CyberSec Weekly

# Happy Monday!

Welcome to the 37th Issue of CyberSec Weekly.
In this issue:



## Two Critical Flaws Found in Alibaba Cloud's PostgreSQL Databases

A chain of two critical flaws has been disclosed in Alibaba Cloud's ApsaraDB RDS for PostgreSQL and AnalyticDB for PostgreSQL that could be exploited to breach tenant isolation protections and access sensitive data belonging to other customers.

To read the full story...

**Click Here**

## What happened to the wireless bluetooth speaker when it drank coffee?

It became wired.


## Google Patches Second Chrome Zero-Day Vulnerability of 2023

CVE-2023-2136 is a high-severity integer overflow issue in Skia, reported by Google Threat Analysis Group researcher Clement Lecigne. The latest Chrome 112 update includes eight security fixes, five of which address vulnerabilities reported by external researchers. Google gave out $20,000 in bug bounty rewards to the reporting researchers

To read the full story…

**Click Here**

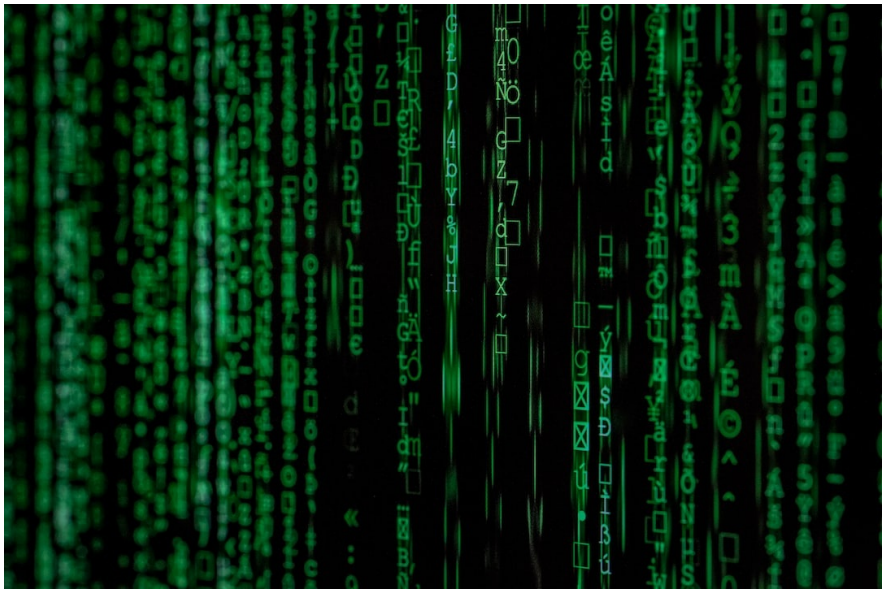
# Microsoft SQL servers hacked to deploy Trigona ransomware

Attackers are hacking into poorly secured and Interned-exposed Microsoft SQL (MS-SQL) servers to deploy Trigona ransomware payloads and encrypt all files.
The MS-SQL servers are being breached via brute-force or dictionary attacks that take advantage of easy-to-guess account credentials.

After connecting to a server, the threat actors deploy malware dubbed CLR Shell by security researchers from South Korean cybersecurity firm AhnLab who spotted the attacks.

To read the full story…

**Click Here**



# Introducing DevOpt: A Multifunctional Backdoor Arsenal

In recent years, malware attacks have become increasingly sophisticated, and attackers are always finding new ways to exploit vulnerabilities and steal sensitive data. To stay ahead of these threats, security researchers must constantly monitor the landscape and identify new threats as they emerge.

In this article, we'll take a closer look at the findings of a recent study conducted by Zscaler's ThreatLabz team, which uncovered a new backdoor built using Free Pascal that has the ability to steal data from infected systems. We'll explore the techniques used by this malware, as well as the tactics employed by cybercriminals to entice users into downloading malicious payloads.

By understanding these threats, we can take steps to protect ourselves and our systems from the dangers of malware attacks.

To read the full story…

**Click Here**