The Rising Tide of DNS Threats
Are You Prepared?

In the last year alone there has been an increase of 216% on DNS attacks¹ and 47% DDoS attacks² on a DNS attack, the amount of traffic delivered to a victim can be huge.

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 year³

- US
- China
- Thailand
- Turkey
- Brazil
- Japan
- Germany
- India
- Korea
- Italy

DNS attacks are rising for 3 reasons:

1. Easy to spoof
2. Asymmetric amplification
3. High-value target

TCP/UDP/CMP 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 exfiltration.
DNS based exploits: Exploit vulnerabilities in DNS software.
DNS reflection/DrDoS: Use third party DNS servers to propagate DDoS attack.
Phantom domain: Force DNS server to resolve multiple non-existent domains and wait for responses.
DNS hijacking: Subverting resolution of DNS queries to point to rogue DNS server.
DNS amplification: Use amplification in DNS reply to flood victim.
Protocol anomalies: Malformed DNS packets causing server to crash.
Reconnaissance: Probe to get information on network environment before launching attack.
Fragmentation: Traffic with lots of small out of order fragments.
NXDOMAIN: Flood DNS server with requests for non-existent domains.

Financial impact is huge

Estimated cost of a DDoS attack can be upwards of $100,000 per hour⁴.

Resulting in:

- Revenue loss
- Customer defection
- Brand damage
- Data theft from “smokescreening”

55% of DDoS targets were also victims of theft⁵.

Top industries targeted⁶

- Media & Entertainment: 16%
- Public Sector: 20%
- Enterprise: 28%
- Consumer Goods: 9%
- Financial Services: 27%
- Healthcare: 16%
- Automotive: 9%
- Retail: 28%
- Hotels: 20%
- Media & Entertainment: 16%
- Public Sector: 20%
- Enterprise: 28%
- Consumer Goods: 9%
- Financial Services: 27%
- Healthcare: 16%
- Automotive: 9%
- Retail: 28%
- Hotels: 20%

The bottom line is

“CIOs should make sure that DNS services are delivered efficiently, reliably and securely.”

- John Pescatore, SANS Institute⁷

Infoblox helps protect against the widest range of DNS threats

www.infoblox.com/securedns

Find out more with this whitepaper

Sources:

©2014 Infoblox Inc. All Rights Reserved. | www.infoblox.com | info@infoblox.com