Dell data breach on May 2024

In May, Dell alerted customers to a massive data breach after a threat actor claimed to have obtained data on about **49 million** people. Dell started sending out notifications, confirming that a portal containing customer information regarding purchases had been breached.



Dell’s statement at the time disclosed that the leaked data consisted of: customer names, physical addresses, order service tags, item descriptions, order dates, and warranty information. Fortunately, no financial or payment information, email addresses, or phone numbers were involved, which Dell believed helped reduce the potential risk to customers.

The cybercriminal, identified as **Menelik**, had attempted to sell the stolen data on the Breach Forums hacking site, claiming it included records of purchases made between 2017 and 2024. Dell immediately launched an investigation and notified affected customers. The company reassured users that no highly sensitive information had been compromised.

Cyber Kill Chain

**Reconnaissance:** The threat actor, "Menelik," likely gathered information about Dell's systems and infrastructure, focusing on the partner portal as a potential entry point. This involved exploring Dell's partner portal and discovering an unsecured Application Programming Interface (API). The API lacked proper authentication mechanisms, making it susceptible to unauthorized access.

**Weaponization:** Leveraging the information gathered, Menelik devised a method to exploit the unsecured API. By systematically generating and inputting service tag numbers—unique identifiers assigned to Dell products—into the API, the attacker could retrieve corresponding customer data

**Delivery:** The delivery phase involved automating the process of inputting service tag numbers into the vulnerable API. This automation allowed for the efficient extraction of vast amounts of customer information over a period of several weeks.

**Exploitation:** By exploiting the API's lack of authentication controls, Menelik gained unauthorized access to sensitive customer data. The compromised information included customer names, physical addresses, hardware details, order information, and warranty specifics. Notably, financial data, email addresses, phone numbers, and passwords were reportedly not affected.

**Installation:** The installation phase pertains to the attacker's establishment of a persistent method to continue data extraction. By maintaining access to the unsecured API and automating data retrieval, Menelik ensured ongoing exfiltration without detection.

**Command and Control:** While traditional C2 involves establishing a channel to control compromised systems, in this scenario, the attacker had maintained control over the data extraction process through the automated scripts interacting with the vulnerable API.

**Action:** Having amassed a substantial volume of customer data, Menelik proceeded to monetize the breach. The stolen information was advertised for sale on hacker forums, posing significant risks for affected customers, including potential identity theft and targeted phishing attacks.

Prevention and Mitigation Strategies

To mitigate breaches of this nature, organizations like Dell should implement a multi-layered defence strategy:

1. **Advanced Threat Detection and Response**: Implementing robust **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS)** can help detect lateral movement early.
2. **Multi-Factor Authentication (MFA)**: MFA should be mandatory across the organization, especially for high-privilege accounts. It reduces the risk posed by stolen credentials.
3. **Regular Vulnerability Scanning and Patching**: Regular scanning of internal systems, combined with timely patching of vulnerabilities, is essential to close the door on exploit attempts.
4. **Behavioural Analytics**: Using **User and Entity Behaviour Analytics (UEBA)** can help identify anomalous behaviour, such as unexpected data access or unusual data exfiltration patterns, even if an attacker is using legitimate credentials.
5. **Zero Trust Architecture**: Adopting a **Zero Trust** model ensures that every request, both inside and outside the network, is verified before granting access to resources, minimizing the risks associated with lateral movement.

Conclusion

In conclusion, we can say that this particular breach underscores the critical importance of securing APIs with more robust authentication and authorization mechanisms to prevent unauthorized data access. The leaked data of about 49 million costumers makes this one of the biggest data breaches of 2024 and a lesson for organisations to take cyber security more seriously.