FIM+ Augments Immutable Backups to Defeat Ransomware Attacks

Synopsys: Immutable backups are highly useful for recovering active data but may not be ideal to help restore the system and application software (infrastructure) that was compromised in order to attack your site. If you simply restore your database there is nothing to stop perpetrators from just re-encrypting the target using a different back door, time bomb or other malicious software implemented prior to the attack.

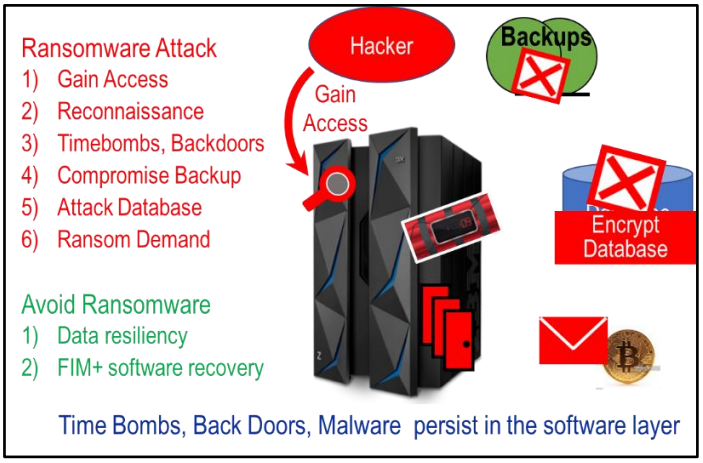
This secondary attack can be eliminated by restoring both the correct data and trusted infrastructure components in a single process. Since modern attacks are persistent and take weeks to complete, it is likely that the data and the software infrastructure will need to be restored to different points in time.

In cooperation with industry leaders, MainTegrity has implemented a backup selection feature in its advanced file integrity monitoring product, FIM+. This feature corelates malicious attack detection with backup creation data, so customers can easily select the most recent, uncompromised copy to restore. When coupled with FIM+ Recovery Assist, the combined solution makes recovering the software infrastructure and databases a straightforward process. By restoring only the components that were compromised, you can also avoid regressing desirable changes that were implemented in the attack interval.

Ransomware / Encrypting your Database: Image copies and backups are your primary recovery assets in case of malicious attack. However, the restore process can be complex, requiring the customer to use a "trial and error" process to select the correct copy to restore. Having the storage complex create frequent backups works well for highly active data, but, realistically, if you are unable to determine when the attack started, and what parts of your trusted software have been compromised, are you better off?

Let's assume some malicious actor encrypts your database. The DB2 or IMS application will fail almost immediately. If you simply restore the latest snapshot to get back on the air, you may be leaving yourself open to a secondary attack.

Hackers these days, whether they are independent, or state sponsored, are intelligent, well-funded and persistent. An efficient phishing program or buying legitimate credentials on the dark web will get them around access control and onto your mainframe. By the time they encrypt your database, the bad actors may have been on your mainframe for days or weeks.



The time will have been put to good use. Typically, hackers will obscure their entry point and implement multiple back doors and time bombs. They will also have sought out a high value target like a database and will subsequently attack the target, often using encryption. **If you recover the database from the latest snapshot the hackers can counter this action by simply re-encrypting your data using back doors and time bombs installed long before the primary attack**.

It is in the software infrastructure where the hacker's malware resides. Recovering your database is a required step, but the bad guys may still be welded in. Compromised components will need to be recovered prior to the implementation of the back doors and time bombs. Detection of these malicious changes should be a key element of your mainframe defense strategy.

Similarly, internal threats, originating from disgruntled employees or rogue activities, can be detected and neutralized using the same techniques as an external perpetrator.

The solution: FIM+ is the premier file integrity monitoring solution available for z/OS mainframes. It requires no new hardware or software. The primary mission is to detect unexpected and undesired changes to mainframe software infrastructure. It also links together many other tools to provide a cohesive barrier of shared information, then makes that knowledge available in a z/OS native browser interface that is intuitive to both experienced and newer support staff.

FIM+ does away with the need for multiple iterations to select the right copy. As noted above, FIM+ uses all the relevant security information available. This is made possible by the regular FIM+ scanning process, which detects all changes in the software infrastructure.

FIM+ interoperates with:

1. ServiceNow, BMC Helix for Problem / Change
2. SPLUNK, QRadar, BMC AMI, other SIEMs
3. ISPW, Endevor, Changeman for DevOps security
4. RACF, TSS, ACF/2, firewalls for perimeter security
5. Multiple Storage products

It then uses that knowledge, combined with up to the second SMF data to recommend what needs to be restored. Concurrent with database recovery, the compromised infrastructure components can be restored to a point in time which eliminates all the malicious changes that may have been introduced. This is both faster and more precise than conventional processes.

Corporate data is a key asset to every organization, but only by recovering both your data and a trusted version of your infrastructure will you ensure a speedy recovery from a breach.