Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:112 **13-11-2020**

Name: New Linux version of RansomEXX ransomware

Threat Classification: Ransomware

Summary:

A Linux version of the **RansomEXX** ransomware, new ransomware strain, has recently been reported for targeted cyber-attacks. The RansomEXX group has created this version from their Windows ransomware knowing that many firms are running their critical IT infrastructure on Linux environment.

For more details on RansomEXX, please visit following link:
https://cert.bournemouth.ac.uk/linux-version-of-ransomexx-ransomware-discovered/

Recommendations:

- **Backups, including offline backups of all critical servers and information systems** should be maintained. Ensure that an efficient Data Backup strategy is in place and practiced. e.g. backup copies of critical data should be maintained with **3-2-1 Backup Strategy**, i.e. 03 Total copies of critical data, 02 of them Local on different Medias and 01 copy at a secure Remote/ DR site.
- Implement filters at Email gateway to **filter out emails with known malware spamming indicators**. Also block the suspicious IP addresses at perimeter firewall.
- **Execution of unsigned executables** from sensitive webservers and endpoints must be blocked.

- Implement Software Restriction Policies (SRP) to **block unsigned binaries running from %APPDATA% and %TEMP%** locations.
- **Block email attachments commonly associated with malware like .dll and .exe**, also block outbound network connections originating from **WinWord.exe, Powershell.exe, Powershell_ise.exe, Mshta.exe** and block inbound connections if remote access of system is not required.
- **Block Tor** (The Onion Router) **Gateways** as they are the primary means for ransomware threats to communicate with their C&C servers.
- **Privileged rights on Updates Servers, Domain Controller, Email Servers, Application Servers, Antivirus Servers** should be reviewed and reassigned only on need to know basis.
- All changes on end user machines should be restricted (e.g. installing software, giving admin rights and similar).
- **All unnecessary ports, protocols and services on end user machines and servers should be blocked**.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.