IBM UK Newsroom

IBM, Packet Clearing House and Global Cyber Alliance Collaborate to Protect Businesses and Consumers from Internet Threats

New Quad9 DNS Privacy and Security Service Designed to Protect Users from Millions of Malicious Websites

ARMONK, NY - 16 Nov 2017: IBM Security (NYSE: IBM), Packet Clearing House (PCH) and The Global Cyber Alliance (GCA) today launched a free service designed to give consumers and businesses added privacy and security protection as they access the internet. The new Quad9 Domain Name System (DNS) service helps protect users from accessing millions of malicious internet sites known to steal personal information, infect users with ransomware and malware, or conduct fraudulent activity.

Businesses and consumers can safeguard their online privacy as the Quad9 (9.9.9.9) DNS service is engineered to not store, correlate or otherwise leverage any personally identifiable information (PII) from its users. In contrast, other DNS services often capture Information about the websites consumers visit, devices they use and where they live for marketing or other purposes.

Quad9 provides an automated security solution at a time when it is needed most by consumers. New polling1 of consumers across the U.S., U.K., France and Germany released today found that just 27 percent of consumers think they are capable of staying ahead of the latest online threats and only 14 percent have ever changed the DNS settings on their computer.

To take advantage of the security and privacy of Quad9, users simply need to reconfigure a single setting on their devices to use 9.9.9.9 as their DNS server. Full instructions on what a DNS service does and how to switch to Quad9 can be found at www.quad9.net.

The protections delivered via Quad9 cover not only traditional PCs and laptops but can also be extended to internet connected devices (TVs, DVRs) or Internet of Things (IoT) technologies such as smart thermostats and connected home appliances. These devices often do not receive important security updates and are also difficult to secure with traditional anti-virus tools, yet remain connected to the internet leaving them vulnerable to hackers.

How Quad9 Works

With the launch of Quad9, consumers and businesses have a way of protecting themselves that is both effective and affordable with minimal configuration changes. Quad9 makes using security threat intelligence a hands-off effort and designed to give users “automated immunity” from known internet threats by automatically blocking access to known malicious websites.

Every website has a unique numerical address – known as an IP address. To make it easier to navigate the internet, those numeric addresses are translated to company names or words we can remember, understand, and search. Quad9 helps translate those numeric addresses into the URLs we are all familiar with, while adding in a layer of security and privacy before users land on the web address.

Whenever a Quad9 user clicks on a website link or types an address into a web browser, Quad9 checks the site against IBM X-Force’s threat intelligence database of over 40 billion analyzed web pages and images. The service also taps feeds from 18 additional threat intelligence partners including Abuse.ch, the Anti-Phishing Working Group, Bambenek Consulting, F-Secure, mnemonic, 360Netlab, Hybrid Analysis GmbH, Proofpoint, RiskIQ, and ThreatSTOP.

Quad9 provides these protections without compromising the speed that users expect when accessing websites and services. Leveraging PCH’s expertise and global assets around the world, Quad9 has points of presence in over 70 locations across 40 countries at launch. Over the next 18 months, Quad9 points of presence are expected to double, further improving the speed, performance, privacy and security for users globally. Telemetry data on blocked domains from Quad9 will be shared with threat intelligence partners for the improvement of their threat intelligence responses for their customers and Quad9.

Why is DNS Security Needed?

The stakes are high – cybercrime is estimated to cost the global economy more than $2 trillion by 2019. Cybercriminals use tools and techniques to build realistic-looking websites that mimic legitimate companies. These websites might even have names that look similar to a household national chain or a local store – but in reality, are not because they have a different IP address – something that most users would find hard to detect.

The problem is compounded by the fact that there will be 80 billion internet connected devices (or IoT devices) in homes and businesses by 2025. It has proven difficult for users to secure and update these devices, as software vulnerabilities and misconfigurations are discovered.

With Quad9 used in a home or business network at the router or gateway level, users will have an added level of protection for their IoT devices. These smart devices would also be blocked from accessing remote hosts which have been identified as being harmful or IoT botnets such as Mirai, which infected millions of IoT devices in late 2016.

Globally, regulations relating to security and privacy also continue to emerge. In May 2018, Europe will enact the General Data Protection Regulation (GDPR), a set of sweeping regulations meant to protect the personal data and privacy of its citizens. Quad9’s emphasis on data privacy is built with efforts like GDPR in mind.

How to Use Quad9

In four easy steps, consumers and businesses can have Quad9 filtering out websites that pose a threat to their devices and networks. Individuals or businesses can use this DNS service from their computer, router or network devices to resolve DNS requests and receive domain-blocking protection.

Setting up Quad9 is a simple configuration change. Most organizations or home users can update in minutes by changing the DNS settings in a central DHCP server (router or Wi-Fi access point) which will update all clients in a few minutes, with no action needed at end devices at all.

In order to start using Quad9 today, simply change your DNS settings in your device or router to point to 9.9.9.9.

Quad9 has laid out the four easy steps for Mac OS and Windows.

The Genesis of Quad9

Quad9 began as the brainchild of GCA. The intent was to provide security to end users on a global scale by leveraging the DNS service to deliver a comprehensive threat intelligence feed.

This idea lead to the collaboration of the three entities:

- GCA: Provides system development capabilities and brought the threat intelligence community together;
- PCH: Provides Quad9’s network infrastructure; and
- IBM: Provides IBM X-Force threat intelligence and the easily memorable IP address (9.9.9.9).

Quotes from Quad9 Partners

“Protecting against attacks by blocking them through DNS has been available for a long time, but has not been used widely. Sophisticated corporations can subscribe to dozens of threat feeds and block them through DNS, or pay a commercial provider for the service. However, small to medium-sized businesses and consumers have been left behind – they lack the resources, are not aware of what can be done with DNS, or are concerned about exposing their privacy and confidential information,” said Philip Reitinger, President and CEO of the Global Cyber Alliance. “Quad9 solves these problems. It is memorable, easy to use, relies on excellent and broad threat information, protects privacy, and security and is free.”

"PCH is pleased to participate in Quad9 by allowing the system to leverage our global network and infrastructure. Through local deployment of technology versus some distant datacenter, Quad9 works to significantly improve performance for the entire end-user experience and Internet transactions,” said Bill Woodcock, Executive Director, Packet Clearing House. “We strongly support the values Quad9 places on end-user privacy. The personal information protections and selectable DNS encryption, DNSSEC, and blocklist that are in place show that this project is in line with PCH's values. Quad9 will inspire trust in both individuals and businesses who understand the importance of securing their private browsing data.”

“Leveraging threat intelligence is a critical way to stay ahead of cybercriminals,” said Jim Brennan, Vice President, Strategy and Offering Management, IBM Security. “Consumers and small businesses traditionally didn’t have free, direct access to the intelligence used by security firms to protect big businesses. With Quad9, we’re putting that data to work for the industry in an open way and further enriching those insights via the community of users. Through IBM’s involvement in Quad9, we’re applying these collaborative defense techniques while giving users greater privacy controls.”

1 Four online surveys of 1,000 U.S. consumers, 602 French consumers, 633 German consumers and 611 United Kingdom consumers were conducted from Nov. 3-6. The U.S. polling has a margin of error of +/- 3.1% and the French, German and U.K. polls have a margin of error of +/- 4.0%

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. For more information, please visit www.ibm.com/security or follow @IBMSecurity on Twitter.

About Packet Clearing House

The Packet Clearing House is the international organization responsible for providing operational support and security to critical Internet infrastructure, including Internet exchange points and the core of the domain name system. For more info, please visit www.pch.net.

About Global Cyber Alliance

The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to confronting cyber risk and improving our connected world. Learn more at www.globalcyberalliance.org.

Contact(s) information

Nilima Patwardhan

UK External Relations +44 (0) 7921021329nilima.patwardhan@uk.ibm.com

https://uk.newsroom.ibm.com/2017-11-17-IBM-Packet-Clearing-House-and-Global-Cyber-Alliance-Collaborate-to-Protect-Businesses-and-Consumers-from-Internet-Threats