Quad9 service aims to help protect users from attacks

November 19 2017, by Nancy Owano

(Tech Xplore)—IBM Security, in partnership with the Global Cyber Alliance and the Packet Clearing House, on Nov 16 launched a new free DNS service.

The DNS (Domain Name Service) was launched to help users enjoy Internet use with less security risks. Its backers are calling it Quad9 DNS—for a reason. Quad9 refers to the IP address 9.9.9.9.

Sean Michael Kerner, *eWeek*: "DNS is a foundational element of internet infrastructure, matching IP addresses with domain names."

Kerner explained the roles of the other two players, in addition to IBM.

"The Packet Clearing House is providing the network infrastructure for Quad9," said Kerner. It provides the network on which Quad9's packets travel.

The system development capabilities are delivered by the Global Cyber Alliance. GCA is described by *Ars Technica* as "an organization founded by law enforcement and research organizations to help reduce cyber-crime."

Supporters think the service could be a significant lesson for people to see how much safer the Internet and IoT could be.

So how does it work? Brandon Vigliarolo, *TechRepublic* said that it "uses threat intelligence from IBM's X-Force Threat Intelligence database, along with 18 other threat intelligence agencies, to compile a thorough blacklist of websites."

This is a feature that merits further mention. If the very idea of DNS to secure traffic is nothing new, Quad9 is special. John Todd, executive director of Quad9, talked about this in *eWeek*.

He said that the Quad9 security model is not just based on a single stream of threat intelligence data. In addition to IBM, they have "18 other threat intelligence partners who each contribute threats based on their own observations of the malware and phishing landscape."

Trying to navigate to a website known to contain malicious code? They have you covered. Quad9 will block it and "it won't return name

resolutions for sites that are identified via threat feeds the service aggregates daily," said Sean Gallagher in *Ars Technica*.

If the system detects that the site you want to reach is known to be infected, you'll automatically be blocked from entry.

The system is "primarily targeted at organizations that don't run their own DNS blacklisting and whitelisting services," said Gallagher, *Ars Technica*.

But with all this talk about blocking, does the service also filter content? The Quad9 site says No. "Quad9 will not provide a censoring component and will limit its actions solely to the blocking of malicious domains around phishing, malware, and exploit kit domains."

How does the service impact privacy?

Phil Rettinger, GCA president and chief operating officer, said in an interview with *Ars Technica* that the service is to be "privacy sensitive," with no logging of addresses making DNS request. Only geolocation data is kept, he said, in order to track the spread of requests associated with particular malicious domains. "We're anonymizing the data, sacrificing on the side of privacy."

The Quad9 site stated "There are no other secondary revenue streams for personally-identifiable data, and the core charter of the organization is to provide secure, fast, private DNS."

Vigliarolo commented, "If Quad9's ability to filter bad websites out at the DNS level is successful, one major element of cybercrime—spoof websites—could vanish overnight."

One can enable Quad9 by changing some network settings on the

computer. Quad9's website carries two [videos](#) for setup instructions, one for Apple computer setups (MacOS) and the other for Microsoft computer setups.

Setup is quite easy and takes four steps.

More information: quad9.net/#/

© 2017 Tech Xplore

Citation: Quad9 service aims to help protect users from attacks (2017, November 19) retrieved 20 March 2024 from https://techxplore.com/news/2017-11-quad9-aims-users.html