

# Introduction to DNS Security

WRITTEN BY JAN VČELÁK  
LEAD SOFTWARE ENGINEER, NS1

## CONTENTS

- > Introduction
- > The Race to the Cloud and DNS Attacks
- > Common Threats to Authoritative DNS
- > Strategies for Secure and Resilient DNS
- > DNSSEC Dive Down
- > Conclusion

## Introduction

Authoritative DNS plays a critical role in our connected culture. It started as a simple phone book that routed requests to websites. But now, with virtually every application and computing activity connected to a sprawl of clouds, data centers, CDNs, and devices, authoritative DNS has emerged to new prominence in the internet infrastructure.

In this Refcard we'll look at how authoritative DNS's ubiquity and critical position in application infrastructure make it both a prime target for attackers and an opportunity to dodge downtime and defend against threats. Although no layer of your application delivery infrastructure is immune to attack, with the right tools you'll be better equipped to meet the challenges head-on.

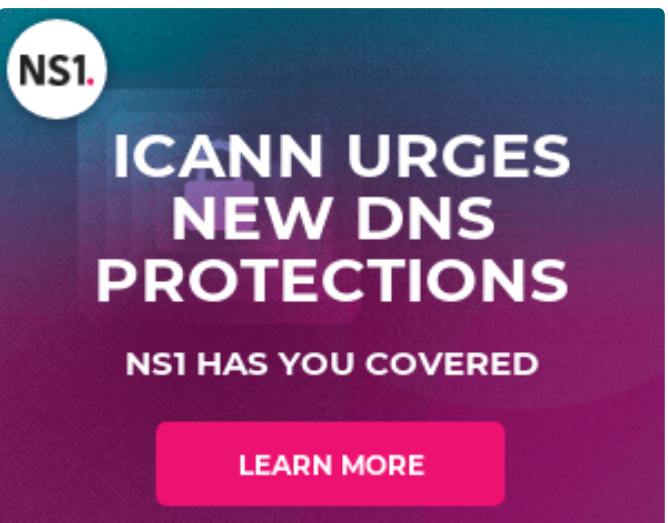
## The Race to the Cloud and DNS Attacks

Yes, the cloud brings efficiencies with it, and the majority of enterprises racing to the cloud see it as a platform for innovation. According to an [IDC research paper](#), "public cloud adoption is accelerating in large part as enterprises recognize that the cloud has become the launchpad for virtually every new IT innovation," and those companies not on public clouds find themselves in "innovation isolation."

There's no greater single driver for DNS-based threats than the race to adopt the innovation inherent in digital experiences and cloud computing by enterprises and consumers alike. DNS is the primary mediator between users and any online service or application, and

any disruption in DNS denies access to these services. The misdirection of DNS services can send users to malicious sites for further manipulation and can be used to gain access to private networks.

DNS is a potential single point of failure and a rich source of attack and manipulation techniques, and attackers are taking advantage of it. 40 percent of cloud-based application downtime is a result of attacks on DNS servers and services. For many companies (and even cloud providers), the race to embrace the cloud is outpacing the security and resiliency upgrades required in core enterprise and internet infrastructure to ensure not only security, but uptime and optimal end-user experience.



**NS1.**

**ICANN URGES  
NEW DNS  
PROTECTIONS**

**NS1 HAS YOU COVERED**

**LEARN MORE**

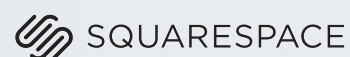


**The race to cloud creates a lightning rod for DNS Attacks - be prepared!**

No one company controls the entire Internet and application delivery infrastructure, but one strategic technology—DNS—intersects it all. And many companies use basic or legacy DNS for their domains, applications and users, unaware of the risks.

Visit our *Getting Serious about DNS Security* resource center to learn about the different types of DNS attacks and how to circumvent or mitigate them.

**Visit our DNS Security Resource Center for more**  
[ns1.com/dns-security-resource-center](https://ns1.com/dns-security-resource-center)



The cloud introduces fundamental changes that older architectures and technologies weren't designed for, which opens the door for security risks. These include:

- **Expansive connectivity and diversity.** On the surface, the cloud seems much simpler for enterprises since the infrastructure is no longer onsite. But the massive connectivity of cloud computing adds new layers of complexity. According to Gartner, "the increased trend toward dynamic, fragmented, and distributed cloud-based applications complicates the task of maintaining visibility and availability of key resources." There isn't just "one" cloud, and the various options don't all function in the same manner. 87 percent of enterprises use multiple clouds and as multi- and hybrid clouds emerge, there's increased complexity in the number of potential clouds, how, where, and when users are routed to those resources, and how those resources are managed and protected.
- **Concentration of information and risk.** While the infrastructure may be fragmented and diverse, the data attackers want to steal can be highly concentrated in the cloud, vastly increasing its attractiveness to bad actors.
- **Uneven innovation and security across clouds and enterprises.** Not all clouds are equal in their capabilities, offerings, stability, and security. There's little security equality across the vast landscape of cloud providers, and even less with the enterprises adopting them.
- **Technical debt.** The rapid innovations born from the cloud have not migrated quickly or evenly to the enterprises leveraging clouds. Enterprises are spending the vast majority of their budgets maintaining older, outdated systems, leaving critical projects on the cutting room floor — and perhaps worse, sometimes sending them shopping for cheaper cloud providers without robust security.

## Common Threats to Authoritative DNS

Attack and risk take a number of forms and vary in impact from complete outages and data breaches to dramatic slowdowns that drive users away. Here's a look at common DNS attacks and threats to authoritative DNS in more detail.

### DISTRIBUTED DENIAL OF SERVICE (DDOS)

Attackers use botnets to flood servers with massive amounts of traffic in an attempt to overwhelm unprepared DNS infrastructure that simply can't handle the volume of requests. DDoS attacks can target any connected server, not just DNS. A 2018 [Nexusguard](#) report shows a 500% increase in the size of DDoS attacks, and [Kapersky](#) reports an increase in the duration of mixed and HTTP flood attacks; suggesting

bad actors are turning to more sophisticated methods. Instead of attacking DNS directly, a DDoS attack can also use authoritative DNS to amplify an attack on another target.

### DNS SPOOFING AND CACHE POISONING

Authoritative DNS resolvers are the servers that receive DNS queries from end-user devices and retrieve the answers from authoritative name servers. Resolvers gain efficiency by caching the answers to avoid repeated look-ups to authoritative servers for the same name. The original DNS specifications didn't provide for adequate security mechanisms that would prevent resolvers from accepting bogus DNS data. Attackers can send a series of bogus requests to the domain resolvers as well as fake responses to those requests. If a fake response gets accepted by the resolver before a response from a legitimate authoritative server gets to that resolver, that fake information is cached — poisoning the resolver. A poisoned cache can redirect users to false sites for phishing attacks, or even take over an entire domain. Cache poisoning is difficult to detect, and you won't always know it's happening. The bogus DNS data is cached by the resolver and disappears after a prescribed amount of time. Deploying the DNSSEC protocol can ensure that only authenticated responses are used.

### MALWARE

Cache poisoning is one way to redirect requests for malicious purposes. Additionally, malware infections can take control of various DNS server resources that communicate with each other throughout the Internet's infrastructure. DNS is a highly connected server infrastructure, giving malware a large attack surface to target and spread across once it penetrates a single server or device. DNS Changer is a well-known example of malware deliberately targeting and manipulating DNS resources. DNS Changer infects computers and forces them to point to malicious servers instead of the proper ones at ISPs and other locations. Once hijacked and taken to a malicious server, bad actors put their plans into practice; like phishing attempts to gain passwords or personal or financial information, installing more malware directly on a user's computer or router, or injecting fake ads for malicious pay-per-click schemes.

### DOMAIN HIJACKING

Over the past several years there have been many high-profile domain hijacks, including Wikileaks and The New York Times. Although the causes of each of these vary or is unclear, one of the most common paths to gaining control of a .com property is social engineering. Using phishing or other clever methods, attackers can gain an administrator's credentials, change DNS resources (like the registration) to gain control of the domain, and then misdirect traffic from that domain to malicious sites. Sometimes a domain hijack is an embarrassment, while other times it has serious financial or data privacy consequences from hacking that can occur on the misdirected site.

## Strategies for Secure and Resilient DNS

No service or application on the Internet is completely immune to the effects of a cyber-attack. But there are strategies and key selection criteria to follow when choosing DNS providers that can mitigate or avoid DNS-related threats.

### UPGRADE DNS IN THE APPLICATION INFRASTRUCTURE

The lack of attention to DNS lags behind the innovation of cloud infrastructure, creating cracks for possible exploitation. As organizations increasingly embrace a new generation of “cloud-first” computing environments with multiple, connected clouds, data centers, and CDNs, they also need to adapt and upgrade the underpinning infrastructure, including DNS and security technologies and policies. Many cloud, CDN, and other providers “throw in” simple DNS offerings, running default configurations that lack robust resiliency, scale, and security. And on the enterprise side, many still rely on homegrown DNS, developed decades ago.

### MIGRATE TO A MANAGED, ANYCAST DNS SOLUTION

Borrow a page from your cloud computing playbook and use an external, managed DNS solution with a globally distributed, anycast network that has modern features and the skills and resources to track threats, defend against hackers, and better withstand or mitigate a massive DDoS attack. Picking an expert provider with resilient and modern networks can remove the constant management and attention needed for secure DNS.

An anycast network is a one-to-many routing solution that has multiple endpoints around the globe that all respond to the same IP address. Anycast, using BGP, determines the location of services the closest to the user, and chooses that server to create its one-to-one connection. This greatly improves DNS response time by delivering queries to the closest nameserver and provides for resiliency and failover by using internet routing to steer queries away from nameservers or POPs that are not available, performing poorly, or under attack.

### USE DNSSEC — AND CONFIRM YOUR PROVIDERS DO, TOO

Application layers use security protocols (like HTTPS, DMARC, etc.), and DNS is no exception. The Domain Name System Security Extensions (DNSSEC) is one of them. DNSSEC reinforces the authenticity of DNS query responses by using digital signatures to authenticate communications, protecting applications (and the caching resolvers used by those applications) from using fake DNS data in cache poisoning and spoofing attacks. DNSSEC is not widely adopted, even by some of the largest cloud providers, and hackers are exploiting DNS without DNSSEC.

Why do so few companies deploy DNSSEC? Some have held back because of complexity and traditional and perceived drawbacks of DNSSEC, including giving up the DNS traffic management capabilities

ties relied on to deliver high-quality online services. Signing zones, storing keys, and fine-tuning DNSSEC can be complex. It's important to note that DNSSEC is not a silver bullet. It's very effective against cache poisoning, but it does not protect the availability of your DNS. That requires redundancy.

### DEPLOY A SECOND DNS NETWORK FOR REDUNDANCY AND RESILIENCY

The sites that bounce back the fastest from cyber-attacks utilize a now mission-critical strategy: redundant DNS. Even with anycasting, you still have a single point of failure for technical errors, outages and security events. Managing redundant networks can be challenging with some providers. Just like a multitude of clouds, not all DNS networks easily share information, or have the same levels of security. A dual provider approach to redundancy can be challenging to manage and maintain, especially when the DNS records leverage capabilities such as failover and geo routing.

Some enterprises simply manage their two DNS systems separately (dual primary DNS) which doubles the DNS management workload and adds risk that DNS records are not well synchronized. Others rely on middleware based on homegrown scripts or tools such as OctoDNS and Terraform. These approaches also are challenging in that they require customization that is specific to the enterprise setup and need to be maintained and supported over time by internal IT staff.

It's important to note that your redundant DNS provider should itself implement security best-practices like DNSSEC. Ask your DNS providers what types of attacks they see, how they defend against them, and what redundancies they have in place to avoid single points of failure.

## A Closer Look at DNSSEC

The Domain Name System Security Extensions (DNSSEC) prevents attacks that can compromise the integrity of answers to DNS queries. As we've said before, when successful, these attacks can result in users being falsely directed to bogus websites masquerading as legitimate sites or they can be used as a form of denial of service. Although attacks on the integrity of DNS information can have serious consequences, many organizations have not protected their zones with DNSSEC; holding back because doing so traditionally meant giving up the DNS traffic management capabilities they rely on to deliver high-quality online services. These technical barriers have resulted in an unfortunate trade-off between functionality and security.

### DNSSEC AND TRAFFIC MANAGEMENT

DNS traffic management has become a staple for organizations of all sizes. Small organizations and enterprises alike have come to rely on traffic management capabilities that range from the relatively basic, such as:

- Monitoring your sites and directing users away from sites that are currently down
- Geo routing – sending users to the closest PoP

To advanced:

- Routing users to the best performing, most cost-effective CDN
- Using real-time load telemetry to balance traffic between multiple data centers

Unfortunately, DNSSEC implementations on standard DNS platforms and on most DNS managed services are incompatible with traffic management. DNSSEC “breaks” even basic functions such as geo-routing. It’s often the case that the most important zones – the ones you should secure with DNSSEC – are the very same ones where traffic management is most valuable. The trade-off is security versus the quality of your digital offering.

### REDUNDANT DNS AND DNSSEC

DNSSEC helps protect the integrity and authenticity of your DNS records. It prevents man-in-the-middle attacks from corrupting information on DNS resolvers (cache poisoning). However, DNSSEC does

not protect the availability of DNS systems. The need for redundancy in your DNS is crucial with or without DNSSEC. A dual-provider DNS infrastructure where both providers support DNSSEC can provide availability assurance.

### Conclusion

The distributed nature of the Internet — along with a new generation of cloud platforms and multiple data center and CDN strategies — brings with it a concentration of risk, with massive targets and rippling effects downstream. But after waves of high-profile attacks, some DNS providers have built incredible resiliency into their networks, and combined with the strategies and best practices outlined in this Refcard, you can greatly reduce your exposure and risk with a modern, resilient DNS infrastructure.



Written by **Jan Včelák**, *Lead Software Engineer, NS1*

Jan is a lead software engineer at NS1 and expert on DNS and DNSSEC. He is active member of the DNS-OARC community and several IETF working groups. He enjoys contributing to open-source software and speaking at industry conferences. Before joining NS1, he worked as a developer and researcher at CZ.NIC on the open-source authoritative server Knot DNS.



DZone communities deliver over 6 million pages each month to more than 3.3 million software developers, architects, and decision makers. DZone offers something for everyone, including news, tutorials, cheat sheets, research guides, feature articles, source code, and more. "DZone is a developer's dream," says PC Magazine.

Devada, Inc.  
600 Park Offices Drive  
Suite 150  
Research Triangle Park, NC

888.678.0399 919.678.0300

Copyright © 2019 DZone, Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by means electronic, mechanical, photocopying, or otherwise, without prior written permission of the publisher.