UNODC
United Nations Office on Drugs and Crime

UNODC-ROSA's response to COVID-19: The LEA and Cybercrime Segment

The fallout of the COVID-19 pandemic is having profound impacts on society and the economy, and it is likely to influence, and shape organized crime and illicit markets.

With the enforcement of isolation and reduced social contact, and the reduced supply of essential commodities, particularly medicines, the criminal groups have started reorganizing themselves into greener pastures. With the sudden spurt in the demand for personal hygiene products and the preventive as well as the regular medicines for usual health conditions like hypertension, diabetes, rheumatoid arthritis, pain killers, insomnia, etc. there is a shortage to meet the heightened demand, especially when users are tempted to store the stock for a few weeks if not months.

Several agencies, including INTERPOL have reported large scale supply of fake medical items[1], particularly anti-flu and anti-viral preparations, various testing kits, vaccines, preventive masks, sanitizers, and even antiseptic solutions.[2]

Further, to sell these products, several online have for e-commerce apps have surfaced.[3] With simple techniques of Search Engine Optimization (SEO), these sites and apps surface as preferred ones and easily trap the innocent victims. Once the sites are opened, they become potential source for access to bank details.

Social media platforms are also reported to be used and even fake calls are made to entice the victims in making online payments by faking a call from the hospital where the near and dear ones are hospitalized.[4] Further, fake news requires moderation of content across social media

[1] Operation Pangea, https://www.securingindustry.com/pharmaceuticals/fake-coronavirus-meds-prominent-in-2020-operation-pangea-/s40/a11481/#.Xn2gaIgzaUk

[2] Globally, 2,000 online advertisements related to COVID-19 were found and more than 34,000 fake or substandard masks, unlicensed products called 'corona spray', 'coronavirus packages' or 'coronavirus medicine', and dodgy diagnostics kits and surgical instruments were intercepted.

[3] Shopify registered more than 500 ecommerce sites for COVID or coronavirus in last two months. https://www.nytimes.com/2020/03/24/business/coronavirus-ecommerce-sites.html

[4] Facebook-owned WhatsApp has seen a 40% increase in usage that grew from an initial 27% bump in the earlier days of the pandemic to 41% in the mid-phase. For countries already in the later phase of the pandemic, WhatsApp usage has jumped by 51%. In individual markets, that usage may be even higher. For example, WhatsApp usage in Spain was up 76%. https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19-pandemic/

platforms.[5] The charity and investment scams are also on the rise.[6] Fake news on behalf of non-descript or low performing medical companies suggesting a breakthrough in treatment can spurt the stocks and can be encashed quickly by scamsters.

The phishing and personal data stealing for bank frauds has also seen a rise.[7] Trojan and self-executing phishing files are uploaded into the devices, including mobiles, computers and tablets by interlacing them to the sensational social media messages, which itself could be fake.[8] Thus, it hurts the society both ways – spread of fake rumor and the stealing of personal data, including passwords.

As the demand reduction among the addicts has always been a tall order. The supply, it appears, continues to a large extent.[9], Further it is noticed that supplies of illicit drugs are being concealed and morphed through the essential commodities and services. A regular exchange of information could keep the LEAs more vigilant, without disrupting the supplies. There is a need to study the repercussions of the squeezed supply due to lockdown on the regular drug users.[10]

The related issue is of the cybercrime. The vulnerabilities of the system become highly prone to be exploited by the criminals, including cyber terrorism, where the hospital, health-security, logistics and related supplies platforms can be breached and disrupted. With major lockdowns, frontline dealers are seeing the effect of people being progressively moved off the streets, which is their major point of sale. This may also prompt a shift to online and dark-web markets.

In the light of the above, several urgent steps are recommended by UNODC-ROSA specifically for the LEAs specifically for South Asia:

1. Set up a multi-agency cyber vulnerability cell and monitor closely the complaints of cyber-frauds.

[5] Facebook, Google, YouTube, Twitter, LinkedIn, Reddit and Microsoft have already started taking steps for content moderation, but it is also acknowledged that perhaps verification of fake a difficult terrain. https://www.lawfareblog.com/covid-19-and-social-media-content-moderation

[6] https://www.waff.com/2020/03/26/scams-look-during-covid-/

[7] New research from both KnowBe4 and Barracuda Networks has revealed the extent to which phishing campaigns during the Covid-19 pandemic could impact organizations. KnowBe4 benchmarking has found that 37.9 percent of users without social engineering awareness training will fail a phishing test, up 8.3 percent from last year, suggesting that non-specific cyber-awareness is declining. This comes while Barracuda Network researchers, who have been monitoring the global phishing activity surrounding the coronavirus outbreak, saw a rise of 667 percent in such incidents to date compared to February: a total of 9,116 phishing attacks directed related to the pandemic. https://www.scmagazineuk.com/wfh-awareness-training-becomes-important-covid-19-phishing-scams-increase/article/1678394

[8] The FBI's Internet Crime Complaint Center (IC3) has issued a public service announcement warning citizens to watch out for email-based fraud and malware schemes that take advantage of the coronavirus pandemic. https://www.scmagazine.com/home/security-news/cybercrime/fbi-warns-of-covid-19-phishing-scams-promising-stimulus-checks-vaccines/

[9] http://www.emcdda.europa.eu/publications/topic-overviews/covid-19-and-people-who-use-drugs_en

[10] http://www.emcdda.europa.eu/publications/topic-overviews/covid-19-and-people-who-use-drugs_en

2. Selectively monitor new apps which have emerged regarding the supply of medicines, essential commodities and health care products.
3. Selectively track the online fund flows to accounts which have been dormant or low balanced till recent past.
4. Launch a widespread awareness program among the public to avoid sharing personal details including banking details with unknown apps.
5. Educate families who are dependent upon internet as the basic source of communication in the times of lock down on safe internet usage, including frequent change of passwords, etc.
6. Instruct all banks to regularly share the online transmission data with Financial Intelligence Unit, and particularly the transfers which are made outside the state and country, as these could be for the promises that could seldom be fulfilled.
7. Establish a cyber intelligence-sharing center with regular reporting of the cases and modus operandi for the benefit of all participating Governments.
8. Online training programs can be organized for the benefit of the LEAs free of charge or on low cost basis to combat with emerging horizons of crimes.
9. Support civil-society groups and frontline social-service providers (e.g. teachers, social workers and youth groups) in delivering outreach to children and youth who are vulnerable to falling into criminal behaviour and being drawn into the activities of criminal groups looking to recruit new members.
10. Regular online webinars by UNODC at Regional level with the LEAs to apprise them of the latest updates and approach.