Monthly Intelligence Report

27th April 2025

Date prepared: 27th April 2025

Prepared by: CTI Analyst author – Samantha Coleman

Prepared for: Full Sail CISO, Professor McQuiggan

Summary

In the last month, the month of March we saw major cyber incidents which affected cloud services, mobile banking users, and critical infrastructure. The major cyber incidents that happened in the month include: The Oracle Cloud breach, a fake banking app on Telegram, and the Ukrainian Railway. These cyberattack gives us a glimpse of the growing threats to cloud environments, mobile platforms, and national systems. Attackers are not resting but advancing every minute and it is seen by the fact that their tactics combines both social engineering and technical aspects at an increasing pace. Organizations therefore, have to implement strong security measures to thwart the increasing threats. This article will examine the three cyber incidents that took place in the month of March and analyze each with different type of threat model.

Headline 1 – Oracle Cloud Breach

Assessment:

The **Oracle Cloud Breach** was a vulnerability in the Oracle Cloud infrastructure whereby there was a flaw in the Identity and access management. This vulnerability allowed certain tenants to escalate their privileges and access resources and data beyond their boundaries and scope, meaning. It was a cross-tenant risk and it allowed attackers to access another organizations' s crucial data, which is a very serious security flaw. Cloud service providers, including Oracle, have become hotspots for cybercriminals due to the volume of sensitive data they store. In this breach, the attackers were able to bypass several layers of security controls. This basically shows that we need to constantly monitor and update security measures, especially for cloud services. The attack could lead to data exposure, potential customer trust issues, and significant financial and reputational damage.

Recommendations:

It is important for organizations to enforce strong cloud security controls, including multi-factor authentication (MFA) for both users and administrative access. This will ensure that there is a strict and identity and access management controls. Cloud service providers should also review and strengthen the tenant configurations by ensuring that users have the least-privilege and should also have the minimum permissions they need. Another important feautre that organizations must apply is the encryption technique. All data stores must be encrypted to ensure that even if attackers if attackers gain access, the data remains unreadable. Security teams should continuously monitor for suspicious activities and implement the principle of least privilege (PoLP) for user access to sensitive data.

Next Steps:

- Take a measure to review tenant isolation configurations and permission boundaries in Oracle Cloud environments.
- Conduct investigations to know if any customer data was accessed improperly across tenants and assess the scope of exposure.
- Work with Oracle to get to know about the mitigation timelines and confirm whether patches or architectural changes are being implemented as it should be.

Complete MITRE ATT&CK Model for Oracle Cloud Breach

Stage	Activity
Reconnaissance	Attackers took their time and researched to identify vulnerable cloud systems and misconfigurations.
Resource Development	No malware was used exploit the vulnerability in Oracle's cloud infrastructure but a proof of concept was used instead, to show the cross-tenant access privilege.
Initial Access	The attacker used a valid account on Oracle cloud to do the breach.
Execution	API requests were issued to OCI services using crafted parameters, which triggered the unintended access behaviour.
Persistence	It was not applied as the breach was something of access management.

Stage	Activity
Privilege Escalation	Exploited a flaw in Oracle's internal tenancy checks, allowing a low-privilege user to access another tenant's resources.
Defense Evasion	No defense was needed as the access seemed to be legitimate, it was only due to a poor tenant boundary enforcement.
Credential Access	No credentials were stolen. An attacker used a legit account.
Discovery	The researcher explored accessible resources (e.g. Object Storage) to confirm that tenant boundaries had been bypassed
Lateral Movement	The movement was logical since it involved moving from one tenant's resource to another.
Collection	The attackers collected sensitive data belonging to the other organization or tenant.
Command and Control	Not applicable since it was not a malware.
Exfiltration	Sensitive data was exfiltrated from Oracle Cloud to the attacker's remote infrastructure.
Impact	Data exposure, loss of customer trust, potential legal action, and significant reputational damage.

Headline 2 – Fake Banking App on Telegram

Assessment:

The use of **fake banking apps on Telegram** demonstrates the persistent and evolving nature of social engineering and phishing attacks. The attackers took the advantage of Telegram being popular to distribute a malicious app that resembled a legitimate banking application. This tricked many to providing sensitive information such as bank account details and login information. This is a very serious attack as it compromises the users' finances. This form of attacks also destroys the reputation of legitimate banking services, leading to a loss of consumer trust. Organizations must be aware that phishing campaigns are becoming more sophisticated and are being distributed through popular platforms that users trust.

Recommendations:

Organizations should educate users about the risk of downloading apps from unofficial sources, and encourage the use of official app stores only. It is also very important to implement multi-factor authentication (MFA) for online banking services to reduce the chances of credential theft. Financial institutions must put into considerations the effort of constantly monitoring for fraudulent applications that are attempting to impersonate their legitimate apps and take swift action to remove them. Another way is to implementing URL filtering and blocking known malicious domains could also prevent users from being exposed to malicious apps and websites.

Next Steps:

- Identify and track Telegram channels that are known to distribute fake banking apps.
- Analyze the infrastructure behind these malicious apps to determine how they bypass app store vetting and gain user trust.
- Continue to monitor user reports of suspicious apps and unauthorized account activity in order to identify new trends in phishing attacks.

Complete Cyber Kill Chain Model for Fake Banking App on Telegram:

Stage	Activity
Reconnaissance	Attackers identified a popular banking app and gathered information about the target’s user base.
Weaponization	A fake banking app was created to impersonate the legitimate app, with the goal of stealing user credentials and financial data.
Delivery	The malicious app was distributed through Telegram, taking advantage of the platform's wide user base and trust.
Exploitation	Users installed the fake app, unknowingly providing their personal and banking details.
Installation	The fake banking app was installed on the victim’s device, and attackers could begin harvesting sensitive data.
Command and Control	The app communicated with remote command and control servers, thus transmitting users information.

Stage	Activity
Exfiltration	Stolen credentials, banking information, and other personal data were exfiltrated from the victim's device to the attackers.
Impact	Users' banking credentials and financial information were stolen, leading to financial loss and reputational damage to the bank.

Headline 3 – Ukrainian Railway Cyberattack

Assessment:

The Ukrainian Railway Cyberattack demonstrates the imperative vulnerabilities in infrastructure networks, namely those responsible for national logistics and transportation.The cyberattack was on Ukraine's rail system, with an impact on operations and suspension of train service. The attack is a model of the growing trend of nation-state actors embracing cyberattacks as a hybrid war strategy, melding cyber and physical disruption to cause enormous damage. The rail attack is a stark reminder of how critical infrastructure may be targeted by adversaries and cause cataclysmic operational, economic, and public safety impacts. Organizations within the same industries need to acknowledge the danger to critical infrastructure, especially in periods of political unrest or conflict.

Recommendations:

Governments and private-sector organizations managing critical infrastructure must implement robust cybersecurity frameworks to protect their networks. Continuous monitoring of network traffic for signs of intrusion and employing network segmentation can help contain attacks before they escalate. Regular security assessments, penetration testing, and collaboration with cybersecurity experts should be prioritized to identify vulnerabilities in SCADA and control systems. Additionally, organizations should establish incident response protocols specific to critical infrast

rcture attacks to ensure rapid recovery and minimize downtime.

Next Steps:

- Conduct a detailed post-mortem analysis to understand the attack's vectors and tactics employed by the attackers.
- Do thorough investigations about the origins of the threat actor and explore whether this attack was part of a larger geopolitical strategy.

- Implement modern cybersecurity measures which ensure that they can defend a system from being attacked and are also resilient against future attacks.

Complete Diamond Model for Ukrainian Railway Cyberattack:

The **Diamond Model** for this attack focuses on identifying the key components of the cyberattack, including the adversary, infrastructure, capability, and victim.

Field	Details
Adversary	Nation-state actors and the suspect is Russian due to ongoing geopolitical wars.
Infrastructure	Exploited vulnerabilities in the Ukrainian railway's IT infrastructure. It possibly targeted SCADA systems, operational networks, and other logistics platforms.
Capability	The attackers used malware that disrupted the operations of the Ukrainian rail system.
Victim	Ukrainian state-owned railway company, and the entire country at large.

Summary:

The **Ukrainian Railway Cyberattack** clearly shows as a major example of how other nations use cyberattacks to hinder their rival countries and even their enemy. The Diamond Model emphasizes the complexity of such attacks, where the adversary’s capabilities exploit critical infrastructure vulnerabilities with potentially catastrophic consequences. This highlights the urgent need for improved security measures, particularly in sectors that are integral to national security and public services.

Report sources

1. Caution: Fake Telegram Channels Impersonating the bank, KapitalBank, https://kapitalbank.uz/en/press_center/news/caution-fake-telegram-channels-impersonating-the-bank/?mobile=Y
2. Ukraine state railway says online services partially restored after cyber attack, Reuters, https://www.reuters.com/technology/cybersecurity/ukraine-state-railway-says-online-services-partially-restored-after-cyber-attack-2025-03-27/
3. Oracle says its cloud was in fact compromised, The Register, https://www.theregister.com/2025/04/08/oracle_cloud_compromised/
4. Aebi, S., Hauri, A., & Kamberaj, J. (2024). Critical infrastructure resilience in Ukraine: Energy, transportation, and communication. *CSS Risk and Resilience Reports*.