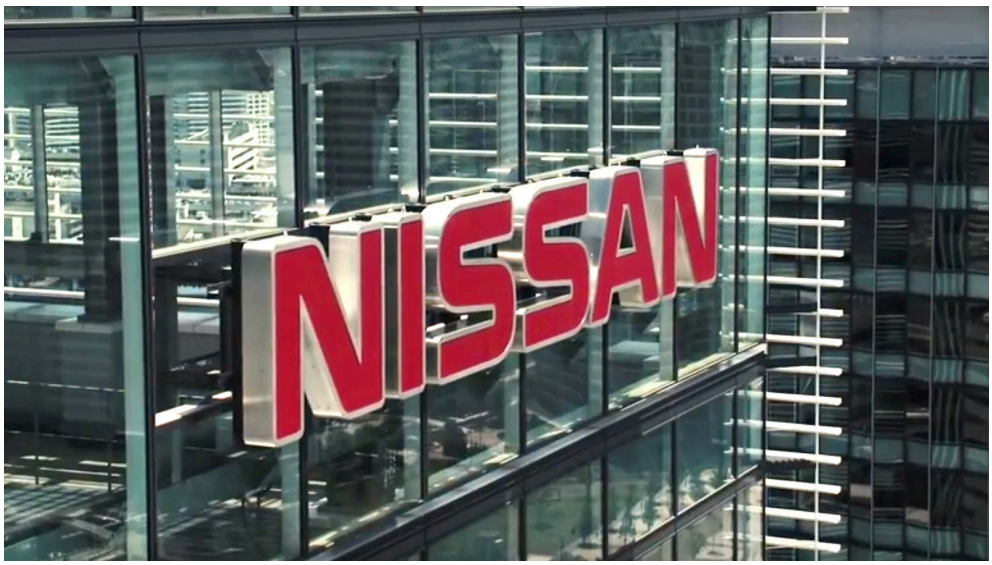
Nissan Australia cyberattack claimed by Akira ransomware gang

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)**

December 22, 2023 11:38 AM **0**



Today, the Akira ransomware gang claimed that it breached the network of Nissan Australia, the Australian division of Japanese car maker Nissan.

In a new entry added to the operation's date leak blog on December 22, Akira says that its operators allegedly stole around 100GB of documents from the automaker's systems.

The attackers have threatened to leak sensitive business and client data online, as ransom negotiations with Nissan failed after the company either refused to engage or pay the ransom.

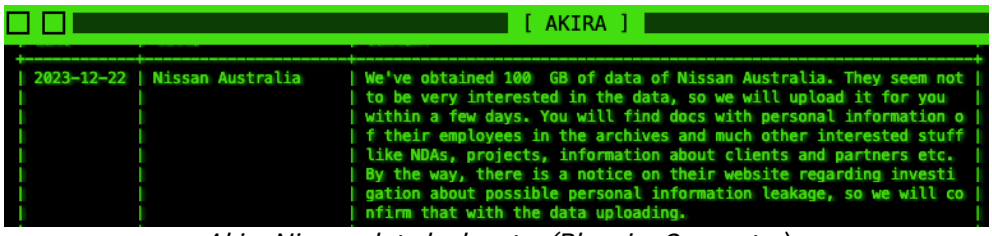
"They seem not to be very interested in the data, so we will upload it for you within a few days," the ransomware group says. "You will find docs with personal information of their employees in the archives and much other interested stuff like NDAs, projects, information about clients and partners etc."

Akira surfaced in March 2023 (https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/) and drew attention after quickly amassing a large number of victims from various industry sectors.

In June 2023, Akira ransomware operators started deploying a Linux variant of their encryptor (https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/) designed to target VMware ESXi virtual machines widely used in enterprise environments.

According to negotiations seen by BleepingComputer, the ransomware group is asking for ransom payments from $200,000 to millions of dollars, depending on the breached organization's size.

While another ransomware strain named Akira was released five years ago (https://twitter.com/struppigel/status/902413046852845570), in 2017, the two operations are unlikely to be related.



Akira Nissan data leak entry (BleepingComputer)

Nissan still working to restore systems

While the company has yet to attribute a cyberattack disclosed on December 5 (https://www.bleepingcomputer.com/news/security/nissan-is-investigating-cyberattack-and-potential-data-breach/), it did add a new update to its website today confirming that attackers have breached some of its systems in Australia and New Zealand.

Nissan says it's still investigating the incident's impact and whether personal information has been accessed. It's also working on restoring systems affected in the attack (a process that started on December 5, after the incident was disclosed.

"We cannot yet confirm the extent of the cyber incident. We are working with our global incident response team and cybersecurity experts to investigate the incident as a matter of urgency," Nissan said.

"Some dealer systems will be impacted however, your local Nissan Dealership is operating. Please speak directly to your local Nissan dealer to assist with all vehicle and servicing queries."

After detecting the breach, Nissan notified the Australian and the New Zealand Cyber Security Centres and relevant privacy regulators and law enforcement bodies.

Likely because of the risk that some data stored on the compromised systems was either accessed or stolen, Nissan also warned customers to "be vigilant for any unusual or suspicious online activity."

Nissan has yet to reply to a request for comment and additional information on the cyber incident from BleepingComputer.

Related Articles:

Nissan confirms ransomware attack exposed data of 100,000 people (https://www.bleepingcomputer.com/news/security/nissan-confirms-ransomware-attack-exposed-data-of-100-000-people/)

Alpha ransomware linked to NetWalker operation dismantled in 2021 (https://www.bleepingcomputer.com/news/security/alpha-ransomware-linked-to-netwalker-operation-dismantled-in-2021/)

LockBit claims ransomware attack on Fulton County, Georgia (https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-fulton-county-georgia/)

Ransomware payments drop to record low as victims refuse to pay (https://www.bleepingcomputer.com/news/security/ransomware-payments-drop-to-record-low-as-victims-refuse-to-pay/)

The Week in Ransomware - January 26th 2024 - Govts strike back (https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-26th-2024-govts-strike-back/)

AKIRA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/AKIRA/)

AUSTRALIA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/AUSTRALIA/)

CYBERATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CYBERATTACK/)

DATA THEFT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DATA-THEFT/)

DOUBLE-EXTORTION (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DOUBLE-EXTORTION/)

EXTORTION (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/EXTORTION/)

NISSAN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/NISSAN/)

RANSOMWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RANSOMWARE/)