Hackers Hit a Small Town

If you are connected to the internet, you must read this.

Imagine, it is Friday morning. You stop at the local coffee spot; your mind is on the day and weekend ahead. You are thinking about your patients, events for the kids, chores at home. Your life is smooth right now, your business is thriving, and you love where you live.

What is any dentists worst nightmare? Losing their data? Losing their business? This story includes both possibilities.

Your phone rings and it is your office manager telling you the computer is not working. Probably no big deal, you head to the clinic. What happens next pulls at your heart. Good people, taking care of others, are put in to a terrible situation by a faceless cyber-criminal.

Sunset Case Study

Upon arrival the doctor and staff see a ransom note on the computer asking for seven bitcoins (approximately $60,000) to get access to the data…the clinic has been hit with ransomware. This begins an uncomfortable emotional rollercoaster.

Sunset receives the first call at 8:09am. The clinic's system was infected with a "Zero Day" type of ransomware which means this attack was new to the entire world. We verified the Zero Day designation with the FBI. Sunset deploys its emergency response team comprised of on-site and remote staff.

<u>The Rollercoaster</u>

Friday

Concerned but hopeful - There are patients walking in to the clinic and you have no ability to check them in or see any of the details of their appointment. The team quickly pivots to paper and stress is building. Sunset validates the cyber-attack and begins the restore process.

Concern rises – Sunset arrives and brings loaner equipment and begins to look for the backup files. The doctor has been thinking about the backup. He grows concerned because there have been no updates for some time from the outside company he uses for his backup (not a Sunset solution). He remembers receiving daily emails regarding the backups.

Shock then stressed out! – Sunset confirms, the outside company was not backing up the practice management system, only other parts of the business. The most recent backup files for the practice management software are seven months old. Sunset begins two processes on parallel paths:

1. Find any back doors or other methods to restore data
2. Track down the perpetrator and try to negotiate

The doctor leaves the clinic in disbelief. Desperate thoughts enter his brain. He is unable to eat yet had to attend a friend's birthday party and pretend nothing has happened. He has called his partner and they are thinking:

- Raise money and just pay the ransom. Yet they know this could lead to more demands and more money and still not get the data back.
- They live in a small town, this has put the business in jeopardy. If word leaks out they are concerned they may still lose patients or the entire business.
- Was this a HIPAA breach? If so, what do we do with that?
- Try to rebuild the data manually.
- Start over.
- What happens on Monday morning?

Saturday

No sleep. Stress remains constant.

Sunset Path 1 – Sunset has had no luck finding a back door. One of the doctor-owners is at a game for their child, but mentally completely absorbed with what might happen. Waiting is horrible.

Sunset Path 2 – Sunset's cyber team has begun to track down the cyber-actor. There are methods we have learned and developed as a member of Infragard (a private sector organization tied to the FBI) to track down cyber-actors. In part we place tools in the network that help us perform our analysis.

With cyber actions, in general, there are two possibilities i) a larger organized crime entity or ii) an individual. We caught our first break, the cyber-actor was an individual, larger organized crime entities do not typically negotiate. In these situations, the clock has started, which is usually 36 hours. Also, payment is only through bitcoin. As a result, time is critical. After fast research, an initial email is sent. The game of cat and mouse is on.

Sunday

Helpless, Insecure, Depressed and more…

The doctors call an all-staff meeting on a Sunday. The situation is dire. The entire team digs through the garbage, they look through all paper files to try to lessen the blow and solve Monday. The team does find one ray of sunshine: the clinic uses an online appointment reminder company and have one-week's information! They can at least deal with Monday, yet the larger questions remain. The team goes home after several hours at the clinic. The doctors are still full of doubt and continue to wait.

Sunset Path 1 – new computers have been put in, the team is working on restoration plans, either if they receive a key, or if they need to rebuild. The team is in constant and close communication with the doctors, which at least provides some sense of relief.

Sunset Path 2 – Our cyber team has been playing email cat and mouse with the cyber-actor through the night. The negotiations have been fruitful, break-throughs have occurred. Late Sunday afternoon, we received the key and began decrypting. IMPORTANT NOTE: the game is not done, because the cyber-actor can still disrupt the decryption. We keep the conversations going while we do our work.

Monday - Very early Monday morning, the data is restored. The cyber-actor realizes he has been beaten – until another day.

The total negotiated ransom:	$304.55

Back to the Zero Day designation: Sunset also reported all of this information to the FBI (IGuardian), which resulted in helping many organizations across the country.

Monday

Relief!
The doctors have avoided a potentially catastrophic event to their business. The rollercoaster of the weekend is behind them. One doctor commented after, "I feel like I lost one year off of my life!"

Summary

We roll the clock back on this story. The clinic decided to stick with a separate backup solution from Sunset. Unfortunately, as hackers become more sophisticated, situations such as these happen more often. Let Sunset Technologies help you to minimize your risk through these services provided as part of the Sunset Core™:

- Monitor the health of your network
- Qualified technicians are available around the clock for any problems that may arise
- Continuously monitor and manage your server and workstations to ensure minimal disturbances
- Scheduled reviews to discuss changes in technology and security
- Disaster recovery plan in the event of a data loss or breach
- Insurance coverage in the event of a data breach

Sunset's knowledgeable employees can help you when you need it the most. Their support lines are answered 24 hours a day, seven days a week. Sunset Technologies knows what to do and how to handle situations such as these to ensure downtime is kept to a minimum. Sunset also knows how to avoid these situations. Your company is important to you and to us, let us help you keep it protected.

"REST ASSURED" with Sunset Technologies.

Call Sunset Technologies at (855) 861-8833 or visit us online at www.SunsetSecure.com.