Robert Scott Lake
IT-210-A
February 2, 2015

Entertainment and Mass Media: Software Vulnerabilities

Cyber attacks are increasing at an alarming rate and many industries are affected with dire monetary loss. Following is a brief history and account of just a few of these incidents and the outcomes thereof.

The entertainment and mass media industry is diverse with many different areas included under this heading, and can be classified into different categories such as exhibition, live, electronic and mass media entertainment. Within these categories there are numerous subcategories. Exhibition entertainment includes amusement and theme parks, art exhibits and museums among others. Live entertainment covers performance art, nightclubs, vaudeville and other adult establishments to name a few. Electronic entertainment encompasses video games, and SMS content along with social media outlets. Mass media comprises film, broadcasting (television and radio), the music industry, news media, the fashion industry and more. This all-encompassing industry provides escape and pleasure to the senses and is what many Americans work to live for in their free time. In the United States, in many cities and towns, one can find an outlet dispensing products that originate from this industry. The main centers of activity in the United States are New York and Los Angles, but as technologies advances, smaller or "indie" companies are competing with the powerhouses of Hollywood and the east coast venues.

Of any industry in the United States that may be vulnerable to attack, or the world for that matter, the entertainment and mass media is at the top of the list. As with any cybercrime, the individuals attacking want information whether it is the script to the newest movies that is only in the infancy of production, to a previously unreleased track on the new Taylor Swift album. Other types of attacks are hijack a news organizations twitter feed or possibly insert false information masked as coming from credible sources to be passed on to the general public, or to disrupt gaming networks frustrating millions of online game players during peak hours or days. At the root of these attacks, whether or not it is the violator's intent, companies stand to lose money damage their reputations. This industry controls the content many of us encounter throughout the day. ARNnet.com.au reported that cybercriminals have increased their attacks on the entertainment and media industry according to the Prolexic Q1 2014 Global DDoS Attack report with "54 percent of malicious packets mitigated by Prolexic during the first quarter [of 2013] were directed at this industry" (Karlovskyon, 2014.). Due to the prevalence and high

profile of this industry, there is no doubt that we have and will hear when major attacks occur.

Some of these incidents in recent months have occurred in the gaming, motion picture and video game areas of this industry. In 2013, hackers thought to be based in Iran "crippled the computer network of the giant Las Vegas Sands Corp… to punish [Sheldon Adelson] for saying that Iran should be bombed if it cannot be stopped from obtaining a nuclear weapon" (Ben-Gedalyahu, 2014). This attack from a malware virus wiped out several hard drives and sent engineers rushing to the casino floors to pull the network cords from the computers. This attack was not to siphon money from the casino but to do actual damage to the Sands Corp(Ben-Gedalyahu, 2014). According to the Mirror, over the last Christmas holiday, when thousands of new PlayStation and Xbox owners unwrapped their new gamming consoles and tried to login to Microsoft's Xbox live and the PlayStation Networks, many found that they could not access the network (Rkaina, 2014). This attack was the result of three individuals named the Lizard Squad, whose intent was to raise awareness of the low security at these companies (Rkaina, 2014). However, the most prevalent incident in the entertainment and mass media industry is the attack on Sony.

In the past few months Sony Pictures Entertainment reported that they were the victims of a cyber attack that crippled the company. Deadline.com reported that on Monday, November 24, 2014, on every employee's computer screen flashed a message that indicated that all of Sony's internal data had been obtained and that if certain demands were not fulfilled, all of their "top secret" information would be released (Robb, 2014). This information was subsequently released in several mass data dumps to the public. This information included internal e-mails discussing past, ongoing and future projects, movie scripts, payroll information, movies which were in theaters or previously unreleased were downloaded, e-mail and voice mail systems were down and many more systems were affected. The monetary damage is still unclear. Some report that it could be as low as $10 million up to $100 million; however, the full extent of the loss will be better six months down the road from the incident (Richwine, 2014).

Most of the above incidents came from out of the United States but cyber attacks are not limited to or originating from one location. The Sands attack is believed to originate in Iran in response to a comment made about Iran's possible obtainment of a nuclear weapon. In another instance a few individuals perpetrated the attacks against Xbox and PlayStation networks in order to raise awareness about the lack of security there. Finally, the attacks against Sony Pictures Entertainment is believed to be carried out by the North Koreans; however that claim is unclear at this time with some saying that it also looks as if a disgruntled

employee could be to blame ("Timeline of key events in the Sony Pictures Entertainment hack," 2014).

It seems all of these cases revolve around network security and the software programs that are involved there in. There are two people at the table when these systems are developed, the customer and the system engineer. There are two ends of the spectrum, ease of use for the end user or tight security. In each of these situations, there are tradeoffs that can leave systems vulnerable to attacks. What theses specific holes were we may never know. We do know they happen, and that they are preventable with better security, and data encryption at production and storage.

Sources

Ben-Gedalyahu, T. (2014, December 12). Cyber Attacks Crippled Adelson's Casino Firm because He Said "Bomb Iran." Retrieved from http://www.jewishpress.com/news/breaking-news/cyber-attacks-crippled-adelsons-casino-firm-because-he-said-bomb-iran/2014/12/12/

Karlovskyon, B. (n.d.). Media and entertainment industry targeted in cyberattacks. Retrieved February 2, 2015, from http://www.arnnet.com.au/article/543484/media_entertainment_industry_targeted_cyberattacks_/

Richwine, L. (2014, December 9). Sony's Hacking Scandal Could Cost The Company $100 Million. Retrieved February 3, 2015, from http://www.businessinsider.com/sonys-hacking-scandal-could-cost-the-company-100-million-2014-12

Rkaina, S. (2014, December 27). Playstation and Xbox attack: "Hacker says he targeted consoles for amusement." Retrieved February 2, 2015, from http://www.mirror.co.uk/news/world-news/playstation-xbox-cyber-attack-hacker-4881948

Robb, D. (2014, December 22). Sony Hack: A Timeline. Retrieved from http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/

Timeline of key events in the Sony Pictures Entertainment hack. (2014, December 18). [Text.Article]. Retrieved February 3, 2015, from http://www.foxnews.com/us/2014/12/18/timeline-key-events-in-sony-pictures-entertainment-hack/