Amazon confirms employee data breach after vendor hack

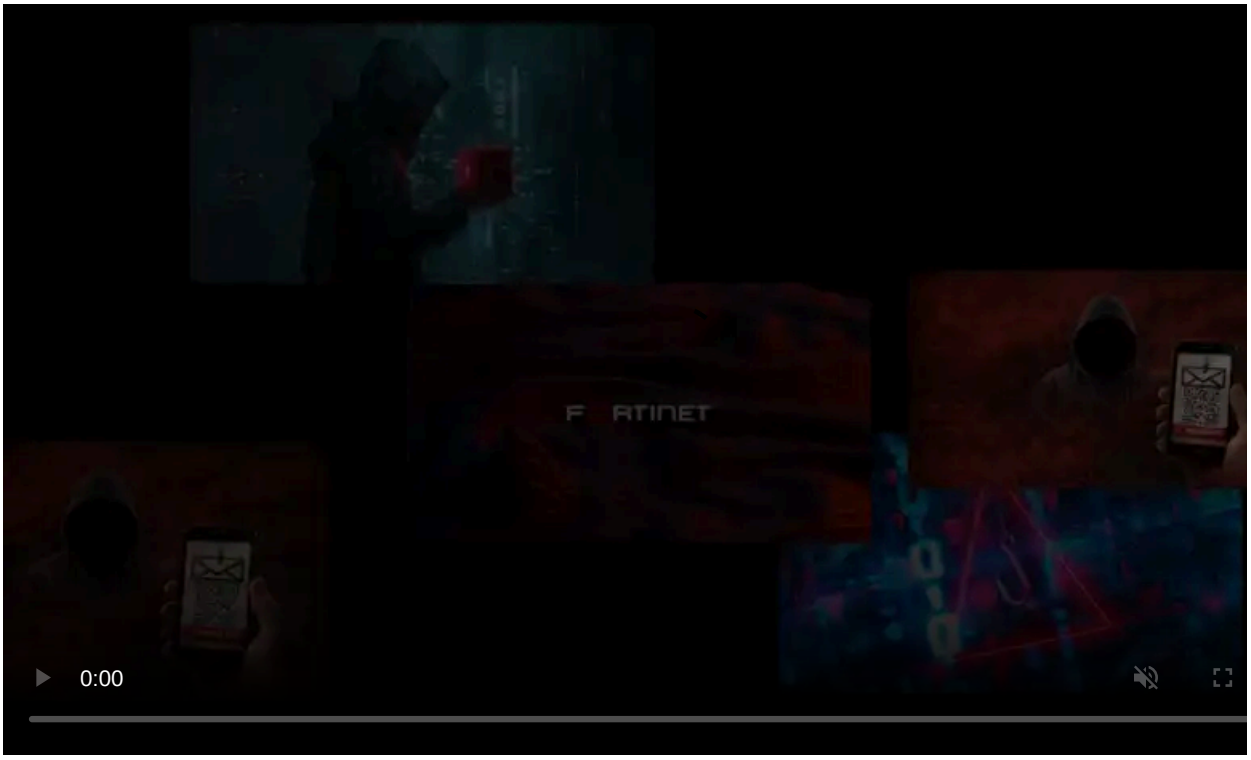
By Sergiu Gatlan

Published: 2024-11-11 · Archived: 2026-04-06 01:03:47 UTC

Amazon confirmed a data breach involving employee information after data allegedly stolen during the May 2023 MOVEit attacks was leaked on a hacking forum.

The threat actor behind this data leak, known as Nam3L3ss, published over 2.8 million lines of Amazon employee data, including names, contact information, building locations, email addresses, and more.

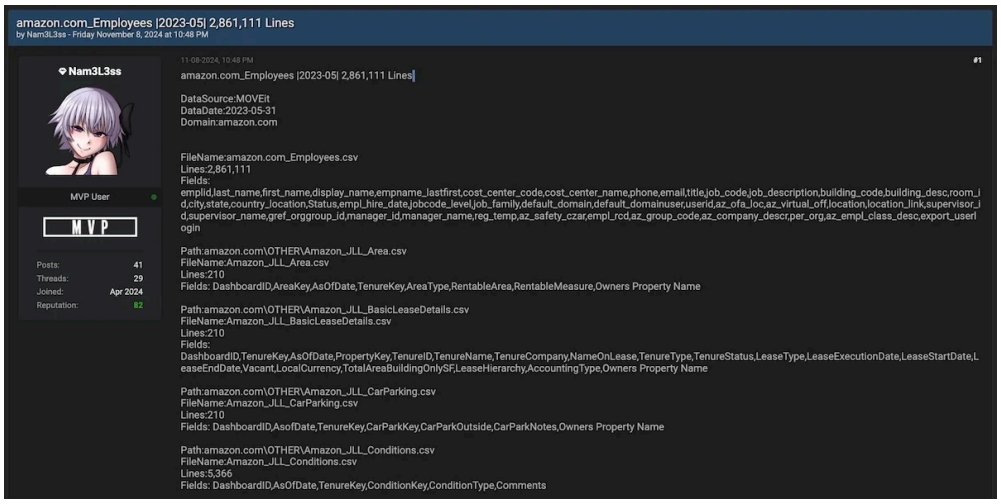
Amazon spokesperson Adam Montgomery confirmed Nam3L3ss' claims, adding that this data was stolen from systems belonging to a third-party service provider.


F RTINET
0:00

"Amazon and AWS systems remain secure, and we have not experienced a security event. We were notified about a security event at one of our property management vendors that impacted several of its customers including Amazon," Montgomery said.

"The only Amazon information involved was employee work contact information, for example work email addresses, desk phone numbers, and building locations."

The company said the breached vendor only had access to employee contact information, and the attackers didn't access or steal sensitive employee information like Social Security numbers, government identification, or financial information. Amazon added that the vendor has since patched the security vulnerability used in the attack.



Amazon employee data for sale (BleepingComputer)

Nam3L3ss has also leaked the data from twenty-five other companies. However, they say some of the data was obtained from other sources, including ransom gangs' leak sites and exposed AWS and Azure buckers.

"I download entire databases from exposed web sources including mysql, postgres, SQL Server databases and backups, azure databases and backups etc and then convert them to csv or other format," they said.

"DO NOT ask me for access to my storage etc, at present I have well over 250TB of archived database files etc."

The list of companies whose data was stolen in MOVEit attacks or harvested from Internet-exposed resources and has now been leaked on the hacking forum includes Lenovo, HP, TIAA, Schwab, HSBC, Delta, McDonald's, and Metlife, among others (as shown in the table below).

BleepingComputer has contacted multiple companies and will update this article when additional information is available.

Company	Date Stolen	Number of Employees
Lenovo	2023-05	45,522
McDonald's	2023-05	3,295
HP	2023-05	104,119
City National Bank	2023-05	9,358
BT	2023-05	15,347
dsm-firmenich	2023-05	13,248
Rush University	2023-05	15,853

URBN	2023-05	17,553
Westinghouse	2023-05	18,193
UBS	2023-05	20,462
TIAA	2023-05	23,857
OmnicomGroup	2023-05	37,320
Bristol-Myers Squibb	2023-05	37,497
3M	2023-05	48,630
Schwab	2023-05	49,356
Leidos	2023-05	52,610
Canada Post	2023-05	69,860
Amazon	2023-05	2,861,111
Delta	2023-05	57,317
Applied Materials	2023-05	53,170
Cardinal Health	2023-05	407,437
US Bank	2023-05	114,076
fmr.com	2023-05	124,464
HSBC	2023-05	280,693
MetLife	2023-05	585,130

The MOVEit data-theft attacks

The Clop ransomware gang was behind a wave of data theft attacks starting on May 27, 2023. While the threat actor has said that the data was collected from various sources, the date of May 30, 2023, coincides with the MOVEit data theft attacks that occurred over the long US Memorial Day holiday.

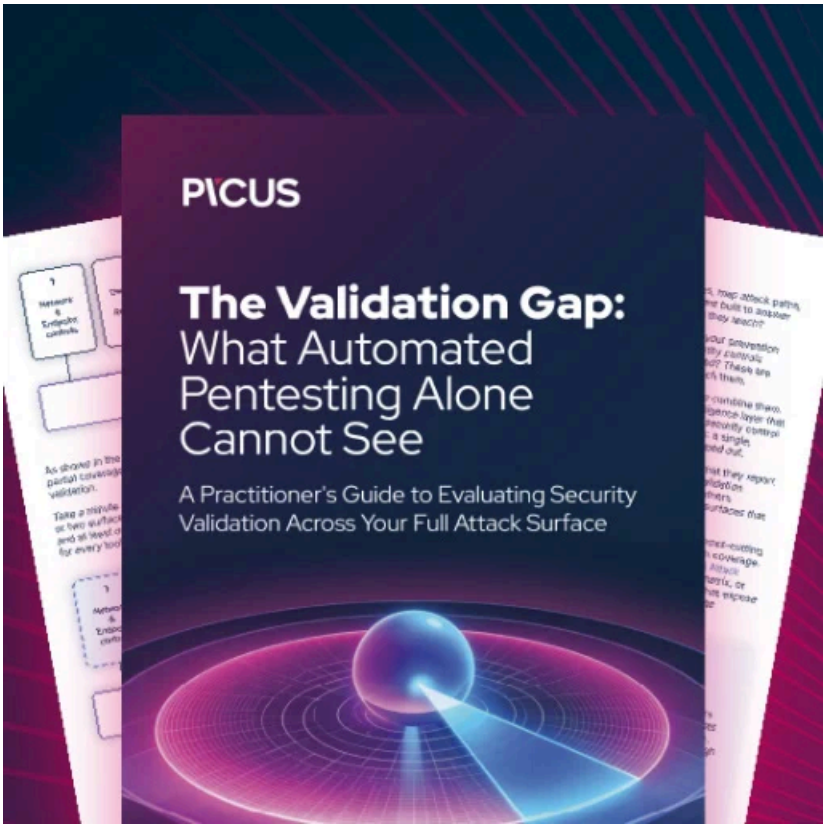
The data leaked for each of the twenty-five companies is similar, so it is believed that the data was stolen from a single vendor during these attacks and has now been released as separate data sets for the impacted customers.

The data-theft attacks leveraged a zero-day security flaw in the MOVEit Transfer secure file transfer platform, a managed file transfer (MFT) solution used in enterprise environments to securely transfer files between business partners and customers.

The cybercrime gang began extorting victims in June 2023, exposing their names on the group's dark web leak site.

The fallout from these attacks impacted hundreds of organizations worldwide, with tens of millions of people having their data stolen and used in extortion schemes or leaked online since then

Multiple U.S. federal agencies and two U.S. Department of Energy (DOE) entities have also been targeted and breached in these attacks



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/amazon-confirms-employee-data-breach-after-vendor-hack/