Erik C. Sorto
CS 462
Dr. Andy Ramlatchan
November 29, 2025

Course Project Blog:
The Impact of the Insomniac Games Cyberattack

Introduction

Video games have had a huge impact on my life since I was a kid, starting with the original PlayStation released in the late 90's. It was this same era when the newly formed gaming studio Insomniac Games released their first game, Spyro the Dragon, one of the first PlayStation games I ever played. As technology rapidly evolved, so did their games from 3D platformers to creating vast worlds with some of the most memorable characters and stories. Some of their recent games had multimillion dollar budgets that would rival some of Hollywood's blockbuster movies They created one of my favorite video games of all time, Spider-Man for the PS4, which featured movie like storytelling and combined it with the best gameplay for any Spider-Man game. Unlike movies where you are just watching the story unfold and seeing the characters interact, in video games you are interacting with the world, engaging with the story and characters that other forms of media just can't replicate.

It is widely known that ransomware is a common cyberattack that affects a multitude of industries such as hospitals and banks, but I didn't consider gaming studios to be victims of such attacks. So, when I learned about the December 2023 ransomware attack which directly attacked Insomniac Game, it didn't feel like any other Company-that-got-hacked headline. This felt personal since it attacked a video game studio that I respected and created some of my favorite video games. Initially when this attack occurred, there was reddit post and YouTube videos with headlines that stated there were leaked pictures, videos and even gameplay footage of their upcoming game, Wolverines I was in complete shock since the game was in early development. However, when I found out that their employee's sensitive information was also comprised and leaked as well, it impacted me so much that it became the catalyst that pushed me to seriously pursue a career and major in cybersecurity.

In this report I will examine the Insomniac Games ransomware attack of December 2023. I will go over the background of the attack, how the attack worked, the impact it had on the company, and finally the industry-wide security lessons learned. Not only was there an operational impact of the attack, but most importantly the attack impacted people's lives and the studio's reputation.

Background on the Ransomware Attack

In December 2023, Insomniac Games suffered a major ransomware attack carried out by the Rhysida ransomware group. Rhysida was able to gain access to their network and obtain domain administration in under 25 minutes. They exfiltrated more than 1.67 terabytes of data from Insomniac's internal network, including early gameplay builds of their upcoming project Wolverine, development roadmaps, legal agreements with Marvel, proprietary tools, and confidential business documents. As a first-party PlayStation studio owned by Sony, Insomniac Games refused to pay the $2 million that was demanded by Rhysida which ultimately led to that data to be leaked online.

According to BBC Newsbeat, the attack left many employees of the studio and other gaming developers "extremely distressed," Insomniac made a public announcement stating how they were "saddened and angered" by they referred to as a "criminal cyberattack" (BBC Newsbeat, 2023). Insomniac publicly stated that they intentionally waited several days before making a statement of the matter so their employees could "support each other" and process how the attack and data breach emotionally took a toll on them.

One of the most concerning aspects of the breach was how it exposed personal employee data such as passports, PII, payroll information, and internal communications. In the Polygon article, it emphasized how catastrophic the employees felt for having one of their biggest upcoming project's playable testing builds leaked out to the entire internet, spoiling the game, which led to a huge effort of damage control since the only news thus far of this Wolverine game was a 45 second reveal trailer back in 2021, announcing the

studio's newest project. The fallout of this attack led to fear of identity theft, fraud, harassment, and of course the embarrassment of having such a high-profile studio which is revered in the gaming community to fall victim of a cyberattack of this magnitude. The studio finally released an official trailer of Wolverine in September 2025.

How the Attack Worked

While Insomniac did not publish a full technical breakdown, key details can be reconstructed from cybersecurity advisories, incident analysis, and Rhysida's known methods.

Initial Access through Phishing and Credential Theft

Rhyside commonly uses phishing emails that are disguised as password reset messages, multifactor authentication (MFA) prompts, or other official internal notices which are all common social engineering techniques. Modern gaming companies rely on remote access and stolen account credentials to provide entry immediately to internal networks and servers. Once the bad actor acquires the username and password, they can bypass the initial perimeter of defense.

Lateral Movement Through Windows Administrative Tools

After entering the targeted network, Rhysida typically moves laterally using "living off the land" techniques. Basically, abusing Windows tools like Powershell, PsExec, or similar

remote management programs. By moving laterally across various programs, they can covertly avoid raising alarms since their activities appear as normal administrative operations. Insomniac and other companies often utilize a series of development environments that are interconnected on build servers, and shared asset storage that is used within the organization. If the segmentation of their system is weak or if access controllers are in place improperly, then this could be a huge vulnerability, and the attack can simply pivot seamlessly across systems.

Data Exfiltration

This stage of the attack was the most devasting since Rhysida copied over a terabyte of data from Insomniac's network, consisting of internal communications through Slack, roadmaps for future projects, playable test builds, and private data from employees. The method of Exfiltration includes using encrypted archives, uploading tools from cloud storage, or custom scripts that move massive amounts of data without raising any flags that it is happening.

Ransomware Deployment and Public Leak

Once Rhysida has successfully infiltrated the network, exfiltrated the data, the next stage is to deploy ransomware to encrypt portions of the company's systems for the company to be out of control of the attack and be locked out. Insomniac refused to comply, and Rhysida subsequently published the data on their ransomware leak site. This tactic is

designed to pressure victims into paying the requested amount in this case of $2 Million and to cause reputational damage if they don't pay.

Impact of the Attack on Insomniac Games

Exposure of Employee Personal Information

One of the worst consequences of ransomware attacks is the exposure of employee private information such as passports, home addresses, family members, and financial data. For bad actors such as the Rhysida group, this is the usual target of data to acquire. It allows them to believe that they have the leverage to expect their victim to comply with payment. For the victim, there could be more long-term risks in having that sensitive data leaked such as identity theft, financial fraud, and even harassment.

For me, especially this was the part that made the attack feel the most personal. Leaking unfinished gameplay is one thing but targeting the private lives of the people who are just doing their job working on a project that they passionately love crosses a different line entirely. It revealed how cyberattacks can harm real people, not just companies, computer systems, or intellectual property.

Damage to Projects and Morale

Developers often spend several years developing a video game, especially a high-profile IP such as Marvel's Wolverine and are extremely particular to release any sort of gameplay

footage or trailer to the public until they feel for certain it is ready for the public to view. The attack led to leaked photos, videos, and even a playable test build of the game which was in an extremely early stage of development. This harmed the public's perception of the game since the game was in a rough state. This in turn placed an emotional pressure on the developers who had already been working on the game for at least 2 years and the public's perception of the game as being just reskin of their previous Spider-Man game. Apart from the leaks of the game, the roadmap of future projects was also leaked, forcing the studio to make adjustments to their future developments and strategies to marketing for the sake of damage control.

Industry-Wide Security Lessons Learned

The scale of the attack to such a high-profile gaming studio echoed all throughout the internet not only angering the studio but also their fans and alarmed other studios across the gaming industry to re-evaluate their security measures, so they too won't be another target. Around this time there were other high-profile gaming studios that fell victim to cyberattacks, notably Rockstar Games, the creators of Grand Theft Auto fell victim to a similar attack but ironically to a smaller hacking group. Gaming studios and companies of all sizes had a wake-up call to tighten their security measures, so they too won't become victims.

Many companies began reviewing their MFA policy enforcement, proper network segmentation, management of remote access tools, and comprehensive training for

employees especially regarding phishing emails and being vigilant to opening certain links, login requests despite how credible it may seem. With how common remote work has become to a lot of companies, especially game development, these precautions are more prevalent than ever. The ransomware attack on Insomniac Games proved that cybersecurity is no longer optional but a requirement to not only protect their intellectual property, but also the people who make the games that people love to play.

References

BBC Newsbeat. (2023). *Insomniac studio victim of huge hack*.

https://www.bbc.com/news/newsbeat-67805736

Cybersecurity and Infrastructure Security Agency (CISA). (2023). *#StopRansomware: Rhysida Ransomware*.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a