BILL BOOTHE
Bill Boothe is president and owner of The Boothe Group, LLC, an independent consulting firm that helps clubs understand computer technology, make good decisions and receive the highest value from their technology investment.
Bill can be reached at bboothe@boothegroup.com

Ransomware: A True Story

Wikipedia: "Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid."

And so, the story begins…

Day 1: Begins like any other Tuesday morning for the club's outsourced managed services provider (MSP). Nothing to speak of until mid-morning, when the front gate guard calls the club's controller complaining he is unable to print anything. The controller, who is tech savvy and handles many minor systems issues herself, drives out to the front gate to see what could be done. Looking at the guard's desktop, she senses that something serious is happening.

At about the same time, a technician at the MSP notices that the previous night's backup did not go through. Sensing that something is amiss, the technician drives over to the club and logs into the club's server. He quickly notices that an intruder is attempting to disable the antivirus software that protects the club's network. He also sees that the network is not functioning normally. A quick bit of investigation reveals the answer: a ransom note. The technician immediately begins physically unplugging all desktops, POS terminals, and the network servers.

"Greetings. You have serious security vulnerabilities. This can lead to leaks of important information for your company. We can help you in this matter."

Thus, begins a painful 11-day period of the club's computer network being completely paralyzed by the threat actors.

Days 2-4: Initiates the forensics stage of the restoration process. The club is fortunate to have in place a cyber liability insurance policy with an experienced and reputable carrier. The carrier's forensics team immediately begins its work and identifies the network entry point to be a tablet PC using Remote Desktop (RDP) without a secure VPN connection. This is a simple oversight on both the club's and the MSP's part. An oversight that opens up the club's network to the threat actors.

In the process of securing the network from further damage, it is discovered that the threat actors had actually entered the network a full two months earlier, giving them ample time to thoroughly explore the network's files and obtain passwords. And as is the common result of a ransomware attack, they have encrypted the server and all backups.

Wikipedia: "More advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them."

Day 5: The insurance carrier's negotiating team makes contact with the threat actors. The ransom demand begins at mid-six figures. Here is a redacted portion of the online negotiations:

Insurance carrier negotiator: *"How are we supposed to pay $XXX,XXX?? There's no way we can do that. And we don't even know what we get for that price…"*

Threat actor: *"You will get decryption program to recover all your infected data and any details about vulnerabilities you have."*

Negotiator: *"So it costs that to get our files unlocked? What if we can't afford that?"*

Threat actor: *"You can afford. It is reasonable price. This is an unexpected expense for you, I understand, but the price is acceptable for you."*

Negotiator: *"We can't pay that kind of money for this. We're better off recreating some of the data. We just thought this would be a quicker solution for a decent price."*

Threat actor: *"You can make an offer and we will consider it, but we do not expect small money from you."*

Negotiator: *"We'll have to see because we have a rough idea of how much it may cost to recover ourselves."*

Threat actor: *"Also take into account the fact that we have your files; if you are not aware of our methods of work, you should be aware that we publish confidential data of companies that do not pay."*

Simultaneously, the insurance carrier's public relations and legal team begins to formulate a communique to the club's

SEE TECHNOLOGY PERSPECTIVE | 102

from Green Committee | 64

ming to address these issues. We live in a desert and must be good stewards of our natural resources. Golf courses get a bad reputation, but we are the most efficient users of water compared to things like HOAs, community parks, businesses and homeowners. Our courses are equipped with a state-of-the-art weather station to measure rainfall, humidity and other weather data to help determine the proper amount of irrigation water to put on the course, so as not to waste that precious resource. Each individual sprinkler head can be adjusted daily based on fluctuating water needs.

OVERSEED

Located in the Southwest, our members enjoy golf year-round … and want to see green no matter the season. This means we undergo overseed nearly every year, which is extremely hard on our base Bermuda grass. Basically, as soon as the summer Bermuda grass is strong and vibrant, we scalp it almost to the dirt and plant Ryegrass. It's a constant cycle that injures the base turf and requires the team to shift how we care for and maintain the course as each type of grass needs different things in terms of water and fertilization to thrive.

This continuous transition between the two types of grasses is one of the largest challenges we face. There are only about four months out of the year that we are maintaining turf, the other eight months are spent either growing it in or eliminating it, scalping, overseeding, transitioning and nurturing into recovery. I like to joke that for those four months, when the grasses are at their peak and courses are lush and green, we are the smartest staff members on the property. Members think we're heroes. The rest of the year … well, let's just say we are apparently not so smart.

This year, to improve long-term course conditions, Superstition has made the tough decision to not overseed tee tops, greens or any of the rough – in some cases these are areas that have been overseeded every single year. It's a huge change for our members, especially the greens, but we believe it's a necessary evil to maintain the future health of the turf. It's a leap of faith and I'm grateful for the support we have from the club's owners and the understanding of our members.

At the end of the day, our goal is to provide members with a consistent, high-quality playing surface. As the course continues to age, the challenges we face will continue to change. And we'll adjust. Just as we have for the past 23 years. BR

---

from Technology Perspective | 84

members. So right from the beginning three teams are working on the club's behalf: forensics, negotiating and public relations/legal.

Day 6: The negotiating team settles the ransom amount for a low six figures – still a considerable amount.

Day 7: The club wires the ransom amount, in Bitcoin, to the threat actors. Once the funds are received, the encryption key is immediately provided.

Days 8-11: The MSP spends the next four days decrypting the club's files, rebuilding the servers, decrypting and restoring the backups, adding intrusion detection software to the network, and restoring operations.

Lessons learned

1. Don't think for a moment that private clubs are not ransomware targets. During my recent technology education sessions, when I ask for a show of hands from clubs that have had a network breach in the recent past, about a quarter of the participants raise their hands.

2. If you don't already have cyber liability insurance, get some – from an experienced and reliable carrier. The club shared with us that their annual cyber insurance premium is a tiny fraction of the ransom amount. Not a bad investment to have their system back up and running in 11 days – not to mention saving almost the entire amount of the ransom payment. Note: It's not uncommon to hear stories of clubs' systems being down for months as they muddle through the forensics, negotiating and restoration process on their own.

3. Get serious about protecting your club's network. Make sure your network is being constantly monitored for intrusions. Train your users to recognize attack ploys, such as phishing emails. Outsource your backups to a hardened data center to avoid having them encrypted by a threat actor. Schedule an annual systems security review with a qualified provider. BR