PRECURSOR ANALYSIS REPORT: MUMBAI 2020 POWER OUTAGE – RELIABILITY FAILURE EXPOSES MALWARE INTRUSION

Cybersecurity for the Operational Technology Environment (CyOTE)

30 SEPTEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

INL/RPT-22-69764

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: MUMBAI 2020 POWER OUTAGE – RELIABILITY FAILURE EXPOSES MALWARE INTRUSION

1. EXECUTIVE SUMMARY

The Mumbai 2020 Power Outage – Reliability Failure Exposes Malware Intrusion Precursor Analysis Report leverages publicly available information about the 12 October 2020 power outage in Mumbai, India. While the outage itself was due to a series of reliability failures, the cyber investigation it prompted led to the discovery of a malware intrusion that held the grid's Information Technology (IT) and Operational Technology (OT) systems at risk, and about which the grid operators were completely unaware. This study catalogs anomalous observables for each technique employed in the intrusion, framed in the context of the reliability failures. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

The outage began with the failure of the four high-voltage transmission lines feeding power from the national transmission network into the Mumbai grid. One of the lines was already out of service, undergoing repairs after a conductor snapped on 10 October. A damaged insulator tripped a second line over-voltage at around 4:30 AM on 12 October, not long before the city's 2,500 electric commuter trains began their morning rush hour service. While grid operators called for additional hydro generation from Mumbai's embedded capacity early in the 9:00 AM hour, over half of that generation tripped roughly 45 minutes later due to a fault at a hydro station. This loss overloaded the third high voltage transmission line, which tripped at about 10:00 AM. Shortly thereafter, operators manually tripped the final incoming transmission line after they observed the line sparking due to a voltage overload at one of the substations. This led to the triggering of Mumbai's islanding scheme, which isolates the local grid and relies on embedded generation to keep the city's grid functioning in case of fluctuations in or failure of the national grid. Unfortunately, Mumbai's embedded generation capacity fell well short of the existing grid demand, tripping the city's power stations and sending the city into a blackout.[1,2,3]

While investigations confirmed the outage was indeed due to reliability issues, Maharashtra state power officials remained concerned about the possibility of a cyber attack in light of recent regional tensions with China and commissioned the state police cyber authorities to conduct an investigation. The resulting report, released to the state government in March 2021, revealed that the IT and OT systems of the state's grid control systems had been compromised, likely by Chinese state-sponsored adversaries.[4,5] The report claimed the adversaries were able to "easily" breach multiple firewalls and implant at least 14 trojans in both the IT and OT environments of the control networks governing the state's power distribution system. In addition, central government officials revealed that cyber attacks had been carried out against other segments of India's grid infrastructure at the time but claimed they were not linked to Mumbai's grid failure.

Researchers and analysts identified 14 unique techniques related to the malware most likely utilized for the intrusion with a total of 183 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques to identify opportunities to detect malicious activity. If observables accompanying the techniques are perceived and investigated during an intrusion or prior to the triggering event of a cyber attack, earlier comprehension of malicious activity can take place.

While the cyber intrusion against Mumbai’s power grid never resolved into an actual attack, CyOTE analysts used the publicly available data on the intrusion to create a cyber attack scenario depicted by the notional attack sequence found in Section 3. In this scenario, 11 of the identified techniques were precursors to the notional triggering event. Analysis identified 133 observables associated with these precursor techniques, 86 of which were assessed to have an increased likelihood of being perceived in the 160 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack. Organizations can use these products if they experience similar observables or to prepare for comparable scenarios.

2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for organizations to independently identify adversarial tactics and techniques within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1. CyOTE Methodology applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. The program utilizes MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) as a common lexicon to assess triggering events. By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables, which could represent a faint signal of an attack requiring investigation. CyOTE can assist organizations in prioritizing their OT environment visibility investments.

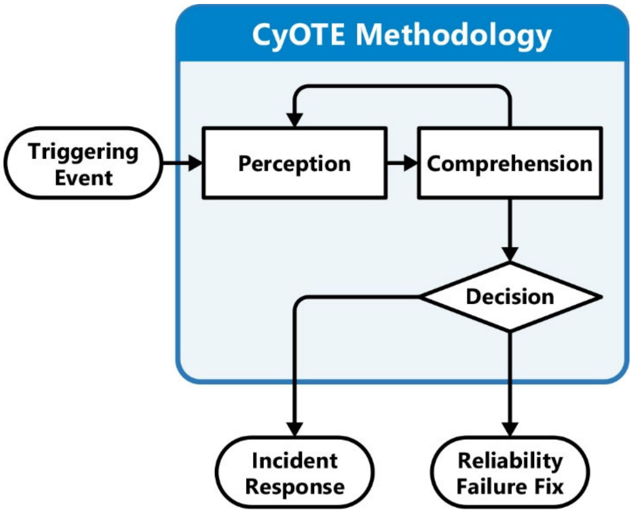

Figure 1. CyOTE Methodology

Historical case studies such as this one support continued learning through analysis of incidents that have impacted OT. This precursor analysis report is based on publicly available reports and provides examples of how key concepts in the CyOTE methodology appear in the real world, providing insights on how similar novel attacks could be detected earlier and therefore mitigated. The analysis enables OT personnel to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the precursor analysis report's cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the organization. The point on this timeline when each technique appears is critical to the organization's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since halting those techniques will generally have greater potential to limit additional attack vectors using other techniques, defeat the cyber attack, and limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes