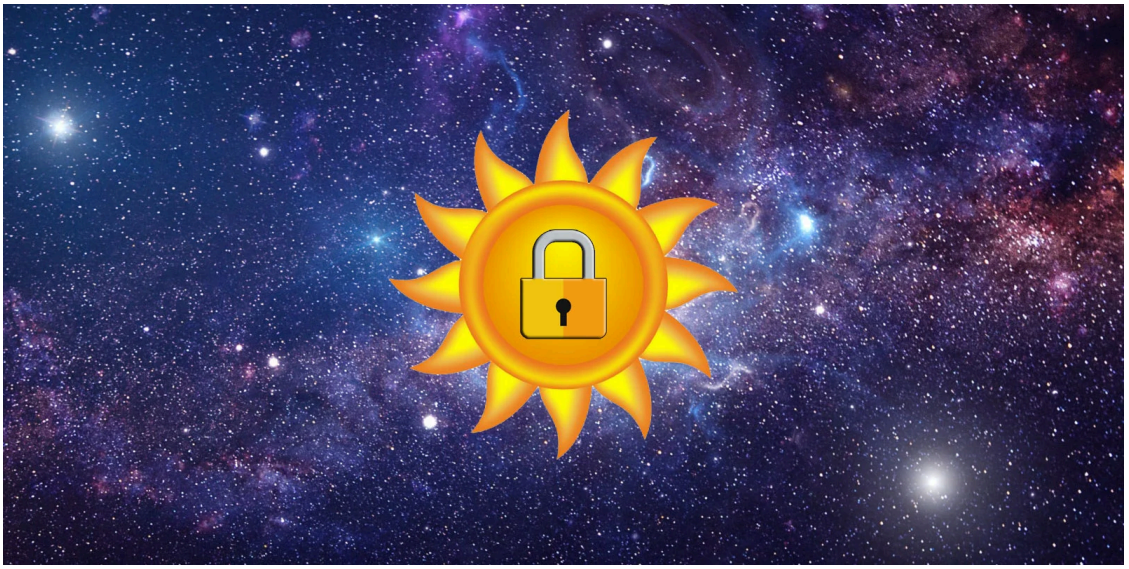
SunCrypt Ransomware shuts down North Carolina school district

By Lawrence Abrams

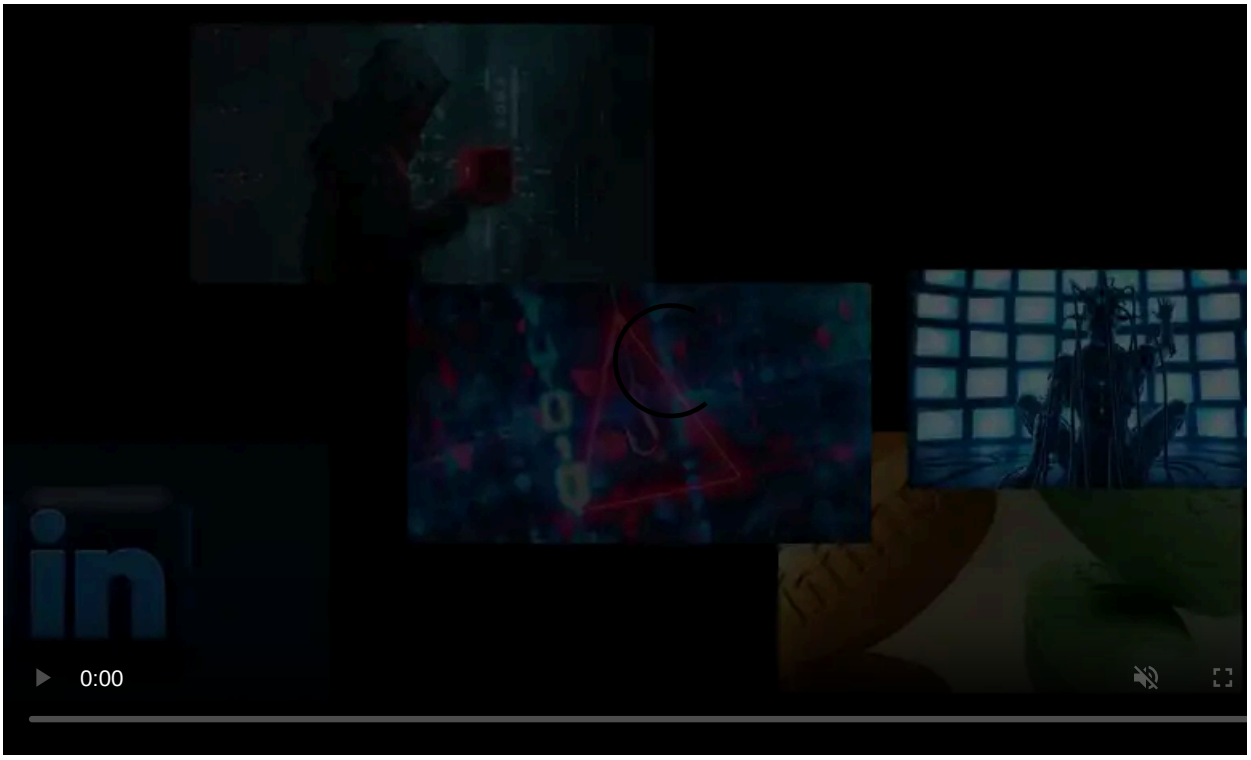
Published: 2020-09-04 · Archived: 2026-04-05 16:57:31 UTC

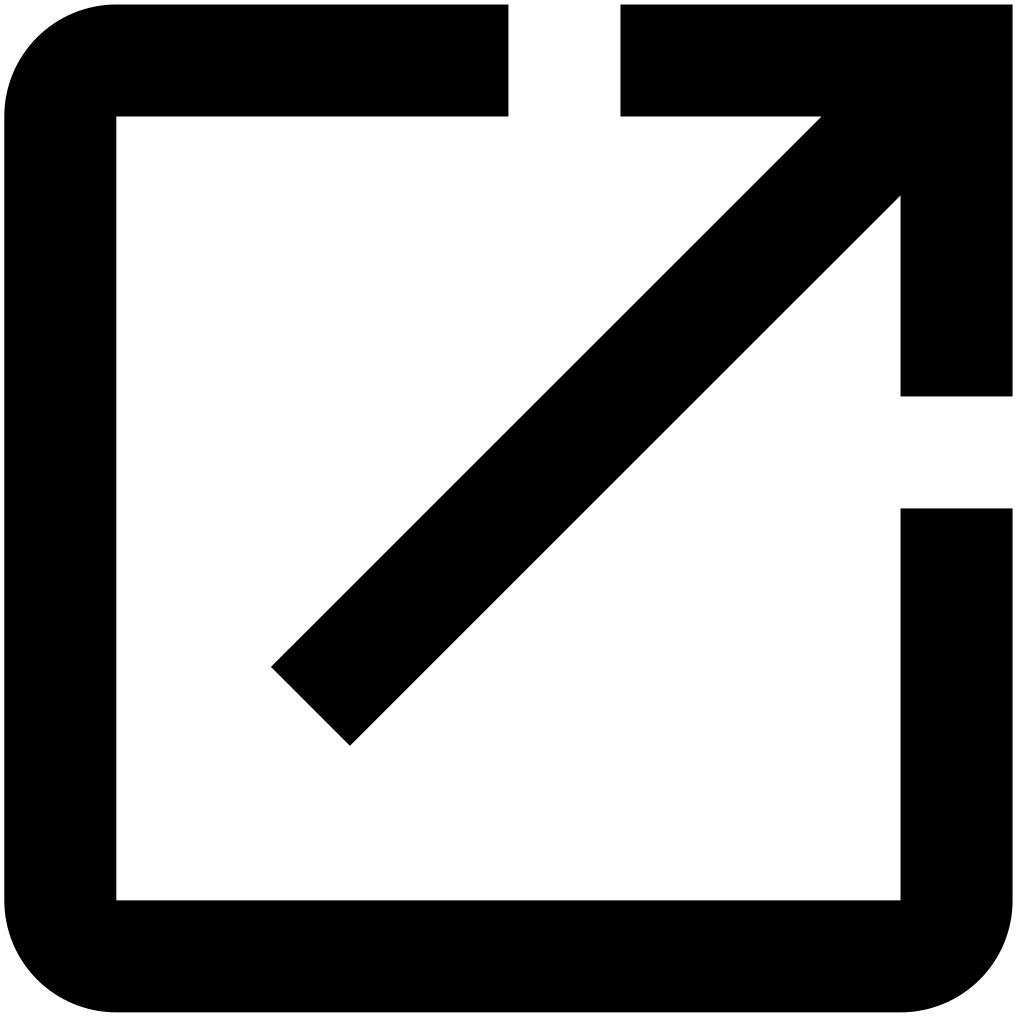


A school district in North Carolina has suffered a data breach after having unencrypted files stolen during an attack by the SunCrypt Ransomware operators, BleepingComputer has discovered.

The Haywood County School district in North Carolina announced that they had suffered a ransomware attack on August 24th, 2020, but had not stated what ransomware was used.

This attack caused the district to shut down its network and halt remote learning, which had started on August 17th.


0:00



Visit Advertiser websiteGO TO PAGE

"Our delay in restarting remote instruction is the uncertainty about the use of staff computers. We will know more when the forensic work is complete."

"We apologize for being unable to communicate as effectively as normal. Servers, Internet, and telephone services are still down in the school system. We will send another update at the end of the day," the Haywood County School District explained in their report to parents.

The school district has since resumed remote learning on August 31st, but with some school technology services still impacted.

Ransomware attack led to a data breach

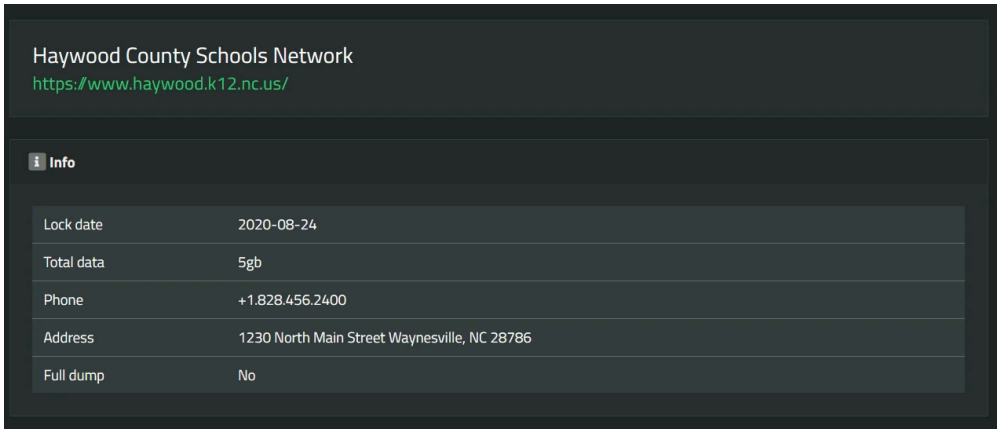
After performing an investigation, the Haywood Country School District states that unencrypted data was stolen during the ransomware attack.

"In announcing the ransomware attack on Monday, we wanted everyone to understand a data breach was possible. We have now confirmed a data breach occurred. We are taking every possible step to eliminate any potential harm to staff, students, and affiliates. At this point, the forensic work has not determined the extent of specific data that was stolen. We ask staff, students, and parents to monitor for any suspicious activity," the school district announced in a new update this week.

BleepingComputer has learned that the SunCrypt Ransomware operators are behind the attack on the school district.

As part of their tactics, the SunCrypt operators will steal unencrypted data before encrypting an organization's devices and threaten to release the data if a ransom is not paid.

After not paying, the ransomware operators have published a 5GB archive containing data stolen from the school district.



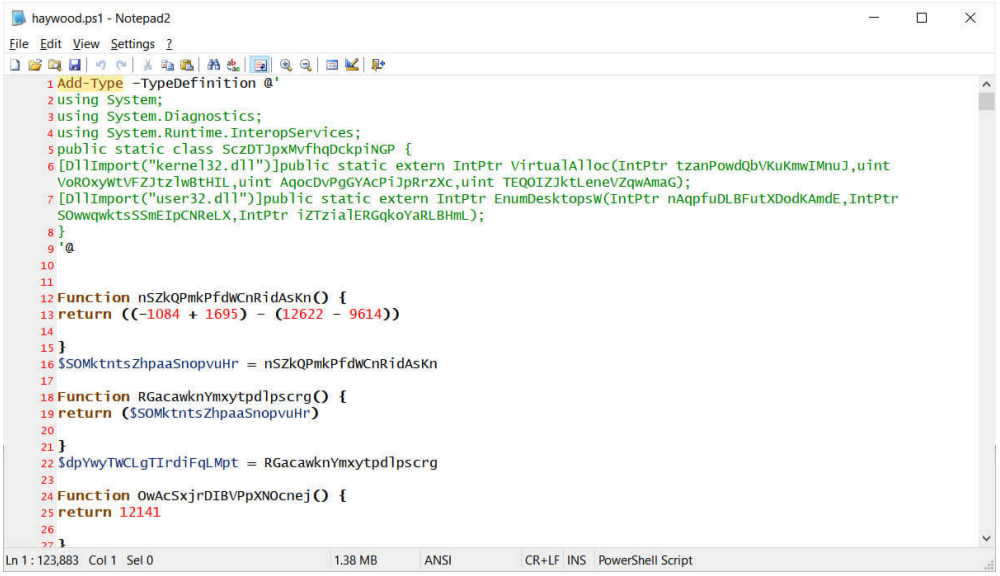
SunCrypt data leak site

This leaked data contains numerous sensitive documents and personal information related to the school district, students, and teachers.

A closer look at the Haywood County School District attack

When the SunCrypt ransomware operators perform an attack, they create a PowerShell script named after the victim and store it on the network's Windows domain controller.

BleepingComputer obtained the PowerShell script used in the Haywood County School District attack, as shown below. When executed on a device, it will launch the ransomware and encrypt the files on the computer.

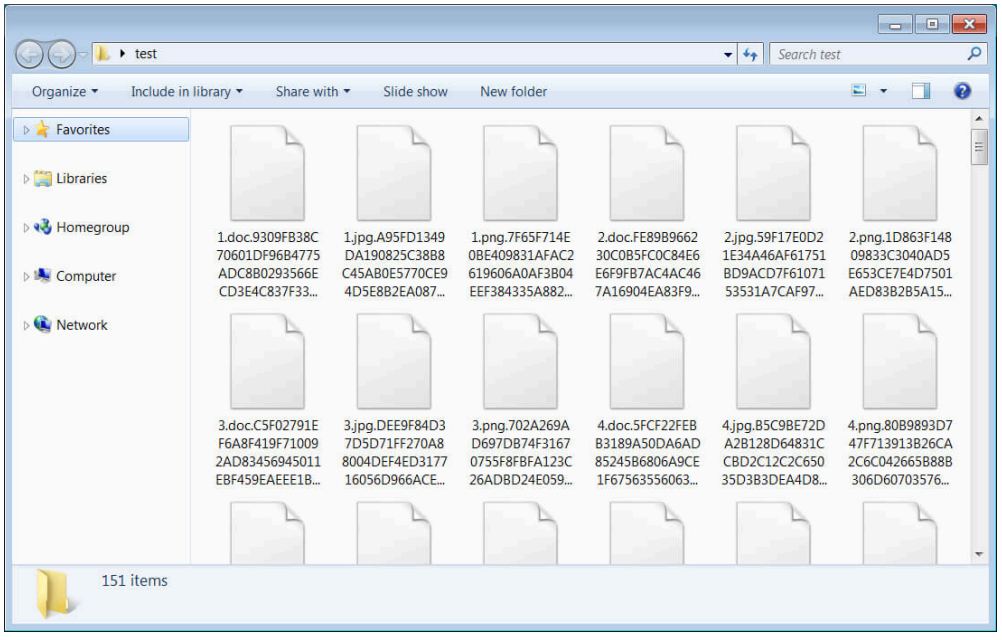


Haywood.ps1 PowerShell file

To launch the PowerShell script on every computer, the attackers will push a batch file to each Windows device on the network. When executed, this batch file will run the haywood.ps1 script stored on the domain controller and encrypt the computer.

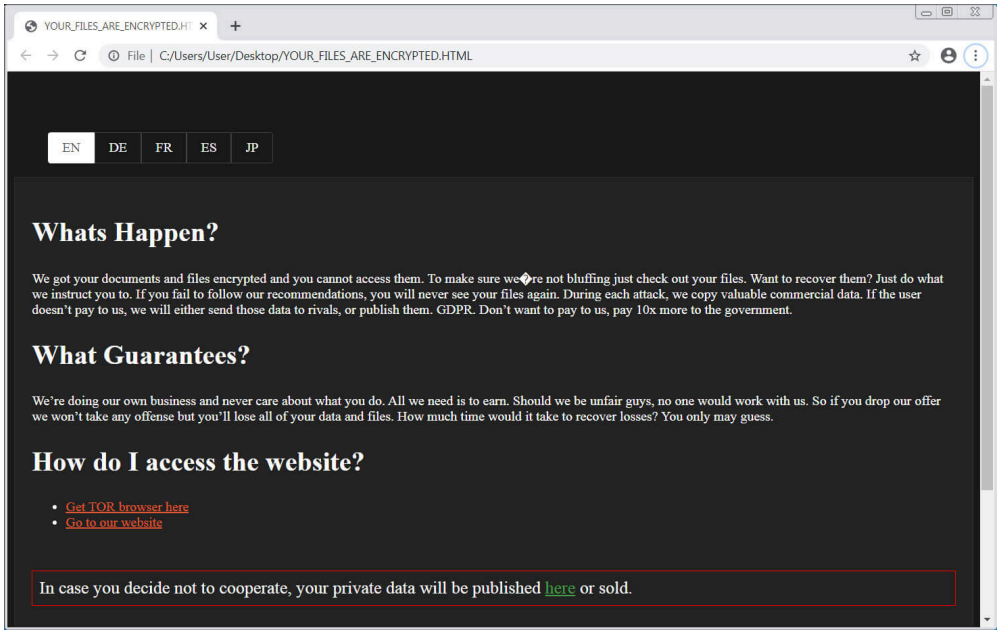
By performing the attack in this way, attackers can compromise a network, quietly harvest files to steal, and then push out the ransomware to all of the devices simultaneously. This method allows the attackers to quickly encrypt all devices on the network without being detected.

Once done, the victims will be left with folders containing files that have been renamed and encrypted.



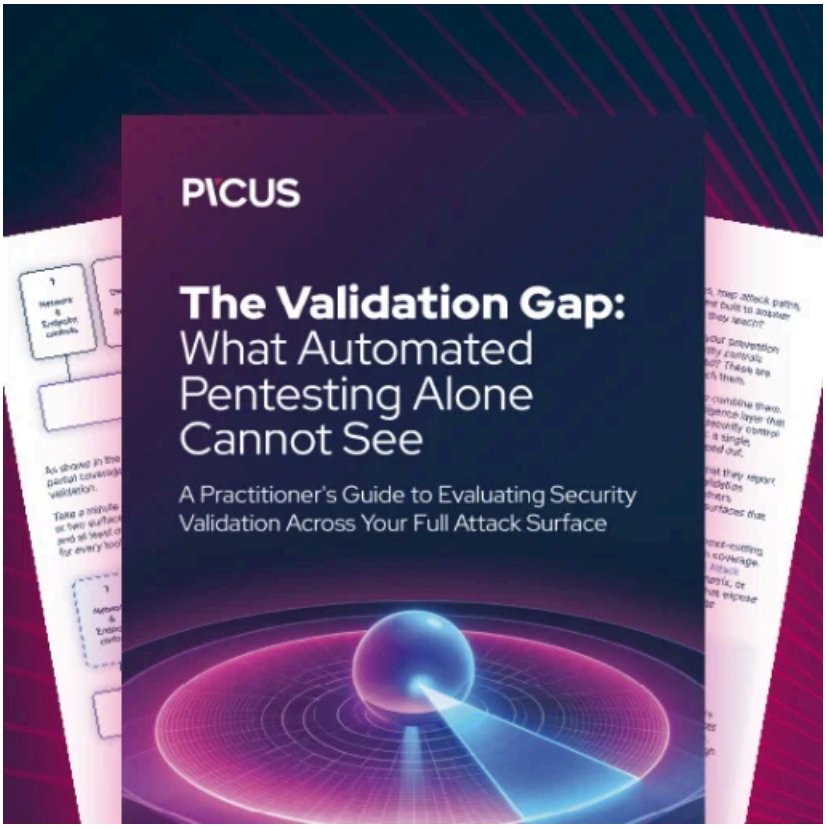
SunCrypt Encrypted Files

In each folder is a ransom note named YOUR_FILES_ARE_ENCRYPTED.HTML, which contains instructions on how to access the Tor payment site where a victim can negotiate with the ransomware operators.



SunCrypt ransom note

Unfortunately, SunCrypt appears to be secure, which means there is no way to currently recover files for free.



Automated Pentesting Covers Only 1 of 6 Surfaces.

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.

Source: https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-shuts-down-north-carolina-school-district/