REMEDYS: Research Exploring Malware in Energy DeliverY Systems

Website: http://cred-c.org/researchactivity/remedys

Researchers (MIT): Stuart Madnick, Michael Siegel, Keri Pearlson, and Research Assistants

Industry Collaboration:

- This research will be conducted in collaboration with Pacific Northwest National Laboratory (PNNL), Oak Ridge National Laboratory (ORNL), the U.S. Department of Energy, and an extensive list of vendors, cybersecurity service providers, owners/operators, industry associations, government entities, and universities.

Description of research activity: Numerous public and private organizations providing valuable services such as information sharing and malware analysis for the sector exist today. REMEDYS will close the existing gap by connecting and integrating the expertise and resources of the multiple and diverse relevant organizations and stakeholders in a unified effort to protect the sector and nation. Those organizations and stakeholders, within this structure, then accelerate the identification, development and availability of solutions for new malware.

To develop this solution, the Department of Energy is coordinating with two national laboratories in a research effort that will engage energy sector stakeholders to develop an effective model for REMEDYS. The end goal is of this effort is for REMEDYS to *provide a platform and synchronized actions across the energy sector that assists the members during a cyber event and makes pertinent mitigation processes available.* Ultimately, REMEDYS will gain enough traction to become self-sustaining, having demonstrated value to its participants within the life of the project.

The REMEDYS project will provide:

- An evaluation of the current state of the art for the processes of malware identification and remediation in the energy sector and the identification of potential groups or classes of contributors that will be critical to the success of the program. This may include specific organizations that are currently relevant, but will remain flexible to allow for the later inclusion of new or newly relevant organizations.
- A report of the research conducted, including methodologiesused in the research and analysis, the assessment criteria, and the results of the research for each organization structure evaluated.
- A recommended optimal organization structure including descriptions of its charter, how it will operate, value proposition, legal agreements that will need to be in place, and how might be implemented in practice.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This research will address the following roadmap areas:

- Build a Culture of Cyber Security
  - Since the culture is composed of the attitudes, beliefs and values of an organization, the creation of a trusted malware-mitigation organization will highlight the importance of cybersecurity in the energy sector, building a stronger culture of security within each of the stakeholders in the ecosystem, including EDS.
- Develop and Implement New Protective Measures to Reduce Risk
  - A successful organizational structure will enable scalable future relationships in the EDS ecosystem since it is designed to reduce risk and increase speed of deployment of mitigations.
- Sustain Security Improvements
  - The research team will hold practice case studies to learn and continuously improve security, to better guide the development of the organizational models.

Summary of EDS gap analysis: Currently, when malware is suspected or found in energy sector Operational Technology (OT) control systems there is no single coordinating organization that can ensure a timely and comprehensive National

mitigation process. There are multiple organizations across the United States that each have their roles and responsibilities in validating, assessing, analyzing and developing malware mitigation processes. However, the lack of synchronized actions among public, private, and government sectors can have the potential for an adverse impact in our critical energy infrastructure.

Targets for addressing new malware rely on their own expertise and relationships with others to identify and resolve issues. As an industry, this working of issues in relative isolation lengthens the time from initial discovery to the deployment of a solution. This gives an adversary an unnecessary and distinct advantage in an already tenuous battle. Reducing this window of opportunity for the adversary is crucial to the protection of the energy sector and our Nation's security. In today's increasingly hostile cyber landscape, we as a sector and as a nation can no longer afford to work these issues in relative isolation. The time has come to provide a mechanism that rapidly and securely engages the best and brightest from across utilities, industries and government in facilitating solutions to addressing these threats.

The research team, composed of members from ORNL, PNNL, MIT and other supporting organizations, will design and evaluate ways to create an organization of organizations to insure rapid deployment of mitigations. A recommended organization structure, including descriptions of its charter and how it will operate, will be designed to serve as a mechanism to make it easier for energy sector stakeholders, including EDS operators, to respond instantly to threats and breaches that may occur in their environment.

Full EDS gap analysis:

Motivation:
Making sure EDS and other energy sector entities can manage a malware situation is top of mind of energy leaders. When malware is suspected or found in energy sector operational technology (OT) control systems, there is no single recognized approach or mutual aid function that can be leveraged to ensure a timely and comprehensive coordination of mitigation efforts. There are multiple organizations engaged with validating, assessing, analyzing and developing mitigations, but they often rely on their own expertise and relationships with others to identify and resolve issues. This approach lengthens the time from initial discovery to deployment of a solution and gives adversaries an unnecessary advantage. Reducing this window of opportunity for adversaries is crucial to the protection of the energy sector, and ultimately to our Nation's security. With today's increasingly hostile cyber landscape, we can no longer afford to leave this window open.

A new research partnership led by Oak Ridge National Laboratory (ORNL) and Pacific Northwest National Laboratory (PNNL) is being formed to find a solution to this problem. The initial objective of this partnership is to design, analyze and evaluate organizational structures composed of multiple energy sector stakeholders and dedicated to rapid research, development and distribution of mitigations to reduce the risk that malware might disrupt energy delivery. There is a need for organizational design thinking built on research in the organizational theory, technology management, and cybersecurity domains.

While numerous private and public organizations are addressing malware identification and remediation, there remains an open research question:

- In the event of new malware that could disrupt critical energy infrastructure, how would these different types of organizations most effectively interact to rapidly recognize the cyber-attack for what it is, develop mitigations, and make them available nationwide?

Addressing the gap:
This proposed project, REMEDYS, will both support and co-lead the initiative to design and evaluate organizational structures as part of the research partnership being established by the Department of Energy (DOE). The goal of REMEDYS is to develop, evaluate, and refine an organizational structure which could be used to coordinate the nation's multiple energy sector stakeholders in rapid research, development and distribution of mitigations that reduce the risk of imminent or emerging threats from a malware cyber-attack in the energy sector. These mitigations could be technology-based or process-based or both and must consider other factors of the energy delivery system (EDS)

stakeholders such as organizational culture and governance. The design and development is a complex problem requiring multi-disciplinary thinking. The results will lead to tools and technologies that operators can use to mitigate cyber threats through interaction with REMEDYS.

To address this challenge will require:

- An understanding of the challenges, motivations, incentives, and functions of each of the stakeholder organizations involved.
- A clear articulation of the goals, requirements and imperatives of REMEDYS.
- A grounded plan utilizing the best research around organizational trust, communications, design and operations.
- A set of contingencies to address unanticipated consequences and inevitable changes occurring in the environment and the stakeholders.

Just pulling together the steering committee to bring this project to life has a unique set of management challenges that need to be addressed in the early, formation stage REMEDYS. There are many divergent interests and motivations of each of the stakeholders.

MIT research staff with extensive experience in the impacts of technology on organizational design, business process design, virtual organization design, and cybersecurity leadership will join the leadership team developing organizational models, providing research support, idea generation, guidance and case studies.

Bibliography:

[1] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[2] Electric Sector Failure Scenarios and Impact Analyses – Version 3.0, National Electric Sector Cybersecurity Organization Resource (NESCOR), 2015 December. http://smartgrid.epri.com/NESCOR.aspx

[3] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, http://dx.doi.org/10.6028/NIST.SP.1108r3

[4] Sterman, J. D. 1992. "Teaching Takes Off," *OR/MS Today* (35:3), pp. 40-44.

[5] Huang, K., Pearlson, K., Madnick, S. 2017. “Trust and Collaboration to Enhance Cybersecurity,” (IC)3 White Paper, Sloan School, MIT.

[6] Huang, K., and Pearlson, K. 2018. “Profiling the Organizational Cybersecurity Culture: Toward a Cybersecurity Culture Framework,” (IC)3 White Paper, Sloan School, MIT.

[7] Ozer, O., Subramanian, U. and Wang, Y. 2017. “Information Sharing, Advice Provision, or Delegation: What Leads to Higher Trust and Trustworthiness?” *Management Science*. Articles in Advance [23].

[8] Porter, C. E., Donthu, N. 2008. “Cultivating Trust and Harvesting Value in Virtual Communities.” *Management Science* 54(1):113-128. https://doi.org/10.1287/mnsc.1070.0765

[9] Pearlson, K., Saunders, C. and Galletta, D. 2016. *Managing and Using Information Systems: A Strategic* Approach 6e. Wiley and Sons.