WHAT'S A BETTER DEFENSE AGAINST

RANSOMWARE

CLOUD BACKUP OR DRaaS

By Dean Nicolls

Infrascale™

RANSOMWARE IS REACHING PANDEMIC PROPORTIONS

According to a recent study[a], more than 40% of businesses have experienced a ransomware attack in the last year. Of these victims, more than a third lost revenue and 20% had to stop business completely.

Unfortunately, the news continues to go from bad to worse. Ransomware developers are now going after the crown jewels of many organizations - their production databases. For the uninitiated, let's explain why this is such a big deal. In today's digitalized world, massive amounts of data are being gathered every day and stored in production databases, such as Oracle, Microsoft SQL Server, and MySQL. They are so ubiquitous, that they really form the bedrock for most web applications--sending and fetching data about customers, purchases, traffic, and website movements to and from the database. These databases are so critical that it's common for businesses to hire professional, certified database administrators just to manage these systems and keep them operational.

So, when these production databases get infected by ransomware, it can threaten an organization on a number of levels. The business costs fall into a few categories and they typically far outweigh the cost of the actual ransom, including:

- Productivity loss
- Lost revenue (via e-commerce transactions)
- Operational costs and lost data (lost time clock entries, supply chain updates, and customer notifications).
- Potentially lost customers and lost credibility (i.e., brand damage)
- IT opportunity costs (impact of having your IT staff drop everything to address the infection)

The bad guys know this-- and they know that they can demand a much higher ransom if they can infect these vital production databases.

So, let's walk through the steps that a System Administrator would have to take to recover a database if it gets infected by ransomware. In this side by side comparison, we will outline the steps taken and the approximate time required to recover your production database from a recent backup. We will contrast that experience with the recovery process if a DRaaS (Disaster Recovery as a Service) solution was in place.

Why are we drawing this comparison between recovering from a backup vs. recovering via a DRaaS solution?

Most ransomware guidance speaks to the importance of having a regular backup process in place, so you can recover a clean, unencrypted version of your files when you get infected. While this guidance is sound, especially for individual files and folders, it's a time-consuming option when you're trying to restore a critical business application- like a Microsoft SQL Server, MySQL, or an Oracle database. Businesses need a solution that can quickly restore databases and make them operational. This is the sweet spot of DRaaS.

RECOVER A RANSOMWARE-INFECTED DATABASE WITH A TRADITIONAL BACKUP SOLUTION

Let's assume your production database has been infected by ransomware.

Here's what you can expect. When your database is encrypted, not only will the filename be scrambled, but the extension may be replaced as well. For example, this means that a file that was previously named databasename.sql would be encrypted to something like 5NgPiSr5zo.cerber3 (assuming you were infected by Cerber ransomware).

When the file name is modified, the production services that write to the database will stop functioning. Any transaction related to your database fails. This is the “Houston, we have a problem” moment when network admins realize that something has gone terribly wrong.

At this point, you should immediately isolate the database from the rest of the network and power it down. Quickly powering it down increases your odds of recovering the hard disk by plugging into an isolated machine -- in so doing, hopefully halting the encryption process. This also assumes that you have not been hit with newer versions of ransomware (e.g., Thor or Odin) which automatically reach out and start encrypting non-protected machines and shares. Then admins can utilize speciallized third-party software (e.g., Kroll) to restore corrupted database transactions as long as you have a recent backup.

If you don't have a backup of your production database, you are truly in a bind. You will have to rebuild the database from scratch since all data is lost to encryption. In fact, you may be best served paying the ransom since there is no other way to recover your data. This is tough guidance to dispense since there's a good chance that even if you pay, you may not get a decryption key or you may find that your data was corrupted during the encryption process anyway.

If your database is part of a cluster, then you have more work ahead of you. For each machine connected to the cluster, you will have to repeat the steps below. You'll need to rebuild the database which includes replacing a new drive, installing a new OS, and re-installing the database software. You can expect that this process will take you about an hour per machine depending on how adept you are at building production databases from scratch.

Next, you'll need to reconfigure your database services to prepare for the injection of your database. Using your most recent, clean backup, you'll inject your old database into the newly rebuilt production database.

HOW TO DETERMINE THE DATE OF INFECTION

Identify the date of infection

Determining which backup to restore after a ransomware infection is imperative, but you must first ensure that your most current backup does not also contain ransomware. The way you actually do this is pretty manual.

With cloud backup solutions, you must go through these steps:

1. Inspect individual files and folders of each backup
2. Look for the date when file names started to get encrypted
3. Restore affected files from a clean backup just prior to infection

NOTE: If thousands of files have been infected, this will take a long time to isolate and pinpoint the date of infection. However, if your backup solution has Anomaly Detection you will be alerted when an abnormally large number of files are modified.

With a modern Disaster Recovery as a Service (DRaaS) solutions, the process is far simpler. Admins can more quickly browse a disk image to quickly determine if the files contained in the image have been encrypted. Determining the date of infection and restoring clean copies of infected files with traditional backup solutions is cumbersome and time consuming; with DRaaS, this entire process is far easier and faster.

Is your Backup Infected?

A critical question at this point is how do you know if your backup is also infected. Depending on the frequency of your backups, you will want to determine how much data was actually lost. The time it takes to inject your DB will vary based on its size and whether or not its clustered.

After injecting your DB, you'll need to establish connectivity between database and input services. At this point, your database should be back online and operational.

Total Downtime: 4 - 5 hours.

Best case, this entire process will take 4-5 hours, but this estimate will vary significantly based on the size of the cluster and administrator's technical proficiency. The impact of this downtime will also vary- in some cases, it may be trivial, in other cases, it could wind up being catastrophic depending on the business, size, industry, and the types of transactions feeding your production databases.

HOW TO RECOVER A RANSOMWARE-INFECTED DATABASE WITH A DRAAS SOLUTION

Now, let's examine how the process looks if you have a modern cloud-based DR solution. You will want to follow the same set of initial steps: isolate the infected machine and remove it from the network. With DRaaS, you simply log into an online dashboard, find the most recent non-infected backup image/vitural machine (VM) of the production database, and boot up the virtual machine. This can be done over a VPN, RDP, or FQDN connection. Connectivity has already been preconfigured, meaning transactions will resume and write to your database.

Since transactions are now flowing, administrators can take their time to rebuild the corrupted database, including preparing the restoration candidate, replacing the disk, and installing the OS and database software. Once the database has been rebuilt, admins can fail back recent transactions captured, while running in the cloud to the new production database, during a regularly scheduled maintenance window.

Total Downtime: A few minutes.

NOTE: This estimate does not account for the time and cost of re-entering the lost transactions between the last backup (recovery point) and the point at which the VM is booted. For example, if the last backup of your production database is a week old, then booting a VM will get operations back online, but someone will need to recreate all the database transactions for the past week. If clean VMs/images of the infected databases were readily available, organizations can completely wipe the infected hardware and restore them to the last good version. This is why organizations need to think about the importance of selecting RPOs (recovery point objectives) based on acceptable productivity loss.

Is DB part of a cluster? Repeat each of these steps for each machine connected to cluster.

CLOUD BACKUP

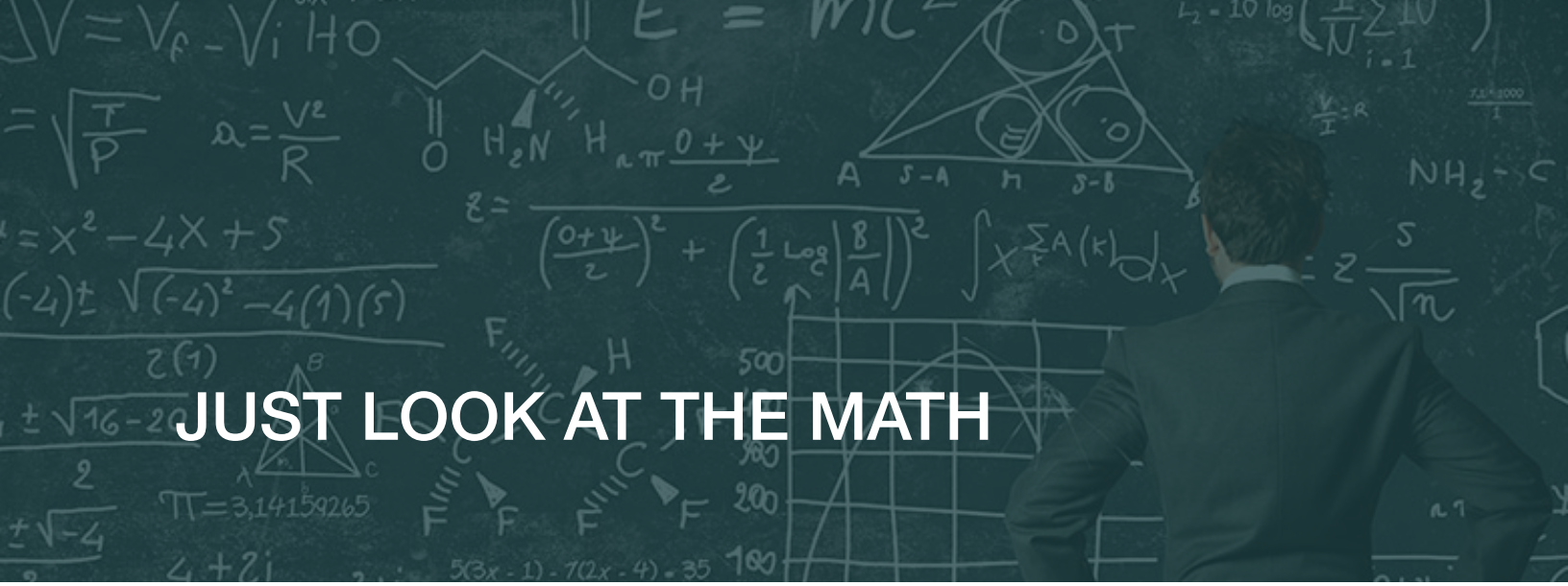
1. Ransomware Infection
2. Power down machine
3. Determine date/time of infection
4. Rebuild server (OS and software installation)
5. Reconfigure DB services
6. Restore clean DB files from backup
7. Inject old DB (from restored backup) to rebuilt DB
8. Establish connectivity (DB & input svcs)

TOTAL DOWNTIME (BEST CASE): 4-5 hours

DRaaS

1. Ransomware Infection
2. Power down machine
3. Determine date/time of infection
4. Log into DRaaS dashboard
5. Boot VM (from last clean backup)

TOTAL DOWNTIME: 1-2 minutes



JUST LOOK AT THE MATH

When dealing with today's ransomware threats, time is your worst enemy. The faster you can detect the encryption, the more time you have to take actions to restore your database.

Simple backup procedures will let you restore your production database, but it will take significantly more time than a modern DRaaS solution. In the scenario above, the difference went from 4-5 hours to few minutes. That's a quantum difference.

Clearly, the actual cost of downtime depends on the size and type of each individual organization. But, if you're an SMB, 4-5 hours can cost as much as $10,000 per hour. For larger organizations, the costs are exponentially higher--some estimate the average hourly cost of downtime to be over $100,000.

The good news is that deploying a modern cloud-based DRaaS solution helps you recover your vital systems from a myriad of downtime threats ranging from ransomware attacks to full-scale natural disasters. Plus, DRaaS solutions deliver rapid payback if you consider the productivity and amount of revenue salvaged from failover events (like ransomware infections and server outages).

DRaaS offers the added benefit of de-stressing the ransomware situation by equipping you with the ability to quickly stand up and failover to a disaster recovery environment. This buys much-needed time to rebuild the production database, re-populate it, and quickly fail back to the rebuilt database.

Unfortunately, ransomware extortionists aren't stopping at infecting your users' individual files. They're following the money all the way to your mission-critical business applications. Think about the other business apps you're running, like Microsoft Exchange, your accounting/financial system, your ERP solution. How much ransom would you be willing to pay to recover that data? Everything we outlined in this article for recovering databases is also relevant for recovering corrupted applications (and their backend databases), though the individual steps may differ.

Ransomware is becoming more sophisticated every day. Thankfully, you can stay one step ahead of the cyber extortionists by training your users, deploying enterprise-grade malware detection, and taking advantage of modern DRaaS solutions that let you failover and fail back with the simplicity of a few mouse clicks.

---

[a] **source:** MalwareBytes ransomware study surveying 540 CIOs, CIS0s and IT Directors from companies with an average of 5,400 staff across the U.S., Canada, U.K. and Germany (August 2016).

Infrascale™

www.infrascale.com

LEARN MORE

ABOUT INFRASCALE

Infrascale provides the most powerful disaster recovery and cloud backup solutions in the world. Founded in 2006, the company aims to give every organization the ability to recover from a disaster- quickly, easily and affordably. Combining intelligent software with the power of the cloud, Infrascale cracks the disaster recovery cost barrier by removing the complexity and cost of standby infrastructure to restore operations in minutes with a push of a button. Infrascale equips businesses with the confidence to handle the unexpected by providing less downtime, greater security, and always-on availability.

Gartner VISIONARY Disaster Recovery as a Service (DRaaS)

Gartner 2015 CoolVendor

CRN COOLEST CLOUDS STORAGE VENDOR 2016