Federal Aviation Administration

INFORMATION NOTE

02 August 2024

Black Basta Ransomware Risk to the Aviation Sector

The Federal Aviation Administration (FAA) assesses Black Basta ransomware group's exploitation of a known critical vulnerability presents a significant risk to aviation critical infrastructure and civil aviation operations. The Black Basta ransomware group is suspected of exploiting CVE-2024-26169, a Windows privilege escalation vulnerability, as a zero-day vulnerability. In March 2024, Microsoft issued a patch for CVE-2024-26169; however, successful exploitation of CVE-2024-26169 could result in the compromise of critical aviation networks that support civil aviation operations. The interconnected nature of aviation systems potentially enables an attack on one component of aviation critical infrastructure to have cascading effects across the multiple systems that support civil aviation operations, including ticketing, ground services, and flight planning and scheduling.

- In May 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released a joint cybersecurity advisory to provide information on Black Basta ransomware operations affecting 12 of the 16 critical infrastructure sectors, including the aviation sector.[1] Black Basta affiliates have impacted a wide range of businesses and critical infrastructure in North America, Europe, and the Pacific. As of May 2024, Black Basta affiliates had impacted over 500 organizations globally.

- In January 2024, the Black Basta ransomware group claimed to have stolen data relating to customers, staff, human resources, and non-disclosure agreements (NDAs) from a commercial aircraft engine company.[2] Black Basta posted a sample of the stolen documents online, which included a screenshot and various human resources documents that revealed the personally identifiable information of what appears to be company staff across various divisions.

Owners and operators of aviation critical infrastructure are urged to apply security patches for CVE-2024-26169 immediately, implement advanced monitoring to identify and respond to any signs of compromise and update incident response plans to ensure preparedness for potential cyber incidents involving Black Basta or similar threats.

What is Black Basta?

Black Basta is a ransomware operator and ransomware-as-a-service (RaaS) criminal group that first emerged in early 2022 and immediately became one of the most active global RaaS threat actors.

During the period of April 2022 to May 2024, Black Basta compromised over 500 organizations in the U.S., Japan, Canada, the United Kingdom, Australia, and New Zealand in highly targeted attacks. The group's ransom tactics employ a double extortion tactic, encrypting their victim's critical data and vital servers and threatening to publish sensitive data on the group's public leak site.

Black Basta's ransomware group's core membership likely consist of former members from the defunct Conti threat actor group due to similarities in their approach to malware development, leak sites, and communications for negotiation, payment, and data recovery.

For additional information on the CISA Joint Cybersecurity Advisory on Black Basta Ransomware Activity, please visit https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

Contact Information

For any questions, please contact the FAA Threat Intelligence and Analysis Division:

- Aviation Technical Intelligence Team at: faa-cyber-intel@faa.gov

For any questions outside the regular working hours, please contact the FAA's Current Intelligence and Threat Evaluation (CITE) Watch at 202-267-3203 or FAA-Watch@faa.gov.

References available upon request.
