**Resumen:**

* Tomado de: “TrafficAV: An Effective and Explainable Detection of Mobile Malware Behavior Using Network Traffic”, Shanshan Wang et al

Los autores proponen un método llamado TrafficAV, que es efectivo, entendible y que detecta comportamientos malignos de malware para terminales móviles (Android) a través de su tráfico web. El tráfico web generado por las Apps es reflejado desde el punto de acceso inalámbrico hacia el servidor para el análisis de los datos. El análisis de datos, y la detección de malware se realizan en el servidor, por lo que consume lo más mínimo de recursos del terminal móvil sin afectar la experiencia del usuario.

Debido a la dificultad para identificar comportamientos maliciosos no similares de malware de tráfico web, TrafficAV realiza un análisis de tráfico web multinivel,

reuniendo tantas características del tráfico web como sea necesario. El método propuesto combina el análisis de tráfico web con un algoritmo de aprendizaje automático (árbol de decisión C4.5) que es capaz de identificar el malware de Android con alta precisión. En una evaluación con 8,312 aplicaciones benignas y 5,560 muestras de malware, el modelo de detección de flujo TCP y modelo de detección HTTP funcionan bien y alcanzan tasas de detección del 98.16% y 99.65%, respectivamente. Para el beneficio del usuario, TrafficAV muestra los resultados de detección y simultáneamente crea un mecanismo de puntuación para dar los motivos para tomar tal decisión. Esto permite a los usuarios investigar más adelante la contribución de cada característica en el resultado final, y captar las ideas detrás de la decisión final.

Características HTTP request header:

1. Host (This field specifics to the Internet host and port number of the requested resource.)
2. Request-Uri (The URI is from the request source.)
3. Request-Method (The method from HTTP indicates the action to be performed on the identified resource.)
4. User-Agent (This field contains information about the user agent originating the request.)

Características flujo TCP:

1. upBytes (Uploading bytes(client->server))
2. downBytes (Downloading bytes(server->client))
3. upPckNum (Total uploading packet number in a session(client->server))
4. downPckNum (Total downloading packet number in a session(server->client))
5. averageUpPckBytes (Average bytes of uploading packets(client->server))
6. averageDownPckBytes (Average bytes of downloading packets(server->client))