TO: All MS-ISAC Members and Partners

DATE: September 1, 2020

SUBJECT: Activity Alert (AA) - Technical Approaches to Uncovering and Remediating Malicious Activity - TLP: WHITE

On September 1, 2020, a joint advisory based on collaborative research from Australia, Canada, New Zealand, the United Kingdom and the United States was released on the US-CERT website as Activity Alert AA20-245A. This advisory highlights technical approaches to uncovering malicious activity and includes mitigation steps according to best practices. The purpose of this report is to enhance incident response among partners and network administrators along with serving as a playbook for incident investigation.

The details of the information can be found in the Activity Alert found at the US-CERT link below:
https://us-cert.cisa.gov/ncas/alerts/aa20-245a

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.