Manufacturer Stops Breach Cold, Thanks to CRITICALSTART Incident Response Services

CASE STUDY

AT A GLANCE

- Major International Manufacturing Organization
- 20 Offices Worldwide
- Shifted 85-90% of Its Office Staff to Remote Work
- Several Acquired Companies Not Yet Unified Under One Security Umbrella

CORE AGENDAS

- Contain
- Remediate
- Monitor

CRITICALSTART

They're good. We're better.

A major international manufacturing organization with over 20 offices worldwide places a premium on delivering on the promise of its brand.

Manufacturer Profile

Due to the sensitive nature of this account, this customer's name is redacted for security.

When the COVID-19 pandemic began, this company kept its distribution center in operation but shifted 85-90% of its office staff to remote work to ensure product continued to reach customers and exceed their expectations. This move to remote work brought with it a new set of challenges.

"I think COVID opened the door for opportunities to the hacking world," explained the manufacturer's North American IT director. "Businesses were not prepared to do a full shutdown, and the move to utilizing remote home equipment resulted in so many configuration issues, such as the ability to have enough VPN tokens for every endpoint. Another issue I noticed when I first joined the company was that security was managed individually by each division, with each doing whatever they felt was best. To address this, I started putting together a roadmap to unify our team and our security environment, but that's when it happened."

This business had acquisitions that were not yet unified under their security umbrella. A ransomware attack started at one of these divisions and began to spread across the organization, including databases, VMware, and file servers. This set off alarm bells throughout the company as a competitor was recently shut down for a week due to an attack, and this manufacturer had end-of-month targets approaching. This IT director knew finding someone to help with the incident response might be a problem, as many IR firms would require volumes of information up front before being willing to make a commitment. Fortunately, one of the company's vendors recommended CRITICAL**START** to help the company respond to this attack in the quickest manner possible.

Always Ready

“We got in touch with CRITICALSTART late on a Friday night,” the IT director shared. “It was kind of an interesting way to start a partnership. There was no time to get to know each other, do formal introductions or go through a presentation deck. This was, ‘We’re going to push you into the deep end of the pool and see if you can swim.’ We signed the contract around one in the morning.”

At this point, the story is picked up by Allyn Lynd, CRITICAL**START** Senior Digital Forensics & Incident Response (DFIR) Manager. “One of our channel partners asked us to jump on a call late on Friday night,” he shared. “They talked us through what they had seen and provided us with a file extension for the malware. We deployed Carbon Black Response and Cylance Protect to their environment and worked with some open-source methods, and within less than an hour, we identified and confirmed the ransomware file. We were then able to identify scripts, PowerShell, and other tools that had to run in order to execute that file. At that point we had a good level set of indicators of compromise (IoCs) to actually run it. We isolated and blacklisted the machines with the malware files, and they were able to bring their system back up and online.”

The IT director for this manufacturer outlined what it was like to work with a brand-new partner on an issue of such critical importance to his organization with zero time to prepare in advance. “They hit the ground running,” he declared. “They determined the exact extent of the infection and which systems were infected. They became an extension of my team where we just went back and forth sharing information. Normally, with an event like this, you’re talking days, if not weeks of downtime. In our case, the initial word on the breach went down on a Friday afternoon, **and we were back up and shipping product by Monday around lunch.”**

“This was a monumental task,” he added. “We were very fortunate that our backups were not compromised. But you can restore all day long, and it won’t help you if you do not find the source. Working with CRITICAL**START**, we were able to remove the malware behind the attack instead of just trying to mitigate the consequences.”

Ransomware as a Service

While it’s difficult to confirm in this case, CRITICAL**START** has been identifying a phenomenon in ransomware that we’ve termed Ransomware as a Service. Affiliate attackers do not have the expertise to develop their own sophisticated malware. They instead acquire malware from a third party (possibly with the agreement to pay a portion of the ransom back to this individual or group) and customize it to suit their own purposes.

> “We’re going to push you into the deep end of the pool and see if you can swim. We signed the contract around one in the morning.”

Next steps

"We went live on Monday, which was priority one, but the engagement did not end there," the IT director stated. "For the better part of three months, the CRITICAL**START** team kept up the same level of effort. They were not only monitoring all our systems and all our networks; they were also monitoring our New Jersey servers because we saw the virus hop over to New Jersey, and they were advising us on what to do."

The CRITICAL**START** IR team continued to contain and remediate the ransomware from several U.S.-based subsidiaries and advise the manufacturer on actions that needed to be taken. The team also helped the company rebuild its active directories and started a forensic analysis to determine the attack vectors. The analysis included areas such as backup servers, file servers, and domain controllers. The team also performed a network log analysis, including areas such as the firewall and web proxy, and a VPN and email analysis .

The next phase included recommendations on new preventive security measures to take in the future. This includes multi-factor authentication, deploying Microsoft 365 Defender, phishing training for employees, increasing maintenance of firewall logs from 30 to 60 days, maintaining of web proxy logs as a regular process, and adding privileged account management for domain admin accounts.

But to the IT director, there was one primary advantage: "I think the number one point is having everybody under the same security coverage," he said. "From a software and vendor perspective, you gain visibility from one team that sees the entire picture, and they're able to connect the dots in a much more efficient manner than if you have multiple vendors. It's the number one reason why you want to keep everything under one umbrella."

"I think I see myself as a straight shooter," he added. "Give me the facts, and don't sugar coat anything. And I think that's the team I partnered with in CRITICAL**START.** If something is wrong in my environment, I need to know, and these guys are exactly what I need to ensure I have that visibility. I think that level of partnership is typically hard to come by. These guys get directly to the point and take action, and that's the best type of relationship from my perspective."

Effective security with a new partner or acquisition

The IT director for this manufacturer considers it critical to fully understand the level of input protection of anyone joining a parent company network. He provided some questions to consider asking when evaluating the security of a new entity that is going to be joining your own environment:

- ✓ How often do you scan for viruses and malware?
- ✓ Do you have a dedicated security team?
- ✓ Is this team in-house or outsourced?
- ✓ Are your operating systems end-of-life or no longer supported?

He believes these answers are essential before you even consider building a VPN tunnel between two entities. Once vulnerabilities are identified, then you need to get permissions in place to address issues or at least only connect to the segments that are secure.