

The Rising Tide of DNS Threats

Are You Prepared?

In the last year alone there has been an increase of

200%
DNS attacks¹

58%
DDoS attacks¹



With a possible amplification of up to

100x

on a DNS attack, the amount of traffic delivered to a victim can be huge

28M

Pose a significant threat to the global network infrastructure and can be easily utilized in DNS amplification attacks²

33M Number of open recursive DNS servers²



With enterprise level businesses receiving an average of **2 million** DNS queries every single day, the threat of attack is significant

Countries of origin for the most DDoS attacks in the last year



DNS attacks are rising for 3 reasons:

1 Easy to spoof

2 Asymmetric amplification

3 High-value target

Financial impact is huge

\$27 million

The average loss for a 24-hour outage from a DDoS attack³

Avg estimated loss per DDoS event in 2012³

-\$7.7M	-\$13.6M	-\$17M
Government	Technology company	Financial services

TCP/UDP/ICMP floods:
Flood victim's network with large amounts of traffic

DNS cache poisoning:
Corruption of a DNS cache database with a rogue address

DNS tunneling:
Tunneling of another protocol through DNS for data ex-filtration

DNS based exploits:
Exploit vulnerabilities in DNS software

DNS reflection/DrDoS:
Use third party DNS servers to propagate DDOS attack

DNS amplification:
Use amplification in DNS reply to flood victim

Protocol anomalies:
Malformed DNS packets causing server to crash

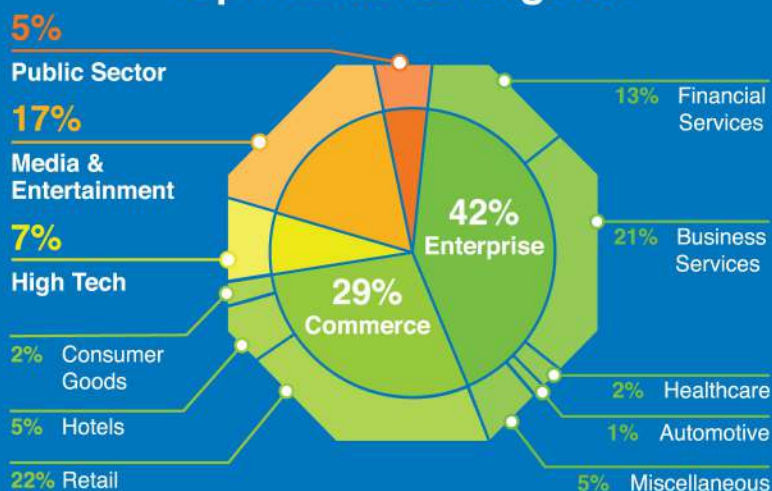
DNS hijacking:
Subverting resolution of DNS queries to point to rogue DNS server

Reconnaissance:
Probe to get information on network environment before launching attack

Fragmentation:
Traffic with lots of small out of order fragments

Top **10** DNS attacks

Top industries targeted⁴



The bottom line is

“Organizations should invest in protecting their DNS infrastructure.”

– Gartner⁵

Infoblox helps protect against the rising tide of DNS threats

www.infoblox.com/dnsprotection

Find out more with this whitepaper

Sources:
1. Quarterly Global DDoS Attack Report, Prolexic, 1st Quarter, 2013 2. www.openresolverproject.org 3. Develop A Two-Phased DDoS Mitigation Strategy, Forrester Research, Inc. May 17, 2013
4. State of the Internet, Akamai, 2nd Quarter, 2013 5. Leverage Your Network Design to Mitigate DDoS Attacks, Report ID G00253330, Gartner, July 2013