**DNS TTL Values as Potent Allies of DDoS Attackers:**

**A Fact Overlooked by Some Major US and EU Banks**

N. Vlajic, U. T. Nguyen

---

**INTRODUCTION**

**DDoS Attack**
- Concentrated effort to saturate the victim machine (web-server) with a large volume of traffic. Attack traffic is generated by compromised third-party computers, so-called zombies.

**Short-term Goals**
- Prevent the victim server from providing service to regular users

**Long-term Goals**
- Tarnish the image of the victim company and cause major financial loss

**DDoS Defences**
- Almost exclusively concentrated on the victim server and/or the attacker and zombies. Way too often DDoS vulnerabilities involving regular, non-compromised clients/users remain overlooked.

**DDoS and DNS Records**
- DNS Records (DNS TTL times) have an important effect on the operation of web-clients and, if inappropriately managed, can amplify long- and short-term impact of a DDoS attack on a web-site:

**Short-term Impact**
- Increased number of regular users ‘cut-off’ from the web-site over prolonged periods of time

**Long-term Impact**
- Increased number of users that become unsatisfied with the service & ultimately switching to a competitor

---

**DNS TTLs and Web-User Experience**

**DNS Record**
- Generated and managed by Authoritative DNS Server of a company; maps the company’s domain-name to IP address(es) of the company’s web-server(s) (www.XYBank.com ↔ 121.73.49.11)

**DNS TTL Time**
- Controls the ‘lifetime’ of a DNS Record. Once the TTL expires, intermediate DNS servers and end-hosts must discard the Record from their caches and request its new copy.

**Pros of Long DNS TTL Time**
- DNS requests likely served directly from clients’ Caches ⇒ faster web-page download
- Fewer requests sent to Local & Authoritative DNS Servers ⇒ better load balancing

**Cons of Long DNS TTL Time**
- Infrequent updates of clients’ DNS Caches ⇒ problems in case of site failure and/or server migration to new location (IP address)

---

**Empirical Study: DNS-TTLs of Major US and EU Banks**

**Group 1** - 15 best performing US banks according to Forbes.com
- 9 banks use DNS TTL > 60 min
- All 15 banks advertise one single ‘symbolic-name to IP’ mapping - no provisions for server migration / redundancy

**Group 2** - 15 largest US banks (asset-value) according to Forbes.com
- 3 banks use DNS TTL > 60 min
- 9 banks use DNS TTL < 1 min
- 2 banks use multiple ‘symbolic-name to IP’ mappings

**Group 3** - 15 largest EU banks according to BanksDaily.com
- 3 banks use DNS TTL > 60 min
- 4 banks use DNS TTL = 0 min
- 2 banks use multiple ‘symbolic-name to IP’ mappings
- 1 bank use services of Akamai CDN

---

**Client DNS-Cache Lock in Case of DDoS Attack**

**Server Migration / Redundancy**
- Common DDoS Incident Response procedure in which web server gets migrated from the attacked IP address (location) to one or more new IP addresses (locations).

**Client DNS-Cache Lock**
- Users accessing a web site (server) shortly before the onset of a DDoS attack, followed by the server migration, are ‘locked’ by the initially obtained (cached) DNS Record - for up to TTL time units.

**Solution**
- In Windows console type: `ipconfig /flushdns` - command likely NOT known by the average user