University of Utah pays $457,000 to ransomware gang

By Catalin Cimpanu

Published: 2020-08-21 · Archived: 2026-04-06 03:13:17 UTC

Image via University of Utah; Composition: ZDNet

The University of Utah revealed today that it paid a ransomware gang $457,059 in order to avoid having hackers leak student information online.

The incident is the latest in a long string of ransomware attacks where criminal groups steal sensitive files from the hacked companies before encrypting their files; and in case victims refuse to pay, threaten to release the stolen documents as a second extortion scheme.

Unfortunately, this is exactly what happened in the case of the University of Utah. In a statement posted on its website today, the university said it actually dodged a major ransomware incident and that the hackers managed to encrypt only 0.02% of the data stored on its servers.

The university said its staff restored from backups; however, the ransomware gang threatened to release student-related data online, which, in turn, made university management re-think their approach towards not paying the attackers.

"After careful consideration, the university decided to work with its cyber insurance provider to pay a fee to the ransomware attacker," the university said today.

"This was done as a proactive and preventive step to ensure information was not released on the internet.

"The university's cyber insurance policy paid part of the ransom, and the university covered the remainder. No tuition, grant, donation, state or taxpayer funds were used to pay the ransom," University of Utah officials added.

University officials also provided details about the attack today, such as the date when it took place (July 19, 2020), and what part of the network it impacted (the network of the university's College of Social and Behavioral Science [CSBS]).

However, the university did not reveal which ransomware gang was behind the attack.

All signs point to NetWalker

Brett Callow, a threat analyst at cyber-security firm Emsisoft, told *ZDNet* today that, although lacking concrete evidence, the NetWalker ransomware gang is most likely behind the attack.

This particular group, which is believed to have made more than $25 million from ransom payments this year, has been behind a recent wave of attacks against university networks, such as the attacks against Michigan State, the University of California at San Francisco (paid $1.14 million), Columbia College Chicago, and the City University of Seattle.

But Callow also took issue with University of Utah officials paying the attackers to stop a data leak; warning against such practice has little benefits.

"Paying ransoms to prevent data being published seems to make little sense," Callow told us.

"All what organizations are paying for in this scenario is a pinky promise from a bad faith actor that the stolen data will be destroyed. Whether the groups do ever destroy data is something only they know, but I suspect they do not. Why would they? They may be able to monetize the information at a later data or use it for spear phishing or identity theft."
