REvil ransomware gang publishes 'Elexon staff's passports' after UK electrical middleman shrugs off attack

By Gareth Corfield

Published: 2020-06-01 · Archived: 2026-04-05 16:54:43 UTC

The REvil/Sodinokibi ransomware gang has just published what it claimed were files stolen from UK power grid middleman Elexon.

As reported here, the company was hacked two weeks ago.

The stolen data was published on REvil's Tor webpage as a cache of 1,280 files, which we understand include documents that appeared to be passports of Elexon staff members and an apparent business insurance application form. *The Register* has not verified whether the cache, in a .rar file, contains further information intended to harm Elexon and its staff.

Elexon said at the time of the "cyber attack" in mid-May that it had identified the "root cause" and was "taking steps to restore" its IT systems.

Responsible for a key financial part of the UK's part-privatised electricity markets, Elexon tots up forecast electrical demand from the whole nation in half-hour blocks. It then reconciles the forecast against actual demand and electrical generation supplied to the National Grid. Cash then flows either from the grid to generators (in cases where supply exceeded demand, so the forecast was wrong) or in the other direction, where underperforming power generators pay the grid for not supplying enough at the right times.

Elexon did not immediately respond to *The Register*'s request for comment. Judging by its previous responses, it appears the company shrugged off the ransomware attack and simply rebuilt its IT infrastructure from backups, ignoring the criminals' demands to pay them lots of money.

Today's disclosures, if genuine, could be interpreted as revenge for being snubbed – though if this is what happened, of course, Elexon absolutely did the right thing by refusing to engage.

Brett Callow of infosec biz Emsisoft told *El Reg*: "In the past, ransomware crims' graft and grift would have all been for naught if the company they'd hit was able to restore its data from backups. But half-inching a copy of companies' information provides them with additional leverage and monetisation options.

"Companies with usable backups may still be willing to pay to prevent their data being published and, even if they are not, the data may be sold to competitors or sold and traded with other criminals."

Callow also speculated, based on previous reports elsewhere, that Elexon may have been running an unpatched Pulse Secure VPN server, although this is of course unconfirmed.

The REvil group has also claimed to have hacked a bunch of organisations, recently including a law firm whose clients included Madonna, Elton John and Lady Gaga among others. The gang's modus operandi is simple: pay up or we publish.

As a financial organisation, Elexon's woes have no impact on electrical generation or supply. Despite REvil's rage, the lights will remain resolutely on across the UK tonight. ®
