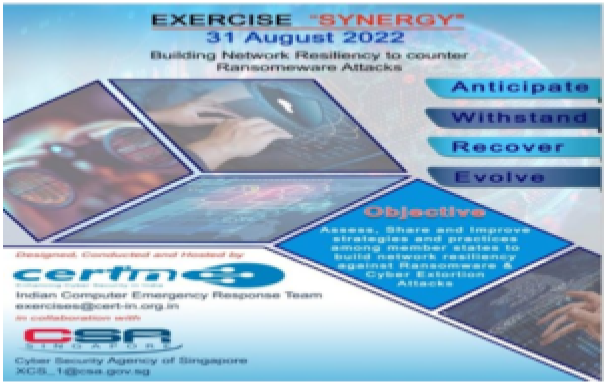
Cyber Security Exercise “Synergy”

September 1, 2022

In news– CERT-In under Ministry of Electronics & IT, in collaboration with Cyber Security Agency of Singapore (CSA), has successfully conducted the Cyber Security Exercise “Synergy”.

About the Exercise-

- It was conducted for 13 countries **as part of the International Counter Ransomware Initiative- Resilience Working Group** which is being led by India under the leadership of National Security Council Secretariat(NSCS).
- **The theme of the exercise was** “Building Network Resiliency to Counter Ransomware Attacks”.
- The exercise scenario was derived from real life cyber incidents, in which a domestic level (limited impact) ransomware incident escalates to a global cyber security crisis.
- Exercise “Synergy” was hosted by CERT-In on its exercise simulation platform.


EXERCISE "SYNERGY"
31 August 2022
Building Network Resiliency to counter Ransomeware Attacks
Anticipate
Withstand
Recover
Evolve
Objective
Assess, Share and Improve strategies and practices among member states to build network resiliency against Ransomware & Cyber Extortion Attacks
Designed, Conducted and Hosted by
certin
Indian Computer Emergency Response Team
exercises@cert-in.org.in
in collaboration with
CSA SINGAPORE
Cyber Security Agency of Singapore
XCS_1@csa.gov.sg

- **Each State participated as a National Crisis Management Team** having composition from different government agencies including National CERTs/CSIRTs, Law

Enforcement Agencies (LEA), Communication & IT/ICT Ministry and Security agencies.

- The specific **objective of the exercise was to Assess, Share and Improve strategies** and practices among Member-States to build network resiliency against ransomware & cyber extortion attacks.

What is Ransomware?

- Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.
- Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

Examples of Ransomware-

WannaCry:

- **A powerful Microsoft exploit was leveraged to create a worldwide ransomware** worm that infected over 250,000 systems before a kill switch was tripped to stop its spread.

CryptoLocker:

- This was **one of the first of the current generation of ransomware** that required cryptocurrency for payment (Bitcoin) and encrypted a user’s hard drive and attached network drives.
- **Cryptolocker was spread via an email** with an attachment that claimed to be FedEx and UPS tracking notifications.

NotPetya:

- **Considered one of the most damaging ransomware attacks,** NotPetya leveraged tactics from its namesake, Petya, such as **infecting and encrypting the master boot** record of a Microsoft Windows-based system.

- NotPetya leveraged the same vulnerability from WannaCry to spread rapidly, demanding payment in bitcoin to undo the changes.
- **It has been classified by some as a wiper, since NotPetya cannot undo its changes** to the master boot record and renders the target system unrecoverable.

Bad Rabbit:

- Considered a cousin of NotPetya and using similar code and exploits to spread, Bad Rabbit was a visible ransomware that appeared to target Russia and Ukraine, mostly impacting media companies there.
- Unlike NotPetya, **Bad Rabbit did allow for decryption if the ransom** was paid.
- The majority of cases indicate that it was spread via a fake Flash player update that can impact users via a drive by attack.

REvil:

- **REvil is authored by a group of financially motivated attackers**.
- It exfiltrated data before it encrypts it so that targeted victims can be blackmailed into paying if they choose not to send the ransom.
- The attack **stemmed from compromised IT management software used to patch Windows and Mac** infrastructure.
- Attackers compromised the Kaseya software used to inject the REvil ransomware onto corporate systems.

Ryuk:

- **Ryuk is a manually distributed ransomware application** mainly used in spear-phishing. Targets are carefully chosen using reconnaissance.
- **Email messages are sent to chosen victims**, and all files

hosted on the infected system are then encr.