5 DNS Security Risks That Keep You Up At Night (And How To Get Back To Sleep)

There are things that go bump in the night, and things that go bump against your DNS security. You probably know about the risk of distributed denial of service (DDoS) attacks, but other threats lurk in the dark.

Security threats against DNS infrastructure are both serious and growing. In fact, according to a 2013 Arbor Networks survey, the largest DDoS attack (60 Gbps) targeted DNS infrastructure. In that same survey, twice the number of respondents claimed to have experienced customer-impacting DDoS attacks on their DNS infrastructure in 2013 versus 2012.

Yet, 19% of organizations have no dedicated group responsible for DNS security.[1]

When it comes to keeping your DNS secure, do you know what you're up against? Here are five of the most pervasive DNS threats that you need to be thinking about, and how to keep them from creating a performance or security nightmare.

1. DDoS Attacks

What's The Threat?

The most common of DNS boogeymen, DDoS attacks prevent a service from working by using a large number of machines from all over the Internet to send enormous amounts of traffic towards a target website or application. When the DNS infrastructure is sufficiently overloaded by incoming requests, performance crashes or completely fails, impacting your ability to serve customers.

How Does It Occur?

An attacker clogs network services by overloading one or more DNS servers with recursive queries from "zombie" computers — computers compromised and controlled remotely by an attacker. When server processors hit max capacity by trying to respond, the DNS service becomes unavailable to the people trying to access your website or applications. 54% of DDoS attacks in 2013 were over 1 gigabit per second, up from 33% in 2012.

SURVEY SAYS:

25% of survey respondents reported customer-impacting DDoS attacks on their DNS infrastructure.

21% of survey respondents permit unrestricted recursive lookups by their DNS servers.[1]

WANT TO LEARN MORE ABOUT DDOS? READ OUR WHITEPAPER:

Everything You Need To Know About A DDoS Attack

DOWNLOAD AVAILABLE AT:

http://bit.ly/DDoS101

[1] "Network Operators Speak Out on the Status of DNS Security," Arbor Networks, 2013.

How To Prevent It

Fight fire with fire. Prevent distributed attacks with a distributed network of anycast servers that can handle a deluge of DNS traffic. Don't have a dispersed fleet of anycast servers? You're not alone. Look to managed DNS providers, which are committed to building out widely distributed, highly redundant networks of anycast servers. They'll mirror your own DNS servers to mitigate a DDoS attack and generally improve network performance by load balancing queries.

2. DNS Amplification

What's The Threat?

Rather than a standalone attack, DNS amplification exploits powerful recursive DNS servers to increase the strength of a DDoS attack. The attacker uses the target's own strength to overwhelm the network and cripple performance.

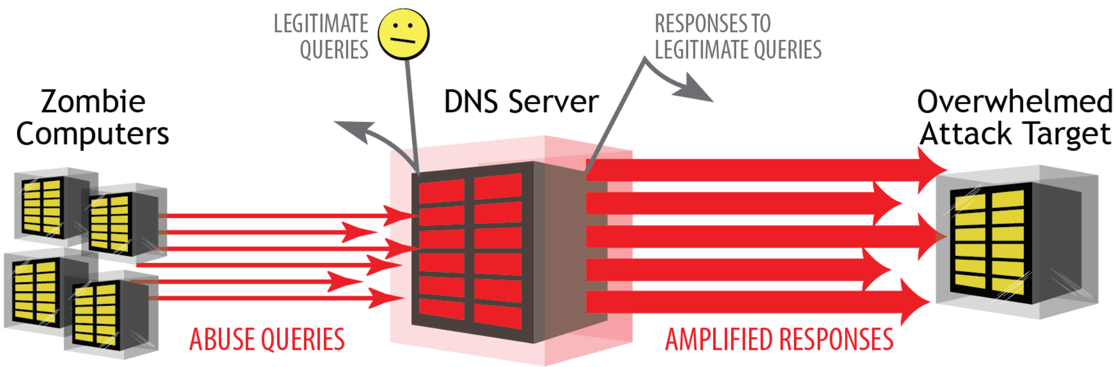
How Does It Happen?

Attackers spoof the source address on DNS queries to match that of the target, and use bots to send bogus packets to a recursive name server, effectively amplifying the packets by a ratio as high as 70:1. DNS amplification gives attackers with small botnets the same power as large botnets. So if you have an open recursive DNS server, the number of attackers you need to be concerned with is amplified as well.

How To Prevent It

Is your recursive DNS server open to the Internet? If yes, put this threat to bed right now by changing your server configuration. That is all.

DNS Amplification Attack



3. Cache Poisoning

What's The Threat?

Cache poisoning (aka pharming or redirection) sends unsuspecting people to malicious websites attached to legitimate URLs. And if the attacker's site looks just like the attack target's actual site—not a difficult task—there's practically no way for someone to know they are being scammed, leading to them entering their personal information (address, birthday, credit card number, social security number) into a site that "pharms" information.

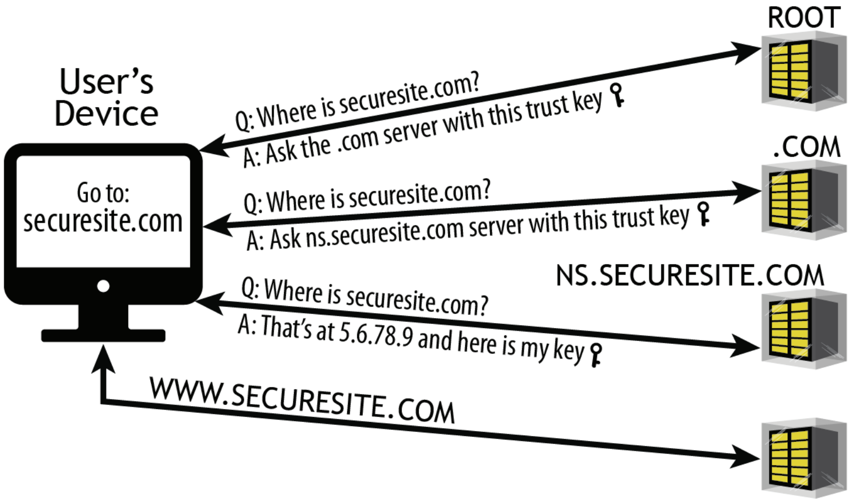
How Does It Occur?

Researcher Dan Kaminsky discovered a serious flaw in the DNS protocol that made it an easy target for attacks. The vulnerability, now known as the Kaminsky bug, enables an attacker to trick an Internet Service Provider (ISP) into caching malicious DNS information into the recursive DNS server caches. That's how a legitimate website URL can redirect users to the wrong IP address.

How To Prevent It

You can ward off cache poisoning attacks by making sure your DNS server configurations are secure, but the best protection is to apply the DNS Security Extensions (DNSSEC) protocol to each step in the DNS lookup—from root zone to the final domain name. Registries and registrars worldwide use the DNSSEC add-on to digitally sign data, ensuring its validity. (It's important to note, however, that it doesn't encrypt the data.)

DNSSEC In Action


ROOT
User's Device
Q: Where is securesite.com?
A: Ask the .com server with this trust key
.COM
Go to: securesite.com
Q: Where is securesite.com?
A: Ask ns.securesite.com server with this trust key
NS.SECURESITE.COM
Q: Where is securesite.com?
A: That's at 5.6.78.9 and here is my key
WWW.SECURESITE.COM

18% of survey respondents saw DNS cache poisoning attacks to or through their DNS infrastructure, while 38% lack the visibility to know of such attacks.

"Network Operators Speak Out on the Status of DNS Security," Arbor Networks, 2013.

4. Registrar Hijacking

What's The Threat?

It's likely that you have your domain name registered with a registrar company. That means that if your registrar is under attack, you're probably under attack. Registrar hijackers can take control of your domain name and direct it to a server (name, web, email, etc.) of its choice. The attacker could even transfer your domain to a new registrar, cutting ties with the compromised account and making it difficult for you to regain ownership.

How Does It Occur?

A registrar hijacker may aim to attack all of a registrar's accounts, or it could target your account specifically. It may try to crack the code on your password or manipulate one of your registrar's technical support operatives into revealing it.

How To Prevent It

Avoid the temptation to sign with the first registrar to offer a promotional discount or to laugh at your jokes. Ask questions. Be picky. Register with a managed DNS provider that takes security seriously and has features such as multi-factor authentication and high-value services that can substantially curb risk. These services may come at an additional cost, but compared to the revenue loss and reputation damage that may result from a hijacking, they end up paying for themselves.

There are almost 1,000 ICANN-accredited registrars, including Dyn. View the complete list:

http://bit.ly/ICANNregistrars

5. Footprinting

What's The Threat?

Footprinting isn't an attack itself, but it sets the stage for a successful DNS attack by gathering information about DNS domain names, computer names, registration details, server type, IP address, location, and other details. With this information, the attacker knows which resources to target and can plan an IP spoofing attack.

How Does It Happen?

Effective footprinting requests a zone data transfer from your DNS server to an attacker's zone server, giving it a complete copy of the DNS records for the entire zone. This is very easy for attackers to do when you allow any Internet user to execute zone transfers.

How To Prevent It

Don’t allow any ol’ Internet user to execute zone transfers. Instead, control DNS zone transfers by restricting them to specific DNS servers. You can also run your DNS services on domain controllers and configure them to authenticate each other before exchanging data. Then, use Active Directory integrated zones for replication. An attacker can no longer impersonate a domain controller and receive the zone transfer information.

A DNS Security Solution To Sleep On

Now that you know about key threats to your DNS security, don’t let them keep you up at night. This paper details steps you can take to protect yourself, but you don’t need to tackle them alone. Managed DNS provides risk mitigation for the newest of threats with the latest technologies, overseen by security experts. Delivered as a service, it handles your DNS needs without requiring onsite hardware, software, or additional personnel. You get all the security benefits without the effort or capital costs.

The security of your DNS is too important to chance, so consider partnering with a managed DNS provider like Dyn to be assured that you’ll be protected.

Need backup against these DNS threats? Give us a call.

REVIEW OF THE 5 DNS SECURITY RISKS

1. DDoS Attacks
2. DNS Amplification
3. Cache Poisoning
4. Registrar Hijacking
5. Footprinting