INTERPOL informó el martes que desactivó más de 22,000 servidores maliciosos asociados a diversas amenazas cibernéticas en el marco de una operación internacional.

Conocida como Operación Synergia II, el esfuerzo coordinado tuvo lugar del 1 de abril al 31 de agosto de 2024, y se centró en infraestructuras dedicadas al phishing, ransomware y robo de información.

> *"De las aproximadamente 30,000 direcciones IP sospechosas detectadas, se desactivó el 76% y se confiscaron 59 servidores. También se incautaron 43 dispositivos electrónicos, incluidos laptops, teléfonos móviles y discos duros"*, señaló INTERPOL.

Las acciones resultaron en el arresto de 41 personas, y otras 65 siguen bajo investigación. Algunos de los principales resultados en diferentes países incluyen:

- Desactivación de más de 1,037 servidores por parte de la policía de Hong Kong
- Incautación de un servidor y la identificación de 93 personas vinculadas a actividades cibernéticas ilegales en Mongolia
- Interrupción de 291 servidores en Macao
- Identificación de 11 personas relacionadas con servidores maliciosos y confiscación de 11 dispositivos electrónicos en Madagascar
- Incautación de más de 80 GB de datos en Estonia

Group-IB, uno de los socios del sector privado junto con Kaspersky, Team Cymru y Trend Micro, indicó que identificó más de 2,500 direcciones IP vinculadas a 5,000 sitios web de phishing, y más de 1,300 direcciones IP asociadas a diversas actividades de malware en 84 países.

David Monnier, evangelista principal de Team Cymru, dijo que su contribución incluyó *"la identificación y categorización de infraestructuras maliciosas"* tras un análisis detallado.

La primera fase de Synergia se llevó a cabo entre septiembre y noviembre de 2023, lo que condujo al arresto de 31 personas y a la identificación de 1,300 direcciones IP y URLs sospechosas utilizadas para ataques de phishing, malware bancario y ransomware.