Fingerprinting Malicious Traffic in DNS over QUIC

Hafiz Farooq, RSSAC, ICANN

Abstract

DNS-over-QUIC (DoQ) is a bigger cybersecurity problem as it's a difficult to selectively block malicious DoQ traffic (C2 Tunnels, UDP punch holes) in an enterprise network. Blocking the whole DNS-over-QUIC protocol actually restricts access to all QUIC and HTTP 3.0 based services to the enterprise users.

Therefore, enterprises have no other option except allowing QUIC protocol therefore posing a greater risk of exploitation of vulnerabilities in DNS-over-QUICK protocol. This presentation will highlight different fingerprinting guidelines which might be helpful in discovering such exploitations of DNS-over-QUIC protocol, by utilizing ML/AL algorithms.

Reference

[1] https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/
[2] https://sec-consult.com/blog/detail/better-dont-be-too-quick/

My Profile

I am a Senior Cyber Security Architect for **Saudi Aramco**'s Security Operations Centre (SOC) since last 8 years. He has around 20 years of experience of working in Data Center, Telecommunications & Security domains. He has also worked with Dell Inc and other telecommunication companies in the area of Network & Cyber Security.

He is currently member of ICANN's RSSAC Caucus, Universal Acceptance (UA) Working Groups and also presenting Saudi Aramco at ICANN's Business Constituency (BC). He is a fellow at ICANN75 (Kuala Lumpur, Malaysia), ICANN76 (Cancun, Mexico), ICANN77 (Washington DC, USA) and ICANN79 (San Juan, PR). He holds a master's degree in Next Generation Networks (**Aston University**, United Kingdom), Computer Engineering degree (**NUST, Pakistan**) and holds multiple routing and security certifications including JNCIP-SP (Service Provider), JNCIE-Security, SANS Forensic Examiner & Exploit Researcher, CISSP and CISM. He is also member of ISOC (Internet Society, Islamabad Chapter) and ISOC's Cyber Security Special Interest Group (SIG), and Forum of Incident Response Team (FIRST).