Ransomware scumbags leak Boeing, Lockheed Martin, SpaceX documents after contractor refuses to pay

By Shaun Nichols and Gareth Corfield

Published: 2020-04-10 · Archived: 2026-04-06 00:24:54 UTC

Internal confidential documents belonging to some of the largest aerospace companies in the world have been stolen from an industrial contractor and leaked online.

The data was pilfered and dumped on the internet by the criminals behind the DoppelPaymer Windows ransomware, in retaliation for an unpaid extortion demand. The sensitive documents include details of Lockheed-Martin-designed military equipment – such as the specifications for an antenna in an anti-mortar defense system – according to a *Register* source who alerted us to the blueprints.

Other documents in the cache include billing and payment forms, supplier information, data analysis reports, and legal paperwork. There are also documents outlining SpaceX's manufacturing partner program.

The files were siphoned from Visser Precision by the DoppelPaymer crew, which infected the contractor's PCs and scrambled its files. When the company failed to pay the ransom by their March deadline, the gang – which tends to demand hundreds of thousands to millions of dollars to restore encrypted files – uploaded a selection of the documents to a website that remains online and publicly accessible.

Visser is a manufacturing and design contractor in the US whose clients are said to include aerospace, automotive, and industrial manufacturing outfits – think Lockheed Martin, SpaceX, Tesla, Boeing, Honeywell, Blue Origin, Sikorsky, Joe Gibbs Racing, the University of Colorado, the Cardiff School of Engineering, and others. The leaked files relate to these customers, in particular Tesla, Lockheed Martin, Boeing, and SpaceX.

When asked about the dump, a Lockheed Martin spokesperson told us: "We are aware of the situation with Visser Precision and are following our standard response process for potential cyber incidents related to our supply chain.

"Lockheed Martin has made and continues to make significant investments in cybersecurity, and uses industry-leading information security practices to protect sensitive information. This includes providing guidance to our suppliers, when appropriate, to assist them in enhancing their cybersecurity posture."

Visser Precision did not respond to a request for comment on the leak. Tesla, SpaceX, and Boeing did not respond either.

This is not the first time the DoppelPaymer crew has publicly shared stolen confidential data after a victim failed to pay the ransom demands. In fact, the crooks have a regularly updated website full of internal documents belonging to organizations that didn't cough up, though admittedly most are significantly less interesting than the Visser Precision cache.

The dumps are intended to scare others who are infected with the ransomware into paying the group's demands. *The Register* will not be linking to the site.

For what it's worth, the DoppelPaymer gang vowed to lay off attacking hospitals during the coronavirus pandemic. Whether or not this promise was honored is another question.

While law enforcement agencies and security experts uniformly agree that paying a ransom demand is a bad idea and poor substitute for keeping offline backups and properly securing data, some experts have conceded that, when it's your corporate data on the line, caving in and paying up can be an option. ®
