efficient iP™
DEFINING SMART DDI

White Paper

# DNS Security Threat Landscape

## Learn All About:

- Volumetric Dos Attacks
- Stealth/Slow Drip Attacks
- Exploits
- How to Protect Against any Kind of Threat

In this day and age it is understood that the DNS service is one of the most critical IT services of any company in any industry. Many reports from internationally recognized experts, analysts and research institutes have demonstrated the utmost importance of the DNS service to ensure business continuity, which arguably is the most important objective of any network & security teams. So, no doubt, DNS services must be part of the global company's security plan. The important question is "What is your strategy for DNS security". Existing solutions such as firewalls, Intrusion Prevention Systems or generic anti-DDoS systems have clearly demonstrated their ineffectiveness to protect mission-critical DNS service (IDC security survey 2014).

Starting with a clear understanding of the threat landscape is key to discern the appropriate security approach.

## DNS Security Threat Landscape

Hackers have different possible objectives. They may aim for instance to interrupt business, corrupt data, steal information or all of these at the same time! To reach their goals, they continuously look for any vulnerability and have developed a high variety of DNS attacks that fall into three main categories.

1. **Volumetric DoS attacks:** Attempt to overwhelm the DNS server by flooding it with very-high number of requests from one or multiple sources, leading to degradation or unavailability of the service.

2. **Stealth/Slow drip DoS attacks:** Low-volume of specific DNS requests causing capacity exhaustion of outgoing query processing, leading to degradation or unavailability of the service.

3. **Exploits:** Attacks exploiting bugs and/or flaws in DNS services, protocol or on operating systems running DNS services.

Additionally it is fundamental to understand that most often DNS threats are geared towards a specific DNS function (cache, recursive & authoritative), with precise damage objectives. This aspect must be integrated in the DNS security strategy to develop an in-depth-defence solution, ensuring comprehensive attack protection.

The list below of the most common attacks aims to emphasize the diversity of the threats and details the extent of the attack surfaces.

| Volumetric Attacks | |
|---|---|
| Direct DNS DoS attacks | Flooding of DNS servers with direct requests causing saturation of cache, recursion or authoritative functions. This attack is usually sent from a spoofed IP address. |
| DNS amplification (DDoS) | DNS requests generating an amplified response to overwhelm the victim's servers with very large traffic. |
| DNS reflection | Attacks using numerous distributed open resolver servers on Internet to flood victim's authoritative servers (Usually combined with amplification attacks). |
| NXDOMAIN | Flooding of the DNS servers with non-existing domains requests implying recursive function saturation. |

| Stealth/Slow Drip DoS Attacks | |
|---|---|
| Sloth domain attacks | Attacks using queries sent to hacker's authoritative domain that very slowly answers requests, just before the time out, to cause victim's recursive server capacity exhaustion. |
| Phantom domain attack | Attacks targeting DNS resolvers by sending them sub-domains for which the domain server is unreachable, causing saturation of cache server capacity. |
| Random subdomain attack (RQName) | Attacks using random query name causing saturation of victim's authoritative domain and recursive server capacity. |

| Exploits | |
|---|---|
| Zero-Day vulnerability | Zero-day attacks take advantage of DNS security holes for which no solution is currently available. |
| DNS-based exploits | Attacks exploiting bugs and/or flaws in DNS services, protocol or on operating system running DNS services. |
| DNS Tunneling | The DNS protocol is used to encapsulate other protocols or data in order to remotely control malware or/and the exfiltration of data. |
| Protocol anomalies | DNS Attacks based on malformed queries intending to crash the service. |
| DNS cache poisoning | Attacks introducing data into a DNS resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer. |

Keep in mind first, that DNS attacks are more and more sophisticated, combining multiple attack vectors at the same time and secondly that the DNS landscape security is continuously moving. To keep ahead of the threats, security solutions must protect against a family of attacks rather than a limited list of predefined attacks that must be frequently updated or tuned. This last approach is costly with a high risk to block legitimate clients (false positives).

## Detect, Protect & Remediate DNS Attacks with 360° Security Solution

EfficientIP offers game-changing technologies to tackle DNS security threats. EfficientIP's innovative security solutions ensure unmatched protection of DNS services continuity regardless of the attack type, without risk of blocking legitimate clients or requiring complex configuration and laborious filtering rules. The solution is fast to deploy, easy to maintain, immediately capable of protecting against new threats and is highly cost-effective.

EfficientIP offers a unique 360° security technology for both public and private infrastructures to detect, protect and remediate DNS attacks with a unified solution.

### DNS Guardian: Intelligence to Protect Against DNS Attacks

DNS Guardian is a unique solution to detect, protect and remediate DNS attacks on cache servers. DNS Guardian offers graduated and adaptive countermeasures to mitigate DNS attacks and ensure services continuity. For instance, under DoS attacks on the recursive function, DNS Guardian identifies and blocks source IP addresses to ensure service availability. However, in the case of distributed slow-drip attacks it is most likely impossible to identify the source IP addresses. DNS Guardian detects the risk of exhaustion of the server capacity and activates the patented Rescue Mode innovation to ensure 100% availability of the DNS service.

### DNS Blast: Performance that Absorbs Volumetric DoS Attacks on Cache DNS

DNS Blast, the world's fastest cache appliance, can answer up to 17 million queries per second and absorbs large volumetric DoS attacks. Advanced cache sharing among servers reduces network resources consumption and improves user experience. DNS Blast embeds DNS Guardian security solution, offering unmatched power to intelligently protect against DNS security threats, regardless of the attack type.

### Hybrid DNS Engine: the Ultimate Answer against Zero-Day Vulnerabilities

EfficientIP SOLIDserver™ incorporates a combination of three DNS engines (BIND & Unbound/NSD), managed transparently as a single unit. DNS Hybrid technology provides the highest-level of security against Zero-Day vulnerabilities while enabling the ability to switch with a single action from the running name server software to the alternate name server software that's unaffected by new security threats.

### DNS Cloud: Protecting Authoritative Services against DNS DoS Attacks

EfficientIP's DNS Cloud enables deployment of "On demand" DNS services across 52 DNS spots globally, while providing best-of-breed performance and resilience. The integration of Route 53 from Amazon AWS is immediate, transparent and managed from a centralized management console with Internet and/or private DNS infrastructures. The DNS Cloud solution is extremely scalable, simple to deploy, very cost effective while flexible that brings a complementary key component to any security strategy.

### DNS Firewall: Ensure Proactive and Efficient Protection against Malware

Based on DNS query analysis, SOLIDserver™ DNS Firewall detects and isolates clients infected with malware, blocking all communication to external websites and then disrupting malware activity.

**ABOUT EFFICIENTIP**

EfficientIP solutions address organizations' needs to drive business efficiency through the innovative use of IT. Its unified management framework for DNS-DHCP-IPAM, devices and network configurations enhances security, availability and agility of the IT infrastructure. EfficientIP's solutions have been chosen by hundreds of the most demanding organizations across all industries.
**www.efficientip.com**

**EUROPE**

EfficientIP SAS
90 Boulevard National
92250 La Garenne-Colombes
+33 1 75 84 88 98

**USA**

EfficientIP Inc.
17 Wilmont Mews, Suite 400
West Chester PA 19382 USA
+1 888.228.4655

Copyright © 2015 EfficientIP, SAS. All rights reserved. EfficientIP and SOLIDserver logo are trademarks or registered trademarks of EfficientIP SAS.

All registered trademarks are property of their respective owners. EfficientIP assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document.