SHANKAR
IAS PARLIAMENT
Information is Empowering

Ransomware

Why in news?

\n\n

\n

- New Virus, Ransomware becoming a global threat in day-to-day computer handling.
\n
- The phenomenon that users of computers and researchers in cyber security were witness to from, May 13 has raised many questions of vulnerability.
\n

\n\n

What is the operation of the Ransomware?

\n\n

\n

- It is a type of malicious software **designed to block access to a computer system until a sum of money is paid.**
\n
- The intrusion was a phishing attack, persuading a user to open a mail sent by a motivated intruder, appears to be from a genuine and authorised source, and the result of a malware (WannaCrypt 2.0) assembled not at one place but in several centres across the globe.
\n
- The ransom demanded in each instance was $300 to be paid in Bit coin — a digital currency which renders the beneficiary anonymous and is difficult to locate.
\n
- One rough estimate is that the ransom-seekers **will eventually net $1 billion,** and that they have already received about $33,000.
\n

\n\n

What is the origin of Ransom ware?

\n\n

\n

- The malware was possibly stolen from a stockpile of weapons which **the National Security Agency (NSA)** had built up over the years as a counter-offensive to cyber-attacks on the US and its allies by nations such as Russia, China and North Korea.
  \n
- Shadow Brokers (whose exact identity is yet to be unravelled) had started posting online certain tools they had stolen from the NSA ‘armoury’.
  \n
- It revives memories of **Stuxnet,** a worm that both the US and Israel used against Iran’s nuclear programme more than five years ago.
  \n
- While there is no corroboration to the charge levelled against the NSA, it is interesting that a few former intelligence officers have taken the stand that the tools used in the latest episode were indeed from **the NSA’s ‘Tailored Access Operations’ unit.**
  \n

\n\n

What are the annoying aspects of the threat?

\n\n

\n

- There are two aspects to the outrageous attack that are worrisome.
  \n
- The first is that the holes in the older version of Windows were known to Microsoft, but **it did not do much to patch them up,** except for customers who paid to remove the deficiencies.
  \n
- The other theory is that customers who were aware of the risk **did not bother to act** because of the costs involved and the problems related to adapting to upgrades.
  \n
- Either way, this was a lesson to be learnt by both software manufacturers and users.
  \n

\n\n

What is the way forward?

\n\n

\n

- The final question is whether anything can be done to predict or prevent a similar attack, repeated appeal not to open attachments received from

unknown sources has fallen on deaf ears.
\n

- The only way is to minimise damage through encryption of vital, if not all the data in the hardware or system.
\n
- The speed of the attack was somewhat curtailed by counter-measures. But we still have to keep our fingers crossed for there is no knowing if the aggressors have more tools in their possession to cause further damage.
\n
- The good news for us is that there are no reports of any major intrusion into computers or systems in India.
\n

\n\n

\n\n

Source: Business Line

\n