DNS Security Risks

Section 0x02

Joke/Cool thing

- traceroute 216.81.59.173

- https://www.youtube.com/watch?v=5_dRqPLP1dc

DNS Overview (Basics)

- World's largest distributed database (maybe?)
- Maintains name <-> address relationship on the Internet
- Critical component of the Internet

DNS Overview (Data Flow)

- Client tries to resolve a name
- Asks the next level ("zone") up
  - If the next highest zone knows, it answers
  - If not, it asks the next highest zone
  - Each zone has an authoritative server responsible for answering these requests

Potential Attacks

- **Why** might we want to exploit DNS requests?
- **How** might we exploit DNS requests?

Simple Attacks

- Typosquatting
- Denial of Service
- Registrar Hacking

Typosquatting

- Register an address that's very similar to a well-known, legitimate one
  - Examples: www.goggle.com, www.yaho.com, www.whitehouse.com
- Occasionally used for phishing attacks
  - Usually just for ad views or financial squatting

Denial of Service

- Hosts must query DNS servers to find the IP addresses mapped to by unknown hostnames
- Overloading these servers can cause them to be unable to respond to requests
- Root DNS servers are the prime targets of attacks
- Can make it impossible to connect to web servers without knowing their IP address

Registrar Hacking

- Domain name-to-IP mappings are registered with a number of companies
- These companies' name servers supply IP information about their managed domains
- If these servers are hacked, traffic can be redirected
- Happened to www.nytimes.com in August 2013
  - Melbourne IT registrar was hacked by the Syrian Electronic Army (with valid user credentials) and IP addresses were changed

Complex Attacks

- Rogue DNS Servers
- DNS Cache Poisoning

Rogue DNS Servers

- When a system doesn't know a name <-> IP mapping, it goes to the next level up
  - If this next level up is a server controlled by a malicious entity, the response it gets may be wrong!
- Malware can manipulate the IP address that a system accesses to get DNS responses
- Alternatively, a DNS server along the chain may maliciously return incorrect data
  - Packets can be introduced into the flow, even without a proper DNS server in place: this is DNS spoofing!
- Certain ISPs (e.g., Comcast) use this technique as well!
  - Common example: if an uncommon or nonexistent hostname is typed in, the ISP's DNS server may respond with a search page rather than an error
- A.k.a. "DNS hijacking" or "DNS redirection"

DNS Cache Poisoning

- Various DNS servers along the chain serve requests from a local cache (your own system also has a cache)
- This cache is supposed to expire regularly, but should mostly be correct
- By directly or indirectly altering this cache data can cause a trusted nameserver to return incorrect responses

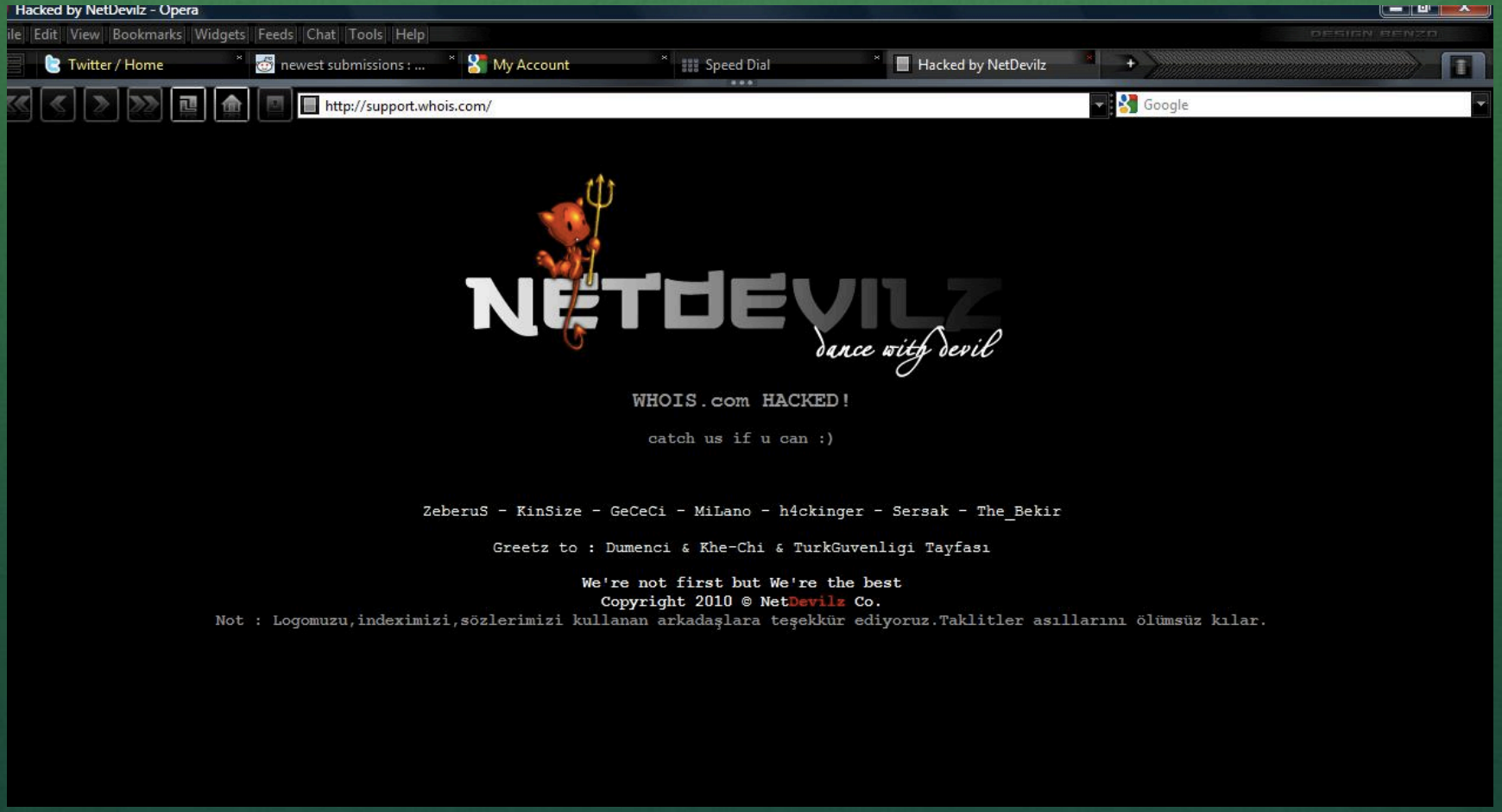
DNS attack story #1

- October 2002 and February 2007 root server attacks
  - DDoS attacks on DNS root servers
  - Peak ~900 Mbps; ~2000 Mbps
  - Only briefly affected performance
  - DNS redundancy, large number of root servers

DNS attack story #2

- ICANN June 2008 attack
  - Internet Corporation for Assigned Names and Numbers
  - Social engineering attack
  - Compromised name servers redirected www.icann.com to hacker-controlled IP address

DNS attack story #2



Possible Solutions

- Typosquatting
  - Buying up typos
  - Trademarking
- Denial of Service
  - Redundancy
  - Selectively blocking traffic
  - Already mostly solved!
- Registrar Hacking
  - Strong passwords
  - Anti-social engineering training

Possible Solutions (cont.)

- Rogue DNS Servers and Cache Poisoning
  - Trusted DNS servers (8.8.8.8, etc.)
    - ISPs may still rewrite certain DNS requests
  - Cryptographic security for requests
  - Digital signatures for data authenticity (secure DNS)
  - Server certificates (to verify that you've reached the right IP address)

www.questions.com ?

- 173.194.79.121