The article by Microsoft Threat Intelligence on “Mercury and DEV-1084: Destructive attack on hybrid environment” explains about the new naming system which they introduced during April 2023 update. Now The Mercury is called has Mango sandstorm and Dev-1084 as Storm-1084 respectively. The change in the naming is done in the view to enable customers to have more understanding of the threats quickly and clearly. With the help of new naming the security professionals will be able to understand the type of TA’s they will be dealing with just by the name of it.

The attacks are sophisticated and destructive cyberattack which are made to target hybrid environments, involving both on-premises and cloud resources. This operation is carried out by MERCURY, which is a group linked to the Iranian government. Whereas DEV-1084 is a collaborating actor to it. MERCURY, at first attacked the unpatched applications to get access and then given the control to DEV-1084 to perform further actions. DEV-1084's activities include extensive reconnaissance, creating access to the network and ultimately carrying out the attacks such as server farms, virtual machines, storage accounts, and virtual networks. They have used various techniques like installing shell, creating fake user accounts with admin access, installing legitimate remote access and using scripts for backdoors. They are taking breaks for weeks or months between every big steps in their attack to be unnoticed by the system admin.

At first it looked like an attack for ransomware, but after some time we get to know the reason for the attack is damaging the system.

In today's digital landscape, cloud computing has become an essential tool for businesses of all sizes. However, migrating sensitive data and applications to the cloud also introduces new security challenges. To ensure the safety of their assets, organizations must prioritize robust cloud security practices.

Cloud Security:

Security and IT information technology are referred has the measures taken to protect information and systems from Illegal access, use, disruption, modification. There are three types of security. They are

* Confidentiality: Information is only available to authorized individuals.
* Integrity: Protects data from modification or alteration.
* Availability: Guarantees that authorized users have access.

Define:

Cloud security is defined has set of technologies, controls, policies and services, which are designed to protect cloud-based data, applications, and infrastructure against cyber threats. It involves a shared model where both the cloud provider and the organization using the cloud share responsibility for security.

Best Practices and Technologies for Cloud Security:

There are several different practices and technologies that can help organizations enhance cloud security. Some of them are as follow:

Policy and Governance:

* Develop comprehensive cloud security policies: These policies should clearly defined for roles, responsibilities, access control methods and IR protocols.
* Implement strong identity and access management (IAM): we can use multi-factor authentication.
* Monitor and audit activity: Monitor for suspicious activity in the cloud.

Data Security:

* Encrypt data at all time.
* Implement data loss prevention.
* Have back up taken at regular intervals.

Infrastructure Security:

* Secure virtual networks
* Up-to-date software to patch vulnerabilities.
* Implement IDS
* Implement IPS.

Cloud Security Technologies:

* Cloud security posture management platforms.
* Cloud access security brokers
* Data encryption tools

Common Cloud Security Pitfalls:

* Lack of knowledge on cloud activity: Organizations may not have sufficient knowledge on their cloud activity.
* Misconfiguration of cloud resources.
* No proper/predefined data protection.
* Weak access controls.
* No incident response planning