# Ransomware Operators Demand $14 Million From Power Company

By Ionut Arghire

Published: 2020-07-02 · Archived: 2026-04-05 13:51:54 UTC

**The threat actor behind the Sodinokibi (REvil) ransomware is demanding a $14 million ransom from Brazilian-based electrical energy company Light S.A.**

The company has confirmed that it was hit with a cyberattack without providing specific information on the type of compromise, but AppGate's security researchers, who have obtained a sample of the malware believed to have been used in the attack, are confident that the incident involves the Sodinokibi ransomware.

"Although we can't confirm that this was the exact same file used in the attack, the evidence points to being connected to the Light SA breach, such as the ransom price, for example," AppGate notes.

According to the researchers, someone from within the company submitted the same sample to a public sandbox, likely in an attempt to "understand how it works."

Analysis of the configuration of the malware revealed information on the threat actor, the campaign ID, as well as the URL that the victim is asked to access for instructions.

On that page, which is hosted on the deep web, the victim is informed that they need to pay a ransom of 106,870.19 XMR (Monero) by June 19. The deadline, however, has passed, and the amount doubled, to 215882.8 XMR, which amounts to $14 million.



The same web page reveals information about the attackers, clearly mentioning the name Sodinokibi, and attempts to persuade the victim to pay the ransom by promising full decryption of the affected data.

“The whole attack looks very professional, the web page even includes a chat support, where the victim can speak directly with the attacker,” the researchers note.

Available under the RaaS (Ransomware-as-a-Service) model, Sodinokibi is operated by a threat actor likely affiliated to “Pinchy Spider,” the group behind the GandCrab ransomware.

While investigating the malware itself, AppGate discovered that it includes functionality to escalate privileges by leveraging 32-bit and 64-bit exploits for the CVE-2018-8453 vulnerability in the Win32k component of Windows.

“Unfortunately, there is no global decryptor for the family, which means that the attacker’s private key is required to decrypt the files,” AppGate also notes.

**Related: Sodinokibi Ransomware Operators Target POS Software**

**Related: Hackers Leak Data Stolen From UK Electricity Market Administrator Elexon**

**Related: Hackers Threaten to Leak Files Stolen From Australian Beverage Firm Lion**

---