You Can Avoid Paying Cyber Ransom!

Protect your valuable data from Cyber Attacks by implementing a capable backup and disaster recovery strategy

- When many businesses first recognize that a cyber-attack has occurred, it is already too late to prevent critical data loss or encryption. The virus protection software either failed to recognize the intrusion or recognized it after encryption had begun.
- The first instances of ransom cyber-attacks against hospitals in the U.S. involved compromised data being encrypted and held until the demand for payment was met.
- A reliable and safe analysis of the infected data must take place before the system can be brought back online. In order to accomplish this, a robust and reliable backup and disaster recovery strategy, like SEP Software, must be in place prior to the attack.

Boulder, CO – March 9, 2016 – Cybercrime is continually taking on the new forms. Recent cyber-attacks launched against hospitals and other businesses, cybercriminals are using the new encryption Trojans, Locky and TeslaCrypt, to extract payments in exchange for releasing their data. IT departments from around the world, across all industries, must now be prepared for this new form of cybercrime.

In a recent report released by Google's virus warning service, VirusTotal, only three of the 54 different virus scanning software were able to recognize the initial intrusion of the spyware*. In some cases, these Trojans were at work for weeks infecting the unprotected data without the knowledge of company personnel or IT administrators. Unfortunately, this situation in the U.S., has led to the first recorded hospitals paying cybercriminals a substantial sum of money to release the hospitals' critical patient data.

SEP Software, the developer of a platform independent backup and disaster recovery solution, is an expert in this area. SEP can advise companies to avoid such situations and provide expert assistance creating a thorough backup strategy to eliminate the possibility of blackmail during a cyber-attack. Using SEP as your backup software, a company can confidently restore all critical data, even after a ransom attack.

The following procedure is the only way to completely prevent the encryption of your data.

1. **Steps to be taken before the attack**

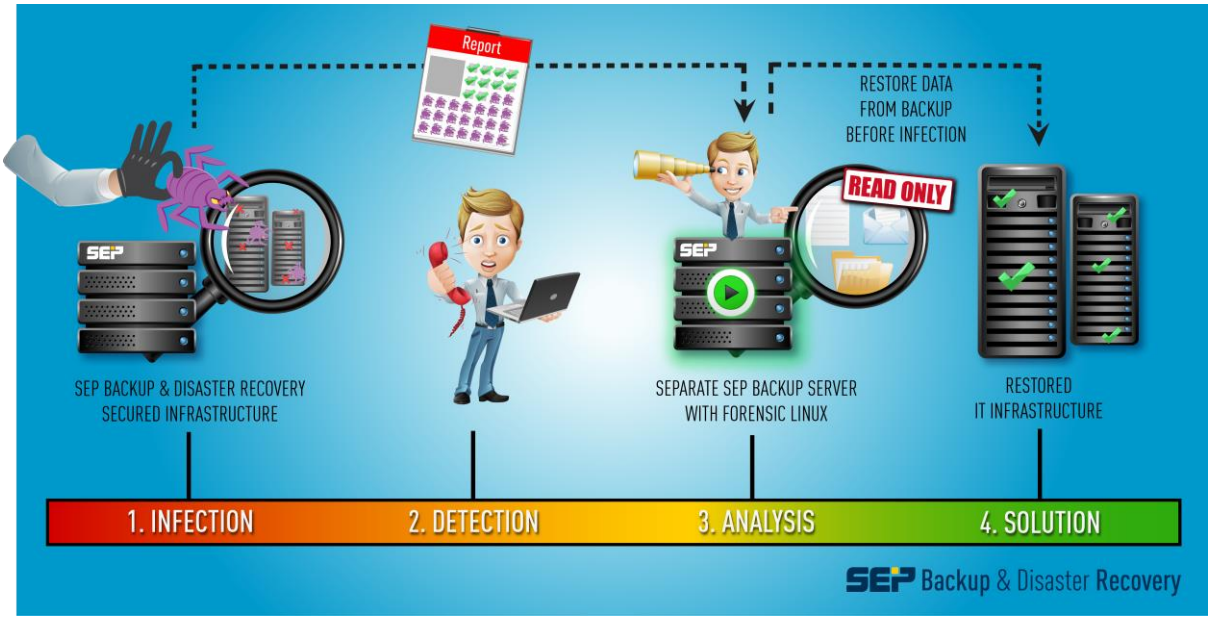
   In addition to the classic backup practices, including weekly full backups and daily incremental backups, the following measures are required:

   - The backed up data must be written to tape or removable disk drives and, when possible, stored at a remote location.
   - Due to the fact that the virus can lay dormant for a long period of time, the retention period should be extended.
   - The backup software must be capable of managing the tape drives and auto loaders.

2. **Steps taken after the attack**

After the attack is discovered, you must determine when the attack began and if any infected data was included in a backup.

- SEP is able to restore all required data from any chosen backup point-in-time to a protected system. This system should, of course, be clean and free of all viruses.
- Using the Read-Only-Mode, SEP can restore data to 'cleaned' servers, where your anti-virus program has been used to rid the contagion from infected computers. As the data is restored, it is checked by the anti-virus software to ensure that the Trojan will not be re-introduced into the new environment.
- In the event the encryption command from the cybercriminals has not yet been executed and you can still read your data, SEP supports forensic Linux distributions, like KALI, that have been developed specifically for analysis after a cyber-attack. This provides the capability to check every backup, regardless of the source: Linux or Windows Backup Server or Remote Device Server. Any file can be opened and screened for the virus.
- The malware does not have any ability to re-infect the system during the forensic analysis.
- Once the last uninfected backup data set is determined, all systems will be restored in a clean and usable state.
- All safety and anti-virus mechanisms must be updated and verified to prevent another attack.
- All systems can be restored and all processes can return to normal.



Infographic:

Restoration and Rehabilitation Procedures after a Cyber Attack

1. The infection has occurred.
2. Detection by the IT Administrator.
3. Determine when the virus entered the system by analyzing recent full and incremental backups. Pinpoint the last successful set of backups before the infection. Using a forensic Linux program like KALI on a protected server, find the infected files by comparing backup records, begin to analyze the virus and remove it from all servers.

- The backed up data will be restored from removable devices, like removable disk or tape, to the cleaned and verified system disk drives and mounted using Read-Only-Mode.
- Compare data sets from various points-in-time.
- Restore data sets that are confirmed clean of the virus.

4. Check that all systems safety and anti-virus mechanisms are updated and verified to prevent another attack.
5. Restart the systems and resume regular operations.
6. Continue regular backups and test restores to maintain the integrity of your DATA!

*VirusTotal Report:
https://www.virustotal.com/en/file/5e945c1d27c9ad77a2b63ae10af46aee7d29a6a43605a9bfbf35cebbcff184d8/analysis/1455638481/

About SEP Software
SEP Software offers a single backup and disaster recovery solution for heterogeneous environments of any size. SEP's flagship backup and disaster recovery solution uses its multi-streaming technology to facilitate unlimited simultaneous data streams to provide some of the highest performance in the backup market. SEP is cross-platform, multi-OS, and supports every popular database and Groupware solution available. Exceptional remote management capabilities allow users to easily and efficiently manage thousands of locations around the globe from one central location. SEP specializes in replacing multiple backup software products with one standardized solution for the entire enterprise. For more information on SEP and its product offerings, www.sepusa.com or email info@sepusa.com.

Corporate Media Contact
SEP Marketing
marketing@sepusa.com
303.449.0100