The Nefilim Ransomware Group Has Hit ‘Spirit Airlines’

By Bill Toulas

Published: 2021-03-06 · Archived: 2026-04-06 02:03:17 UTC

- **American ultra-low-cost airline "Spirit Airlines" had a ransomware breach by the Nefilim group.**
- **Parts of the stolen data are leaked on the dark web, and they contain credit card and transaction details.**
- **The airline hasn’t acknowledged the security incident yet, and neither have they sent notices of a breach.**

The Florida-based low-cost airline "Spirit Airlines" has been hit by the Nefilim ransomware group, which is already publishing samples of the stolen data on their dark web portal. The first block of the stolen data has a size of 40GB.

It contains over 33,000 files, including financial information and various sensitive personal details of customers who bought a ticket and flew with Spirit between 2006 and 2021. So, apparently, the stolen data corresponds to the last 15 years of the airline’s operational information.

We have used specialized dark web intelligence tools provided by KELA to check what type of data is being leaked exactly. Unfortunately, we’ve seen credit card lists and detailed transaction records, email addresses, holder names, and partially hidden card numbers.

Spirit Airlines. Part 1.

0

Posted on March 4, 2021 by site_admin

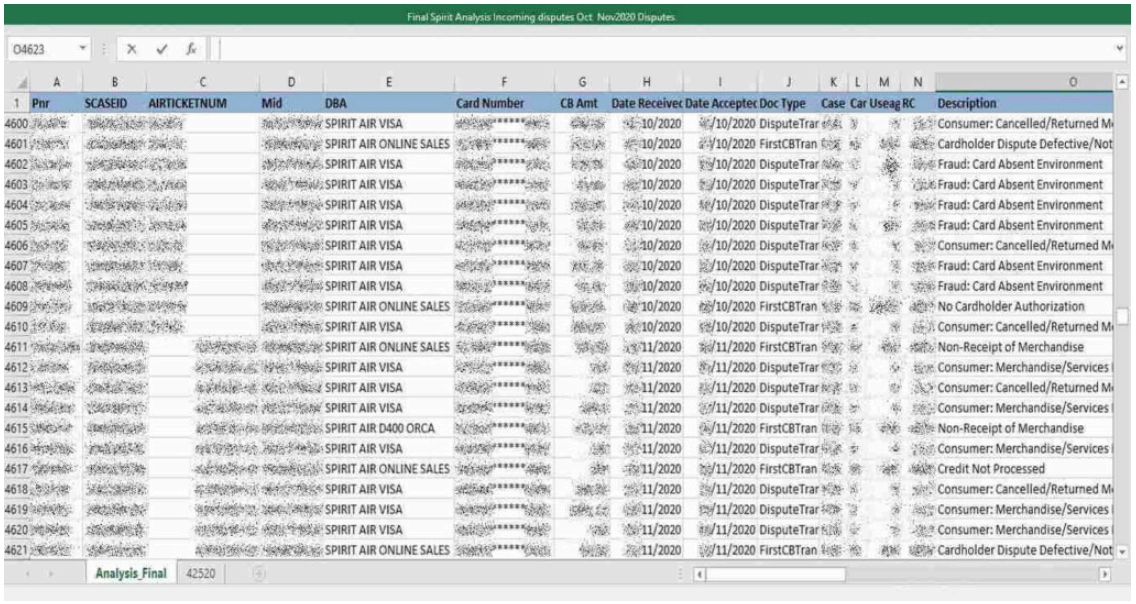
SPIRIT_part_1_CREDIT_CARD_REPORTS_2006_2016.7z
SPIRIT_part_1_CREDIT_CARD_REPORTS_2017.7z
SPIRIT_part_1_CREDIT_CARD_REPORTS_2018.7z
SPIRIT_part_1_CREDIT_CARD_REPORTS_2019_2021.7z
SPIRIT_part_1_CREDIT_CARD_REPORTS_other.7z

SPIRIT_part_1_CREDIT_CARD_REPORTS_2006_2016_filelist.txt
SPIRIT_part_1_CREDIT_CARD_REPORTS_2017_filelist.txt
SPIRIT_part_1_CREDIT_CARD_REPORTS_2018_filelist.txt
SPIRIT_part_1_CREDIT_CARD_REPORTS_2019_2021_filelist.txt
SPIRIT_part_1_CREDIT_CARD_REPORTS_filelist.txt

Headquarters: 2800 Executive Way, Miramar, Florida, 33025, United States
Phone: (954) 447-7920
Website: www.spirit.com
Employees: 8,938
Revenue: $3 Billion
Stock Symbol: SAVE

Source: KELA

On one of the sets, the crooks are leaking dispute records where one can see dates, credit card details (partial again), travel and ticket-related details, and a short description of the dispute. These details are obviously violating the privacy of the exposed individuals and open the door to spammers, scammers, phishing actors, and even extortionists, depending on the case.



Source: Suspectfile.com

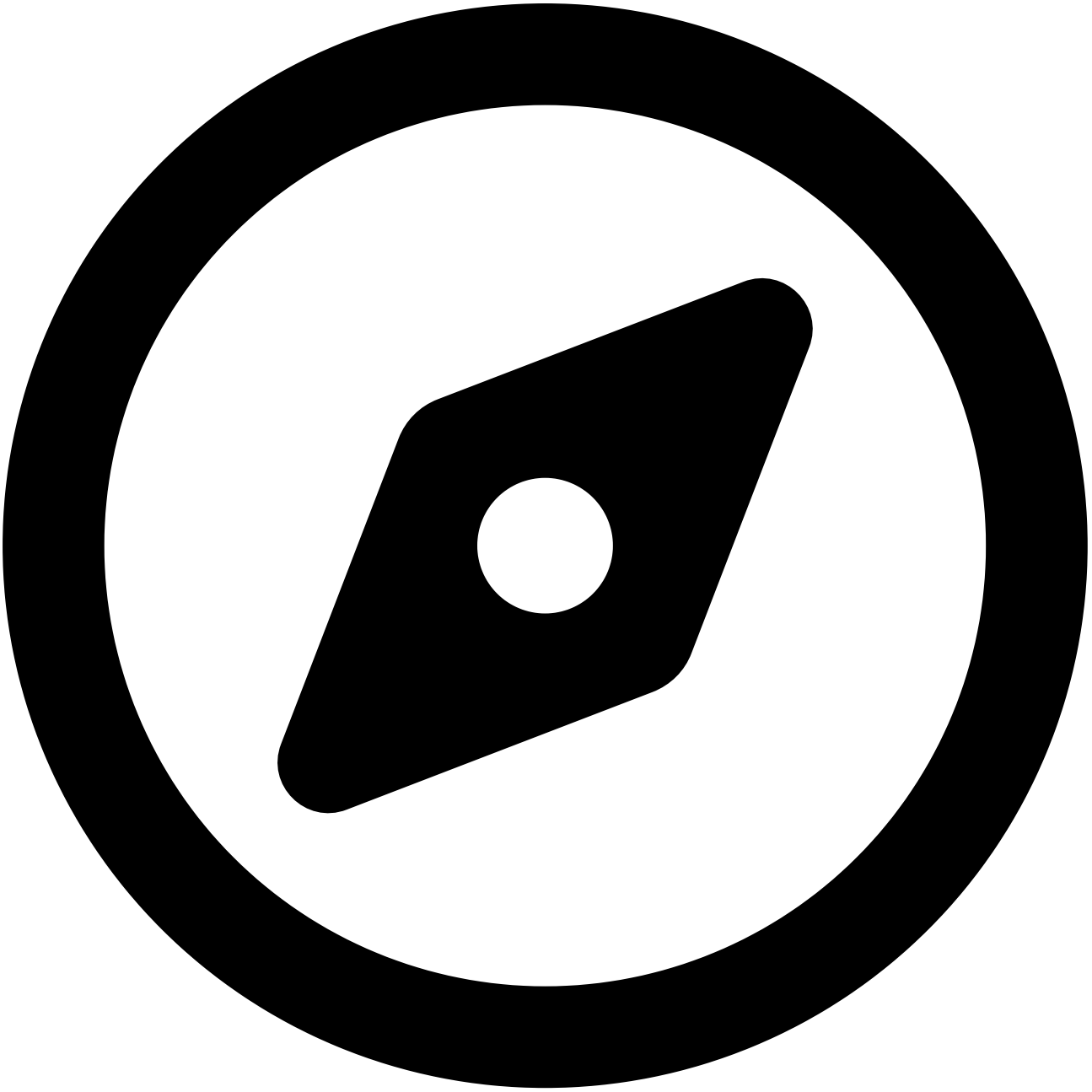
For this reason, one would expect Spirit Airlines to send out notices of a breach immediately. Still, when writing this, the low-cost airline hasn't made any public statements about the leaking data, hasn't distributed any notices to its customers, and hasn't even acknowledged any security incidents. So it wouldn't be far-fetched to suggest that the airline may not have realized the breach yet, so Nefilim actors could still be roaming on its network.

Further Reading

- SITA Announces Data Security Incident Affecting Several Airlines
- Almost All Airlines Are Vulnerable to Email Fraud Attacks
- Beware of 'AlumniLocker' and 'Humble,' Two New Ransomware Strains

It is very hard not to notice the encryption and system lock-down aspect of a ransomware infection. However, if Nefilim snatched the data from an unprotected database or a backup server that isn't used for "live" operations, then the "Spirit Airlines" IT team wouldn't notice it immediately. Also, considering that ultra-low-cost airlines cut expenses everywhere they can, especially during these times when the pandemic shattered their business, maintaining an active IT team that monitors everything would be improbable.

We have reached out to the customer service of Spirit Airlines, and we will update this piece as soon as we hear back from them.



Explore More

Most Popular


AWS

Source: https://www.technadu.com/nefilim-ransomware-group-hit-spirit-airlines/252679/