# **DNS**

Note : si plusieurs réponses alors le trafic est divisé

## — Combien de noms de domaines sont résolus et quand ?

2 à 0s (une double requête ipv4 et ipv6), 4 à 24s(double à chaque fois et même une triple car pas de reponse directement), 2 à 25s(requête wpad, cherche un proxy mais n’en trouve pas, 2 à 26s (pas sur que ca vienne de whatsapp)

Note : double requête pour s’assurer que l’app peut se connecter au serveur même si il est ipv4 ou ipv6

## --Quels sont les serveurs autoritatifs pour ces noms de domaines ? Sont-ils gérés par des entreprises différentes ?

a.ns.whatsapp.net appartient à whatsapp

## --À quelles entreprises appartiennent les noms de domaines résolus ? Il y en a-t-il d’autres que celle qui détient l’application ?

Latin American and Caribbean IP address Regional Registry (LACNIC)

Amazon, facebook,akamai(service de cache)

## — Quels sont les types de requête DNS effectuées ?

SOA,CNAME,A et AAAA (toujours une A et AAAA en même temps)

## — Lorsqu’une requête DNS souhaite obtenir une adresse IP, quelle est sa famille ? Il y a-t-il une version IP préférée par l’application ?

IPv4 et IPv6 a chaque fois

## — Les requêtes contiennent elles des records additionnels ? Le cas échéant, à quoi servent-ils ?

Non aucun, elles permettent normalement d’accélérer la recheche dns suivante

## — Observez-vous des comportements DNS inattendus ?

Non

# Couche reseau

## Lorsque IPv4 est utilisé, l’application utilise-t-elle des techniques pour traverser les NAT ?

Aucune idée

## Quels sont les adresses vers lesquels des paquets sont envoyés ?

## Retrouvez à quels noms de domaine elles correspondent, observez-vous une tendance particulière dans la famille d’adresse ? Pouvez-vous l’expliquer ?

# Couche transport

## Quels sont les protocoles de transports utilisés pour chaque fonctionnalité ?

Début : TCP pour message et texte car plus fiable, un peu d’udp pour appel car plus rapide(ajouter reference)

## Il y a-t-il plusieurs connexions vers un même nom de domaine ? Si oui, pouvez-vous l’expliquer ?

Déjà répondu avant

## — Si vous observez du trafic QUIC, quels sont les versions utilisées ? Pouvez-vous identifier des extensions négociées dans le handshake ?

Aucun quic(analyse wireshark) , surement pas utilisé par whatsapp

## Lorsque vous observez du trafic UDP, identifiez-vous d’autres protocoles que QUIC et DNS ? Expliquez comment ils sont utilisés par l’application.

Non TLS avec TCP mais pas UDP

# Chiffrement et sécurité

# L’utilisation du DNS est-elle sécurisée ? Comment ?

Non rien trouvé

## Quelles versions de TLS sont utilisées ? Précisez les protocoles de transport sécurisés par ces versions.

V1.2 et v1.3

## Quel est la durée de vie des certificats utilisés ? Par qui sont-ils certifiés ?

— Lorsque vous pouvez observer l’établissement du chiffrement, quels sont les algorithmes de chiffrement utilisés ?

tls\_aes\_128\_gcm\_sha25

## Si vous observez du trafic UDP, semble-t-il chiffré ? Comment est-il sécurisé ?