The problem

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

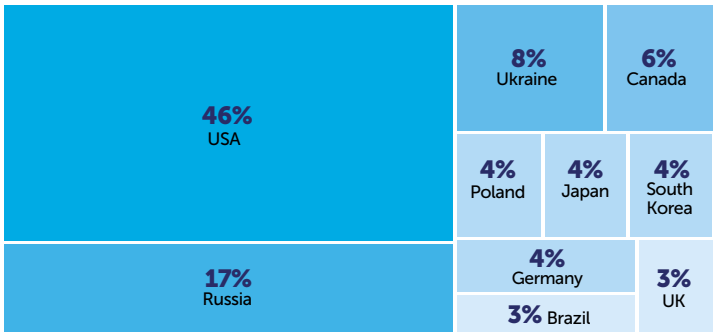
With connections taking place in a fraction of a second, you run the risk of connecting to domains that are used to install malware, ransomware, botnets or have been compromised by cyber criminals. Mitigate this risk by using threat feeds to block malicious sites, preventing the DNS process from resolving to malicious domains and IP addresses.

What to do now

Deteque is a division of Spamhaus so existing Spamhaus users can contact their usual local re-seller.

New users can sign up for a 30-day free trial: Contact us at www.deteque.com

It's global! Deteque index of top ten countries by number of bot infected domains



Adaptable network security

ISP – DNS Firewall provides protection for users without impacting the demand for high-volume, high-speed connectivity

Hosting – Cyber criminals are keen to abuse someone else's well-equipped network. Threat intelligence provides the hijacking protection you need.

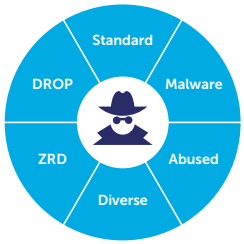
Hybrid – Many enterprises complement their own network with the systems of supply chain and distribution partners. DNS Firewall mitigates the risk of malicious connections introduced by external systems.

Hospitals and Universities – Open and easy access to a public network is essential, and with DNS Firewall you can minimize the risk of malicious connections initiated by high volumes of occasional users.

DNS Firewall The Deteque approach

Deteque's DNS Firewall evolves to stay ahead of the threats

Online fraud, disruption and exploitation take many forms so Deteque is always evolving to take into account new types of threats and new ways cyber criminals abuse the DNS process. Each threat feed is tailored to a particular type of threat; choose the feeds that are right for you.



Standard

Deteque's global research team works on your behalf to bring you the most comprehensive set of malicious domains on the internet. DNS Firewall provides automated protection from visiting malicious websites and domains (particularly useful as a defence against phishing).

Malware

Don't let cyber criminals abuse or hijack your network – these Malware zones block domains that are used specifically to abuse your systems.

Abused

Even the best run networks can be abused occasionally – Deteque keeps track of those that should be temporarily avoided.

Diverse

Cyber criminals change their methods constantly – this zone contains the datasets of varying and evolving threats.

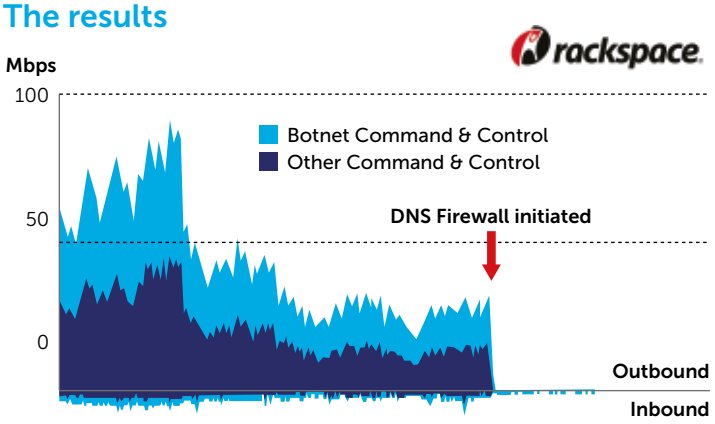
DROP

There are some domains that you should not connect to under any circumstances – Deteque has compiled a list of the 'worst of the worst'.

ZRD

Blocks connections to newly-registered and previously dormant domains for 24 hours. Domains are removed after 24 hours or transferred to another zone feed based on reputation assessment.

The results



DNS Firewall reduced outbound beaconing traffic from approximately 80 Mbs to almost zero immediately.

Security that works for your organization

When implementing Deteque's DNS Firewall you can set up the responses that are right for your organization's security policies and employee awareness programs.

Whitelists

Ensure that you keep essential connections in place.

Blocklists

Automatically block malicious domains and unsafe connections.

Advisory

Use a blocked return to send a customized warning message to users.

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 DNS abuse.

www.deteque.com

deteque | A division of SPAMHAUS