Visser, a parts manufacturer for Tesla and SpaceX, confirms data breach

techcrunch.com/2020/03/01/visser-breach/

Zack Whittaker, Kirsten Korosec

A precision parts maker for space and defense contractors has confirmed a “cybersecurity incident,” which TechCrunch has learned was likely caused by ransomware.

Visser Precision, a Denver, Colorado-based manufacturer, makes custom parts for a number of industries, including automotive and aeronautics. In a brief statement, the company confirmed it was “the recent target of a criminal cybersecurity incident, including access to or theft of data.”

The company said it “continues its comprehensive investigation of the attack, and business is operating normally,” a spokesperson told TechCrunch.

Security researchers say the attack was caused by the DoppelPaymer ransomware, a new kind of file-encrypting malware which first exfiltrates the company’s data. The ransomware threatens to publish the stolen files if the ransom is not paid.

DoppelPaymer is the latest in an emerging list of data-stealing ransomware. In December, security staffing firm Allied Universal was one of the first companies that had sensitive employee and business data published after the company declined to pay a $2.3 million

ransom for the data.

Brett Callow, a threat analyst at security firm Emsisoft, first alerted TechCrunch to the website that was publishing files stolen by the DoppelPaymer ransomware.

The website contains a list of files stolen from Visser, including folders with customer names — including Tesla, SpaceX, and aircraft maker Boeing, and defense contractor Lockheed Martin. A portion of the files were made available for download. (We are not linking to the ransomware's website.) The documents included non-disclosure agreements between Visser and both Tesla and SpaceX. Another file appeared to be a partial schematic for a missile antenna was marked as containing "Lockheed Martin proprietary information."

Spokespeople for Tesla, SpaceX, and Boeing and did not immediately comment outside business hours.

A Lockheed Martin spokesperson said the company is "aware of the situation with Visser Precision and are following our standard response process for potential cyber incidents related to our supply chain."

The DoppelPaymer ransomware has been active since mid-last year, and its victims have included the Chilean government and Pemex, Mexico's state-owned petroleum company. But unlike the Maze ransomware, from which DoppelPaymer derives much of its data-stealing inspiration, the ransom note does not say that data has been stolen. Instead, it's only disclosed if the company goes to the ransomware's website to pay.

"Some companies may not even realize that their data has been exfiltrated prior to it being published," said Callow.

The website hosting the stolen files said there was a "lot" more files to be published.

"Data theft is a strategy that multiple groups have now adopted and, consequently, ransomware incidents should be treated as data breaches until it can be established they are not," said Callow.

Updated with Lockheed comment.

> As ransomware gets craftier, companies must start thinking creatively