What is Ransom Denial of Service? How to prevent RDoS

Ransom Denial of Service is when a hacker asks you to pay them some money, threatening to launch a Distributed Denial of Service (DDoS) attack if you don't pay in advance a certain date and time.

You may have heard about DoS and DDoS. The idea behind such an attack is to destroy any organization's servers, thus not allowing them to provide services to the users of that organization. Usually, the organization's main server is attacked by so many requests for access that it hangs, denying any service to anyone.

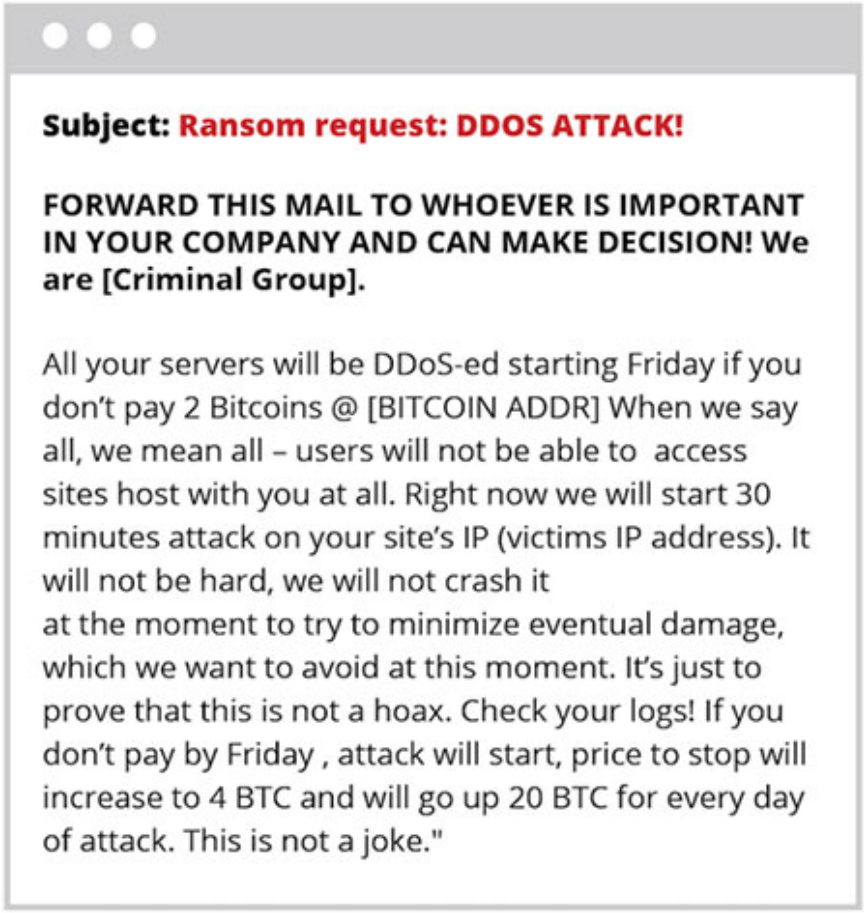
Ransom Denial of Service (RDoS) is similar, except that hackers act as blackmailers. Let's see what Ransom Denial of Service (RDoS) is and how to prevent it by taking the appropriate precautions.

What is Ransom Denial of Service (RDoS)?

Ransom Denial of Service is when a hacker asks you to pay them some money, threatening to launch a Distributed Denial of Service (DDoS) attack if you don't pay in advance a certain date and time.

To show the seriousness of an RDoS attack, a hacker can also launch a DDoS attack for a small amount of time against the organization they are asking for ransom. You may also have heard of Ransomware: Hackers demand money after encrypting all data on any organization's servers.

In the case of Ransomware, the hacker first encrypts the data of an organization and then sends a ransom request saying they will decrypt the data once the money is taken. With RDoS, the note is sent before any action, clearly stating that the hacker has access to the company's server and requests a certain amount in cryptocurrency before a specified date. If the money is not transferred to hackers, they can encrypt the organization's data.



RDoS strikes fear of data loss and makes people pay money to avoid a DDoS attack.

Should I pay the ransom?

Experts say you should not pay the ransom. They claim that if an organization agrees to pay hackers for ransom, other hackers will also emerge eager to make money this way. Doing this will encourage other hackers to commit blackmail.

Experts also say there is no guarantee that there will not be a DDoS attack or a Ransomware attack even if the ransom has been paid. Furthermore, such acts will encourage other hackers to carry out similar blackmail practices.

Should you let blackmailers scare you and pay for the money they ask for? The answer is no. You'd better plan against such a scenario. The next section talks about how to prepare for a DDoS attack. If you already have a plan, you don't need to worry about DDoS, RDoS, ransomware or similar hacking issues.

RDoS attack prevention measures

If a DDoS attack occurs after a hacker demands a ransom, being prepared is the key to handling the situation easily. That's why it's important to have a DDoS attack protection plan in place. When planning DDoS attack protection, assume that it can happen multiple times. That way, you will be able to create a better plan.

Some people create a disaster recovery plan and use it to recover from a DDoS attack. But this is not the main purpose of the article. You need to minimize traffic to your company's website or its servers.

For an 'amateur' blog, a 1-hour downtime may not have a big impact. But for real-time processing services - banking, online stores, and the like - every second matters. This is something you should keep in mind when creating a DDoS attack response plan instead of a recovery plan.

Some important points to consider when an RDoS or DDoS attack takes place are:

1. How can your Internet service provider help you?

2. Can your hosting provider help you by removing the website from your host for a while (until the DDoS attack stops)?

3. Do you have third party security providers, like Susuri, Akamai or Ceroro that can detect DDoS attacks as soon as they start? These services can also block attacks by identifying various factors such as geography, etc.

4. How long will it take to change the server's IP address for the attack to stop?

5. Have you looked at a cloud-based package that can increase bandwidth when DDoS occurs? Increasing bandwidth means that hackers will have to put more effort into performing attacks. DDoS attacks will stop quickly because hackers will have to arrange more resources to bring down the company's servers.