druva

Checklist

YOU'VE GOT RANSOMWARE. NOW WHAT?

Q319-CON-10939

The Threat

So, the unthinkable has happened: your corporate server (or maybe just a few employees) has been infected with ransomware. At least you're not alone. According to CyberSecurity Ventures, global damage costs from ransomware are estimated to be more than $8B in 2018 and up to $11.5B in 2019. By the end of 2019, they expect there to be a ransomware attack every 14 seconds (up from every 40 seconds in 2016). And since many of these criminals continue to operate with zero consequences, it's likely such crimes will not only increase in frequency and severity, but also become a standard part of a company's daily threat landscape.

> ***"Successful ransomware attacks primarily reveal the lack of adequate endpoint protection planning and strategy for every-sized organizations throughout every vertical."***
>
> *— Gartner, Seven Myths That Could Compromise Your Ransomware Response*

How well you've prepared for a ransomware attack will have a huge impact on how quickly and effectively your company can recover. You *could* pay the ransom, of course, but there is no guarantee that the hackers will honor the "agreement" and release your data—after all, why would a criminal suddenly start playing by the rules, when they already have your money? While it's critical to ascertain where the weak points are within your organization and to shore up your defenses against future attacks, your most immediate task is to limit the damage and roll back your systems to a time prior to infection.

Before You're Attacked

Ransomware recovery options are far more limited if no preparation has been done before the attack. Each step below represents an action you can take today that will help reduce the impact of ransomware and other malware attacks on your company's systems, and enable you to create a viable recovery plan. By consistently monitoring data anomalies and by quickly restoring data from time-indexed copies, organizations will be far less vulnerable to costly and debilitating ransom demands.

1. Protect Distributed Data: "How"

An enterprise-grade automated data protection solution that performs regular backups across devices, desktops, servers, and cloud apps such as Office 365 will protect distributed data and act as an insurance policy in case of a ransomware strike or other intrusion. Make sure to select a cloud-based backup solution, as it provides off-site storage. Off-site storage is, by its very nature, safer: data is isolated from the enterprise network where day-to-day business requires constantly opening email and running executables that may host malware.

Leveraging a Software as a Service (SaaS) tool hosted on Amazon Web Services (AWS) or Microsoft Azure not only provides the necessary off-site capabilities, but also complies with local data residency laws by storing all of your data in the same region. These cloud platforms will also allow you to immediately access your files and get employees back to work, while an attack is still taking place.

2. Backup Distributed Data: "Who"

Does your current backup plan cover 100 percent of your business critical data, including data from geographically distributed teams and servers? To reduce your exposure to potential data loss, review and validate the deployment scope of your backup plan to ensure your chosen solution deploys automatically to all devices that need protection. At a minimum, you should confirm that key users are covered by your data protection policy.

3. Review the Scope of Your Data Backup: "What"

What are you backing up? You're probably protecting servers, desktops, and email, but what about other sources where business critical data is generated and stored, like Office 365 or G Suite? Make sure you are capturing user-specific data sets such as profiles, system and app settings, and/or folders, so that employees can get back to work as quickly as possible. We highly recommend that you review, validate, and modify backup content as needed to ensure that all important data can be restored. If you need a more comprehensive plan, consider creating custom folders where users can store data for backup to further reduce data loss.

4. Check Backup Frequency Across Distributed Teams: "When"

How often are you backing up? Every two days? Eight hours? Four hours? Do you need an even more aggressive schedule for executives? What about remote office servers? Review, validate, and modify backup frequency if needed to ensure that automated replication of mission-critical data is periodically completed for all critical content. As a general rule, we recommend that you backup data, at a minimum, once every four hours, and every two hours for key users. You may also want to select a different backup frequency depending on the requirements of specific servers, users, and teams.

5. Validate Your Retention Policy: "How Long?"

How long are you keeping your backups? 14 days? Six months? Review, validate, and adopt a longer retention policy if needed to meet internal objectives and ensure a sufficient Recovery Point Objective (RPO), especially for key people, servers, and departments. Your data retention policy will vary depending on your industry, regulations, and internal IT policies—IT, legal, and compliance teams may need to weigh in on data retention needs.

6. Test Your Backups and Reassess Policies Periodically: "Looking Ahead"

It's not enough to have a backup solution without having a "restore" solution. Regular restore tests from backup data will ensure you have an effective tool when ransomware strikes. We also highly recommend that you revisit your backup policies approximately every six months to ensure they continue to meet your organization's needs. IT often has the primary responsibility for these routines and, in some cases, acts in coordination with the legal team.

7. Monitor for Ransomware Attacks: "Be Aware"

Keeping track of unusual file deletions, modifications, encryptions, and header changes can minimize damage by enabling fast responses such as isolating infected hardware before malware has the chance to spread. The earlier you isolate a problem, the more-recent a backup you'll be able to restore, minimizing downtime and lost productivity.

After You're Attacked

So the inevitable has happened, and one (or several) of your company machines has become infected. What do you do now? The following checklist walks you through what should be done once ransomware hits.

1. Don't Pay the Ransom

While it may be tempting to consider a payment of the ransom as the quickest way to get your data back, there is no guarantee the attackers will actually unlock your files once payment is received. Unfortunately, a recent 2018 survey, conducted by an Australian telecommunications company, Telstra, found that nearly half of business ransomware victims ultimately pay up, despite the fact that nearly half of the victims don't get their files back anyway.

2. Turn All the Devices Off and Disconnect Them From the Network

Once you've identified the devices that are infected, immediately unplug the network cable, turn off the Wi-Fi, and shut those devices down. Many types of ransomware can spread via a network connection, so the sooner you disconnect the infected devices, the better your chances of containing the breach. It's also important to take all of your shared drives offline temporarily until you have determined that all the infected systems have been identified. Continue to monitor systems to identify if new files are getting encrypted or disappearing.

3. Find The Source

Now that you have taken steps to contain the immediate (known) damage, reach out to all of your users to find out who experienced the first signs of the attack and when. Was it after they clicked on a link in an email? Were there any unusual prompts coming from their web browsers?

Getting these details from your users to find out how the malware got on their computers will not only help you contain the breach, but it will also better prepare you for any future attacks.

Ransomware attacks in many cases can be identified by the following:

- Users reporting that files are missing or cannot be opened
- IT administrators observing files that are missing or encrypted on servers or shared drives
- Alerts from a monitoring dashboard, showing that anomalies in device activity have been detected for files being deleted or encrypted
- Users reporting that their desktop picture has changed and/or that a ransom note has appeared on their display screen

4. Alert All of Your Users

It's always a good idea to send an email announcement and post warnings on any company message board, but that is not enough. You'll need to physically walk around and check with everyone in person to ensure that they're all aware of what is happening and what they need to look out for.

5. Restore From a Backup to a Clean Device

After the damage has been contained and you've alerted all users to the current threat to prevent further infection, the best way to get your data back without paying the ransom is to restore it from your backup. With an enterprise-grade automated backup solution and the knowledge of when and where the attack took place, you can immediately go back to an uninfected, time-indexed snapshot of

each system's data. Modern ransomware packages leverage strong file encryption methods like AES-128 or RSA-2048, which make it impossible to retrieve your data without a backup copy available.

It's critical that the files are restored to a new device, or to the same device after it's been completely wiped clean.

6. Reimage the Infected Devices

Once a device has been infected, there is no way to guarantee that the ransomware is completely gone unless you wipe that device clean and start with a new image. Reimaging every computer that has been infected gives your organization the confidence that ransomware has been remediated and won't resurface later. For instance, many forms of ransomware can have a secondary payload that remains on a device after the attack.

Summary

Companies today can no longer pretend that having a solid firewall in place will protect them from ransomware. The increasing sophistication of phishing techniques, taking advantage of the inevitability of human error, means that a successful attack is not a case of if, but when. Therefore, the key to successfully recovering from a ransomware attack is to have a comprehensive plan in place for backing up your mission-critical data, long before hackers can even get close to your servers and your employees' laptops. By completing each step in the checklists above, you will significantly reduce your organization's exposure to risk. Above all else, remember this: *If you don't have a Plan B, you don't have a plan.*

About Druva

Druva is the global leader in Cloud Data Protection and Management, delivering the industry's first data management-as-a-service solution that aggregates data from endpoints, servers and cloud applications and leverages the public cloud to offer a single pane of glass to enable data protection, governance and intelligence—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations, and protects over 100 petabytes of data. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44 (0) 203-7509440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729
sales@druva.com
www.druva.com