AI-Enhanced Cybersecurity: Detecting and Characterizing Network Scanner

ID# 2020-5127

Technology Summary
This invention focuses on addressing challenges in detecting and characterizing malicious scanning activities in network data. It proposes the use of network telescopes, also known as “Darknets,” to capture and analyze unsolicited traffic directed towards unused IP addresses. The data collected from Darknets can help identify patterns of malicious scanning, which are crucial for preventing cyber-threats. However, analyzing Darknet data presents difficulties due to its heterogeneous nature, high dimensionality, and non-linear interactions. To overcome these challenges, the invention introduces a framework involving deep neural networks for dimensionality reduction and clustering. This framework aims to create information-preserving representations of scanner data, enabling the identification of distinct scanning behaviors.

Application & Market Utility
The need for strong cyber security exists across many different industries including manufacturing, communication and financial services, energy sector, and health care. The system operates in a cloud-based hardware environment and can be accessed through a user interface to provide analysis results to users or third parties interested in cybersecurity insights.

Next Steps
The next steps for this invention involve refining the framework using deep neural networks to detect malicious scanning activities in network data. Seeking collaboration and/or licensing opportunities to further develop and integrate the framework into existing cybersecurity systems.

TECHNOLOGY READINESS LEVEL
4

Seeking
Investment | Licensing | Research

Keywords
- Cybersecurity
- Deep neural networks
- Cyber-threat prevention
- Network security
- Anomaly detection

Researchers
John Yen, PhD
Professor

Other Researchers
Donald Welch, Junjie Liang, Vasant Honavar, Michalis Kallitsis

Originating College
College of Information Sciences and Technology

Office of Technology Management Contact
Swope, Bradley
bas101@psu.edu
814-863-5987