Preventing Malicious Backup Deletion

Background

Ransomware has become a nightmare for IT organizations. It is a multi-billion-dollar headache.

A new variant of ransomware appears every 18 seconds. Seven out of ten ransomware attacks penetrate the firewall, and pass anti-virus scanning and network deep packet inspection.

Traditionally, the last line of defense against ransomware is a clean backup, but the malicious actors behind ransomware know this. Backups threaten their revenue streams. To protect that revenue stream, ransomware has evolved and gotten smarter. Unfortunately, businesses' defenses and processes are stuck in the past and are no longer effective against ransomware.

Key Problems

The latest ransomware variant evolution is neutering backups as a defense by deleting them. Upon deletion, they detonate, encrypting the applications and the data on the machines they have infected. Different variants utilize different backup attack vectors. They generally identify the well-known default backup directory of the backup software, such as /.bak, and delete the entire directory of backups. Other variants steal the backup admin credentials, login as that admin, then delete all of the backups. And yet another ransomware variant utilizes the published APIs of the backup software to delete the backups. The vast majority of backup vendors have been targeted.

As soon as an organization realizes a ransomware attack is underway, they go to their backups to defeat it. They then discover that they have no backups and must pay the ransom. The malicious actors behind the ransomware commonly charge a ransom that the organization can afford to pay. However, authorities strongly recommend not to pay the ransom because the malicious actors frequently do not return all of the data. They will first release some of the less important data, and then only return the rest of the data after an additional ransom is paid. In addition, that attacked organization goes on a list of ransom payers, identified as a company that *will* pay, making them a known target to be hit again and again.

As previously stated, end point security, firewalls, and deep packet inspection are being circumvented. Many of these variants have a very low detection rate by anti-virus software. The front door security is not enough. Backups are the last line of defense and now they too are being attacked. They must be defended.

Most backup vendors are recommending 3-2-1 backups as a defense against this type of ransomware attack. Three copies of the backup data on two different media, with one copy air-gapped offsite. In terms of networking, an air gap is a security measure that ensures a computer or network has no network interfaces connected to other networks. This means the air-gapped copy that is offsite cannot be located and deleted by ransomware.

There are significant issues with this defense. A tape recovery takes a significant amount of time and includes several steps:

1. The tapes have to be found at the offsite vault.
2. They are transported back to the organization's data center.
3. Then they are mounted in tape drives in a tape library and read into the backup media server before the data can be recovered.
4. This is going to take hours or days, and assumes the tapes have not been corrupted, damaged, or degraded.

It is a lengthy and convoluted process that only ensures you will not be back up and running for several hours or days.

While the traditional 3-2-1 backup process is a time-honoured strategy, it only protects against very basic data loss scenarios. And it does not account for modern data storage requirements, such as:

- Reducing the amount of backup data stored;
- Moving away from tape as a backup medium because of recovery times, complexity, and offsite storage costs;
- Delivering near instant recoveries – 30 minutes or less.

ioFABRIC believes there is a more intelligent way to prevent ransomware from deleting backups and has developed that better way.

ioFABRIC's Intelligent Software Solution

ioFABRIC Software is designed specifically to prevent ransomware from deleting backups or archives.

This means none of the ransomware variants can delete the backups. ioFABRIC Software also prevents hackers or disgruntled employees from doing the same. And it prevents deletions caused by human error.

How does it work? It does this by setting a retention lock that makes the data immutable during the retention period. The retention period can be extended, but not reduced, once it is set for a specific backup data set.

The ioFABRIC Software flips the tables on ransomware. It makes sure IT organizations are able to recover nearly instantly from a ransomware attack with the latest local backups. No triple the storage consumption, no tape, no offsite storage costs, and no lengthy recoveries.

ioFABRIC delivers this intelligent software solution as either a physical or virtual appliance. The ioFABRIC Software physical appliance is provided by ioFABRIC partners. These ioFABRIC software solutions are available at extremely affordable costs.

For more information, contact us at: iofabric.com/contact or 1-833-IOFABRIC (463-2274).