Nwgen Ransomware Removal Report

enigmasoftware.com/nwgenransomware-removal/

CagedTech

A group of cybercriminals is targeting corporate organizations with a potent malware threat named the Nwgen Ransomware. The attackers infiltrate the computers of their victims, deploy the threatening payload, and let it encrypt nearly all of the files stored there. The threat can render all documents, databases, archives, and more inaccessible completely.

Looking at the affected files, revealed that each one has been marked by appending '.nwgen' to their original names as a new extension. After finishing with the encryption of all suitable files, Nwgen will proceed to create a text file on the system's desktop. This file is named 'How To Restore Your Files.txt' and it carries a ransom note with instructions from the hackers.

Ransom Note's Details

According to the note, Nwgen uses a combination of the AES-256-CRT cryptographic algorithm and the ChaCha8 Cipher. It also states that to receive the decryptor software from the attackers, victims are expected to pay the sum of $150,000. The funds must be sent to the crypto-wallet address found in the note. Furthermore, the hackers state that they would only recognize payments made using the Monero cryptocurrency.

To put further pressure on the compromised organization to pay up, the crybercriminals also claim to have obtained vast amounts of sensitive data (200GB) from the infected systems. Now, they threaten to start leaking the information to the public partially, while trying to find a suitable buyer. To avoid this outcome, victims are expected to initiate communication within 12 hours of the ransomware attack. They can do so by messaging the 'yourd34d@ctemplar.com' email or the '@redeyeg0d' Telegram account.

The full text of the Nwgen Ransomware's demands is:

'*You are probably wondering why you are receiving a message from me.*
*Yesterday, * got breached.*

You are probably not aware, but over the past few days we have been exfiltrating all of your data that we could get our hands on.
We took over 200GB in data (dba's / patient's userdata / netshares / vdi servers).

What happened to your files?

Your network was been penetrated.

All of your files were encrypted using AES-256-CTR with ChaCha8 Cipher.

WARNING:

Don't try to decrypt your files, shadow copies were removed,
recovery methods can lead to the impossibility of recovery of the certain files.

We exclusively have decryption software for your situation,
no decryption software is available in the public.

Pay 150,000 (USD) in XMR (Monero) to this address:
4BExj4Z7n73316oWSd6k3Wj7A12PFVUSeHoobSPpaCJVdH6Z1oRBBssemrpwW5GyRt7xi3SQCeJzUa1uFoWWNySYCxoHv13
How do you buy XMR?

hxxps://bisq.network/ to buy XMR using fiat.

Alternatively use a Cryptocurrency exchange to buy XMR:

hxxps://www.kraken.com/

Use this guide: hxxps://www.getmonero.org/

After sending the specified amount to our wallet we will provide you
with the decryption keys to unlock your files.

If you do not respond (24 hour deadline, starting now), or we do not receive a response from you

we will start showing the data to our potential buyers, and leak a partial,

All of your clients (customers / employers) will be informed and given proof that their data has been compromised
and publish everything in a public way in multiple places and outlets to get more customers interested in buying the data
and also reporting the availability of this data to the appropriate news platforms.

Contact:
telegram: @redeyeg0d
email: yourd34d@ctemplar.com'