Here’s what happens after a business gets hit with ransomware

intel471.com/blog/how-to-recover-from-a-ransomware-attack

When the cybersecurity community focuses on ransomware, the concentration tends to be two-fold. There’s tons of information on how the software encrypts files, how it spreads from machine to machine, and the various vectors by which it causes havoc. Then there is the chase to figure out who is responsible for creating the variant, what marketplaces they may be attached to, and if they can be tied to any other attacks.

What’s often neglected is the recovery work that needs to be done by enterprises once they’ve been attacked. The lack of knowledge is understandable -- few companies want to admit they’ve been hacked, and keeping it quiet often allows a business to stay on the criminals’ good side. As the problem has grown, outside voices in the form of law enforcement, federal agencies, and even some industry experts have put extra pressure on enterprises to refrain from paying ransoms. But when faced with cutting a check or going out of business, enterprises have little recourse.

This environment makes it difficult to get a full picture of how destructive ransomware can be. Intel 471 recently spoke with a chief information officer who was directly involved in the recovery process after his employer — a U.S.-based construction company — was hit by a ransomware attack in 2018. We have withheld his name due to legal purposes, further showing that talking about an attack years after it occurred is an extremely sensitive issue.

The company, which has been around for over 50 years, had to deal with the possible loss of its entire business after a criminal gang locked up its IT systems. In the interview below, he discussed how the remediation process went, why he ultimately ended up choosing to comply with their ransom demands, and whether he would do anything differently if the criminals threatened to leak company data.

This interview has been edited for length and clarity.

What happened with your particular ransomware attack?

We were phished by a banking trojan in June 2018. From what we determined, those credentials were then sold to the larger ransomware group that hit us. We came in on a Friday morning and (the criminals) were in our network and they had wiped all of our backups. We had backups in multiple locations and they locked us out of those. From about midnight on, they had scripts that were running and were encrypting our files everywhere: all of our servers, a lot of our desktops, it was large scale. Fortunately that morning, we were able to wrestle them for control and shut everything down. From then on, what really began was the recovery process. We tried going through the back door to get the keys, but were ultimately unsuccessful. We ended up paying a seven-figure ransom to get the keys. Thankfully, we had insurance, but not that it really mattered, because we were on our knees at that point.

We spent the next two weeks trying to get things back online. We never turned anything back on, we actually rebuilt our entire environment from scratch. We rebuilt our domain. Once we got data back, we had to scrub and clean it to rebuild Active Directory. None of the servers that were hit have ever been turned back on, but we still have them in a virtual state.

When you said they had ‘all your servers,’ how many servers are we talking about?

We have about 300 servers; not a big environment. And they didn’t hit all of them. But they hit all of our domain controllers and all of our file servers. They had been on our network for a couple of weeks. I think they had keylogged some of our infrastructure and support teams, who had administrative rights to a lot of things. So they just watched where that team went. They knew which backup servers we had, where our appliances were, I think they had the lay of the land.

So they hit the main servers, and it was just fallout from there, with those servers talking to their other servers. They didn’t hit all of them, but they hit the most important ones. Then we decided to shut down everything out of precaution because we didn't know what was still compromised, where scripts were sitting, if it would start all over and wreak havoc again. So we chose to shut off everything and start from scratch.

When you said you ‘shut everything down,’ how did that impact the business? Did things grind to a halt?

Our company was shut down from a systems standpoint. From a construction standpoint, we weren’t shut down because out in the field, we could still physically build buildings, they just didn’t have the systems to log a bunch of things. They were keeping track of everything by paper. We had to go back and enter stuff into the end of the system, and we were able to restore back to a couple days prior to the incident. So from a construction standpoint, we didn’t lose a lot of data. The architecture side of the business came to a grinding halt because their drawings were on the servers. Email was down for the better part of multiple days. Fortunately, it happened on a Friday, so we had a couple days to get some things sorted out. By Monday, we had email back up, so we could communicate. Fortunately, we had just done salary payroll, so we had two weeks to get everything back up and running there. We didn’t miss any major deadline from a business standpoint.

Did the whole recovery process fit into that two-week timeline? Is that how long it took to remediate this entire episode and get back to normal business?

No. It was a week just to get the keys. We paid the ransom, and that took the better part of a week. It wasn’t because we were negotiating, it was the communication [with the attackers.] As we were communicating, maybe you would get back a message a day-and-a-half later, you might get it back the same day. The communication process with the hackers took time. You’re at the mercy of the hackers. We tried many, many different ways to get keys, and we were just very unsuccessful, like many people who take that route.

From there, we were able to get some “swing gear” from one of our partners. Fortunately, we were in a very good situation where we had a virtual desktop infrastructure environment that we were able to repurpose and use as a scrubbing environment for all of our data. That probably sped our process up by month. Had we not been able to do that, we would have spent at least the better part of a month recovering and restoring data. Because we had a highly powerful environment, we were able to decrypt and scrub in a matter of days. Had we not had that environment, we would have been talking a month, maybe two. Once we had the keys, we were able to get job sites back online day by day.

We physically had people drive their servers from different states because it was our only copy of the data, albeit encrypted. It was the only copy. We couldn't risk putting those on the plane, having them get damaged, or lost in transit. So we had people drive from multiple states, their servers — job site servers, regional servers — to our headquarters. When they came in, they waited around a day, we recovered, restored, scrubbed, put it back in their car, and they went back to their office.

How would you describe your interactions with the attackers? Did they mess with you at all or did it seem like an organized operation?

The attackers didn’t mess with us. We decided working with our legal team and insurance right away, that we knew we had coverage. And so we said, ‘That's what it's for, we're going to use it.’ Our initial conversation with the hackers was “We are prepared to pay, please provide instructions on how to pay, and we will meet your ransom terms.”

We spent the first two days with legal and insurance. They brought in their team of experts, because obviously, they've dealt with this before, so we consulted with them in the beginning to help us understand how these things typically work. Then ultimately we just decided to meet [the attacker’s] demands.

Some of the things that people don't think about is if you have insurance, there's a way in which you have to go through the process in order to be covered. Who you use for recovering, who you use for forensics, you got to follow the carrier's process, or they won't cover you. Fortunately, we were able to ask enough questions up front, and probably because we had the time to do so, we were able to do everything by the letter of the law, to make sure that we were covered in the recovery process.

Did you ever get the FBI or any other form of law enforcement involved?

We got hit on Friday and we had the FBI in our office on Sunday. They took copies of the data back to their office to see if it matched anything that they had already seen. Unfortunately, it didn't. I think they were able, with the work of some of the forensic teams, to track this back down to a Russian group. We never had a clear identification of who it was, we really didn't have a full chain of custody of our data.

Did the FBI ever weigh in on the fact that you paid the ransom?

FBI agents encouraged us not to pay. But they also were completely understanding that we didn't have an option. I think had we had our data and the good backups, they would have really strongly encouraged us not to pay. But they knew the situation we were in -- it was very, very damaging. So when we said we're going to pay, they were like “We completely understand we ask people not to pay because it only fuels the buyer, but we understand the situation, and you have to do what's best for your business.”

Ransomware groups have moved from locking data up to taking data and threatening to dump it online if a ransom isn’t paid. Had that been the scenario you were facing, would you have done anything differently?

It's hard to imagine that because we immediately were like “We're going to pay.” Let's say we had all of our backups and [the attackers] said they were going to dump it online. You know, because we wouldn’t have known what data they had, payroll data, employee information, etc., I mean, we would have paid again. Knowing that you have insurance makes some of these decisions a lot easier. If you don't have insurance, they're probably much tougher decisions to make.

Look, the criminals are smart. They're not throwing out ransoms that you can't afford. They do their research. They knew the size of our company, they knew the revenues. I think [the idea of dumping data online] changes anybody's tune, knowing what data could get potentially dumped and what it exposes. From a customer employee standpoint, there's some data that's highly sensitive. From just an employee morale standpoint, that can be damaging. All those things have to be taken into consideration. When you don't have the ability to pay, I think you really want to take all things off the table. And I will say, the hackers, you know, when we were communicating with them, I think one of the early emails was like, “Hey, if you pay, there won't be a problem.” I think we said “We're happy to pay, we want to put an end to all this and get our business back in process.” To answer your question, I think you have to take all those things into consideration. And if you don't have insurance, some of it is what can you afford to pay? Right? Either you have the cash flow to pay, and it's worth it to keep your business running, or you don't have the cash flow. But all things have to be taken into consideration.