**How to Recover from a Ransomware attack (or any other catastrophic event).**

Now is a good time to remind you about the importance of a data backup "habit". In the Vets Page of saratogaradar.org, there is a link to Technical Info. Here you will see a article named "Road to Saratoga Radar Website" which may help you with backing up all your data. This article will also be there for future reference.

**Ransomware** is all over the news and social media lately, and may be quite devastating to those that get infected with it. A type of malicious software commonly known as malware that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid.

While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult. The "pirates" will send you a de-cryption key to release your pc from the virus once the ransom is paid. But, they now know you will pay, so be ready for another attack in the future.

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers on a network without user interaction.

**1. Make a Rescue Disk**

A rescue disk allows the computer to boot up using the CD, thumb drive or external disk drive instead of its hard drive, which is handy when the hard drive is damaged or infected with a virus. The rescue disk also contains programs that can run an automated repair operation, roll back to a previously established restore point. Google "Rescue disk" to find the process for your specific operating system and storage media. You will also see many software packages for sale to make a rescue disk, a disk image if (recommended for the technically challanged) A Rescue Disk is usually made once and after it is made should be stored away safely in hopes that it will never have to be used.

**2. Make a Disk image**

A disk image is a single file or storage device that holds a replica of all data on a storage medium or device, such as a hard drive, tape drive, CD, DVD, floppy disk or key drive. A disk image is usually created through a sector-by-sector replication of the original - or source - storage medium, including the structure (directories and folders) and contents (files). Google "Disk image" to find the process for your specific operating system and storage media. You will also see many software packages for sale to make a rescue disk, a disk image if (recommended for the technically challanged).

A disk image may take a few hours to make and there is no need to make one daily as long as you are diligent about backing up your data. I make a new image disk maybe twice a year or typically after a new program or operating system upgrade is installed.

If your hard drive is maliciously encrypted or otherwise scrambled, first use your rescue disk to format your hard drive which will destroy any virus and also destroy everything that was on your hard drive.  Then restore your hard drive to what it was when you made the image disk using the image disk.  Again, for the technically challenged, buy one of the available programs and relax.

Maybe this will help you of maybe it will add to the confusion, I hope it helps.

Now you can see why corporations will pay the ransom. Many thousands of hours may be wasted imaging and restoring thousand of computers or pay the ransom.

Mike “Doc” Dougherty
Web Guy, saratogaradar.org
doc@saratogaradar.org