Activision Dec 2022 Social Engineering Attack and Data Breach

Date Written by Intel	February 28th, 2023
Incident Name	Activision December 2022 Social Engineering Attack and Data Breach
Date of Public Report	**February 27th, 2023**
Date of Incident	December 4th, 2022
Summary	Activision is a video game developer most famous for creating Call of Duty and World of Warcraft. They are currently in negotiations to be acquired by Microsoft. On February 20th, 2023, cybersecurity researchers at vx-underground posted on Twitter that Activision had been breached on December 4th, 2022. The attacker phished employees via SMS and was able to gain access to the network and steal sensitive information. Vx-underground posted screenshots from the breach on Twitter which show details of the schedule for the upcoming Call of Duty release and that an Activision employee's Slack account had been hacked. Activision did not initially announce that it had been breached but a spokesperson told online news outlet Bleeping Computer that the company had come under attack in early December. The spokesperson said that at this time there were attempts to phish employees via SMS which the company quickly intervened to stop and that no employee details, player data, or game data were breached in this attack. This, however, contradicts reports from Insider-Gaming and vx-underground. Insider-Gaming analyzed the breached data and determined that an HR employee for Activision was compromised, which led to the attacker getting ahold of employee information.
February 27th, 2023	The hackers that breached Activision have published the employee data from December 2022 on a popular breach forum. Activision has yet to comment on this data leak.
Key Social Engineering /OSINT Themes	• Recon - Activision employee and organizational information harvested. The hacker leveraged exposed employee information to conduct a social engineering attack. • Smishing - The attacker sent a convincing SMS message to certain employees which prompted one of them to click on a link. Once the user clicked on this link, they were presented with a legitimate-looking phishing site that prompted them for credentials. The attacker then used the harvested credentials to gain unauthorized access.
Picnic's Recommended Remediations **For An Automated Solution, Contact Picnic**	• User social engineering awareness training • Identify and block newly registered domains similar to your org's. This way if used in an attack (e.g., user clicking), the request to domain is blocked. • Monitor for expiring domains which could be leveraged for the above. • Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possible. • Regularly review any external facing components to understand exposure. Allow those that are trusted, remove those that are not, and ensure MFA is securely configured for all accounts. • Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party. • Regularly audit employee access to one of least privilege (including offboarding). • Regularly audit 3rd party access to one of least privilege. • Monitor and remove sensitive information disclosure, including exposed employee phone numbers.
Industry	Video Games
Actor	TBC

Motivations	TBC
Related Hacks	Riot Games, Coinbase, Twilio
Breach Notice/Company Notice	No formal notification
Other Sources	https://www.vice.com/en/article/pkg7pn/hacker-breaches-activision-slack-steals-call-of-duty-info https://twitter.com/vxunderground/status/1627477748359872513 https://www.bleepingcomputer.com/news/security/activision-confirms-data-breach-exposing-employee-and-game-info/ https://techcrunch.com/2023/02/21/activision-did-not-notify-employees-of-data-breach-for-months/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAzqOzRBIWlr916KK9Ou09tbtUn7fv7DADOfsEAowdiunc4ECoHzPcA86K9iofvGhAm5ujt4aQQowuObQnjbPC-DRSm-FhtnSFSyqvScnyftIlOIxLvSHf_-qOjEWV7EJpjjaBceotXQFP2fLp3b4fn1zeV7FaJQC_T7gxcymYvR https://insider-gaming.com/activision-data-breach/ https://www.bleepingcomputer.com/news/security/hacker-leaks-alleged-activision-employee-data-on-cybercrime-forum/