bfore.ai

Case Study

quad9

Stop a global botnet attack a month in advance

PreCrime Network

Situation

In their quest for continuous improvement, Quad9 was seeking to add value to existing users and enhance coverage of their Protective DNS.

Quad9 is a free service that replaces your default ISP or Domain Name Server (DNS) configuration. When a computer performs any Internet transaction that uses the DNS (and most transactions do), Quad9 blocks lookups of malicious hostnames from an up-to-the-minute list of threats. This blocking action protects homes and businesses networks, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets.

Impact

Bfore.ai and Quad9 forged partnership to augment protective DNS with PreCrime Network predictive cyberthreat intelligence.

The integration of Bfore.ai and Quad9 provides more than 30k of new and unique indicators of future cyber threats, enabling their customers to be protected by cyber attacks before they even start.

PreCrime Network with the predictive power of PreCrime, company's proprietary AI engine, brings sophisticated predictive capabilities to avoid domain-based attacks by offering forecasting of malicious attack vectors from six hours to multiple weeks in advance of attacks.

TL;DR

- Quad9 Protective DNS serve billions of resolutions each day, providing Internet protection worldwide
- Bfore.ai and Quad9 forged partnership to augment protective DNS with PreCrime Network predictive cyberthreat intelligence.
- On December 21st, a large botnet attack was blocked by prediction shared more than a month earlier
- The attack lasts 24 hours and produced 94,000 unique resolutions per minute.

About Bfore.Ai

The first truly predictive security solution. We help organizations prevent intrusions and data exfiltration by predicting vectors of future attacks, the information is used in #PreCrime for Network - predictive cyber threat intelligence to upgrade existing security solutions (firewalls, DNS resolvers, anti-phish filters, proxies, etc.) with foresight.

bfore.ai

How it happened

Quad9 saw immediate value in mid-December 2021 with it. Quad9 blocked an attack 30 days before it started. At its peak, the attack produced 94,000 unique resolutions per minute for over 24 hours. Bfore.ai predicted and delivered the malicious domain in early November 2021 and shared it with Quad9 for preemptive blocking.

- November 2021 - Bfore.ai predicted the malicious domain yuansuo(dot)xyz.
- Quad9 takes premptive actions and blocks newly predicted malicious domains by Bfore.Ai.
- 30 days later in December 2021 - Quad9 registerd more than 365 million hits from it.
- The attack lasts 24 hours and produced 94,000 unique resolutions per minute.

PreCrime Benefits

More than 3M daily scoring

Average 90k daily predicted malicious domains

<0.05% false positive rate

24/7 target detection and automated action rules

Easily integrated with existing platforms & by Restful API

We're excited to add Bfore.Ai to the Quad9 threat-intelligence portfolio and are impressed with the significant 'win' that was visible so soon after our deployment of their threat intelligence feed

Each and every one of these threat blocking events saves a user from being harmed, and we're pleased to be able to offer the benefits of Bfore.Ai's predictive threat technology to everyone.

Danielle Deibler, Director of Threat Intelligence for Quad9

Outcome

Anticipation and better analytical tools can make a difference in fighting domain names abuse, where time and accuracy are key factors. PreCrime predictive technology help organizations prevent intrusions and data exfiltration by predicting vectors of future attacks.

Contact Us Now

FR +33 7823 62484
sales@bfore.ai
https://bfore.ai