Chapter 4
Attributed State Actors

ABSTRACT

Chapter 4 looks at the technical aspects and effects of some attributed and high-profile state-sponsored cyber-attacks that have been encountered through our interaction with the networked world. Coverage also includes a look at the approach of nation-states against commercial companies as well as government institutions to achieve various objectives. The author uses these scenarios to focus attention on the important pillars of cyber security that all have important interrelationships in safeguarding of data and information. Within the context of their implementation, a weakness or series of weaknesses within one or more pillars can be enough to facilitate a cyber-attack. These pillars are underpinned by important factors, and the impact of improper cyber security considerations can be directly and indirectly problematic to continued e-commerce and our constructive evolution of knowledge sharing across the internet.

INTRODUCTION

In this chapter, the author discusses a number of cyber-attacks by state actors colloquially known as the 'high threat club.' The author uses the analysis of these high-profile security breaches to outline how society may better defend itself during users' interaction with cyberspace. The author will build upon examples provided in Chapter 3 to discuss the following categories of attacker groups (Chinnaswamy & Milford, 2019):

DOI: 10.4018/978-1-7998-3979-8.ch004

- **Industrial Espionage Campaigns:** First, industrial espionage campaigns target users to deploy home grown exploits and zero-days in order to exfiltrate data over protracted periods of time. As the author alluded to in Chapter 1, some hacker groups can be affiliated or used by nation-states to avoid attribution, and therefore, they may achieve their own goals and those of the state, potentially at the same time.
- **State Actors:** State actors undertake state-sponsored activities using weaponized malware to perform economic, espionage, or politically influenced actions by infiltrating many different public and private organizations and institutions. Depending on the actor, this may involve seeking financial reward for the state or even in some cases, seeking out PII.

BACKGROUND

In 2019, a little-known hacker group called 0v1ru$, which was aligned with the Digital Revolution group, hacked the Russian company SyTech. This contractor has been involved in cyber capability development on behalf of the Russian state-actor *Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii* (FSB) and had already been targeted by Digital Revolution in the past. This was the largest cyber-attack against the FSB, revealing 7.5 Terabytes of leaked secret projects, including a number of interesting capabilities such as The Onion Router (TOR) network de-anonymization project linked to the Kvant Research Institute (Abrams, 2019; Doffman, 2019). This haul has been appended by another series of tools also attained by Digital Revolution after a cyber-attack against the Kvant Research Institute and provided evidence of state sponsored Mirai malware use in 2016. In addition, this breach reveals the Russian Government's intention of targeting and attacking IoT devices through capabilities developed under the Fronton Program (Asif, 2020). Researchers stipulated that the use of default passwords, or hard coded credentials for that matter, was the instigator that allowed the Mirai botnet to infiltrate Linux-based commodity IoT (Hellard, 2018). This is just a small taste of the efforts, deviousness, and capabilities that can be used by state-actors.

Historically, researchers have blamed Russia and China for cyber-espionage activities, but the weaponization of cyberspace that has been gradually building over the second decade of the new millennium includes others, such as Syria, Iran, and Vietnam. Even the U.S. Office of Tailored Access Operations, which came to light after the Edward Snowden revelations, has also been branded