paloalto NETWORKS

Top DNS-Based Attacks your Organization Should Know About

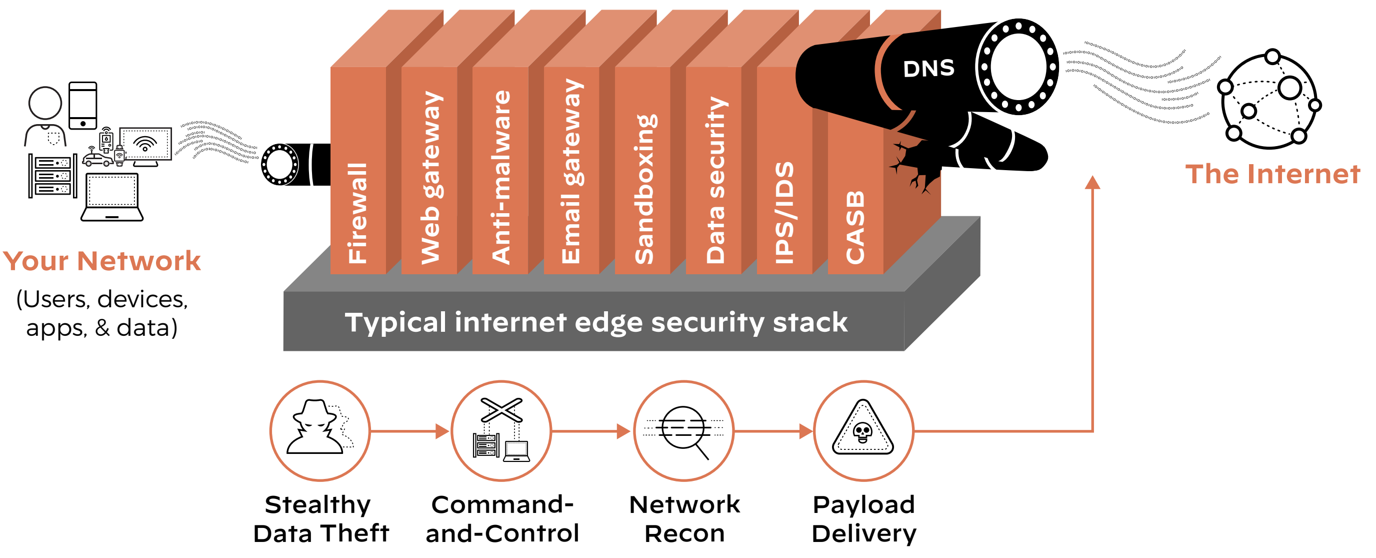
The Domain Name System (DNS) is one of the core foundations of the internet. Every user and device in your network uses DNS to translate domain names to IP addresses, meaning it is impossible to run your business without it. Yet, the lack of protection and ubiquity of DNS makes it an extremely tempting target for attackers.

87%
of organizations experienced one or more attacks using DNS in 2021[1]

42%
of organizations do not use a dedicated DNS security solution[1]

85%
of malware abuses DNS for malicious activity[2]

DNS is a bi-directional and internet facing protocol that carries a tremendous amount of data, making it an attacker's greatest tool. And adversaries today continue to innovate attacks by using a multitude of techniques to evade defenses and deliver malware, exfiltrate data and establish command-and-control.



Amongst the numerous types of DNS-layer attacks out there, here are some of the most commonly used:

Strategically Aged Domains

Attackers register domains months or even years before it is used for an attack in order to lengthen its life. By lengthening the life of the domain, attackers are able to bypass reputation-based checks done by security vendors. This attack can lead to data exfiltration or phishing attacks.

Compromised DNS Zones

Attackers hack legitimate domains to create subdomains and use them to launch phishing and malware attacks to users who think they are visiting a safe site.

Wildcard DNS

Wildcard DNS records allow attackers to redirect users to malicious sites via a nearly infinite number of domains they registered in bulk. Adversaries use this technique to deliver malware and launch phishing attacks.

Domain Generation Algorithms

Attackers continuously generate a number of domains that stay valid for only minutes, or even seconds, in order to bypass defenses and establish command-and-control. Legacy firewalls fail to prevent this attack because they are unable to keep up with the volume of domains as well as the rate in which they change.

Dangling DNS

By hijacking stale DNS zone entries that point to expired domains, attackers can impersonate legitimate domains and redirect traffic to their own site for malicious activities such as phishing, malware delivery, command-and-control and social engineering attacks.

DNS Tunneling

DNS Tunneling allows attackers to exfiltrate sensitive data in small chunks within DNS requests. With the amount of DNS traffic and requests a network typically sees, attackers are able to easily bypass security and exfiltrate data without being noticed.

The evolution of today's DNS-layer threats has made it more crucial than ever for organizations to have a solution that can secure their DNS traffic and prevent the latest attacks using DNS. With predictive analytics and machine learning-powered detections, Palo Alto Networks DNS Security subscription can protect your organization from modern attacks using DNS. Customers can benefit from the industry's most comprehensive solution that offers 40% more threat coverage than any other vendor.

Learn more about how Palo Alto Networks DNS Security can protect your organization from today's most sophisticated attacks using DNS.

[1] https://www.efficientip.com/resources/idc-dns-threat-report-2021/
[2] https://www.paloaltonetworks.com/resources/datasheets/dns-security-service