K12 online schooling giant pays Ryuk ransomware to stop data leak

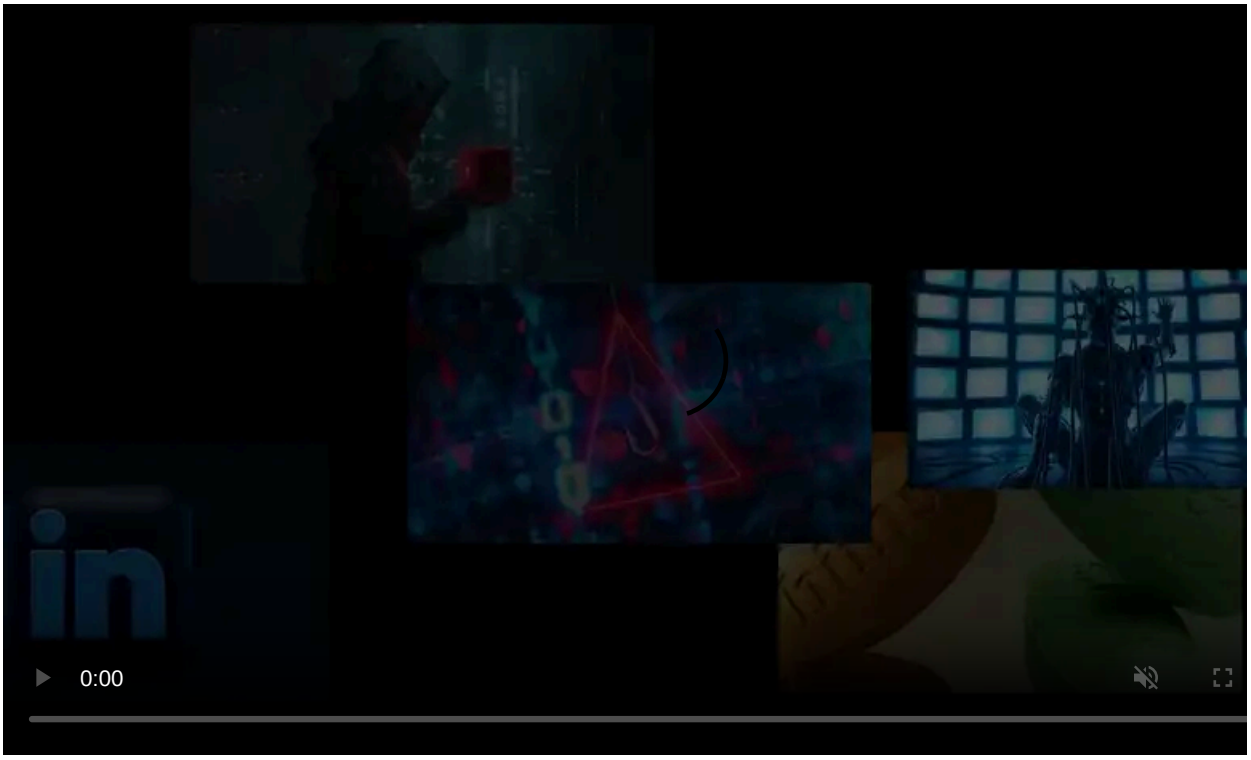
By Lawrence Abrams

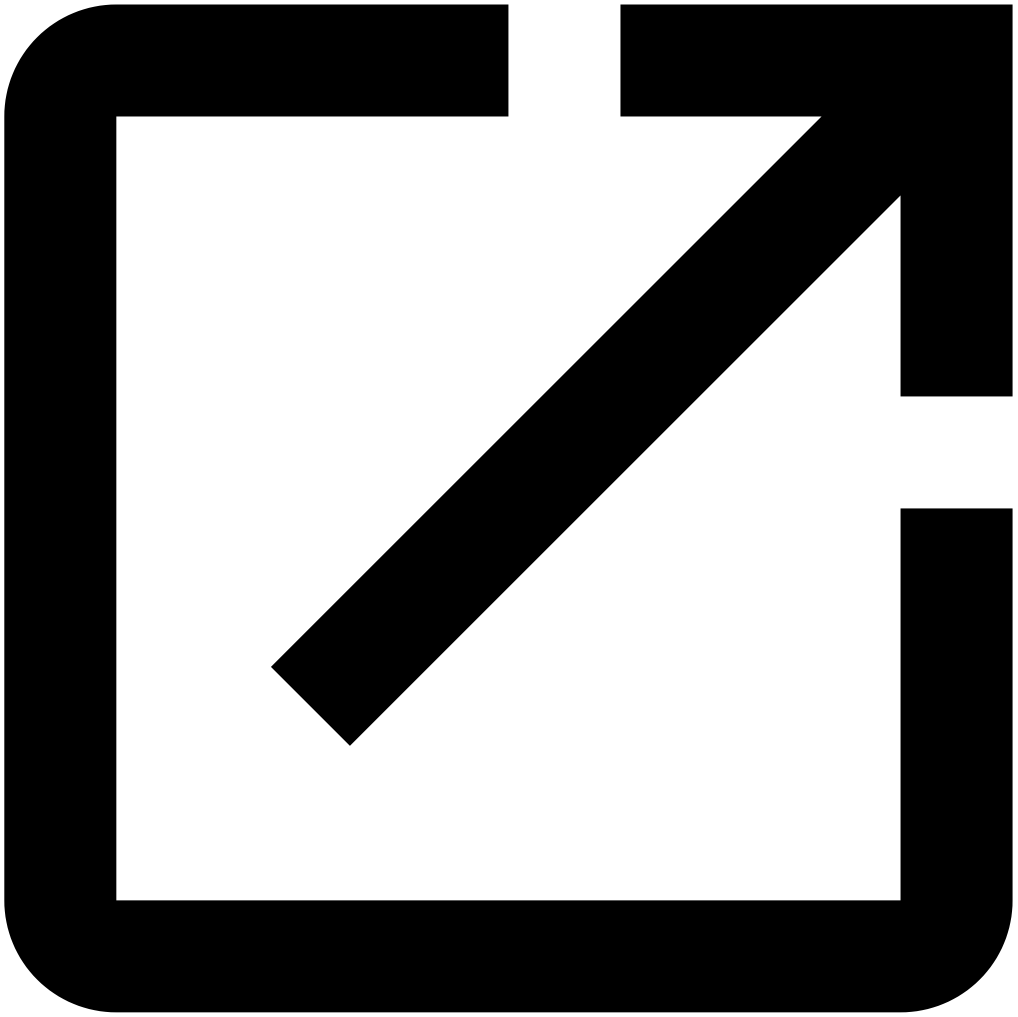
Published: 2020-12-02 · Archived: 2026-04-05 16:58:06 UTC

Online education giant K12 Inc. has paid a ransom after their systems were hit by Ryuk ransomware in the middle of November.

K12 creates tailored online learning curriculums for students to learn from home while in kindergarten through 12th grade. Over 1 million students have utilized K12 to learn from home rather than in traditional public school environments.

K12 announced this week that they suffered a ransomware attack in mid-November that caused them to lock down some of their IT systems to prevent the attack's spread.


0:00



"In mid-November, we detected unauthorized activity on our network, which has since been confirmed as a criminal attack in the form of ransomware. Upon identifying unusual system activity, we quickly initiated our response, taking steps to contain the threat and lock down impacted systems, notifying federal law enforcement authorities, and working with an industry-leading third-party forensics team to investigate and assist with the incident," K12 told BleepingComputer in a statement.

This attack did not impact their online Learning Management System (LMS) to deliver educational content or affiliated charter schools. They also state that most major systems, including payroll, accounting, and enrollment systems, were unaffected.

However, the attackers did gain access to some back-office systems that contained student data and other information.

K12 paid Ryuk ransom to prevent data leak

Sources in the cybersecurity industry have told BleepingComputer that the Ryuk ransomware hit K12 Inc.

When performing attacks, the Ryuk ransomware gang is known to steal unencrypted data before encrypting devices. This data is then used in 'double-extortion' attempts where the ransomware gang threatens to leak stolen data if a ransom is not paid.

As the leaking of student data would be disastrous for any company, K12 utilized their cyber insurance to pay the Ryuk ransom. It is not known how much was paid, but as part of the payment, K12 was assured by the threat actors that they would not release stolen data.

"We have already worked with our cyber insurance provider to make a payment to the ransomware attacker, as a proactive and preventive step to ensure that the information obtained by the attacker from our systems will not be released on the Internet or otherwise disclosed.."

"While there is always a risk that the threat actor will not adhere to negotiated terms, based on the specific characteristics of the case, and the guidance we have received about the attack and the threat actor, we believe the payment was a reasonable measure to take in order to prevent misuse of any information the attacker obtained," K12 announced.

Ransomware negotiators have been increasingly warning that threat actors are not always keeping their promises regarding stolen data.

Due to this, ransomware negotiation firm Coveware tells victims that it does not make sense to pay a ransom as there is no way to know for sure if data will be deleted or misused in the future.
