The
Broadcasters' Desktop Resource
www.theBDR.net
... edited by Barry Mishkind – the Eclectic Engineer

Bits & Bytes

Ransomware Reality

By David Bialik

[May 2021] For most of us, ransomware is just something we read about – an IT issue, more or less, at most an inconvenience for a short time. Perhaps worthy of a sigh. Or a mild chuckle. We might even feel bad for the company hit, but it most likely did not affect us.

Is it real enough for you yet?

We have read a lot about ransomware attacks, how over 2100 companies in this country have been hit, with estimates of as much as $500 million paid, despite counsel not to do so. Yet, for most of us, it is just a news report.

On the other hand, ask the tens of millions of people suddenly thrown into the chaos of long lines for gas – if you could even find a place where there was gas available.

The hit on the Colonial Pipeline earlier this month continues to be a real disrupter of lives, 45% of East Coast fuel, and a warning of worse than could come if key utilities are targeted in the future.

Is it real enough for you yet?

GETTING REAL

So I was visiting a friend's office the other day. A small law firm, five people.

Suddenly one attorney yelled "I can't access my files," followed by expletives that should not be repeated. My friend tells me they got rid of their IT consultant a couple months ago and asked if I could look at the issue.

Many broadcast engineers are afflicted with this situation: People think we can fix anything. For some reason I still said "sure, why not."

RANSOMWARE ALERT

The issue is that they were hit with ransomware.

First, I told them to unplug the network cables – and pull the power chords from the computers.

Next, I started to regret agreeing to work on the issue. Having worked for a large broadcast company that was hit a few times with ransomware, I knew exactly how bad a ransomware attack could be.

Thus, I explained to my friend the seriousness of the situation and why they are going to listen to me carefully step by step.

Since it is a small office, I asked each user what were they working on? What windows had been open? When did they first notice the files were coming up with the ransomware message?

As luck would have it, I was able to determine the hour that this happened.

SPEEDBUMP

To progress further, I asked for the server password.

Silence hit the room with a perplexed look. How could well-educated attorneys trust their documents and their financial data to a server previously managed by a part-timer and not have the credentials to log-in.

I know this is a common issue, but I was still amazed.

Finally, one of the secretaries (yes it seems like it is always a secretary) said "I can call to get our password." As expected, the password was the owner's dog's name.

FIGHTING THE BATTLE

Now the work started.

I downloaded on my notebook the latest copy of Malwarebytes. Yes, there are many programs to use, but I like this one. I took the installer and put it on a usb stick.

I then logged on to each of the workstations as the administrator (oh yes, the password was "admin," argh!!!) Malwarebytes was already installed but I reinstalled it anyway to guarantee it was the latest version with the latest definitions. With that tool, I scanned each machine – with all computers still physically unplugged from the network. I did the same on the server.

Around two hours later and a number of possible culprit files found, we determine that we are clean.

SLOW, STEADY, CAREFUL

Everyone is now getting restless.

Nevertheless, I tell them that this is a process and not following directions will cause greater loss. The room of attorneys suddenly hushed.

Based on the information they gave me and the assurance that they had the previous night's backup, I made the decision to revert the server back two hours by the Shadowcopy. This seemed to be clean but I scanned the server again. So far, so good! It was time for the network connection to be reconnected.

Now I asked for everything to be turned off. Then, I turned on the server, and rescanned it, and we are good. Next, we reconnected and turn on the workstations – and rescanned them to ensure everything was clean.

LEARNING FROM THE INCIDENT

They were back up and happy.

It was now time for me to explain to them that they were extremely lucky. The need for tightened security was evident. They lost around two hours of work – and around six hours of billable time – all was able to be salvaged or redone.

Despite the thousands lost, they were back up, and knew they did not want a repetition. The person who triggered the ransomware committed to greater care in the future in opening email and files. My only statement on this was how fortunate they were to have caught the attack at the right time, and I became a great proponent of Shadowcopy.

NOT ALL OUTCOMES ARE GOOD

This is not a suggested way of fighting a ransomware attack since all are different and at varying scales, but in this case, my recovery plan worked!

Colonial paid the ransom, $4.4 million or so, according to their CEO, Joseph Blount. That did not work. The decryption key did not clear all the damage caused by the malware, administered by an Eastern European group called DarkSide. Reports are normal operations were still weeks away.

"There are three problems contributing to the ransomware crisis," the former head of Britain's cybersecurity agency said. "One is Russia sheltering organized crime. A second is weak cybersecurity in too many places.

"But the third, and most corrosive, problem is that the business model works spectacularly for the criminals." When they get a "hit" they try to replicate. Thus, in the recent past, not one, but several broadcast companies got hit – Urban One or Cumulus or Townsquare or Entercom, as examples.

By the way. After all the getting the law office back on line, my friend took me out for a late dinner.

Is this all real enough for you yet?

- - -

David Bialik has been doing broadcast engineering and IT work for over 40 years. He is the Chairman of the Broadcast and Online Delivery Technical Committee for the Audio Engineering Society.

You can reach David at: dkbialik@erols.com

- - -

- - -

Return to The BDR Menu