

[NEWS RELEASE]

July 3, 2024

KADOKAWA CORPORATION

Notification and Apology Concerning Information Leakage caused by the Ransomware Attack

KADOKAWA CORPORATION (Headquarters: Chiyoda-ku, Tokyo; Chief Executive Officer: Takeshi Natsuno; hereinafter “KADOKAWA”) expresses deep apologies for the significant concern and trouble caused to its readers, users, writers, creators, business partners, shareholders, investors, and other stakeholders by the system failure currently affecting the KADOKAWA Group.

After the discovery of a significant cyberattack including ransomware targeting *Niconico* and the related services, the KADOKAWA Group promptly established a task force and commenced an ongoing investigation into the possibility of information leakage with assistance including external professional organizations. In the process, KADOKAWA Group is investigating the data revealed by the cybercriminal organization regarding the claim that it leaked KADOKAWA Group’s data. We report the information that we recognized is likely to have been leaked by our investigation as below.

In addition, we have confirmed a high possibility of the leakage of some information concerning KADOKAWA DWANGO Educational Institute, for which DWANGO Co., Ltd., a Group company of KADOKAWA CORPORATION, provides educational content and systems.

We sincerely apologize to the students, the graduates, their parents, and all those concerned for any concern and trouble this may cause.

Note that KADOKAWA does not itself store credit card information on KADOKAWA Group customers, including customers of *Niconico* services. This structure prevents the leakage of this information from KADOKAWA, as we have already announced.

In July, we expect to receive accurate information based on the findings of external professional organizations. We shall report this as soon as it is ascertained.

◆ Types of Information Likely to have been Leaked (as of July 3, 2024)

[External Information]

- **Personal information of some students and graduates of N Progressive School and N/S High Schools, and their parents**
- **Contracts with some creators, sole proprietors and companies with whom DWANGO Co., Ltd. does business**
- **Personal information of some creators who use music monetization services (NRC) of DWANGO Co., Ltd.**
- **Information on companies operated by some former employees of DWANGO Co., Ltd.**

[Internal Information]

- **Personal information on all DWANGO Co., Ltd. employees (including contract workers, temp workers, part-time workers, and some retired employees)**
- **Personal information on some employees of affiliated companies of DWANGO Co., Ltd.**
- **Internal documents of DWANGO Co., Ltd. including legal documents**

The attack mainly targeted the dedicated file server of DWANGO Co., Ltd., and no trace of the attack has been confirmed at this moment on the system storing the information of authors, creators, and customers with whom KADOKAWA CORPORATION does business. We have confirmed that personal information of some authors and creators who had direct dealings with DWANGO Co., Ltd. has been leaked, but not confirmed any leakage of information for those who did not have direct dealings with DWANGO Co., Ltd.

◆ Notification to Affected Persons

We extend our apologies and shall individually notify the students, graduates of KADOKAWA DWANGO Educational Institute, and their parents, as well as creators, business partners, and former employees, whose information is newly confirmed as being affected by the leakage. Furthermore, we have established a dedicated helpdesk for inquiries concerning this incident. We shall also explain the matter to our affected employees. For those who cannot be contacted individually, this announcement shall serve as notification.

It is possible that such personal information will be maliciously exploited, and unsolicited email including phishing mail and spam mail will be sent. Please take all precautions if you receive a suspicious email.

<Dedicated Helpdesk for Information Leakage Inquiries*>

1. For users, creators and business partners

https://qa.nicovideo.jp/helpdesk?category_id=982&faq_id=22764&site_domain=default

2. For the students, graduates of KADOKAWA DWANGO Educational Institute, and their parents

https://qa.nicovideo.jp/helpdesk?category_id=984&faq_id=22986&site_domain=default

*Japanese only

Be aware that accessing or downloading data files from websites which the organization claims to have attacked comes with risks, such as malware infection. Although we are currently investigating what the organization claims, we ask for your understanding and cooperation in refraining from sharing the leaked information on social media or elsewhere, as the spread of this personal information could have serious repercussions by infringing upon privacy.

The police have already begun an investigation into this case. In addition, KADOKAWA is providing the relevant authorities with necessary reports. As previously reported, the KADOKAWA Group's business activities have been affected to a certain extent, but we shall stand firm in our response rather than give in to such criminal acts.

Meanwhile, we take this situation very seriously. While proceeding with a more in-depth investigation of the cause, we will further strengthen our information security systems to prevent a recurrence.

KADOKAWA reiterates its deepest apologies to our customers and all those concerned for the considerable concern and trouble this matter has caused.

End of document

For media inquiries, please contact:
Investor and Public Relations Division, KADOKAWA CORPORATION
Email: pr-dept@kadokawa.jp