OVERVIEW

Deteque DNS Firewall: Improve security against malicious and compromised sites

Threat Intelligence updated every two minutes to block domains used by cyber criminals to steal data, carry out fraud and exploit legitimate systems. DNS Firewall blocks malicious domains and is a powerful tool in developing best practices across any enterprise.

What it is

Every day, millions of users, machine-to-machine updates and IoT devices rely on the Domain Name System and associated infrastructure to connect seamlessly to websites, cloud applications, eCommerce sites and other online services.

With connections taking place in a fraction of a second, you run the risk of connecting to domains that are used to install malware, ransomware, botnets or have been compromised by cyber criminals.

Security professionals can mitigate this risk by using Deteque's DNS Firewall to block access to malicious sites by preventing the DNS process from resolving to malicious domains and IP addresses.

Deteque researchers and automated systems gather information from across the internet to identify actively malicious domains, low reputation domains before they become active and compromised IP addresses to provide threat intelligence.

How it works

Without a DNS Firewall, a client queries a local DNS resolver and if the IP address for that domain is not included in its cache, it will query in turn an external root server, the Top Level Domain server and the domain server itself to get access to the site. The process will return both legitimate and malicious sites as there is no check in the process to exclude malicious domains.

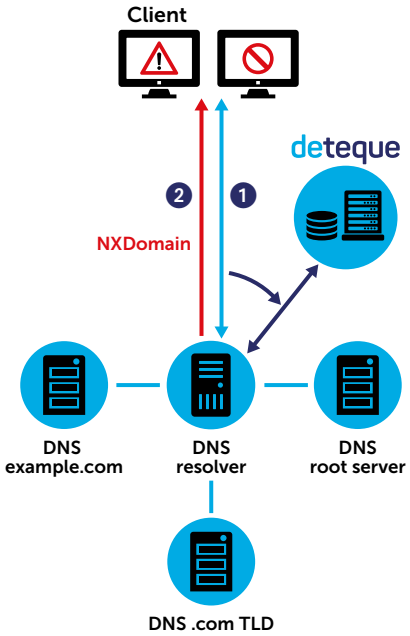
When a client initiates a query on a Deteque enabled nameserver, each step of the recursive DNS lookup process is analyzed to identify known bad domains, addresses and nameservers. If Deteque identifies a security risk the DNS server returns a 'does not exist' type answer which prevents access to the threat.

Each organization can customize the user warning page to include security awareness and best practice training messages. It's an essential step to make sure everyone across an organization contributes to online security.

Deteque's threat feeds can be delivered as a data query service, so it is a DNS Firewall acting on your behalf. For organizations operating larger commercial operations serving more than 5,000 users, Deteque domain-based reputation data is available via IXFR.

Benefits and features

- **Quick to implement**
  No extra hardware needed
- **Fast and accurate**
  Continuously monitored, delivered every 2 minutes
- **Reliable and trusted**
  Deteque researchers work constantly to update threat intelligence on your behalf
- **Easy to integrate**
  Available as a data feed in industry standard formats so no special customization required



1. Client queries local DNS resolver, which queries Deteque first
2. Deteque identifies malicious domain, allowing local DNS resolver to block domain query and also send warning to user

DNS Firewall Threat Feeds Overview

	Standard Feeds Full strength feeds that contain identified bad reputation and maliciousness	**Edited Feeds** Subsets of the Standard Feeds that contain the worst of the worst reputation domains	**Hacked Feeds** Compromised hosts or IPs not included in standard feeds
Bad Reputation Hosts	✓	✓	✓
BotnetCC Hosts	✓	✓	✓
Botnet Hosts	✓	✓	
BotnetCC IPs	✓		✓
Phishing Hosts	✓	✓	✓
Malware Hosts	✓	✓	✓
Adware Hosts	✓	✓	
Bad Nameserver IPs	✓		
Bad Nameserver Hosts	✓		
Bogons	✓		
Domain Generated Algorithm	✓		
Coinblocker	Externally curated feeds included with Deteque		
Tor Exit Nodes			
Zero Reputation Domains	Premium Feed for specialized use cases		
DROP	Free of charge and also included in commercial service		

Deteque – a division of Spamhaus

Deteque is a division of Spamhaus and integrated with a global network of service providers and a community of security researchers who are dedicated to combating malicious online activities.

Since 2008, Deteque has been at the forefront of securing networks by collecting, collating and delivering DNS-related threat intelligence to protect organizations in real-time.

Follow Deteque:

@deteque

@deteque

'Deteque' channel

www.deteque.com

Your contact:

deteque | A division of SPAMHAUS