

AUTONOMOUS FLIGHT TECHNOLOGIES ADDRESSES 2023 BLACKCAT RANSOMWARE ATTACK FOLLOWING FEDERAL CONVICTIONS

Salem, Virginia - In November 2023, Autonomous Flight Technologies, Inc. was the victim of a targeted ransomware attack conducted using BlackCat, also known as ALPHV. The attack caused extensive disruption to AFT's technology infrastructure and inflicted significant operational, financial, and reputational harm on our company.

For nearly three years, AFT refrained from discussing the attack publicly out of respect for the federal investigation. The three individuals responsible have now been convicted and sentenced to federal prison. We can finally speak openly about what occurred.

This was not the work of ordinary opportunistic hackers. The perpetrators were cybersecurity professionals who held trusted management-level positions with cybersecurity firms specializing in ransomware negotiation and incident response. They worked for companies that organizations relied upon for protection and assistance during ransomware attacks while secretly participating in the very criminal conduct they were entrusted to combat.

AFT is sharing its experience first and foremost as a warning to other businesses: ransomware can happen to any organization, regardless of its size or industry. Companies must carefully evaluate not only their technology, but also the people and outside organizations entrusted with access to their systems. In this case, individuals operating within the cybersecurity industry became the bad actors.

AFT did not communicate or negotiate with the attackers. Contrary to multiple misleading news reports, AFT was never presented with a specific ransom amount, and we paid no ransom.

The attack compromised AFT's internal business systems and caused significant data loss. However, our most sensitive information was securely stored separately and remained protected. We also found no evidence that any client network, system, aircraft, or operational environment was affected.

Personal information belonging to AFT's founder and CEO did appear on the dark web. Based on AFT's recovery work and the information available through the federal investigation, we found no evidence that sensitive defense information or protected client information was sold, published, or misused.

AFT immediately began the difficult work of recovering and rebuilding. The attack compromised our company's systems, but it did not compromise our commitment to our clients, partners, or mission. AFT remained in business, continued supporting its customers, and emerged from the incident as a stronger and more security-conscious organization.

Protecting client and company information has always been a priority at AFT. Following the attack, we completely rebuilt our information technology environment from the ground up, reinforcing that longstanding commitment with advanced, enterprise-grade networking and security systems. The rebuilt environment provides substantially enhanced protection, monitoring, access control, backup, recovery, and cybersecurity compliance capabilities.

No organization can credibly promise that it will never face another attempted cyberattack. However, AFT is substantially more secure, resilient, and prepared today. Our clients can remain confident that protecting their information, operations, and trust remains our highest priority.

We extend our sincere gratitude to the Federal Bureau of Investigation's cyber investigators for their persistence, technical expertise, and exceptional work in identifying those responsible. We are equally grateful to the United States Department of Justice and its prosecutors for their dedication in building the case, securing the convictions, and ensuring that all three perpetrators received federal prison sentences. AFT also thanks Gentry Locke, our legal counsel, for representing and guiding the company throughout the investigation and legal process.

AFT has been a trusted American uncrewed-systems company since 2012. That trust remains central to who we are. We are still here, still serving our clients, and moving forward with stronger systems, greater resilience, and an even deeper commitment to protecting the work entrusted to us.

Joshua L. May
Founder and Chief Executive Officer
Autonomous Flight Technologies, Inc.
Salem, Virginia
www.autonomousflight.us