BlackCat Adds Indian Missile Fuel Maker to Its Victims List

By Jayant Chakravarti

Archived: 2026-04-05 13:00:56 UTC

Fraud Management & Cybercrime , Ransomware

Ransomware-as-a-Service Group Purports to Sell Indian Military Data on Dark Web (@JayJay_Tech) • February 2, 2023

BlackCat hackers say they stole sensitive data about the propellant in fuel used for Akash surface-to-air missiles, seen here at a parade in 2007. (Image: India Ministry of Defense)

An Indian rocket propellant manufacturer is facing the possibility of the BlackCat ransomware-as-a-service group leaking what it says is more than 2 terabytes of sensitive data.

See Also: AI Pushes Cyberattacks to New Speed Levels

BlackCat, also known as Alphv, says it stole from Solar Industries specifications for the propellant used in a slew of Indian military missile and rocket systems as well as warhead data and personal information pertaining to the company's employees and customers.

The ransomware group, suspected of being the successor to DarkSide and BlackMatter with ties to some former REvil members, says the data is for sale. Nagpur-based Solar Industries has not addressed the matter publicly. The company’s website has been offline for days now. Nagpur Today reported that senior officials from the ministries of defense and home affairs and intelligence agencies descended on the city and that the Central Bureau of Investigation is poised to investigate.

The stolen data also apparently includes security camera footage of Solar Industries' factory, audits and reports of flaws and vulnerabilities in the company's products and information about supply chain vendors.

The publicly traded company, founded in 1983 as a maker of mining explosives, has a 28% share of India's commercial and military explosives market, market analysis shows.

"BlackCat has one of the most sophisticated malware programs that can purportedly infect various Windows and Linux operating system versions," researchers from cybersecurity firm CloudSEK tell Information Security Media Group.

"It is customizable and heavily human-operated, which is especially important since it primarily targets large entities. The malware can employ four different encryption routines, use several cryptographic algorithms, proliferate via local networks - i.e., spread between computers, terminate virtual machines, etc.," they say.

Naavi Vijayashankar, chairman of the Foundation of Data Protection Professionals in India, tells ISMG that national authorities will almost certainly classify the hack as a "'cyber terrorist attack,' considering the sensitive nature of the activity of the company and the nature of data lost."

He adds that Solar Industries could face its own investigation. Existing Indian law requires the private sector company to have appropriate security measures in place.
