Sodinokibi/REvil ransomware gang pwns British housing biz via suspected phishing attack

By Gareth Corfield

Published: 2020-11-06 · Archived: 2026-04-05 20:26:40 UTC

A social housing provider in Norwich, England, has said it was hit with the Sodinokibi ransomware following what it assumes was a successful phishing attack.

Flagship Group revealed last night that its systems were compromised by a "cyberattack" on Sunday, 1 November.

"Whilst the investigation is still going on we can confirm that the incident was caused by ransomware, known as Sodinokibi, via a suspected phishing attack," said Flagship in a statement on its partially pwned website.

An FAQ document [PDF] published by Flagship explained that an on-premises data centre was infected by the ransomware, "compromising some personal staff and customer data."

The attack is said to have been halted in its tracks, with the usual nameless "leading, independent cybersecurity firm" along with police and the National Cyber Security Centre all gazing into the breach together.

"As we have not engaged with the criminals we are not aware of a ransom demand," Rick Liddiment, Flagship Group's head of communications, told *The Register*.

The Information Commissioner's Office has been notified.

Threat analyst Brett Callow of ransomware recovery firm Emsisoft told *The Register* that not paying the Sodinokibi/REvil gang's ransom demands is the best bet.

"REvil is one of the multiple outfits which pilfers data and then solemnly swears it'll be deleted if the victim pays up ('Of course we'll delete it, Guv. You can trust us.')," he said. "However, to the surprise of absolutely nobody, it turns out the criminals can't be trusted and do not delete the data after ransoms are paid. Instead, they use it as leverage to attempt to extort money for a second time. The bottom line is that it makes no sense for companies to pay for the promise of deletion. You can't buy your way out of a data breach."

Agreeing with Callow, Jake Moore, a cybersecurity specialist from Slovakian infosec firm ESET, told *The Register*: "Regardless of how quickly a company responds to a ransomware attack, data will be encrypted and effectively lost. Frustratingly, the standard cybercriminal doesn't just stop there these days and will attempt to extract data too, which they seem to have successfully achieved here.

"However, although companies are quick to highlight how they take their customer privacy and security seriously, the best course of action is to be proactively prepared for an attack and even expect an attack like this to happen."

The crew operating this particular ransomware strain are known to the public by two names. Earlier this year REvil published passport scans of staff from a British firm that managed to shrug off an infection and ransom

demand. Its modus operandi is to encrypt and exfiltrate files, demand a ransom and then to auction stolen files to other criminals, something it leveraged earlier this year after claiming to have hacked a US law firm.

Under their Sodinokibi moniker, the gang also took down foreign exchange firm Travelex, contributing to the financial firm collapsing into administration this summer. ®
