OFFICE OF THE DISTRICT & SESSIONS JUDGE, SOUTH EAST DISTRICT
SAKET COURT COMPLEX: NEW DELHI

No..8008-8015...../Cir./Computer/F.06/SD/Saket/17 Dated, New Delhi the ..19/05/17

Copy of a circular having endorsement no. 30986-31136/Cyber-sec/Comp/2017 dated 16/05/2017 from Chairman, Central Computer Committee, Delhi has been received in the office of Ld. District & Sessions Judge, South-East District and duly marked to Officer Incharge (Computer). Copy of the same is forwarded to all the Ld. Judicial Officers and A.O.(J)/Branch Incharge of all the branches in South East District, Saket Courts, New Delhi for information and necessary compliance.

Anil Kumar

(Anil Kumar)
Officer Incharge (Computer)
Saket Courts,
New Delhi

C Lady

OFFICE OF THE DISTRICT & SESSIONS JUDGE (HQs): DELHI

CIRCULAR

In view of recent cyber-attack Indian Computer Emergency Response Team (CERT-In) has already issued an advisory with regard to the Wannacry, or Wannacrypt, ransomware, which has affected computers in around 100 countries, including India. These malwares encrypt the computer's hard disk drive and then spreads laterally between computers on the same LAN. The ransomware also spreads through malicious attachments to emails. These malware are also targeting commonly used office file extensions such as .ppt (PowerPoint), .doc and .docx (Word), .xlsx (Excel) etc.

Keeping in view the above advisory, all the officials are directed to take back-up of all necessary files, avoid access to any unsolicited e-mail from office computer under any circumstance. All licensed window-users are requested to be in touch with respective Computer Branch for installation of relevant patches.

Preventive Measures and Tips are mentioned on the backside of this circular. For more information on security from the said ransomware, offcials may also visit http://webcast.gov.in/cert-in/ .

(Manoj Jain)
AD&SJ / Chairman,
Centrlized Computer Committee
Delhi

No. 30986-31136 /cyber-sec/Comp/2017 Dated 16/05/2017

Copy forwarded for information and necessary action to:

1. The District & Sessions Judge, North-West/South/South-West/West/South-East/East/New-Delhi/Shahdara/North-East/North District, Delhi/New Delhi with request to convey the same to all concerned posted within the respective District.
2. All the Presiding Officers posted at Central District, Delhi with request to convey the same to all the officials posted in their respective court.
3. The Officer In-charge/Nodal Officer/Administative Officer (Judl.)/Branch Incharge of all the Branches with request to convey the same to all the officials posted within the respective branches.
4. The Administrative Officer (Judicial)/Branch Incharge, Computer Branch, Tis Hazari/Rohini/Dwarka/Karkardooma/Patiala House and Saket Court Complex, Delhi/New Delhi are directed to conduct surprise checks to ensure that no user has installed any unlicensed windows operating system. Any such instance be immediately brought to the notice of the respective Officer In-charge (Computers) for initiation of necessary disciplinary action besides immediate disconnection of such system from LAN.
5. PS to the undersigned.
6. Dealing Official, Website Room, Tis Hazari Courts, Delhi

AD&SJ / Chairman,
Centrlized Computer Committee
Delhi

674
17/05/17

OIC Comp
DJ/SE
17/5/17

Preventive Measures:

To protect a computer against virus or infections, user is to ensure the below mentioned preventive measures

✓ *Use and keep updated anti-virus software*

✓ *Blocking of removable media devices* - Prevent the use of all unauthorized /infected removable media- use only after scrutiny through anti-virus

✓ Be careful while downloading any free or paid software, it may contain Malware

✓ *Avoid opening suspicious emails* – To avoid clicking on suspicious links or opening suspicious attachments with mails.

✓ *Not to use unsupported Operating system and applications* – Windows XP, Windows 2003, Internet explorer 6 or below and other applications which are currently not supported by vendors (end of life / end of support) are not to be used.

✓ *Restricting account privileges:-*. Configure all standard user accounts to prevent the execution and installation of any unknown or unauthorized software.

✓ *Connect the systems with internet only if it is required, otherwise disconnect it*

Tips for handling Ransomware, if suspected or detected in your computer:-

✓ Isolate the computer from your network to prevent the threat from further spreading.

✓ Remove the PC from Network.

✓ Don't share file from this System to other system.

✓ Don't use pen drive, external drives on this System to copy files to other systems.

✓ Get machine formatted and get fresh OS installed

718 | Court/Exe. Copy)
19/5/17
Received on 17/5/17