Research on the recent cyber attack 2023-2024

What happened?

In mid-2024, Kadokawa Corporation and its video sharing platform Niconico were hit by a ransomware attack by the BlackSuit group. The attackers also stole data about 254,241 users' information was leaked. The attack disrupted services; after discovering the breach, Kadokawa shut down services, including physically disconnecting servers when remote mitigations weren't enough.

Who was affected?

Users of Niconico and other Kadokawa Group services were directly impacted, especially those whose account data was exposed. It also affected business partners and the Kadokawa Dwango Educational Institute, which had its operations disrupted.

How could it have been prevented?

Stronger preventive measures might have included better protections against phishing (since that was believed to be the entry point). Ensuring secure configuration of remote access systems, tight network segmentation, timely patching, and strong authentication (e.g. MFA) could reduce risk. Also, having reliable incident detection and response processes to isolate infected systems quickly would limit damage.