CTC 15

Marvin Newlin

CSCE 525

28 Nov 18

Nation states such as Iran, Russia, or China could attack our cloud services environment. Being that they are nations, they have the resources like manpower, machines, and experts that have nothing else to do but break into our systems. For example, they possess the resources to possibly leverage a Distributed Denial of Service attack on a cloud environment like an Amazon Web Services setup hosting government data like the Amazon Secret Region.

An actor at the criminal level could leverage cloud services as an attack platform as well. If they are able to leverage a cloud environment to break into a personnel system, they could use the power of cloud services to steal a large amount of private information which they could then sell on the black market and make money on. Additionally, actors such as hacktivists or even nation states as well may leverage cloud services to attack and steal information from our personnel systems (Ablon 2018). Nation states such as China could also leverage cloud services to steal intellectual property as they have done in the past (Ablon 2018).

Nation states could also utilize cloud services to perform reconnaissance on a large scale. In 2017, the Chinese group APT 10 was found to be conducting reconnaissance via malware on US systems (Vijayan 2017). If they were able to somehow get into a cloud service that the US government uses, then they could access a large amount of data on their reconnaissance missions.

**References**

Ablon, Lillian. 2018. “Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.” www.rand.org.

Vijayan, Jai. 2017. “China-Based Threat Actor APT10 Ramps Up Cyber ...” 2017. https://www.darkreading.com/attacks-breaches/china-based-threat-actor-apt10-ramps-up-cyber-espionage-activity/d/d-id/1328584.