TR-4802: FlexPod, The Solution to Ransomware

FlexPod

NetApp
July 01, 2021

Table of Contents

TR-4802: FlexPod, The Solution to Ransomware

Arvind Ramakrishnan, NetApp

In partnership with:

To understand ransomware, it is necessary to first understand a few key points about cryptography. Cryptographical methods enable the encryption of data with a shared secret key (symmetric key encryption) or a pair of keys (asymmetric key encryption). One of these keys is a widely available public key and the other is an undisclosed private key.

Ransomware is a type of malware that is based on cryptovirology, which is the use of cryptography to build malicious software. This malware can make use of both symmetric and asymmetric key encryption to lock a victim's data and demand a ransom to provide the key to decrypt the victim's data.

How does ransomware work?

The following steps describe how ransomware uses cryptography to encrypt the victim's data without any scope for decryption or recovery by the victim:

1. The attacker generates a key pair as in asymmetric key encryption. The public key that is generated is placed within the malware, and the malware is then released.
2. After the malware has entered the victim's computer or system, it generates a random symmetric key by using a pseudorandom number generator (PRNG) or any other viable random number- generating algorithm.
3. The malware uses this symmetric key to encrypt the victim's data. It eventually encrypts the symmetric key by using the attacker's public key that was embedded in the malware. The output of this step is an asymmetric ciphertext of the encrypted symmetric key and the symmetric ciphertext of the victim's data.
4. The malware zeroizes (erases) the victim's data and the symmetric key that was used to encrypt the data, thus leaving no scope for recovery.
5. The victim is now shown the asymmetric ciphertext of the symmetric key and a ransom value that must be paid in order to obtain the symmetric key that was used to encrypt the data.
6. The victim pays the ransom and shares the asymmetric ciphertext with the attacker. The attacker decrypts the ciphertext with his or her private key, which results in the symmetric key.
7. The attacker shares this symmetric key with the victim, which can be used to decrypt all the data and thus recover from the attack.

Challenges

Individuals and organizations face the following challenges when they are attacked by ransomware:

- The most important challenge is that it takes an immediate toll on the productivity of the organization or the individual. It takes time to return to a state of normalcy, because all the important files must be regained, and the systems must be secured.
- It could lead to a data breach that contains sensitive and confidential information that belongs to clients or

customers and leads to a crisis situation that an organization would clearly want to avoid.

- There is a very good chance of data getting into the wrong hands or being erased completely, which leads to a point of no return that could be disastrous for organizations and individuals.
- After paying the ransom, there is no guarantee that the attacker will provide the key to restore the data.
- There is no assurance that the attacker will refrain from broadcasting the sensitive data in spite of paying the ransom.
- In large enterprises, identifying the loophole that led to a ransomware attack is a tedious task, and securing all the systems involves a lot of effort.

Who is at risk?

Anyone can be attacked by ransomware, including individuals and large organizations. Organizations that do not implement well- defined security measures and practices are even more vulnerable to such attacks. The effect of the attack on a large organization can be several times larger than what an individual might endure.

Ransomware accounts for approximately 28% of all malware attacks. In other words, more than one in four malware incidents is a ransomware attack. Ransomware can spread automatically and indiscriminately through the internet, and, when there is a security lapse, it can enter into the victim's systems and continue to spread to other connected systems. Attackers tend to target people or organizations that perform a lot of file sharing, have a lot of sensitive and critical data, or maintain inadequate protection against attacks.

Attackers tend to focus on the following potential targets:

- Universities and student communities
- Government offices and agencies
- Hospitals
- Banks

This is not an exhaustive list of targets. You cannot consider yourself safe from attacks if you fall outside of one of these categories.

How does ransomware enter a system or spread?

There are several ways in which ransomware can enter a system or spread to other systems. In today's world, almost all systems are connected to one another other through the internet, LANs, WANs, and so on. The amount of data that is being generated and exchanged between these systems is only increasing.

Some of the most common ways by which ransomware can spread include methods that we use on a daily basis to share or access data:

- Email
- P2P networks
- File downloads
- Social networking
- Mobile devices
- Connecting to insecure public networks
- Accessing web URLs

Consequences of data loss

The consequences or effects of data loss can reach more widely than organizations might anticipate. The effects can vary depending on the duration of downtime or the time period during which an organization doesn't have access to its data. The longer the attack endures, the bigger the effect on the organization's revenue, brand, and reputation. An organization can also face legal issues and a steep decline in productivity.

As these issues continue to persist over time, they begin to magnify and might end up changing an organization's culture, depending on how it responds to the attack. In today's world, information spreads at a rapid rate and negative news about an organization could cause permanent damage to its reputation. An organization could face huge penalties for data loss, which could eventually lead to the closure of a business.

Financial effects

According to a recent McAfee report, the global costs incurred due to cybercrime are roughly $600 billion, which is approximately 0.8% of global GDP. When this amount is compared against the growing worldwide internet economy of $4.2 trillion, it equates to a 14% tax on growth.

Ransomware takes a significant share of this financial cost. In 2018, the costs incurred due to ransomware attacks were approximately $8 billion—an amount predicted to reach $11.5 billion in 2019.

What is the solution?

Recovering from a ransomware attack with minimal downtime is only possible by implementing a proactive disaster recovery plan. Having the ability to recover from an attack is good, but preventing an attack altogether is ideal.

Although there are several fronts that you must review and fix to prevent an attack, the core component that allows you to prevent or recover from an attack is the data center.

The data center design and the features it provides to secure the network, compute, and storage end-points play a critical role in building a secure environment for day-to-day operations. This document shows how the features of a FlexPod hybrid cloud infrastructure can help in quick data recovery in the event of an attack and can also help to prevent attacks altogether.