Advisory- CovidLock Ransomware

Humanity is facing a worldwide crisis. For the safety and betterment of its employees, NHA has taken a decision to fight the emergency by following the nation-wide lockdown for next three weeks. This has shifted the entire onus to "Work from home" infrastructure. Amidst the challenges faced during this catastrophe, there are certain opportunists, persuading people for their own benefit through cyberattacks. This is an opposite time for attackers to infiltrate organizational networks and steal data when major section of the IT industry is dependent on the internet for task completion.

When the researchers began monitoring all the COVID labelled domains, they came across certain websites that lured many users into downloading application under the disguise of a COVID-19 heatmap and awareness. Analysis on the application showed that the APK contained ransomware named CovidLock which delivers malicious payload to the devices and conducts a lock-screen attack against its victims.

CovidLock demands a ransom in bitcoins to the victims and if they don't pay the ransom within 48 hours, it warns of permanently delete all the contacts, videos, images, messages and other personal information on the phone. It also threatens to leak social media account user IDs and passwords on public online platforms.

It is difficult to identify how many fell into the prey of this attack. One thing that can be done to reduce the spread of this attack is to spread as much awareness as everyone can.

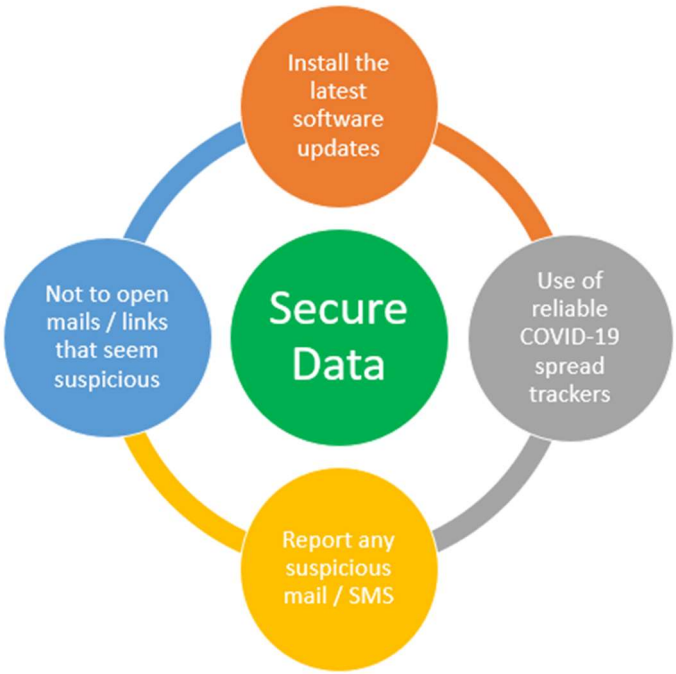

Figure 1: Do's and Don'ts for Working from home