6 Key Steps: What to do After a Ransomware Attack

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 they're paid off. In fact, according to the CyberEdge Group[1], only 19 percent of companies who pay ransoms actually restore all their data and working environments, such as management consoles.

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, scour your IT environment for clues to the source. Any system with out-of-date or misconfigured software is easily compromised, and it's vital to remember that even SaaS productivity apps like Microsoft 365 are vulnerable. 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 or were there unusual prompts coming from their web browsers?

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. Reimage infected endpoints, servers, and virtual machines

Once an environment has been infected, there is no way to guarantee that the ransomware is completely gone unless you wipe devices, as well as virtual machines clean, and start with a new image. Reimaging the original servers and applications ensures that ransomware has been remediated. In the meantime your organization can still keep business productivity on the move without any disruptions if you have a cloud disaster recovery plan in place, allowing your organization to recover critical applications and data in VMs in a virtual private cloud.

6. 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

[1] Forbes, "Why You Should Never Pay A Ransomware Ransom," 2018, Mathews, Lee.

from a backup stored with a reliable cloud service such as AWS. 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.

Check out druva.com/solutions/ransomware/ and find out more recommendations on ransomware protection.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva enables cyber, data and operational resilience for every organization with the Data Resiliency Cloud, the industry's first and only at-scale SaaS solution. Customers can radically simplify data protection, streamline data governance, and gain data visibility and insights as they accelerate cloud adoption. Druva pioneered a SaaS-based approach to eliminate complex infrastructure and related management costs, and deliver data resilience via a single platform spanning multiple geographies and clouds. Druva is trusted by thousands of enterprises, including 60 of the Fortune 500 to make data more resilient and accelerate their journey to cloud. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.