CS352: Cybersecurity Principles

Semester 1, 2025

Assignment - Report 1

Title: Analysis of the 2025 Oracle Cloud Data Breach: Contributing Factors, Technical Details and Cybersecurity Implications

Abstract

This report examines the 2025 Oracles cloud data breach, highlighting the overview of the security incident including compromise of more than 140,000 customers sensitive information and credentials, initial response from Oracle of denying the breach and a technical analysis of the breach highlighting the CVE vulnerability. The analysis delves into how the unpatched vulnerability in the Oracle fusion middleware were exploited by the threat actor "rose87168" and methods used to compromise the security of the cloud infrastructure leading to a long-term impact on Oracle along with the users of the cloud services and the related stakeholders. The report outlines the possible failure in Oracles security policies that led to the data breach such as lack of patch management and identify the security gaps leading to the compromise. Furthermore, the report highlights mitigation techniques to avoid any future risks.

Declaration

I hereby acknowledge that this report titled “Analysis of the 2025 Oracle Cloud Data Breach: Contributing Factors, Technical Details and Cybersecurity Implications” is my original work. All sources used have been referenced using IEEE referencing style.

Name: Vishant Chand

Student ID: S11219214

Course: CS352

Date: 24TH April 2025

Signature: *VChand*

Table of Contents

Introduction: Understanding Cybersecurity Principles and Theoretical Aspects

A strong cybersecurity foundation relies on core principles which are put in place to protect digital assets of individuals and organizations where data is key for organizational function and providing consistent services. Cloud service providers such as Oracle provide services such as cloud storage to store confidential data on their cloud infrastructure. Therefore, it is important to prioritize these principles to ensure that the customers' data is safe. These cybersecurity fundamentals are referred to as the CIA triad which compromises:

- **Confidentiality**: This ensures that sensitive information is only accessible to authorized individuals. This can be achieved through access controls and encryption. However, this principle was violated in context of the Oracle Cloud breach where SSO passwords and LDAP passwords were compromised leading to unauthorized access to confidential information.
- **Integrity**: This focuses on data consistency and accuracy. Ensuring that data is not altered by unauthorized people. Manipulation of an organization's data can affect the overall operations and affect its related services.
- **Availability**: Ensures that data and systems are available when needed and operating as intended when required for access or use by authorized individuals. If a successful cyberattack occurs such as a ransomware attack or data leaks, then this can affect the availability of essential data or services. This can be seen in the case of Oracles data breach where affected customers were asked for ransom, or their sensitive information would be sold on the dark web. [1]

These three elements are crucial in maintaining a secure and robust cloud environment. If one of those is violated, then there is a possibility of a data breach. A data breach is when confidential, sensitive or protected information about a person is exposed to an unauthorized individual [2] .

Relevance of compliance standards

The Oracle Cloud Infrastructure and its related services adhere to cybersecurity compliance standards. They provide a framework for trust and security in this digital world. This helps protect a company's reputation, maintains customers' trust and allows for a secure and reliable cloud environment for its global customers.

The ISO/IEC 27001 framework focuses on managing and identifying security risks to ensure there is confidentiality, integrity and availability (CIA) being maintained in an organization [3].

GDPR (General Data Protection Regulation) is a regulation that is concerned with individuals' personal data and right to privacy [4]. It focuses on individuals' rights to privacy as everyone should have the right to know how their data is being collected, stored and used. It also ensures that there is transparency and accountability when personal data is processed [5].

Ethical responsibilities in cybersecurity

Cloud service providers such as Oracle Corporation need to adhere to ethical responsibilities when dealing with sensitive data of customers. They need to follow all legal compliance (e.g. ISO 27001, GDPR) and be transparent and take accountability if a security incident occurs which Oracle wasn't effective as seen in this recent data breach [6].

Overview and Understanding of the 2025 Oracle Cloud Data Breach

Overview of the Breach

The Oracle cloud infrastructure provides the performance of on-premises hardware with greater flexibility for applications, resource sizing, pricing and deployment locations. OCI offers 150-plus cloud services in each cloud region [7]

On the 21st of March 2025, a major security breach was announced by CloudSEK which involved compromise of the Oracle Cloud's login system. A threat actor named "rose87168" on the dark web forum BreachForums made a post claiming to have access to Oracle Cloud's login servers. This included sensitive data of users with 6 million records exfiltrated including encrypted SSO (Single sign-on), LDAP credentials, JPS (Java Platform Security) keys. This has compromised over 140,000 customer tenants' information [8] .

This leaked data is crucial for user authentication and security of the OCI (Oracle Cloud Infrastructure). The attacker has demanded ransom from companies to remove their data from the list before it is sold on the dark web. Additionally, the threat actor is willing to trade the stolen data for zero-day exploits with other cybercriminals.

The compromised data reportedly includes:

- Encrypted SSO passwords: one set of credentials allows users to sign in on multiple applications or websites. If compromised it can lead to unauthorized access.
- Encrypted LDAP passwords: These are passwords that are stored as hashed format and are used for user authentication without revealing the actual password.
- Enterprise Manager JPS keys: It is used for the Oracle Enterprise Manager for managing access and encryptions.
- Java Key Store (JKS) Keys: stores authorized certificates, public and private keys for encryption and SSL. [9]

Timeline of the Events

Date	Event
Feb 9-15, 2025	Initial breach where the threat agent "Rose87168" allegedly gains unauthorized access to login.us2.oraclecloud.com by exploiting a vulnerability and claims to have stolen 6M records affecting the 140,000+ tenants across multiple regions.
Late Feb 2025	Rose87168 gets in contact with Oracle and demands 200M USD to exchange details about the vulnerability exploited. Oracle refused and no deal was made.
Mar 3, 2025	Proton mail of Rose87168 could be found as text file on login.us2.oraclecloud.com when accessed by Internet Archives, showing that the threat actor has some level of access
Mar 21, 2025	Rose87168 makes a public post on BreachForums announcing the exchange of 6m stolen data records in exchange for money or zero-day exploits. The hacker also asks for help with decryption and if companies want their data to be removed then they had to pay a fee.
Mar 22, 2025	Oracle denies breach saying that "No breach of Oracle Cloud. Published credentials not for Oracle Cloud. No customer data lost." However, the server 'login.us2.oraclecloud.com' which contained the mail address of the hacker was taken offline.
Mar 23-24, 2025	Cybersecurity outlets such as (CloudSEK, BleepingComputer) start investigations on the zero-day exploit. Customers claim to receive messages to reset Oracle passwords.
Mar 25, 2025	Situation escalates further when Rose87168 releases 10,000 lines of sample data which was exfiltrated from the Oracle server. The situation remains unsolved.

[10]

Technical Breach Insights

The threat actor had allegedly compromised the Oracles login endpoint on the subdomain (login.us2.oraclecloud.com), it was running a vulnerable version of Oracle Fusion Middleware. This subdomain was taken down since the hack.

According to FOFA (a cyberspace search engine), the oracle fusion middleware server was last updated around 27th September 2014. It had a critical vulnerability addressed as "CVE-2021-35587" which affected the OpenSSO Agent (Oracle Access Manager). This was added to CISA KEV (Known Exploited Vulnerabilities) in December 2022.

The Oracle Access Manager, which is a component of the Oracle Fusion Middleware, had known critical vulnerabilities affecting versions:

- 11.1.2.3.0
- 12.2.1.3.0
- 12.2.1.4.0

This vulnerability allows an attacker who has access to the network via HTTP to compromise OAM (Oracle Access Manager). Successful exploitation can possibly lead to complete control of the Oracle Access Manager. This breach had mainly occurred due to Oracles' poor patch management [11].

Impact of the Breach

According to CloudSEK, the breach has had significant impacts such as:

- Mass Exposure: Over six million sensitive data from users including authentication data have been compromised and are now at risk of being sold on the dark web leading to greater security concerns.
- Ransom Demand: The hacker "rose87168" has demanded ransom payment of 20M from Oracle and undisclosed fee payment from affected customers to remove their data from ending up on the dark web.
- Credential Compromise: The hacker has access to encrypted credentials, however if the credentials are decrypted or cracked, it could lead to further breaches. (WK 8 LECTURES)
- Zero-Day Threat: The oracle server had unpatched vulnerability that was exploited, and this indicates the possibility of more overlooked vulnerabilities that could pose a security risk.
- Supply Chain Fallout: The data breach can not only affect Oracle but also its customers as they rely on various services [12].

Initial Oracle Response

Oracle has been privately warning customers regarding the breach where the threat actor had stolen confidential information and client credentials stored on the vulnerable server. According to reports by cybersecurity firms, throughout March and April Oracle has been privately communicating with its clients to address the breach even though Oracle has not publicly addressed the breach yet. The company wrote in an email to one of its clients stating that "the hacker did access and publish client usernames from two servers that

were not part of the Oracle Cloud infrastructure". However, FBI and CrowdStrike are investigating this incident further.

CISA stated that having access to sensitive credentials such as usernames, passwords, emails, authentication keys and encryption keys can increase the severity risk for organizations. This allows attackers to benefit from the extracted information by using it to gain privileges to unauthorized systems through Identity Management System, conducting more attacks such as phishing and identity theft. According to at least three Oracle cloud customers who have confirmed to news outlets that their information was in the leaked data set [13].

Topic- Risk Mitigation, Policies and Defense Strategies

Risk Assessment and Mitigation

Risk identification involves the process of identifying and documenting potential risks to an organization. This can include data breaches, insider attacks or natural disasters that could interrupt viable systems. Some risks can be categorized as having a low impact while others may have a higher impact. However, it is important to have systems in place to help identify risks in a timely manner [14].

Mitigation refers to taking prior actions such as fixing software vulnerabilities and preventing any potential exploits by threat actors. It is crucial to identify what assets need to be protected, what the current security risks are identified and measures taken to address those risks to protect assets such as company and customers data to be compromised. According to ISO 31000, the following risk treatment mitigation methods can be adapted by organizations [15]:

- Risk Avoidance: Avoid any task or activity that involves risk or could lead to it.
- Risk Reduction: Proactive measures to avoid the chances of a threat occurring by implementing security measures such as Firewalls, software patch management and regular system updates.
- Risk Sharing or Transfer: Involves referring the risk to another party faced by an individual or entity. The most common way is through an insurance policy.
- Risk Acceptance: Accepting the risk when the cost of mitigation outweighs potential impact [16].

Cybersecurity Policies and Procedures

The ISO/ IEC 27002 is an information security standard which specifies policies and procedures such as:

- Access Control Policies: Involves Role-Based Access Controls (RBAC) which allows access to systems and resources based on user roles in an organization. Multi-Factor Authentication (MFA) adds extra verification steps for users to access sensitive resources.
- Data Protection Policies: Sensitive data such as credentials needs to be encrypted and ensure backups are available.

- Incident Respond Policies: An IRP needs to be put in place for organizations to address and respond to breaches quick and effectively and prevent the breach from escalating further [17].

Risk Mitigation Strategies for Future Defense

Since the breach has already occurred, Oracle should take precautionary measures to prevent similar breaches in the future. Some of the strategies that the company can adopt are:

- Regular system updates and patch management- Oracle overlooked their outdated servers which in turn led to the exploitation of sensitive customer data.
- Continuous logging and monitoring- Using tools such as SIEM (Security Information and Event Management) can help detect anomalies on a network in real time.
- Penetration testing and Vulnerability scans- This could have helped Oracle identify any existing vulnerabilities or bugs in the system that could pose a risk to its assets [3].
- Zero Trust Architecture- while this breach did not directly involve any insider attack, it is still safe to design and implement a zero-trust security model to prevent any future breaches.

Conclusion and Bibliography

Conclusion

In conclusion, the 2025 Oracle cloud data breach is a reminder that vulnerabilities need to be identified and patched immediately. Overlooking or neglecting it could lead to exploits and may cause unrecoverable impacts on the systems and the overall reputation. The affected customer has confirmed about their usernames and emails being compromised. However, Oracle has denied the breach. The hacker has access to over 6 million records of encrypted sensitive credentials that would be sold on the dark web if actions are not take immediately. The response from Oracle is being heavily criticized as they are not taking accountability and are also denying the breach claims in public which leads to the GDPR's 72-hour breach rule. Instead, they have discretely contacted some of their customers to notify them about the breach in their outdated servers. As of April 17th, 2025, The FBI and CloudStrike are actively investigating on this incident and have urged the affected customers to take protective measures as outlined in this report.

Bibliography

[1] "Cybersecurity Principles – Week 1: Course Introduction," 11 February 2025. [Online]. Available: https://elearn.usp.ac.fj/pluginfile.php/702545/mod_resource/content/5/CS352_Week_1.pdf. [Accessed 24 April 2025].

[2] "Technical Challenges - Week 8 Lecture: CS352 - Cybersecurity Principles," 11 February 2025. [Online]. Available: https://elearn.usp.ac.fj/pluginfile.php/702583/mod_resource/content/5/CS352%20Week%208%20Lecture.pdf. [Accessed 24 April 2025].

[3] "Risk Management - Week 4 Lecture: CS352 - Cybersecurity Principles," 11 February 2025. [Online]. Available: https://elearn.usp.ac.fj/pluginfile.php/702559/mod_resource/content/8/CS352%20Week%204%20Lecture.pdf. [Accessed 24 April 2025].

[4] "Compliance & Law – Week 7 Lecture: CS352 – Cybersecurity Principles," 11 February 2025. [Online]. Available:

https://elearn.usp.ac.fj/pluginfile.php/702576/mod_resource/content/2/CS352%20Week%207%20Lecture.pdf. [Accessed 24 April 2025].

[5] "Cybersecurity Principles: Week 3 - Identity Management," 11 February 2025. [Online]. Available: https://elearn.usp.ac.fj/pluginfile.php/702551/mod_resource/content/2/CS352_Lecture_Week_3.pdf. [Accessed 24 April 2025].

[6] "Cybersecurity Principles: Week 2 - Privacy & Confidentiality," 11 February 2025. [Online]. Available: https://elearn.usp.ac.fj/pluginfile.php/702546/mod_resource/content/1/CS352_Lecture_Week_2.pdf. [Accessed 24 April 2025].

[7] Oracle, "Oracle Cloud," 2025. [Online]. Available: https://www.oracle.com/cloud/. [Accessed 24 April 2025].

[8] CloudSEK, "The Biggest Supply Chain Hack of 2025: 6M Records for Sale Exfiltrated from Oracle Cloud Affecting Over 140K Tenants," 21 March 2025. [Online]. Available: https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants. [Accessed 24 April 2025].

[9] Y. Broder, "Oracle Cloud Breach Exploiting CVE-2021-35587: How to Protect Your Organization," 22 March 2025. [Online]. Available: https://orca.security/resources/blog/oracle-cloud-breach-exploiting-cve-2021-35587/. [Accessed 24 April 2025].

[10] SOCRadar, "Everything You Need to Know About Oracle Cloud Security Incident by rose87168," 25 March 2025. [Online]. Available: https://socradar.io/oracle-cloud-security-incident-by-rose87168/. [Accessed 24 April 2025].

[11] Secutec, "Oracle Cloud Breach 21-03-2025," 25 March 2025. [Online]. Available: https://secutec.com/sites/default/files/2025-03/Oracle%20Cloud%20Breach%2021-03-2025%20-%20Report%20Secutec_0.pdf. [Accessed 24 April 2025].

[12] N. Profit, "Oracle Cloud Data Breach: CloudSEK Confirms Attack, Compromise Of 6 Million Records In New Report," 21 March 2025. [Online]. Available: https://www.ndtvprofit.com/technology/oracle-cloud-data-breach-cloudsek-confirms-attack-compromise-of-6-million-records-in-new-report. [Accessed 24 April 2025].

[13] J. Greig, "CISA warns of potential data breaches caused by legacy Oracle Cloud leak," 16 April 2025. [Online]. Available: https://therecord.media/cisa-warns-of-potential-data-breaches-tied-to-oracle-issue. [Accessed 24 April 2025].

[14] S. C. Team, "Risk Identification: Importance & Process," 10 March 2025. [Online]. Available: https://safetyculture.com/topics/risk-identification/. [Accessed 24 April 2025].

[15] "Cybersecurity Principles: Week 5 – Cybersecurity Principles," 11 February 2025. [Online]. Available: https://elearn.usp.ac.fj/pluginfile.php/702562/mod_resource/content/2/CS352_Lecture_Week%205.pdf. [Accessed 24 April 2025].

[16] 6clicks, "What are the four cybersecurity risk treatment mitigation methods?," [Online]. Available: https://www.6clicks.com/resources/answers/what-are-the-four-4-cybersecurity-risk-treatment-mitigation-methods. [Accessed 24 April 2025].

[17] A. Harvey, "ISO 27002:2022, Security Controls. Complete Overview," 19 December 2024. [Online]. Available: https://www.isms.online/iso-27002/. [Accessed 24 April 2025].

[18] T. Carroll, "Our Investigation of the Oracle Cloud Data Leak [Flash Report]," 1 April 2025. [Online]. Available: https://cybelangel.com/oracle-data-leak-breaking-news/. [Accessed 24 Aril 2025].

[19] rose87168, "Profile of rose87168 on X," [Online]. Available: https://x.com/rose87168. [Accessed 24 April 2025].

Appendices

Appendix A: Evidence from CloudSEK blog article

This appendix contains four screenshots referenced from the CloudSEK article outlining the Oracle Cloud breach.

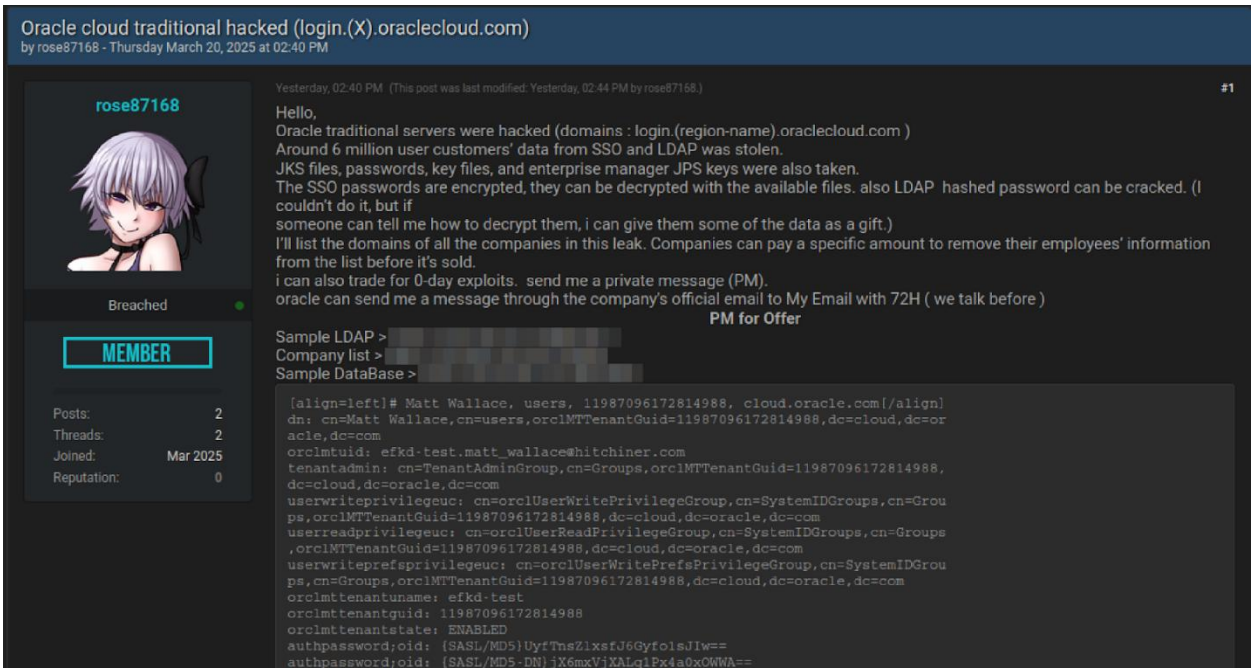

Figure 1: Forum post of the hacker claiming to have access to around 6M user customers data [8]

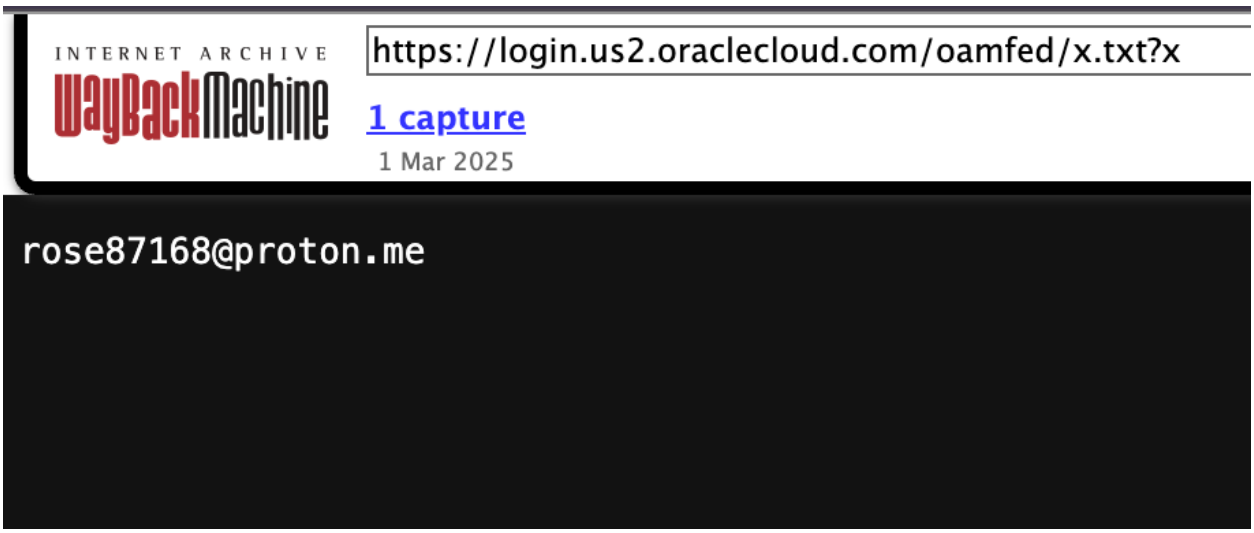

Figure 2: Compromised login endpoint showing the hacker uploaded a text file containing their email address [8]

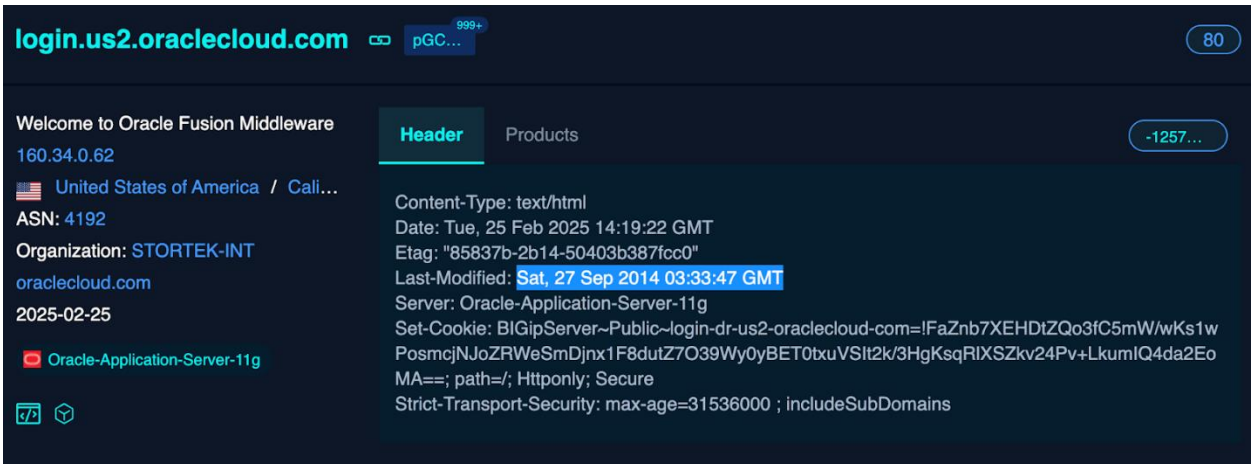

Figure 3: Showing the last update of the oracle fusion middleware server [8]

Appendix B: Blog post from CybelAngel

This appendix shows the hacker listing the domains of companies compromised and asking them to pay a specific amount to remove their employees information before it is sold.

Figure 4: Hacker uploads fresh sample of compromised data to show proof of the Oracle Cloud breach [18]

Appendix C: Hacker's twitter (X) account

This appendix shows information about the hacker's twitter (X) account which is still active.

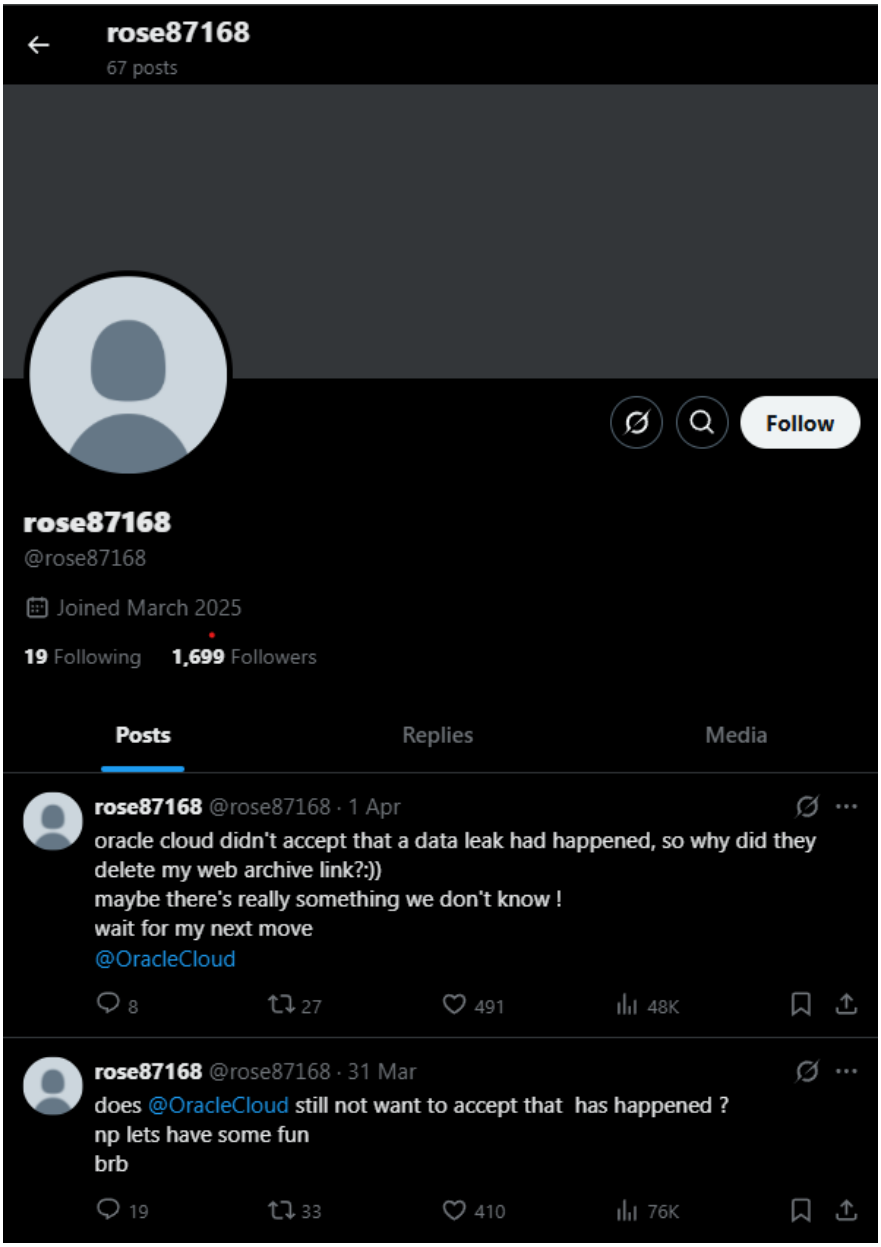

Figure 5: Hackers official Twitter(X) account [19]

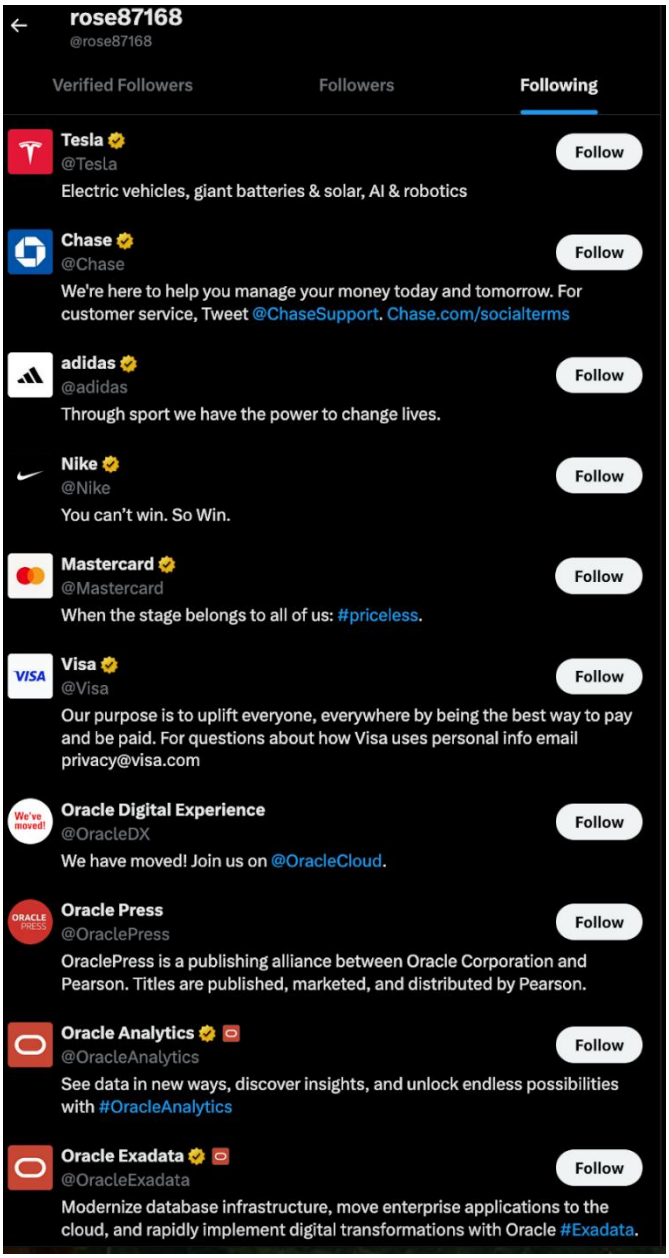

Figure 6: Hacker's following list [19]

Figure 7: Hacker demanding ransom from Oracle [19]