TCPWave®
Born in the Cloud, Made for the Cloud.

www.tcpwave.com

TCPWAVE'S PIONEERING APPROACH TO DNS SECURITY

Decoding the 2023 DNS Threat Landscape

As the modern world grows increasingly digital, the importance of the Domain Name System (DNS) – often referred to as the internet's phonebook – cannot be overstated. It's this very significance that makes DNS a prime target for cyber adversaries. Given the escalating threats, TCPWave, with its research-driven focus, has emerged as a cybersecurity leader, offering solutions that can detect, prevent, and alert on these attacks with unparalleled precision.

DNS: A Prime Target

The DNS plays an essential role in transmuting well-known names into numbers that computers understand, facilitating website access and email sending. But with its widespread use, DNS has become a hot target for attackers aiming to hijack corporate and confidential data. Recent findings from IDC's research reveal that the costs associated with DNS attacks have surged by 49%, with some attacks costing companies over $5 million. The multifaceted nature of these attacks, ranging from brute-force tactics to sophisticated internal network breaches, demands advanced mitigation tools.

TCPWave's Atlantis & XgBoost: Revolutionizing DNS Security

TCPWave's groundbreaking approach leverages state-of-the-art machine learning techniques, including Atlantis and XgBoost, to identify and thwart DNS attacks. These advanced methods have enabled TCPWave to achieve an astounding 98.5% accuracy in detecting network anomalies. In situations where potential threats are detected, TCPWave's defense mechanisms can automatically initiate corrective actions, such as shutting down a switch port, to ensure network integrity.

The 2023 DNS Threat Landscape

1. DNS Cache Poisoning Attack:

Cybercriminals utilize this method to redirect web users to fraudulent websites, attempting to steal information ranging from login credentials to credit card details. TCPWave's solutions, backed by the DNSSEC tool, ensure data authentication, thwarting these malicious attempts.

2. Distributed Reflection Denial of Service (DRDoS):

An attack aiming to cripple assets using a barrage of UDP responses. TCPWave emphasizes diversifying organizational assets and fortifying networks, ensuring they're resilient against such threats.

3. DNS Hijacking:

An attacker redirects traffic from genuine servers to malicious destinations. TCPWave's robust security protocols and monitoring ensure immediate detection and mitigation.

4. Phantom Domain Attack:

Attackers target the DNS resolver, causing performance issues or complete failure. TCPWave's intelligent algorithms can swiftly detect and neutralize such attacks.

5. TCP SYN Floods:

These attacks focus on exploiting the TCP handshake mechanism. With TCPWave's multi-faceted security program, organizations are equipped to detect and counteract such threats.

6. Random Subdomain Attack:

Attackers inundate a genuine domain with queries targeting non-existent subdomains. TCPWave's solutions can identify and neutralize these threats efficiently.

7. DNS Tunneling:

Cybercriminals utilize this to bypass interface controls or perform remote attacks. TCPWave’s advanced threat detection can promptly identify and halt such attempts.

8. Domain Hijacking:

Attackers exploit vulnerabilities to divert traffic. TCPWave's security protocols ensure that domain integrity remains uncompromised.

9. Botnet-based Attacks:

These involve multiple infected devices performing coordinated attacks. TCPWave's solutions can detect botnet formations and neutralize them swiftly.

10. DNS Flood Attack:

A massive influx of DNS queries aims to overwhelm servers. TCPWave's innovative techniques can filter out malicious traffic, ensuring continuous service availability.

The TCPWave Advantage

TCPWave's commitment to research and innovation in cybersecurity has established it as an industry leader. With a holistic approach encompassing detection, prevention, and timely alerts, TCPWave ensures that organizations remain safeguarded against the ever-evolving DNS threat landscape. In a world where cyber threats are escalating, trust TCPWave to shield your digital assets and maintain the sanctity of the DNS – the very backbone of the internet.

Contact Us for a quick demo on how to detect and prevent cybersecurity attacks.