**Fighting cybercrime in a connected world**

Interpol is the world’s largest police organization with 194 member countries. Its primary function is to assist law enforcement agencies around the world in combating all forms of national crime and terrorism. Interpol strives to make the world a safer place by working with other like-minded organizations to respond to today’s crime challenges. Additionally, the organization encourages an international commitment and partnership with the private sector to protect citizens, infrastructures, businesses, and investments from the threats of terrorism, cybercrime, and organized crime.

One of the crimes that Interpol continuously fights is cybercrime. On October 11, 2019, the organization published an article regarding a cybercrime conference that was aimed at fighting cybercrime in a connected world. According to the article, the conference brought together various cyber experts from law enforcement, private industry, international organizations, and academia for in-depth discussions on the latest cyber threats, trends, and strategies. They discussed new developments in technology which could be exploited by criminals but also used to benefit the police force. Interpol’s director of cybercrime Craig Jones, also mentioned that “the cybercriminal world is agile and adapting, connecting and cooperating in ways we never imagined even just a few years ago.” Hence, he mentioned that law enforcement must adapt to the continuously changing cyber environment. It must also adopt new techniques to prevent cybercrimes, identify offenses, patterns of crime, and lines of inquiry that are robust enough to justify a criminal investigation. During the conference, Interpol also presented the findings of its first cybercrime threat assessment report. The report provided an analysis of the latest cybercrime trends identified in different regions using the information provided by member countries, private partners, and open source intelligence. A trend identified by the report was a shift of malware from targeting computers to targeting mobile devices. This scenario is due to the fact that mobile devices are being used more and more frequently as payment platforms. Lastly, the conference addressed the rise of crypto jacking, a technique criminals use to remotely accesses victims’ system using malware and hijack the computing power to create cryptocurrency. Interpol concluded the conference by Steven Wilson, Head of Europol’s European Cybercrime Centre (EC3 stressing the importance of working together in the prevention, legislation, enforcement, and prosecution of cybercrimes.

References

https://www.interpol.int/en/News-and-Events/News/2019/Fighting-cybercrime-in-a-connected-world

https://www.interpol.int/content/download/5267/file/Cybercrime.pdf