Ransomware Threat and its Impact on SCADA

Submitted by grigby1 on Fri, 07/10/2020 - 1:08pm

Title: Ransomware Threat and its Impact on SCADA
Publication Type: Conference Paper
Year of Publication: 2019
Authors: Javed Butt, Usman Abbod, Maysam Lors, Anzor Jahankhani, Hamid Jamal, Arshad Kumar, Arvind
Conference Name: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)

Keywords: business productivity, Coin Miner, Computer crime, control engineering computing, critical infrastructure, critical infrastructures, cryptocurrency, cryptojacking, Cryptor, Cyber Actor, cyber attack, cyber threat, cyber-attack incidents, cybercrimes, cybercriminals, cybersecurity, Data and System Access, Data Backup, Data Extortion, Data Mitigation, Device Compromising, Downtime, Encrypting, Human Behavior, human factors, Human Machine Interface, ICs, industrial control, industrial control systems, industrial networks, industrial processes, Infected System, Information security, invasive software, Locker, malicious software, Malware, Metrics, Network, operation technology, Petya, production engineering computing, Programmable Logic Controllers, pubcrawl, Ransom, ransomware, ransomware attack, Ransomware Deadline, Ransomware Incidents, Ransomware Prevention, Ransomware Strategies, Ransomware Taxonomy, ransomware threat, Ransomware Threating, Remote Terminal Units, resilience, Resiliency, SCADA systems, supervisory control and data acquisition, Threat report, WannaCry
Abstract

Modern cybercrimes have exponentially grown over the last one decade. Ransomware is one of the types of malware which is the result of sophisticated attempt to compromise the modern computer systems. The governments and large corporations are investing heavily to combat this cyber threat against their critical infrastructure. It has been observed that over the last few years that Industrial Control Systems (ICS) have become the main target of Ransomware due to the sensitive operations involved in the day to day processes of these industries. As the technology is evolving, more and more traditional industrial systems are replaced with advanced industry methods involving advanced technologies such as Internet of Things (IoT). These technology shift help improve business productivity and keep the company’s global competitive in an overflowing competitive market. However, the systems involved need secure measures to protect integrity and availability which will help avoid any malfunctioning to their operations due to the cyber-attacks. There have been several cyber-attack incidents on healthcare, pharmaceutical, water cleaning and energy sector. These ICS’ s are operated by remote control facilities and variety of other devices such as programmable logic controllers (PLC) and sensors to make a network. Cyber criminals are exploring vulnerabilities in the design of these ICS's to take the command and control of these systems and disrupt daily operations until ransomware is paid. This paper will provide critical analysis of the impact of Ransomware threat on SCADA systems.

DOI 10.1109/ICGS3.2019.8688327
Citation Key javed_butt_ransomware_2019