www.TheBusinessNewsOnline.com

Protect you business from ransomware attacks

SCOTT TORNIO
GUEST COLUMNIST
TECHNOLOGY

This is not a judgement, just a true story of what can happen when busy schedules and tight budgets get in the way of managing business technologies. At the end of the day, this is not uncommon. There are a lot of companies who make these exact mistakes. We have businesses to run and that is the priority.

It was a Saturday, and I was out of town at my son's baseball tournament when I received a call from a business (let's call them Company X). This business has their own IT department, and we don't often provide IT assistance, so I assumed this would be a real quick, "Hey, how do I configure this" sort of thing. Unfortunately, my expectation was not reality. In a calm, yet panicked voice (like a duck on water) I heard, "We were infected this morning and cannot access any of our files".

"Infected? With what?"

He answered, "SamSam. They want six Bitcoin."

Six bitcoins, at this time, were worth about $40,000 U.S., and SamSam is a nasty ransomware. Similar to CryptoLocker, SamSam exploits weakness in networks or process to encrypt company files on a network. SamSam was best known for going after hospital systems but also hit some metropolitan agencies and a handful of larger corporations.

Unlike most ransomware, SamSam left a calling card in the form of the word "Sorry." Seems facetious and a little cocky to apologize as you are committing a crime, but by the end of everything I definitely felt that they were sorry. Not that they infected the business, but that this business opened themselves up to the infection. "Sorry, but you deserve this," is what I believe they meant.

Company X has multiple locations and utilized an outdated system to backup files from one location to another. The technology for all of this comes from the days of tape backups. An application makes a backup of all files that have been altered, condenses everything into a file and deposits that file into the backup receptacle of your choosing. It used to be tapes, today it is a server, located across the country. The problem with that particular technology is files. SamSam encrypts files, all of them, including the backups.

With most modern backups, we do what's called a bare-metal backup. What this means is the backup system is backing up the entire computer or server, operating system and all. In the event of infection, you are able to simply restore the server, as it was before the infection. There will be some obvious clean up and security tasks, but most businesses are back up and working in about 24 hours. A modern backup system could have saved the day here.

Old school backups: Strike one.

Back to Saturday: Within an hour or so, we determined that paying the ransom was about all that could be done. With no available backups to restore from, buying back access to their data was the only path forward. We called in whoever was available and got to work researching options and making calls.

The ransom note from SamSam provided a phone number for customer service. You read that right. The cyber criminals had a customer service team. To be honest, they were super friendly and helpful. Customer service instructed us on how we can get Bitcoin, who to call to assist with the data cleanup and some helpful pointers on avoiding future infections. Ransomware is nothing new, but we weren't about to fork over $40K without asking around, so we contacted a couple firms that specialize in SamSam infections.

Although the SamSam customer service folks directed us to a specific firm for help, we went with a firm we found through an organic search. Would you choose a home security company suggested by your home invaders while they were still in your home? The firm we chose was going to be an additional $50,000, on top of the six bitcoin we were paying the bad guys. Who's really the bad guy, right? The $50,000 came with a guarantee to get all data back, and also clean all traces of the SamSam infection. By the end of the day Sunday, the bitcoin was purchased, a specialist firm was hired.

Monday went by fast. We had two system administrators on-site at the Wisconsin facility and two (myself included) flew to another facility across country. Just before we arrived, all transactions had completed, and we were given the tools and access necessary to start decrypting data. Seven total people, in two facilities started work:

1. Run the decrypter.
2. Back up the decrypted files offline.
3. Run a search and destroy malicious software removal tool.
4. Uninstall the old antivirus.
5. Install a new antivirus, provided by the specialists.
6. Mark the PC or Server as clean and move on to the next.

There were about 100 total computers and/or servers, and each took about an hour to complete. We could each do about two or three at a time, but our ability to work accurately was draining as we finished around 4 a.m. Back in Wisconsin, the guys got a hotel and planned to be back at 8 a.m. We did the same, except for Company X's IT Director—he continued to dot "I"s and cross "T"s, hopeful to start up production at 8 a.m.

We took an Uber to a hotel, but I couldn't sleep. I reflected on the day's events and created a list of what would need to be addressed as soon as we were past the emergency. As I worked through the list I remembered a comment from one of Company X's administrators. He mentioned (off hand, like it was unrelated) an issue he had encountered the previous week: They have a facility overseas that uses Remote Desktop Protocol (RDP) to access systems. Using RDP to access inside stuff from outside is always a bad idea, but they had taken steps to secure the connection. By only allowing RDP access to a specific IP address, they could ensure that only the computers they allow will have access to their system. Still a bad idea, but at least they did something to secure the connection. However, the issue they had the previous week was that the remote facility was no longer able to access the system they needed through RDP. The fix implemented, by a busy IT administrator, was to open RDP access to all IPs, hence allowing all Internet traffic access to their systems. Want to guess how the SamSam guys got into their network? That's right, strike 2.

With no sleep, but lots of coffee, we all arrived back to the respective business sites Tuesday morning. Everything went well getting production back up and running. With the exception of a few quickly fixed hiccups, our efforts were officially a success. Back in business and time to start planning for system upgrades, disaster recovery plans and process implementations. I won't go into too much detail there as there isn't much to tell. The business did the right thing and got the systems and processes they needed.

I do, however, want to recount some of the conversations that we had on Tuesday. The first of which was with the professional firm of SamSam experts. They were very helpful with getting the encryption removed, but then they sent a series of quotes for further services. With the purchase of "their" antivirus, they could guarantee no further SamSam infection would take place. Business upsell, after the fact you would say, but that was not the tone of these conversations. It sounded more like a couple of mafia enforcers, telling a hardware store owner that he needed to "pay for their protection or something might happen to his store". Owner refuses and his store gets trashed by… the mafia guys. Yeah, that's how it works, it's called extortion. It was pretty clear that this was also.

Here's the thing, SamSam was not going to reinfect anyway. Even if they could, it would be foolish to do so. Ransomware is a business model. Bad guys encrypt your stuff, you pay a ransom, bad guys give you back your stuff and they don't bother you again. If the bad guys don't give your stuff back or take your stuff again, you are going to jump on the internet and tell everyone about it, and everyone will stop paying the bad guys. It's bad business. I'm not saying you'll never get infected or hacked again. I'm saying that once you pay the ransom for this particular breed of malicious infection, you most likely won't get that particular infection again.

The firm that was hired to help is now the firm monopolizing on weakness and is now also a bad guy. Next step: rebuild the entire network and all data, offline, so we can box out the new enemy. An unfortunate after-effect, but one that should have been expected.

The second conversation that I need to mention is about the private equity company that owns Company X. They have a published policy that states to pay the ransom if they are infected with ransomware.

Take a moment and think about that.

They have a policy.

The policy is shared with the public.

The policy states they will pay, whatever you ask for, if you take their stuff.

Someone took their stuff. Shocking, I know…

Actually, I get it. The idea is that it costs so much money, time and effort managing data restoration and updating security that they just add budget to pay the ransom. The $40,000 in bitcoin isn't actually all that much. Is this really that bad of a policy? Look at it this way, why does the United States refuse to negotiate with terrorists? Is it because our people aren't worth the cost or because as soon as you pay the first terrorist, 500 more terrorists will come out of the woodwork, snatching Americans. You don't pay the bad guys because that just creates more bad guys. Strike three. Big strike three.

What's the point of all this? Consider the strikes:

- Strike three: They have a public policy to pay ransom. Don't do that. I imagine an Excel spreadsheet on the dark web somewhere titled "People Who Pay." Criminals buy names for $40 and then exploit weakness for ransom. Invest in avoiding attacks like this by maintaining a disaster recovery plan.
- Strike two: They used an unsecure connection to grant access to remote facilities. Don't do that. Invest in the right tools and technologies and make sure you have — or partner with — the right IT people.
- Strike one: Outdated, ineffective data backups. Don't do that. Data backups need to protect against all threats. Your data is the most valuable asset you company has. Failing to protect it puts your business, your clients and the personal information of your employees at risk. Bad backups is bad business.

The company and the story are real, and this actually happens a lot. In this case, the business recovered within a couple days, made the necessary adjustments and is doing great. Despite the cost of this episode, they are thriving. That doesn't usually happen though. Small businesses are shut down by events like this. "Why didn't they call the justice department," people ask. They did. Everybody does, and everybody finds out that the government is not going to save you from bad decisions or short sightedness. Get a disaster recovery plan that starts with avoiding the disaster. Make policies that protect your business. Back up your data properly with modern technologies. Work with actual experts who have your best interest in mind. Protect your data and your business.

I've said it before: This computer and internet stuff is probably going to stick around for a while. There is no going back to ledgers and file cabinets. You don't have to be a computer expert to manage your business, but you can't ignore technology and expect to have a business. Learn it or hire it.

There is some sad commentary in all of this. The cyber criminals provided better customer service than the majority of some current service providers. Seems like there is something there, but that may be another column for another time.

Scott Tornio is president of HawkPoint Technologies.