Chapter 3
Hacker and Non-Attributed State Actors

ABSTRACT

Chapter 3 sets the scene by exploring some challenges from both a technical and societal viewpoint and contrasts situations against an undertow of cyber-attacks. This chapter investigates various cases of how vulnerabilities originating from the software supply chain can have catastrophic outcomes when weaknesses slip through the net such as unpatched software or software misconfigurations during an organization's software maintenance regime. Examples are provided of high-profile hacks, security breaches, and cyber-attacks undertaken by hackers suspected of being affiliated to foreign states. These case studies provide various salient contexts as well as examples of threats, vulnerabilities, and their resultant impacts; ultimately, the consequence of flaws that create vulnerabilities occur through misconfigurations or from unpatched software weaknesses.

INTRODUCTION

This chapter explores high-profile and newsworthy security breaches that have not been directly attributed to nation-state entities. The author discusses these events over successive years. Additionally, the author identifies and discusses each root cause. This approach will build a picture of key catalytic circumstances behind these security breaches.

DOI: 10.4018/978-1-7998-3979-8.ch003

BACKGROUND

A colleague, who has worked in the cyber security profession for a considerable number of years, provided a view regarding the existing *status quo* and the ongoing defensive battle to protect oneself against ensuing cyber-attacks. He called this 'peak cyber.' 'Peak cyber' refers to the legacy vulnerabilities found in code that could top-out in the near future and potentially regress; this is because past weaknesses in code could be phased out due to rigor instilled by agile practices and regimes used as part of Development Operations (DevOps). This view has some credence on the basis that in 2015, 70% of vulnerabilities could be predated to at least 2013, and 44% of security breaches caused by vulnerabilities were at least two to four years old (Dignan, 2015). This was true of the infamous Heartbleed vulnerability (Synopsys Inc, 2019) that had been introduced as far back as 2011. It had the effect of discrediting Open SSL version 3 to the point that bodies such as the Payment Card Industry dropped legacy SSL as an adequate means of encrypting E2E communications in favor of TLS (Man, 2015).

Another offender was the Shellshock bug that, at the time that FireEye identified it in 2014, had been around for two decades. Shellshock was related to the Bourne Again Shell that is used extensively in a multitude of Linux servers connected to the Internet. The wider online adoption of such operating systems made this remotely exploitable vulnerability a serious problem (Lin & Seltzer, 2014). A more recent vulnerability reinforced the point that there are still problems. Dubbed the Mutagen Astronomy Integer Overflow Vulnerability, it resided within the Linux kernel and could enable an unprivileged user to gain superuser privileges. This weakness affected kernels 2.6.x, 3.10.x, and 4.14.x released between 2007 and 2017 and affected Red Hat Enterprise Linux, CentOS, and Debian distributions (Mitre, 2015; Kumar, 2018).

In addition, researchers have found that VxWorks, which is a Unix-like closed Real-Time Operating System (RTOS), has at least eleven vulnerabilities reaching back thirteen years. Industry deploys this RTOS across a variety of equipment ranging from commodity devices to aerospace assets (Khandelwal, 2019a). This has been surmounted by the panic caused by the Bluekeep vulnerability in May 2019. This flaw is associated with the Remote Desktop Services of legacy Microsoft Windows systems going back to Windows XP. Within two months, a weaponized exploit was available to attack unpatched systems (Cimpanu, 2019a). Subsequently, Microsoft found two Bluekeep-like