Scottish Environment Protection Agency refuses to pay ransomware crooks over 1.2GB of stolen data

By Paul Kunert

Published: 2021-01-18 · Archived: 2026-04-05 13:49:55 UTC

Scotland's environmental watchdog has confirmed it is dealing with an "ongoing ransomware attack" likely masterminded by international "serious and organised" criminals during the last week of 2020.

"On Christmas Eve, the Scottish Environmental Protection Agency (SEPA) confirmed that it was responding to a significant cyber-attack affecting its contact centre, internal systems, processes and internal communications," it revealed.

Efforts to respond to the assault continue at the agency, which probes allegations of land, water and air pollution, and the "matter is subject to a live criminal investigation and the duty of confidence is embedded in law," it said.

Some "internal systems and external data products" remain offline as the investigation proceeds but the priority regulatory, monitoring, flood forecasting and warning services "are adapting and continue to operate," SEPA added.

Staff schedules, some specialist reporting tools, systems and database are down and out, potentially for a "protracted period". Contact centres and web help services are being gradually restored, and regulatory teams are focusing on the most important workloads.

Certain systems have been "isolated" but SEPA warned that security experts working with the Scottish government, Police Scotland and the National Cyber Security Centre "confirm we remain subject to an ongoing ransomware attack likely to be by international serious and organised cyber-crime groups intent on disrupting public services and extorting public funds."

It is now clear that "recovery may take a significant period" and a "number of SEPA systems will remain badly affected for some time, with new systems required".

So what's been pinched? Security specialists going over the attack and its impact have so far identified a loss of around 1.2GB worth of data, an indication that "at least four thousand files may have been accessed and stolen by criminals", SEPA said.

"Whilst we don't know and may never know the full detail of the 1.2GB of information stolen, what we know is that early indications suggest that the theft of information related to a number of business areas," it added.

This was said to include publicly available regulated site permits; authorisation and enforcement notices; some SEPA corporate plans; project data involving procurement awards; project information connected to commercial work with international partners; and staff information – though "limited sensitive data was accessed".

SEPA has yet to identify the crew behind the attack but, according to Bank Info Security, the Conti ransomware gang appears to have published the data stolen.

Brett Callow, a threat researcher with Emsisoft, told The Register: "Conti may well be operated by the group responsible for Ryuk. There are similarities in code, note and distribution mechanisms. Additionally, Conti emerged during a period of decreased Ryuk activity, which also suggested that it may be a successor for Ryuk. That said, there has since been an uptick in Ryuk activity, with no corresponding decrease in Conti activity which could, perhaps, indicate the group has splintered."

SEPA CEO Terry A'Hearn said the agency will not pay.

"We won't be using public funds to pay ransom to criminals. This has commonly happened to other organisations, so we are following the experience that others have had, the advice from the police. We will recover our ability to have data and systems, that may take some time but others have been through this," he told BBC Scotland.

"We will not be using public funds to pay ransom. We are already in the first three weeks re-establishing our ability to carry out our critical services, and over the next few weeks and months we will continue to do that so that we can protect the environment." ®
