How a Manufacturing Firm Recovered from a Devastating Ransomware Attack

By Kelly Jackson Higgins

Published: 2019-05-20 · Archived: 2026-04-05 13:05:23 UTC

The tiny IT team at C.E. Niehoff & Co. had been working for two weeks to run down and clean up a malware infection that had infiltrated its network after an employee clicked on a URL in a phishing email. Unbeknownst to the company as it scrambled to quell the attack, the malware, which was later identified as Trickbot, was quietly spreading among its endpoints and servers, gathering intel about the manufacturing firm and stealing credentials from the compromised machines.

It wasn't until the morning of Sunday, Oct. 14, when C.E. Niehoff IT manager Kelvin Larrue logged into the company's network from home, that it became clear to the company that the attack was something much more serious than a bot infection. A stunned Larrue could see that an intruder was running a PowerShell session on one of the company's servers, moving from server to server with stolen credentials and disabling security tools.

"I could see what he was actually doing. I knew we were in real trouble and someone was in our system," Larrue recalls. "They literally had the keys to the kingdom."

Larrue jumped into his car and drove the 20-minute route to the data center on the company's campus in Evanston, Ill., which houses its corporate headquarters and the manufacturing plant where it builds heavy-duty alternators for government and emergency vehicles. Racing to shut down the network in order to shut out the attacker, Larrue and his team pulled the plug in hopes of preventing the attacker from getting any deeper into the network, but it was too late.

"By that time, the perpetrator had done extensive damage to our network," he says. The attacker had begun dropping ransomware: "He had started routines to encrypt files on all of the servers and any workstations he happened to be on at that point," Larrue says.

What Larrue was witnessing firsthand, he later learned, was a Ryuk ransomware attack on his company. Ryuk is part of the recent generation of ransomware variants that is typically used for custom and targeted attacks on bigger and potentially more financially lucrative targets. According to Check Point Security, which has studied Ryuk and its attack methods, Ryuk's authors built it with an encryption scheme that targets critical resources and assets in a victim's network; for maximum impact, its payload is released manually by the attackers once they have the intel and stolen credentials they need.

"When [Ryuk attackers] infect a new victim, they can stay for a while to observe the network ... and see if the infected machine or network is interesting," explains Itay Cohen, a security researcher with Check Point who tracks Ryuk. "They do not automatically drop Ryuk; they drop it manually" if they decide it's a useful target. That's a departure from earlier ransomware attack campaigns that were more random and automated, he says.

Ryuk has claimed several high-profile victims since the fall of 2018, including newspapers such as the Chicago Tribune and the Los Angeles Times; the city of Stuart, Fla.; and Onslow Water and Sewer Authority, which was hit with a ransomware attack in October 2018, around the same time frame as C.E. Niehoff.

Ryuk and other ransomware, such as GandCrab and LockerGoga, which crippled Norwegian aluminum manufacturer Norsk Hydro, are all about targeting what CrowdStrike calls "big game," or large organizations theoretically able to pay a higher ransom than randomly infected consumers or small organizations.

Larrue says C.E. Niehoff believes the malicious URL in the phishing email that dropped Trickbot was the first phase of its attack and where the intel-gathering and credential-stealing occurred. In some Ryuk attacks on other victims, the gang has used Emotet as the bot and Trickbot as the intel- and credential-stealer in advance of dropping Ryuk and locking down the victims' machines.

"What was happening behind the scenes was that Trickbot got in and set up the whole command-and-control thing, and we later found out what was actually going on. They siphoned off credentials, set up the C2, and then we got hit with the big one," the Ryuk ransomware, Larrue explains.

While he and his team were "chasing our tails" trying to quell the infection's spread, the attackers had set up a reverse-shell attack, he says, possibly exploiting an unpatched vulnerability in Java. The company's Vipre anti-malware tools didn't recognize or catch the variant.

With the stolen credentials, the Ryuk attackers then set up Remote Desktop Protocol (RDP) connections to the network and, via the PowerShell commands, set off the Ryuk ransomware payload, server by server, he says.

But what Larrue and his team didn't realize at the time was that unplugging machines from the network actually exacerbated the attack: The Ryuk attackers apparently had set the attack to corrupt the firmware of the infected machines if the ransomware's encryption process was disrupted. Larrue and his team of three IT staffers had not seen the ransom note warning them not to shut down or risk their systems getting corrupted when they frantically did the shutdown; they finally got a look at the message in the wake of the response.

"They were expecting us to come in Monday morning [to the ransom message]," he says. "They didn't expect us on Sunday."

Unplugging the machines "was a mistake on my part," Larrue adds. "Part of the encryption scheme ... was if we did pull the plug, something would corrupt the firmware on all the servers," including the manufacturing firm's email and ERP servers.

"At that point it was totally lost. Even if we wanted to pay ransom, we couldn't," he recalls.

It turned out the ransom note had warned that only the attackers could help decrypt the files, and that resetting or shutting down systems could damage the files. It didn't include a ransom fee, but instead instructions on how to proceed in working with the attackers to get the files decrypted.

"I've had bad days in my life, but I've never had one like that," Larrue says. "I had the weight of the world bearing down on me."

Paper and Pen

C.E. Niehoff is a relatively small, privately held manufacturing firm, with 400 employees and a three-person IT department that also works on security issues. Its customers include the US military, which uses its industrial alternators for vehicles, for instance. One of the first worries in the wake of the attack was the loss of its ERP manufacturing server to the Ryuk attack.

The good news was the attackers hadn't stolen any customer or sensitive information, but the bad news was the manufacturing process had to rely on paper and existing orders to keep the shop floor open. "We had enough paperwork to keep the manufacturing floor running on jobs already issued," Larrue says. "The ERP system provides information to execute on the shop floor, but we can still produce without it. Production didn't come to a grinding halt."

But "we couldn't see too far into the future" until the ERP system was back online, he recalls.

By some stroke of luck, the company's human resources and payroll server wasn't infected with ransomware. Neither was its two backup appliances, although there were signs the attackers had tried to encrypt the Arcserve 8200 Series devices but had failed for some unknown reason. One appliance sat in Building A, and the other in Building B, on the campus, and were set to run a data backup rotation and handle file compression for terabytes of the firm's data.

"So this was more or less all we had," as well as some older backup tapes that only contained data for the past four years, Larrue says.

And C.E. Niehoff had not actually set up the appliances for full system recovery yet — the devices were relatively new — so Larrue had to get help from an Arcserve engineer/technician to restore the backups to the new computers, which the manufacturing firm had to quickly purchase to replace the compromised systems. A couple of the systems that had been configured for bare-metal restoration were back online quickly, he recalls, but there were challenges with several other systems that had not been configured for full restoration.

"We had to more or less rebuild the machine," which took longer to restore, he says.

One way to keep backup systems safe from ransomware attacks is to keep them on a separate domain, advises Gary Sussman, the Arcserve engineer who helped Larrue restore the manufacturing company's systems. He also recommends setting them with strong credentials and ensuring that hardware encryption "is turned on."

In all, it took C.E. Niehoff two-and-half weeks to get all of its systems fully back up and running, starting with its email server.

Larrue says the company since has added additional layers of security and is working on beefing up redundancy in its systems and storage, including some cloud-based storage. Ransomware threats are the new normal.

"The lessons learned here is this is an ongoing campaign and it's not going to stop," he says of the threat of ransomware attacks.

Related Content:

About the Author

Editor-in-Chief, Dark Reading

Kelly Jackson Higgins is the Editor-in-Chief of Dark Reading and VP, cybersecurity editorial at Informa TechTarget, where she leads editorial strategy for the company's three cybersecurity media brands: Dark Reading, SearchSecurity and Cybersecurity Dive. She is an award-winning veteran technology and business journalist with three decades of experience in reporting and editing for various technology and business publications and major media properties. Jackson Higgins was selected three consecutive times as one of the Top 10 Cybersecurity Journalists in the U.S., and was named as one of Folio's 2019 Top Women in Media. She has been with Dark Reading since its launch in 2006.
