Ransomware on SQL Server

What does ransomware do to a SQL Server?

Ransomware

The way that ransomware generally does their thing it encrypts files and then leaves some clues around telling you that you need to pay the ransom, which often times is to be paid by bitcoin. The amounts vary, but the times I have seen this the ransom has been between $50,000 and $350,000 to get your files back.

If SQL Server has the files locked or in use, how can the ransomware encrypt those files? Typically the ransomware is devious enough to detect things like SQL Server and to stop the SQL Service (or reboot) in order to get access to encrypt the database and log files. In the situations that I have seen the ransomware has been able to find the backups on a local or network share and encrypt those also.

Worse than ransomware is having to pay the ransom because you do not have good backups. When I say good backups, I mean a couple of things there:

- The backups have been tested regularly, known good, and you know how to restore them.
- The backups are up to date and close enough to the time of the ransomware attack that you don't lose too much data.
- The backups are not on the same computer as the ransomware. Backups to the same computer will likely be ransomware locked as well.
- The backups are moved to somewhere that the ransomware can't destroy them. Not just a network share that the database has access to, but move someone like Azure storage or Amazon storage where it is more difficult to destroy them.
- The backups include your system databases (master and msdb) that contain things like the users, jobs and maintenance plans.

If you have good backups that are up to date enough, for instance with transaction log backups or differential backups that are transferred off site and you can get you back to a point in time then you probably don't have to pay the ransom to recover your SQL Server. Instead you may just need to rebuild your SQL Server from the OS up, and restore all your backups.

Even worse than paying the ransom is paying the ransom and not entirely getting your files back. Would you trust that whoever created the ransomware and infected your computer actually had a solid QA team to test the software and confirm that when you paid that it actually decrypted things correctly. I have been part of repair projects where it appeared that after paying the ransom that the process to give you your files back happened to fail on really large files. What part of your network systems have the largest files, it is typically your database. Even paying the ransom decrypted the small files, but the decryption process failed on the big database files, the things that are really important to your company.

Preventative measures to reduce the impact of ransomware

Backups - More that a daily backup, preferably frequent transaction log backups, and perhaps a differential backup.

Offsite Backups - Move your backups off site at least once a day if not more frequently. Your backups won't do you any good if your ransomware has access to them.

Frequent System Checks - Knowing every time the SQL Server restarts or every time the SQL Server Service is restarted can give you clues when things go wrong.

Good Security Measures - Secure your SQL Server as though it is on the public internet, even if it is inside your firewall.

Have you experienced ransomware on your SQL Server? If so, please leave a comment and share the experience. Feel free to use a fake name or stay anonymous you wish.