U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

REMEDYS: Research Exploring Malware in Energy DeliverY Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

A trusted malware mitigation organization for national energy sector collaboration and security

Multiple organizations across the U.S. individually validate, assess, analyze, and develop components of malware mitigation processes. However, asynchronous actions between the public and private sectors adversely impact critical energy infrastructure by lengthening response time and opening a window of opportunity for malicious interference. REMEDYS connects and integrates the expertise and resources of the multiple and diverse relevant organizations and stakeholders engaging in information sharing and malware analysis. The research team is developing, evaluating, and refining an organizational structure to coordinate key players in rapid research, development, and distribution of mitigations that reduce the risk of imminent or emerging threats from malware-based cyberattacks in the energy sector. REMEDYS will serve as a mechanism to make it easier for energy sector stakeholders, including energy delivery system operators, to share information and tools to respond instantly to threats and breaches that may occur in their environment.

KEY TAKEAWAYS

- Provides a collaborative platform to synchronize malware identification and remediation across the energy sector
- Minimizes response time to malware-based cyberattacks for all participating organizations
- Engages relevant organizations and stakeholders to create and sustain a culture of security

OUTCOME

REMEDYS will engage energy sector organizations to more effectively interact and share information, increasing the efficiency with which members identify and mitigate cyberattacks. The organizational methodologies used by the project team create a self-sustaining community of stakeholders for long-term nationwide coordination.

PARTICIPANTS	ROLE
CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM	The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts.
Massachusetts Institute of Technology	Lead institution; supports leadership efforts at Pacific Northwest Nation Lab and Oak Ridge National Lab by developing organization models, provided research support, idea generation, and case studies.
Pacific Northwest NATIONAL LABORATORY	National lab co-lead
OAK RIDGE National Laboratory	National lab co-lead

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Stuart Madnick
Site Lead, Professor
Massachusetts Institute of Technology
617-253-6671
smadnick@mit.edu

Michael Siegel
Principal Research Scientist
Massachusetts Institute of Technology
617-253-2937
msiegel@mit.edu

Keri Pearlson
Executive Director, Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity
Massachusetts Institute of Technology
kerip@mit.edu

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

This is a subproject sponsored by the CREDC academic consortium, led by the University of Illinois.

CREDC Period of Performance: October 2015 – May 2022

CREDC Total Award Value: $28,099,258
DOE Share: $22,476,290
Cost Share: $5,622,968

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021