

Recovering from Ransomware

What is Ransomware?

Ransomware is one of the latest forms of malware plaguing the Internet today. In a ransomware scenario, a user's system is held hostage until the user agrees to pay the proposed ransom through BitCoin or other hard to trace online payment method. Despite best efforts to recover – system resets, flashing BIOS or installing new hard drives – all the user sees is a ransom note telling them how much they need to pay to regain access before their data is permanently deleted. These ransoms can range anywhere from a few hundred dollars to over tens of thousands of dollars!



Ransomware propagates itself as Trojan, disguising itself as a legitimate file. It will typically spread through e-mail attachments, infected programs and compromised websites. These attacks target multiple platforms, including both Mac and PC operating systems. Some recent examples of ransomware are CryptoLocker, Cryptowall, Locky and KeRanger.

Challenges with Ransomware

Ransomware groups are getting sneakier. In order to avoid detection and boost probability of infection, ransomware techniques are increasingly becoming more sophisticated and may lay dormant for days (or weeks) on end. Newer versions of the malware try to infect network shares in addition to local direct-attached hard drives. Recent ransomware attacks try to disable data recovery options by either disabling Microsoft VSS to eliminate local recovery options and/ or encrypt/decrypt backups to make recovery from traditional backup impossible.

Solution

As ransomware becomes more sophisticated, so must the solutions from the Anti-Virus security providers. As part of a multi-faceted security plan it is imperative to have:

- A well thought out perimeter security
- Intrusion/ malware detection and isolation
- Backup/ recovery process with well-defined frequency

Progressive companies have taken advantage of the features provided by their next generation storage vendors to recover from such attacks. For example, the snapshots on the Exablox scale-out NAS Appliance are OneBlox Scale-out NAS Recovering from Ransomware designed to be completely immutable, fully protecting the unstructured data on the OneBlox. The OneBlox CDP (Continuous Data Protection) feature takes immutable snapshots automatically every 10 seconds for the first hour, then on an hourly, daily, weekly and monthly basis. Should a ransomware attack occur, encrypting the data and corrupting the primary file system, the snapshots are completely unaffected, immune from any modification or deletion. The ability to take such granular snapshots at 10-second intervals is critical to ensure recovery of the latest version of the data. Unlike legacy RAID-based volume snapshots, users can easily recover individual file, folder or complete network share.

Summary

Exablox's next generation storage helps protect users from ransomware attacks looking to take your data hostage. It is critical to ensure that an IT organization is well prepared with a multi-faceted security plan. Having Exablox to complement these procedures ensures a painless recovery and an added layer of protection to give you confidence that your users are safe and your data secure. Exablox customers such as **Christopher Rural Health** and **Pendleton Grain Growers** have recovered from ransomware infection painlessly.