This old ransomware is using an unpleasant new trick to try and make you pay up

By Written by Danny Palmer, Senior WriterSenior Writer Jan. 8, 2019 at 5:00 a.m. PT

Archived: 2026-04-05 16:56:52 UTC

An old family of ransomware has returned with a new campaign which uses information about children stolen from crowdfunding websites and claims that payments made in exchange for unlocking encrypted files will be donated to good causes.

Security

-
-
-
-

First spotted in early 2016, CryptoMix is a combination of CryptXXX and CryptoWall ransomware. While it has caused issues for users over the years, it's a relatively low-profile form of file-locking malware that until recently appeared to have fallen off the radar.

However, researchers at cyber security firm Coveware have uncovered a new CryptoMix campaign that looks to make up for its lack of notoriety with this unpleasant new trick.

This ransomware attack begins, like many others, with brute force attacks targeting weak passwords on RDP ports. Once inside the network, the attackers harvest the admin credentials required to move across the network before encrypting servers and wiping back-ups.

Victims are then presented with a ransom note that tells them to send an email to the ransomware distributors, who also warn victims not to use any security software against CryptoMix, with the attackers claiming that this could permanently damage the system (a common tactic used by attackers to dissuade victims from using security software to restore their computer).

SEE: 17 tips for protecting Windows computers and Macs from ransomware (free PDF)

But if a victim engages with the attackers over email, they'll find out that those behind CryptoMix claim that the money made from the ransom demand -- usually two or three bitcoins -- will be donated to charity.

Obviously, this isn't the case, but in an effort to lure victims into believing the scam, the CryptoMix distributors appear to have taken information about real children from crowdfunding and local news websites. The researchers have notified the families of the children affected.


cryptomix-ransomware-message.png

CrytoMix ransomware message.

Image: Coveware

The hackers claims that children will receive presents and medical help as a result of the payment -- but also threaten that the 'donation' will be doubled if the payment isn't received within 24 hours.

If the victim pays up, they're told that the payment will be noted in their name -- but this is of course false; the only people benefiting from any payments made are the attackers.

"They are naive about the level of intelligence of the people and companies they attack. Even if the victims believed that the hackers were donating the ransom proceeds to charity, it would not alter how they thought about paying or not paying," Bill Siegal, CEO of Coveware told ZDNet.

To avoid falling victim to CryptoMix and other forms of ransomware, users should secure their RDP ports and ensure that two-factor authentication is employed on critical systems, so that if attackers do breach the network, they can't wipe or encrypt backups.

For those who become infected with CryptoMix, help is at hand -- Avast and CERT Poland have previously released a free decryption tool, which is available as part of the No More Ransom initiative.

READ MORE ON CYBER CRIME

- **Ransomware: Not dead, just getting a lot sneakier**
- **US charges Iranian hackers over ransomware attacks on major cities** **CNET**
- **Giant ransomware bundle threatens to make malware attacks easier for crooks**
- **How SMBs can minimize damage from ransomware attacks** **TechRepublic**
- **Cybercrime: Ransomware remains a 'key' malware threat says Europol**

Editorial standards