SECURITY ARTICLES

VIKRAMADITYA REDDY VARKALA

Z1973679

**ARTICLE 1: Microsoft: Solar wind hackers access source code**

The SolarWinds hack, which came into the limelight December 2020 is believed to be operated by a state-sponsored group from Russia .It is the largest and most sophisticated cyberattacks ever reported that targeted multiple government agencies and private companies .

The hackers infiltrated SolarWinds systems and planted a bug into a software update that was then used by the company's customers.This bug allowed the hackers to infiltrate the networks of multiple U.S. security departments as well as major tech companies such like Microsoft,Cisco etc.

Microsoft disclosed that the hackers were able to access a small portion of their source code repositories, but did not have access to the code for any of their major products or services. Microsoft stated that like other firms it found malicious versions of SolarWinds’ software inside its network.The company also said that they had found no evidence of the hackers using their access to compromise any Microsoft systems or customer data.

**How the company could have stopped from the crime:**

Preventing a cyber attack like the SolarWinds hack is a difficult task, but there are several steps that companies can follow to reduce the risk

* They should implement strong cybersecurity measures, such as using multi-factor authentication, encrypting data, and regularly updating software and systems.
* They should implement fraud detection software.
* They should train their employees on cybersecurity best practices and also train them in security awareness programs.
* Regular vulnerability assessments help companies identify shortcomings in their systems and hence can upgrade them before they get exploited by hackers.

Sources:

* <https://www.theverge.com/2021/7/14/22577471/microsoft-solarwinds-hack-zero-day-serv-u>
* <https://www.reuters.com/article/us-global-cyber-microsoft/solarwinds-hackers-accessed-microsoft-source-code-the-company-says-idUSKBN2951M9>

**ARTICLE 2: T-Mobile :Data breach of 37 million user accounts**

T-Mobile had revealed the company’s second major breach in less than two years, admitting that a hacker was able to obtain customer data, including names, birth dates, and phone numbers, from 37 million accounts. he telecom giant said in a [regulatory filing](https://www.sec.gov/Archives/edgar/data/1283699/000119312523010949/d641142d8k.htm) on Thursday that it currently believes the attacker first retrieved data around November 25th, 2022, through one of its APIs.

T-Mobile says it detected malicious activity on January 5th and that the attacker had access to the exploited API for over a month. The company says it traced the source of the malicious activity and fixed the API exploit within a day of the detection. T-Mobile says the API used by the hacker did not allow access to data that contained any social security numbers, credit card information, government ID numbers, passwords, PINs, or financial information.

**How the company could have stopped from the crime:**

* T-Mobile could have implemented stricter authentication measures, such as multi-factor authentication or rate limiting, to prevent unauthorized access to their APIs.
* Regular monitoring of network activity and data access.
* Regular employee training on security best practices and how to recognize and report suspicious activity can help prevent successful attacks.
* T-Mobile could have encrypted customer data to prevent unauthorized access.Implementing strict access control measures

Sources:

* <https://www.theverge.com/2023/1/20/23563825/tmobile-data-breach-api-customer-accounts-hacker-security>
* <https://www.wired.com/story/tmobile-data-breach-again/>

**ARTICLE 3: Facebook: 553 million users data leak**

Facebook has been grappling with data security issues for years.The 533 million user data leak, also known as the Facebook-Cambridge Analytica data scandal, was a massive data breach that occurred in 2019 but came to lime light in April 2021.The availability of the data set was first reported by Business Insider. According to that publication, it contains information from 106 countries including over 32 million records on users in the US, 11 million on users in the UK, and 6 million on users in India.It includes phone numbers, [Facebook](https://www.theguardian.com/technology/facebook) IDs, full names, locations, birthdates and email addresses.

After the data leak was discovered, Facebook stated that the data was scraped in the year 2019 due to a vulnerability in its contact importer feature. The data was then sold on the dark web, and it is unclear how many people have access to it. This data is potentially valuable to cybercriminals, who could use it to conduct phishing attacks, identity theft, and other types of fraud.

The company also stated that it had fixed the vulnerability once it was discovered. Facebook has encouraged users to check their privacy settings and enable two-factor authentication to protect their accounts. Facebook has taken steps to improve its data security, including increasing the number of security researchers on its team and implementing new protocols for third-party access to user data.

**How the company could have stopped from the crime:**

* Facebook could have implemented stronger security measures like implementing multi-factor authentication, encryption, and more rigorous testing of its features and code which prevents hackers from exploiting vulnerabilities in the platform.
* Facebook could have implemented better monitoring of its platform to detect unusual activity, such as large-scale scraping of user data.
* Facebook could have implemented stricter controls on third-party access to user data, they should monitor their systems for suspicious activity and implement fraud detection software.
* The company should have been transparent about any breaches and should have notified affected users as soon as possible.

Sources:

* <https://www.bbc.com/news/technology-56815478>
* <https://www.theguardian.com/technology/2021/apr/03/500-million-facebook-users-website-hackers>
* [https://en.wikipedia.org/wiki/Facebook–Cambridge\_Analytica\_data\_scandal](https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal)