Insomniac Games Ransomware Attack

- Pratham Badge

In Number 2023, Insomniac Games, a subsidiary of Sony Interactive Entertainment, was attacked by the Rhysida ransomware group. The attackers gained unauthorized access to the company's network through phishing techniques and exploiting system vulnerabilities. The got access to approximately 1.67 terabytes of sensitive data consists of 1.3 million files.

On 12th December 2023, Rhysida publicly announced about the data breach and demanding a ransom of 50 bitcoin and threatening to auction the data on the dark web if their demands were not fulfilled. Insomniac with respect to Sony neglected and failed to negotiate. So Rhysida group released 98% of the stolen data on their dark web site. That included sensitive employee information, internal communications and in development materials for the upcoming Marvel's Wolverine game. The leaked data compromised operation integrity of Insomniac and exposed personal information of over 400 employees including ID Scans, Disciplinary Reports and Internal HR Documents.

Rhysida ransomware attacked involved use of multiple layers of infiltration and exploitation techniques the firstly get Phishing Farming attacks were performed to get login credentials and then get access to the internal network . VPNs were used to be to prevent detection of access from outside network of Insomniac. Cobalt Strike Framework was used to exploit system and navigate through servers and deploy the ransomware payload effectively and without any detection. Rhysida used vulnerabilities in Remote Desktop Protocol (RDP) these exploitations allowed them to gain unauthorized access to the systems through brute force attacks and exploiting weak passwords. The Rhysida Ransomware uses Chacha20 encryption mechanism for file encryption and making data inaccessible without the decryption key. This ransomware also modifies system settings to display ransom notes and create schedule task for persistence. Before encrypting files, they exfiltrated sensitive data from Insomniac Systems which was used for double extortion and threatening to publish all stolen data if ransom is not paid.

The attack was possible and viable because of Multi-Factor Authentication MFA were not used so because of this so simple and immature mistake in Insomniac's IT Infracture, Rhysida got access to login credentials so easily and rest was exploited because of this single point of failure that let Rhysida make this attack successful.

Insomniac Games and Sony Interactive Entertainment have initiated several mitigation strategies to address the breach and enhance their cybersecurity posture:

1. **Data Breach Notifications:** Insomniac promptly notified affected employees about the breach, detailing the nature of the stolen data and the potential risks involved.
2. **Extended ID Monitoring Services:** The company offered two additional years of complimentary credit monitoring and identity restoration services through ID Watchdog to affected employees.
3. **Dedicated Support Channels:** A call center was established to assist employees with inquiries related to the breach and provide necessary support.
4. **Enhanced Cybersecurity Training:** Implementing comprehensive training programs to educate employees on recognizing phishing attempts and other social engineering tactics.
5. **Multi-Factor Authentication (MFA):** Strengthening access controls by implementing MFA across all critical systems to reduce the risk of unauthorized access.
6. **Regular Security Audits:** Conducting frequent audits and vulnerability assessments to identify and remediate potential weaknesses in the IT infrastructure.
7. **Incident Response Planning:** Developing and regularly updating an incident response plan to ensure swift action can be taken in the event of future breaches.
8. **Network Segmentation:** Implementing network segmentation to limit the spread of ransomware and protect sensitive systems from being compromised.