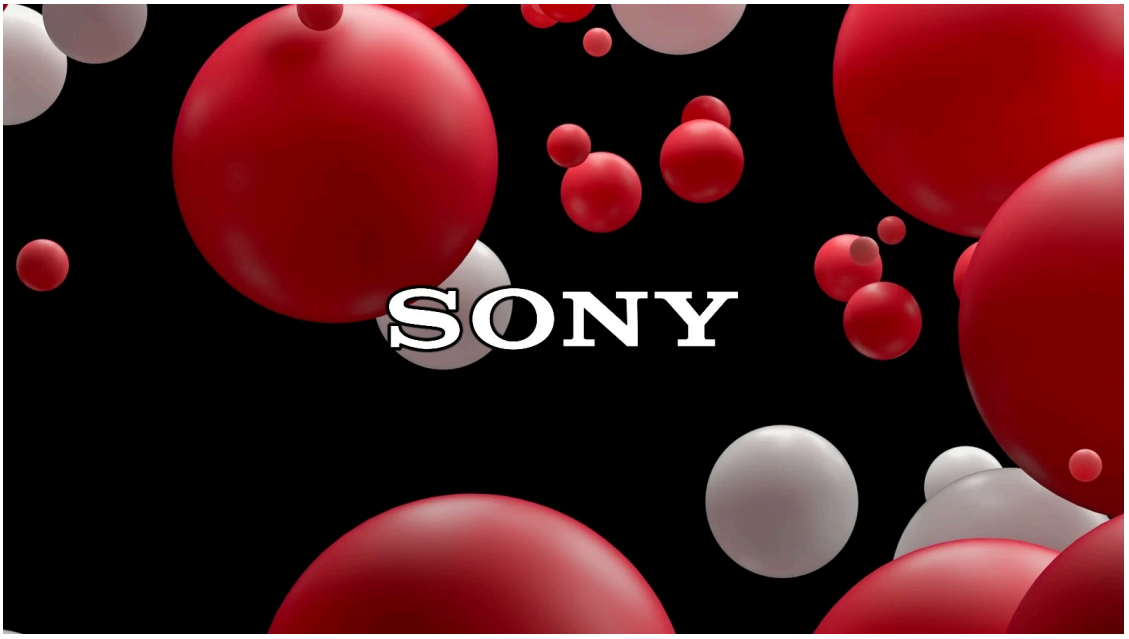
Sony confirms data breach impacting thousands in the U.S.

By Bill Toulas

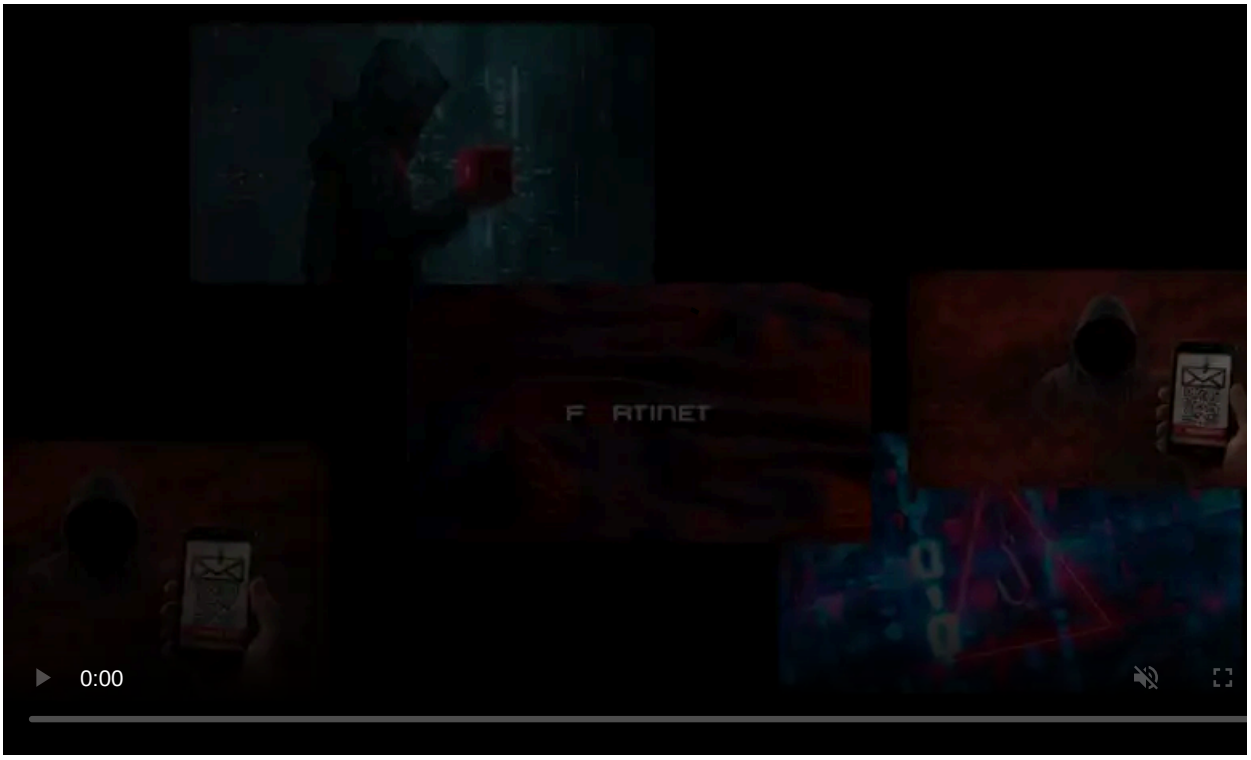
Published: 2023-10-04 · Archived: 2026-04-05 22:47:13 UTC

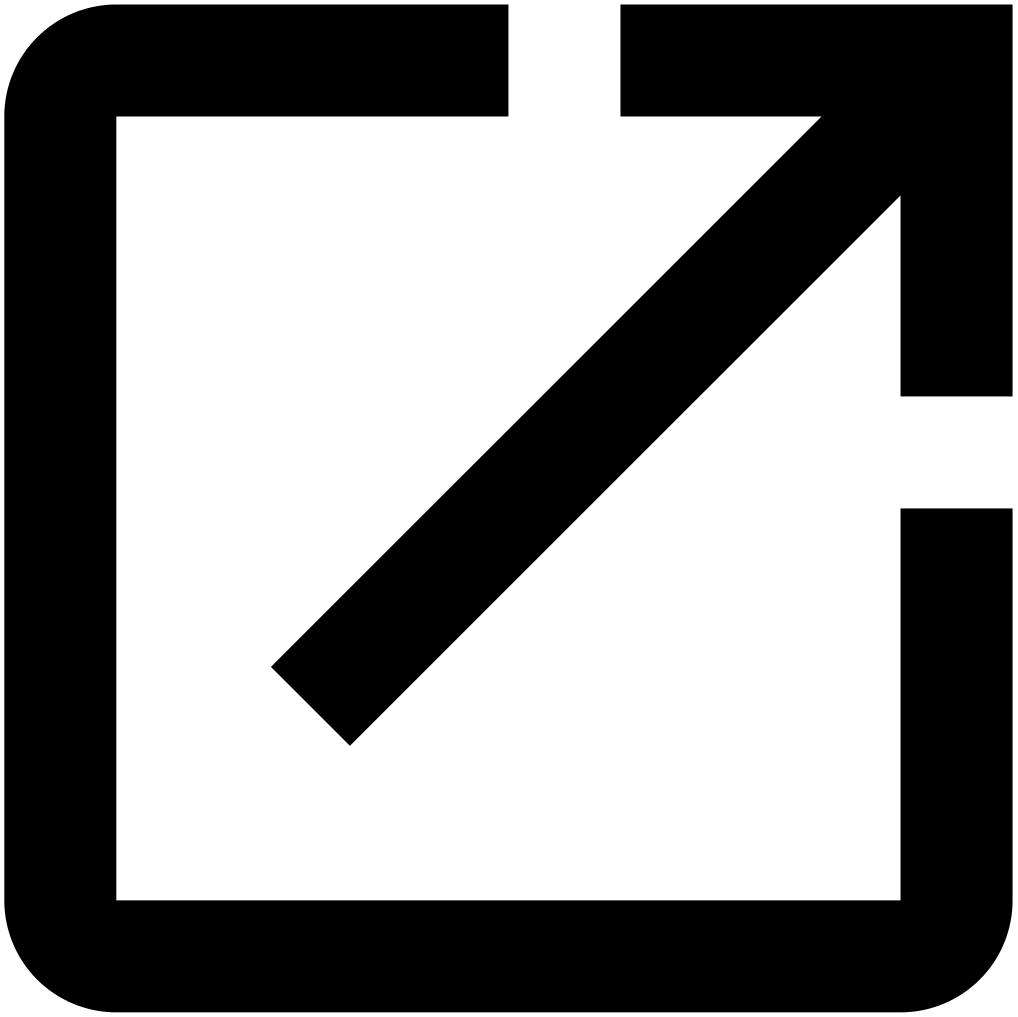


Sony Interactive Entertainment (Sony) has notified current and former employees and their family members about a cybersecurity breach that exposed personal information.

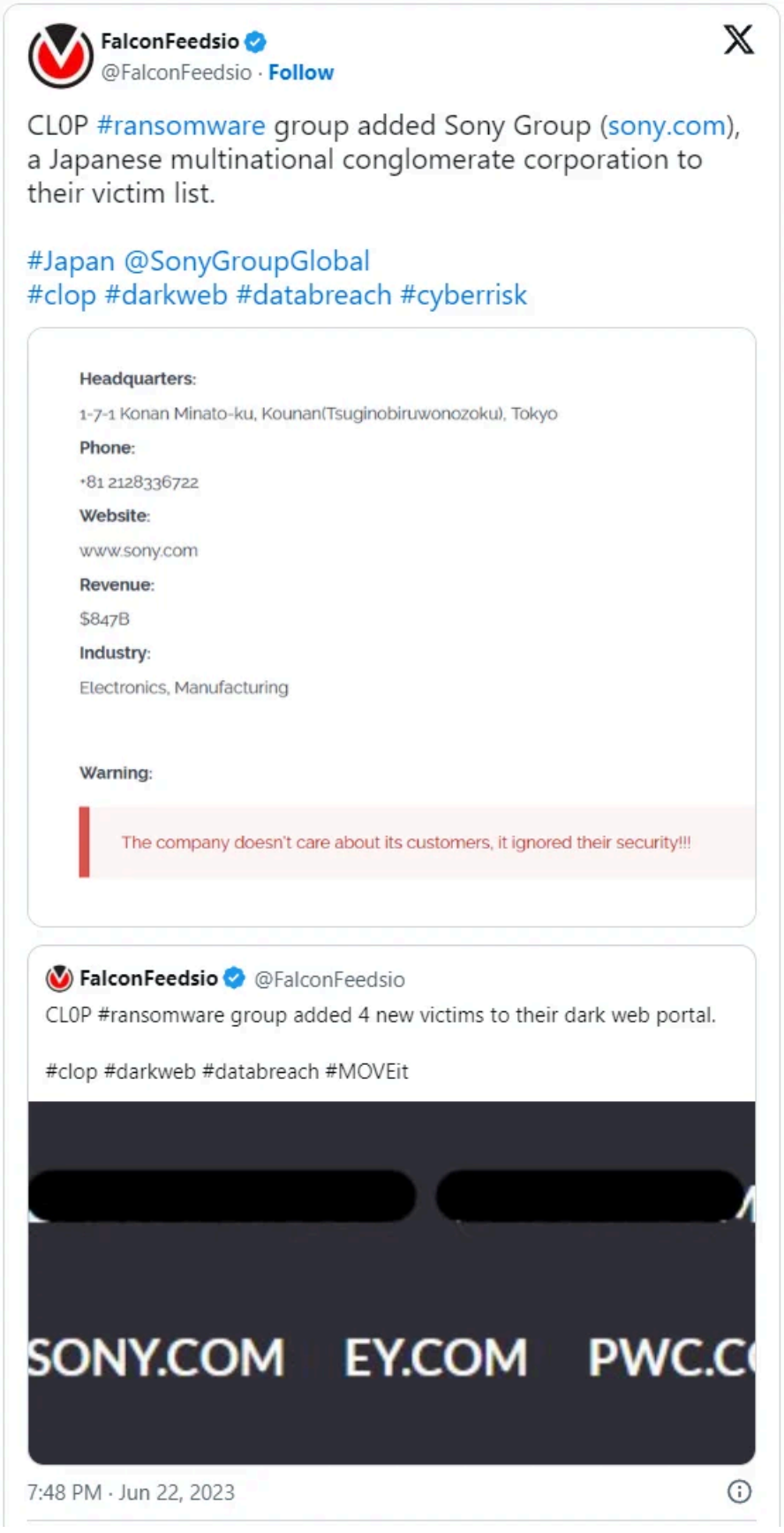
The company sent the data breach notification to about 6,800 individuals, confirming that the intrusion occurred after an unauthorized party exploited a zero-day vulnerability in the MOVEit Transfer platform.

The zero-day is CVE-2023-34362, a critical-severity SQL injection flaw that leads to remote code execution, leveraged by the Clop ransomware in large-scale attacks that compromised numerous organizations across the world.


F RTINET
0:00



Clop ransomware gang added Sony Group to its list of victims in late June. However, the firm did not provide a public statement until now.



According to the data breach notification, the compromise happened on May 28, three days before Sony learned from Progress Software (the MOVEit vendor) about the flaw, but it was discovered in early June.

“On June 2, 2023, [we] discovered the unauthorized downloads, immediately took the platform offline, and remediated the vulnerability,” reads the notice.

“An investigation was then launched with assistance from external cybersecurity experts. We also notified law enforcement,” Sony says in the data breach notification.

Sony says the incident was limited to the particular software platform and had no impact on any of its other systems.

Still, sensitive information belonging to 6,791 people in the U.S. was compromised. The firm has individually determined the exposed details and listed them in each individual letter, but it is censored in the notification sample submitted to the Office of the Maine Attorney General.

The notification recipients are now offered credit monitoring and identity restoration services through Equifax, which they can access by using their unique code until February 29, 2024.

Sony’s more recent breach

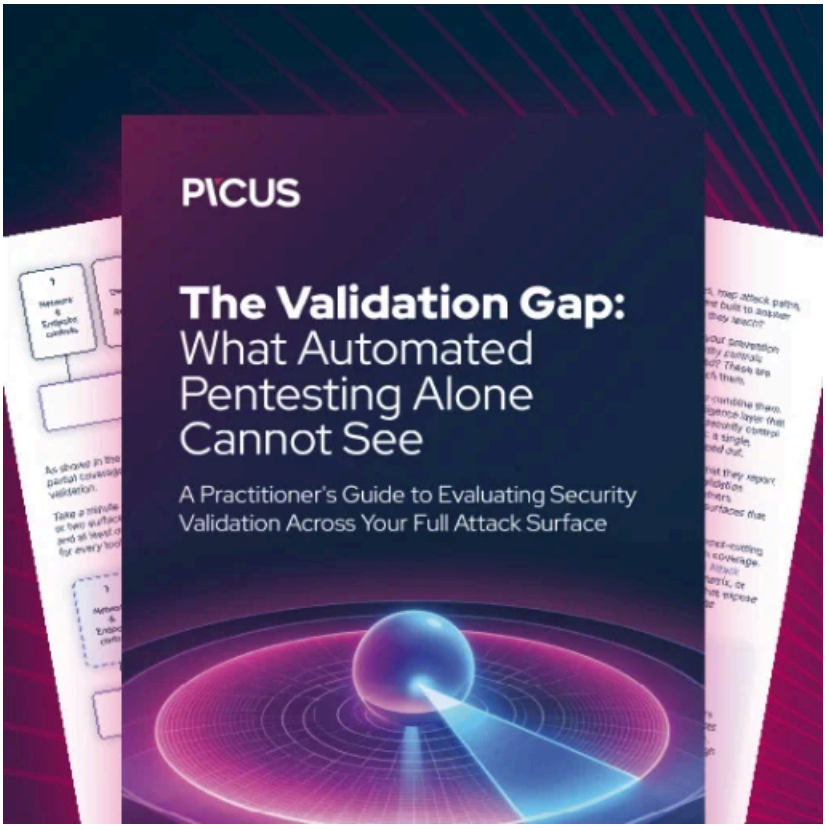
Late last month, following allegations on hacking forums that Sony had been breached again and 3.14 GB of data had been stolen from the company’s systems, the firm responded by saying it was investigating the claims.

The leaked dataset that at least two separate threat actors held, contained details for the SonarQube platform, certificates, Creators Cloud, incident response policies, a device emulator for generating licenses, and more.

A Sony spokesperson shared with BleepingComputer the statement below, which confirms a limited security breach:

> Sony has been investigating recent public claims of a security incident at Sony. We are working with third-party forensics experts and have identified activity on a single server located in Japan used for internal testing for the Entertainment, Technology and Services (ET&S) business.
>
> Sony has taken this server offline while the investigation is ongoing. There is currently no indication that customer or business partner data was stored on the affected server or that any other Sony systems were affected. There has been no adverse impact on Sony's operations.

This confirms that Sony has suffered two security breaches in the past four months.



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/sony-confirms-data-breach-impacting-thousands-in-the-us/