Lockbit Ramps Up Attacks on Public Sector

By Phil Muncaster

Published: 2022-07-26 · Archived: 2026-04-06 02:52:19 UTC

The prolific Lockbit ransomware gang appears to have claimed another two scalps in recent days: the Canadian town of St Marys and the Italian tax agency.

The local administration at St Marys explained in an update on Friday that the attack occurred last Wednesday, locking an internal server and encrypting data on it.

“Upon learning of the incident, staff took immediate steps to secure any sensitive information, including locking down the town’s IT systems and restricting access to email. The town also notified its legal counsel, the Stratford Police Service and the Canadian Centre for Cyber Security,” a statement read.

“The town is now working with cyber incident response experts to investigate the source of the incident, restore its back up data and assess the impacts on its information, if any. These experts are also assisting staff as they work to fully unlock and decrypt the town’s systems, a process that could take days.”

Critical local services, including fire, police, transit and water/wastewater systems were apparently unaffected by the incident, but it’s unclear if any sensitive data was stolen in the raid.

That’s not the case in Italy, where an attack by affiliates using the Lockbit ransomware reportedly resulted in the theft of 78GB of data.

Hackers targeted Italian revenue agency l'Agenzia delle Entrate, so that data could theoretically contain highly sensitive personal and financial information.

According to the local ANSA news wire, the revenue service has asked Italy’s Sogei IT agency to look into reports that the threat actors have given it five days to pay up or else risk the files being made public.

Mike Varley, threat consultant at Adarma, argued that public sector organizations are often targeted because hackers believe they’re more likely to pay.

"Organizations seeking to improve their overall ransomware resilience should be proactively asking themselves, ‘where are we most vulnerable to external threats?’ ‘what are we protecting?’ and ‘where are those assets housed?,’ he added.

“Security teams need to be actively hunting out control gaps and closing them by either tweaking existing controls, through technology acquisition, undertaking additional monitoring or by doing all three.”