BIZCOMMUNITY

# Ringleader behind thousands of online scams arrested in Nigeria

The head of an international criminal network behind thousands of online frauds has been arrested in a joint operation by Interpol and the Nigerian Economic and Financial Crime Commission (EFCC).


The 40-year-old Nigerian national, known as ‘Mike’, is believed to be behind scams totalling more than USD 60 million involving hundreds of victims worldwide. In one case a target was conned into paying out USD 15.4 million.

The network compromised email accounts of small to medium businesses around the world, including in Australia, Canada, India, Malaysia, Romania, South Africa, Thailand and the US. Financial victims were mainly other companies dealing with these compromised accounts.

Heading a network of at least 40 individuals across Nigeria, Malaysia and South Africa, which both provided malware and carried out the frauds, the alleged mastermind also had money laundering contacts in China, Europe and the US who provided bank account details for the illicit cash flow.

Following his arrest in Port Harcourt in southern Nigeria, a forensic examination of devices seized by the EFCC showed he had been involved in a range of criminal activities including business email compromise (BEC) and romance scams.

The main two types of scam run by the 40-year-old, targeted businesses: payment diversion fraud – where a supplier’s email would be compromised and fake messages would then be sent to the buyer with instruction for payment to a bank account under the criminal’s control; and ‘CEO fraud’.

In CEO fraud, the email account of a high-level executive is compromised and a request for a wire transfer is sent to another employee who has been identified as responsible for handling these requests. The money is then paid into a designated bank account held by the criminal.

‘Mike’ first came onto the law enforcement radar through a report provided to Interpol by Trend Micro, one of its strategic partners at the Interpol Global Complex for Innovation (IGCI) in Singapore. This, combined with actionable analysis and intelligence from Fortinet Fortiguard Labs in 2015, enabled specialists at the Interpol Digital Crime Centre, including experts from the Cyber Defense Institute based at the IGCI, and the EFCC to locate the suspect in Nigeria. This led to the suspects arrest in June.

Abdul Chukkol, head of the EFCC’s Cybercrime Section said the transnational nature of business email compromise makes it complex to crack, but the arrest sent a clear signal that Nigeria could not be considered a safe haven for criminals.

“For a long time we have said in order to be effective, the fight against cybercrime must rely on public/private partnerships and international cooperation,” said Chukkol.

“The success of this operation is the result of close cooperation between Interpol and the EFCC, whose understanding of the Nigerian environment made it possible to disrupt the criminal organisation’s network traversing many countries, targeting individuals and companies,” added Chukkol.

Noboru Nakatani, executive director of the IGCI, warned that BEC poses a significant and growing threat, with tens of thousands of companies victimised in recent years.

“The public, and especially businesses, need to be alert to this type of cyber-enabled fraud,” warned Nakatani. “Basic security protocols such as two-factor authentication and verification by other means before making a money transfer are essential to reduce the risk of falling victim to these scams.

“It is exactly through this type of public and private sector cooperation that Interpol will continue to help member countries in bringing cybercriminals to justice no matter where they are,” concluded Nakatani.

The 40-year-old, along with a 38-year-old also arrested by Nigerian authorities, faces charges including hacking, conspiracy and obtaining money under false pretences. Both are currently on administrative bail as the investigation continues.