Don’t WannaCry? The Single Best Ransomware Prevention: Backup Computer Now

NEW YORK CITY, N.Y., May 16, 2017 (SEND2PRESS NEWSWIRE) — AOMEI Technology releases special version: AOMEI Backupper Free – Especially For WannaCry Ransomware, which has caused over 200,000 computers across 150 countries infected, and the number is growing. Hackers use a cyber-weapon called EternalBlue, developed by U.S. National Security Agency (NSA), as one method for spreading the ransomware. Once the system is infected, your most commonly used files will be encrypted with the extension .WCRY. What’s worse, it can spread to all the computers on the same network.

Send2Press® Newswire

This ransomware spreads through a vulnerability in Microsoft Windows. For now, more than 1.3 million computer systems are still vulnerable to WannaCry Ransomware. To protect against ransomware like WannaCry, you should download and install Microsoft patch MS17-010 immediately. At least two new variations of the WannaCry Ransomware have been detected already.

If unfortunately, your computer is infected, you are facing three options:

- Pay the ransom. Be aware that there is no guarantee that your files will be decrypted after paying $300. We don’t suggest you pay the ransom. If you fear your files will be lost after the end of the countdown, you can

backup all the encrypted files with Windows backup software.

- Restore from the previous backup to your original computer or another.
- Format your hard drive and reinstall Windows.

Obviously, backing up your data is the best defense against ransomware. If you have no backups, you should create an offline backup including all your files before the WannaCry variations delete the encrypted files.

Looking backward to the recent virus attack events, the new type of computer viruses will become increasingly insidious and threatening. It is never enough to only rely on that Microsoft or security agencies release patches. Although backup is an old routine, it can save you time and money in the event of ransomware or virus infection.

To ensure your backup is effective against ransomware, you should use 3-2-1 backup strategy. It means three copies of your data in two different locations, one of which is offsite. Even if one copy of your backup is encrypted by ransomware, you will still have other copies on external storage that ransomware cannot touch.

The easiest backup service provider – AOMEI Backupper is such a data backup and restore software. It allows you to automatically backup your system, files, disk, or partition to external hard drives, USB flash drives, CDs/DVDs, and NAS devices. In the case of ransomware running during backup process, you can create a bootable media and then boot from it to create offline backup.

About AOMEI Technology:
The Easiest Backup Service Provider – AOMEI Technology provides solutions for home and business users worldwide. We started in 2009 and our mission is your data will never be lost. Information: http://www.aomeitech.com.