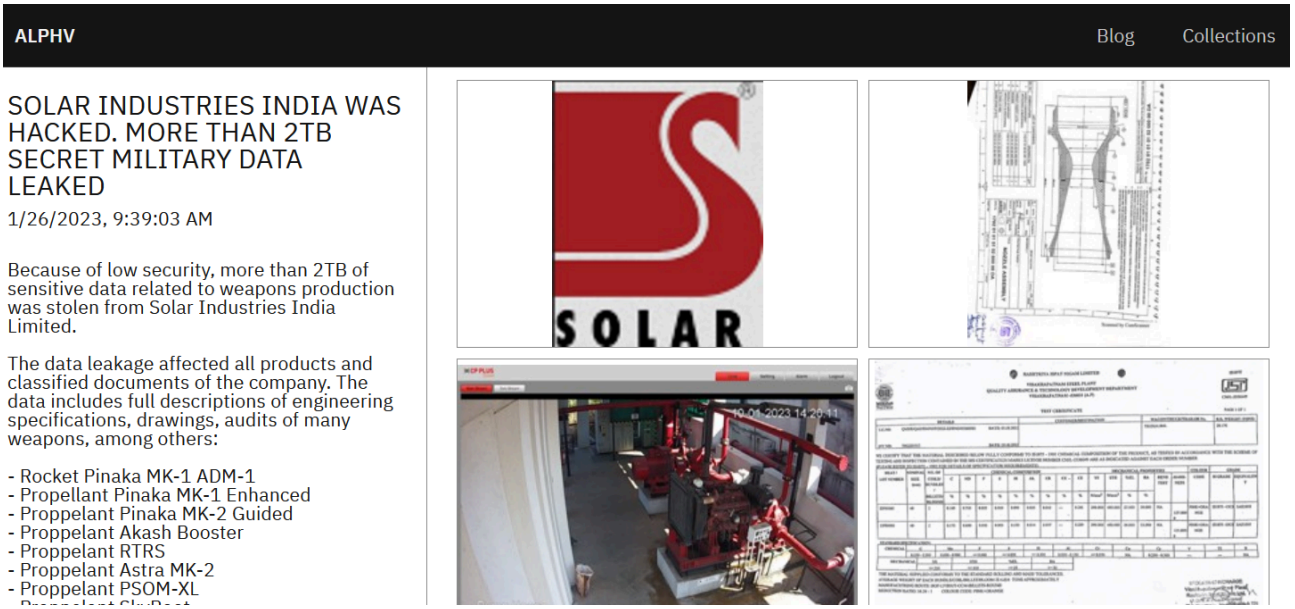
BlackCat Ransomware gang stole secret military data from industrial explosives manufacturer

By Pierluigi Paganini

Published: 2023-01-27 · Archived: 2026-04-05 15:06:03 UTC



The BlackCat Ransomware group claims to have hacked SOLAR INDUSTRIES INDIA and to have stolen 2TB of “secret military data.”

The BlackCat Ransomware gang added SOLAR INDUSTRIES INDIA to the list of victims published on its Tor leak site. The company is a globally recognised industrial explosives manufacturer, it provides complete blasting solutions, including packaged, bulk explosives and initiating systems to meet its customer needs across the globe.

The BlackCat Ransomware group claims to have breached the company infrastructure and to have stolen 2TB of data, including secret military data related to weapons production.

“Because of low security, more than 2TB of sensitive data related to weapons production was stolen from Solar Industries India Limited.” reads the message published on the leak site. “The data leakage affected all products and classified documents of the company. The data includes full descriptions of engineering specifications, drawings, audits of many weapons, among others:

- Rocket Pinaka MK-1 ADM-1
- Propellant Pinaka MK-1 Enhanced
- Proppelant Pinaka MK-2 Guided
- Proppelant Akash Booster
- Proppelant RTRS

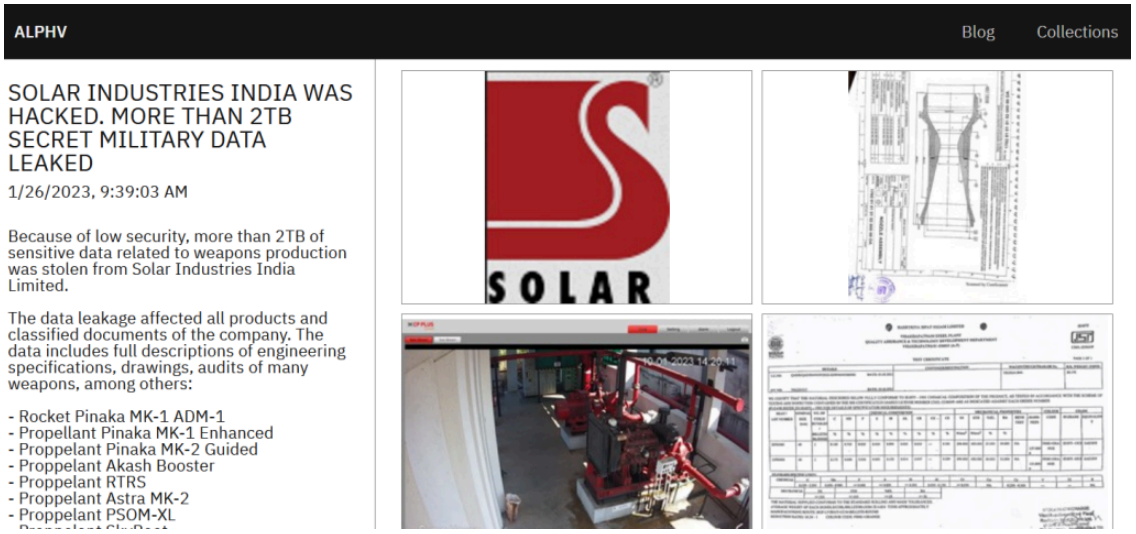
- Proppelant Astra MK-2
- Proppelant PSOM-XL
- Proppelant SkyRoot
- Proppelant Star Booster
- Proppelant HEMRL(PJ-10)
- Proppelant BramhMos
- Proppelant A1-P(P1 & P2)
- Warhead: Konkur, Invar, ATGM MK-2, MPBX Blocks
- Mines: Vibhav, Vishal, Adrashy
- Bomb: PGB 450, GP 250

And much more.”

Stolen data includes:

- Personal information about the company’s employees and customers
- Armament supply chains to various sources
- Blueprints and engineering documentation of the weapons
- Information about who Solar Industries India is partnering with
- Government documents revealing details of cooperation
- Records from all production cameras and offices
- Backups and databases
- Details of warhead composition and engineering documentation of the callout elements of various products
- Audits and reports of flaws and vulnerabilities in the company’s products
- Documentation of technical, power and other characteristics of the company’s products
- Internal product testing documentation with all documentation and approvals
- Information and documents about our future developments
- Contracts with the army and other customers

BlackCat published images of the stolen documents and pictures taken from the company’s security cameras as proof of the hack.



The group invites anyone wishing to bid on all Solar Group data within 24 hours of the publication of its blog to contact them in TOX.

It is interesting to notice that the gang claims have serious evidence of industrial spying in other countries (including friendly states).

Follow me on Twitter: **@securityaffairs** and **Facebook** and **Mastodon**

[adrotate banner="9″]	[adrotate banner="12″]

Pierluigi Paganini

(SecurityAffairs – hacking, BlackCat Ransomware)

[adrotate banner="5″]

[adrotate banner="13″]
