rubrik

Langs Building Supplies: “We’ve been hacked!”

LANGS BUILDING SUPPLIES

INDUSTRY:

Manufacturing

CHALLENGES:

- Ransomware attack initiated through legitimate looking email
- Hundreds of thousands of files deleted
- Hackers demanded $15M ransom in Bitcoin

RESULTS:

- 0% data loss
- $0 paid in ransom
- 100% recovery from ransomware within 24 hours

It was 4:00 in the morning, May 20, 2021. Matthew Day, CIO of Langs Building Supplies (Langs) was excited for a long-anticipated holiday after 14 months of lockdown due to COVID-19. His wife was thrilled. All of his friends, ecstatic. But the day took an unexpected turn. Instead of waking up delighted to leave for his getaway, Day woke up to every CIO’s worst nightmare, the dreaded phone call, “We’ve been hacked.”

Upon arrival at his office, he tried to bring up the system. Nothing. Instead, what came up was a ransom note, ‘You’ve been hacked’. This is when he realized, “This is not just an unplanned outage. This is a targeted attack. We were profiled,” said Day. “The hackers looked at our business and they took their time. They found a source that we trusted implicitly.”

The hacker’s attack vector was a legitimate looking email that came from a proper email address, from the right account, in the right format. The one slight detail that was off was the link within the email. The link that Day’s accounting team typically uses to send purchase orders did not go to them. Instead, it went somewhere else.

Two weeks later, the hackers had access to Langs’ systems. They kicked off the malicious attack at 2:00 AM, when they knew no one would be around. “The hackers are smart. So the attack came in waves,” Day explained. The first wave was Friday morning when he got the call. Aaron Pritchard, Langs’ IT Systems Analyst, spent the day cleaning up their environment. Just when they thought they were able to go home, they decided to test the network once more. After logging in remotely, they realized they could not get in. “This was a pretty scary moment,” Pritchard said about being compromised again.

“RUBRIK WAS OUR SAVING GRACE”

Leveraging Rubrik’s ransomware remediation service, Day and Pritchard could see they were compromised. Pulling up their Rubrik dashboard, they noticed hundreds of thousands of files were deleted and thousands were modified.

“Rubrik is particularly useful for ransomware attacks in which you have tens of thousands, or hundreds of thousands of files in the span of minutes being encrypted, or deleted, like we experienced. It really helps you assess the scope of the threat and where we needed to start targeting our recoveries,” Pritchard stated. “With Rubrik, we were able to analyze the impact, quickly identify what data was encrypted and where it resided in our environment. We did not have to pay the $15M ransom. We had zero data loss. And we were fully recovered, up and running in less than 24 hours. Rubrik really saved us.”

"THE WAR IS WON. PEOPLE'S JOBS ARE SAFE"

There is an extreme amount of pressure facing CIOs, especially when there is no production happening in a factory that employs thousands of people. Day remarked, "When I have to send those people home, I take a personal hit on that. I feel personally obligated. Their livelihoods are in my hands. Not only do the implications of a ransomware attack hit home personally, it also implies revenue loss, production delays, and brand damage."

After Day overcame his roller coaster of emotions from anger, to regret, to failure, he suddenly had this "ra-ra" feeling of knowing his team could handle this. "You think you've been successful in attacking us but here's the counter punch. With Rubrik, we've got a very good right hook and we're going to come back harder. At the end of the day, this attack is just going to be an inconvenience."

"Rubrik was ticking away recovering all our data and I had this blinding flash of the obvious. We've been fighting battles all day but we're at this point where I can happily declare 'the war is won'. I knew that people's jobs were safe. Rubrik is not just about recovering from ransomware. Rubrik is the difference between survival and non-survival in this new digital age," Day remarked.

Straight from the CIO:

- **$0 paid in ransom**: "The hackers originally demanded $15M in Bitcoin. Then, they went down to $1.5M. Either way, we did not have to pay the ransom because Rubrik just works."
- **0% data loss**: "We were fortunate enough to experience zero data loss. Rubrik just did what Rubrik does. That's the beauty of the product."
- **100% recovery from ransomware within 24 hours**: "I know of another manufacturing organization where it took them six months to recover and they did not do any manufacturing for a full month. My managing director pulled me aside and said 'Wow, I don't want to think about what the world would look like if we didn't have Rubrik and didn't do manufacturing for a month. That would be a serious detriment to our business and one we might not be able to recover from.'"
- **Native immutability**: "The singular event that was the saving grace, the hallelujah moment, where we knew we were going to be fine, was being able to recover all the machines with Rubrik. The hackers couldn't get to it because of its native immutability. Without Rubrik… well, I don't want to think about it."
- **Ease of use**: "This was the first large scale event in which I used Rubrik and it was so intuitive, so easy to use, so fast. Just with a click, we're recovering entire servers and entire file sets. Something I never even knew Rubrik was capable of."
- **World-class support**: "Having confidence in the product is having confidence in the people. The constant communication with Rubrik, even during the attack, is what made us feel at ease. I know the support team at Rubrik had my back."

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Langs Building Supplies, founded in 1976, has been committed to delivering the highest quality products and services. In order to maintain confidence and trust among their customers and ensure a zero trust architecture, it is imperative they partner with scalable technologies such as Rubrik to stay top of mind within the manufacturing industry.

20210902_v1