

Toy maker Jakks Pacific reports cyberattack after multiple ransomware groups leak data

By Jonathan Greig

Published: 2023-02-02 · Archived: 2026-04-05 14:05:08 UTC

Toy production giant Jakks Pacific reported a cyberattack to the U.S. Securities and Exchange Commission last week after two different ransomware gangs posted stolen information to their leak site.

On December 22, the company released a notice confirming it had suffered a ransomware attack on December 8 that encrypted their servers.

The firm – which is one of the biggest toy companies in the world thanks to licensing deals with Disney and Nintendo – hired cybersecurity experts to deal with the incident and restore their servers.

The company filed documents with the SEC in mid-December confirming the incident.





“We believe that the data that was unlawfully accessed potentially includes personal information (including names, emails, addresses, taxpayer identification numbers, and banking information of affected individuals and businesses),” the company [said](#) in a statement.

“We suggest that you immediately take appropriate protective measures to safeguard your personal and banking information. This is an ongoing investigation.”

The company said it is still working to restore its network and to “protect the security and confidentiality of the information contained in our computer network.”

In its [letter to the SEC](#), CFO John Kimble said the company used “containment protocols to mitigate the impact of the threat” but realized on December 14 that “certain data, including personal data of employees, had been extracted from the Company’s IT System.”

“The Company is in the early stages of its investigation and assessment of the incident. Based on the information currently known, the Company does not currently believe the incident will have a material adverse impact on its business, operations or financial results,” Kimble said, noting that it is still investigating what other information may have been accessed.

<h1>JAKKS Pacific Inc</h1> <p>Corporate Overview JAKKS Pacific, Inc. is a multi-brand company that, since 1995, has been designing, developing, producing and marketing toys, leisure products and writing instruments for children and adults around the world.</p> <p>The company has become a top six U.S. player in the toys and leisure products sector through product development, licensing agreements and strategic acquisitions. We believe our growth strategy is unique and built upon a concentrated effort to spread earnings across all four quarters. We have accomplished that by expanding and 'counter-seasonalizing' our product lines, adding new retail outlets and leveraging our product development and merchandising expertise on products with staying power.</p> <p>About JAKKS Pacific, Inc. JAKKS Pacific, Inc. is a leading designer, manufacturer and marketer of toys and consumer products sold throughout the world, with its headquarters in Santa Monica, California. JAKKS Pacific's popular proprietary brands include: Fly Wheels®, Perfectly Cute®, ReDo Skateboard Co.®, X Power Dozer®, Disguise®, Weee-Do™ and a wide range of entertainment-inspired products featuring premier licensed properties. Through JAKKS Care, the company's commitment to philanthropy, JAKKS is helping to make a positive impact on the lives of children. Visit us at www.jakks.com and follow us on Instagram (@jakkstoys), Twitter (@jakkstoys) and Facebook (JAKKS Pacific).</p> <p>Website jakks.com</p>	<p>Encrypted at</p> <p> 8 December 2022 12:08:30</p> <p>Share</p> <p> </p> <p>Disclosed at</p> <p> 19 December 2022 20:39:00</p>
--	---

The company [reported record profits in 2022](#) thanks to the success of merchandise resulting from films like Disney's "Encanto" and "Sonic the Hedgehog." Jakks is expecting an even bigger 2023 with the coming release of the "Super Mario Brothers" movie.

But the attack on the company caused a minor stir among cybersecurity experts because two different ransomware groups – [Hive](#) and [BlackCat](#) – posted data stolen from Jakks.

Hive leaked first, posting stolen information on December 19. BlackCat followed on December 28, with screenshots of information uploaded to their leak site.

A spokesperson for the Hive ransomware gang [told DataBreaches](#) that both groups bought access to the company's network from an initial access broker and agreed to split a \$5 million ransom.

The company refused to pay and did not negotiate, the representative said.

The situation highlights one of the more underreported aspects of the ransomware ecosystem: the prevalence of initial access brokers and wholesale access markets.



Many ransomware groups typically do not attack companies themselves, instead buying access from hackers who do the initial leg work and then sell the spoils.

In September, experts [said they had traced](#) almost 700 ransomware incidents back to wholesale access markets — platforms where people sell access to compromised endpoints, and more.

One initial access broker [told The Record](#) in August that it is also common for affiliates from the different ransomware groups to compete in the same network to extort victims.



Know what matters.

Act first.

Get started





[Jonathan Greig](#)

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.

Source: <https://therecord.media/toy-maker-jakks-pacific-reports-cyberattack-after-multiple-ransomware-groups-post-stolen-data/>