

Combating the Impact of Advanced Persistent Threats in Industrial Internet of Things (IIoT)

Dr. Wazir Zada Khan

Head of Research

Department at College of Computer and Information Technology

Co-Founder of Farasan Networking Research Laboratory

Jazan University

Saudi Arabia

Abstract

Industry 4.0 or Industrial Internet of Things (IIoT) with its intelligent monitoring and controlling applications and predictive and preventive maintenance of industrial equipment is capable of collecting and analyzing a large amount of data, achieving high operational efficiency, increased productivity, and better management of industrial assets and processes. However, the connected industrial assets have increased exposure to the new cyber-physical risks including Targeted Attacks or Advanced Persistent Threats (APTs) that are on the rise and have emerged as the most complicated Multi-Stage Attacks, hitting the industrial companies and governmental organizations. APTs that are designed with a particular motive, are sophisticated, professional, state supported and systematic cyber-attack programs in which an attacker is motivated, skilled, organized and well-funded. The existing cyber security intrusion detection techniques and traditional defensive mechanisms are no longer sufficiently effective against APTs which is the most worrisome situation and thus, novel and more effective solutions are required to predict, detect and mitigate APT threats. APTs are a global scourge and a challenging targeted attack so today in this speech we will discuss APT attacks and their characteristics particularly in case of oil and gas industries. Moreover, we would also discuss prevention and detections methods devised for countering APTs as well as some

Biographies:

Currently working with the College of CS & IT, Jazan University, Saudi Arabia. He is Co-Founder of Farasan Networking Research Laboratory and also serving as Head of Research Department at College of Computer and Information Technology Jazan University, Saudi Arabia. Dr. Khan is also serving as a Researcher at the 'Global Foundation for Cyber Studies and Research' which is an independent, non-profit, and non-partisan cybersecurity think-tank based in Washington D.C. Dr. Khan has published over 70 research papers in the journals and conferences of international repute. He is serving as a reviewer of many reputed journals and also a member of the technical program committee for many international conferences. He has more than 15 years of teaching/professional experience in Pakistan and Saudi Arabia. His current research interests are in the area of Security, Privacy and Trust. He is a Senior Member of the IEEE.