COVID-19 based Cyber Attacks

June 23, 2020

Cyber attacks are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception. Cybercriminals are attacking the computer networks and systems of individuals, businesses and even global organizations at a time when cyber defences might be lowered due to the shift of focus to the health crisis.

What are Cyber Attacks?

A cyber attack is an **assault launched** using computers against a single or multiple **computers or networks**. A cyber attack can maliciously **disable computers, steal data**, or use a breached computer as a launch point for other attacks.

Cyber Attack types

- **Malicious domains:** There are a considerable number of registered domains on the Internet that contain the terms: "coronavirus", "corona-virus", "covid19" and "covid-19". While some are legitimate websites, cyber criminals are creating thousands of new sites every day to carry out spam campaigns, phishing or to spread malware.
- **Malware:** Cyber criminals are taking advantage of the widespread global communications on the corona virus to mask their activities. Malware, spyware and Trojans have been found embedded in interactive corona virus maps and websites.
- **Ransomware:** Hospitals, medical centres and public institutions are being targeted for ransomware attacks – since they are overwhelmed with the health crisis and cannot afford to be locked out of their systems, the criminals believe they are likely to pay the ransom.

How Cyber Attacks can be reduced?

Cyber Attacks in India

- India's cyber security nodal agency, CERT-In has issued an advisory warning that the potential phishing attacks could **impersonate government agencies and departments.** The phishing campaign is expected to start on June 21, 2020 with cyber attackers using email IDs such as "ncov2019@gov.in".
- The attackers are expected to send malicious emails under the pretext of local authorities. Such emails are designed to drive recipients towards fake websites where they are deceived into downloading malicious files or entering personal and financial information.

Source: Interpol Website, Bloomberg Quint