NCA Arrest Man as HardBit Ransomware Blamed for Airport Outages - Aga

Data: 2025-09-26 00:55:13

Autor: Inteligência Against Invaders

British investigators have arrested a man in connection with a suspected ransomware attack which

continues to cause flight delays across Europe.

The UK's National Crime Agency (NCA) revealed the news in a brief statement issued yesterday afternoon.

"NCA officers, supported by the South East ROCU, arrested a man in his forties in West Sussex yesterday evening on suspicion of Computer Misuse Act offences. He has been released on conditional bail," the statement read.

NCA deputy director, Paul Foster, head of the agency's National Cyber Crime Unit, said the investigation was still in its early stages.

"Cybercrime is a persistent global threat that continues to cause significant disruption to the UK. Alongside our partners here and overseas, the NCA is committed to reducing that threat in order to protect the British public," he added.

Read more on the Collins Aerospace attack: Airport Chaos Enters Third Day After Supply Chain Attack.

Separately, security experts linked the cyber-attack on US firm Collins Aerospace, which has led to the flight disruptions,to the HardBit ransomware variant.

Noted cybersecurity researcher Kevin Beaumont revealed the news on his Mastodon account, without sources, claiming that the variant "doesn't have a portal and is incredibly basic."

Airports began reporting problems on the evening of September 19, with hundreds of flights delayed and cancelled over the Saturday and Sunday. The problem was traced back to the ARINC vMUSE (Multi-User System Environment) software used by several airlines at multiple airports to share check-in desks and boarding gates.

The developer of that software, US firm Collins Aerospace, released an SEC filing confirming ransomware on "systems that support" MUSE.

"The MUSE airport systems operate outside of the RTX enterprise network, residing on customer-specific networks," it added. RTX is the aerospace and defense giant that owns Collins.

“Upon detecting the incident, the company activated its incident response plan and promptly took steps to assess, contain, respond to and remediate the incident.”

Incident Response Hits Problems

However, those steps appear not to be going to plan.

“They’ve had to restart recovery again as the devices keep getting reinfected. I’ve never seen an incident like it. Somebody like the NCSC needs to go in and help them with IR,” wrote Beaumont. “The payloads used in this one are detected by free Defender AV with decade-old static AV detections. This is not some cyber-mega attack by a ransomware group: it’s extremely poor security hygiene.”

In the meantime, airlines have been forced to use pen and paper to check in and board passengers, leading to continued delays at affected airports including Heathrow, Brussels and Berlin Brandenburg.

As of Thursday morning, most of those delay times appear to be falling. In Heathrow, 56% of planes departed late, with an average delay of just 17 minutes. In Berlin, the figures were72% and 28 minutes. In Brussels, delays are moving in the opposite direction, with 80% of departures late this morning, on average by 26 minutes.

EU security agency Enisa has blamed a third-party supplier breach for the ransomware incident, but has not provided more details.

“The company is diligently investigating the incident with the assistance of internal and external cybersecurity experts and has notified domestic and international law enforcement authorities and certain other government agencies,” the SEC filing concluded.