Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 15, Issue 4

How to Attack-Proof Backup Data Against Ransomware

By: Eran Farajun

Ransomware is one of the most significant malware variants impacting businesses globally—with attacks like WannaCry and NotPetya affecting more than 200,000 machines in 100 countries. The attacks by NotPetya alone resulted in a total loss of more than $1.2 billion with many other attacks driving up financial losses globally. To address this situation, individuals and organizations are investing in protective measures, including new data protection and security solutions, which have increased the ransomware protection market to new heights. In fact, forecasts show that this market will reach $33.21 billion by 2025, growing at a CAGR of 16.58 percent from 2017 to 2025, according to Trade Market Research.

Ransomware is a type of malware that encrypts all of the data on the system upon which it resides and demands a ransom for the decryption key. It then ransoms access to the data back to the system owners. The ransomware perpetrators threaten to destroy the key if they are not paid. They commonly do so in stages based on set time limits. If they are not paid the ransom, the ransomware destroys the key and, as a result, prevents access to all of the organization's data.

The most widely used approach used by businesses to recover from ransomware attacks has been to recover the criminally encrypted data from the backup set. This has provided a very successful workaround to paying the demanded ransom. Success in recovering ransomware encrypted data from the backup has reduced the profits of hacker revenue streams and, as a result, ransomware designers have evolved these attacks to not only target primary but also secondary (backup) data as well. One of the most aggressive strategies by ransomware developers for targeting backup data has been the attack-loop.

Cyber-criminals produce attack-loops and stealthily insert the malicious executable code within an organization's file system. Once in place in the primary storage environment, the ransomware does not detonate. The software is timed to hold off on executing until a predetermined day and time. In the meantime, this Trojan horse ransomware undergoes repeated backups over weeks and many months. When the execution date arrives, the encryption process begins, starting with the primary data. When IT administrators realize an attack has taken place, they will most commonly turn to their backup data and begin the restoration process. However, instead of restoring clean data, the backup solution instead recovers data infected with the hidden ransomware. Once recovered, the ransomware—which has been hiding in the backup data—begins to encrypt the files all over again, making it impossible to recover clean data because the company is now caught in a continuous encryption loop.

To contend with this increasingly sophisticated and disastrous situation, backup vendors are responding to ransomware in a variety of ways. There are still backup vendors in operation that are not implementing anti-malware technologies in order to keep development costs low. This gap, however, is leaving business customers exposed to attack. Some vendors are making attempts to deal with ransomware by implementing detection in order to discover ransomware detonations once they occur and are offering reactive strategies to recover data. The unfortunate consequence to this approach, though, is that there is little confirmation that encrypted data can be recovered once it has been impacted because of the fatal attack-loop. While a reactive solution will take action once the ransomware has detonated, a preventative approach is designed to stop backup deletions and encryptions from the outset. The question is, which is the better option for your organization?

A reactive approach leverages the backup software's incremental or changed block tracking mechanism. After the first backup, the amount of data being incrementally backed up is typically very small. When ransomware detonates and encrypts the data, the backup software sees the encrypted data as all-new and is forced to backup up all the data. When this occurs, it becomes an issue for the backup solution, resulting in backups taking considerably longer periods to complete. This action provides the backup software with an alerting mechanism and enables the user or software determined policy-based triggering thresholds to detect a likely ransomware detonation, notify the administrator, and suggest recovery responses. Some can start the recovery process immediately.

The problem with this increasingly popular approach to ransomware recovery is that it reacts to a detonation instead of preventing one. It assumes the ransomware infection has not made its way into the backups and thus enables recoveries from the most recent backup to solve the ransomware detonation. This is a dangerous supposition. Even assuming the backup software has an effective response to preventing the ransomware from encrypting or deleting the backups is a risky proposition, as previously discussed. Reacting to detonations does nothing to prevent the nefarious attack-loop. Therefore, detecting and reacting to ransomware detonations is an ineffective response.

Preventing a ransomware attack-loop requires a unique cyber security capability that must detect ransomware infections in the backup stream. This capability would need to isolate the infected files, prevent them from being backed up, and notify the backup and security administrators. The administrator can then identify the infected files and remove them from their origin before they detonate, stopping ransomware in its tracks. A backup solution with this capability also prevents infected files that may have been backed up in previous generations of backup data to ensure a clean recovery. The solution would need to detect and isolate the infected file and notify the backup and security administrators of any issues, giving them the option to recover or not.

Therefore, to avoid the evolving ransomware threat and the inevitable attacks on backup data, administrators must remain several steps ahead of these attacks by introducing strategies and technologies that make backup data attack-proof against this kind of threat. The first of these strategies is to identify backup solutions that acknowledge ransomware and have taken steps to defend the backup data against such attacks. Avoid solutions that are reactive by design and that only provide a response once the attack has taken place. Instead, seek solutions that prevent malware attacks in the first place.

As part of your mission to discover an effective anti-ransomware backup solution, refine the available candidates by identifying those that offer defensive responses to attack-loops. This would include a bi-directional malware scanning and mitigation capability that seeks to stop ransomware from entering the backup stream and, if ransomware is already present, stops and quarantines the ransomware so that it cannot be recovered and reinfect the network while also notifying those who can address the matter.

A multifaceted solution will provide the greatest defense-in-depth of the company's backup infrastructure. Look for solutions that make specific types of backup data hard to locate in the first place by using variable repository naming. This will make it much more difficult for the more intelligent strains to identify backup data with important customer records, personally identifiable information, very important financial data or valuable operational data. Experts also recommend going further and demanding two-factor authentication (2FA) that prevents the deletion of data with a single mouse-click or API call.

But if you are using backups as a form of data protection, do you really need to worry about ransomware hackers finding their way into your network? Why pay extortionists money if you already have your data backed up? The reason to move toward an evolved backup solution capable of preventing ransomware attacks in the first place is because traditional approaches to enterprise backup are failing when it comes to ransomware recovery efforts, as evidenced by the hundreds of millions of dollars lost due to these attacks.

While backups should be a critical component of every company's data protection plan, simply having backup infrastructure in place is not enough. Backup technology has evolved and now it is

possible to all but guarantee that backup data will be safe by using the right backup and recovery solution, giving organizations the best chance of defeating the extortion attempts of malicious ransomware coders.