

New Jersey Synagogue Suffers Sodinokibi Ransomware Attack

By Lawrence Abrams

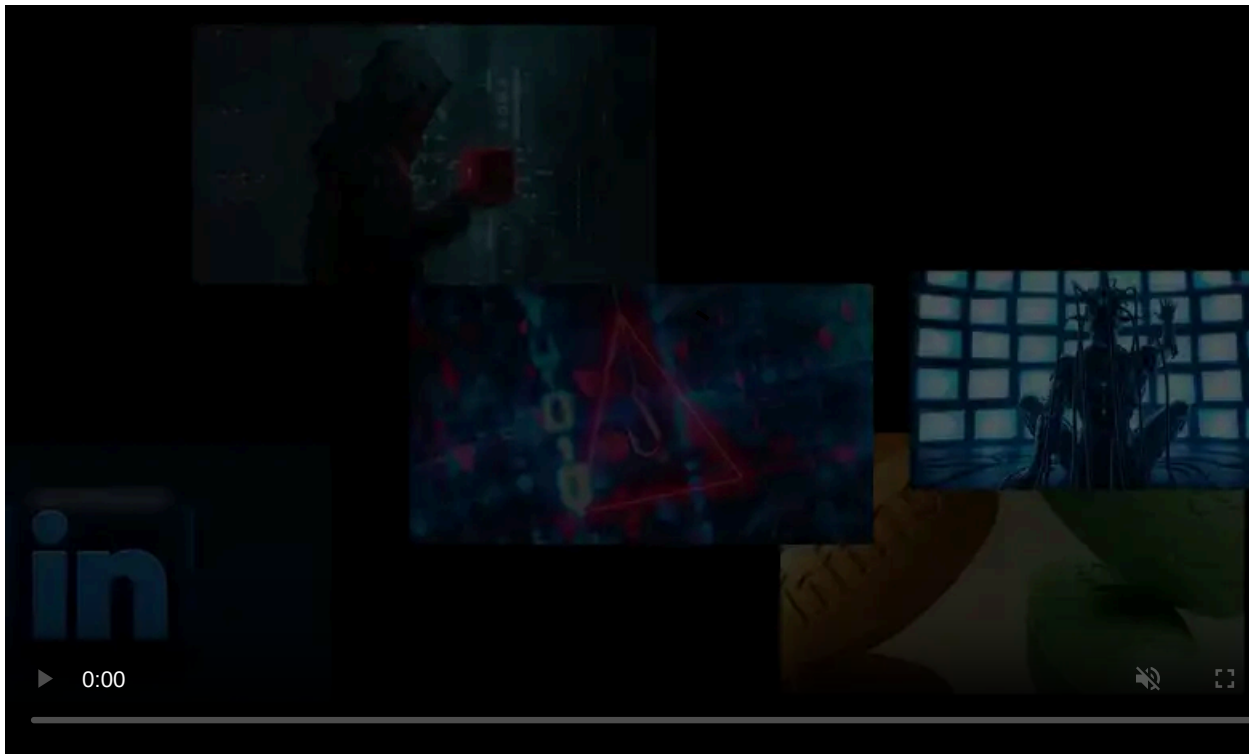
Published: 2020-01-18 · Archived: 2026-04-05 18:08:04 UTC



Temple Har Shalom in Warren, New Jersey had their network breached by the actors behind the Sodinokibi Ransomware who encrypted numerous computers on the network.

In an email seen by BleepingComputer, Temple Har Shalom informed their congregation that they discovered the ransomware attack on January 9th after staff had trouble connecting to the Internet

After checking their servers, they found that the Temple's files were encrypted and a ransom note was left behind. Other computers on the network had been encrypted as well.



Visit Advertiser website [GO TO PAGE](#)

"The encryption affected all of our server-based files and electronic data. We have a mechanical back up for those files and data, but the back-up was encrypted as well. Certain computers were affected in full. Others were unaffected and remain functional," the email from Temple Har Shalom stated.

A source familiar with the matter told BleepingComputer that Sodinokibi was demanding close to \$500,000 ransom to receive a decryptor for their network.

Temple Har Shalom states that they will be contacting congregation members for information needed to recreate encrypted files. This indicates that they have no intention of paying the ransom.

Like all ransomware victims, the temple feels violated by the attack but does not think they were targeted as a Jewish organization.

"The attack is violative of us as a community, though we have no reason to believe that we were targeted because we are a Jewish organization."

As Sodinokibi is known to steal files before encrypting them, they may have gained access to the personal data of congregants.

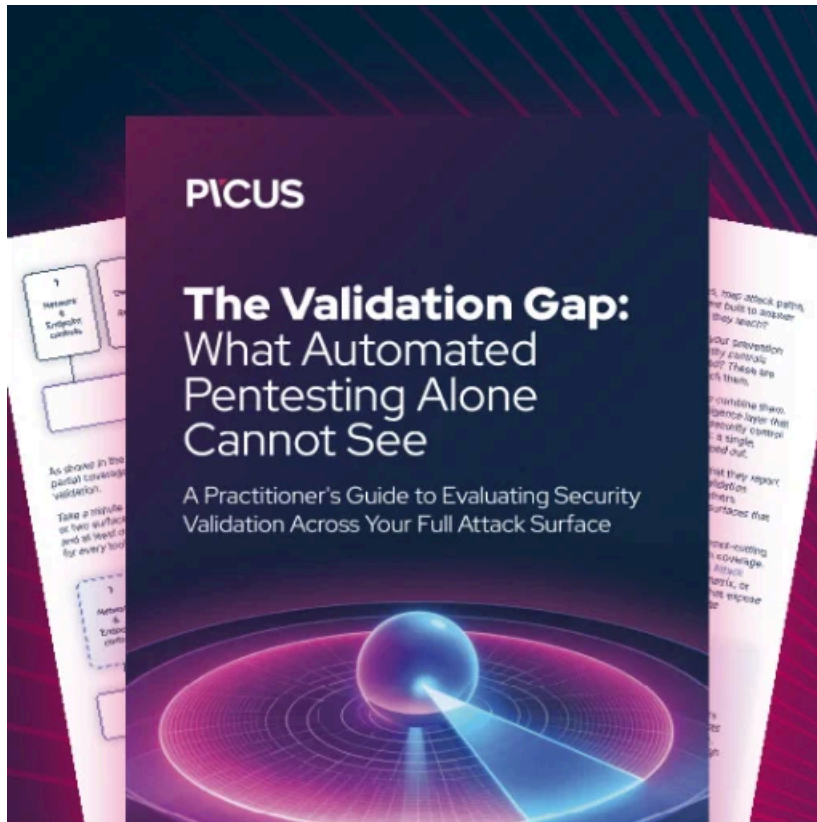
The synagogue states that this data may include a congregant's name, address, and email address, but they do not believe the attackers had access to their financial information.

"Beyond names, addresses and e-mail addresses of congregants, because of the way we segregate our files, we do not believe that confidential personal membership information (such as financial information) was accessed," the email stated. "Nonetheless, as we note above, be particularly mindful of phishing scams."

Temple members, though, should be on the lookout for targeted phishing emails using their personal information.

Sodinokibi has also [started to publicly leak the stolen data](#) of victims if a ransom is not paid. It is not known how much data, if any, was stolen from the temple or if they intend to publish it for non-payment.

BleepingComputer has contacted both the ransomware actors and the temple, but have not heard back at this time.



[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/new-jersey-synagogue-suffers-sodinokibi-ransomware-attack/>