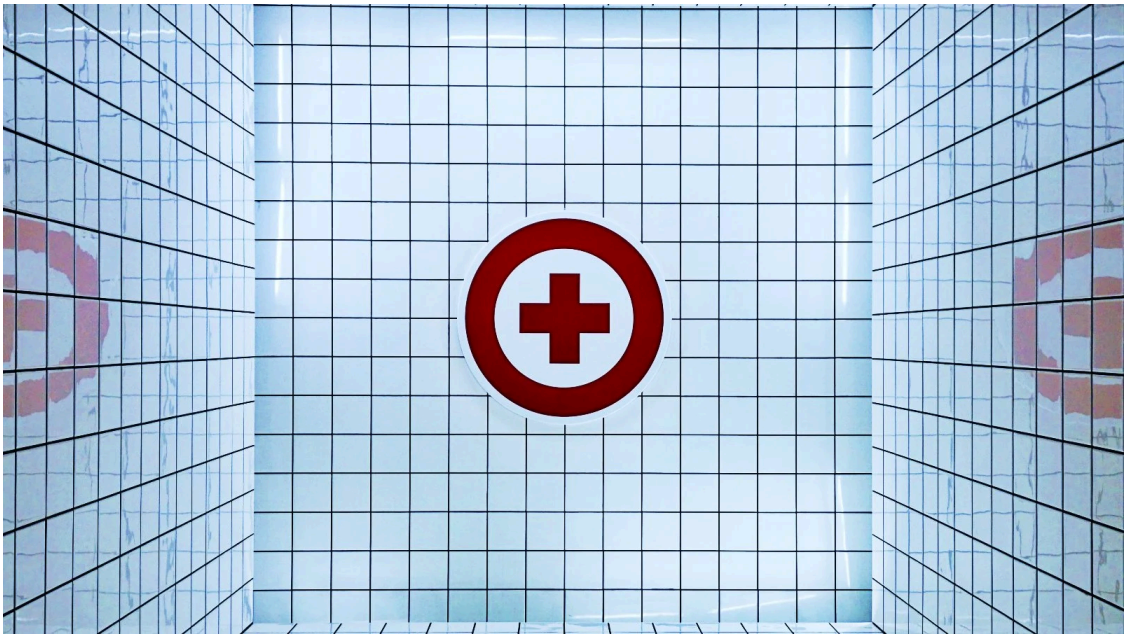
Conti ransomware gives HSE Ireland free decryptor, still selling data

By Lawrence Abrams

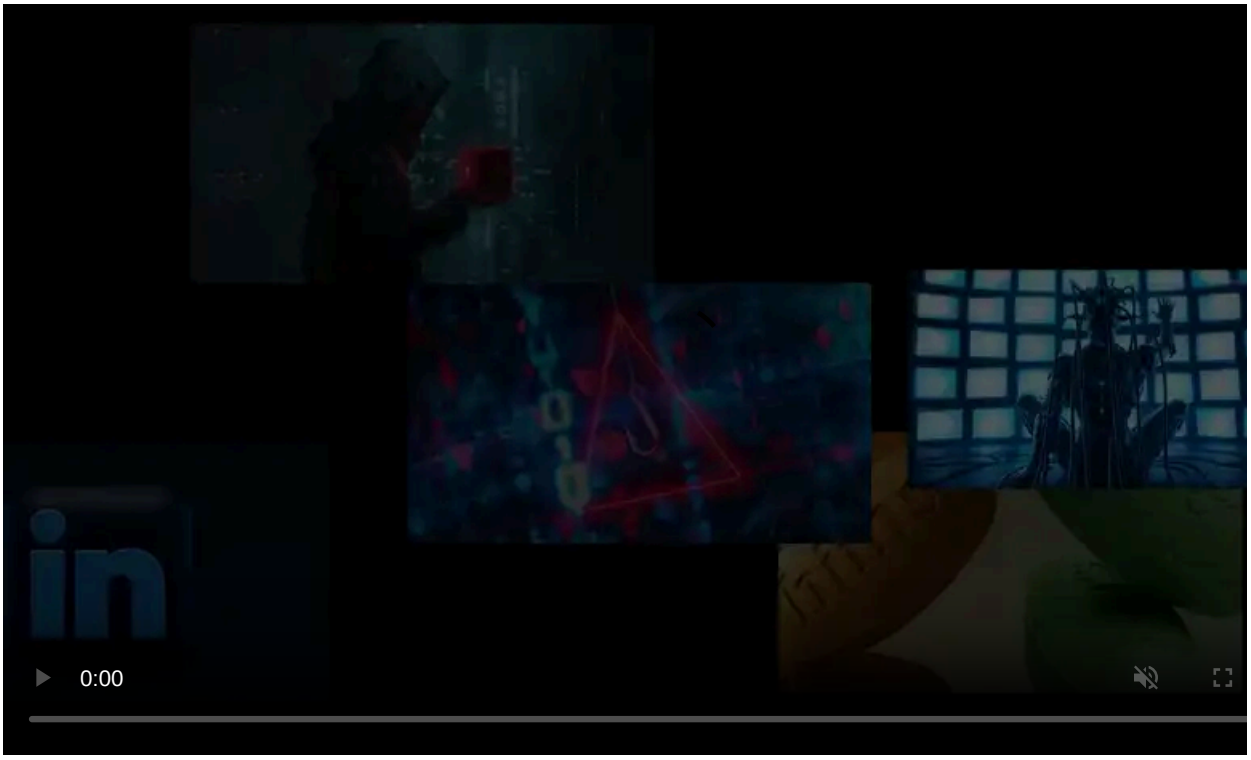
Published: 2021-05-20 · Archived: 2026-04-05 17:33:04 UTC

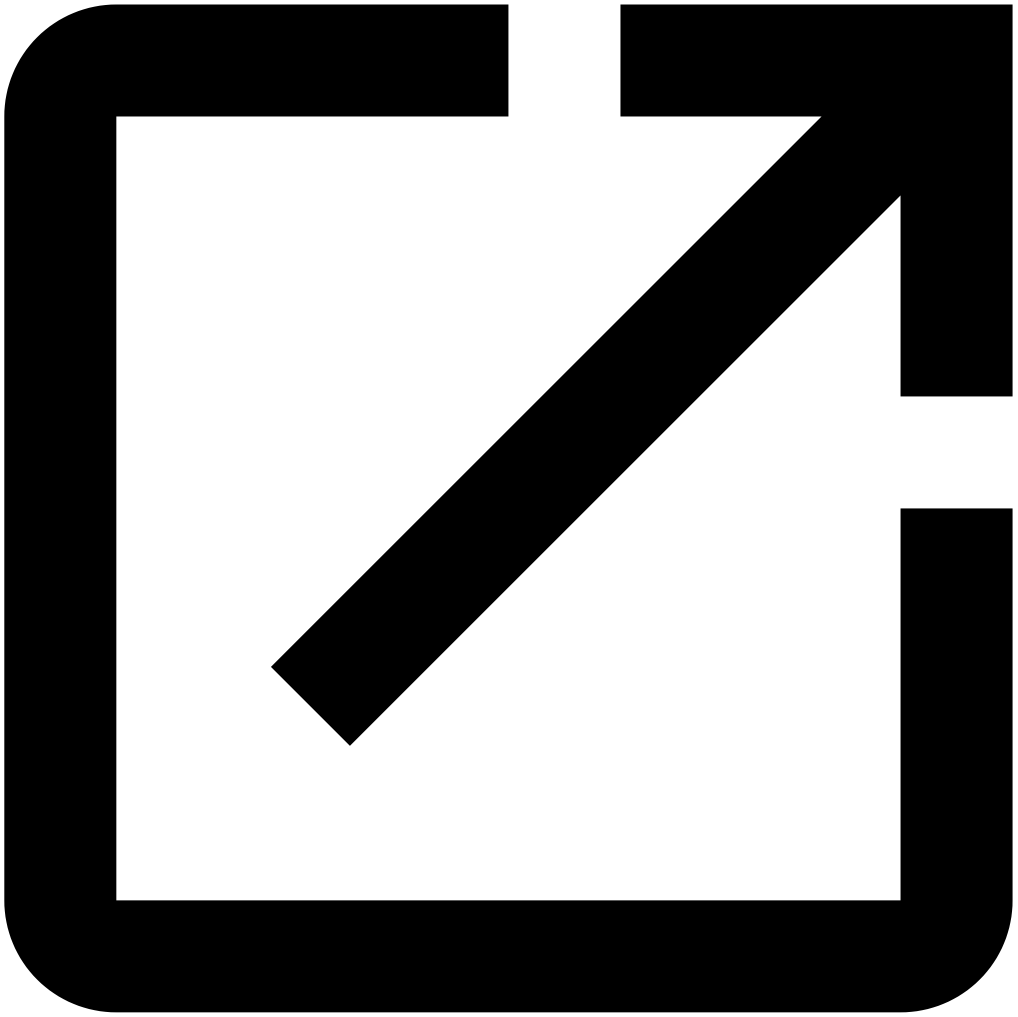


The Conti ransomware gang has released a free decryptor for Ireland's health service, the HSE, but warns that they will still sell or release the stolen data.

Ireland's HSE, the country's publicly funded healthcare system, and the Department of Health were attacked by the Conti ransomware gang last Friday.

While the Department of Health was able to block the attack, the HSE was not as lucky and was forced to shut down their IT systems to prevent further devices from being encrypted.


0:00



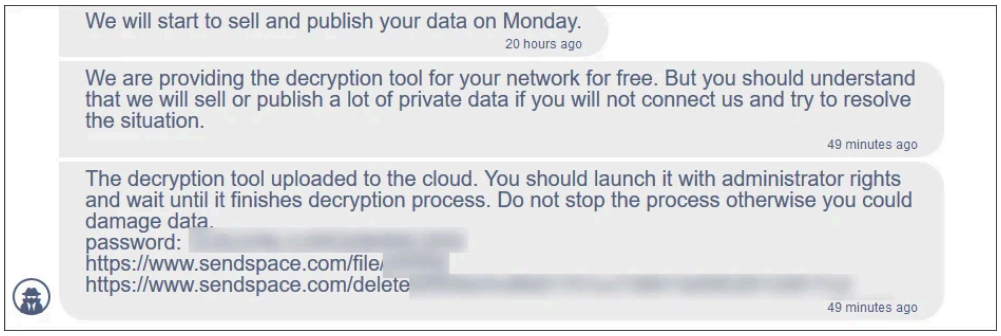
This IT outage has led to widespread disruption in the country's healthcare system as the HSE recovers from backups and the concerns that the ransomware gang would soon release patient's data.

Free decryptor released

Today, the ransomware gang posted a link to a free decryptor in their negotiation chat page for the HSE that can be used use to recover encrypted files for free.

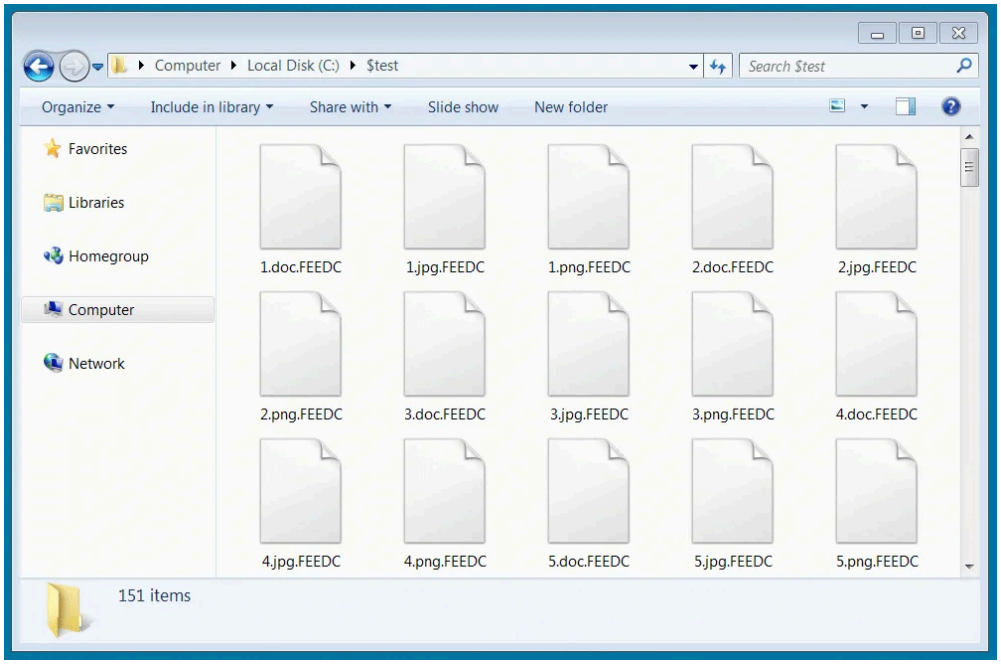
However, the threat actors warn that they will still be selling or publishing the stolen private data if a ransom of $19,999,000 is not paid.

"We are providing the decryption tool for your network for free. But you should understand that we will sell or publish a lot of private data if you will not connect us and try to resolve the situation," says the Conti ransomware gang on their Tor payment site.



Free decryptor released for HSE

As the ransomware sample used in the attacks on HSE is publicly available, security researcher MalwareHunterTeam and BleepingComputer have confirmed that the decryptor can decrypt files that were encrypted during this attack.



Decrypting files encrypted by HSE ransomware sample

Since the initial attack, there has not been any further conversation between HSE, or someone else who had access to the chat, and the Conti ransomware gang.

The safest approach continues to be to reimage all of their servers and recover from backups, but the decryptor can be used as needed to recover data missing from backups.

The government of Ireland is aware of the free decryptor but will be performing a technical review of the tool for malicious properties before using it.

"The HSE is aware that an encryption key have been provided," the Ireland Department of Health told BleepingComputer in a statement. "However further investigations have to be conducted to assess if it will work safely, prior to attempting to use it on HSE systems."

As threat actor's decryptors are known to be buggy and not optimized to decrypt files quickly, cybersecurity firm Emsisoft has created a 'Universal Decryptor' two times faster when decrypting files.

Ireland's HSE can use Emisoft's decryptor free of charge as part of their ongoing free assistance program to healthcare providers.

While the HSE can now recover encrypted files for free from prior activities of the ransomware gang, the release of the alleged 700 GB of stolen data is likely imminent.

Update 5/20/21 2:10 PM EST: Added statement and information about Emsisoft's Universal Decryptor.
