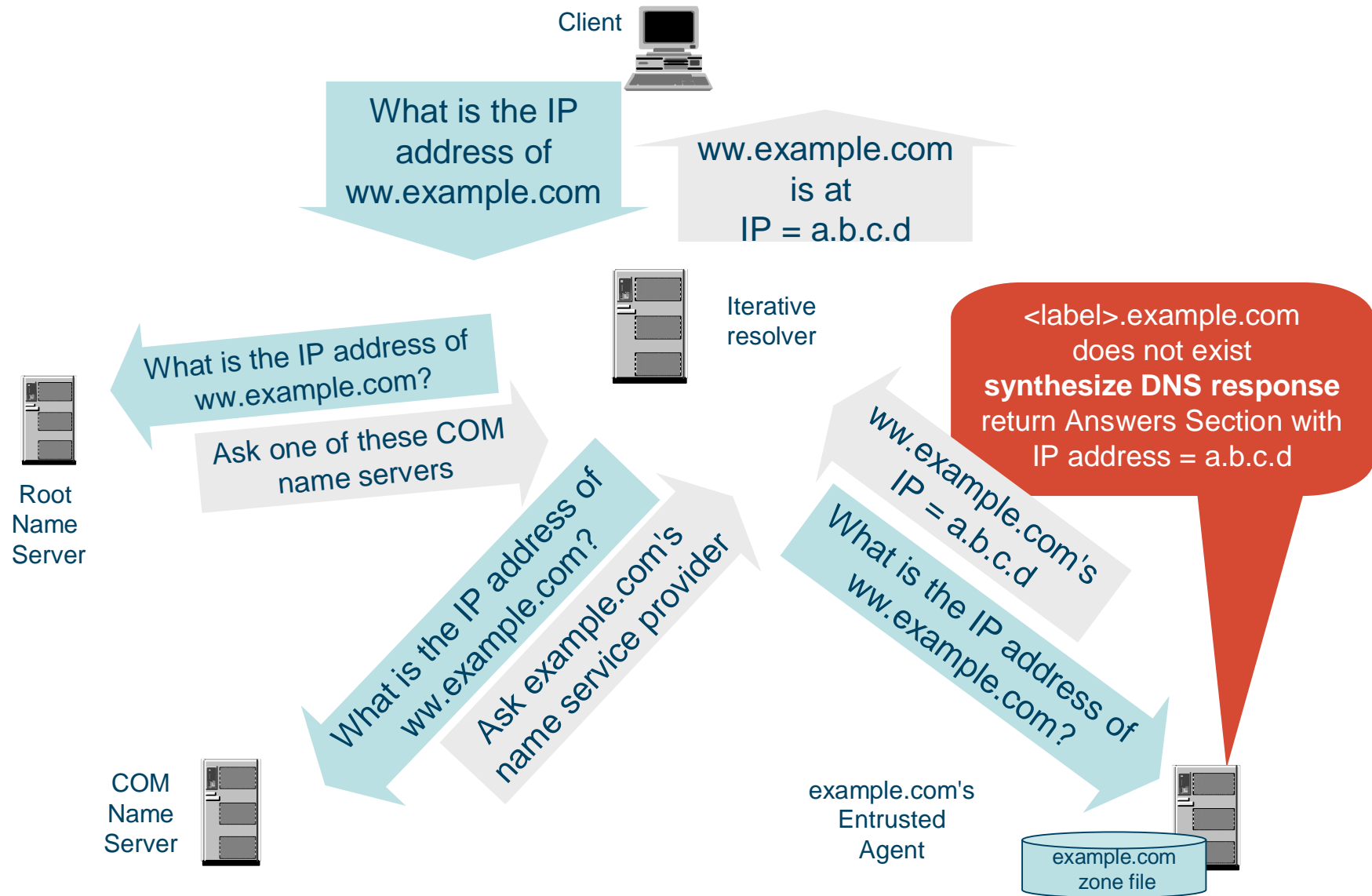
DNS Response Modification

- Practice of altering *NXDomain* DNS responses
 - NXDomain = non-existent domain
 - Same as a Name Error DNS response code
- RFC 1035 says "only meaningful in responses from an *authoritative name server*"
 - The response is **more than an error indication**
 - **It is content** that the authoritative name server expects the client to receive
- This content may be modified by
 - Entrusted Agents (authoritative name service providers)
 - Third parties (any name server that processes the response)
- Often done without notice and consent to user or registrant
 - Even when notice is provided, full disclosure of the security implications are not identified

Form 1: Synthesized DNS response

- An Entrusted agent operating as a zone authority
 - Receives a name query from a client
 - Determines the name does not exist in the zone file
 - Returns a *name exists* response containing an IP address mapping the entrusted agent chooses
 - Common implementation is to include a *wildcard entry* in the registrant's zone file
 - All names not found resolve to an IP address the agent chooses

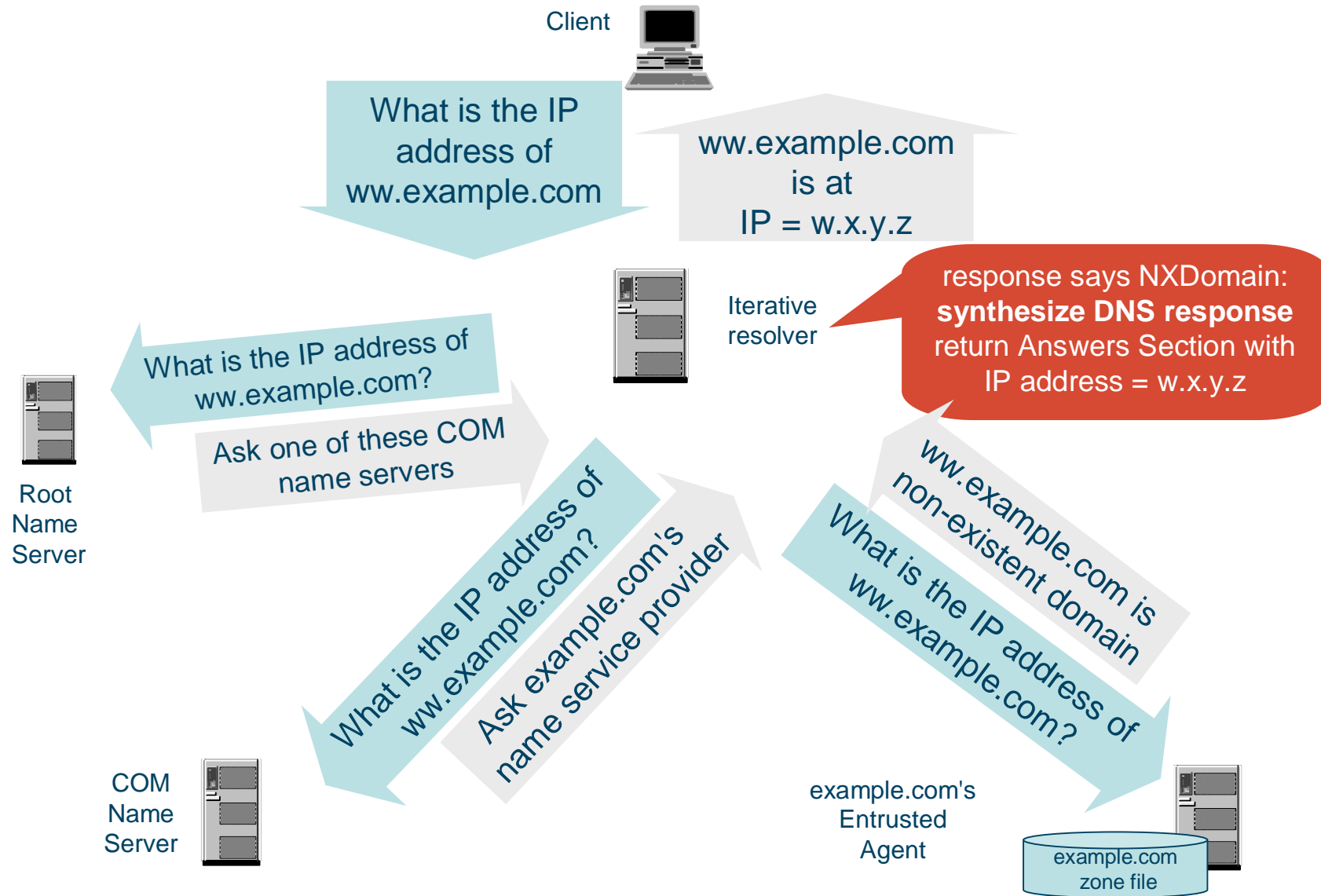
Synthesized DNS Response (Simplified)



Form 2: "On the fly" response modification

- A **third party** NS operator
 - Examines DNS responses messages it attempts to resolve for a client
 - When it encounters a *non-existent domain* response it
 - Silently alters the response code from *non-existent* to *name found*
 - Inserts an IP address mapping the third party chooses

NXDomain Response Modification(Simplified)



Who has the means, motive and opportunity?

Who	How	Why
Sponsoring registrar	Entrusted agent (EA)	Promote business
Public DNS provider	Third party NS operator	Promote services
ISP	Third party NS operator or EA	Advertise
Web (proxy) operators	Third party NS operator	Affiliate advertising
"for fee" DNS provider	Third party NS operator or EA	"Enhance the user experience" 😊
Domain registrant	EA	Enforce a policy Remedial Education
Attackers	"own" a DNS server	Fun, fame, fortune...

How are registrants and users affected?

- A modified DNS response
 - signals a different state of the zone to the user than the operating state
 - alters the content the domain authority intended to have delivered
 - Why should DNS messages be treated differently from mail, IMs or voice?
 - can cause address mapping conflicts when multiple NS operators alter responses
 - can result in inconsistent responses
 - the response a user receives depends on the resolver it asks
 - has business and brand implications
 - Redirection hosts benefit from the domain registrant's brand, reputation, site and link popularity, and sponsored link agreements...

Security Implications

- A modified DNS response
 - subverts a "parent trusts the subdomain" security assumption common to web applications
 - Affects registrant's ability to perform compliance testing and auditing
 - wrests security of hosts from the registrant
 - a host is named in your domain but secured by "someone else"
 - **creates opportunities for attack via a host you cannot secure**
 - Phishing via false site injection
 - Redirect hosts can intercept, monitor and analyze traffic (extract data)
 - Redirect hosts can intercepted cookies to acquire personal, credit or financial data
 - facilitates attacks against brand
 - 3rd level labels you don't control are as dangerous as 2nd level labels

Other issues

- **A Records today, what about tomorrow?**
 - Assumption is that most NXDomain responses are for web sites so they lead to "eyeballs"
 - Imagine a future of modified DNS responses that includes MX, NAPTR, SRV and other resource records
- **Dueling rewrites**
 - DNS responses can be processed by many third parties
 - Any party downstream from a synthesized response can rewrite the response
 - Interesting problem for error resolution marketers
- **Is this the tip of the iceberg?**
 - How long before responses from other application servers are "in play"?

SSAC Recommendations

- Synthesized responses at any level in the DNS has unanticipated consequences
- Registrants should choose an entrusted agent that asserts it will not modify DNS responses in its terms of service
- Registrants should study ways to provide end-to-end authenticated proof of non-existence of subdomains (DNSSEC)
- Entrusted agents should not inject DNS wildcards in a zone without informed consent and without fully informing the domain registrant of the risks this practices exposes
- Entrusted agents should provide opt-out mechanism that allows clients to receive the original DNS answers to their queries.
- Third parties should disclose that they practice NXDomain response modification and should provide opportunities for users to opt out