Authorities across Africa have arrested 1,209 people and recovered nearly $100 million in a sweeping cybercrime crackdown coordinated by INTERPOL, officials announced Friday.

Operation Serengeti 2.0, carried out between June and August across 18 African nations and the United Kingdom, targeted ransomware groups, business email compromise (BEC) schemes and online fraud. Investigators dismantled more than 11,400 malicious online infrastructures linked to nearly 88,000 victims, according to INTERPOL.

“This global network is stronger than ever, delivering real outcomes and safeguarding victims,” said INTERPOL Secretary General Valdecy Urquiza.

In Angola, police dismantled 25 illegal cryptocurrency mining centres operated by 60 Chinese nationals. Authorities also seized 45 illicit power stations and IT equipment valued at more than $37 million. The Angolan government said the confiscated equipment would be repurposed to support electricity distribution in vulnerable communities.

Zambian investigators broke up a massive online investment scam that defrauded some 65,000 victims of an estimated $300 million. The fraudsters lured investors through heavy advertising campaigns that promised high-yield returns from cryptocurrency schemes, then directed victims to download apps to participate. Authorities arrested 15 suspects and seized domains, mobile numbers and bank accounts linked to the operation. In a separate raid, Zambian police and immigration officials disrupted a suspected human trafficking ring, seizing 372 forged passports from seven countries.

Officers in Côte d’Ivoire dismantled a transnational inheritance scam operating out of Germany. The scheme tricked victims into paying fees to claim fictitious inheritances, generating losses estimated at $1.6 million. Authorities arrested the alleged mastermind and confiscated cash, vehicles, jewellery, electronics and key documents.

The operation was strengthened by private sector collaboration, with partners including Fortinet, Group-IB, Kaspersky, Trend Micro and TRM Labs providing intelligence and training. Investigators took part in workshops on cryptocurrency tracing, ransomware analysis and open-source intelligence techniques ahead of the operation, which helped them act quickly on leads and identify offenders effectively.

Prevention was also central to the campaign. Through a partnership with the International Cyber Offender Prevention Network (InterCOP), investigators sought to identify and disrupt criminal activity before it occurred.

Operation Serengeti 2.0 was conducted under the African Joint Operation Against Cybercrime and funded by the United Kingdom’s Foreign, Commonwealth and Development Office. Participating countries included Angola, Benin, Cameroon, Chad, Côte d’Ivoire, Democratic Republic of Congo, Gabon, Ghana, Kenya, Mauritius, Nigeria, Rwanda, Senegal, South Africa, Seychelles, Tanzania, Zambia, Zimbabwe and the UK.