CLIENT - A LARGE EUROPEAN MULTINATIONAL ORGANIZATION

A Multinational Enterprise Restores Microsoft SQL Database Affected By NotPetya Ransomware

The client is a large European enterprise with business operations spread in more than 100 countries. The organization was using a SQL Server-based Management Information System for managing activities like employee time tracking, leaves, and business trips, etc.

Due to database corruption, its regional employees could no longer clock in their work hours, request for time off, and other work hours-related activities. Around a hundred such users complained of not being able to log into the time tracking system.

A primary investigation revealed that the application was not able to connect to the backend SQL database, since the database was offline due to corruption. This system relied heavily on the backend data to populate the requested information by users and store new entries by users.

Third-party database recovery applications and SQL native recovery command DBCC CHECKDB with repair were used to repair the database, but the results were not up to the expectations due to the extent of corruption.

Root Cause Analysis

The SQL database team investigating the issue found the root cause of the corrupted database. There was a spread of the NotPetya virus in the network, which had corrupted the database and its backups. This is another type of Petya ransomware; however, the NotPetya is more dangerous as it can spread on its own.

The ransomware does not require a user to click on the spam email, launch it, and give it administrative permissions before it can do any damage. This virus uses different methods to spread with little to no human intervention. It encrypts everything in its path including the Master Boot Record (MBR) which causes disk-related issues.

A further look into the SQL error logs and Windows Event Log indicated that there were hardware issues on the disk subsystem or disk controller.

Technical Challenge

The disk vendor was contacted and they immediately started working on resolving the hardware issue. It was found out that the physical disk drives were not communicating with the computer, which indicated possible bad disk array controllers.

The disk array controller is a device that manages and presents physical disk drives to a computer as logical units for partitioning and other disk management capabilities.

The vendor then had to replace some faulty disk array controllers in the system and re-create the partitions.

The servers were also patched with the Microsoft Windows patch (MS17-010) which blocks the loophole exploited by ExternalBlue that NotPetya relies on. After the patch was completed, the team decided to run some windows disk commands (Fsutil repair | diskpart) to query the disk subsystem and ensure there is no existing corruption in the subsystem.

The database administrators attempted to repair the corrupted database by using known third-party tools as well as the SQL native DBCC CHECKDB with REPAIR utility. The corruption of the database had spread out to the header pages and multiple attempts to repair the database were unsuccessful. The administrators tried a few software, but unfortunately they were not able to recover the .MDF and .NDF files because Meta data such as header page information, transaction log numbers, and constraint information were lost due to severe database corruption.

Business Need

The need was to manually recreate the database and try to migrate as much data from the corrupt database to rebuild a new one. This would have to be done by putting the corrupt database in emergency mode and trying to extract as much data as possible into a new database. The database was huge and there was no way to estimate how much time it would take to achieve this migration and the amount of data that could be extracted from the corrupt database. The task was possibly going to consume hundreds of hours of IT resources, without any guarantee of successful resolution.

Solution

The organization reached out to Stellar Data Recovery to fix the SQL database corruption issue. Stellar Repair for SQL – a database software that specializes in repairing large database files without losing data – was used. It features an intuitive interface to help the database administrators quickly configure the right settings and run the software.

The tool was able to successfully repair the corrupted database and decrypt the data that was encrypted by NotPetya virus. The recovered SQL database was reinstated online, allowing the time tracking management tool to connect to the database. The employees could get into the system and perform their task as needed.