ORGANISED CRIME GROUPS EXPLOITING HIDDEN INTERNET IN ONLINE CRIMINAL SERVICE INDUSTRY

29 Sep 2014

Press Release

The 2014 iOCTA (Internet Organised Crime Threat Assessment), published today by Europol's European Cybercrime Centre (EC3), describes an increased commercialisation of cybercrime.

A service-based criminal industry is developing, in which specialists in the virtual underground economy develop products and services for use by other criminals. This 'Crime-as-a-Service' business model drives innovation and sophistication, and provides access to a wide range of services that facilitate almost any type of cybercrime. The iOCTA report highlights that, as a consequence, entry barriers into cybercrime are being lowered, allowing those lacking technical expertise - including traditional organised crime groups - to venture into cybercrime by purchasing the skills and tools they lack.

Cybercriminals also abuse legitimate services and tools such as anonymisation, encryption and virtual currencies. The report highlights the abuse of Darknets that are used by criminals for the illicit online trade in drugs, weapons, stolen goods, stolen personal and payment card data, forged identity documents and child abuse material. This 'hidden internet' has become a principal driving force in the evolution of cybercrime and represents a highly complex challenge for law enforcement.

Adding to the complexity of the dynamic cybercrime picture, the 2014 iOCTA emphasises that criminals predominantly operate from jurisdictions outside of the EU which, combined with outdated legal tools and insufficient response capacities, allows them to operate with minimum risk.

"The inherently transnational nature of cybercrime, with its growing commercialisation and sophistication of attack capabilities, is the main trend identified in the iOCTA. It means that issues concerning attribution, the abuse of legitimate services, and inadequate or inconsistent legislation are among the most important challenges facing law enforcement today," says Rob Wainwright, Director of Europol.

Mr Wainwright's concerns are shared by the EU Commissioner of Home Affairs:

"These days, almost anyone can become a cyber-criminal. This puts an ever increasing pressure on law enforcement authorities to keep up. We need to use our new knowledge of how organised crime operates online to launch more transnational operations. We need to ensure that investigations into payment card fraud and online child abuse don't stop at national borders," says Cecilia Malmström,

Commissioner Home Affairs."

The 2014 iOCTA delivers a set of recommendations for law enforcement to successfully address the evolving and trans-national nature of cybercrime in a diverse and flexible manner. Awareness raising, capacity building, standardisation of practices and procedures, international and cross-border cooperation, exchange of relevant information and intelligence, development of adequate and harmonised legislation, and the dismantling and disruption of the criminal infrastructures behind illicit online services online are among these proposals.

The report also highlights the important role that Europol's EC3 can play in the fight against cybercrime by providing a platform for the exchange of information and intelligence, as a source of technical and tactical expertise and by providing the support and coordination required for the joint, multi-national operations that modern cybercrime investigations demand.

The 2014 iOCTA is EC3's flagship strategic product. The report informs decision-makers at the policy, strategic and tactical levels about on-going developments and emerging threats in the field of cybercrime, affecting governments, businesses and citizens in the EU. The report will contribute towards the setting of priorities, in the context of the EU Policy Cycle against serious organised crime, for the Operational Action Plan for 2015 in the three cybercrime sub-areas: cyber-attacks, online child sexual exploitation and payment fraud.

Benefiting from its central position in supporting EU law enforcement in combating cybercrime, Europol's EC3 based the iOCTA on contributions from Member States and subject matter expertise from EC3 and other Europol departments. The work was further enhanced with input from the private sector and academia.

The joint INTERPOL-Europol Cybercrime Conference, starting on 1 October 2014 in Singapore, will provide the first opportunity for representatives from law enforcement, the private sector, academia and international organizations to discuss their cooperation in the light of the iOCTA findings and recommendations.

Click here for the ePub formats.

EN The 2014 iOCTA (Internet Organised Crime Threat Assessment) [11.4 MB]

EN IOCTA 2014 Summary-Findings and Recommendations [763.29 KB]

CRIME AREAS Cybercrime • Child Sexual Exploitation • Forgery of money and means of payment • Payment Fraud

TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/newsroom/news/organised-crime-groups-exploiting-hidden-internet-in-online-criminal-service-industry