efficient iP™

White Paper

DNS Security Threat Landscape

Learn About:

- The importance of protecting the cache, recursive, and authoritative functions
- The most common volumetric, stealth/slow drip, and exploit attack types
- Blocking a comprehensive “family” of attacks, versus relying on limited predefined attack signatures
- An evolved 360° security solution

Outline:

A Vast DNS Security Threat Landscape

Volumetric Attacks

Stealth/Slow Drip DoS Attacks

Exploits

In this day and age, it is understood that the DNS service is one of the most critical IT services for any company in any industry. Many reports from internationally recognized experts, analysts and research institutes have demonstrated the utmost importance of DNS service to ensure business continuity, which is arguably the most important objective of any network and security team. Without a doubt, DNS services must be part of a global company's security plan. The prevailing 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[1].

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

[1] *IDC Security Survey 2014*

A Vast DNS Security Threat Landscape

Hackers have different possible objectives. They may aim 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:

- **Volumetric DoS attacks:** Attempt to overwhelm the DNS server by flooding it with a very high number of requests from one or multiple sources, leading to degradation or unavailability of the service.
- **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.
- **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 and authoritative), with precise damage objectives. This aspect must be integrated in the DNS security strategy to develop an in-depth defense 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 a very large amount of 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 domain 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 capacity exhaustion on victim's recursive server.
Phantom domain attack	Attacks targeting DNS resolvers by sending them subdomains 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.

It is important to understand that the DNS service has become a favored attack target, and at the same time a commonly used threat vector. As of today, the DNS is among the most targeted application layers for DoS attacks (over email[1]), while 91% of malware[2] abuses the protocol to silently communicate with remote CnC servers (Command and Control) or exfiltrate confidential data. Hackers persistently try to take advantage of any system weaknesses, and actively scan new DNS vulnerabilities to compromise the IT infrastructure security, making it highly sensitive to zero-day exploits. The most recent critical security alerts on BIND DNS services demonstrate the degree of importance of these threats.

Additionally, attacks are becoming more and more sophisticated, combining multiple attack vectors simultaneously, in a rapidly evolving DNS threat landscape. The connectionless nature of the DNS protocol requires real-time advanced analytics capabilities to truly identify threats hidden in the traffic and provide adapted countermeasures, ensuring service continuity and integrity. To keep ahead of 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. The latter approach is costly, with a high risk of blocking legitimate clients (false positives).

While existing traditional security systems (more specifically DNS filtering security solutions) offer a first level of protection against DNS attacks, they are not efficient enough and can even be dangerous if used inappropriately. It's time to look at new ways to mitigate DNS attacks.

EfficientIP offers a specialized layer of in-depth defense to fill the gap left by traditional security solutions to tackle DNS security threats. Previously, external layers of defense protected DNS services. Security is now embedded in the DNS servers themselves, and uses the DNS' own mechanisms to protect against attacks. DNS is its own security solution, with more intelligence, more performance and adapted countermeasures.

[1] According to the 2016 Worldwide Infrastructure Security Report from Arbor Networks

[2] 2016 Cisco Security Report

This unique 360° DNS security solution protects against any type of attack for both public and private DNS infrastructures, even when it is not possible to identify the attack source. It includes the following solutions:

DNS Guardian (2015 patent): Adaptive security on cache and recursive DNS to ensure service continuity, even under unidentifiable attack sources

DNS Firewall: Protection against DNS malware and phishing

DNS Cloud: 100% availability of public DNS services with a global network of DNS servers, at a series of worldwide locations

Hybrid DNS Engine: DNS zero-day vulnerability mitigation

DNS Blast (2014 patent): The world's fastest DNS server, absorbing extreme DDoS attacks at up to 17 million queries per second

efficient iP™

REV: C-1708

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

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

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752