



Cyber Attacks

 drishtiias.com/printpdf/cyber-attacks-1

- Recently, the Nuclear Power Corporation of India Ltd. (NPCIL) has confirmed that a malware had infected its system at the **Kudankulam Nuclear Power Plant (KKNPP)**.
- The malware named '**Dtrack**' is a **new spyware tool** that is believed to be actively targeting a large number of **Indian institutions**, in order to steal confidential data as well as a **remotely downloading malicious tool**- tracking key logs and monitoring IP (internet protocol) traffic.

Dtrack was originated in **North Korea** by the hackers' group Lazarus.

- The attack revived the memories of **Stuxnet virus** attack on an **Iranian nuclear facility** in 2010.
- The acceptance of cyberattack in NPCIL systems highlights the fact that **nuclear reactors are not only prone to natural disasters but also to cyberattacks**.

Cyber Attacks Definition

- It is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.
- There are various **types of cyberattacks** like malware, phishing, denial of service attacks, etc.

Recent Instances of Cyber Attacks

- **WhatsApp** recently filed a lawsuit against Israel's NSO Group, alleging that the firm was incorporating cyber-attacks on the application by infecting mobile devices with malicious software.

Users affected included journalists, human rights activists, political dissidents, and diplomats.

- A massive cyber-attack took place at multiple targets in **Georgia** on October 28, 2019, taking down several websites.

Report on Cyber Attacks

According to the U.S. global computer security software company **McAfee**, the month of October 2019 saw the most terrible cyberattacks and cyber scares so far.

- The cyberthreats varied from malicious malware to restricting ransom wares.
- Malware like '**Ghostcat**' infects a user when the user visits a particular website and is served with a malicious advertisement. It collects the device information and eventually leads the user to malicious content. It **targets** the **mobile devices** in general.
- '**MedusaLocker**' is a **ransomware** (a type of malware) that makes its way into users' devices by encrypting files.
- According to the report, a technique called **steganography** is used which can hide malicious code inside a file that appears normal and allow hackers to bypass security software and firewalls.

Way Forward

- **Real-time intelligence** is required for preventing and containing cyber attacks. To achieve that, India needs to secure its computing environment and Internet of Things (IoT) with current tools, patches, updates and best-known methods in a timely manner.
- The need of the hour is to **develop core skills** in cyber-security, data integrity, and data security fields and setting up of **stringent cyber-security standards** to protect the institutional infrastructure of the country.

Source: TH