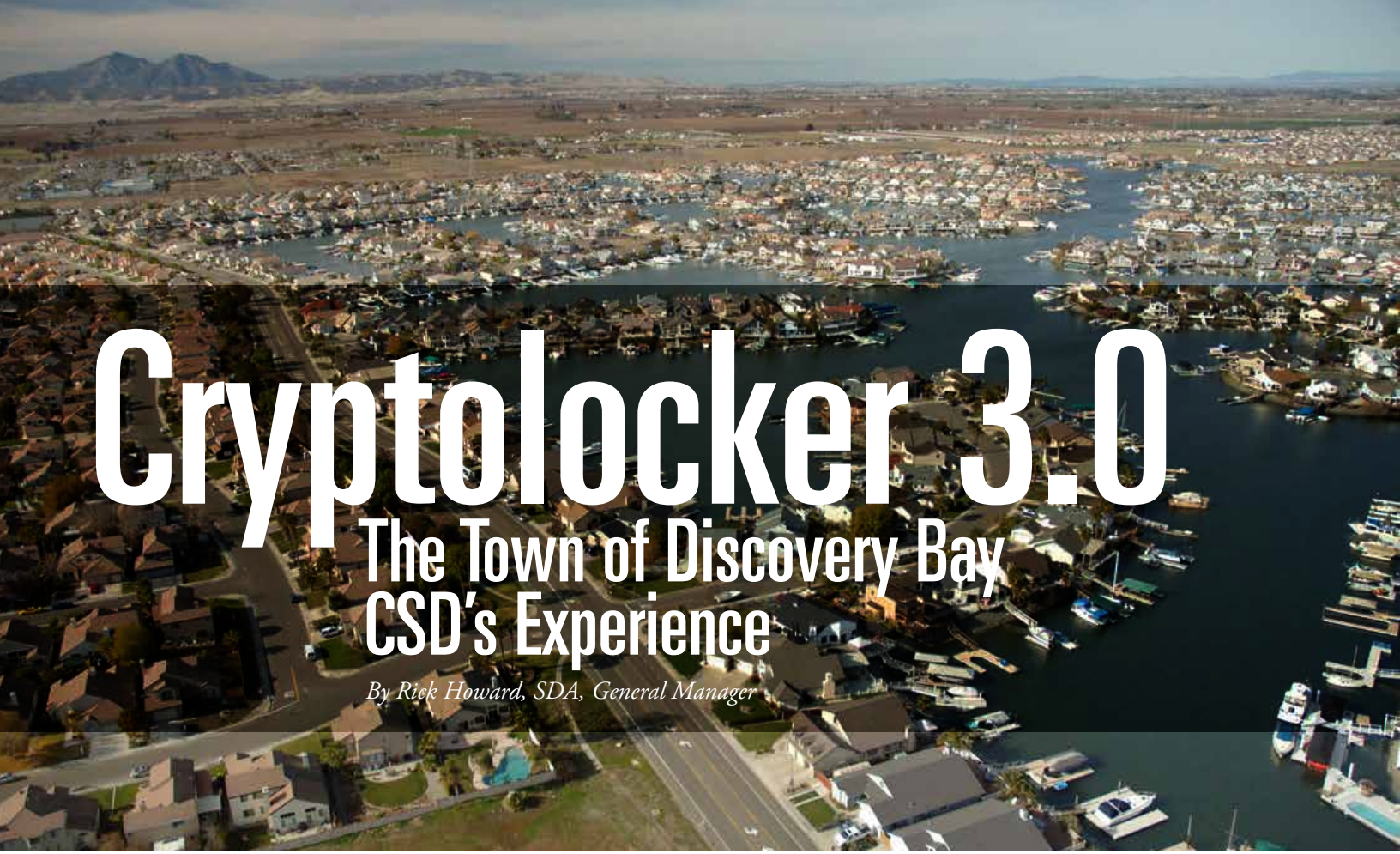

Cryptolocker 3.0

The Town of Discovery Bay CSD's Experience

By Rick Howard, SDA, General Manager

Monday, March 30, 2015 started off as any other regular Monday. Staff was rolling into the office, pouring their morning coffee and telling stories of weekend activities, little league games, and new restaurants that they had tried. Firing up computers, checking email, and returning phone calls all seemed natural. Until the unthinkable occurred.

Being a public agency, it's not uncommon to receive email from people seeking employment, and since we had a pretty high profile vacancy at the time, it was nothing but ordinary. The email was innocent enough – it had been sent from someone who had a common first and last name, the subject line was "Resume", and it didn't raise any red flags whatsoever.

Once the attachment was opened, however, our world turned upside down. A pop-up window appeared indicating that a little over 37,000 of our files had been encrypted with something called Cryptolocker 3.0, a Ransom Ware program that essentially locks files and doesn't provide the de-encryption codes unless you pay a ransom. In our case, $700. You have only so many hours to make the payment before the ransom doubles, and if you decide not to make the payment at all, the encrypted files are gone forever.

The immediate havoc that resulted was unimaginable. Once all network workstations, servers, and backup storage devices were shut down, it was time to figure out what we were going to do and how we were going to address this situation, get our files back, and get back to work. Our immediate reaction was to do what everyone would do – not give in to the cyber criminals and restore the encrypted files from our cloud back-up storage.

After notifying local law enforcement and the FBI's unit specializing in internet criminal activity (which surprisingly was no help at all), it was time to get to work and resolve the situation.

Being a relatively small agency, we don't have the resources to be able to have full-time IT staff. We utilize a local small business to provide that service for us. We also hired Innovate Computer Systems (ICS), a local Bay Area cyber security consulting firm with offices throughout California to assess our predicament, and eventually, provide an analysis of our vulnerability and ways to protect ourselves in the future, which I'll address a little later.

Once our team was fully assembled and onsite, the ICS expert reported that some of the files appeared to have characteristics that could possibly infect our cloud storage if we attempted to restore them using traditional back-up methods. Based on all of the analysis, we were doomed, and as untasteful as that seemed, we paid the ransom. The risk of potentially infecting our entire network made the $700 ransom seem small in comparison.

Paying the ransom was no easy task, and was extremely frustrating. The attackers require that the ransom be paid in Bitcoin, an internet currency that is hard to trace and the preferred method of payment for criminals indulging themselves in illegal cyber activity. The attackers even provide an FAQ and Help link to walk you through the payment process. A little bit of criminal customer service, if you will.

The only way to obtain Bitcoins is to go through a third party broker, and in our case, we utilized a Brooklyn-based international currency exchange that converts cash into Bitcoin. In order for this to occur, we had to get the cash, and in a public agency that doesn't deal in cash transactions, it wasn't as easy a task as one might think. Once we finally had the cash in hand, we had to deposit it into the currency house's Bank of America holding account. The money house instructed us to not identify them as the account holder or to mention how the funds were being utilized. They warned that if the bank knew that this was for a Bitcoin exchange, Bank of America would likely not process the transaction. If questioned by the bank, we were instructed to tell them that it was to complete an eBay purchase. This whole clandestine operation seemed incredibly inexplicable, but the bizarre didn't just end there.

Once the deposit was made, the clearing house provided very specific directions on what to do next. We were told to upload front and back photos of the bank deposit slip, along with a series of numbers provided to us to authenticate the money was deposited into their account and that we are who we say we are. Illogical as it all seems, at the time, it made sense. The photos had to be taken outside on a flat white surface in direct sunlight. We followed the instructions as directed, and shortly thereafter received confirmation that the currency house had received the funds and had transferred $700 in Bitcoin to an unknown account holder hiding out in a dark smoky room with only his computer screen providing illumination - which was the visual tale we had weaved into our minds.

About three hours later, we received a cryptic note on the infected computer (which we left up and running but disconnected from the network and using a mobile hotspot for internet connectivity) that our payment had been received, we were thanked for our promptness, and that our files had been unencrypted. At least they were courteous crooks. The encryption process that literally took seconds to lock up took almost 24 hours to unlock.

What started with a fairly mundane email on a Monday morning ended up costing us not just the $700 ransom, but the services of cyber experts, our IT consultants, and portions of 10 days of lost productivity. All told, approximately $5,000 in both hard and soft costs will never be seen again.

While some systems were up and running that week, we wanted to ensure that all of our financial data files and customer information, including any potential financial data breaches, did not take place. After a painstaking top to bottom system analysis by ICS, and knowing that our network was totally secure, we were finally fully operational the middle of the following week.

Continued on page 30

Town of Discovery Bay [continued from page 21]

Our Root Cause Analysis, or RCA, determined that the Ground Zero computer's anti-virus was out of date by less than a week. The employee had been on vacation the prior week, and, but for a series of events, this situation never would have occurred. Not taking anything or anyone for granted, the Town has also purchased four - 4TB NAS devices that are backed up every week, disconnected from the network, and stored off-site and in a secure and safe location.

ICS prepared a thorough system-wide examination of our network with a complete threat and vulnerability assessment, along with an analysis and list of recommendations on addressing any remaining computer and network security concerns.

While we are now back to peak operational efficiency, I can assure you that this is something your district does not want to face. The vulnerability we felt, the violation we sustained, and the harm it caused was unbelievably frustrating. It was a painful lesson, and one that could, and should, have been avoided.

I highly recommend you never open an attachment from anyone you may suspect is fraudulent, and never, under any circumstances, open a Zip file from an unknown source, as this is the preferred payload for Cryptolocker 3.0. Make sure all of your virus software is up-to-date and working as intended. Contact a cyber-security firm such as ICS if you have any concerns or want to conduct a vulnerability assessment. I hope that Discovery Bay's painful lesson will provide the wake-up call to every special district that if it can happen to us, it can just as easily happen to you. It just takes one click. ■

Rick Howard is the general manager for the Town of Discovery Bay Community Services District, an SDLF District of Distinction.

District **Snapshots**

The 13th annual Solar Cup competition was held in May. Los Osos High School, from Rancho Cucamonga, competed against 41 schools from throughout Southern California and placed 3rd overall in the veteran division. The school's team was sponsored by the Cucamonga Valley Water District and the Inland Empire Utilities Agency. Solar Cup is an annual competition that teaches high school students practical application of engineering, science, math, problem-solving, and management and conservation of environmental resources.