Digital Forensics in the Era of Covid-19

The CoronaVirus (COVID-19) pandemic has caused the whole world to come to a stand-still. Sectors like tourism, manufacturing, service industry, etc. have taken a huge beating in the last six months and there has been a global slowdown in the first half of the year 2020. However, the IT industry has shown a lower growth rate at 3-5%. IT-Sector is expected to be impacted by the pandemic for a shorter period compared to others.

As India battles an alarming rise in corona positive cases, there's another villain already at the door and lurking into our private lives. This villain is none other than a cybercriminal targeting private individuals and their wallets. Home ministry officials say that there is an 86% increase in cybercrime activity in the months of April and May. From trying to sell the statue of unity in Gujarat for 4 billion dollars to scams for free mobile recharges for Jio and Netflix and has also seen a surge in phishing and spam emails in this period. Indian authorities have notified people from time to time to stay alert and not to give in to these scams.

The increase in this cyber activity happened due to a large mass of Indian working-class forced to work from home due to the pandemic. Cyber Criminals use this opportunity to target their wallets and private information. These threat actors range from script kiddies to government-sponsored actors to cyber terrorists.

All these factors have greatly impacted on the digital forensics sector. A market study states that a change in strategy is necessary to tackle the problems faced by this sector. Since people continue to work from home, forensics needs to instill a new methodology which goes hand in hand with societal goals of self-isolation and social distancing. While going forward in this environment, insider threats, intellectual property, and confidentiality breaches will rise. Significant acceleration in current working is needed for proactive and reactive analysis of these threats.

Artificial Intelligence (AI) and machine learning algorithms are needed to monitor heavy traffic and find any corruption or malicious activities by the user. The use of remote access will be necessary to capture and process misconduct by an employee. Data protection mechanisms have to be built to protect or encrypt important data from leaking out of the organization.

Monitoring of system logs and browser activity becomes mandatory to find out suspicious user behavior and suspicious logins. Secure procurement and transport of digital evidence like mobile phones or forensic images must be taken into consideration. The use of reliable file distribution methods has to be implemented and the use of safe virtual meetings is also necessary.

The use of robotic process automation and big data will be essential for proactive monitoring measures. Internet of Things (IoT) devices like drones and robots will be an additional data source for collecting and analyzing evidence. Cloud storage will be used to remotely gather digital data and evidence.

If these issues are not addressed, they can cause huge damage to the organization and individual user's privacy. The government and organizations need to rethink their cyber risks and containment methods.

For the sector of computer forensics, various techniques of analysis such as live analysis, cross drive analysis, stochastic forensics, etc have to be re-evaluated in this current COVID-19 crisis. By adapting to these new times, we bring a more diligent and resilient wing of computer forensics committed to solving cyber crimes and delivering swift justice.

Article by
Saket Thombre