Nine Entertainment warns ransomware recovery 'will take time'

By Ry Crozier

Published: 2021-03-29 · Archived: 2026-04-05 14:35:36 UTC

Nine Entertainment warned Monday night that it would be some time before it could fully restore core systems and connectivity following a ransomware infection over the weekend.

Chief information and technology officer Damian Cronan said in a letter to staff that 9Technology - the company's IT organisation - had contained the attack, mostly by isolating the company's corporate network from the rest of the group's operations.

News of containment came after a report by *The Australian Financial Review* - which is owned by Nine - that pinned the infection on the MedusaLocker ransomware.

MedusaLocker first appeared in 2019 and attempts to establish persistence in targeted environments while also deleting any backups that it finds.

Cisco Talos Intelligence Group researchers said last year that MedusaLocker had several features not found in other malware variants, including the ability to "encrypt the contents of mapped network drives", "force network drives to be remapped so that their contents can also be encrypted", and "profile the network to identify other systems that can be used to maximise the likelihood of a ransom payment."

Nine has not officially confirmed whether MedusaLocker is the type of malware that was involved.

Cronan called the attack “significant, sophisticated and complex”.

The company has previously suggested it has not received a ransom demand, and security researchers are yet to see a public claim of the attack.

Nine CEO Mike Sneesby said that “a number of core systems remain offline”; Cronan added that connectivity between different business units, geographies and external partners had been disabled to prevent further spread of the malware.

Staff across Nine have been asked to “run a diagnostic on [their] laptop to ensure [the company has] isolated any infected workstreams.”

Cronan said the company is confident it has been able to “isolate the attacker and the specific destructive activity that was initiated.”

He did not say how bad the damage is, but sources told *iTnews* yesterday that potentially thousands of machines were impacted, either directly through infection or indirectly by being switched off.

“The consequence of this containment strategy is that our corporate network has been disconnected from the internet, and all internal networks separated from one another (e.g. broadcast from publishing, Sydney from Melbourne etc),” Cronan said in an email to staff.

“Other upstream and downstream providers have also been disconnected.

“This has been an effective strategy however, it also means several services that are dependent on the corporate network are not available.

“This will have a significant impact on business-as-usual processes across the organisation.”

Cronan said that 9Technology is working to recover its most critical aspects of service delivery as a priority.

These include “on-air and print operations, revenue-driven services, and other critical business services.”

Cronan warned that full recovery from the infection may not be quick.

“We will be carefully assessing how we bring back controlled levels of connectivity into the network with an emphasis on service restoration,” Cronan said.

“I want to be clear it will take time before all our systems are back up and running.”
