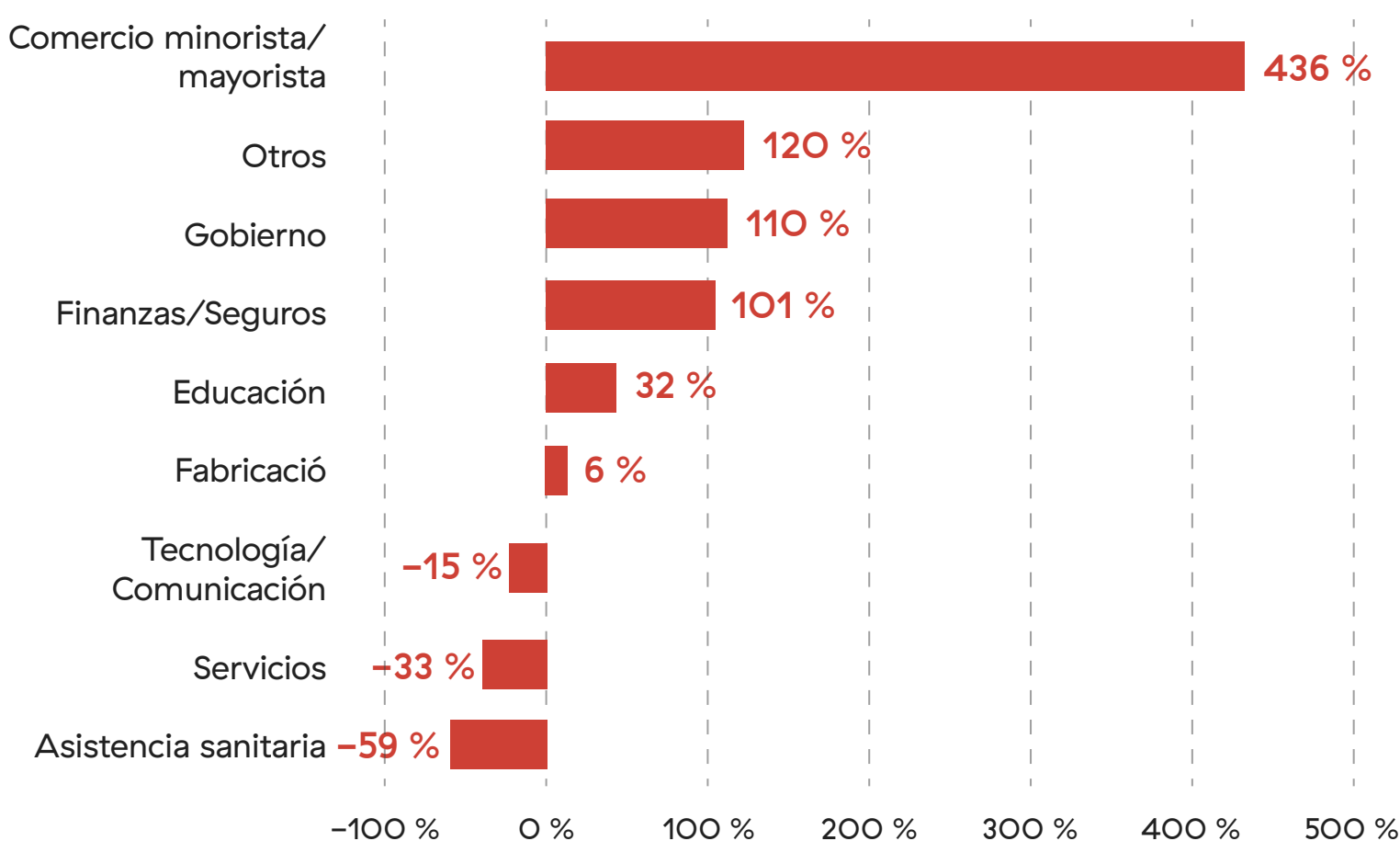


# Informe sobre el phishing 2022 de ThreatLabz

Según un estudio de ThreatLabz sobre los datos de la mayor nube de seguridad del mundo, el phishing aumentó un 29 % en 2021 frente a 2020.

La venta al por menor y al por mayor fueron los sectores con el mayor aumento de los ataques de phishing, con un 436 %.

Aumento porcentual en los intentos de phishing, 2021 frente a 2020

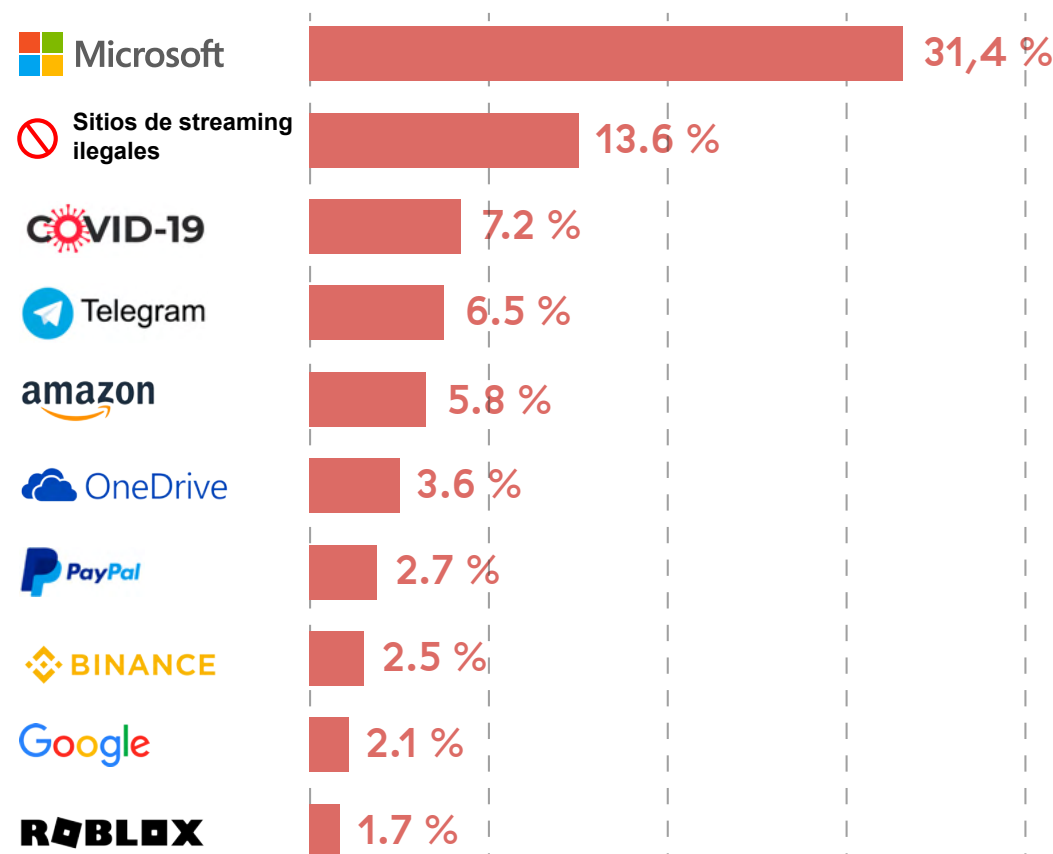


Entre los países más afectados se encuentran los Estados Unidos, Singapur, Alemania, los Países Bajos y Reino Unido.



Los ataques de phishing imitan a marcas populares y se aprovechan de eventos de actualidad

Temas principales en 2021



El phishing como servicio (incluidos los kits de phishing y los marcos de código abierto) permite realizar ataques con muy pocos conocimientos técnicos. Estos incluyen:

- Archivos web PHP/HTML
- Sistemas de distribución de tráfico
- Mecanismos de evasión de detección
- Métodos de exfiltración
- Entornos de control del back-end

## Proteja su organización del phishing

1

Comprenda los riesgos para diseñar mejor la política y la estrategia

2

Aproveche las herramientas automatizadas y la información sobre amenazas para reducir los incidentes de phishing

3

Implemente arquitecturas de confianza cero para limitar el radio de afectación de los ataques exitosos

4

Imparta la formación oportuna para fomentar la concienciación sobre la seguridad y promover la denuncia por parte de los usuarios

5

Simule ataques de phishing para identificar las vulnerabilidades en su programa

Para conocer más estadísticas, tendencias, predicciones y orientaciones, lea el

[Informe sobre el estado del phishing 2022 de ThreatLabz](#)