How We Overcame a Ransomware Attack

By Tony Mendoza, Senior Director of IT, Spectra Logic

If you're in the data storage business, the last thing you want to do is "announce" a ransomware attack. But that's actually counterintuitive. We were hit with ransomware, and as a data storage business, we feel it is important to share the story in order to help others prepare.

As Senior Director of IT, I'm not usually involved in the small, day-to-day glitches that occur. I've got a great team of IT professionals, and they rarely have to involve me in such normal operations. Thursday morning, May 7, 2020, would prove to be anything but "normal operations."

On that day, at roughly 9:20 a.m., I had two members of my staff report that lots of little things (none of which were related) were breaking. This was not normal. When a third staff member came in to report the same, there was a pause and then a scramble. We all thought the worst – have we been breached? We're now in the hall and running to the data center.

One of my guys jumped on a server to see if we could figure out what was happening. Searching the files, he found a ransom note. Our hearts dropped, but our feet hit the floor. We ran around physically cutting the cord between servers so they couldn't communicate with other servers to spread the virus further. Then we brought them all down.

It was now 10:45 a.m. and we heard one of the strangest sounds we had ever heard -- complete silence. Our data center hadn't been silent since we moved into it in 2012. We'd planned for this situation for years, but it was still uncharted waters for all of us. Once we got the machines down, we had a minute to breathe. The ransom note informed us that we had been hit by the "Netwalker" virus. With a rough calculation, I figured the ransom would be around $3.6 million, and we had five days to pay it off in bitcoin or we were on our own.

I had one person checking on backups to figure out exactly what we had for a disaster recovery scenario. We rely on CommVault for our daily backups to both Spectra tape and Spectra BlackPearl® NAS. In addition, we augment those backups with VM snapshots and StorCycle® software for data migration.

We realized that our email server was not compromised. At least we could still communicate with the rest of the company and the rest of the world. We put as much protection around it as possible and brought it back up.

By noon, I emailed the appropriate individuals and groups throughout company. I also contacted the FBI, explained the situation, and they promised that someone from their cybersecurity team would call me back.

I assigned a group to start bringing up department servers completely disconnected from the network. We realized that if a server had 100TB of data, it now showed up as a single 100TB encrypted file. Out of a total of 600 servers, including virtual machines, we had 150 servers that were compromised.

By 2 p.m. we confirmed a few things that helped us take heart. We had tape backups from the previous Friday. Our total possible data loss would be three working days – not what you want to have happen, but we would be within my SLA. Tape would get us back to the beginning of the week, but we're a transactional company; every minute represents thousands of transactions. We run disk snapshots of our Nimble Flash arrays daily. We confirmed that we had uncompromised disk images for about 90 percent of our systems.

Our legal department informed me that they'd bought "ransomware insurance" a few months earlier -- something the IT team was not initially aware of. It was a stroke of luck. By roughly 4 p.m., our insurance company set us up with a security consulting firm that deals with these issues. They told us exactly what to do to "stop the bleeding." I put my team on split shifts around the clock. They were either working or getting a few hours of sleep.

Around 7:30 p.m., we were on a call with the FBI cybersecurity team. They've dealt with this a lot and said our only options were to negotiate with the threat actors or rebuild our data center from scratch. We were roughly 10 hours into the ordeal, and it already felt like it had been days.

This attack started on a Thursday morning. By the wee hours of Monday morning, we'd stopped the bleeding and did a full triage to assess our options. We had roughly 24 hours before we had to pay the ransom or lose that option altogether. Keep in mind, at this point, we hadn't recovered a single file. It had taken that long just to secure all servers and ensure that we had stopped the virus from spreading.

We had a meeting with all involved players: The FBI, our security team, our legal department, and my entire staff. I told them we weren't going to pay the ransom. In actuality, I never considered it an option. Once we confirmed that we had a backup on tape, we had the confidence to walk away from any options involving paying or negotiating the ransom.

We knew what our recovery effort would be. This wasn't just about restoring some files; this was a full-on disaster recovery operation, including complete wipes and rebuilds of every server. Based on feedback we got, it was estimated that it would take four to six weeks for us to get back up and running. With that in mind, we started rebuilding. It took five days to get the company back up; it took another week or so to get all of our systems back online; and it took another two weeks after that to get all of the kinks in connections worked out.

Postmortem

So, how did this happen? In late March, roughly a month before the attack, we'd sent hundreds of employees home to work remotely due to COVID-19. We went from a 99 percent on-premise work environment to a 99 percent remote-office environment -- overnight. Cybercriminals were all too aware of what was happening in the world, and they exploited it. In fact, I've come across some scary facts since this event. According to VMware Carbon Black, ransomware attacks have increased by 900 percent this year. And the security firm McAfee recently reported that Netwalker cybercriminals have made more than $25 million in ransom payments since March.

One of our employees was VPN'd in on a private laptop. They opened a piece of malware that would have been stopped by our virus protection software, Sophos, but Sophos wasn't installed on that system. It never would have been allowed pre-COVID, but we were acting quickly to respond to the pandemic, and unfortunately, one risk averted was another risk created.

Lessons Learned

Data First – Have multiple copies of data on multiple mediums in multiple locations. The best IT experts in the world can't help you get your data back if every copy is compromised. We never could have taken the bold step we did if we had not had those tape copies. Our data had been encrypted by the virus as fast as disks could carry it. You have to have a copy of data that can't be touched. Tape provided an air-gap, an electronically disconnected copy of data that could not be accessed.

Even if you're willing to pay a ransom, encryption-by-ransomware is messy. There's no guarantee you'll get the decryption tool if you pay the ransom, and there's no guarantee it will work. We relied on both tape backups and disk snapshots to restore our systems. We are now exploring ways to replicate our disk snapshots to a dark site. The decentralization of data can create management challenges, but we're exploring some pretty promising ways to centrally manage it.

Experts Second – Have cybersecurity experts onboard or close at hand. Not all companies are large enough to justify a full-time cybersecurity team. Four years prior to this, we had had three test servers that were not protected by our VPN become infected. Our production LAN was protected by the firewall. The servers were easily cleaned and restored from backups. That experience was useful, however. A few of the protections we put in place then helped us during this event. We actually do an amazing job of security here, but we don't deal with the aftermath of an attack on a daily basis the way cybersecurity experts do. Having ransomware insurance was a brilliant way to have a cybersecurity team there in an instant. You're never 100 percent safe. These attacks happen to organizations of every size and level of expertise, from world governments to the biggest names in industry. You don't want to go this alone. The cybersecurity team we had access to was able to help decrease the amount of downtime we experienced as well as take other actions such as verify that no data had actually been stolen or accessed. This avoided a nightmare that many organizations are strapped with for years afterward.

Balance Third – Good IT security is a balance of culture and security strategy. No matter what the level of security you deploy, you could always add more. At some point, however, that will start to impact your user experience and possibly the goals of the company which are accomplished through IT. Will you allow the use of Macs *and* PCs? Will you allow remote access, or require everyone to work on premise? How much will your virus protection software filter? Will vital communication be blocked due to extreme protection? It's all a balance. You may think you're willing to accept a risk that you really

aren't willing to accept once it hits. Figure this out ahead of time. Consult with security experts to develop a strategy that balances risk and IT policy.

In the end, we overcame the attack with virtually no data loss and absolutely no data stolen. One of our servers was not being backed up appropriately. Data for that server had to be reconstructed. It was time consuming and costly.

As difficult as it was, this is what success looks like after such an attack: Assess your infrastructure, your access to experts and your approach to IT security. There's no lock that can't be broken into, but by taking this approach, you will be able to minimize the damage and assure business continuance.

About Spectra Logic

Spectra Logic develops data storage and data management solutions that solve the problem of long-term digital preservation for organizations dealing with exponential data growth. Dedicated solely to storage innovation for over 40 years, Spectra Logic's uncompromising product and customer focus is proven by the adoption of its solutions by leaders in multiple industries globally. Spectra enables affordable, multi-decade data storage and access by creating new methods of managing information in all forms of storage — including archive, backup, cold storage, private cloud and public cloud.

To learn more, visit www.SpectraLogic.com.

V1-110520

303-449-6400 • 800-833-1132 • 6285 Lookout Road • Boulder, CO 80301 USA • spectralogic.com