KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express ▮ (▮▮▮▮) ▮▮▮–▮▮▮

www.elsevier.com/locate/icte

Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems

Aaron Zimba*, Zhaoshun Wang, Hongsong Chen

Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing, China

Received 3 November 2017; accepted 27 December 2017
Available online xxxx

Abstract

The inevitable integration of critical infrastructure to public networks has exposed the underlying industrial control systems to various attack vectors. In this paper, we model multi-stage crypto ransomware attacks, which are today an emerging cyber threat to critical infrastructure. We evaluate our modeling approach using multi-stage attacks by the infamous WannaCry ransomware. The static malware analysis results uncover the techniques employed by the ransomware to discover vulnerable nodes in different SCADA and production subnets, and for the subsequent network propagation. Based on the uncovered artifacts, we recommend a cascaded network segmentation approach, which prioritizes the security of production network devices.

Keywords: Critical infrastructure; Cyber-attack; Industrial control system; Crypto ransomware; Vulnerability

1. Introduction

Industrial Control Systems (ICS) oversee many of today's Critical Infrastructure (CI), which include smart grids, electrical power plants, nuclear power plants, air traffic control, water and waste treatment plants, transportation etc. CI provides essential services and resources required for basic human needs. Due to their importance, they have traditionally been safeguarded and secluded from other publicly available systems [1]. The emphasis, as far as security is concerned, has been on physical security and environmental safety. This is evidenced by the tight physical security and safety systems present in almost all critical infrastructure. Notwithstanding the aforementioned, the advent of robust and advanced technologies, the Internet in particular, has seen the gradual disappearance of the "air-gap" between CI and public systems. The demand to enhance productivity by reducing manufacturing and operational costs has led to the adoption of technologies that have eventually led to the integration of CIs into public systems such as the Internet [2]. Moreover, the integration of enterprise and corporate systems with the Internet have provided new avenues for real-time data acquisition, which has considerably fostered efficiency. Nevertheless, considering the diversity of CI sectors, the integration of CIs with public or corporate networks has been diverse and lack a standard secure framework [3]. Thus, the approach in securing these integrated systems has largely been determined by the different security goals of organizations, which are inadvertently dictated by the underlying business objectives. Since the IP protocol (the protocol upon which private and public networks are built) is unsecure, cyber-attacks have found their way into CIs, which for a long time have been believed to be isolated and secure. This has resulted in cyber-threats, where the different network design patterns in CIs have resulted in a number of attack entry points into CIs. Fig. 1 depicts the threat model against CI and ICS, which shows the various attack entry points.

* Corresponding author.
E-mail addresses: azimba@xs.ustb.edu.cn (A. Zimba), zhswang@sohu.com (Z. Wang), chenhs@ustb.edu.cn (H. Chen).

Peer review under responsibility of The Korean Institute of Communications Information Sciences.

https://doi.org/10.1016/j.icte.2017.12.007

Please cite this article in press as: A. Zimba, et al., Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems, ICT Express (2018), https://doi.org/10.1016/j.icte.2017.12.007.

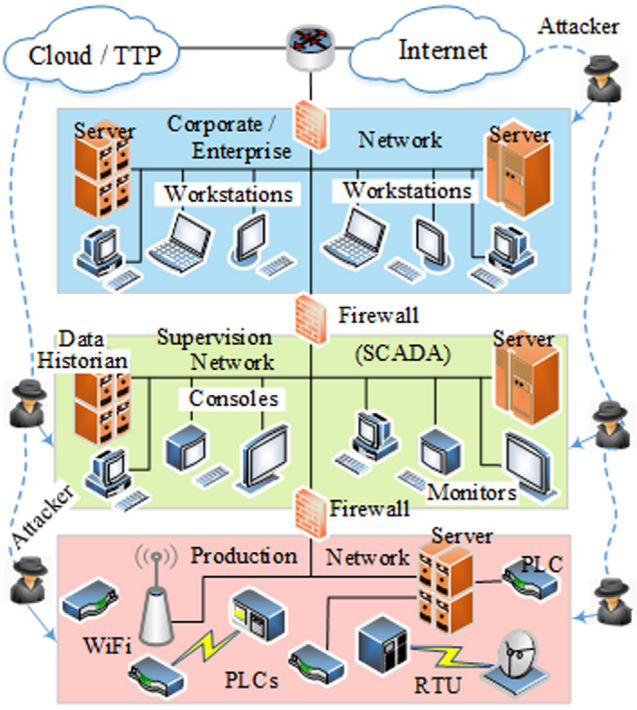

Fig. 1. Threat model against CI and ICS.

The production network is similar to the physical world and comprises sensors, actuators, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) for remote access, and general Wi-Fi and RF networks. In some of the network design patterns, these low level components are directly connected to the Internet [4]. This is one entry point for malwares such as ransomwares. Some network design patterns only have a supervision network, which houses the Supervisory Control And Data Acquisition (SCADA) system to connect to the Internet. The attacker can thus infiltrate the supervision network upon vulnerability discovery and elevate the attack to the production network if possible. Some network design patterns connect the corporate and enterprise networks via a cascaded approach as in the Purdue Model [5]. In this case, the attack has to infiltrate the corporate network in order to reach the underlying ICS, provided such a design is categorically secured via a defense-in-depth strategy. The worst-case scenario is where the three networks are not properly segmented but designed in a single broadcast domain without proper demarcation points. Therefore, given a certain network design pattern, an attacker can, upon discovery of a vulnerability, deposit malware in the corresponding CI network. In this study, we aim to model and characterize the attack techniques employed by cyber attackers to infiltrate CIs through publicly accessible networks. To validate our modeling approach, we use ransomware attacks through reverse engineering (static malware analysis). We perform source code analysis on the infamous WannaCry ransomware, which has not spared CI, and uncover the underlying network attack techniques. In Section 2, we present the attack model of ransomware on CI based on the corresponding threat model. We perform static code disassembly and malware analysis in Section 3. The recommended best practices based on the observed attack patterns and the conclusions are provided in Section 4.

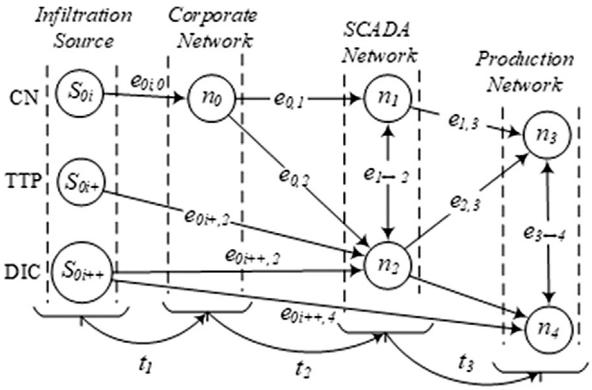

Fig. 2. Attack model against CI and ICS.

2. The attack model

As shown in Fig. 1, CI and ICS, once connected to the Internet whether directly or otherwise, present three points of entry through which the attacker can deliver the ransomware payload. The entry points are denoted as:

(1) Corporate Network (CN)
(2) Trusted Third Party (TTP) i.e. cloud outsourcing or technical support
(3) Direct Internet Connection (DIC).

We model the attack process using an attack graph with three entry nodes denoting three infiltration sources. The other three sections of the graph denote vulnerable node instances in the three network types found in typical CI and ICS as illustrated in Fig. 1. The edges between the node instances denote the exploitation of a vulnerability, which further enhances the traversal of the ransomware across the network. The threat actor of our attack model is a ransomware with worm-like capabilities (as those witnessed in WannaCry), which is capable of propagating the payload to adjacent network upon vulnerability exploitation [6]. The resultant attack model is shown in Fig. 2. The target of any crypto ransomware attack is to breach availability by encrypting a victim's files, thereby rendering them inaccessible. In our model, the ransomware seeks to attack the SCADA or production networks to make CI and ICS data inaccessible. Therefore, even though ransomware attacks are indiscriminate, the presence of a ransomware in the corporate or enterprise network of a CI implementing the Purdue model does not constitute an actual attack. Rather, the network is used as a pivot to traverse the underlying SCADA or production network.

We differentiate three infiltration sources CN, TTP and DIC denoted by three sources S_{0i}, S_{0i+}, and S_{0i++}, respectively. The attack edge $e_{0i,0}$ denotes infiltration of the corporate network via an insider or outsider attack. We postulate the Markov assumption [7], and therefore constrain the history of how the corporate network gets infiltrated. However, exploit kits and

Please cite this article in press as: A. Zimba, et al., Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems, ICT Express (2018), https://doi.org/10.1016/j.icte.2017.12.007.