Informe tecnico

Nemotek

19 de julio de 2024

1. Resultados de la prueba de concepto

Whip Solutions ha llevado la prueba de concepto de DNS Filter en conjunto con Nemotek del día 28 de junio del 2024 al día 19 de julio del 2024, tras este proceso de PoC podemos visualizar la siguiente información en la plataforma de DNS Filter.

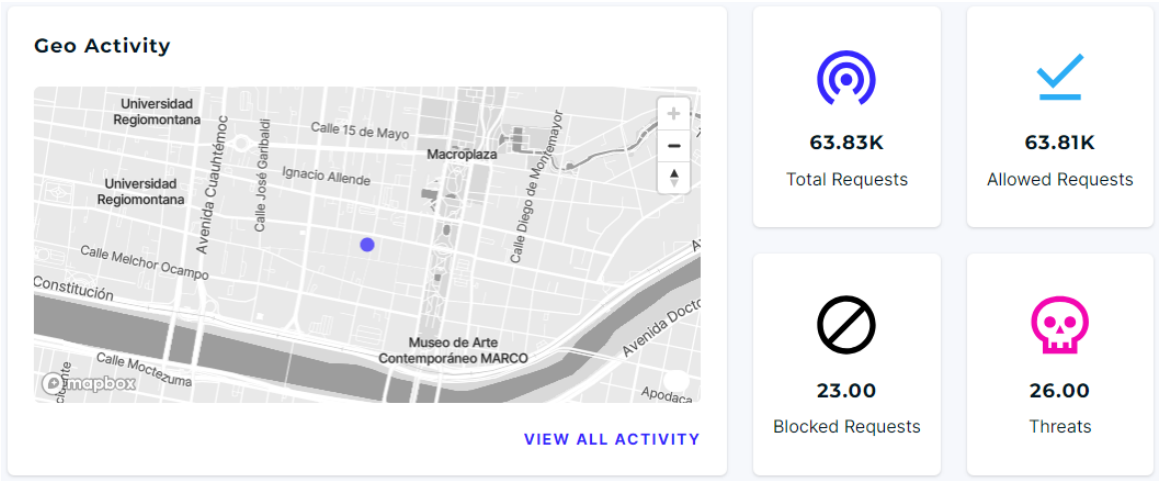


Figura 1: Vista General

Se puede observar el total de peticiones, peticiones permitidas, peticiones bloqueadas y las amenazas que se tuvieron durante dicho proceso, la prueba se llevó a cabo con 3 clientes que se instalaron sobre sus dispositivos, se desplegaron diversas políticas con las cuales se probaron las funciones de DNS Filter. Se configuró solo un sitio y de este se pueden obtener las siguientes métricas.

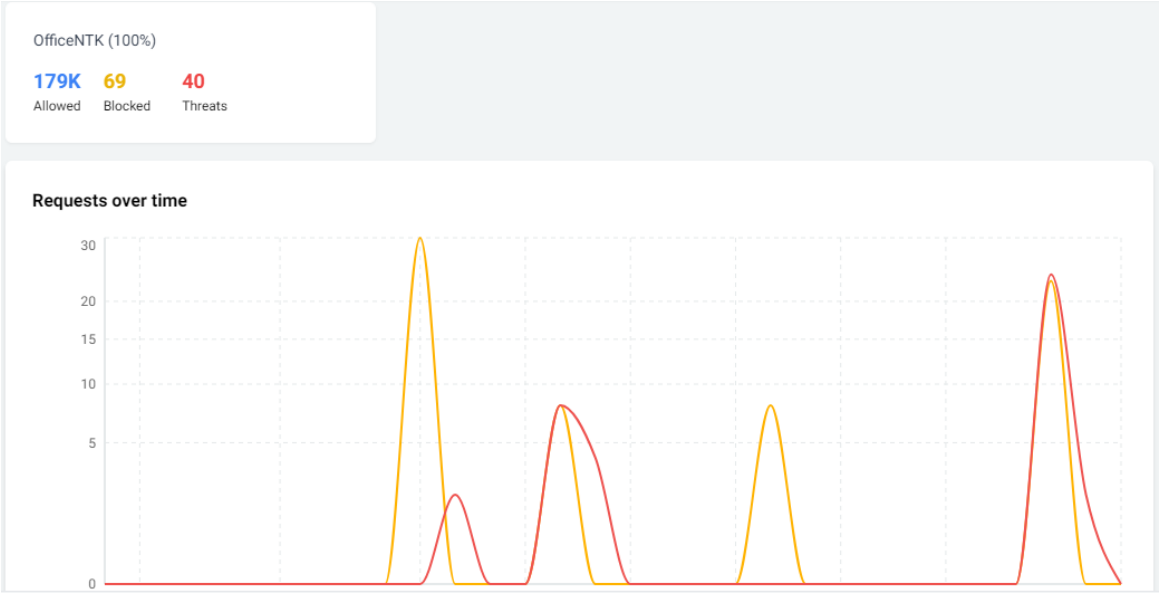


Figura 2: Métricas Totales

Podemos visualizar el top 5 de DNS más consultados en todo nuestro tráfico, además de las categorías a las que pertenecen. Se identificaron las amenazas que fueron bloqueadas y las que fueron permitidas. También se puede observar cuáles clientes realizaron más peticiones permitidas, cuáles peticiones fueron de amenazas y cuáles fueron bloqueadas. Además, se registraron los usuarios que realizaron todas estas consultas. Esto nos permite monitorizar el uso de los dispositivos y la red que estamos supervisando, brindando una vista completa de todas las consultas realizadas.

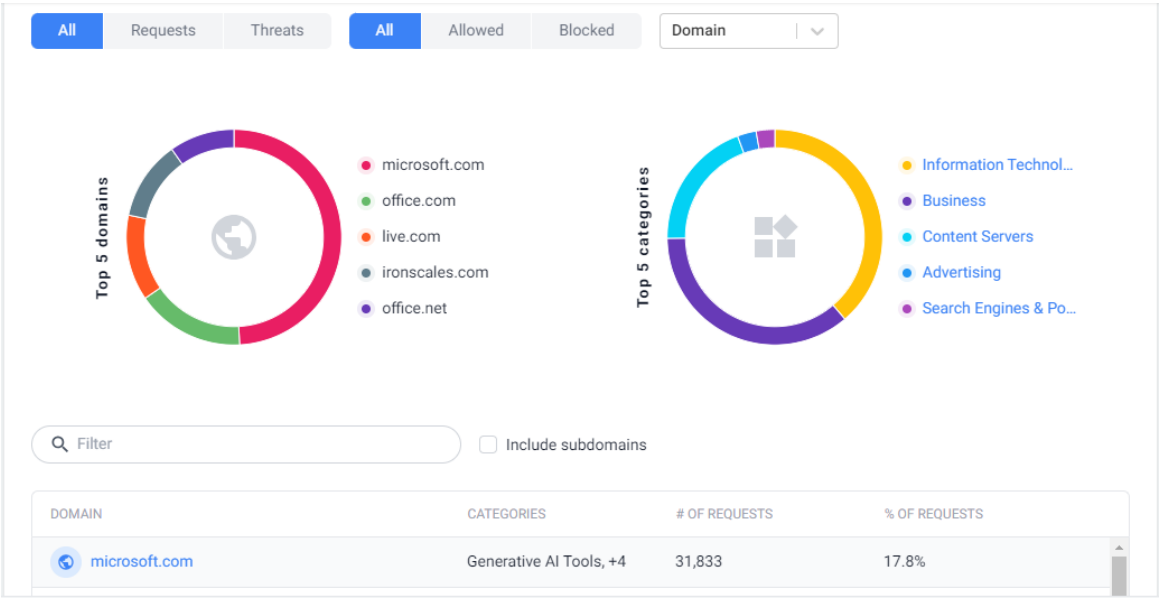


Figura 3: Top de DNS de las peticiones totales y categorías

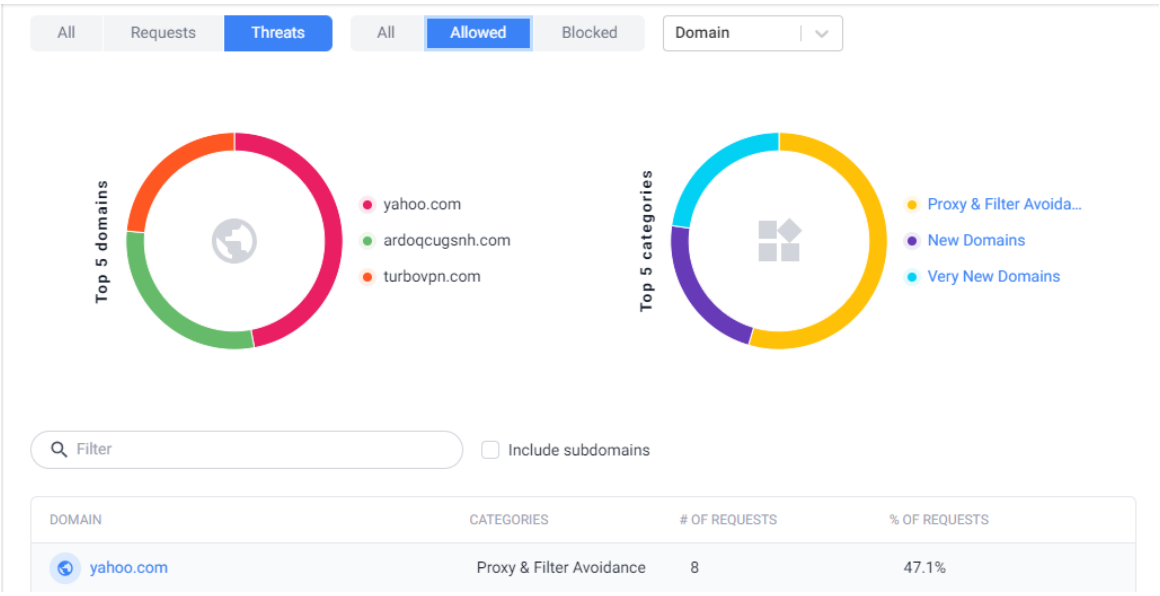


Figura 4: Top de DNS de las peticiones maliciosas permitidas

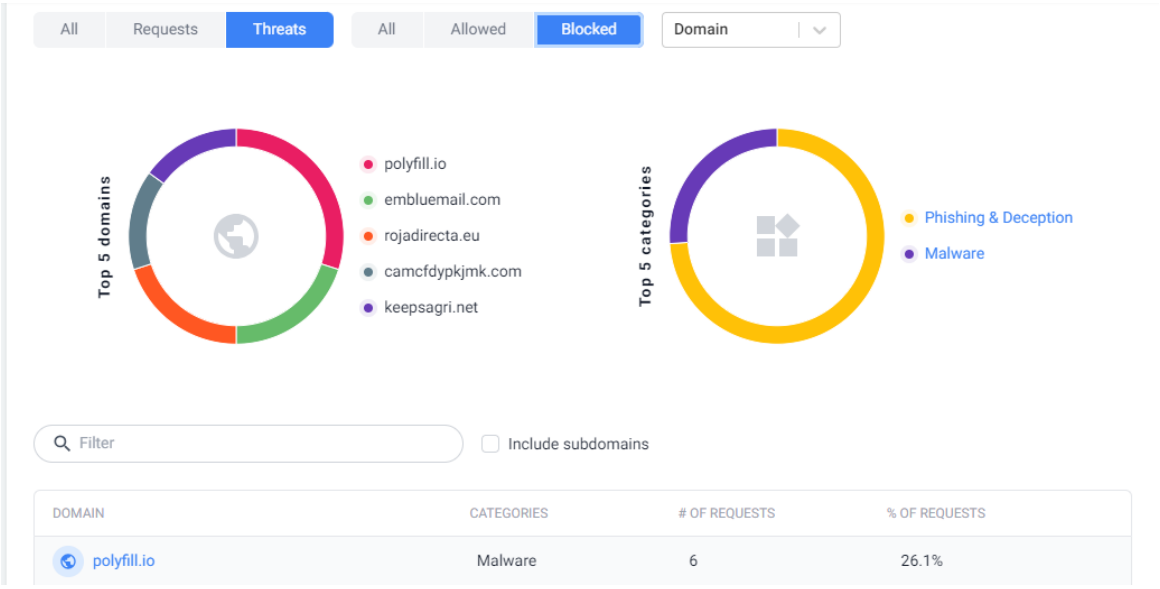


Figura 5: Top de DNS de las peticiones maliciosas denegadas

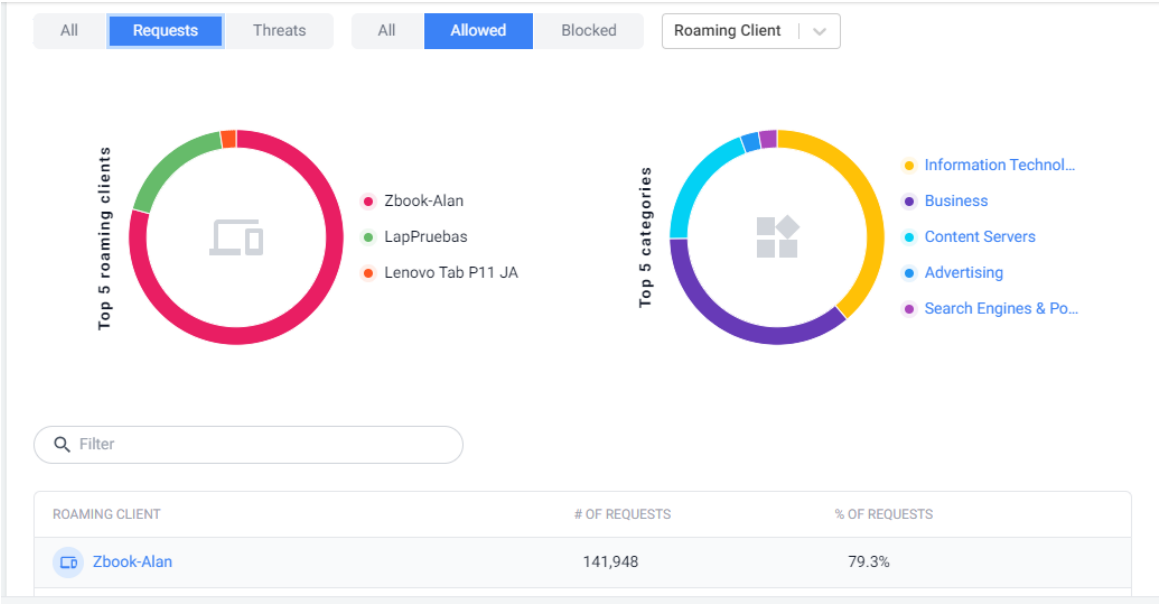


Figura 6: Top de Roaming client con peticiones permitidas

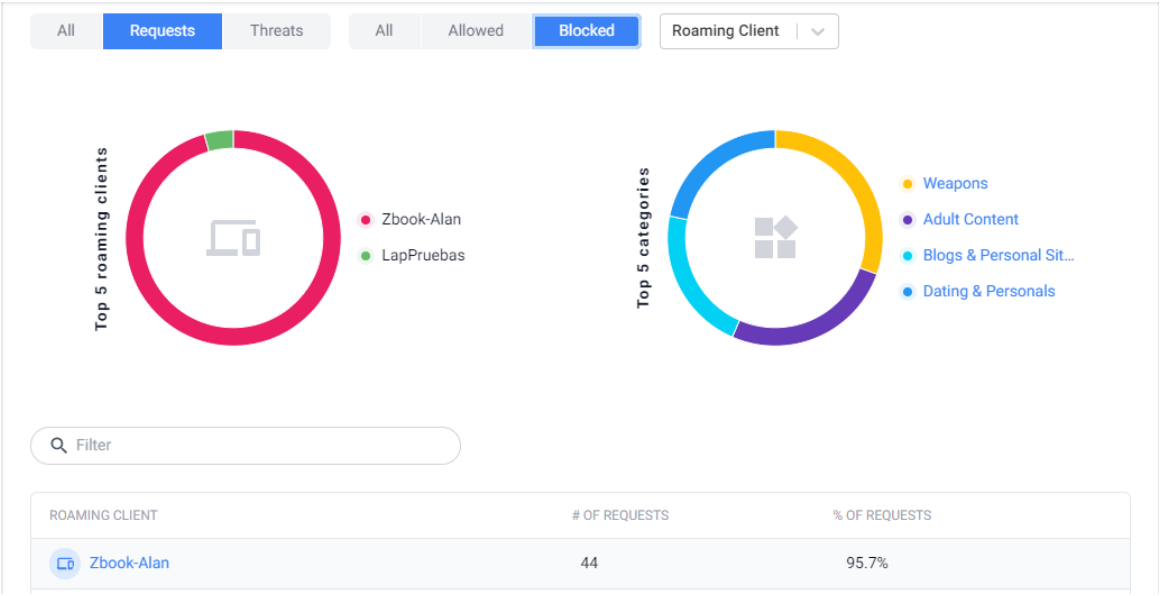


Figura 7: Top de Roaming client con peticiones denegadas

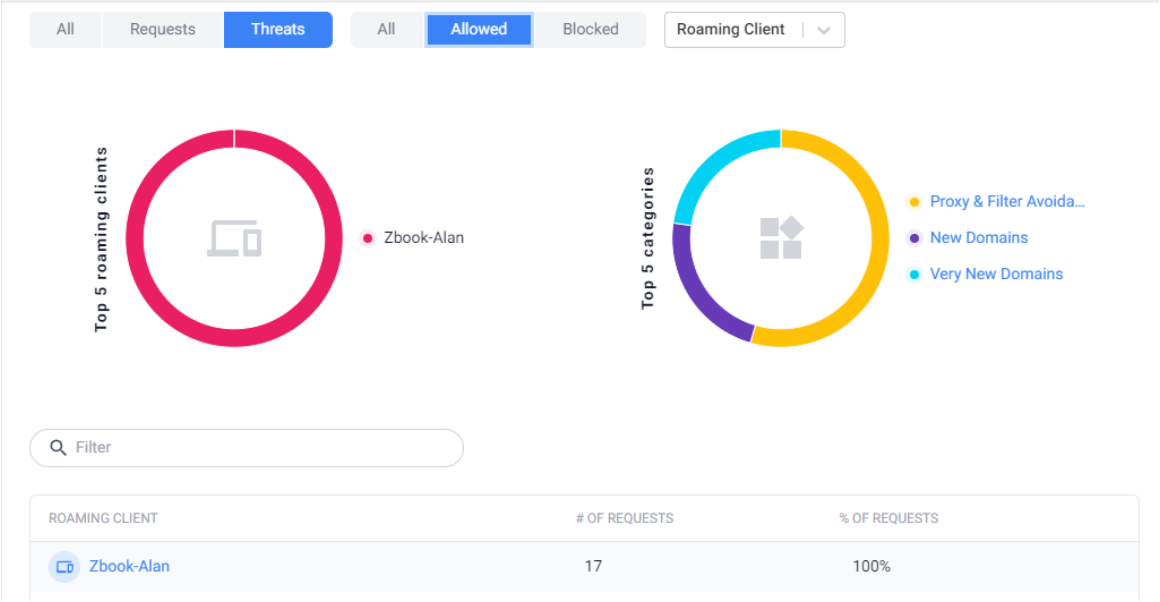


Figura 8: Top de Roaming client con peticiones maliciosas permitidas

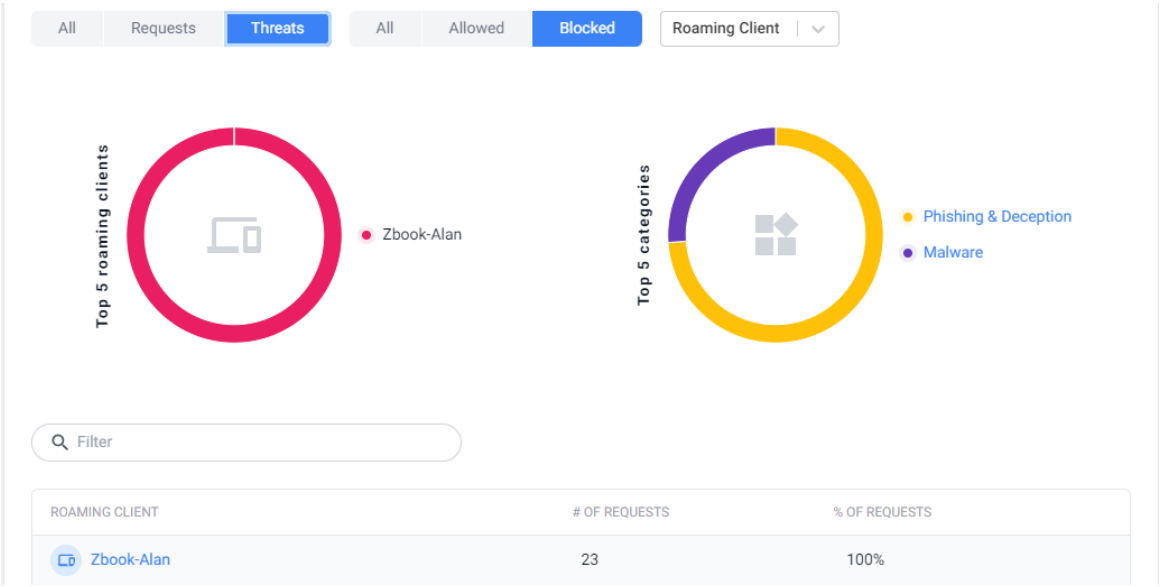
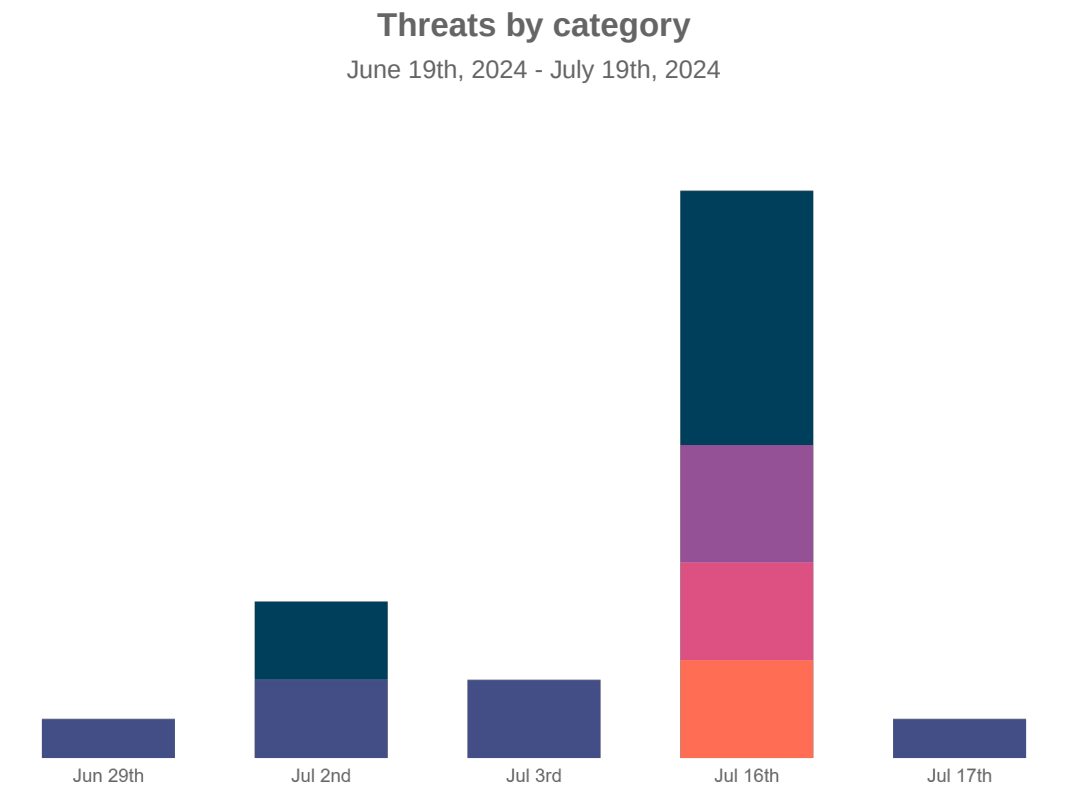
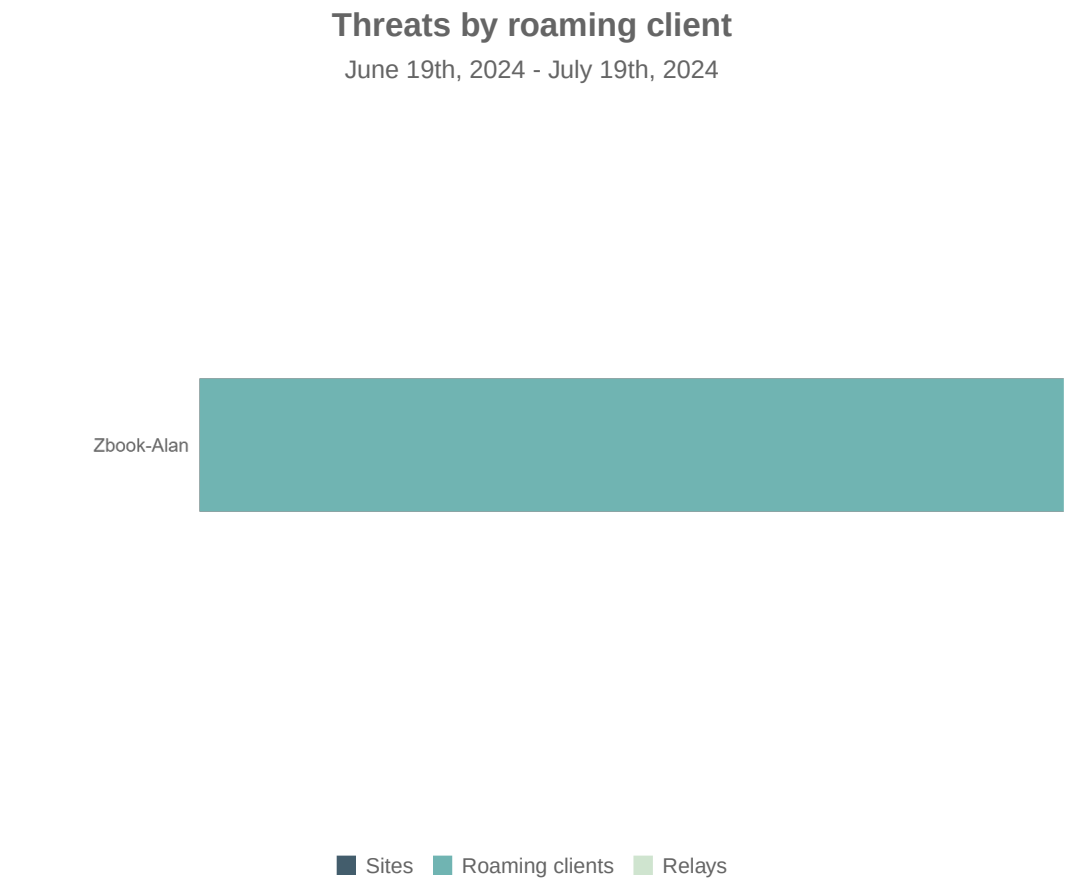


Figura 9: Top de Roaming client con peticiones maliciosas denegadas



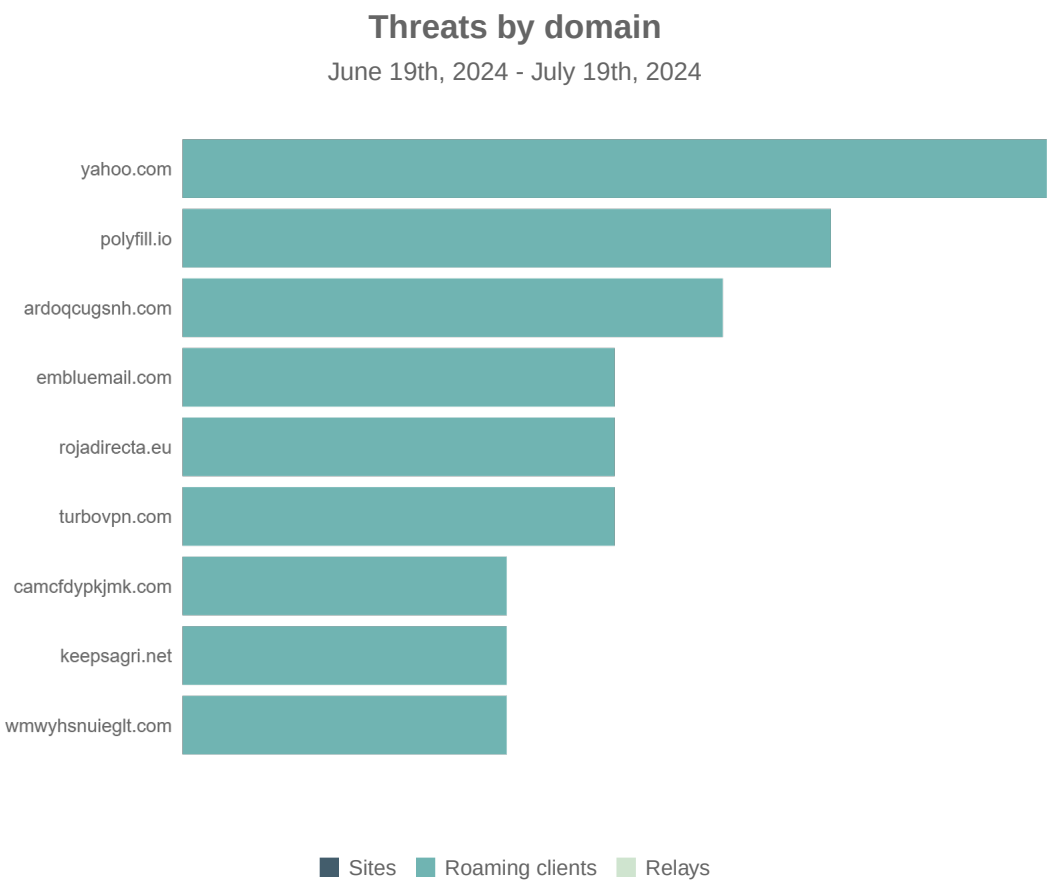
Category	# of threats	% of threats
Phishing & Deception	17	37.78%
Proxy & Filter Avoidance	12	26.67%
Malware	6	13.33%
New Domains	5	11.11%
Very New Domains	5	11.11%

Figura 10: Amenazas por categoría



Roaming client	# of threats	% of threats
Zbook-Alan	40	100.00%

Figura 11: Amenazas por cliente



Domain	# of threats	% of threats
yahoo.com	8	20.00%
polyfill.io	6	15.00%
ardoqcugsnh.com	5	12.50%

Figura 12: Amenazas por dominio

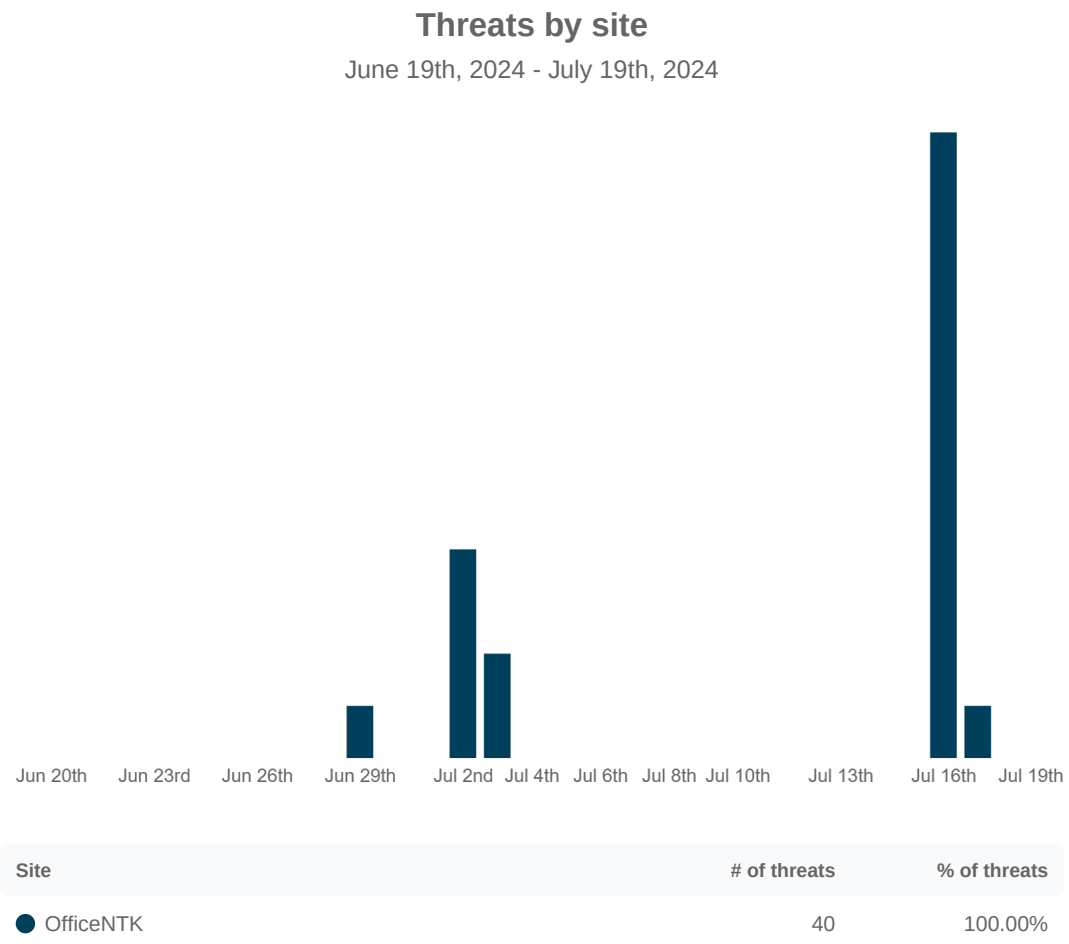
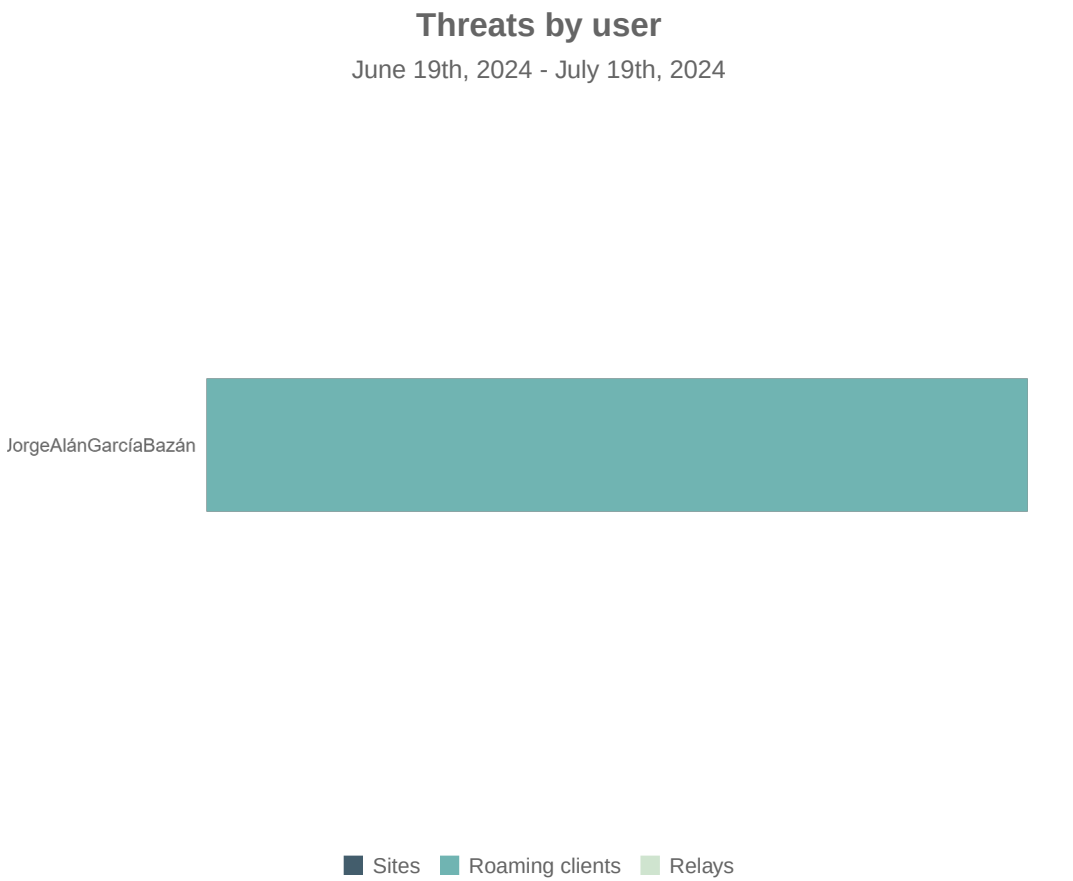


Figura 13: Amenazas por sitio



User	# of threats	% of threats
JorgeAlánGarcíaBazán	38	100.00%

Figura 14: Amenazas por usuario

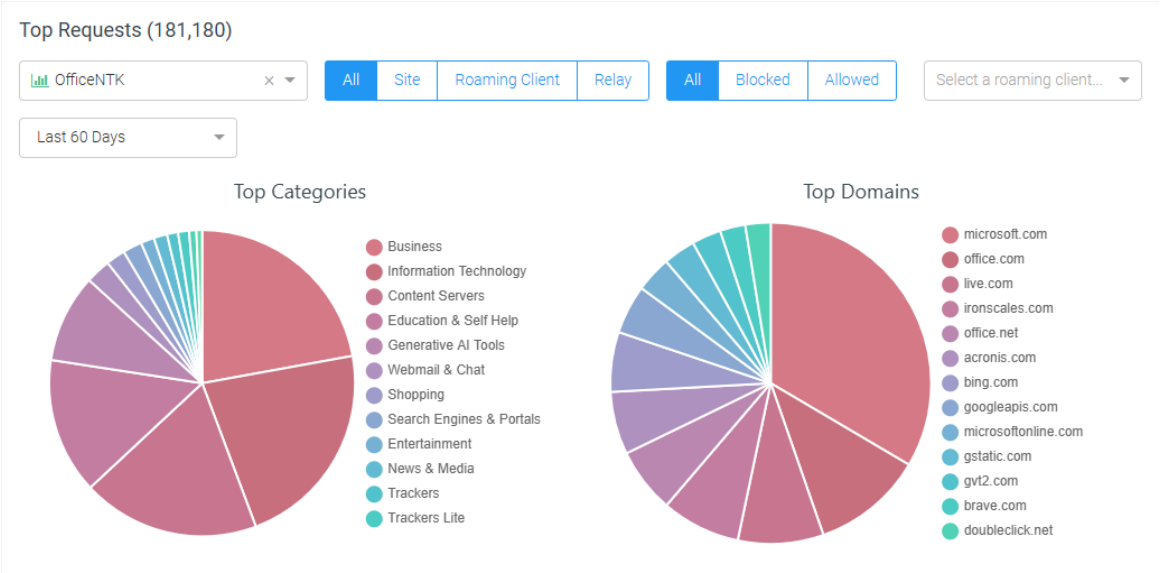


Figura 15: Peticiones totales permitidas

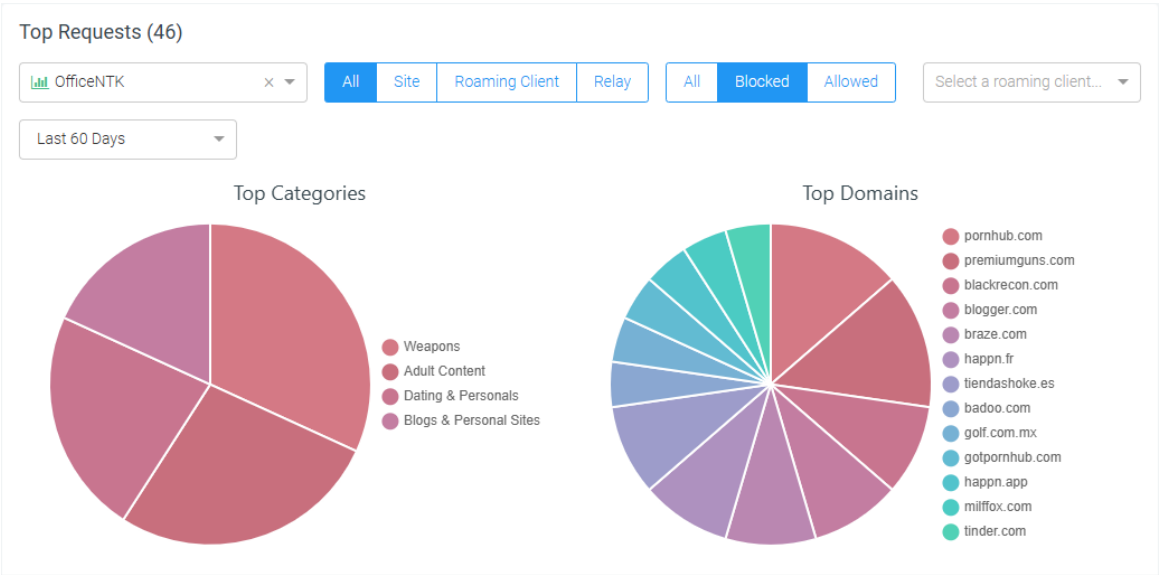


Figura 16: Peticiones totales denegadas

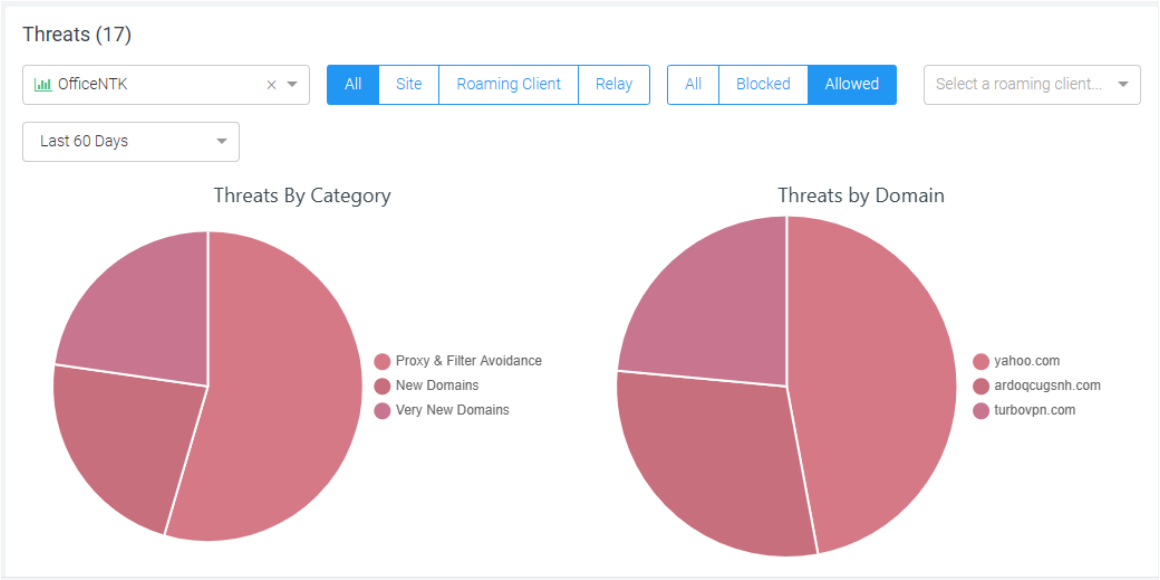


Figura 17: Amenazas totales permitidas

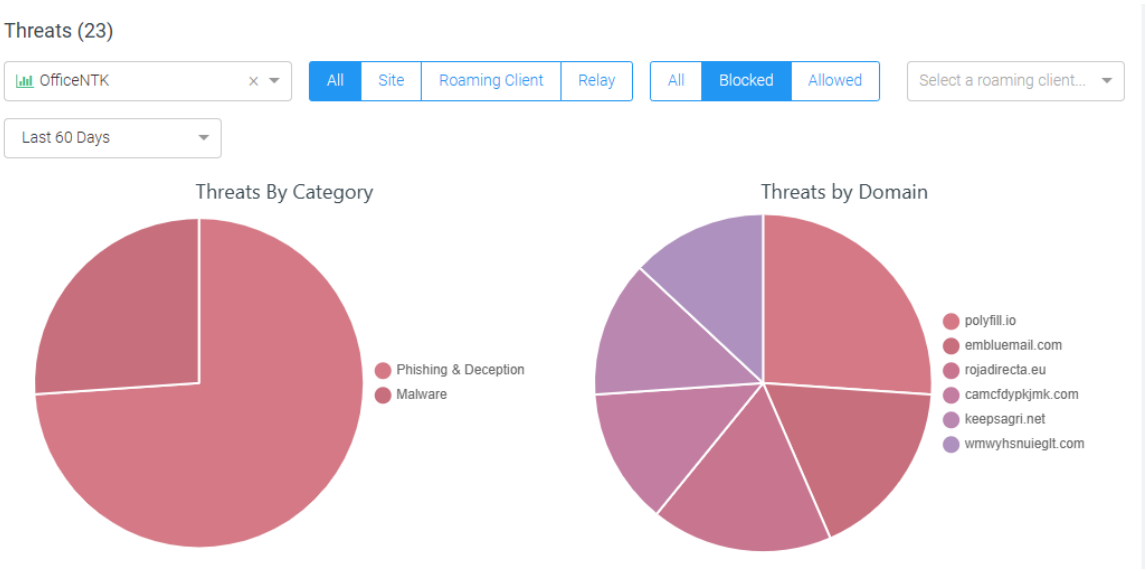


Figura 18: Amenazas totales denegadas

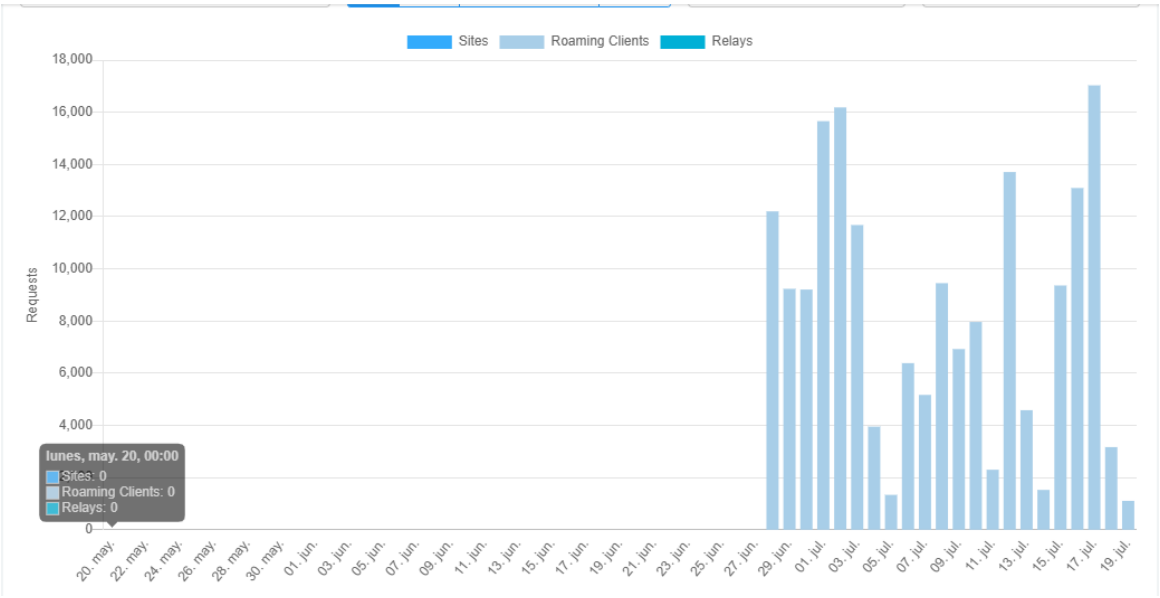


Figura 19: Trafico Total en la red