Should I be worried about Ransomware or Cryptolocker malware? Uh, yes...

If you have to ask, "Should I be worried about Ransomware or Cryptolocker malware?" you just might need to know a few facts before you find your business between a rock and hard place.

A Los Angeles hospital discovered the meaning of that saying earlier this year. The “rock” was a ransomware infection of its network where hackers froze all the hospital vital computer systems. The hard place was its decisions to a $17,000 demand to get everything back on line so that it could treat patients.

The hospital fought valiantly to recover its data without paying up, but ransomware encryption is so hardened, that without the encryption key, the victim can’t crack it. In fact, one FBI cyber expert advised that the best course of victims might simply be to pay up.

The CEO of the affected hospital agreed. In his statement of February 17, 2016, he wrote:

“The quickest and most efficient way to restore our systems … was to pay the ransom….In the best interest of restoring normal operations, we did this.”

Types of Ransomware

Ransomware comes in two unsavory flavors: encrypting and non-encrypting. The first uses an algorithm to scramble files so that the hacker can demand money to return everything to normal. Non-encryption ransomware simply blocks access to system files, is less harmful, and is susceptible to easy removal.

The Jigsaw

In other worse news, hackers are selling even more insidious versions of encrypting ransomware on the black market of the Darknet. For example, there is a new crypto-ransomware version called Jigsaw. Instead of simply taking the victim’s files hostage, this version begins deleting everything incrementally until the victim agrees to pay up. Jigsaw also steals data from the victim’s system.

Continued on Page 2

Avoiding the avalanche to stay away from the hard place

So until some white-hatted hacker comes up with silver bullet to bypass PC ransomware decryption, the best approach is to avoid the avalanche. Ransomware arrives on the back of phishing emails or booby-trapped links.

Educating the gatekeepers on the working side of a firewall even with alert malware detection software is a first line of defense. Fall back in case of penetration must include a disaster recovery plan, because a successful ransomware incursion means that the system is lost and data is gone—unless the victim has no backup for a complete restoral.

Isolate your backup devices

It is important to note that ransomware can also encrypt backup data directly accessible from the network. The backup plan must, therefore, include an off-site location along with local redundancy. The latter would be a separate server or drive, which is only connected to the system when it is actually backing up.

Looking for a IT services team with the people and expertise to keep your network running smoothly and safely? Contact us. We have successfully rescued clients locked up in Ransomware malware.

CST
Combined Systems Technology
800-944-2966 515-270-5300
www.cstoncall.com info@cstoncall.com