Chapter 11
The APT Cyber Warriors With TTP Weapons to Battle:
An Review on IoT and Cyber Twin

Diana Arulkumar
Kalasalingam Academy of Research and Education, India

Kartheeban K.
Kalasalingam Academy of Research and Education, India

Arulkumaran G.
https://orcid.org/0000-0002-5166-3037
Bule Hora University, Ethiopia

ABSTRACT

Due to the blooming of Industrial 4.0 such as internet of things (IoT), cloud computing, industrial IoT (IIoT), and artificial intelligence (AI), with their innovative ideas and opportunities, the cyber attacker's modus operandi against the cyber defense triage is incredible. The genre of advanced persistent threat (APT) actors/group are equipped with sophisticated and substantial resources of tools, techniques, and procedure (TTP) at a breakneck pace. The IoT gadgets such as sensors, intelligent devices, and various rapidly emerging resources with energy, memory, and processing power are exponentially prone to multiple vulnerabilities. The nature of IIoT prompts heterogenous and rapid changes ranging the vulnerabilities from simple to complex attacks. APT menace follows the covert TTPs to target the asset of any organization like the government, military, or financial industry.

DOI: 10.4018/978-1-6684-5722-1.ch011

INTRODUCTION

In this pandemic covid season, the cyber warriors use disruptive cyber weapons as inexorable tide of the cybercrimes, data breaches, industrial espionage, and budding ruin of national infrastructure. The cyber incident reports leaves footprint impression and covering the tracks of new pernicious threats and drowning in tides of new risks. The challenges are due to sheer lack of knowledge about the new tools launched in the market and their consequence, the allocation of unsophisticated budget in mitigating the advanced cyber threats and unreliable attack vectors (one click, water holing, drive by downloads etc.). The data sources can be collected from external feeds, mining hacker discussion forums and academic researchers and also looping with security professional and their experiences.

In cyber era, millions of devices are connected through the internet, which is inevitability prone to vulnerable attacks by the perpetrators. The cyber actors whose are prone to espionage /sabotage different sectors, such as, industrial, military, economic, technical and intellectual property, financial extortion, and political manipulation. As there are numerous existences of cyber threats or zero-day threats, one among is Advanced Persistence Threat (APT). The APT are pernicious, highly – sophisticated, well-organized, with full spectrum proficiency of TTPs (Tactics, Techniques and Procedures or TTPs) and exploit target or IT networks of an organizations and cover their track and persist for long term endurance of access. WEBC2 backdoor family, that targets millions of computers to steal banking information and other credentials. The Three main operating systems are the sources which defines the structure of the cyber threats are Microsoft, Apple, and Linux. Many APT threat actors are capable of generating the variants of APT with Cyber threat intelligence (CTI). The CTI could be collected in 4 ways such as operational, tactical, technical and strategical.

The Internet of Things (IoT)is the most ubiquitous from Consumer (smart homes),Machine to Machine(mobile fitness devices, smart cities, smart factories, and the smart grid) and Industry the Industrial Internet of Things (IIoT) (smart agriculture).Among that IIoT is adopted and enabled by the cheap cost of affordable sensors, actuators, processors and its availability facilitates the real time data access possibility and from that the data can be analysis to predict the future events.

BACKGROUND

In order to categorize the identity of attackers, in 2006 APT Phrase is framed by U.S. Airforce Analysts. The characteristics of an APT attackers are well skilled and persistent, equipped with sophisticated resources and targeted. The APT attackers launch an attack in multi stages. The APT is multi stage model. Quintero-Bonilla