NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Security Bulletin

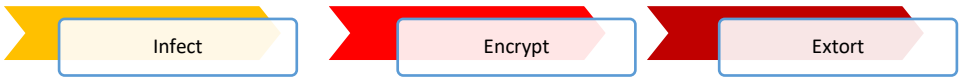
TLP: WHITE

April 13, 2021

NPCC is publishing this security bulletin to engage and inform NPCC entities on aspects of Bulk Power System security and reliability.

Ransomware Awareness

Ransomware is a type of malicious threat or malware, that locks access to a computer system or files by encrypting its data, until a ransom is paid. Paying the ransom does not guarantee the attacker will provide the encryption key or prevent another attack.



- **Key Indicators:**
  - You no longer have access or have been locked out of your files
  - Odd File extension names, e.g., micro, wallet, zzzzz, lol!, file0locked, kkk, vvv, fun, etc.
  - Message(s) to pay a "ransom"
- **Preventative Action:**
  - Keep Cyber Security defenses current (Firewalls, IDS/IPS, Segmented networks, restrict user permissions, maintain system baselines, only allow approved programs, review activity logs, enable email spam filters, etc.)
  - Monitor, test, verify and deploy operating system, software, and Firmware patches
  - Follow NIST/CIS Cybersecurity framework version 1.1 to enhance cybersecurity posture
  - Review open firewall ports, especially RDP and close them
  - Create, maintain, and test local and offline backups
  - Create, maintain, and drill your incident response plan
  - Educate your organization on current cyber threats and what to look for:
    - Phishing Emails, Malicious Attachments, Malicious websites
- **Incident Response:**
  - Report anything suspicious to your organization IT or your organization incident response team; have them investigate the incident and follow mitigation actions
  - Contact outside support (Law enforcement, CISA, Third Party Cyber Security Firm) as required

DHS Ransomware Resources

- DHS CISA: Ransomware Guide
- DHS CISA: Ransomware Resources
- NIST: Cyber Security Framework
- CIS: The 20 CIS Controls