Incident Prevention

1. Use firewalls to create a buffer zone between the Internet and other untrusted networks used by creating firewall rules to deny traffic by white-listing only authorized protocols, ports and applications to exchange data across the boundary to reduce the exposure of systems to network based attacks.

2. To limit the lateral movement as well as other attack activities, use end point / network firewall to prevent Remote Procedure Call (RPC).

3. Adopt application whitelisting policy on all endpoint workstations to prevent malicious code or unauthorized software from gaining execution on endpoints.

4. Remove unused or unpatched software from the computer, particularly remote desktop software, if any.

5. Ensure that application control (to allow only approved scripts to run) prevents unapproved programs running regardless of their file extension.

6. Ensure all end point systems having antivirus or a malware protection program running on it and is always up to date with latest signatures.

7. to prevent malicious scripts from running on click, the notepad program can be associated (with always use this app option) With script file extensions such as .hta, .js, .jse, .vbs, .vbe, .wsfand, .psl.

Incident Detection

1. Monitor DNS activity for potential indications of tunneling and data exfiltration.

2. Regularly check for configuration changes and appropriate usage of configuration for possible intrusion.

3. Block I Restrict connectivity to the malicious domains /lPs shared by various security agencies. Take the forensics image of the identified machine connecting to such domains after Isolating.

4. Restore the system to a last-known good back up or proceed to a fresh installation.

Incident Response

1. Disconnect the infected computers from LAN / Internet immediately;

2. Remove unused or unpatched software from computers, particularly remote desktop software, if any;

3. Change passwords of all email and online services from another secure computer:

4. Hard disks of the infected computers may be formatted after taking backup of data files;

5. Operating systems and applications should be re-installed from clean software;

6. Backup data should be scanned for virus before restoring it.