Fairfax County schools hit by Maze ransomware, student data leaked

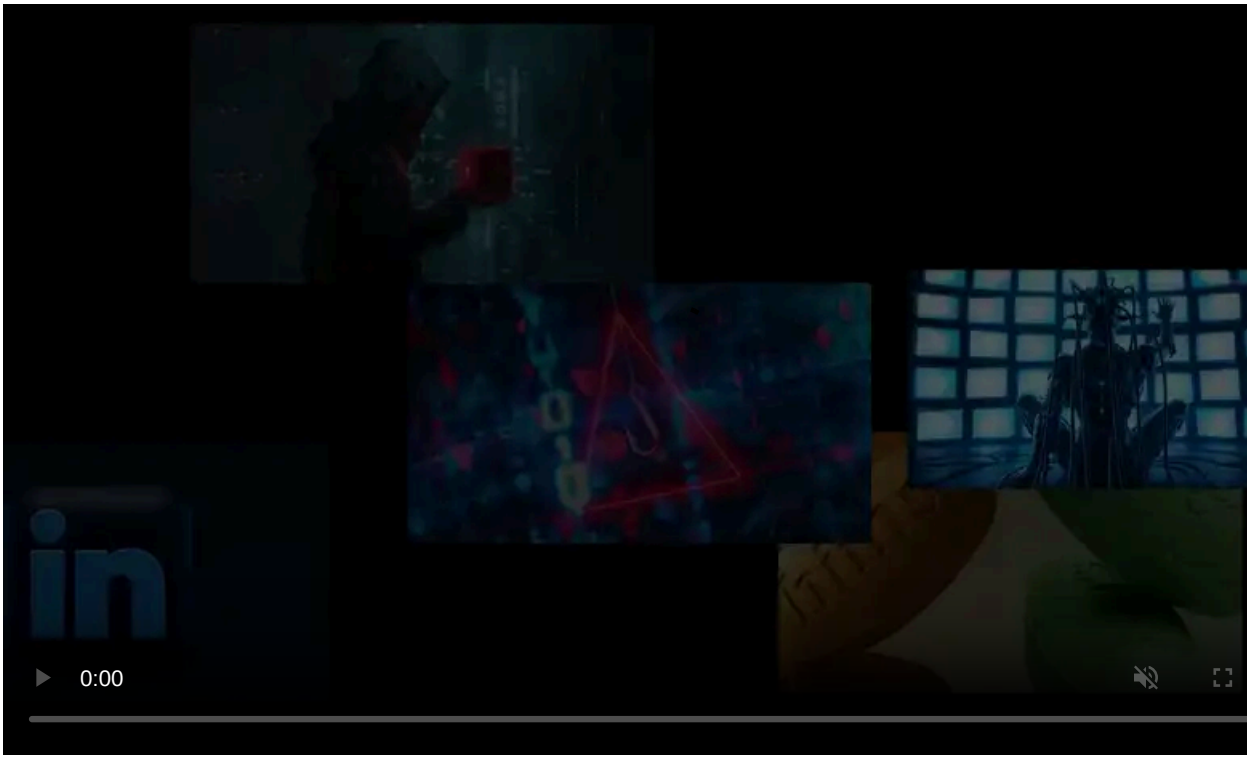
By Sergiu Gatlan

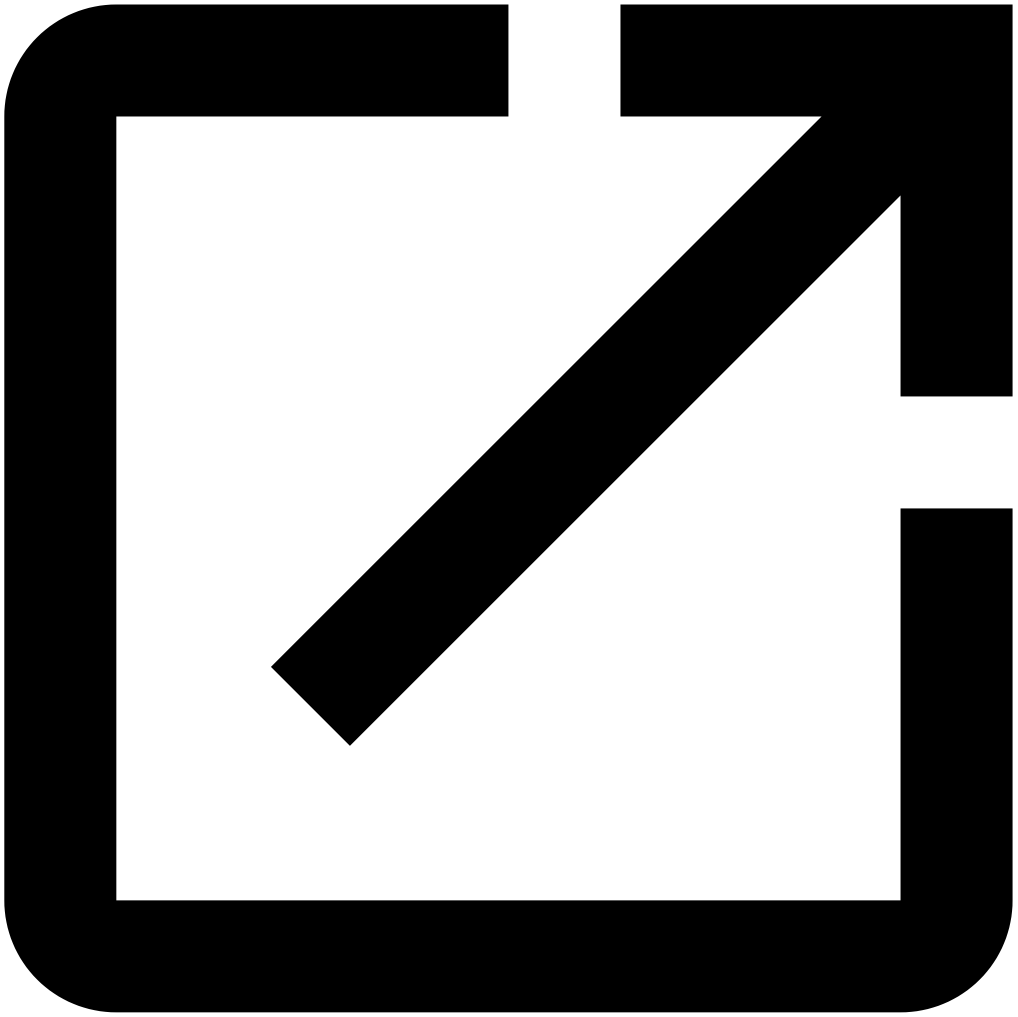
Published: 2020-09-12 · Archived: 2026-04-05 18:13:32 UTC

Image: Rubén Rodriguez

Fairfax County Public Schools (FCPS), the 10th largest school division in the US, was recently hit by ransomware according to an official statement published on Friday evening.

The school district is also the largest in the Baltimore-Washington Metropolitan Area and it has a budget of $3.1 billion approved for 2021.


0:00



FCPS has over 188,000 current students and approximately 25,000 full-time employees working in 198 schools and centers within the U.S. commonwealth of Virginia.

FBI involved in the ongoing investigation

At the moment the exact date when the ransomware impacted FCPS's network is not yet known but the school district says that it collaborating with the FBI to determine what ransomware gang is behind the attack.

"FCPS recently learned that ransomware was placed on some of our technology systems. We are taking this matter very seriously and are working diligently to address the issue," the statement reads.

"We currently believe we may have been victimized by cyber criminals who have been connected to dozens of ransomware attacks in other school systems and corporations worldwide."

FCPS has also retained the services of external security experts to help with the ongoing investigation, as well as to get the affected systems back online and determine the full scope of the attack.

"FCPS is committed to protecting the information of our students, our staff, and their families," the school division added.

"We will work with law enforcement to the fullest extent to prosecute any individuals or groups that attack our systems."

BleepingComputer has reached out to FCPS for additional details on the attack but had not heard back at the time of this publication.

Attack claimed by the Maze ransomware gang

FCPS did not reveal the identity of the ransomware operators who encrypted their systems but it said says that they are known for dozens of attacks on other school districts and enterprises.

However, the attack on FCPS was already claimed by the Maze ransomware operators who have already leaked 2% (an archive of roughly 100MB) of what they claim to be data stolen from the Virginia school division's servers.

The data leaked by Maze contains information on some of the school district's students, as well as administrative documents and what looks like an LSASS dump that can be used to extract Windows credentials.

Name	Size	Packed Size	Modified
Admin	403 457	355 726	2020-09-10 1...
Archive	206 162	104 582	2020-09-10 1...
ETL Environments	13 312	10 424	2020-09-10 1...
Issues	174 025	160 440	2020-09-10 1...
Metadata Queries	18 566	15 613	2020-09-10 1...
PAM	1 396 440	1 133 438	2020-09-10 1...
Portal	43 008	6 435	2020-09-10 1...
Rulepoint	3 554 776	2 685 193	2020-09-10 1...
Upgrade	535 498	255 801	2020-09-10 1...
Upgrade_to_10.0	1 501 285	1 161 785	2020-09-10 1...
Upgrade_to_10.2	540 425	393 693	2020-09-10 1...
Upgrade_to_10.4.1	36 073	30 290	2020-09-10 1...

Some of the data leaked by Maze

Maze ransomware is the one behind the new ransomware tactic of stealing victims' files before encrypting systems and using them as leverage to pressure the victims into paying the ransoms.

Maze attacks were first spotted in May 2019 and, since then, its operators have escalated their attacks via exploit kits, spam, and network breaches.

In November 2019, Maze was the first to publish a victim's stolen data, in that case, files stolen from Allied Universal, for not paying the ransom.

Afterward, they started publishing the data for their victims via posts on hacker forums and, eventually, through their own dedicated leak site.

Maze are known to be behind behind numerous high profile attacks including ones against cyber insurer Chubb, Canon, business giant Xerox, LG Electronics, Conduent, IT services giant Cognizant, system-on-chip (SOC) maker MaxLinear, the City of Pensacola, and Banco BCR,

---