**The Activision Data Breach of December 2022**

Mike Green

Old Dominion University

CYSE-300

Dr. Joseph Kovacic

May 21, 2023

On December 4, 2022, Activision experienced a data breach that resulted in the exposure of both confidential employee information and confidential details about Call of Duty content that was set to be released throughout 2023. The hackers gained access by means of a social engineering technique known as phishing, and they specifically targeted employees of Activision that had the permissions/privileges to see and/or access this information. The hackers sent text messages to multiple employees claiming to be an “Activision Automated SMS Dispatcher,” that was addressed to the employee, and had a link to a website where they would have to input their login credentials. Once they input their credentials, the hackers then sent another message to the employee that told them to respond with the two-factor authentication code that was sent to them, possibly via email. If the employee responded back with the two-factor authentication code, it is assumed that the login credentials were valid. An employee fell for the phishing attempt, and from there the hackers gained access to confidential employee information such as employee salaries and work locations.

The main vulnerability that led to this breach of data dealt with a lack of employee information security awareness, training, and/or education. Just by examining the images of the text message chats from these phishing attempts, it becomes clear that not everyone who was sent these messages was educated properly on this topic. There is incorrect grammar in one of the messages; computers/AI/automated messages do not typically make grammatical errors since they are programmed/trained not to do so. That was the first warning sign of the phishing attempt. The second warning sign, from an objective standpoint, was the fact that the text message sent from an unknown source involved employment status. Typically, issues of employment status are handled through various websites, employee portals, in person etc, with methods of authentication like multiple security questions, as an example. Besides all of that, messages from an unknown source, objectively, should not be trusted unless advised otherwise.

The data breach, and the method in which the data was obtained, is a prime example of why the user is the weakest link when it comes to information security. While all these phishing attempts were happening, no employees alerted the IT Security team or whoever handles IT security for Activision. In addition, the company itself did not alert any of the employees that this data breach occurred until late February 2023 (the breach occurred in the beginning of December in 2022). The cybersecurity measures that should have been taken to mitigate the consequences of this breach strictly deal with information security education and awareness. Had the employee that granted access been educated/trained and keen enough to spot the warning signs of this phishing text and been aware of the fact that the text was from an unknown source, there is a high chance this would not have happened, based off of the fact that the other employees saw that it was a phishing attempt. This data breach and lack of communication ultimately altered the plans of Activision for 2023, and probably changed the way other companies and both current & future employees view the company.

References

Drapkin, A. (2023, February 22). *Activision Suffers Data Breach, Call of Duty Plans Stolen*. Tech.co. <https://tech.co/news/activision-data-breach>

*Call of Duty 2023 Plans Revealed in Possible Activision Data Breach*. (2023, February 20). Game Rant. <https://gamerant.com/call-of-duty-2023-plans-activision-data-breach/>

*Security Breach at Activision: The Importance of Reporting Incidents - Kaduu CTI*. (2023, February 23). <https://kaduu.io/security-breach-at-activision-the-importance-of-reporting-incidents/>

‌

‌

‌