Cybercrime groups restructuring after major takedowns: experts

AFP- Cybercrime gangs are looking to rebuild with new tactics after global police operations this year made a huge dent in their activities, experts have told AFP.
The gangs have had a bad year so far, with law enforcement operations taking out some of prominent groups including LockBit, a loose network of largely Russian-speaking cyber criminals.

LockBit was one of the major developers of malicious software that allows criminals to lock victims out of their networks, steal their data and demand a ransom for its return.

Ransomware attacks using LockBit and other software have led to major disruption of governments, businesses and public services like hospitals.

Victims have paid hundreds of millions of dollars to gangs, usually in untraceable cryptocurrencies.

The disruption of LockBit in February and another network of malicious bots in May led to a "cleaning up" of the ransomware scene, said Nicolas Raiga-Clemenceau of the XMCO consultancy in France.

But he said "a number of new groups" had since appeared and started to organise themselves.

Allan Liska of US cybersecurity firm Recorded Future agreed and said there were worrying trends emerging with some of the new groups.

– 'Violence as service' –

Some of the newer gangs appeared to be considering threats of physical violence rather than just online intimidation, he said.

Liska pointed out that gangs would already have stolen a bunch of personal information, like the addresses of senior executives.

“And so if you’re not getting anywhere in your negotiations, that’s something you can threaten,” he said.

“We’re going to do something in the real world to hurt you or hurt your family.”

He called this “violence as a service”.

Liska and other experts are still assessing the new landscape, saying a bunch of new groups had emerged.

“There’s about a dozen of them that have popped up since the LockBit takedown, which is a higher number than we’ve ever seen in that short period of time,” he said.

They had all launched extortion websites that showed lists of victims, but it was unclear how effective the new groups would be, he added.

– ‘Bounce back’ –

LockBit’s operations were taken down by law enforcement in February.

The gang had targeted over 2,000 victims and received more than $120 million in ransom payments since it formed four years ago, according to US authorities.

Those targeted have included Britain’s Royal Mail postal service, US aircraft manufacturer Boeing and a Canadian children’s hospital.

The US authorities said hundreds of encryption keys had been

recovered and given to victims, and the network’s services had effectively been taken over.

But the software is still out there.

A gang attacked a government data centre in Indonesia last month using LockBit, asking for $8 million in ransom.

And experts interviewed by AFP agreed that ransomware attacks were likely to rebound quickly – possibly in the next few months.

“It’s going to bounce back,” said Liska.

“Right now there’s just so much money in ransomware that people don’t want to stop.”