Computer Bytes – Ransomware

Provided By: Harv Oliver, HANDS-ON Consultations

Greetings and Happy New Year! I hope that all your endeavors, personal and business, are rewarding in the upcoming year.

I'm starting the year off with an issue that is hot off the presses. While this issue has been around a while, it rears its ugly head from time to time and has recently done so again. It concerns "RANSOMWARE".

What happens is your files get infected, encrypted and a 'key lock' is put on. Now you cannot open them without paying the guys who did it for the "unlock key". It's completely frustrating, wrong, and a real problem. Below, courtesy of: Catlain Cimpanu/Bleeping Computer, is a recent and a huge incident.

The Los Angeles Community College District (LACCD) agreed to pay a ransom demand of $28,000 to crooks who managed to infect the computer network of the Los Angeles Valley College (LAVC) with ransomware. According to LACCD officials, the infection took place on Friday, December 30, 2016, just days before the new year. School and district officials didn't reveal the type of ransomware that infected their network but based on events the district officials released online, the infection appears to have spread to their entire network, affecting several services, such as faculty and staff email servers, voicemail services, and more.

Attackers gave the school a week to pay the ransom. LACCD announced last Friday, January 6, 2017, that they've agreed to pay the ransom demand to quickly recover access to their systems and data. The District might have had their hand forced by the fact that classes resumed on Tuesday, January 3, with the start of the winter session. Officials used funds from a cybersecurity insurance policy to pay the ransom. After making the payment, LAVC staffers received a decryption key from the crooks who hijacked the school's network.

*LAVC officials said the decryption key worked as expected and the scho*ol's IT staff is currently slowly unlocking encrypted files and restoring service to computers, one at a time.

Having shared this, please note this is a real problem and a pain. HOWEVER, keep in in mind depending on the level of the infection, in many cases, you could recover from GOOD BACKUPS. I obviously don't know the details in the LAVC case but I have dealt with this type of infection personally. First, we remove the infection then restore data from backup. In our real world dealings, one client lost six months as they were not monitoring backups and for some reason the schedule was interrupted. Other times, after fixing the bug, we simply restored from “last night’s backup” and were back in business. We of course assist in setting up backups and if tasked will monitor, however, if we're not, things happen and users themselves must keep an eye on and verify backups are routinely performing.

This once again reiterates my continuing recommendation to stay up on your backups. It's a 'taken for granted' function but if you get bit, you really feel the pain! Once again, HAPPY NEW YEAR and success for 2017!

NOTE: Our sharing of information within articles includes suggestions and tips. USE AND/OR APPLY AT YOUR OWN RISK. If you have any questions or concerns, please contact our offices for professional service/guidance.

Until next time, don't forget your backups! For more information, contact Harv Oliver, **HANDS-ON Consultations**, **(805) 524-5278, www.hocsupport.com**