Business giant Dussmann Group's data leaked after ransomware attack

By Lawrence Abrams

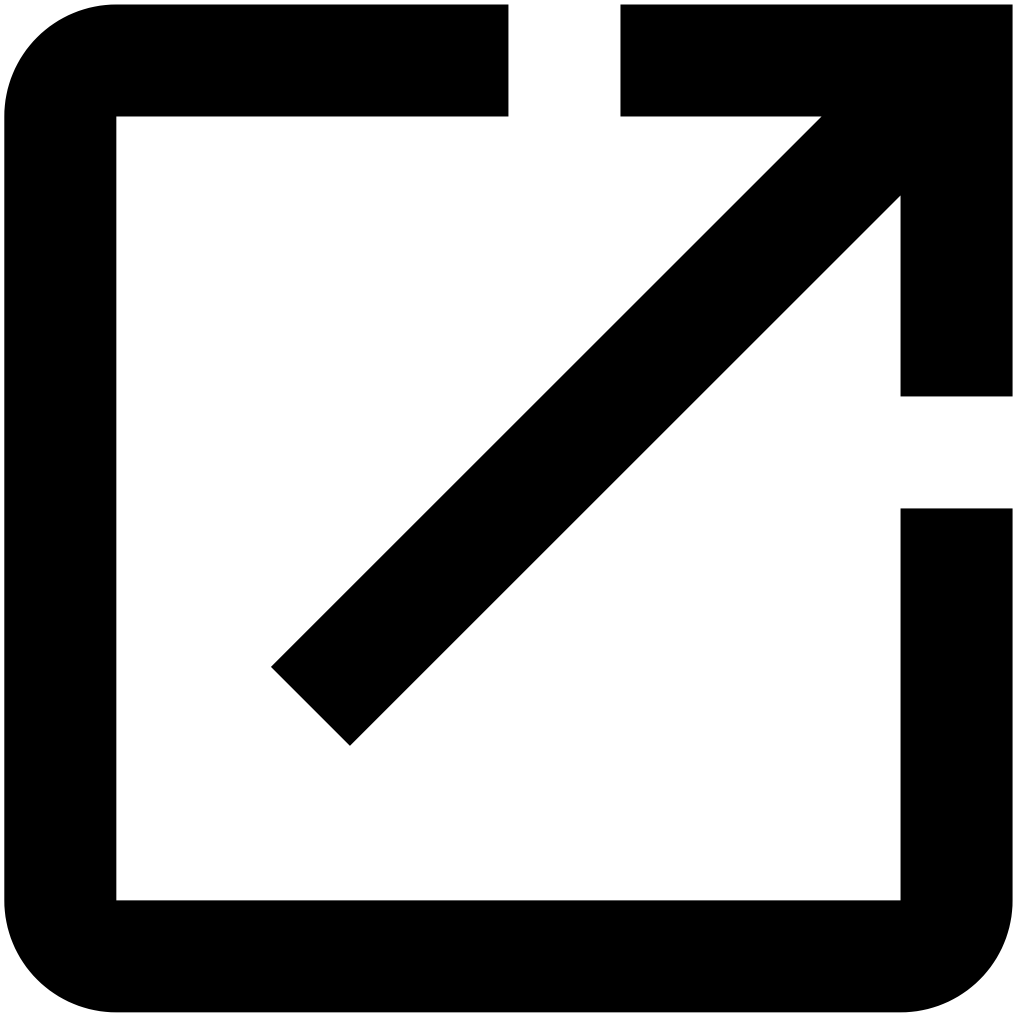
Published: 2020-07-28 · Archived: 2026-04-05 13:50:53 UTC

The Nefilim ransomware operation has begun to publish unencrypted files stolen from a Dussmann Group subsidiary during a recent attack.

The Dussmann Group is the largest multi-service provider in Germany with subsidiaries focusing on facility management, corporate childcare, nursing and care for the elderly, and business systems solutions, including HVAC, electrical work, and elevators.

The company has confirmed to BleepingComputer that one of their subsidiaries, Dresdner Kühlanlagenbau GmbH (DKA), recently suffered a ransomware attack where data was stolen.


DIE LINKE.
0:00



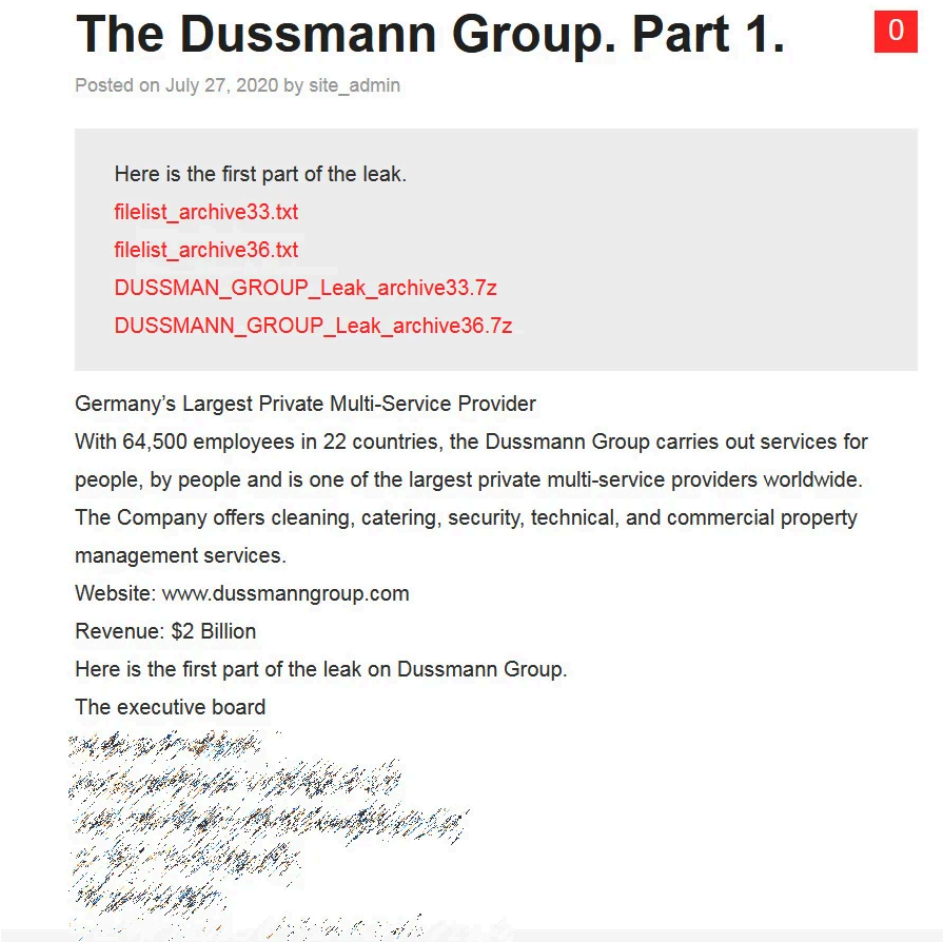
Nefilim publishes DKA's stolen data

During the DKA attack, the Nefilim operators claim to have stolen unencrypted files before deploying the ransomware.

These stolen files are then used as leverage against victims to coerce them to pay the ransom under the threat that the data will be publicly released on ransomware data leak sites.

In a post to their data leak site yesterday, the Nefilim operators have published two archives containing 14 GB worth of stolen files.

According to the file lists, these archives contain numerous documents, including Word documents, images, accounting documents, and AutoCAD drawings.



Nefilim DKA data leak

After learning about the data leak, BleepingComputer contacted Dussmann Group, who confirmed that their subsidiary, DKA, was breached and files were stolen.

"The refrigeration specialist, Dresdner Kühlanlagenbau GmbH (DKA) with 570 employees has been the target of a cyber attack during which data was encrypted and copied. DKA is a subsidiary of the Dussmann Group. The servers were shut down as a precaution. The data protection authorities and the State Office of Criminal Investigation in Saxony have been informed and charges have been filed."

"DKA is in close communication with the authorities and external cyber-security experts. Operational processes in the business unit for refrigeration air-conditioning plant engineering are secure. DKA has already informed clients and employees about the cyber-attack and the data outflow. Due to ongoing investigations, we cannot say more at present," Michaela Mehls, Dussmann Group's Head of Corporate Communications, told BleepingComputer.

The Nefilim ransomware operators have told BleepingComputer that they encrypted four domains and stole approximately 200GB of archives.

It is not known how the Nefilim operators gained access to DKA's network, and cyber intelligence firm Bad Packets was unable to find any vulnerable VPN gateways or devices located on their network.

With exposed remote desktop servers estimated to be responsible for 70-80% of all network breaches, the attackers likely gained access through an exposed server or a phishing attack.

Protecting against ransomware attacks

To protect a network from being breached in ransomware attacks, administrators need a layered approach to securing their system.

With network breaches commonly be conducted via exposed remote desktop services, it is essential to make sure all RDP servers are only accessible over a company VPN.

Ransomware operations commonly target VPN gateways and devices to gain access to corporate and government networks.

With VPN gateways now exposed, they too need to be hardened and secured with the latest security updates and firmware available.

Finally, MFA should be enabled for corporate accounts, and Windows event logs should be monitored for unusual entries.

Microsoft has provided a summary on how to mitigate human-operated ransomware attacks that all system administrators should become familiar with.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
