Clop ransomware gang leaks online what looks like stolen Bombardier blueprints of GlobalEye radar snoop jet

By Gareth Corfield

Published: 2021-02-23 · Archived: 2026-04-05 22:27:24 UTC

The Clop ransomware gang claims to have stolen documents from aerospace giant Bombardier's defense division – and has leaked what appears to be a CAD drawing of one of its military aircraft products, raising fears over what else they've got.

Over on their Tor hidden service, the cyber-extortionists published what they said were screenshots of blueprints swiped from Bombardier as evidence of their crimes. The gang abused the same vulnerability in file-transfer software from Accellion that was exploited earlier this year to nab documents from Trump's lawyers.

Bombardier confirmed its security had been breached, putting out a public statement only minutes after *The Register* grilled the Canadian business jet maker on the Clop gang's claims. "An initial investigation revealed that an unauthorized party accessed and extracted data by exploiting a vulnerability affecting a third-party file-transfer application, which was running on purpose-built servers isolated from the main Bombardier IT network," the biz said.

Bombardier added it is working with "cybersecurity and forensic professionals," and insisted it "was not specifically targeted — the vulnerability impacted multiple organizations using the application." A spokeswoman confirmed the breach came about thanks to a hole in an Accellion file-transfer product.

Thus, Bombardier was among various corporations using Accellion's vulnerable file-transfer software, which were exploited to pilfer documents. A flaw in the application was revealed in December, and it appears criminals were quick to make hay before the world got round to patching their deployments.

Around 130 Bombardier employees in Costa Rica were "impacted" by the hack, we're told, suggesting their personal information was obtained or otherwise accessed by miscreants.

Radar antenna and military jet

Pictures dumped online by Clop, and seen by *The Register*, showed a CAD rendering of a Bombardier GlobalEye aircraft, a Global 6000 business jet converted to carry a distinctive Saab Erieye plank-style radar mounted on top of its fuselage. A second picture showed a detailed 3D view of what appeared to be a radar head complete with its mounting.

The screenshots also showed an email seemingly sent by an employee of Marshall Aerospace of Cambridge, UK, which has previously worked on military conversions of Global 6000s for various countries.

Experts, almost all of whom spoke to us on condition of anonymity because they were not authorized to speak publicly, drew different conclusions about the radar equipment in the picture leaked by Clop.

One, with extensive professional experience of airborne radars, suggested the hardware was a passive array antenna with beam-forming wave guides mounted behind it. Another suggested it was consistent with mechanically scanning radar heads mounted in aircraft, saying: “My first thought upon seeing it was that it reminded me of the old 1970s and 1980s vintage radar arrays in the F-15 Eagles.”

A third said: “I think I know; if so, it’s no comment, I’m afraid”.

Philip Ingram, a former British intelligence officer and now a security commentator, told *The Register*: “The aircraft looks like the GlobalEye,” adding: “It could be a Synthetic Aperture Radar image but neither picture would be sensitive in the detail – they look like they could be out of sales or pre-sales literature.”

The Global 6000 airframe used for the GlobalEye also forms the basis of the British Royal Air Force’s Sentinel airborne early-warning aircraft. In the orientation shown in the CAD image, the radar antennas could be the ones mounted in the Sentinel’s long ventral radome, pictures of which can be seen in this Royal Aeronautical Society feature about the aircraft.

> It’s more likely that the actor responsible for the file-transfer application hacks has delegated the extortion to Clop

Clop has made a habit of targeting high-profile companies for its ransomware extortion activities, which consist of infiltrating a businesses' networks, exfiltrating and encrypting files, and then demanding payment to not only decrypt and restore the scrambled data but also to not publicly release the sensitive purloined materials.

Brett Callow of infosec firm Emsisoft told *The Register* that while Clop is bragging about the intrusion, it may not have been the ransomware gang itself that broke into the corporations.

“It’s more likely that the actor responsible for the file-transfer application (FTA) hacks has delegated the extortion to Clop, as they have the necessary infrastructure and expertise,” he said. “Other organizations which have disclosed FTA breaches include the Reserve Bank of New Zealand, the Australian Securities and Investments Commission, and Colorado University – and it’s not at all unlikely that Clop has those organizations’ data, too.”

Clop also last year hit Software AG. What’s the lesson here? Patch your IT estate promptly and watch out for third-party suppliers. ®
