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

October 13, 2021

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

## E-ISAC Ransomware Attack Techniques

***E-ISAC has released a TLP Green Ransomware Attack Techniques Document***

**Document Access:** To access the document login to the E-ISAC Portal

**TRAFFIC LIGHT PROTOCOL (TLP) Green Restrictions:** Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

**Document Key Topics:**

- **Reoccurring or common intrusion vulnerabilities**
- **Threat classification and detection models**
- **Adversary Tactics, Techniques, and Procedures (TTPs)**
- **Analysis of software employed by identified Advanced Persistent Threats (APTs)**
- **Ransomware References and Resources**

DRAFT



NPCC assumes no responsibility for any material, e.g., information, data, text, software, graphics et cetera, of computer "links" to sites hosted by third parties that are outside of NPCC's control. NPCC does not endorse products, services, or information provided by third parties and shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with, use or reliance on any content available on or through any third party site. Further, the inclusion of links to third party websites within this Security Bulletin does not imply that the owners of such third party websites have given permission for inclusion of these links, or otherwise sponsored or endorsed NPCC's Security Bulletin.
NPCC is not responsible for the accessibility of third party websites via the Security Bulletin. Should you discover that a third party link on a Security Bulletin is broken, no longer pointing to the content so indicated on the Security Bulletin, or points to a third party website containing infringing content, malicious code, or any offensive, libelous, or otherwise illegal or inappropriate content, email: support@npcc.org. To ensure NPCC can quickly respond to the issue, your email should include the originating Security Bulletin, the linked page URL and a description of the content in question.