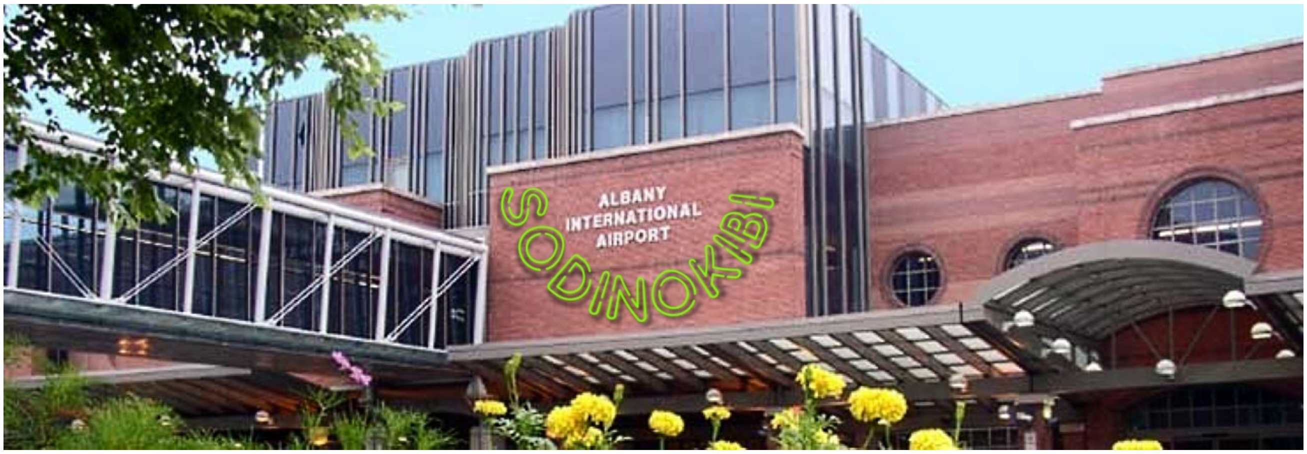
Sodinokibi Ransomware Hits New York Airport Systems

bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-new-york-airport-systems/

Sergiu Gatlan

By
Sergiu Gatlan

- January 10, 2020
- 03:27 PM
- 0



Albany International Airport's staff announced that the New York airport's administrative servers were hit by Sodinokibi Ransomware following a cyberattack that took place over Christmas.

Airport operations were not impacted by the ransomware attack and customers' financial or personal information was not accessed by the attackers according to a statement from airport officials per WNYT-TV.

No airline or TSA servers were affected in the incident, with airport officials saying that the vast majority of encrypted files being administrative documents and archived data.

The Albany County Airport Authority alerted the FBI and the New York State Cyber Command as soon as the attack was discovered, and also hired the services of ABS Solutions to help with the investigation.

MSP's breached systems used as a stepping stone

The attackers were able to infiltrate the New York airport's systems through the maintenance server of its managed service provider (MSP) Logical Net, a Schenectady, NY-based data center services and hosted cloud solutions provider.

The Sodinokibi Ransomware malware spread through the Albany County Airport Authority's network and also reached the backup servers.

Following the attack, airport CEO Philip Calderone told Times Union that "We have severed our relationship with LogicalNet."

Left without backups, the airport paid the "under six figures" ransom the attackers demanded. Albany International Airport's insurer reimbursed part of the ransom payment, with a $25,000 deductible to be recovered from Logical Net.

"Thanks to the fast action by our IT department, airport operations during one of the busiest travel periods of the year were not impacted and no passenger or airline data was acquired or accessed," Calderone added.

"Within hours the authority was able to resume all administrative functions with systems functioning as normal. We are grateful for the assistance provided by the New York State Cyber Command, the FBI and our consultant ABS."

BleepingComputer has contacted the Albany International Airport, Logical Net, and the Sodinokibi actors asking for more details but has not yet heard back.

High-profile Sodinokibi victims

International foreign currency exchange Travelex is another company hit by Sodinokibi on New Year's Eve, with the company being forced to shut down all its systems "to protect data and prevent the spread of the virus."

Following the complete systems shut down, customers were unable to use the site or the app for transactions at around 1,500 Travelex locations across the world.

While Travelex said in a statement that there is no evidence that any of its data was stolen in the attack, the Sodinokibi crew later told BleepingComputer that they copied over 5GB of personal and financial data, including but not limited to names, dates of birth, social security numbers, payment card info.

They also said that Travelex's backup files were also deleted and they will start publishing the stolen data if the company doesn't pay the $3 million ransom in seven days.

U.S. data center provider CyrusOne also had some of its systems encrypted by Sodinokibi Ransomware in early December 2019, while hundreds of dental practices using the online backup product DDS Safe had their files locked in August after the software's developer got infected through its cloud management provider, PercSoft.

Related Articles:

REvil ransomware returns: New malware sample confirms gang is back

US Senate: Govt’s ransomware fight hindered by limited reporting

US links Thanos and Jigsaw ransomware to 55-year-old doctor

US offers $15 million reward for info on Conti ransomware gang

The Week in Ransomware - May 6th 2022 - An evolving landscape

- AirPort
- New York
- Ransomware
- REvil
- Sodinokibi
- USA

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: