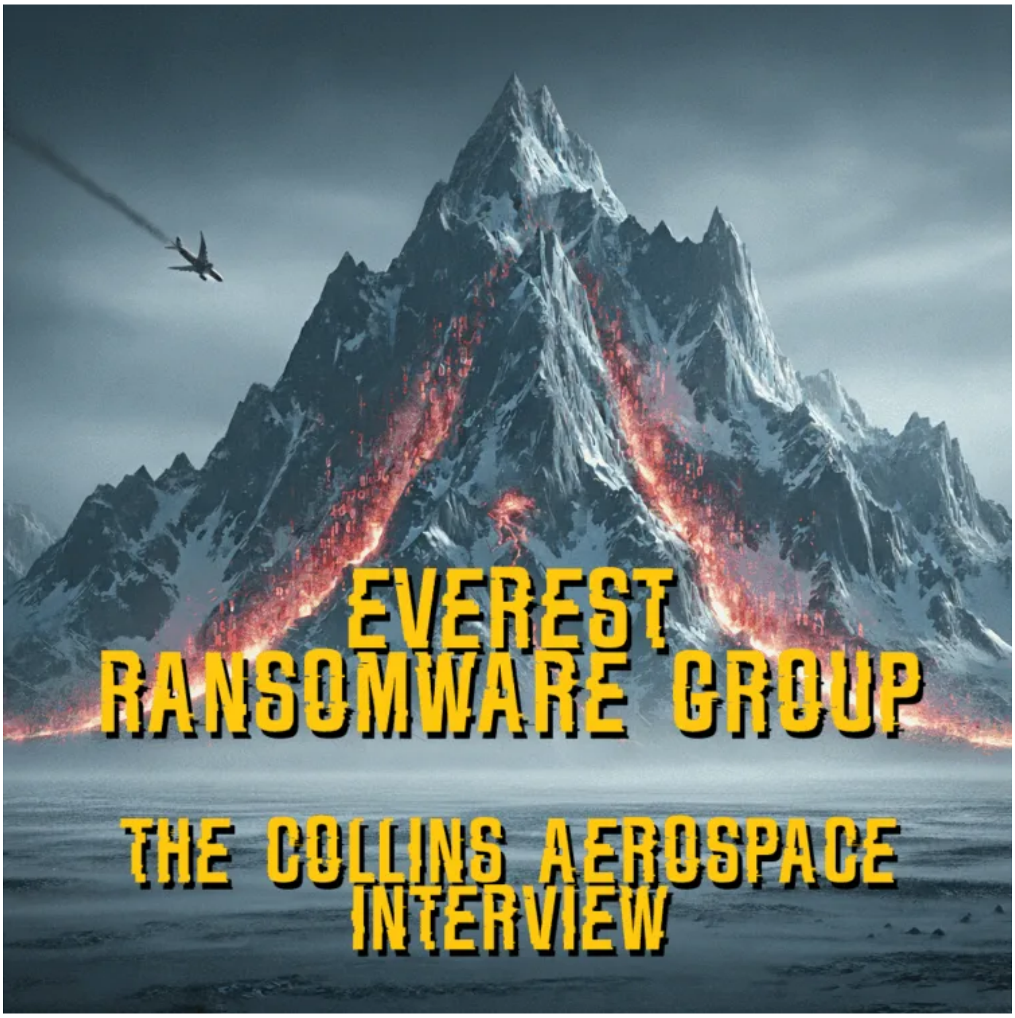
Exclusive: Everest Ransomware Group Interview on Collins Aerospace Breach

November 6, 2025



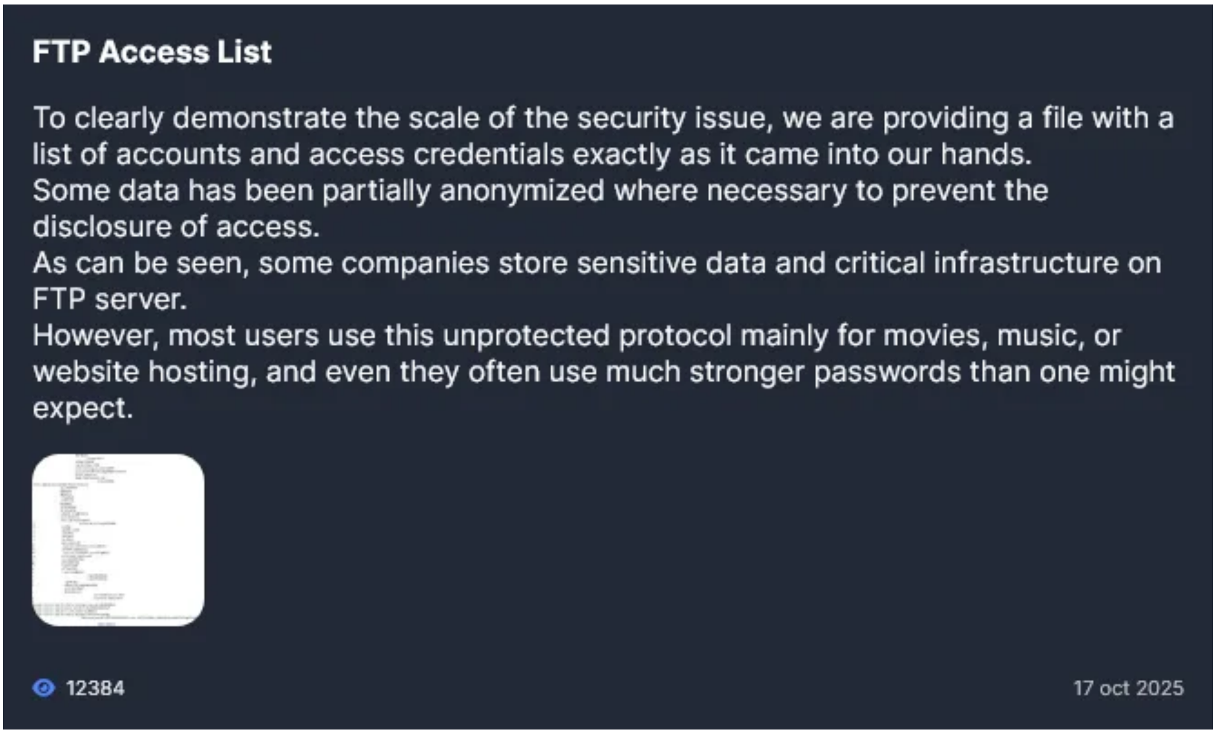
In late September 2025, a crippling cyber event brought European aviation to a standstill. Major airports, including London Heathrow, Brussels, and Berlin, were plunged into chaos as passenger processing systems were taken offline. The disruption centered on the **MUSE** (Multi-User System Environment) software, a critical platform from defense and aerospace giant **Collins Aerospace** (an RTX subsidiary) that manages check-in, boarding, and baggage.

The official story, confirmed by the European Union Agency for Cybersecurity (ENISA) and an SEC filing from Collins' parent company, RTX, was that this shutdown, which began on September 19, was caused by a "cybersecurity **incident involving ransomware** on systems that support its Multi-User System Environment ("MUSE") passenger processing software.". Some security researchers subsequently linked the attack to **HardBit ransomware**.

However, in the days following the shutdown, the cybercrime organization **Everest Ransomware Group** claimed responsibility for the initial breach. This group is known for operating as an **"encryption-less"** ransomware organization, which means they do not encrypt victim data but instead specialize in data exfiltration for the purpose of extortion.

Everest claims they first gained access on **September 10**. The entry point wasn't a new, sophisticated exploit. Instead, they allegedly used a set of **leaked credentials.** This username and password pair was reportedly stolen from an employee's computer by an infostealer (RedLine) back in **2022** and was never changed. The credentials for the public-facing **FTP server** were:

- **Server:** ftp.arinc.com:22
- **User:** aiscustomer
- **Password:** muse-insecure



FTP Access List

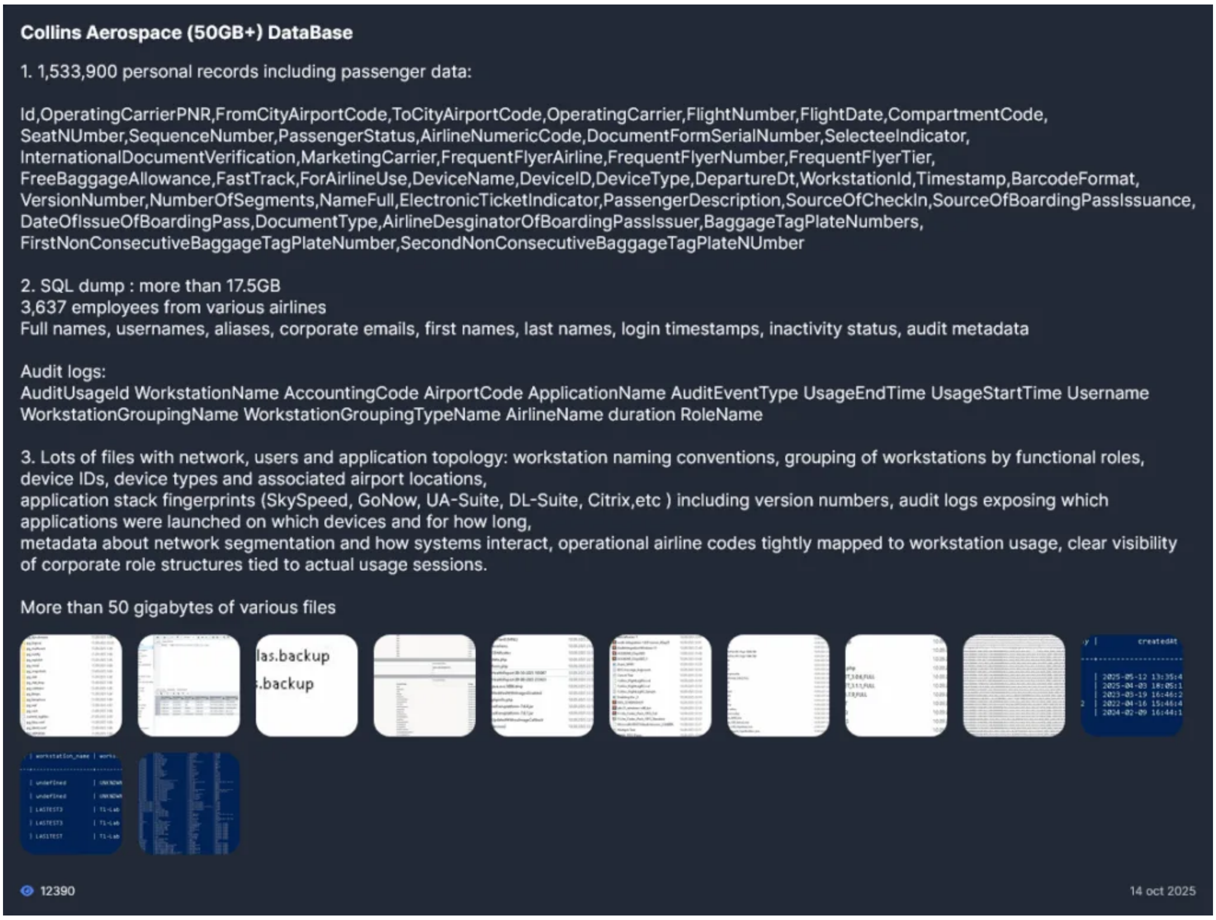
To clearly demonstrate the scale of the security issue, we are providing a file with a list of accounts and access credentials exactly as it came into our hands.
Some data has been partially anonymized where necessary to prevent the disclosure of access.
As can be seen, some companies store sensitive data and critical infrastructure on FTP server.
However, most users use this unprotected protocol mainly for movies, music, or website hosting, and even they often use much stronger passwords than one might expect.

12384

17 oct 2025

From this access, Everest claims to have exfiltrated over 50GB of data, including:

- **1,533,900 personal records** of passengers, including PNRs, flight details, and frequent flyer numbers.
- A **17.5GB SQL dump** containing details on **3,637 employees** from various airlines, including full names, corporate emails, and aliases.
- Extensive files on **network, user, and application topology**, including workstation naming conventions, device IDs, and application stack fingerprints (SkySpeed, GoNow, etc.).



Collins Aerospace (50GB+) DataBase

1. 1,533,900 personal records including passenger data:

Id,OperatingCarrierPNR,FromCityAirportCode,ToCityAirportCode,OperatingCarrier,FlightNumber,FlightDate,CompartmentCode,SeatNUmber,SequenceNumber,PassengerStatus,AirlineNumericCode,DocumentFormSerialNumber,SelecteeIndicator,InternationalDocumentVerification,MarketingCarrier,FrequentFlyerAirline,FrequentFlyerNumber,FrequentFlyerTier,FreeBaggageAllowance,FastTrack,ForAirlineUse,DeviceName,DeviceID,DeviceType,DepartureDt,WorkstationId,Timestamp,BarcodeFormat,VersionNumber,NumberOfSegments,NameFull,ElectronicTicketIndicator,PassengerDescription,SourceOfCheckIn,SourceOfBoardingPassIssuance,DateOfIssueOfBoardingPass,DocumentType,AirlineDesginatorOfBoardingPassIssuer,BaggageTagPlateNumbers,FirstNonConsecutiveBaggageTagPlateNumber,SecondNonConsecutiveBaggageTagPlateNUmber

2. SQL dump : more than 17.5GB
3,637 employees from various airlines
Full names, usernames, aliases, corporate emails, first names, last names, login timestamps, inactivity status, audit metadata

Audit logs:
AuditUsageId WorkstationName AccountingCode AirportCode ApplicationName AuditEventType UsageEndTime UsageStartTime Username WorkstationGroupingName WorkstationGroupingTypeName AirlineName duration RoleName

3. Lots of files with network, users and application topology: workstation naming conventions, grouping of workstations by functional roles, device IDs, device types and associated airport locations,
application stack fingerprints (SkySpeed, GoNow, UA-Suite, DL-Suite, Citrix,etc) including version numbers, audit logs exposing which applications were launched on which devices and for how long,
metadata about network segmentation and how systems interact, operational airline codes tightly mapped to workstation usage, clear visibility of corporate role structures tied to actual usage sessions.

More than 50 gigabytes of various files

12390

14 oct 2025

They then entered into negotiations with an RTX representative on September 16.
Here is the central conflict: **Everest** explicitly denies any involvement with ransomware. Instead, they allege that **Collins Aerospace**, already aware of Everest's data theft, ***intentionally* shut down its own servers** on September 19 and publicly blamed "unspecified ransomware" in a coordinated effort **to commit insurance fraud**.
This complex and contradictory scenario is further complicated by the UK's National Crime Agency, which arrested a suspect in connection with the attack on September 24, though their affiliation remains unconfirmed. Meanwhile, Everest continued its operations, claiming new breaches on October 25 at **Dublin Airport** and **Air Arabia**.
In light of these reports and the threat actor's public claims, we initiated contact with the Everest Ransomware Group via an email address listed on their darknet website. We sent a list of 12 questions to get their official statement on the record, seeking to

clarify their role, their alleged connection to HardBit, and the basis for their fraud allegations.

The group responded to our questions. We are publishing the interview in full to provide transparency and allow our readers to see the threat actor's claims in their entirety, which can then be compared against the official statements and public evidence.

Q-1: To begin, could you provide an overview of the Everest group? What do you consider to be your group's core mission?
– Everest: *"Everest is a small group of IT specialists who study how large infrastructures manage their digital security. When companies handling critical data are careless, we draw attention to it. We focus on documents: analyzing files,logs, messages, email and other internal information helps show the real picture, not just the company's words. We search for proof of mismanagement and wrongdoing that companies often try to cover up behind official statements. We do not use ransomware, we do not damage infrastructure, and we do not block systems. Our work involves analyzing, finding valuable documents, and publishing facts that companies usually try to hide"*

Q-2: Are your operations purely financially driven, or are there geopolitical factors that influence your choice of targets? Can you clarify if Everest operates as a fully independent entity, or if you maintain affiliations with other groups or any state-level actors?
– Everest: *"Everest is a commercial organization, and we don't hide that. We earn money for our work, just like any professional who spends time, resources, and knowledge on their job. The financial part is needed to cover expenses, infrastructure, and risks. But money is not our only motivation. We work independently, without support or influence from governments or other groups. When we see systemic incompetence, carelessness, or*

outdated decisions that put millions of users at risk, we take action. First comes the business side, but behind it is a principle: we don't ignore negligence that affects people's safety. The situation with Collins Aerospace is not unique. Similar incidents happen regularly, and the reason is usually the same: careless management of infrastructure. The problem is not just this specific incident, but the overall approach to security, a culture that focuses on metrics rather than real protection of data."

Q-3: Was Collins Aerospace or its parent, RTX, a specific target for your group, or was this discovery opportunistic?
– Everest: *"The access to the FTP server came to us by chance. Seeing a major aerospace company storing operational data with such a weak password, which according to some researchers had already leaked online in 2022, was shocking. After that, our interest shifted from just technical to public. How can a company responsible for the safety of millions of passengers allow this kind of negligence?"*

Q-4: Since the Collins Aerospace incident, you have also claimed breaches at Air Arabia and Dublin Airport. Is the aerospace and aviation sector a new strategic focus for your group, and if so, why?
– Everest: *"No, aviation is not our main focus. The reason we highlight these cases is simple. In aviation, the results of carelessness are obvious right away. Thousands of flights are delayed and millions of passengers are affected. We point out these incidents because a single vulnerable server or a small configuration mistake can paralyze an entire transport system. It is not about choosing a target. It is about showing where the cost of negligence is most visible."*

Q-5: Public reports attribute the airport disruptions to HardBit ransomware, yet your group explicitly denies using ransomware. Investigations connect both of your names, Everest and HardBit, to the Collins Aerospace incident. Can you

clarify this discrepancy? As a known Initial Access Broker, did you sell network access to a HardBit affiliate after your initial breach, or do you claim these were two entirely separate attacks?
– Everest: *"We did not use any ransomware and no encryption took place. The link between Everest and HardBit might be someone's mistake or a deliberate false report in the media. We did not sell or give anyone access to encrypt the systems. Our correspondence with Collins did not mention encryption at all. It was only about various operational details."*

Q-6: A suspect was arrested in the U.K. in connection with the Collins Aerospace attack. Can you confirm if this individual was affiliated with your group or your operational partners?
– Everest: *"We have nothing to do with him. People often get arrested just for being loosely connected to leak sites or maybe being part of a chain of compromised proxy servers."*

Q-7: What criteria do you use to decide whether to exploit a breach yourselves, as you claim you did with Collins Aerospace, versus selling the access to a third party?
– Everest: *"We haven't practiced that in many years and don't plan to"*

Q-8: Your site featured a password-protected "News For CEO" section related to this incident. What specific information did you provide in that section, and what were the full negotiation terms and final requested financial amount?
– Everest: *"This section was intended solely for the company's leadership and will not be disclosed. We will keep the amount private. The main goal of the publication was to get acknowledgment of the incident and responsibility for it, without trying to hide what happened behind the loud label 'ransomware'."*

Q-9: Regarding your public claim that Collins Aerospace was motivated by insurance fraud, what evidence or observations led you to this specific conclusion?

– Everest: *"This is based on the timeline of events. They were aware of the issue for eight days before shutting down the servers. We are not stating it as a fact, but their behavior and timing look too coordinated to be a coincidence. The term "ransomware" says it all. It's the easiest way to blame a virus and do whatever they wanted. Replacing old systems during such a big incident also let them get an insurance payout. They didn't have to warn millions of people that moving to new systems would be slow, difficult, and expensive. This situation worked in their favor, avoiding millions in losses and lawsuits. Since they didn't pay us, they now face potential class-action claims from millions of people. Insurance for a ransomware event must pay, while simply shutting down servers without a reason would not have triggered a payout. They set it up to benefit themselves. We don't use ransomware, and everyone knows it. RTX made a big mistake by not checking this more carefully and probably didn't expect us to make this public or show the correspondence."*

Q-10: We've observed several public events related to your infrastructure, including intermittent downtime after both the Collins and Colonial Pipeline claims, as well as a public defacement in April 2025. Could you comment on these operational challenges?

– Everest: *"Most of the time these were DDoS attacks. We are prepared for that. The main thing is that the information we publish cannot be destroyed, even if the servers are shut down It stays online. After the April events, we updated the site and infrastructure, and it did not affect us at all"*

Q-11: Why have you chosen to speak with the media about this attack? What message are you trying to send to the cybersecurity community, the public, and

potential victims with the interview?
– Everest: *“Staying silent only helps those who are trying to hide their mistakes. We show how systemic negligence affects real people’s lives. The Collins Aerospace case clearly demonstrates how closedness and careless security can lead to complete chaos”*

Q-12: Finally, your group’s tactics have visibly shifted from deploying ransomware to primarily operating as an Initial Access Broker. What drove this strategic pivot, and what is Everest’s long-term plan?
– Everest: *“I won’t repeat myself, the answer has already been given above. Thank you for the interview”*

Thanks to our partner Daily Darkweb