Case Study

Cryptojacking

Tesla

Attack Category: Cryptojacking

1. Description:

- Cryptojacking: Cryptojacking is a type of cyber attack where unauthorized actors exploit vulnerabilities in a target's system to use their computing power to mine cryptocurrency without their knowledge or consent. This attack has gained prominence in recent years due to the increasing value of cryptocurrencies like Bitcoin.

2. Statistics:

- In 2017, cryptojacking attacks increased by 8,500% compared to 2016. By 2018, over 42% of organizations had experienced a cryptojacking attack.

Sources:

- Malwarebytes
- Tesla

Company Description and Breach Summary

1. Company Description:

Tesla is an American multinational company that designs, manufactures, and sells electric vehicles and clean energy products and services

2. Breach Summary:

- 2018, February: Unauthorized access to Tesla's cloud environment is detected.
- 2018, February: Tesla's security team responds and mitigates the threat.
- 2018, March: Tesla notifies law enforcement and launches an investigation.
- 2018, April: Tesla completes the investigation and implements additional security measures.
- 2018, May: Tesla discovers that the threat actors gained access using stolen credentials.
- 2018, June: Tesla confirms that no customer or company data was accessed or exfiltrated.

Sources:

- Tesla

Timeline

1. 2018, February:
Unauthorized access to Tesla's cloud environment is detected.

2. 2018, February:
Tesla's security team responds and mitigates the threat.

3. 2018, March:
Tesla notifies law enforcement and launches an investigation.

4. 2018, April:
Tesla completes the investigation and implements additional security measures.

5. 2018, May:
Tesla discovers that the threat actors gained access using stolen credentials.

6. 2018, June:
Tesla confirms that no customer or company data was accessed or exfiltrated.

Vulnerabilities

Vulnerability Summary: Weak passwords, Unpatched Systems, and a lack of Multi-Factor Authentication allowed hackers to easily gain access to Tesla's cloud environment which was insufficiently monitored

Weak Passwords

The threat actors gained access using stolen credentials with weak passwords.

Lack of Multi-Factor Authentication

Tesla's cloud environment did not have MFA enabled for all accounts.

Insufficient Monitoring

The unauthorized activity went undetected for some time due to insufficient monitoring.

Unpatched Systems

Some systems in the cloud environment were not up-to-date with the latest security patches.

Costs and Prevention

Costs	Prevention
• Tesla did not disclose the financial impact of the attack. However, the cost could include investigation, remediation, and potential downtime	• Enforce strong, unique passwords and MFA for all accounts. • Implement strict access controls and privileged account management. • Enhance monitoring and detection capabilities. • Regularly patch and update systems.