DNS Abuse

What is abuse of the DNS

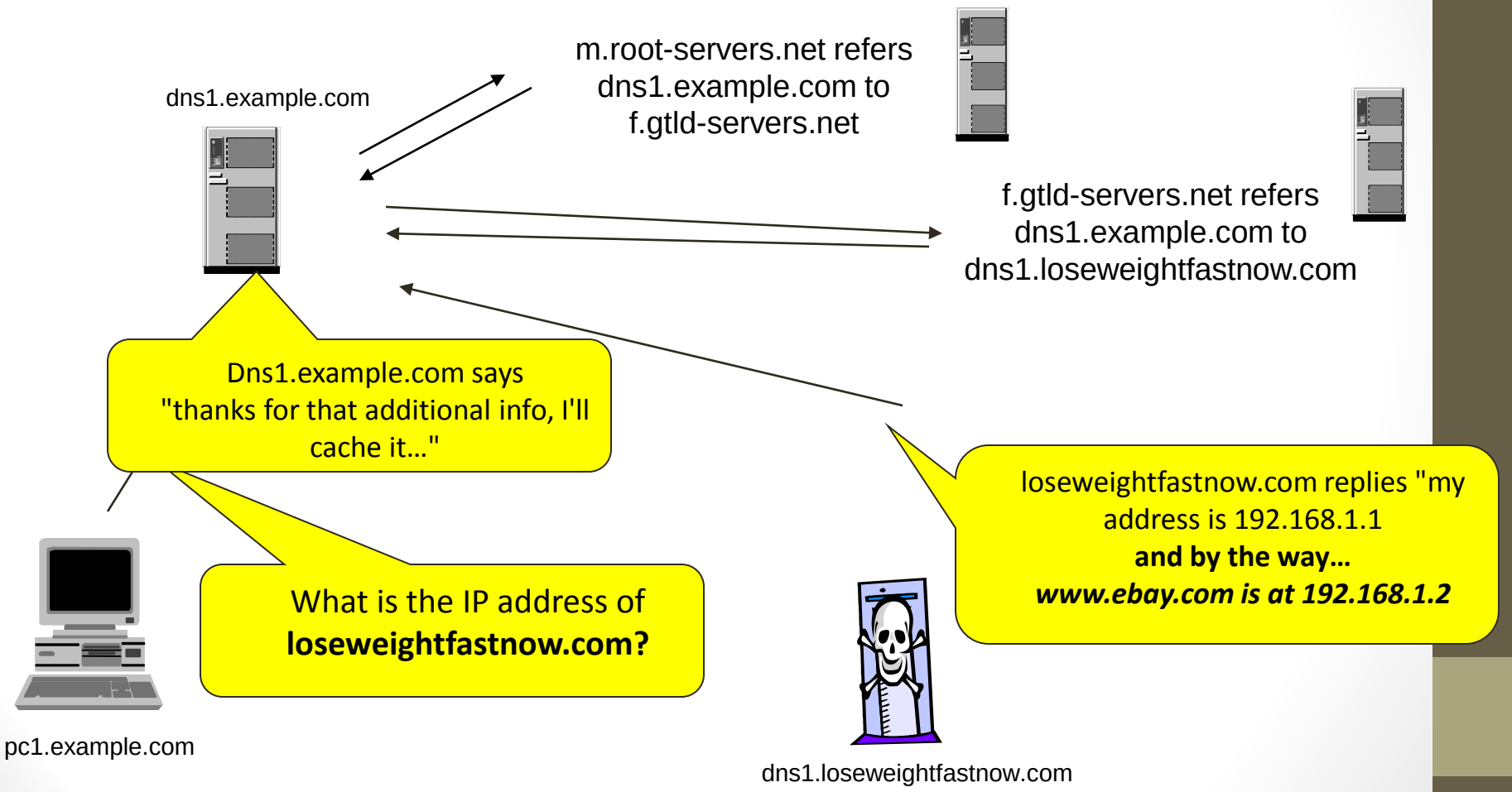
- There is no one clear definition
- I tend to focus on actions that are intended to disrupt or corrupt the process of answering DNS queries.
  - Cache poisoning, use of DNS infrastructure for DDoS
- Some include anything that uses the DNS for “malicious” purposes..
  - Phishing, Pharma

How can bad guys attack DNS?

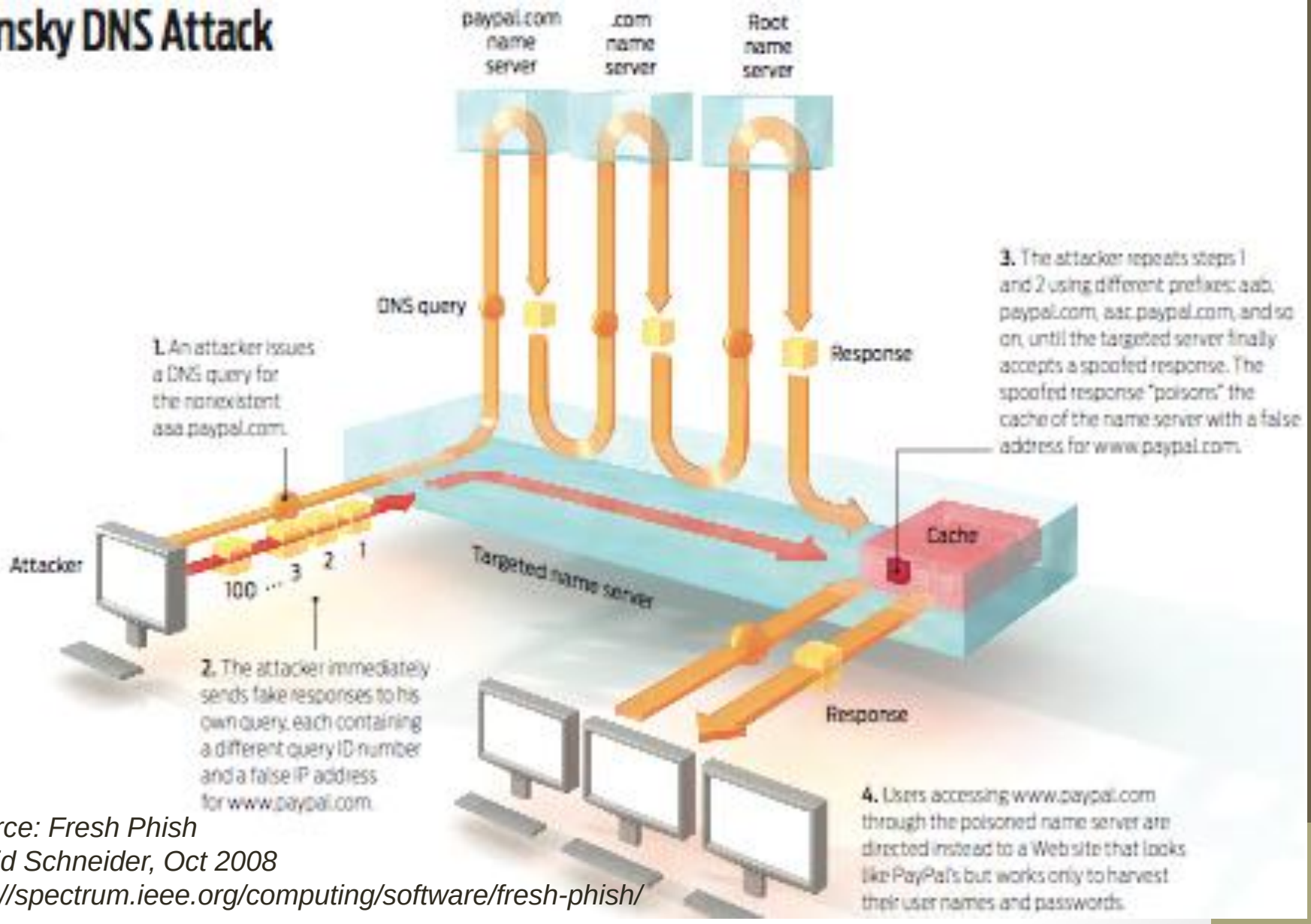
- Cache Poisoning
  - Exploit a configuration error to trick a name server into adding or modifying cached DNS data with incorrect and malicious data
- Pharming
  - Another form of DNS poisoning
  - Malicious code masquerades as a name server and returns bogus responses
  - Malicious code may also poison a client computer's /etc/hosts file

How to poison a cache (Basic)

The user at pc1.example.com clicks on a URL in an email message from loseweightfastnow.com



Kaminsky DNS Attack

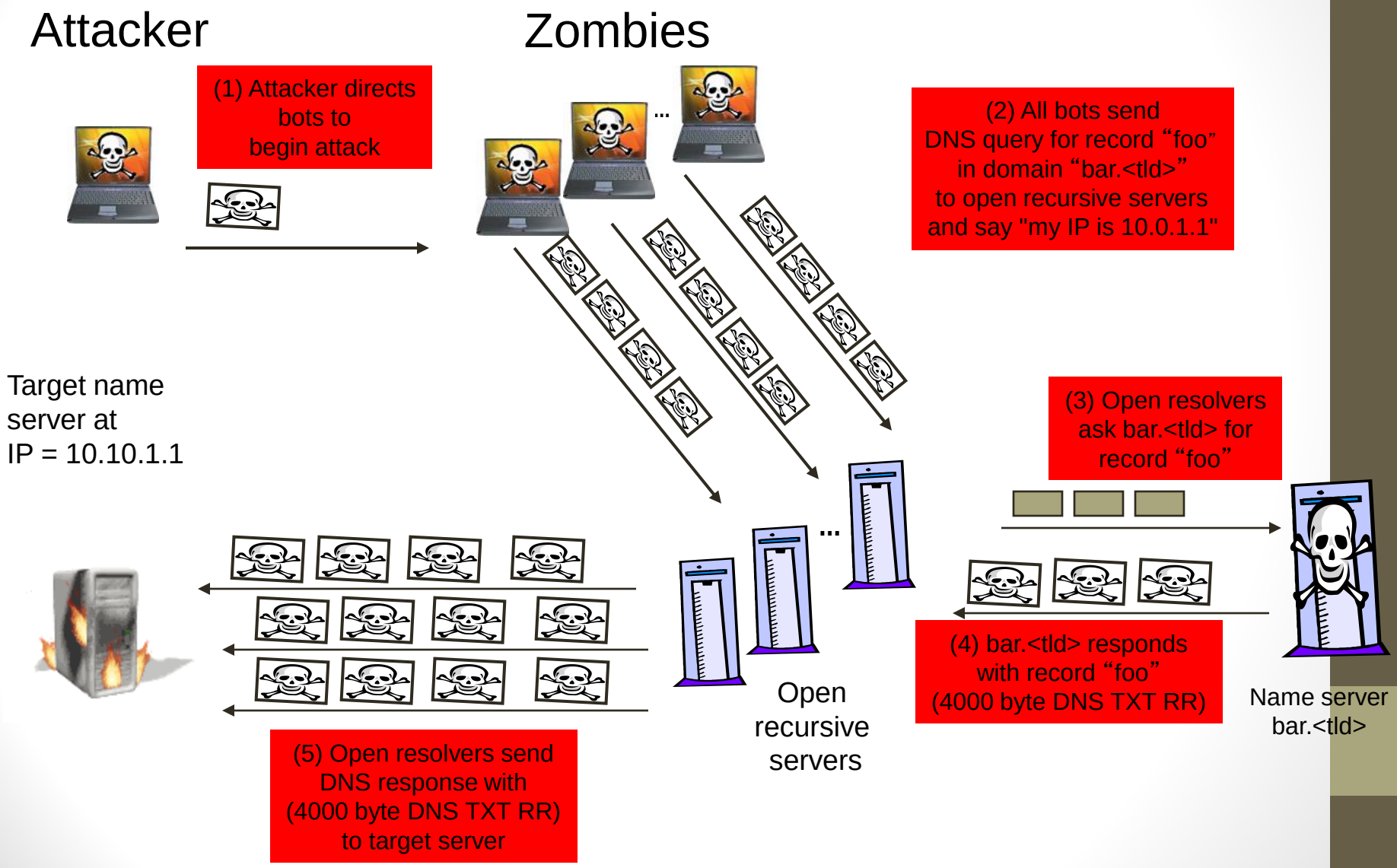


Source: Fresh Phish
David Schneider, Oct 2008
http://spectrum.ieee.org/computing/software/fresh-phish/

Any other attacks on DNS?

- Exploitation attacks
  - When someone discovers a software flaw that causes
  - DNS server software to fail or behave in an unintended
  - way
- Resource depletion attacks
  - Distributed Denial of service (DoS) attack
    - Thousands of compromised computers flood a targeted name server with queries (*flooding)*
  - DDoS amplification attack
    - A DDoS attack in which the queries from thousands of compromised computers "spoof" the IP address of a targeted name server, and the targeted name server receives the very large DNS response message requested by the compromised computers

Anatomy of the Amplification Attack



More?

- DNS zone transfer attack
  - Another DoS attack, where the attacker floods a name server with queries for all the domain data in a zone
- "Double flux" fast flux hosting
  - Attacker makes rapid changes to IP addresses of name servers for a domain used to host illegal or malicious web sites
- DNS wildcarding (redirection), DNS response rewriting
  - Instead of a *Name Error* (NXDOMAIN), a name server or resolver returns a response it chooses

DNS Changing Viruses

A series of viruses exist that change the DNS settings for the infected machines and/or their home routers. Allowing redirection to …. Anywhere they want ☹

In the case of DNS Changer it altered searches and promoted “fake and dangerous” products.

See http://www.dcwg.org/ for details of DNS Changer

Attacks against domain name registration services

- Domain name hijacking
  - Steal a registered name from the rightful registrant
- Typosquatting
  - Registering visually similar or common mistype domain names (Dup0nt,com, Verizom,…) to host pay per click advertising or malicious reason
- Domain name front running
  - Use "insider information" to register a name before the interested party attempts to register it

More?

- Domain name kiting
  - Register a domain name, return it during the add grace period, then register it again, to avoid paying the registration fee
- Domain name sniping
  - Registering a domain name when a registration "at the immediate moment of registration expiry”
- Registrar impersonation
  - A phishing attack where the phish email appears to be from a registrar

Summary

- The DNS is open and thus *open to abuse*
- Registration of names is also open to abuse

- **Being aware of the threats is always a good step!**

- Go read about a kid from my town:
- http://www.wired.com/gadgetlab/2012/09/cosmo-the-god-who-fell-to-earth/all/