Early Warning for DNS Threats

DNS: the gateway to the Internet...

The domain name system (DNS) is the protocol that translates user-friendly domain names to computer-friendly IP addresses. It's what makes it easy for users to navigate the Internet.

...and a gateway for cybercriminals.

But, because DNS was designed with users—not security—in mind, cybercriminals have found ways to exploit DNS client/server communication, using malicious domains to exploit, infect, and cripple organizations.

10 M

malicious DNS requests are blocked by Quad9 on average, every day[1]

Malicious domains. Blocked.

Quad9, a partnership between IBM, Packet Clearing House and Global Cyber Alliance, closes the door on DNS attacks. This secure DNS service utilizes security intelligence from IBM X-Force Exchange and 18 other intelligence partners to block most malicious domains, botnet infrastructures, and malware to make the Internet a safer place.

Access to Quad9's information is easy through the X-Force Exchange API. This RESTful API supports multiple formats such as JSON and STIX/TAXII making it easy to integrate with IBM Security products—like QRadar, Resilient, and i2—as well as third-party security, and proprietary security systems.

Forewarning is forearmed

The X-Force Exchange API's new Early Warning Feed empowers security analysts to act against undergoing/upcoming attacks faster by providing early warning on hundreds of new malicious domains surfaced daily through IBM's collaboration with Quad9.

Deep-dive lifecycles on these domains and volumetric data on their activity provides timely, actionable intelligence that helps analysts stay ahead of threats.

IBM identifies malicious domains on an average of

8 days earlier

than other threat intelligence providers

Early Warning provides continual protection against:

Domain Generation Algorithms (DGA)

Prevents cybercriminals from establishing a communication channel back to a Command & Control server. DGA domains also indicate malware infections.

Squatting

Continually updates intelligence on malicious domains that impersonate legitimate domains.

Phishing

Helps to block phishing attempts by analyzing newly observed domains on Quad9.

Early warning = early action

As your attack surface continues to expand, the never-ending stream of new malicious domains makes it increasingly difficult to protect against upcoming threats.

The experts at IBM Security can help you stay one step ahead. Learn more about IBM X-Force Exchange API Early Warning Feed and start your free 30-day trial today!

Start your 30-day trial

1. IBM Threat Intelligence Index, 2019

IBM Security

IBM