Adobe Cyber Attack: Vulnerabilities, Impacts and Lessons Learned

[1]Ishita, [2]Narpat Suthar, [3]Devraj Singh, [4]Dhruv Parekh

[1]Asst. Professor
AIDS
Arya Institute of Engineering and Technology, Jaipur
[2]Asst. Professor
Computer Science Engineering
Arya Institute of Engineering Technology & Management, Jaipur
[3] (Research Scholar)
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur
[4] (Research Scholar)
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur

Abstract: This paper presents the findings of a comprehensive study on the notorious 2013 cyberattack targeting Adobe. Its primary objective is to unravel the impact, aftermath, and the invaluable lessons derived from this incident within the domain of cybersecurity. The study delves deep into the attack methodologies, the nature of compromised data, and Adobe's response strategies.

1. Introduction

In 2013, a significant event occurred in the world of cybersecurity which shook the security standards of the whole world and exposed the vulnerabilities not just within adobe but also across the whole IT world.

It was one of the biggest data breaches of the 21st Century which resulted in an information leak of 153 million Adobe accounts with each containing sensitive information like passwords and credit card details.

As digital landscape continues to change and new threats continue to evolve, the insights gained from the Adobe cyberattack remain highly valuable. This paper aims to provide the details about the adobe attack and pointing out the importance of safeguarding our digital assets and lessons learnt from the Adobe Attack.

Adobe’s Significance

Adobe is an American multinational computer software company founded in 1982 in United States. Adobe gives a wide variety of software services such as photoshop, acrobat etc. These tools are widely used across the globe in different kinds of industries. Adobe has an extensive user base and the nature of data it handles makes it a prime target for cybercriminals.

Nature of Attack

Adobe witnessed a horrendous cyber-attack in 2013 resulting in significant damage to the users and the Corporation. The Attack occurred in October 2013 when a cybercriminal group successfully hacked a backup server of adobe leading them to the database of adobe. The motive and the identity of hackers is still unknown.
This incident was an alarm to all the organizations about the increasing cyber threats and impact of cybersecurity and safeguarding resources digitally.

Attack Methods

Attackers used various types of methods in process to perform the attack. Attackers used a spear phishing attack using emails to adobe employees to steal the credentials. Hackers then hacked into their network and installed malware on target devices. Later on, they managed to access the data from adobe’s server through encryption and other techniques to hide their tracks at the initial stage of the attack. The combination of these attacks created a such complex attack that posed a challenge against the security teams.

Data Compromised

The 2013 Cyberattack resulted in a substantial compromise of data resulting in loss of data for both company and customers. Millions of users lost their valuable data and credentials to hackers.

Attackers managed to access a vast amount of user data such as Passwords, Phone Numbers and credit card details.

The source code of adobe was also accessed by the attackers, a source code worth of a lot of value which can further result in more vulnerabilities and exploits.

Adobe's Response and Lessons Learnt

After this attack Adobe made some big changes in their security system and removed the old, hacked database and informed all the users, banks and law about the breach as well as working on safeguarding users account after the server got hacked.

This attack showed the mirror to the adobe and whole cybersecurity community about their security standards. Here are some of the key points that were learned by this attack:

- Regular software updates and security patches
- Better data encryption techniques and safeguarding stolen data.
- Threat analysis and response teams with a well-defined response plan
- This attack highlighted the importance of enhancing security against third party apps.
- This attack served as remainder for whole world and adobe how important cybersecurity is.

2. Conclusion

The 2013 adobe cyberattack was a remainder for the whole world to take cybersecurity more seriously. It highlighted the need for data encryption and regular software patching. This breach also emphasized the significance of safeguarding data and digital assets. The lessons learned

from this breach have had a long-lasting impact on the big IT organizations and users on the importance of cybersecurity and data security.

References

[1] P. K. Bhatt and R. Kaushik, "Intelligent Transformer Tap Controller for Harmonic Elimination in Hybrid Distribution Network," 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2021, pp. 219-225

[2] R. Kaushik, O. P. Mahela and P. K. Bhatt, "Events Recognition and Power Quality Estimation in Distribution Network in the Presence of Solar PV Generation," 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 2021, pp. 305-311

[3] Jain, B.B., Upadhyay, H. and Kaushik, R., 2021. Identification and Classification of Symmetrical and Unsymmetrical Faults using Stockwell Transform. Design Engineering, pp.8600-8609.

[4] Rajkumar Kaushik, Akash Rawat and Arpita Tiwari, "An Overview on Robotics and Control Systems", International Journal of Technical Research & Science (IJTRS), vol. 6, no. 10, pp. 13-17, October 2021.

[5] Simiran Kuwera, Sunil Agarwal and Rajkumar Kaushik, "Application of Optimization Techniques for Optimal Capacitor Placement and Sizing in Distribution System: A Review", International Journal of Engineering Trends and Applications (IJETA), vol. 8, no. 5, Sep-Oct 2021.

[6] G. Kumar and R. Sharma, "Analysis of software reliability growth model under two types of fault and warranty cost," 2017 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, 2017, pp. 465-468, doi: 10.1109/ICSRS.2017.8272866.

[7] Kumar, G., Kaushik, M. and Purohit, R. (2018) “Reliability analysis of software with three types of errors and imperfect debugging using Markov model,” International journal of computer applications in technology

[8] T. Manglani, A. Vaishnav, A. S. Solanki and R. Kaushik, "Smart Agriculture Monitoring System Using Internet of Things (IoT)," *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022, pp. 501-505.

[9] R. Kaushik *et al*., "Recognition of Islanding and Operational Events in Power System With Renewable Energy Penetration Using a Stockwell Transform-Based Method," in *IEEE Systems Journal*, vol. 16, no. 1, pp. 166-175, March 2022.