Grand Theft Auto VI Leaks (September 2022)

The greatest illegal disclosure of one of the most anticipated video games

AP/WRIT 2201

November, 17th 2022

By: Lovejivan Sidhu, Victoria Torkos, Yongju Lee, Farhan Aurnab, Joshua Plobner

Table of Contents

Introduction ---------- 3

Abstract ---------- 5

Executive Summary ---------- 6

Initial Leak & The Public's Response---------- 6

Rockstar's Response---------- 8

Border Hacking Group---------- 9

The Arrest---------- 10

Analysis ---------- 11

How the situation could have been worse ---------- 11

Effects on the Company and Workers---------- 13

Effect on Community---------- 14

Solution ---------- 15

Open Source Intelligence —---------- 15

Rockstar Improving Security---------- 16

Learning from Uber's Hack—---------- 17

Multi-Factor Authentication (MFA) / MFA Spamming---------- 17

Employee Training---------- 18

Conclusion ---------- 19

References ---------- 20

Introduction

As the world moves to a more digital age the opportunities for hackers have never been the same. As we move forward, we see that more and more companies are getting hacked by younger and younger people as a result of more technical adoption and more people are trying to hack companies due to the assets that the companies have. Hacking companies & groups have become more and more common as younger people learn programming languages and are able to start to find bugs and issues with programs written to protect companies. These people and groups then start to exploit the bugs for their personal gains, whether it be monetary or social gains [1]. This kind of hacking is known as black hat hacking, which is a type of hacking where there is clearly malicious intent, leading to unauthorized access to computer systems [2]. This was the same hat of hacking that happened with Rockstar Games, leading to GTA 6 files being taken at ransom, in this case, through unauthorized hacking resulting in illegal access to files, which was an attempt at a financial gain as people then offered a lot of money for that precious game data [3]. GTA 6 being hacked is very significant to the gaming community as there has not been a new game in the GTA franchise since 2013, and this hack had consequences for both Rockstar and the Community. Rockstar's stock price decreased 6% after the hack, which was not great at the time, and the long-term effects on the company's reputation have taken a hit, and can negatively affect the development of the game [4]. This hack affected the community in a major way because the development footage was a letdown for everyone due to the graphics being from GTA 5 but the animations and gameplay were from GTA 6 [5]. This hack is also significant to the security of game development, as we see that the hack occurred through the communication platform that was being used to share the footage, and not hacked directly off the servers of Rockstar games, leaving open doors for liabilities in the future as 3rd party communication software like MS Teams and Slack continues to be used [6]. This hack also

opens up the community to see the work that game developers are putting in, and the work that needs to be done to satisfy and meet the expectations of the community for this next revolutionary game [7].

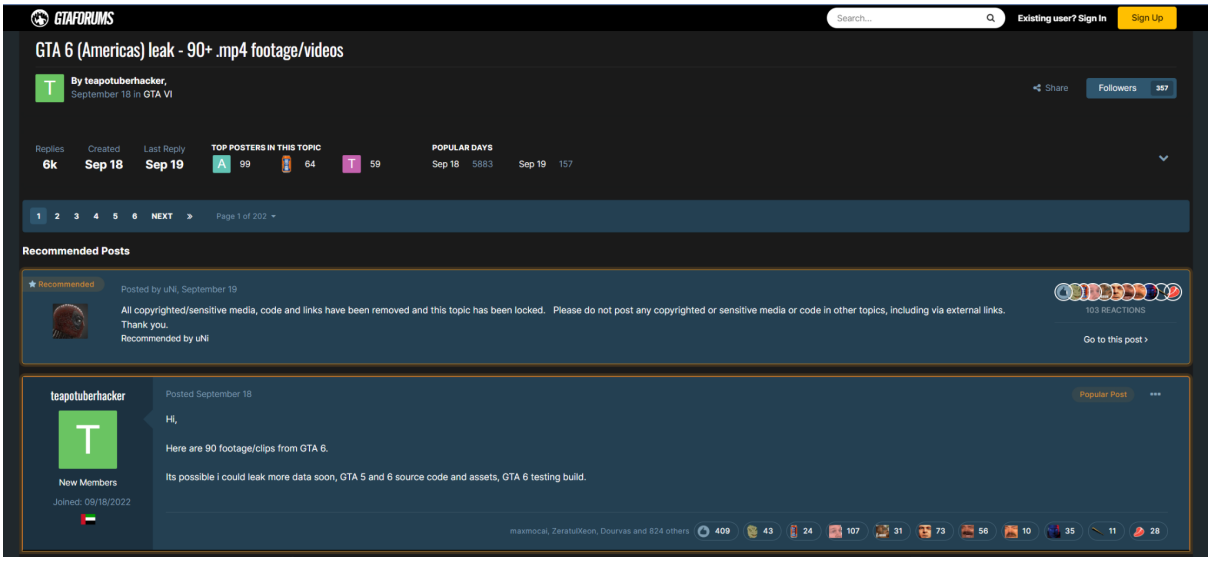
Abstract

This paper will examine the hack that took place on September 18th, 2022, and try to understand what happened, the issues associated with this hack, and the results on the community, developers, and company. This paper will also provide solutions to help improve game security by looking at the point of attack for this particular hack, and how it can be improved and more secure going forward to ensure that there is less variability in the future for Rockstar Games. This hack was one of the largest in the gaming industry ever, and left shockwaves across the gaming community at large due to the sheer amount of data being stolen and then uploaded and leaked [8]. Looking at the contents of the hack, we will see the true scale of what was stolen, from game development footage to game code, there were 3 gigabytes that were stolen and leaked [9]. Through this all, we will then see the Rockstar games respond to this incident, and further develop the situation that was only rumours in GTA forms and Reddit threads till this point. Later, we will also explore the effects on the gaming community, and start to see the community's response to the leaked footage and animations, which had mixed results. This will then form the basis for our analysis of the employees that work at Rockstar, as well as the effects on the company itself. We also will explore the hacking group, known as Lapsus$, and understand the type of hacking they do and why GTA was a target for them [10]. This paper will also understand the greater effects that would have taken place if the attack was more serious, and the results on the community, devs, company, and ultimately the game and its development schedule. We later will explore solutions, from Multi-Factor Authentication to Open Source Intelligence, it is important to understand how to prevent hacking like this from taking place again.

Executive summary

The initial leak and the public's response

On the 18th of September 2022, a day after the 9-year anniversary of the release of GTA V, footage of an in-development version of Rockstar's GTA VI was leaked online. The hacker originally posted a 3-gigabyte file to GTAForms under the username name teapotuberhacker [9]. The figure below shows the forms in which the original post was made, now missing the stolen and copyrighted content [12, Fig.1].



(Figure 1 shows the original website, GTAForums where the post was made)

The file included 90 videos of early gameplay of what he claimed to be GTA VI totaling 50 minutes of footage [9]. Within the post, the user also eerily mentioned his potential release of more detrimental data including the GTA V and GTA VI source codes [12]. Additionally, the hacker attempted to negotiate with Rockstar executives seeking payment to avoid further leaks he supposedly obtained [13]. At the time, fans were unsure if the leaks were genuine. The magnitude of the post even deterred users from opening the link or downloading the file. Those who viewed the leaks compared the footage to other games it resembled. Others believed them to be genuine due to the detail within the clips. The hacker replied to numerous

of these comments skeptical of the validity of the videos ensuring that what he had posted was legitimate. Incriminating himself further, he verified the method of acquiring the data. He plainly stated that the videos were accessed from Slack; a messaging application that Rockstar employees used to communicate. Teapotuberhacker claimed that he easily downloaded the files through this entry point [11] though it is unknown exactly how he got in. However, no matter the plausibility, individuals were quick to spread the leaks across social media outlets thinking that this incredible data must be seen. People reposted the videos and images to Twitter, Reddit, TikTok, and more with the intention to dissect the leaks and cover this potentially massive breach. Fans across platforms were able to get a glimpse into Rockstar's latest project unbeknownst to the company.

What is revealed and assumptions made

The surplus of videos demonstrated vital information about the highly theorized characters, setting, and enhanced features of the gameplay. Though, it is worth noting that the date on which these videos were recorded is not confirmed [13]. This means they could represent really early development subject to change and not the final outcome of the game. Yet, it is unlikely drastic story changes will be made due to this leak thus, broad assumptions can be made based on what is seen.

One of the most obvious questions addressed is the playable characters whose story the players will most likely be following. This includes the first Latina main character of the series seen in the first few videos of the 90. Dialogue subtitles dictated that her name is “Lucia”. The second protagonist can be described as a white male named “Jason” also discovered through dialogue subtitles. This dynamic sparks the idea of a Bonnie-and-Clyde-type storyline.

Purely based on the visuals, the map resembles that of Vice City, a fictional city often compared to the real-world Miami, Florida that first debuted in Rockstar's Grand Theft Auto:

Vice City released in 2002. This can be inferred from the characteristic palm trees, swamp-like areas, and similar infrastructure. The scenery also has an overall appearance of being more colourful when compared to other games in the series like GTA IV [13]. Unsurprisingly, the game also showcases new features and enhancements. Some are reminiscent of GTA V and other features seem to resemble characteristics of other Rockstar titles like Red Dead Redemption 2. Videos also show early animation tests for non-playable characters and improved physics.

Rockstar's response

For some time after the original post was made, fans were still in hot discussion over the legitimacy of the videos. All doubts came to a halt when Rockstar confirmed the breach of data in a tweet the company posted on September 19th, 2022 at 9:10 am. They confirmed that they suffered a network intrusion where “an unauthorized third party illegally accessed and downloaded confidential information” of early development footage for the next Grand Theft Auto [14]. Fortunately, they mention that there will be no major disturbance to the development of this project. The team was saddened to have their project revealed in this way. They concluded by thanking their fans for continued support through the predicament. The sensitive data was soon removed from the forum by moderators after this confirmation with the original thread being put back up afterward [9]. Though, as mentioned previously, the videos were spread out across platforms. Rockstar’s parent company, Take-Two Interactive, attempted to get a grip on the situation by issuing takedown orders to remove stolen footage and links from Youtube, Twitter, and the GTA subreddit [9][12]. Copyrighted material was removed and those in possession are not able to release the videos. Despite their efforts, it is still difficult to completely scrub the internet of these leaks. Even though the footage can no longer be reposted online, screenshots and videos are still floating around.

Commentary videos and news articles on the matter were also prevalent within the GTA community and news outlets.

Further serious matters lay in the arrest of the person responsible. Teapotuberhacker had the intention of negotiating with Rockstar employees by posting his email on GTAForms and requesting they contact him using their corporate email address [15]. Neither Rockstar nor their parent company Take-Two responded to this request. Instead, Rockstar began working with the Federal Bureau of Intelligence (FBI) to catch the alleged perpetrator.

Broader hacking group

The FBI suspected that this same person is linked to the ride-share service Uber cyberattacks creating a dual investigation that ultimately led to the hacker's capture. Based on the nature of the attack, investigators presumed that the individual responsible appeared to be part of a broader online hacking group under the name of "Lapsus$" or DEV-0537(classified by Microsoft). The FBI was made aware of them and is currently searching for members tied to the hacking group [16, Fig.2]

(Figure 2 shows an official FBI infographic requesting any information about the Lapsus$ hacking group)

This extortion-focused group targets companies and the government agencies [17]. Thus far, they have invoked cyber attacks on major companies such as Samsung in 2021, Ubisoft in 2022, T-Mobile in 2022, and more [18]. They were also responsible for the cyber attacks on Brazil's Ministry of Health systems in 2021[18]. Their primary infiltration strategy includes purchasing credentials on the criminal underground or from employees [17]. Members also communicate with victims through Telegram. Even though the usage has diminished, the hacker, in this case, proved to utilize this application when he attempted to negotiate with Rockstar employees.

The Arrest

Only a few days after the initial leak, on the 22nd of September 2022, a 17-year-old boy was arrested by the City of London Police in his home in Oxfordshire [19]. The suspect cannot be properly identified because he is a minor yet the source The Desk has identified his initials as “A.K”. He was arrested as he was suspected to be in connection with the “breach of computer servers at Rockstar Games and Take-Two Interactive” [20] as well as a variety of other charges including the attacks on Uber. The teenager was held in custody and appeared in Highbury Corner Youth Court on the 24th of September [21]. Prosecutor Valerie Benjamin stated in court that “the suspect had used a phone to hack into companies and was “holding them to ransom” to gain access to illegally obtained software”[22]. He pled guilty to other charges such as breaching his bail conditions yet not guilty to computer misuse says City of London detective inspector Micheal O’Sullivan [21]. As of writing, he is being held in a youth detention center [21].

Analysis

How the situation could have been worse

The leaks, though extremely revealing in nature, were not as detrimental as they could have been in general and when compared to previous attacks on other video game production companies. Essentially, the videos and screenshots only gave the public a glimpse into the visuals of Rockstar's latest project. Though it is not the way Rockstar Games wanted to have their work displayed, it is undeniable what the hacker obtained will not directly affect the production of the game. A GTA maker stated that there would in fact be no “long-term effect on development” [23] due to the breach. However, it is unfortunate that deeply awaited information such as the playable characters and location has been discovered. It is safe to assume that Rockstar would have preferred to release teasers on their own terms. Luckily, the leaks do not disclose any crucial storyline information therefore, the project still retains some element of secrecy. Moreover, the breach presented financial impacts to the parent company Take-Two Interactive. Their share price suffered and tanked 6% the day after the breach and seemed to rebound slightly some time after [24]. Via google finance, this drop can be seen to double then finally pick back up [25, Fig. 3].

(Figure 3 shows Take-Two Interactives stock market value via Google Finance over a 6-month period. The highlighted area represents the dip suffered from the time the leak was published to the point where it began to pick back up)

Furthermore, Rockstar was spared as the source code for the game was not among the leaks. Via GTAForms, where the hacker posted the videos, teapotuberhacker mentioned that he obtained the GTA V and GTA VI source codes and put them out on ransom. It is unknown if he actually had access to the codes but, if this was true the financial and legal effects on the company could have been amplified. Outsiders with access to these codes could result in the inspection of how an infamous Rockstar game is put together [26]. They may be able to exploit the software used to create the game, ultimately leading to people obtaining the games for free and Rockstar losing money they otherwise would have earned. Rival game studios could also utilize this information to better their products. The fact that the FBI caught the perpetrator before he had the chance saved Rockstar in this sense.

In comparison to other historical video game leaks, the results of Rockstar's intrusion were quite tame. The game-developing company, CD Projekt Red, recently suffered a cyber attack and leak of some of their most popular titles. Among other company information, the hacker, in this case, had access to the source codes of the company's projects such as *Cyberpunk 2077, Witcher 3, Gwent,* and more. The hacker left a ransom note and offered to negotiate with the company similar to the intent of teapotuberhacker. What sets these breaches apart is that Rockstar had their perpetrator apprehended before he was able to release anything else. On the other hand, CD Projekt Red, publicly refusing to negotiate, suffered the consequences as the attackers claimed to have sold the data online to a bidder [27]. Though it is not known what of this data is sold, the company is still left to fear that their trade secret for video game development (and other sensitive data) is circulating around waiting to fall into the wrong hands and be used against them in their craft.

Effects on the Company and Workers

As technology has grown, information has started to be the most precious property of individuals and society. The reason why hacking is increasing is that hackers can earn a lot of money from it and that inventing technologies themselves requires a lot of money and time. The invention has lower productivity and profit, rather than taking other's tech or source. Furthermore, the increasing number of hacking puts people in danger. It is not only for an individual risk but also for some companies that could be in danger. If the company ignores these risks in modern society, they can be cyber-attacked by unknown sources. It could be leaking user information to social media such as Twitter, Facebook, or Instagram. Leaks affect the company and workers possibly causing negative effects such as losing their motivation to make the game, spending more money to hire white hackers, and losing profit. Yet, leaks can also have a positive aspect to them with the possibility for developers to receive feedback and the publicity brought around the company.

Primarily, the negative effect of leaks on game developers is that they will feel a loss if the game is leaked. It is related to their motivation to make their game because they do not get any accomplishment in the situation causing them to reduce their productivity. This means the workers can not do their work efficiently, which may delay publishing dates. Moreover, leaks can result in a loss of profit for the company. For instance, the video game No Man's Sky was hacked and leaked before publishing. The players will be disappointed with the game's problems such as some bugs and poor graphics. The game is not already finished to build because it is an early access version. Jennifer Mendez argued that "in turn, the opinion and rumour mill affects sales, without so much as giving a game a chance." [28]. It means that the player already tried the game, but it is not even a beta version. Due to these issues, people may refuse to buy the game thus, resulting in a loss in money. The company may then go bankrupt and not be able to afford to pay workers' salaries. Lastly, the company

may have to invest in hiring a white-hat hacker. The definition of a white-hat hacker is “a hired person for an organization to help the owner through ethical hacking find and fix weaknesses in the system’s security before black-hat hackers exploit them.” [29] Nowadays, companies are at serious risk of cyber-attacks and breaches. To protect their information, companies need to hire more white-hat hackers. However, the number of white hat hackers in our society is minimal due to it being a difficult field to master. Additionally, protecting a company's property is more difficult than hacking others’ information. This means the salary of a white hat hacker is really high pressuring the company to prioritize money over security.

On the other hand, the leaking of information has minor positive effects such as getting user feedback and free advertisements. Receiving feedback early on can be helpful as they can receive input from those who will be purchasing their game when it is finished. If players are not satisfied, they still have time to change their plans or fix the graphics, story, or anything that would deter a mass amount of people from giving the company money to obtain their game. Furthermore, leaks can positively be interpreted as free advertisements. With all the current publicity around Rockstars' highly anticipated game, the addition of this media coverage only draws more attention to the company. Conversely, this may cause a negative reaction from the public but, Rockstar employees have been seeing great support from their fans who understand the struggle and the difficult times this situation presents.

Effects on the Community

The effects of the leaks additionally impact the consumers of the game. The gaming community as a whole can be affected by the incident through the sensationalization of hackers, shifted feelings of anticipation, and fabricated assumptions around the game. Being the popular franchise that it is, the Grand Theft Auto VI leaks received massive amounts of media coverage. Though the hacker is not directly exposed, the magnitude of his actions can be seen to attract publicity. Especially among young teens perusing the internet, this can bring

about the idea that conducting such unethical deeds will result in attention. Additionally, the leaks may have either diminished or amplified anticipation for the game. GTA VI has been greatly anticipated since it has almost been 10 years after the release of the previous game in the series, GTA V. The impact the last game had on the gaming community forged a hunger for the next installment in the GTA franchise. Updates to GTA Online and the disappointing announcement of GTA V "Expanded and Enhanced" in June 2020 only fuelled the flames of fans' desire for GTA VI. Rockstar announced in February 2021 that their next game is in development where, at that point, the mystery was in the hands of the creators. Yet, after enduring these leaks, a lot of that secrecy was lost. This may cause more disinterest and distrust in the company and new game with the surrounding negative connotation of how they suffered a breach. On the other hand, there are fans that will not be turned away. Being such an infamous franchise and highly awaited, people would still purchase the completed project regardless. Furthermore, community members may unjustly come to conclusions before the final project is even officially released. On Twitter, many people were expressive on how the game looked unfinished and substandard for a Rockstar production. These people, whether serious or not, are spreading inequitable negative opinions surrounding the GTA VI title causing more unrest among the community. However, there presented more sensible fans who realized that an in-development version does not equate to the final product of the game itself.

Solutions

Open source intelligence

The gaming world was left in a state of immense dismay after the Rockstar Games source code was almost made public, and this prompted investors to lose faith in the company. Increasing their investments in greater intelligence, data security, system

protection, and cybersecurity is their best chance of warding off this threat. These are all areas that need to be protected. After the most recent hack, one option they can put into action is to hire additional employees who have prior expertise working with open-source intelligence. Open-source intelligence helps to increase transparency, so employees are better able to track changes to code. Just recently, it was reported that this is exactly what they are going to be doing, especially considering that they have already begun hiring a large number of investigation analysts [30, Fig. 4]. As a result, the fact that they are already employing this tactic is a very good indicator that they are taking the issue very seriously.

(Figure 4 shows that Rockstar is looking to hire more employees in this department due to the leak)

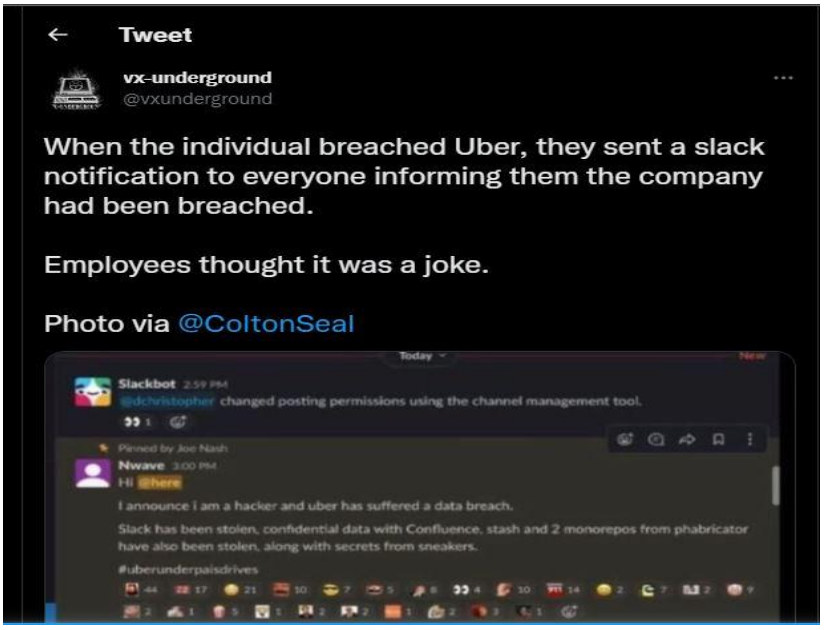
How Rockstar Games Can Improve Their Security

All of the infrastructure devices in a company's network need to have the most recent operating systems and patches installed, as well as be configured in accordance with the company's internal security policies and any applicable government or industry regulations. [31]. If Rockstar Games wishes to keep its reputation and fans intact, then these things must be in order. In order for Rockstar Games to make their system more secure, they should

investigate how other businesses have dealt with hacks of a similar nature and then model their own response.

Learning From The Uber Cyber Attack

Rockstar Games is in a position to learn from the Uber Cyber Attacks since the hacker group used hacking methods analogous to those used in the Uber Cyberattacks. Specifically, hackers breached Uber's security by tricking an employer via Slack [32, Fig. 5]. This allows Rockstar Games to gather expertise from this similar event. They can take the necessary precautions, similar to what Uber did when they were hacked, to reduce the likelihood of future cyber attacks.



(Figure 5 shows how Uber's security was compromised)

Multi-Factor Authentication (MFA) / MFA Spamming

Since Rockstar games was hacked by the same group that hacked Uber, it is possible that they stole all employee credentials in a similar fashion. For instance, Uber was a victim of the MFA fatigue attacks so it is possible that Rockstar games were also likely victims of the same type of attack since it was done by the same group of hackers. [33]. The term "MFA fatigue" refers to a strategy employed by cybercriminals to bypass multi-factor authentication

and get access to user accounts. These cybercriminals are able to do this by exploiting a weakness in the system. One strategy the hackers take to bypass the multi-factor authentication is to repeatedly ask users to prove their identity until one of them eventually gives in. Rockstar Games may easily prevent this type of breach in the future by implementing two simple measures: reducing the number of attempts at identity verification a user is allowed before their account is locked and increasing the amount of time that elapses between prompts [34].

Training Employees About MFA Fatigue Attacks

It is essential to train workers on MFA fatigue attacks because if they do not know what this type of attack is, then they will not be able to cope with the circumstances in the future. That said, if Rockstar wishes to prevent their security from being breached, it is imperative that they educate their employees on what an MFA fatigue attack is and how hackers take advantage of this type of hack to steal information. Also, Rockstar Games needs to make sure that its employees are aware of who they should go to for help in the event that they run into any problems related to cyber attacks like MFA fatigue [34]. This will make it possible for the IT department to provide assistance to employees with tasks such as resetting their passwords for affected services [34]. Therefore, in the event that employees were successfully duped by the MFA fatigue spammings laid out by the hackers in order to steal information, the most logical move for them to take would be to consult the IT department immediately before it gets out of hand. Taking from the Uber cyber attack, security was breached when employees used the Slack platform to click on phishing links that were provided by hackers. Due to this tragic occurrence, Uber has instructed their workers to refrain from using Slack until further notice. This is critical because the alleged hacker gained access to an unprotected Slack channel used by Rockstar employees and duped one of those employees to provide their secure login credentials [35]. Therefore, Rockstar Games can take

some preventative measures by educating their employees on the importance of exercising caution when using communication platforms such as Slack.

Conclusion

While on the surface video game leaks seem relatively harmless, diving deeper can reveal how much effect they can cause the company and community. This monumental leak of Rockstar's newest grand theft auto project presents this adequately. Though the breach of data could have been even more serious and caused more of a problem for Rockstar’s team, it still had a significant impact on the company's employees and the gaming community as a whole. Security should now be closely investigated by Rockstar and enhanced to attempt to eliminate the possibility of a further attack. Potential starting points would be hiring more workers familiar with open-source intelligence, operating on updated systems, and educating their staff on how to recognize attacks when presented with suspicious scenarios. Through these methods, defense against attackers would be strengthened thus reducing the chances of a leak as such from happening again.

References

[1] M. Weaver, “Teenage hackers motivated by morality not money, study finds,” The Guardian, 21-Apr-2017. [Online]. Available: https://www.theguardian.com/society/2017/apr/21/teenage-hackers-motivated-moral-crusade-money-cybercrime. [Accessed: 24-Oct-2022].

[2] O. Buxton, “Hacker Types: Black Hat, White Hat, and Gray Hat Hackers,” Hacker types: Black Hat, white hat, and Gray Hat hackers, 12-Oct-2022. [Online]. Available: https://www.avast.com/c-hacker-types#:~:text=Hackers%20fall%20into%20three%20general,hacking%20is%20malicious%20or%20illegal. [Accessed: 07-Nov-2022].

[3] A. Shome, “GTA 6 hacker was allegedly offered 2.2 bitcoin for Leak,” Sports news, 09-Oct-2022. [Online]. Available: https://www.sportskeeda.com/gta/rumor-gta-6-hacker-allegedly-offered-2-2-bitcoin-leak. [Accessed: 07-Nov-2022].

[4] J. Sirani, “Is the GTA 6 leak gaming's biggest theft ever?,” IGN, 22-Sep-2022. [Online]. Available: https://www.ign.com/articles/gta-6-leak-gamings-biggest-theft. [Accessed: 07-Nov-2022].

[5] J. Aguilar, “Fan reactions to leaked GTA 6 graphics are misplaced, and here's why,” Dot Esports, 18-Sep-2022. [Online]. Available: https://dotesports.com/general/news/fan-reactions-to-leaked-gta-6-graphics-are-misplaced-and-heres-why. [Accessed: 07-Nov-2022].

[6] N. Carpenter, “Rockstar Games blames hacker for major GTA 6 leak,” Polygon, 19-Sep-2022. [Online]. Available: https://www.polygon.com/23360809/gta-6-leak-hack-rockstar-games-confirmed. [Accessed: 07-Nov-2022].

[7] G. Colantonio, “Why the grand theft auto 6 leak is bad for Rockstar and fans,” Digital Trends, 19-Sep-2022. [Online]. Available: https://www.digitaltrends.com/gaming/grand-theft-auto-6-leak-opinion/. [Accessed: 07-Nov-2022].

[8] J. Sirani, “Is the GTA 6 leak gaming's biggest theft ever?,” IGN, 22-Sep-2022. [Online]. Available: https://www.ign.com/articles/gta-6-leak-gamings-biggest-theft. [Accessed: 14-Nov-2022].

[9] K. MacDonald, K. Stuart, and A. Hern, “Grand Theft Auto 6 Leak: Who Hacked Rockstar and what was stolen?,” The Guardian, 19-Sep-2022. [Online]. Available: https://www.theguardian.com/games/2022/sep/19/grand-theft-auto-6-leak-who-hacked-rockstar-and-what-was-stolen. [Accessed: 07-Nov-2022].

[10] “Defending against attacks,” Microsoft: Security Insider, 20-Oct-2022. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-insider/uncategorized/defending-attacks/. [Accessed: 14-Nov-2022].

[11] teapotuberhacker. “GTA 6 (Americas) leak - 90+ .mp4 footage/videos”, GTAForums, [Online]. 18-Sep-2022 Available: https://gtaforums.com/topic/985481-gta-6-americas-leak-90-mp4-footagevideos/#comments [Accessed: 07-Nov-2022].

[12] M. Murphy, “Grand Theft Auto VI footage leaked after Hack, developer Rockstar confirms,” BBC, 19-Sep-2022. [Online]. Available: https://www.bbc.com/news/technology-62960828. [Accessed: 07-Nov-2022].

[13] Matthew Judge [DarkViperAU] “GTA 6 HAS LEAKED! THIS IS ACTUALLY REAL! - Detailed Analysis”, YouTube, 18-Sep-2022. [Online]. Available: https://www.youtube.com/watch?v=AXAHsa3twYg. [Accessed: 07-Nov-2022].

[14] Rockstar Games, “A Message From Rockstar Games”, Twitter, 19-Sep-2022. [Online]. Available: https://twitter.com/RockstarGames/status/1571849091860029455?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1571849091860029455%7Ctwgr%5E3b90bdc10d4363f4822ade42b96c1d80e37cae43%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fvariety.com%2F2022%2Fdigital%2Fnews%2Fgrand-theft-auto-6-leak-rockstar-games-hack-1235376727%2F [Accessed: 07-Nov-2022].

[15] J. Middler, “GTA 6 leaker claims he's looking to negotiate a deal with Rockstar,” VGC, 19-Sep-2022. [Online]. Available: https://www.videogameschronicle.com/news/gta-6-leaker-claims-hes-looking-to-negotiate-a-deal-with-rockstar/. [Accessed: 07-Nov-2022].

[16] “LAPSUS$,” FBI, 28-Mar-2022. [Online]. Available: https://www.fbi.gov/wanted/seeking-info/lapsus. [Accessed: 14-Nov-2022].

[17] “Defending against attacks,” Microsoft: Security Insider, 20-Oct-2022. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-insider/uncategorized/defending-attacks/. [Accessed: 07-Nov-2022].

[18] “Lapsus$,” Wikipedia, 04-Nov-2022. [Online]. Available: https://en.wikipedia.org/wiki/Lapsus$. [Accessed: 07-Nov-2022].

[19] City of London Police, Twitter, 23-Sep-2022. [Online]. Available: https://twitter.com/CityPolice/status/1573281533665972225?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1573281533665972225%7Ctwgr%5Ed6904ad42cb6faf20ace31f2a74076bfc8b3f67b%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fkotaku.com%2Fembed%2Finset%2Fiframe%3Fid%3Dtwitter-1573281533665972225autosize%3D1 [Accessed: 07-Nov-2022].

[20] M. Keys, “Police arrest Rockstar hacker who leaked Grand Theft Auto 6 Data,” The Desk, 24-Sep-2022. [Online]. Available: https://thedesk.net/2022/09/grand-theft-aut-6-hacker-arrested-oxfordshire-uk/. [Accessed: 07-Nov-2022].

[21] T. Phillips, “Grand Theft Auto 6 hacker teen suspect held in Youth Detention Centre,” Eurogamer, 27-Sep-2022. [Online]. Available: https://www.eurogamer.net/suspected-gta-hacker-teen-held-in-youth-detention-centre. [Accessed: 07-Nov-2022].

[22] T. Ivan, “GTA 6 hacker suspect pleads not guilty to computer misuse charges,” VGC, 27-Sep-2022. [Online]. Available: https://www.videogameschronicle.com/news/gta-6-hacker-suspect-pleads-not-guilty-to-computer-misuse-charges/. [Accessed: 07-Nov-2022].

[23] T. Phillips, “FBI investigate Hacker allegedly behind Rockstar GTA 6 leak,” Eurogamer, 23-Sep-2022. [Online]. Available: https://www.eurogamer.net/fbi-investigating-hacker-who-claimed-to-have-breached-rockstar-and-uber. [Accessed: 10-Nov-2022].

[24] E. Makuch, “Take-two's share price sinks after GTA 6 leak,” GameSpot, 19-Sep-2022. [Online]. Available: https://www.gamespot.com/articles/take-twos-share-price-sinks-after-gta-6-leak/1100-6507634/. [Accessed: 10-Nov-2022].

[25] “Take-two interactive software, Inc common stock (TTwo) stock price & news,” Google Finance. [Online]. Available: https://www.google.com/finance/quote/TTWO:NASDAQ?sa=X&ved=2ahUKEwj4ifyEyK77AhUfK1kFHUvUAc4Q3ecFegQILRAg. [Accessed: 14-Nov-2022].

[26] L. Gordon, “Everything we know about the rockstar games grand theft auto 6 leak,” Vulture, 21-Sep-2022. [Online]. Available: https://www.vulture.com/2022/09/grand-theft-auto-6-leak-explained. [Accessed: 10-Nov-2022].
[27] J. Porter, “Cyberpunk 2077 developer says its hacked data is circulating online,” The Verge, 11-Jun-2021. [Online]. Available: https://www.theverge.com/2021/6/11/22529199/cyberpunk-hack-data-leaked-online-employee-game-data. [Accessed: 10-Nov-2022].
[28] J. Mendez, “No man's leak: The polarizing effects of game leaks,” Black Shell Media, 12-Aug-2016. https://blackshellmedia.com/2016/08/12/no-mans-leak-polarizing-effects-game-leaks/, [Accessed: 14-Nov-2022].
[29] Giusel, “Why do companies need to hire white-hat hackers?,” Medium, 23-Nov-2021. https://medium.com/@giusel/why-do-companies-need-to-hire-white-hat-hackers-e50e2c410cb5. [Accessed: 14-Nov-2022].
[30] A. Sahbegovic, “Rockstar seemingly improving their security since GTA 6 leak,” Rockstar seemingly improving their security since GTA 6 leak, Sep. 23, 2022. https://www.sportskeeda.com/gta/news-rockstar-seemingly-improving-security-since-gta-6-leak [Accessed Nov. 11, 2022].
[31] K. Poireault, “Grand Theft Auto Publisher Rockstar Games Hacked,” Infosecurity Magazine, Sep. 20, 2022. https://www.infosecurity-magazine.com/news/gta-publisher-rockstar-games-hacked/ [Accessed Nov. 11, 2022].
[32] “Twitter,” Twitter. https://twitter.com/vxunderground/status/1570626503947485188 [Accessed Nov. 11, 2022].
[33] A. Shome, “Who leaked GTA 6? Everything to know about the alleged hacker so far,” Who leaked GTA 6? Everything to know about the alleged hacker so far, Sep. 26, 2022. https://www.sportskeeda.com/gta/who-leaked-gta-6-everything-know-alleged-hacker-far [Accessed Nov. 11, 2022].
[34] J. Köller, “MFA Fatigue: Everything You Need to Know About the New Hacking Strategy,” tenfold Security, Oct. 07, 2022. https://www.tenfold-security.com/en/mfa-fatigue/ [Accessed Nov. 11, 2022].
[35] @CNBCTV18Live, “Plug those loopholes — what happened at Rockstar Games could happen to any company,” cnbctv18.com, Sep. 20, 2022. https://www.cnbctv18.com/technology/if-security-is-slack-what-happened-at-rockstar-games-could-happen-to-any-company-14763071.htm [Accessed Nov. 11, 2022].