Defense contractor CPI knocked offline by ransomware attack

techcrunch.com/2020/03/05/cpi-ransomware-defense-contractor/

Zack Whittaker

Zack Whittaker @zackwhittaker / 2 years

A major electronics manufacturer for defense and communications markets was knocked offline after a ransomware attack, TechCrunch has learned.

A source with knowledge of the incident told TechCrunch that the defense contractor paid a ransom of about $500,000 shortly after the incident in mid-January, but that the company was not yet fully operational.

California-based Communications & Power Industries (CPI) makes components for military devices and equipment, like radar, missile seekers and electronic warfare technology. The company counts the U.S. Department of Defense and its advanced research unit DARPA as customers.

The company confirmed the ransomware attack.

“We are working with a third-party forensic investigation firm to investigate the incident. The investigation is ongoing,” said CPI spokesperson Amanda Mogin. “We have worked with counsel to notify law enforcement and governmental authorities, as well as customers, in a

timely manner."

According to the source, a "domain admin" — a user with the highest level of privileges on the network — clicked on a malicious link while they were logged in, which triggered the file-encrypting malware. Because the thousands of computers on the network were on the same, unsegmented domain, the ransomware quickly spread to every CPI office, including its on-site backups, the source said.

The source described the company in "panic mode," as only about one-quarter of its computers are back up and running as of the end of February.

Short staffing is hampering the effort, the source said. Some computers containing sensitive military data have been recovered using the decryption key, which the company obtained by paying the ransom. One system is said to have files related to Aegis, a naval weapons system developed by Lockheed Martin.

"We are aware of the situation with CPI and are following our standard response process for potential cyber incidents related to our supply chain," said a Lockheed spokesperson.

Many of the remaining computers are having their operating systems installed from scratch, the source said. A portion of the defense contractor's systems — about 150 computers — are still running Windows XP, which stopped receiving security patches in 2014.

But it's not known what kind of ransomware was used in the attack. CPI's spokesperson did not answer any of our questions, and declined to comment further beyond the brief statement.

CPI becomes the latest victim in a spate of attacks targeting large companies in the past month. This week alone saw legal services giant Epiq Global knocked offline by a ransomware attack, and Visser, a parts manufacturer for Tesla and SpaceX, was hit by a new kind of data-stealing ransomware, dubbed DoppelPaymer, which not only encrypts files but first exfiltrates company data to the hackers' servers.

The hackers behind the DoppelPaymer attack began publishing Visser's internal files last week after the company did not pay the ransom.

Brett Callow, a threat analyst at security firm Emsisoft, said the tactics of traditional file-encrypting ransomware have changed.

"These incidents should be considered to be breaches — and disclosed and reported as such — from the get-go," said Callow. "Criminals are getting too much time to misuse data while companies/people have no reason to be suspicious."

> As ransomware gets craftier, companies must start thinking creatively