DoppelPaymer ransomware hits Newcastle University, leaks data

By Sergiu Gatlan

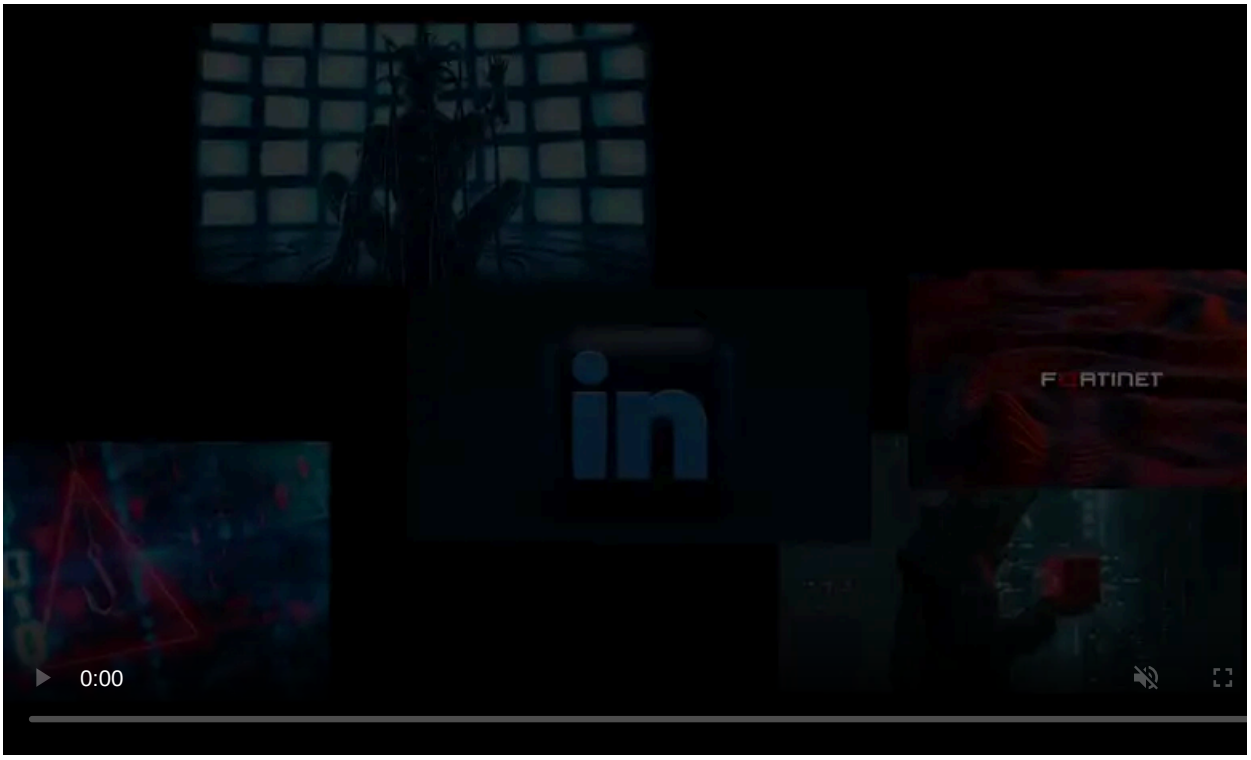
Published: 2020-09-07 · Archived: 2026-04-05 19:44:36 UTC

UK research university Newcastle University says that it will take several weeks to get IT services back online after DoppelPaymer ransomware operators breached its network and took systems offline on the morning of August 30th.

The attack is now investigated by the UK Police and the National Crime Agency in cooperation with the Newcastle University IT Service (NUIT).

Weeks of recovery efforts expected

"On Sunday 30 August 2020, we became aware that the University had suffered a serious cyber incident which is causing operational disruption across our networks and IT systems," the university said at the time.


0:00

"All University systems - with the exceptions of those listed in the communications (Office365 – including email and Teams, Canvas and Zoom) are either unavailable or available but with limitations.

The university hasn't yet decided if account passwords will also be reset but it says that it may do so based on internal support teams and third party consultants' recommendations.

In an update published today, more than a week since the initial attack, Newcastle University says that "[t]he nature of the problem means this will be an on-going situation for some time and ***it will take several weeks to address***."

> The investigation into the incident is still at an early stage. IT colleagues continue to **work hard on the systems recovery plan**, and to support the Police and the National Crime Agency with their enquiries. However, we will not be able to share further detail on the incident until this initial investigation has concluded. The ICO and Office for Students were notified within 72 hours of the cyber incident being detected. - Newcastle University spokesperson

Limited number of IT services available

According to the university, at the moment, many of its IT services are currently offline and will remain down "for the duration," while those that are operating could be taken down without notice during the recovery efforts.

Newcastle University also added in today's update that:

- Colleagues may lose access to their IT accounts without notice and they may not be re-enabled quickly.
- NUIT may need access to any IT system you keep or use.
- We may need to remove PCs, servers or other devices if we find out they are impacted, in order to carry out detail investigations

During the ongoing investigations, students and employees will only have access to a limited set of IT services including Office365 (email, Office apps, and Teams comm channels), SAP core services via the client (the web interface is still down), and Zoom.

The university also advised students and staff to copy essential files from the uni's share drive to their OneDrive accounts.

"Where appropriate, we advise you to copy and save business-critical data and files to your OneDrive," the university said. "New files can also be created and saved on your OneDrive. Please only transfer essential files and do not copy or send files to your personal accounts."

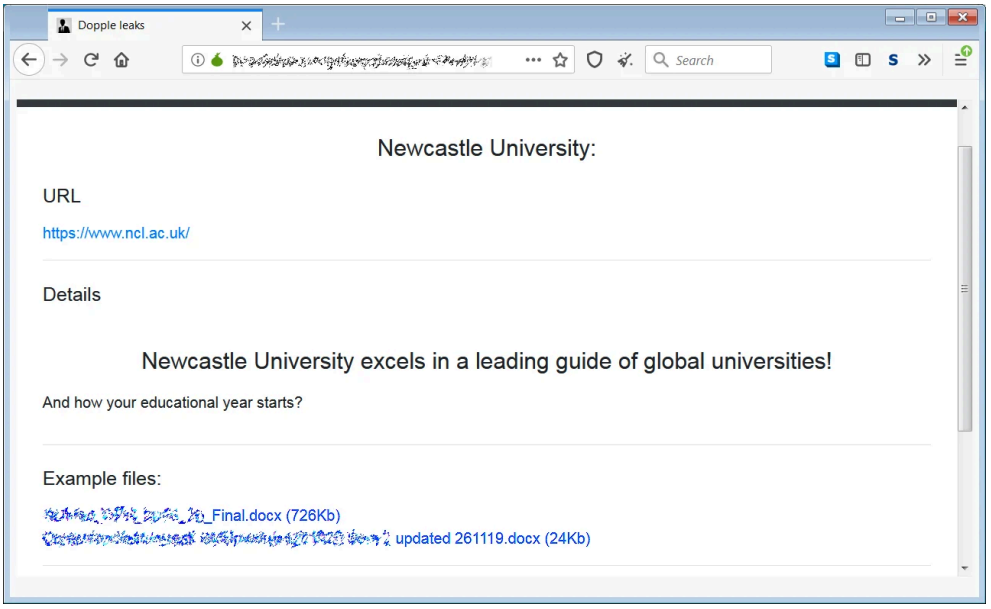
If you work at Newcastle University or know someone working there with first-hand information on this incident, you can confidentially contact us on Signal at +16469613731.

DoppelPaymer claiming to be behind the attack

While Newcastle University has only shared that they have suffered a cyber-attack, the DoppelPaymer ransomware operators are claiming to be responsible.

They have also shared 750Kb worth of stolen data as proof on their data leak site 'Dopple Leaks,' a tactic they've adopted from Maze Ransomware since February 2020.

DoppelPaymer is a ransomware operation known for attacking enterprise targets since at least mid-June 2019 by gaining access to admin credentials and using them to compromise the entire network to deploy the ransomware payloads to all devices.



They are also known for asking for large ransoms since their attacks have been known to encrypt hundreds and even thousands of systems on their victims' networks.

In November 2019, Mexico's state-owned oil company PEMEX (Petróleos Mexicanos) suffered a DoppelPaymer ransomware attack, with the gang asking for $4.9 million worth of bitcoins as a ransom for decrypting files.

DoppelPaymer got its name from BitPaymer, with which it's sharing large portions of code but its operators have added numerous upgrades to the malware including a threaded encryption process for quicker operation.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
