Chapter 6
Modeling of ICS/SCADA Crypto-Viral Attacks in Cloud-Enabled Environments

Aaron Zimba
https://orcid.org/0000-0002-2587-106X
Mulungushi University, Zambia

Douglas Kunda
Mulungushi University, Zambia

ABSTRACT

The production processes of critical infrastructures (CIs) are managed and monitored by Industrial Control Systems (ICS) such as SCADA (Supervisory Control and Data Acquisition). The resulting CIs networks are huge and complex, which have inadvertently called for the integration of other technologies such as the internet for efficiency. The integration of such unsecured technologies and the advent of new computing paradigms such as IoT (internet of things) and Cloud computing which are being integrated into current industrial environments, giving rise to Industry 4.0 have further expanded the attack surface. This chapter considers a new breed of security attacks, crypto-viral attacks (crypto mining and crypto ransomware attacks), which target both the production and control networks of CIs. The authors model these attacks and evaluate their impacts. Such modeling is crucial in understanding the extent of the scope and detection capabilities of the first line of defense (intrusion detection and prevention systems), and possible avenues for mitigation strategies are suggested.

INTRODUCTION

Critical infrastructure (CI) networks have traditionally been separated from networks. This has been mainly because of the prevalent use of proprietary protocols (Rubio, Alcaraz, Roman, & Lopez, 2019). Most of the devices in these networks ran unsecure protocols and little attention was paid since the systems thereof were "air-gapped" and inherently secure from cyber-attacks (Zimba, Wang, & Chen, 2018). As

DOI: 10.4018/978-1-7998-2910-2.ch006

such, in as far as security was concerned; much effort was channeled towards physical security. However, nowadays, critical infrastructures no longer operate in closed environments but are rather being integrated into public technologies such as the Internet and cloud computing. This integration has been fostered due to the standardization of CI devices and protocols as well as the costs associated with outsourcing various services from cloud computing (MacKay, Baker, & Al-Yasiri, 2012). The integration of CIs to public networks has exposed the traditionally unsecure CI devices and networks. This has broadened the attack surface in the CI landscape.

The attack surface has further dramatically increased with the advent of new paradigms such as Internet of Things (IoT) and Cloud computing which are being integrated into current industrial environments, giving rise to Industry 4.0 (Khan & Turowski, 2016). Since most CI networks comprise the production networks, which encompasses networked CI devices and the control networks which comprise Industrial Control System/Supervisory Control and Data Acquisition Systems (ICS/SCADA), the target in these networks is twofold. CIs have been further exposed to cyber-attacks due to the outsourcing of technical services from the cloud. In some cases, both production devices and SCADA systems of some CIs are directly reachable from the Internet (Alcaraz & Zeadally, 2015), which in itself presents a severe security threat. In light of this, it is important to protect both the CI devices and the systems that control them. The diagram in Figure 1 shows a typical ICS/SCADA system and the associated susceptible points to cyber-attacks.

Tier 0 is the Production Network layer which is similar to the physical world and includes input/output (I/O) devices such as sensors, actuators, Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCSs), Remote Terminal Units (RTUs) for remote access, and general Wi-Fi and radio frequency (RF) networks. In some network design patterns, low level devices in this tier are directly connected to the Internet (Zimba et al., 2018) which exposes the network to the attacker (attacker‘).

Tier 1 is the SCADA Network layer which houses among other things the Human Machine Interface (HMI), the Engineering Workstation (EW), the Tier 1 Data Historian (D. Hist1), Central Object Repository (COR), and Application Servers (AS). They are used to configure, monitor and control the devices in Tier 0 while feeding information to the upper tier. Equally, some network design patterns expose the SCADA network directly to the Internet and such systems are easily discoverable (Anton et al., 2018) on IoT search engines such as Shodan (Matherly, 2016) and Censys (Arnaert & Antipolis, 2016). This exposes the SCADA network to attackers from the Internet (attacker❺) if vulnerabilities are discovered. Alternatively, the attacker can traverse through Tier 2 and compromise the system at this layer.

In most CI network design patterns, Tier 2 is the network exposed to the public Internet. It is at this layer where the Tier 2 Data Historian is found. The corporate or enterprise network is usually interconnected at this layer. The attacker (attacker❹) at this layer can compromise the system either from the corporate network by phishing benign users or exploit vulnerabilities directly from the Internet since this is an Internet-facing layer.

Another source of attack is the Cloud Trusted Third Party (Cloud/TTP) where the CI is outsourcing technical services through cloud computing. The attacker (attackerŽ) can exploit the trust relationship between the CI and the technical service provider. The integration of remote access support further increases the attack surface. Other sources of attacks include infection through legitimate remote system users (attackerŒ) and arbitrary Internet attacks from cyber-crime groups (attacker❷). The cyber-attacks assumed thus far are generic. However, with the advent of digital money (crypto currencies), there has been a shift towards attacks that are more rewarding and those that make the acquisition of crypto currencies simpler.