Ransomware Negotiations

Introduction

Ransomware is malware that restricts users' access to their systems in two ways. The first is to lock the screens of these systems, and the second is to lock the users' files until a ransom is paid. Generally, ransomware occurs when specific files on corrupt systems are encrypted, and a ransom is made through an online payment system before a decryption key is sent to the affected party.

Ransomware still appears to rank among the most destructive malware threats that any organization can experience, and there's no assurance that these attackers are willing to stop. Nowadays, ransomware is more prominent, and the demands have risen from thousands to millions of dollars because attackers know that organizations would pay to retrieve any vital information. These attacks affect several organizations like hospitals and other public sectors, limiting their ability to provide essential services for citizens.

How You Can Be A Victim of Ransomware Attack

There are several ways to discover that you have been a victim of a ransomware attack. Firstly, you can unknowingly download ransomware onto your systems when you visit affected websites. Ransomware can also be sent as a payload dropped or downloaded by any other malware and onto your system. Thirdly, some different categories of ransomware are downloaded from malicious pages and sent as attachments from spammed emails.

Once ransomware is successfully downloaded onto your system, it can either encrypt targeted files or lock your computer screen. Once your computer screen has been locked, a full-screen notification displays on the computer, preventing you from using your system. The information on your screen also includes how to pay the ransom successfully. If the hacker carries out the other option, the ransomware will prevent you from accessing vital files, documents, and spreadsheets.

Ransomware is sometimes called "scareware" because it forces you to pay a fandom fee if you want to continue with your organizational activities.

The 7 Effective Tips for Ransomware Negotiations

1. **Handle the Negotiation Like a Business Deal**

It is easy to be agitated once you discover that hackers have hacked your files and systems. But the thing is, these hackers are expecting you to be worked up and, in some cases, will use your anger as a reason to make negotiations difficult for you. So, when you negotiate with them, handle it like a business deal; use professional language, be respectful and leave your emotions out of it.

2. Plead You Can't Afford the Amount They Are Demanding

Remember that although these hackers have restricted your access to your files, they are still business people because they have something to sell to you, so it's normal for them to have a starting price.

Instead of immediately agreeing to the amount you have been asked to pay, tell the hackers that you can't afford the amount they are demanding. This can prove beneficial to your organization and convince the adversaries that you don't have up to their required amount.

Secondly, rather than stalling for time, you can offer to pay them a small part of the money and pay them the more significant amount later on. Hackers are known to customize ransom demands according to an organization's profile. They also accept discounts because they have time pressures and many other victims.

3. Ask for More Time to Pay Up

If you happen to be a victim of ransomware, ask for more time to pay up. Once agreed, the extra time will allow you to explore your other options and possibilities of recovering your data or files. Your reason for the extra time doesn't have to be complicated; just tell them you need more time to raise the required amount. Do not make promises you cannot keep; because if you promise your attackers an agreed date that you can't meet up with, there's no telling what they will do. Sometimes, they will leak and publish all your data because you didn't keep to your words.

4. Request Proof of Life

If it were a hostage situation, you would be in your right to request proof of life; evidence showing that the abducted person is still alive. You can follow the same practices in a ransomware situation. Before you pay the ransom, ask your attacker to decrypt some files as proof of their ability to restore your systems and data once you make payments.

5. Adopt a Team Approach

There are many teams involved in a ransomware situation, and they include insurance carriers, external counsel, and a chief information officer. Because of how prominent ransomware attacks have grown, these teams include crisis management teams, cybersecurity professionals, legal counsel, the board of directors, and the communications department. Handling a ransomware negotiation isn't something that should be done alone. You should adopt a team approach and establish clear communication strategies between all internal and external bodies involved.

6. Hire a Cybersecurity Professional

Haggling with hackers during ransomware negotiations can be an arduous task, and sometimes, these hackers make it even more difficult by refusing to reduce the ransom. So, if you know you can't handle the heat, hire a cybersecurity professional to help you tackle the ransomware negotiations. One benefit of hiring cybersecurity professionals is that they can discuss with your attackers and educate them about your financial circumstances. They also treat all ransomware situations objectively and keep emotions aside, which is the opposite of what you might do if you were to handle the negotiations. A cybersecurity ransomware expert has specialized training to take on any of such cases, and they will assist you with the negotiations and other security incidents you need to avoid.

7. Be Credible

The problem with ransomware negotiations is that it can go both ways, and the attackers can decide to change the directions whenever they wish to. All you need to do is to be willing to listen to their new demands so they don't feel as though the negotiation is one-sided. It would help if you tried to establish mutual trust between you and your attackers, as this can help you maintain credibility and make it easier for you and the attackers to reach an agreed solution.

Conclusion

Summarily, other advice you can use during ransomware negotiations is to ask for a test file to be decrypted, proof of deletion of files if you pay the ransom, and a rundown on how the hacker infiltrated the organization's database. Although there might be no way of knowing, it is also advised that you prepare yourself for the possibility of the sales of your organization's details if the hackers do not keep to their end of the bargain. We strongly advise that you have a cybersecurity professional on your team, as it will go a long way.