Attacks Against The DNS

Dave Piscitello
VP Security and ICT Coordination
27 June 2016
dave.piscitello@icann.org

Introduction

- VP Security and ICT Coordination, ICANN
- 40 year network and security practitioner
- Roles at ICANN:
  - Technology Advisor
  - Threat responder
  - Investigator
  - Researcher

Part 1

- How does the DNS work?
- Overview and Examples of the DNS attack landscape

What Is The Domain Name System?

A distributed database primarily used to obtain

the IP address, a number, e.g.,

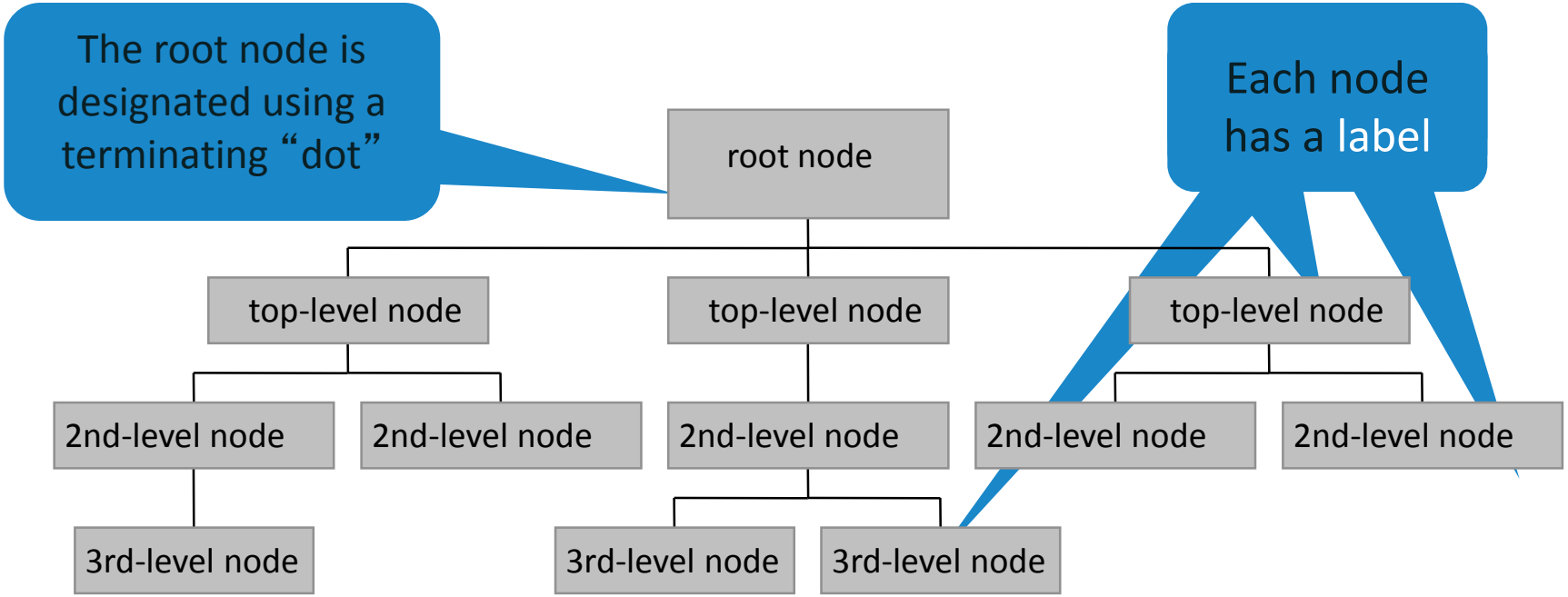
192.168.23.1 or fe80::226:bbff:fe11:5b32

that is associated with a

user-friendly name (www.example.com)

Structure Of The Distributed DNS Database

The formal structure of the DNS database is an inverted tree with the root node at the top

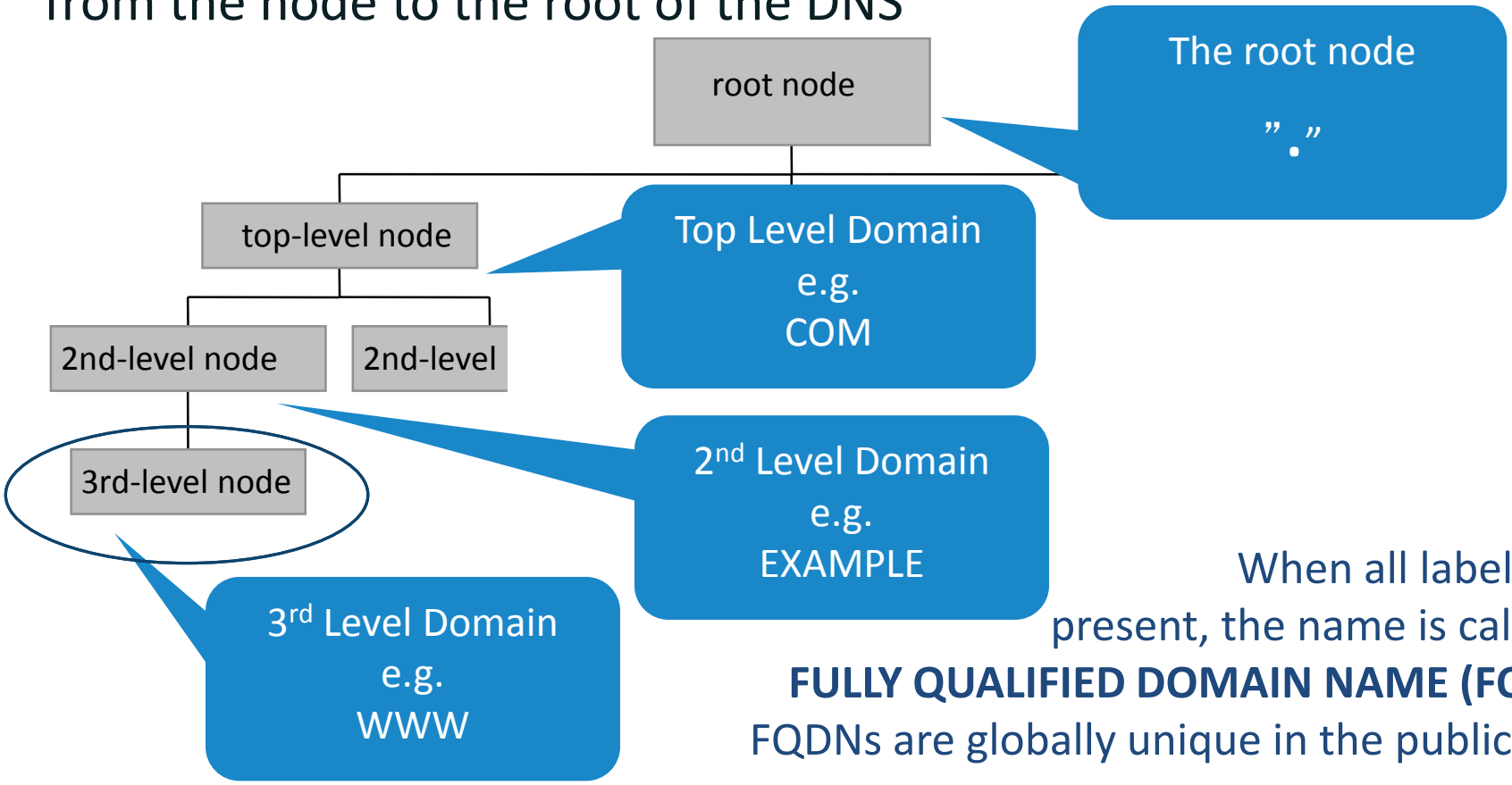


The DNS is *a* public name space.
It is one of *many* name spaces used on the Internet.

Labels And Domain Names

Each node in the DNS name space has a label

The domain name of a node is a *list* of the labels on the path from the node to the root of the DNS



When all labels are present, the name is called a **FULLY QUALIFIED DOMAIN NAME (FQDN)**

FQDNs are globally unique in the public DNS

Operational Elements Of The DNS

- Authoritative Name Servers host zone data
  - The set of “DNS data” that the registrant publishes
- Recursive Name Resolvers (“resolvers”)
  - Systems that find answers to queries for DNS data
- Caching resolvers
  - Recursive resolvers that find and store answers locally for “TTL” period of time
- Client or “stub” resolvers
  - Software in applications, mobile apps or operating systems that query the DNS and process responses

DNS: Internet's Directory Assistance

- Client "stub" resolvers ask questions
  - Software in applications, mobile apps or operating systems that issue DNS queries and process responses
- Recursive name resolvers find answers to queries for DNS data

My PC

What is the IPv6 address for www.icann.org?

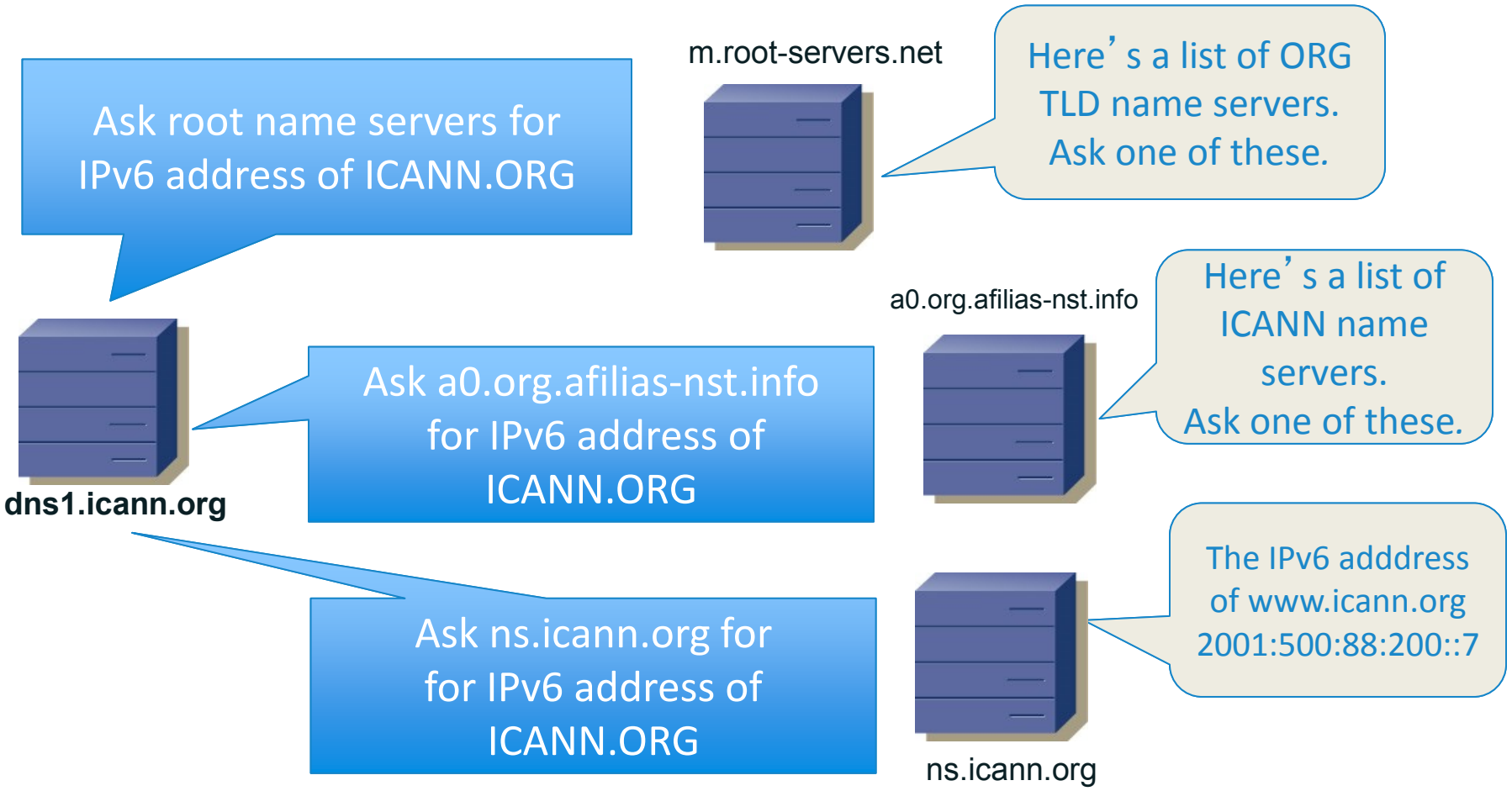
dns1.icann.org

I'll find that answer for you

The Domain Name System Is "Directory Assistance"

How does a resolver find the IP address of ICANN.ORG?

- Resolvers find answers by asking questions *iteratively*



What Is Caching?

- Resolvers may *cache* DNS records they receive from other name servers as they process client queries
  - Speeds up resolution
  - Saves bandwidth
  - Responses are **non-authoritative**
- Are cached records valid forever?
  - No. The time to live (TTL) field in DNS records bounds how long an iterative resolver can cache that particular record

What is the IPv6 address of www.icann.org

I'll cache this response

www.icann.org
AAAA 2001:500:88:200::7

Summary

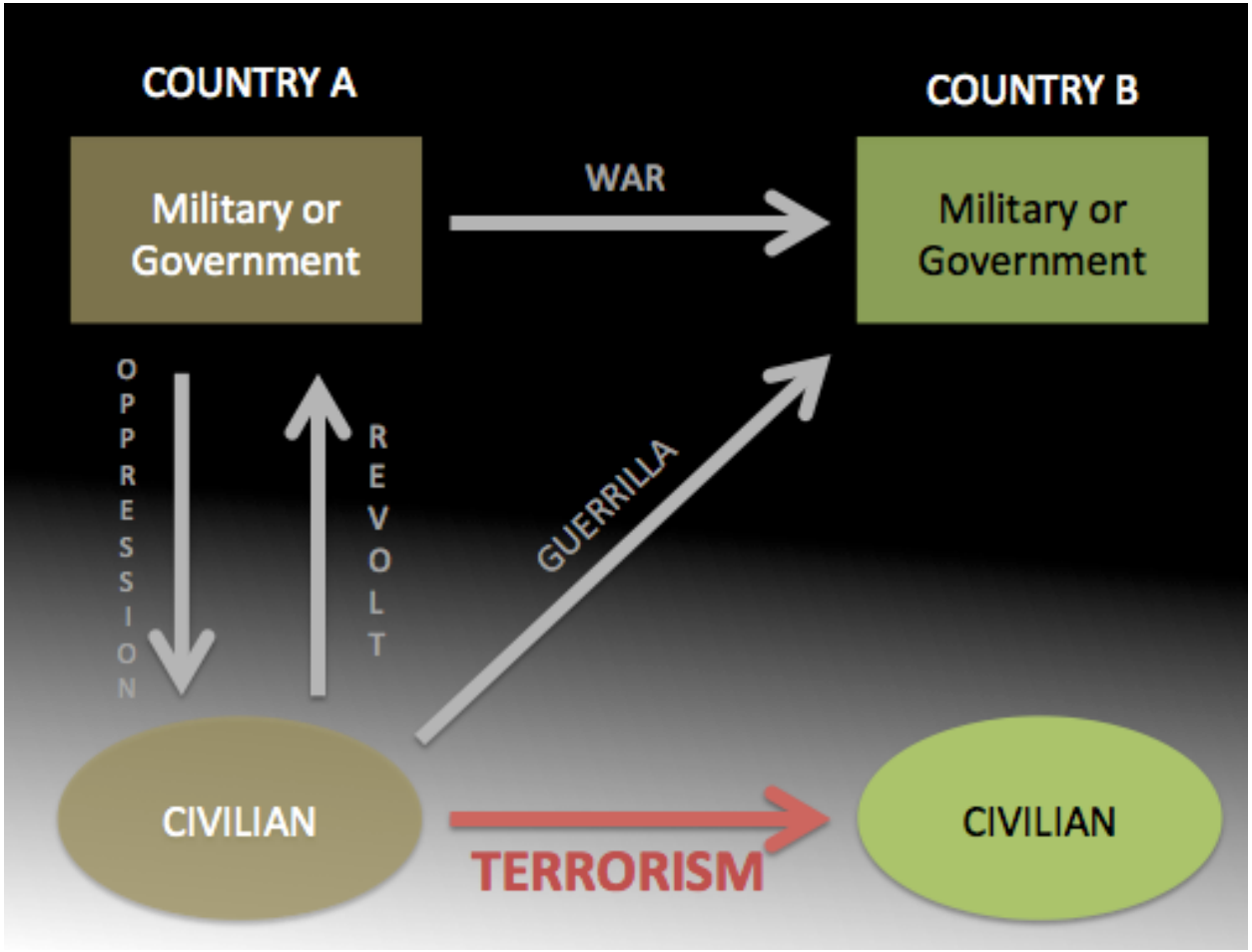
1. The DNS is a public, distributed database
2. The DNS allows us to use names rather than numbers to navigate the Internet
3. The operational elements of the DNS span from critical infrastructure to user devices

Agenda

- How does the DNS work?
- Attacking the DNS

Motives To Attack Or Exploit The DNS

Actors have specific motives or incentives to attack critical cyber infrastructures, including DNS



Where are cybercrime and espionage in this diagram?

DNS Attack Landscape

Target	Authoritative Name Server	Recursive Resolver	Stub Resolver
Access bandwidth	✓	✓	✓
Access network elements	✓	✓	✓
NS or device:			
Hardware	✓	✓	✓
OS software	✓	✓	✓
Name server software	✓	✓	
Cache		✓	✓
Application software			✓
Administration	✓	✓	✓
Configuration	✓	✓	✓

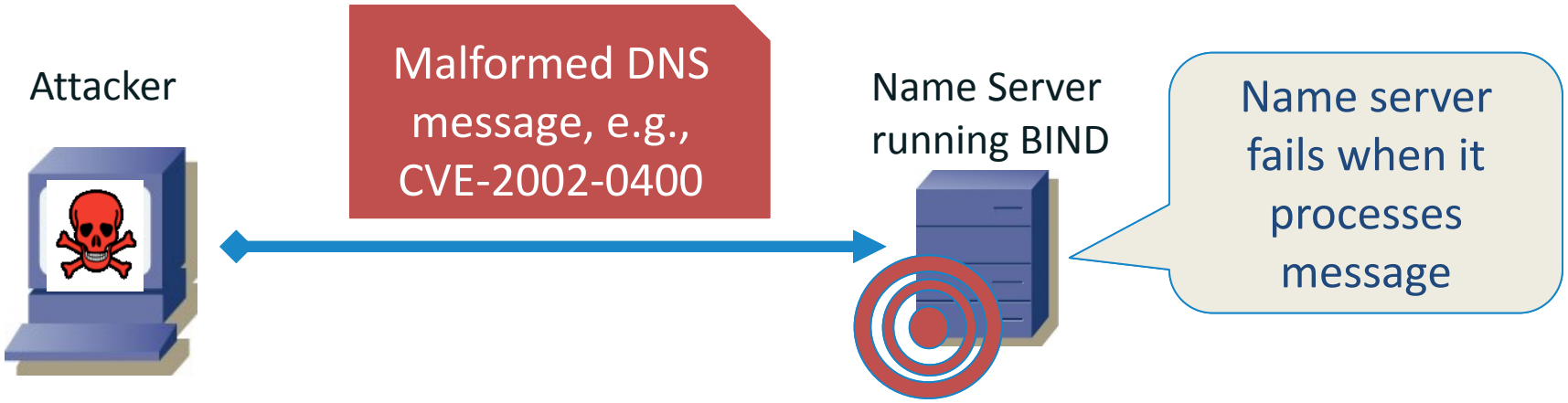
Attacks Against Name Servers Or Recursors

- “Exploit to fail” Denial of Service (DOS) attack
- “Exploit to own” DOS attack
- Reflection attack
- Amplification attack
- Distributed DOS attack
- Cache Poisoning attack
- Exhaustion attack

Let’s look at some examples

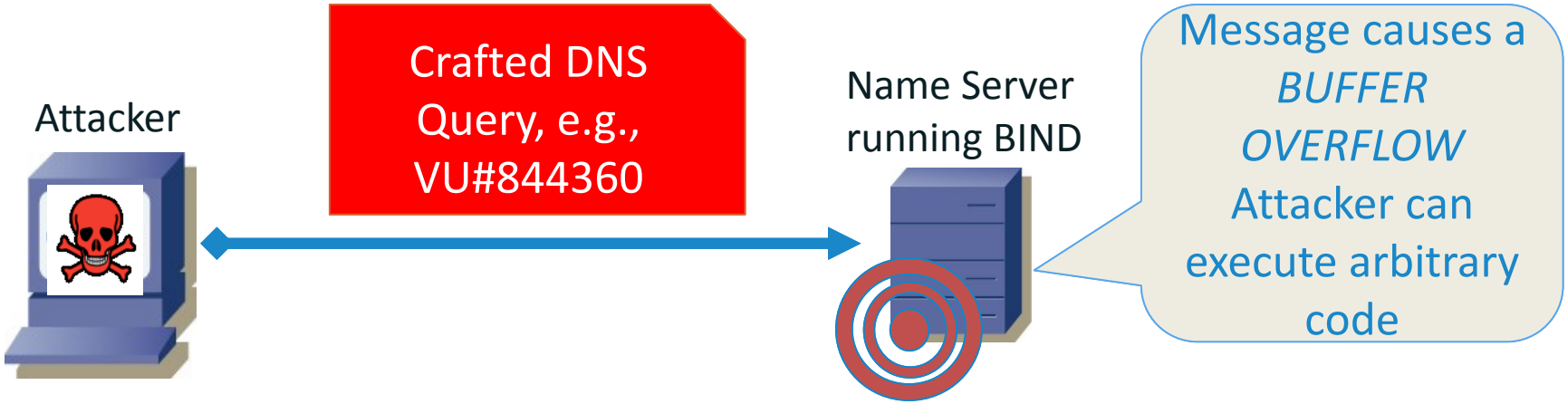
“Exploit To Fail” DOS Attack

- Exploit a vulnerability in some element of a name server infrastructure to cause interruption of name resolution service
- Example: Malicious DNS message injection
  - http://www.cvedetails.com/cve/CVE-2002-0400/

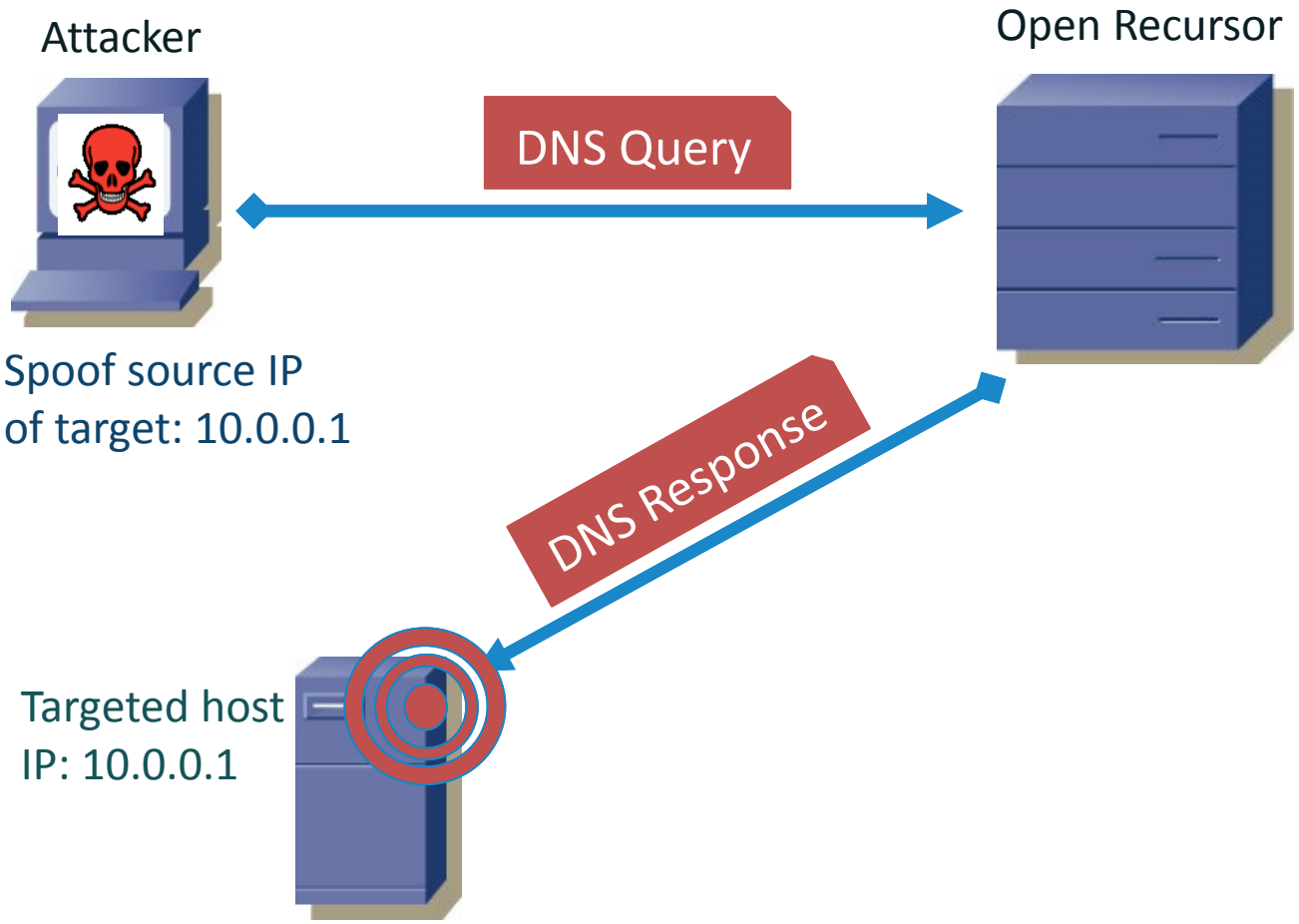


“Exploit To Own” DOS Attack

- Exploit a vulnerability in some element of a name server infrastructure to gain system administrative privileges
- Example: Arbitrary/remote code execution
  - http://www.kb.cert.org/vuls/id/844360

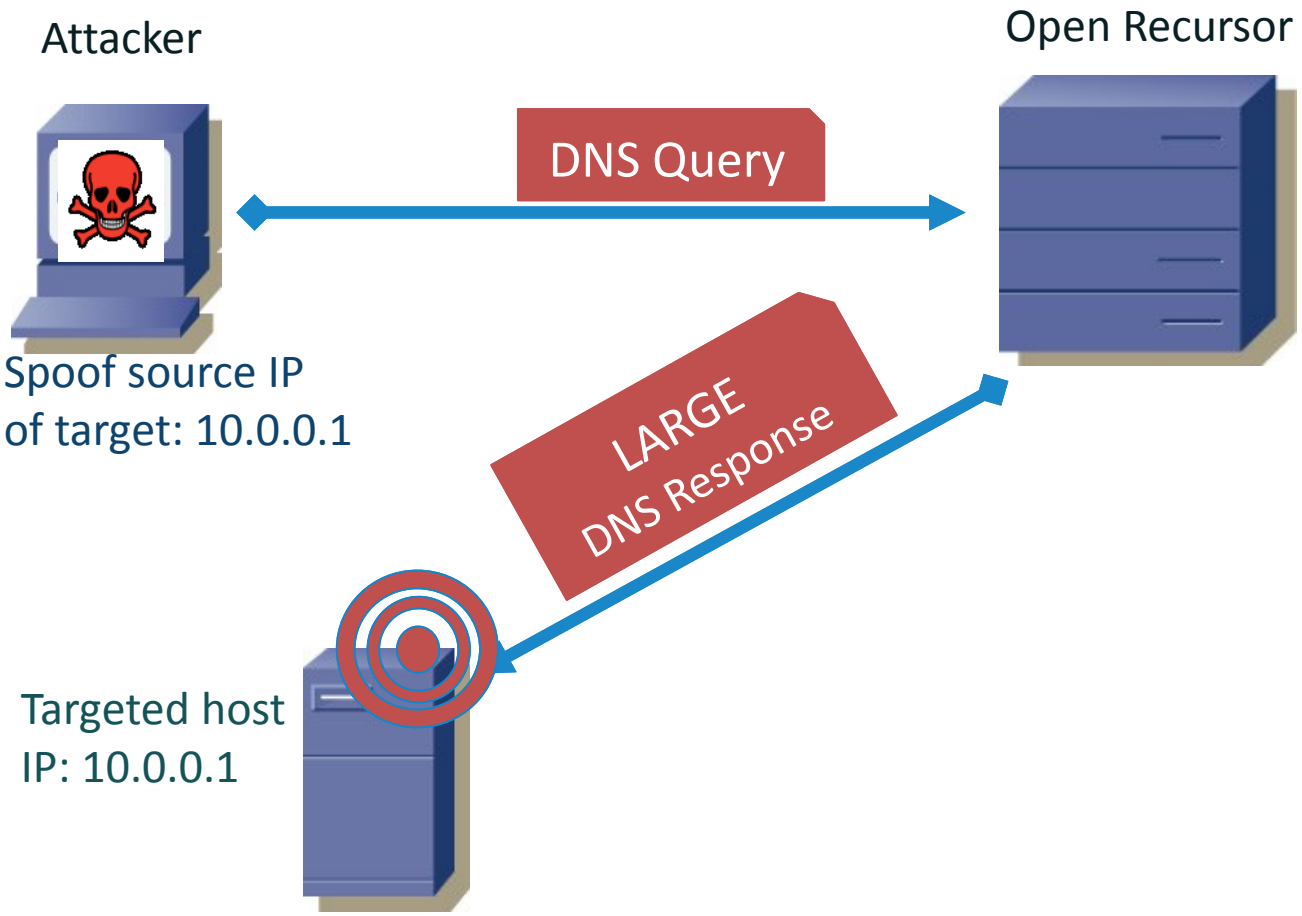


Reflection Attack



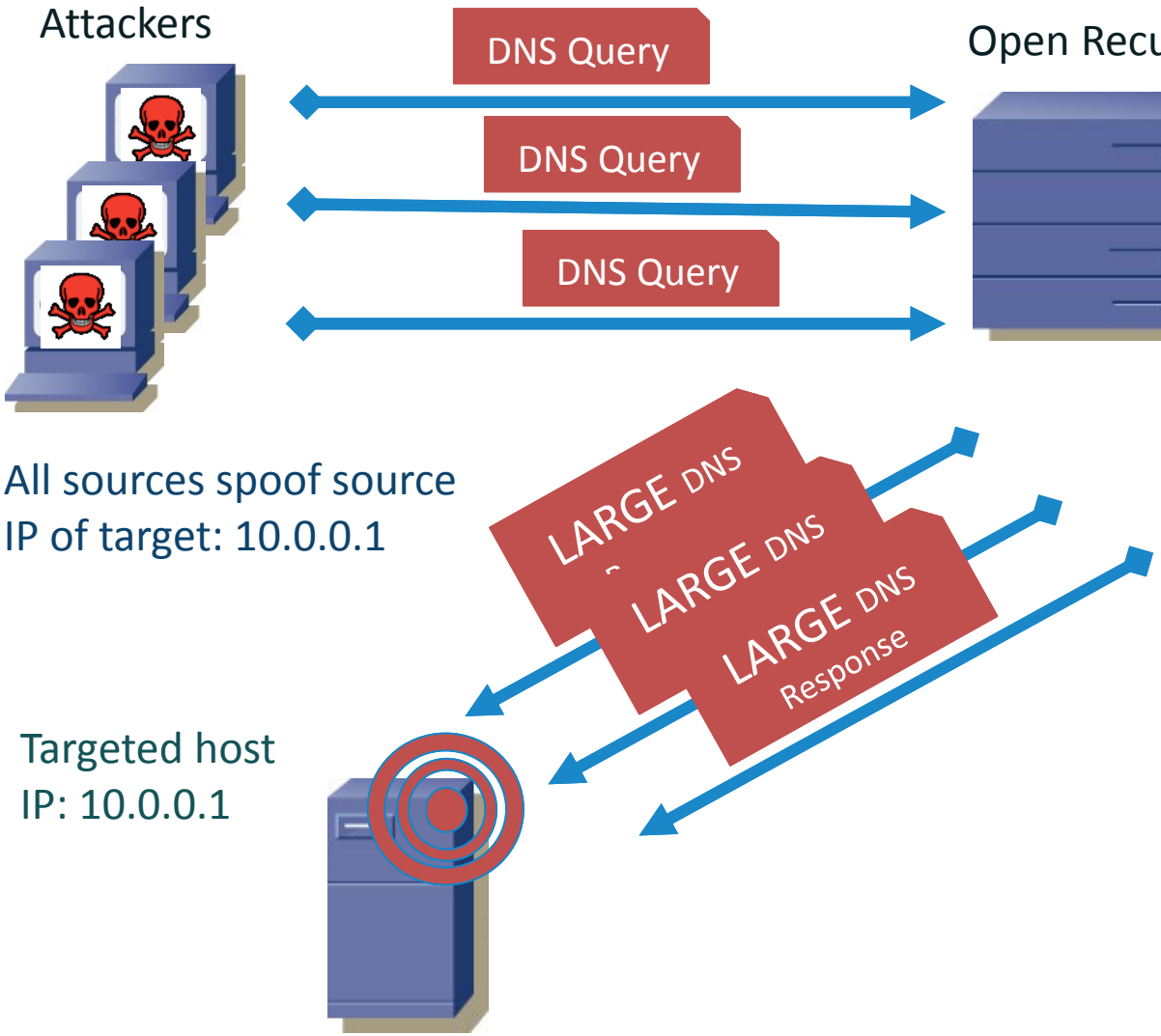
- Attacker spoofs IP address of targeted host
- Attacker sends DNS messages to recursor
- Recursor sends response to targeted host
- Response delivered to targeted host

Reflection And Amplification Attack



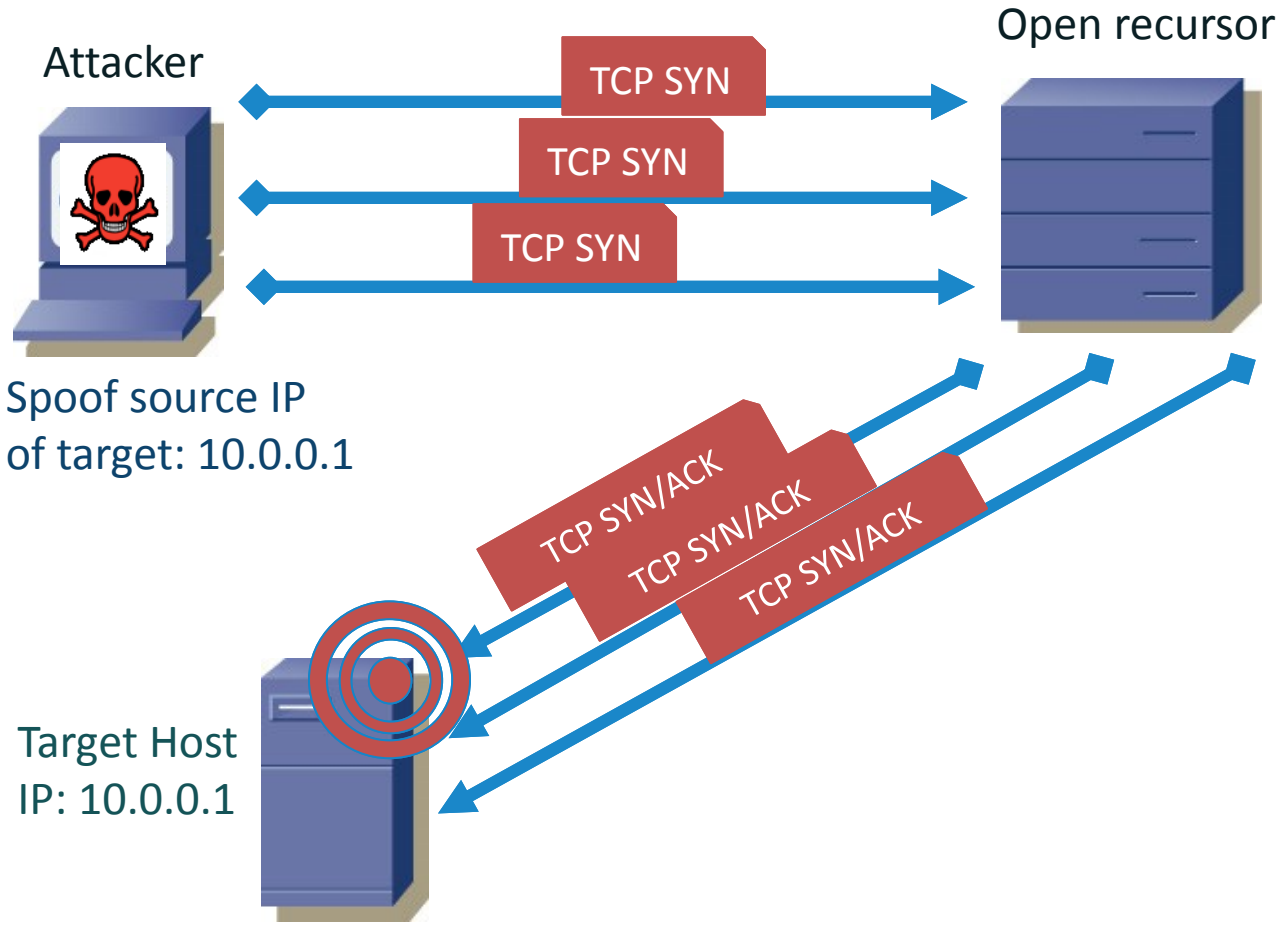
- Attacker spoofs IP address of targeted host
- Attacker sends DNS messages to recursor that elicits a LARGE response
- Recursor sends LARGE responses to targeted host
- The LARGE responses consume target's resources faster

Distributed Reflection And Amplification Attack



- Launch reflection and amplification attack from 1000s of origins
- Reflect through open recursors
- Deliver 1000s of large responses to target

Resource Depletion DOS Attack



- Attacker sends flood of DNS messages over TCP from spoofed IP address of target
- Name server allocates resources for connections until resources are exhausted
- Name resolution is degraded or interrupted

Basic Cache Poisoning

Attacker

- Launches a spam campaign where spam message contains http://loseweightfastnow.com
- Attacker's name server will respond to a DNS query for loseweightnow.com with malicious data about ebay.com
- Vulnerable resolvers add malicious data to local caches
- The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry

My PC

What is the IPv4 address for loseweightfastnow.com

I'll cache this response… and update www.ebay.com

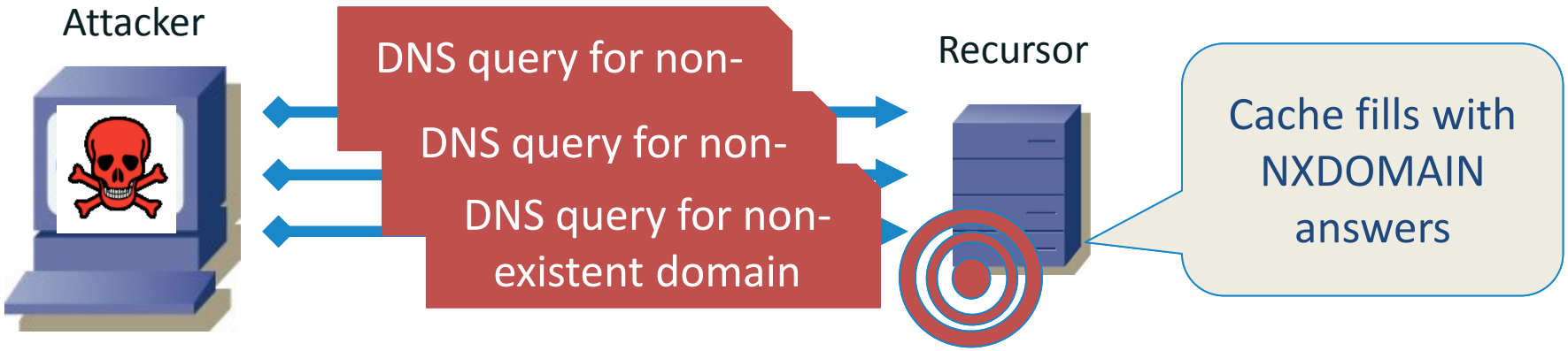
My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1
ALSO *www.ebay.com is at 192.168.1.2*

ecrime name server

NXDOMAIN Cache Exhaustion

- Attacker floods recursor with DNS queries for non-existent domain names
- Recursor attempts to resolve queries and adds each NXDOMAIN answer to cache
- Recursor's cache fills with useless answers
- Processing of legitimate DNS queries is degraded



Phantom Domain Attack has similar effects

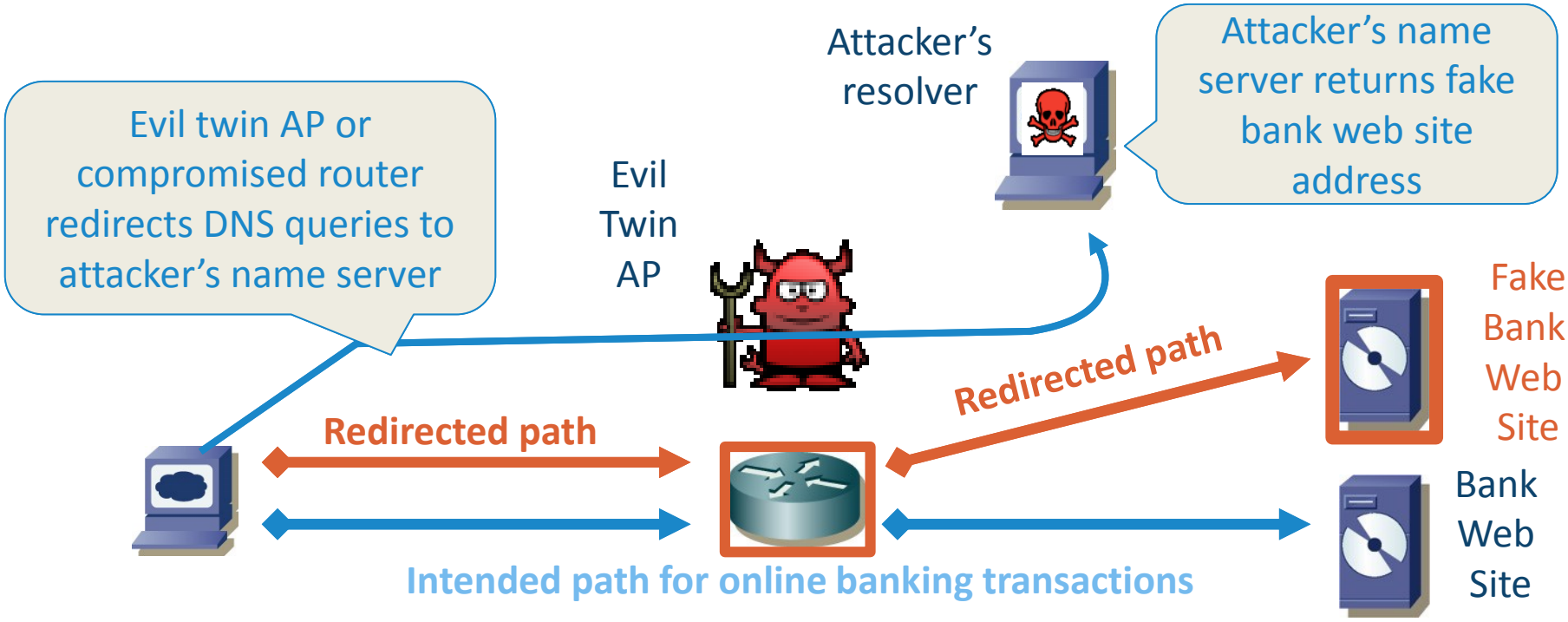
Attacks Against Stub Resolvers

- Query interception attack
- DNS Response modification
  - Also called Name Error resolution
- Configuration poisoning attack
- DNS hostname overflow attack

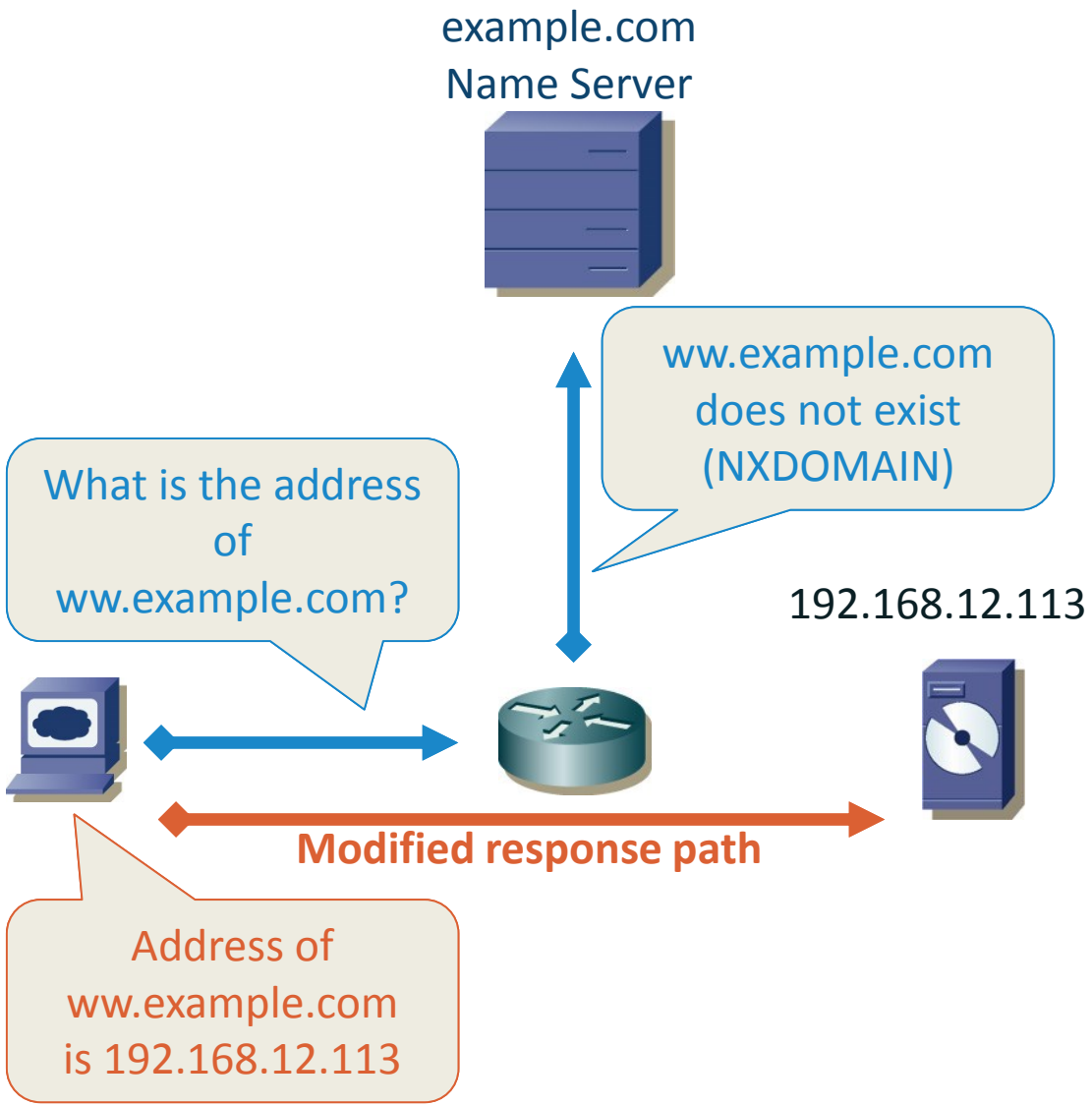
Let's look at some examples

Query Interception (DNS Hijacking)

- A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forge responses
  - Can be done using a DNS proxy, compromised access router or recursor, ARP poisoning, or evil twin Wifi access point



Response Modification



- Recursive resolver is configured to return IP address of web, pay-per-click, or search page when it receives NXDOMAIN response
- Also used by ISPs and 3rd parties for monetizing purposes

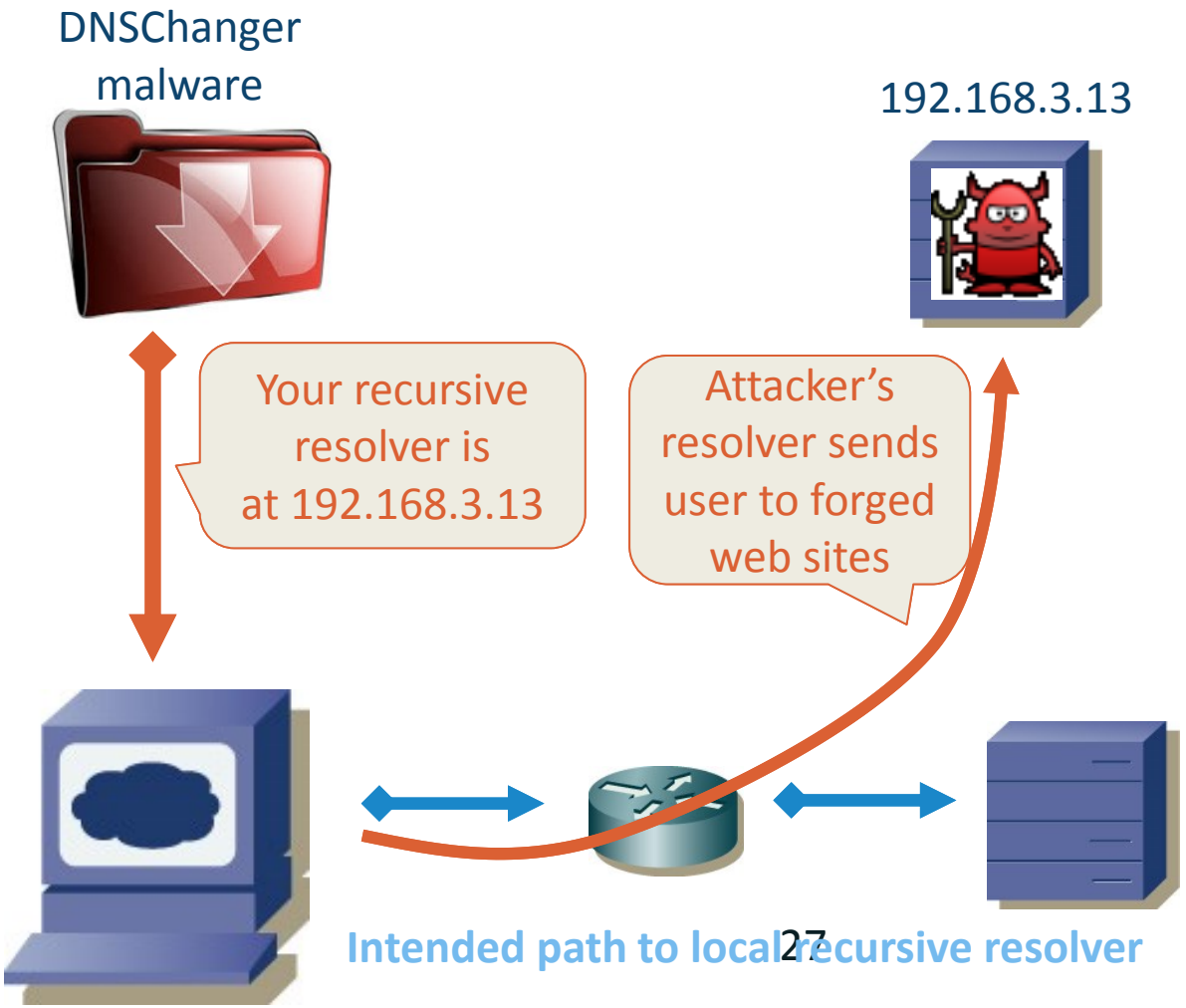
Configuration Poisoning: DNSChanger

Attacker distributes DNS configuration altering malware via

- Spam, drive-by download…

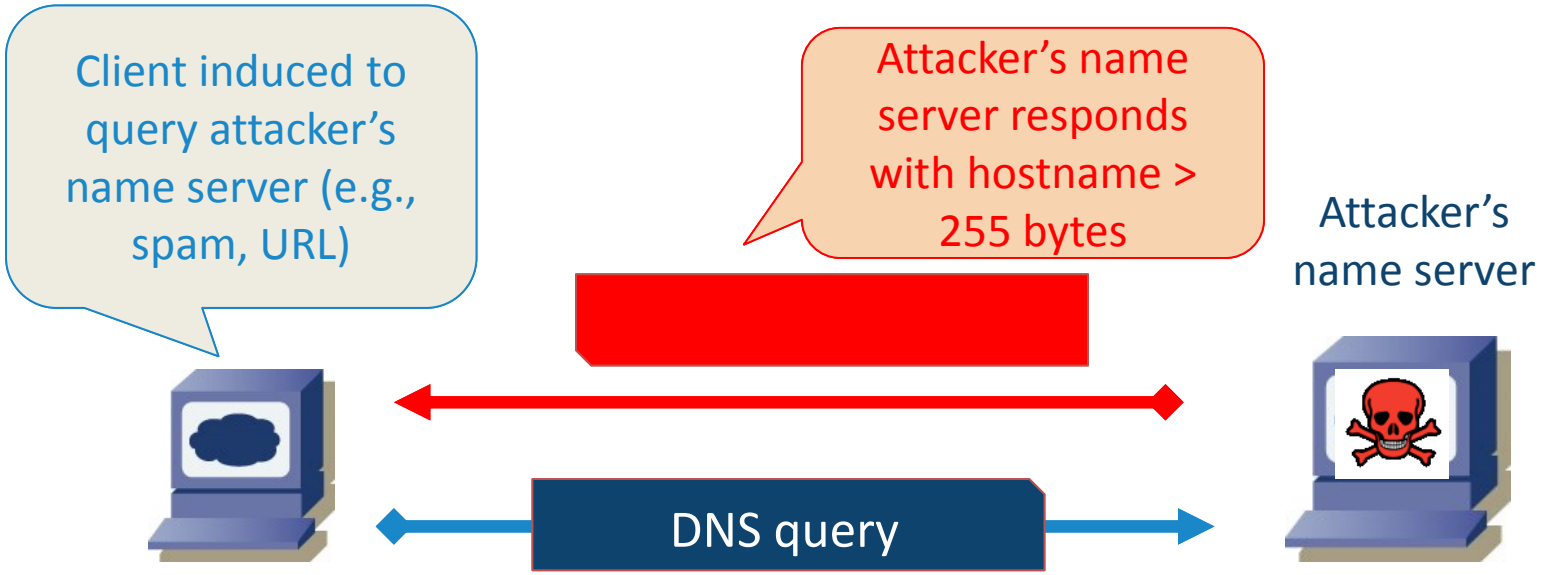
DNSChanger malware

- Alters DNS configuration of infected PC
- Causes all requests to go to a malicious name server run by attackers
- Attacker updates malware to redirect web traffic to a destination of his choosing



DNS Hostname Overflow Attack

- Attacker crafts response message containing domain name > 255 bytes
- *Vulnerable* client queries attacker's name server, fails to check hostname length in response
- Buffer overflow allows a attacker to gain root or execute arbitrary commands



Domain Registration Hijacking

- Attacker compromises registration account, e.g.,
  - Succeeds with brute force, social engineering, or login attack
  - Launches a *registrar impersonation phishing attack*
  - Compromise gives attacker administrative control over domains registered under this account
- Attacker modifies/adds name server record for domain
  - NS record that is published in TLD zone associates domain's name server with IP address of attacker's host
- Attacker publishes "attack" zone data
  - Resource records in zone data support phishing, fraud, or defacement sites, spam mail exchanges, VoIP servers…

Note: An attacker can also compromise a name server directly

Summary

1. The DNS is an open system and *open also to abuse*
2. The DNS is a critical Internet database and thus a *target* for attack
3. Any element of the DNS may be *exploited* to facilitate other attacks

Reading List (Partial)

Title	URL
Top 10 DNS attacks	http://www.networkworld.com/article/2886283/security0/top-10-dns-attacks-likely-to-infiltrate-your-network.html
Manage your domain portfolio	http://securityskeptic.typepad.com/the-security-skeptic/2014/01/avoid-risks-manage-your-domain-portfolio.html
Securing open DNS resolvers	http://www.gtri.com/securing-open-dns-resolvers-against-denial-of-service-attacks/
DNS Tunneling	https://www.cloudmark.com/releases/docs/whitepapers/dns-tunneling-v01.pdf
DNS cache busting	http://blog.cloudmark.com/2014/10/07/a-dns-cache-busting-technique-for-ddos-style-attacks-against-authoritative-name-servers/
DNS Cache Poisoning	http://www.securityskeptic.com/dns-cache-poisoning.html
Anatomy of a DDOS attack	http://www.securityskeptic.com/anatomy-of-dns-ddos-attack.html
DNS reflection defense	https://blogs.akamai.com/2013/06/dns-reflection-defense.html
Protect the world from your network	http://securityskeptic.typepad.com/the-security-skeptic/2013/04/protecting-the-world-from-your-network.html
DNS Traffic Monitoring Series	http://www.securityskeptic.com/2014/09/dns-traffic-monitoring-series-at-dark-reading.html
Protect your DNS servers against DDoS attacks	http://www.gtcomm.net/blog/protecting-your-dns-server-against-ddos-attacks/
Fast Flux Botnet Detection in Realtime	http://www.iis.sinica.edu.tw/~swc/pub/fast_flux_bot_detection.html
DNS resource exhaustion	https://www.cloudmark.com/releases/docs/whitepapers/dns-resource-exhaustion-v01.pdf

Questions?

My Contact Info:

dave.piscitello@icann.org
@securityskeptic
www.securityskeptic.com
about.me/davepiscitello

Contact ICANN:

engagement@icann.org
@icann
icann.org
safe.mn/icannsecurityteam