‘Never Inspected, Never Blocked’

How DNS Security Can Protect You Against Data Breaches, APTs and DDoS Attacks

Both business executives and IT managers are justifiably worried about data breaches, advanced persistent threats (APTs) and distributed denial-of-service (DDoS) attacks. These threats can have a devastating impact on enterprises and government agencies alike, resulting in lost business, damaged brands, disrupted operations and massive data breach notification costs.

Yet not many managers appreciate the role that Domain Name System (DNS) attacks can play in these threats. DNS is perceived as a utility, part of the “plumbing” of the Internet. Few are aware that DNS traffic can be an avenue for attackers to tunnel through security defenses and exfiltrate stolen data to remote servers, or that some of the biggest DDoS attacks ever launched exploited weaknesses in the DNS infrastructure.

It is also not widely understood that DNS security can help identify data breaches, APTs and DDoS attacks, and stop them before they can do major damage.

This paper provides a brief overview of DNS, how attackers abuse the DNS infrastructure to perpetrate data breaches, APTs and DDoS attacks, and how DNS security can help protect against those threats.

Have You Read This Novel?

The fortress walls are high and strong. The stout iron gates can be slammed shut at a moment’s notice. Alert guards scan the faces of everyone entering and leaving. Lookouts high on the walls scan the horizon, ready to sound the alarm at the first sign of trouble.

Yet no one watches the water pipe that runs through the fortress walls, from the moat outside to the cistern within. At midnight, the black-clothed adversaries swim to the mouth of the pipe. Some have orders to start a fire in the stables to distract the guards while others break into the treasury. The leader plans to open the gates from the inside at the appointed hour. Suddenly…

A Brief Refresher on DNS

DNS allows people to refer to websites using words, while allowing computers to track them with numbers (and a few characters). It is often compared to a giant global telephone directory. According to the website of the American Registry for Internet Numbers:

> “The Domain Name System (DNS) is the hierarchical naming system for all resources connected to the Internet or a private network, including websites, mail servers and application servers. For instance, the domain name **www.example.com** translates to the addresses **192.0.32.10** (IPv4) and **2620:0:2d0:200::10** (IPv6). Both identify the same website, but www.example.com is easier for a person to remember and use.”

CLOUDMARK®

TechTarget® Custom Media
A TECHTARGET WHITE PAPER

DNS is the largest distributed database in the world, tracking 877 million hostnames and 178 million active sites.[1]

The typical use case for DNS is shown in Figure 1: A computer user types a domain name into a browser. The browser sends a request to a DNS server asking for the IP address that corresponds to that domain name. Some enterprises have their own DNS server inside the firewall. In other cases, the request goes to a DNS server at the enterprise's Internet service provider or another site in the cloud. If that DNS server does not have the answer (no single DNS server can keep track of nearly 1 billion hostnames), it passes on the request to another DNS server, which may need to pass on the request again. This is called *recursion*.

When the request reaches a DNS server with the answer, a message that includes the correct IP address is sent back down the chain to the browser, which then uses the IP address to "resolve" the domain name and contact the web page the user requested. DNS traffic travels over the Internet but uses the User Datagram Protocol rather than TCP. Requests and responses are normally only a few bytes, so the impact on response times is undetectable—especially if the IP addresses have been cached on a local name server.

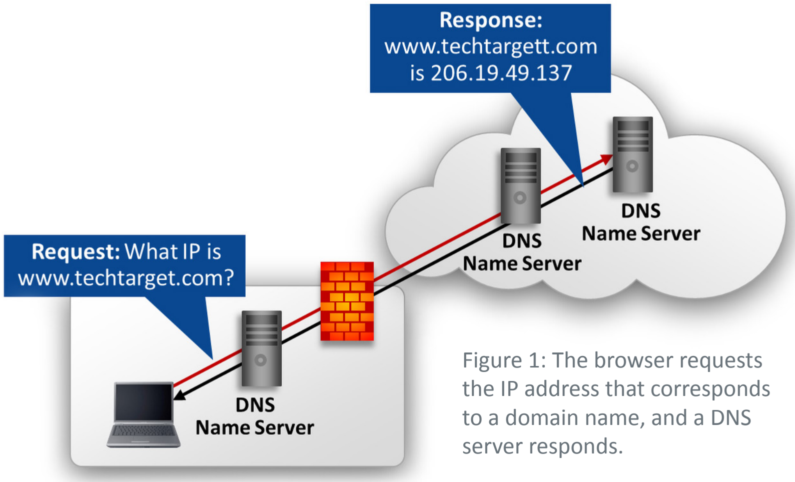

Response: www.techtargett.com is 206.19.49.137
Request: What IP is www.techtarget.com?
DNS Name Server
DNS Name Server
DNS Name Server

Figure 1: The browser requests the IP address that corresponds to a domain name, and a DNS server responds.

Why Attackers Target DNS

Cybercriminals, political "hacktivists" and hackers of all stripes have discovered many ways to exploit weaknesses in the DNS infrastructure. According to Jeff Wilson, principal analyst for security at Infonetics Research:

> "It's not at all surprising that DNS would be a target for hackers and cybercriminals. DNS is a key to the basic function of the internet, it's pervasive, and it was developed over 20 years ago with very little thought about security. Since then it's been constantly retrofitted, which means DNS infrastructure is highly vulnerable to attacks."[2]

Virtually all firewalls allow DNS traffic to pass through, because otherwise browsers could never resolve domain names. Most intrusion prevention systems (IPSs) inspect DNS traffic only minimally or not at all (some can't inspect any UDP traffic). In effect, DNS creates a "tunnel" through perimeter defenses. This makes it a perfect avenue for attackers seeking to send instructions from outside the enterprise perimeter to compromised computers inside, and to exfiltrate data back out.

The DNS infrastructure on the web also can be converted by clever hackers into an extremely potent weapon for creating volumetric DDoS attacks, because it is massive and relatively easy to spoof.

[1] "Web Server Survey," Netcraft, January 2015

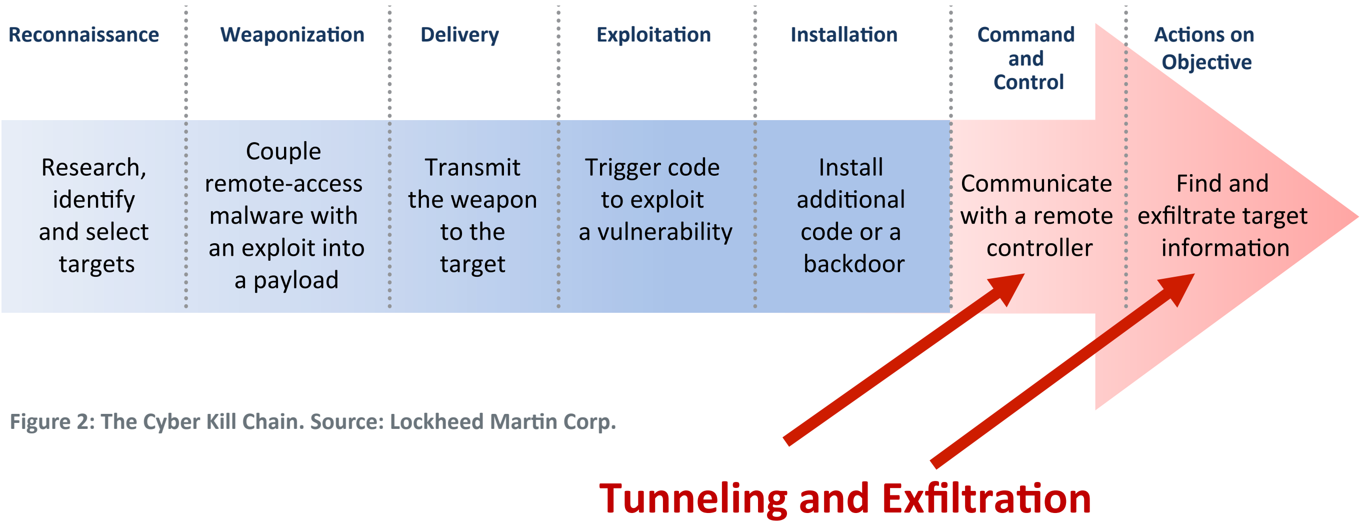
[2] "DNS infrastructure is 'highly vulnerable' to attacks, warns Infonetics," FierceITSecurity, Nov. 13, 2014

Finally, many technologists oblige hackers by ignoring DNS security. They take DNS services for granted, thinking of them as innocuous Internet utilities. As one cybersecurity expert put it, with only slight exaggeration: “[DNS traffic is] never blocked, never inspected.”[3]

How DNS Is Used for Data Breaches and APTs

Data breaches in 2014 affected thousands of enterprises and government agencies and tens of millions of households, with costs that ran into the billions.[4] Many of the most damaging were associated with APTs, sometimes called *advanced threats* or *advanced attacks*. These are multi-stage cyberattacks that last for weeks or months, launched by sophisticated organizations targeting high-value data such as credit card and account numbers, customer data, intellectual property, corporate financial information and trade secrets.

A now-classic model of the typical APT is the Cyber Kill Chain®, developed by Lockheed Martin.[5]



Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on Objective
Research, identify and select targets	Couple remote-access malware with an exploit into a payload	Transmit the weapon to the target	Trigger code to exploit a vulnerability	Install additional code or a backdoor	Communicate with a remote controller	Find and exfiltrate target information

Tunneling and Exfiltration

Figure 2: The Cyber Kill Chain. Source: Lockheed Martin Corp.

Today’s advanced adversaries have become extremely effective at the first five phases, but often find the last two phases the most challenging. They need to establish command and control channels to communicate from their servers, through perimeter defenses to compromised systems inside. Then they need to be able to exfiltrate stolen information back to their servers without being detected by the enterprise’s security and network monitoring tools.

Most of the protocols that could be used for data exfiltration, including HTTP and SMTP, are monitored effectively by IPS and data loss prevention solutions. In contrast, DNS traffic is rarely monitored. Many attackers take advantage of that weakness by using DNS traffic to hide two-way command-and-control communications and bidirectional data communication (*DNS tunneling*). Others employ DNS communication for one-way data transfer of corporate data to external servers (*DNS exfiltration*).

[3] “Protecting DNS Infrastructure: An Internet Utility that Demands New Security Solutions,” Jeff Wilson, Infonetics Research, Nov. 2014

[4] For a list of some of the most important, see “2014 in security: The biggest hacks, leaks, and data breaches,” ZDnet, Dec. 28, 2014

[5] “Intelligence-Driven Computer Network Defense,” Lockheed Martin, March 2011

The basic method is the same:

1. Encrypt the payload (command-and-control instructions or blocks of data).
2. Embed the payload into a DNS query or reply between the compromised computer and a DNS server outside controlled by the attacker.
3. Decrypt the payload at the destination.[6]

This activity usually goes undetected, because firewalls and other perimeter defenses are geared toward screening HTTP and SMTP traffic. Many either cannot inspect DNS traffic, or apply only very rudimentary restrictions. Network anomaly and threat intelligence solutions don't solve the problem either. They rely on detecting communication between known malicious external IP addresses and internal endpoints, whereas DNS tunnels connect an internal endpoint and a trusted external DNS resolver.

How DNS Is Used in DDoS Attacks

The massive global DNS structure provides a powerful weapons platform for DDoS attacks. DDoS attacks are designed to overwhelm websites, or even to saturate Internet links, in order to embarrass the target enterprise, damage its brand, decrease online sales or disrupt business operations. Some are launched by competitors, ex-employees and hackers with grievances against a specific enterprise. Others are attacks by political activists and state-sponsored hackers for propaganda purposes, retaliation against perceived injustices and even cyber warfare.[7]

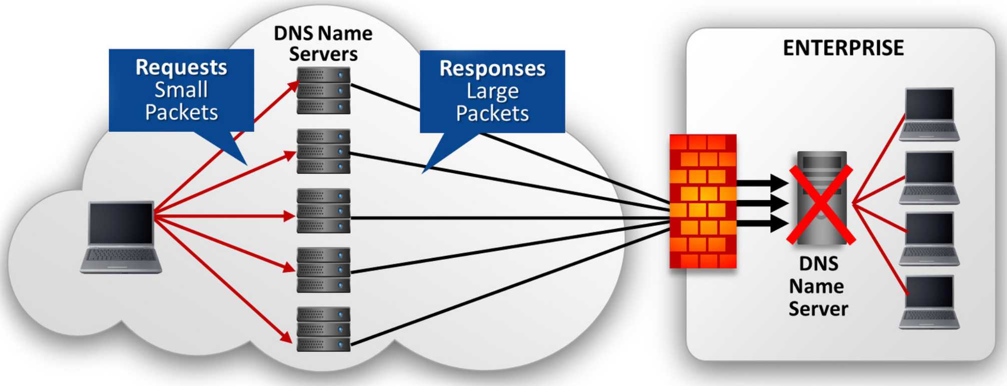


Figure 3: A DNS amplification and reflection attack.

Historically, one of the most dangerous forms of DDoS attacks has been the DNS amplification and reflection attack, which is illustrated in Figure 3. The attacker uses a botnet (a network of compromised computers) to send DNS request messages to multiple DNS servers. The queries are constructed to elicit response messages that are much larger than the request messages (amplification). For example, request messages of 60 bytes might generate response messages of almost 4,000 bytes. In addition, the requests spoof the IP address of the target enterprise, so the DNS servers send all of the response messages to the target website, not the requesting websites (reflection). Some DNS servers are configured to prevent themselves being used in this way, but a very large number are not.

One of the most massive DDoS attacks ever was a DNS amplification attack. Launched against the antispam industry clearinghouse SpamHaus in 2013, this attack reached a volume of over 300 gigabytes per second, making it the highest-volume DDoS attack ever observed at that time.[8]

[6] For more details on how attackers are using DNS tunneling and exfiltration, see "Security Whitepaper: DNS Tunneling," Cloudmark, Oct. 2014

[7] For example, "Bank Attackers Restart Operation Ababil DDoS Disruptions," Dark Reading, March 6, 2013; "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, Jan. 8, 2013; "Hong Kong: Massive DDoS Attacks Continue, Targeting Pro-Democracy News Site," GlobalVoices, June 20, 2014

[8] "Firm Is Accused of Sending Spam, and Fight Jams Internet," *The New York Times*, March 26, 2013; "DNS is ubiquitous and it's easily abused to halt service or steal data," *Network World*, Oct. 23, 2014

The most common DNS DDOS attack today (used by the Lizard Squad hacking group, for example) is the DNS resource exhaustion attack, which is illustrated in Figure 4. The attacker registers a domain and designates a target DNS server, belonging to either a target enterprise or an ISP, as the authoritative DNS server for that domain. The attacker then uses a botnet or open resolvers to send DNS request messages to multiple DNS servers, where each request message contains a unique, nonexistent subdomain of the attacker's domain. Those DNS servers then flood the target authoritative DNS server with the request messages. The target DNS server bogs down as its CPU, memory and bandwidth are consumed trying to look up the nonexistent sub-domains.[9]

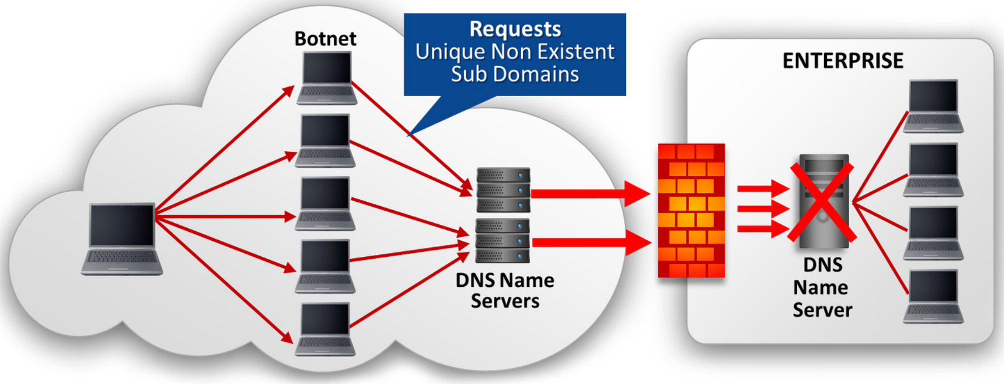


Figure 4: A DNS resource exhaustion attack.

There have been a number of prominent cases, including Sony and Bank of the West, where a DDoS attack was used to distract the IT security staff so cybercriminals could exfiltrate data unobserved. These diversionary DDoS attacks form a bridge between DDoS attacks and data breaches and APTs.[10]

Are DNS-Related Attacks Common?

Unfortunately, DNS-related attacks are becoming more frequent. A survey of U.S. and U.K. IT decision makers found that 66 percent had suffered a DNS attack within the past 24 months. Of those who had experienced a DNS attack, 46 percent had suffered a DNS exfiltration attack, 45 percent had suffered a DNS tunneling attack, and a stunning 74 percent had suffered a DNS-related DDoS attack.[11]

A study in early 2014 confirmed the prevalence of DNS involvement in DDoS attacks: "In Q1 2014, NTP reflection attacks and DNS amplification attacks stood out as the two most common attack types observed."[12]

How DNS Security Can Protect Against Data Breaches, APTs and DDoS Attacks

DNS security solutions can pinpoint warning signs of data breaches and APTs and immediately shut down command-and-control operations and the exfiltration of data through DNS tunnels. They can also provide clues that allow security and incident response teams to uncover and eliminate compromised computers and other elements of the attacks, thus protecting confidential data, intellectual property and brand reputations.

There are several techniques for identifying DNS traffic being used for tunneling and data exfiltration in real time using application-level inspection of the traffic. A DNS security solution can look for:

[9] For more information, see "DNS Resource Exhaustion," Cloudmark, October 2014

[10] "DDoS Attack on Bank Hid $900,000 Cyberheist," Krebs on Security, February 2013; "Sony Data Breach Was Camouflaged by Anonymous DDoS Attack," *eWeek*, May 5, 2011

[11] "New Research Reveals More than Three Quarters of Organizations Have Suffered a DNS Attack," Cloudmark,

[12] "Verisign Distributed Denial of Service Trends Report - 1st Quarter 2014," Verisign, Q1 2014

- Unusually long responses.
- Atypical request and response rates for a requested domain.
- Unusual patterns in the types of DNS records requested and returned.
- Communications with domains or IP addresses known to be associated with DNS-related attacks.
- Malformed and defective DNS request and response messages; DNS requests and responses used by hackers often differ from standard DNS messages because they are truncated, contain extra data in certain sections, have nonstandard characters in the domain names, or show inappropriate flags set.

A DNS security solution can also provide early warning of DDoS attacks based on DNS amplification and resource exhaustion. Observable signs include:

- Unusual-sized responses
- Atypical request and response rates for a requested domain
- Communications with domains or IP addresses known to be associated with botnets and DNS-related attacks
- Unusual patterns in the types of DNS records requested and returned (for example, an abnormal number of NXDOMAIN or “nonexistent domain” records)
- Spikes in the number of unique subdomains being queried
- Spikes in the number of timeouts and delayed responses from a server

Some enterprises have tried to perform similar analysis using security information and event management systems. However, this approach requires a huge amount of data inputs and ad hoc analysis. It also detects attacks after they have occurred.

The value of DNS security is emphasized by cybersecurity experts such as the authors of the Verizon 2014 Data Breach Investigations Report,[13] who wrote:

> “Monitor your DNS connection, among the single best sources of data within your organization. Compare these to your threat intelligence, and mine this data often.”

Implementation Considerations

Before leaving our discussion of DNS security, it is important to note that implementation options are very important.

The ideal solution should offer options to:

1. Operate with detection and alerting alone; or
2. Combine detection and alerting with real-time blocking.

Detection may be useful in some cases, but there are certainly many situations where it is extremely desirable to cut off APT control and communications and DDoS attacks immediately.

[13] Verizon 2014 Data Breach Investigations Report (DIBR)

Software solutions are far more flexible than appliance-based products. Software solutions can be deployed on low-cost commodity hardware, and many can run in virtual environments. They also free enterprises from the worry that picking the wrong appliance model will result in unnecessary costs if the appliance is too big, or a costly replacement if traffic increases. The flexibility to operate in private and public cloud environments is also desirable, especially for enterprises interested in network functions virtualization.

Finally, the solution should be infrastructure-agnostic and not require a rip-and-replace of the current DNS infrastructure. A better approach is to provide a security layer in front of the existing DNS infrastructure. DNS security solutions that require specific equipment or depend on replacing the DNS infrastructure itself are extremely costly, result in vendor lock-in, and can cause interoperability problems if different business units or acquired companies have different systems.

Summary

DNS is a vital component of the Internet, but too many managers have perceived it to be no more than "plumbing." It is precisely this neglect, along with a number of technical weaknesses, that make the DNS infrastructure a very attractive target for cybercriminals and hackers.

DNS tunneling and exfiltration are often important elements of data breaches and advanced persistent threats. DNS amplification and reflection, and DNS resource exhaustion attacks have generated some of the biggest DDoS attacks on record.

For these reasons, no enterprise can afford to leave DNS as a hidden pipe through the fortress walls, an avenue where traffic is never inspected and never blocked. Instead, a DNS security solution should be implemented to carefully monitor DNS traffic, provide early warning, and prevent data breaches, APTs and DDoS attacks.

To find what might be hiding in your DNS traffic, visit www.cloudmark.com and sign up for a free traffic analysis.