

Japanese watchmaker Seiko breached by BlackCat ransomware gang

By Bill Toulas

Published: 2023-08-21 · Archived: 2026-04-05 12:54:36 UTC



The BlackCat/ALPHV ransomware gang has added Seiko to its extortion site, claiming responsibility for a cyberattack disclosed by the Japanese firm earlier this month.

Seiko is one of the world's largest and most historic watchmakers, with roughly 12,000 employees and an annual revenue that surpasses \$1.6 billion.

On August 10th, 2023, the company published a notice of a data breach informing that an unauthorized third-party gained access to at least a part of its IT infrastructure and accessed or exfiltrated data.



Visit Advertiser website [GO TO PAGE](#)

"It appears that [on July 28, 2023] some as-yet-unidentified party or parties gained unauthorized access to at least one of our servers," [reads Seiko's announcement](#).

"Subsequently, on August 2nd, we commissioned a team of external cybersecurity experts to investigate and assess the situation."

"As a result, we are now reasonably certain that there was a breach and that some information stored by our Company and/or our Group companies may have been compromised."

Seiko apologized to the potentially impacted customers and business partners and urged them to be vigilant against email or other communication attempts potentially impersonating Seiko.

BlackCat assuming responsibility

Today, the BlackCat ransomware group claimed to be behind the attack on Seiko, posting samples of data that they claim to have stolen during the attack.

In the listing, the threat actors mock Seiko's IT security and leak what appear to be production plans, employee passport scans, new model release plans, and specialized lab test results.

Most worryingly, the threat actors have leaked samples of what they claim are confidential technical schematics and Seiko watch designs.



Seiko listed on ALPHV website

Source: *BleepingComputer*

This indicates that BlackCat very likely possesses drawings that showcase Seiko internals, including patented technology, which would be damaging to publish and expose to competitors and imitators.

BlackCat is one of the most advanced and notorious ransomware gangs actively targeting the enterprise, constantly evolving its extortion tactics.

For example, the group was the first to use a [clearweb website dedicated to leaking data](#) for a particular victim and, more recently, [created a data leak API](#), allowing for easier distribution of stolen data.

Update 8/21/23: After publishing this story, researchers at [Curated Intel](#) told BleepingComputer that an initial access broker (IAB) was selling access to a Japanese manufacturing company on July 27th, one day before Seiko said they were initially breached.

While the IAB did not share the name of the company they were selling access to, they did say the company is in manufacturing and has '1.8B' in revenue per Zoominfo, which is an exact match to [Seiko's Zoominfo page](#).

JAPAN BIG COMPANY LOCALADMIN Access
By AliceWonderland,

AliceWonderland

byte
● one of most famous companies in world

Geo: Japan
Industry: Manufacturing
Revenue: \$1800kk = 1.8B\$ (zoominfo)

Paid registration
🔒 2
8 posts
Joined
04/05/23 (ID: 142754)
Activity
хакинг / hacking
Deposit
0.035000 ₿

Access type: RDP Access (Anydesk, ngrok, ...)
Access level: Local Admin

Number of hosts: 16000
Number of users: 11000
Domain trusts: 13

AV: Windows defender

Start: \$3000
Minimum step: 500\$
Blitz: \$5000

Initial access broker selling access to Japanese company

Source: *Curated Intel*

BleepingComputer has contacted Seiko for additional comments on the threat actor's claims, but we have not received a response by publication time.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/>