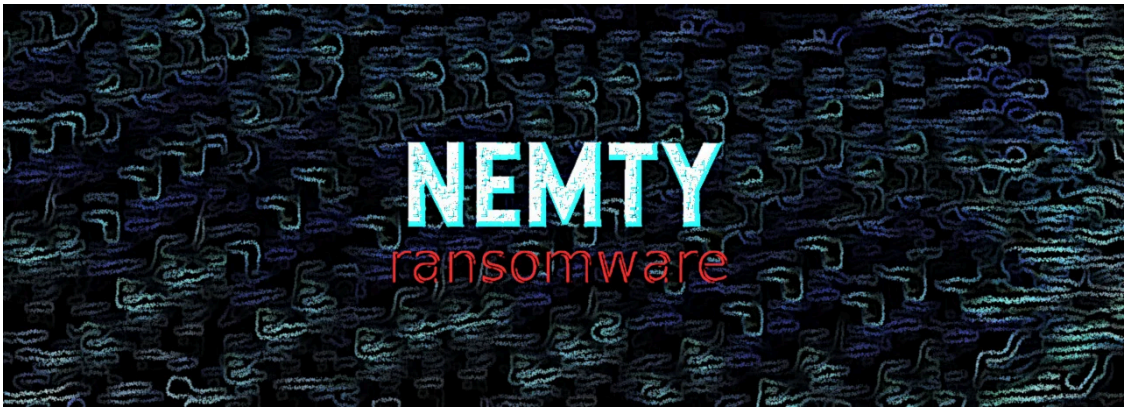
Nemty Ransomware to Start Leaking Non-Paying Victim's Data

By Lawrence Abrams

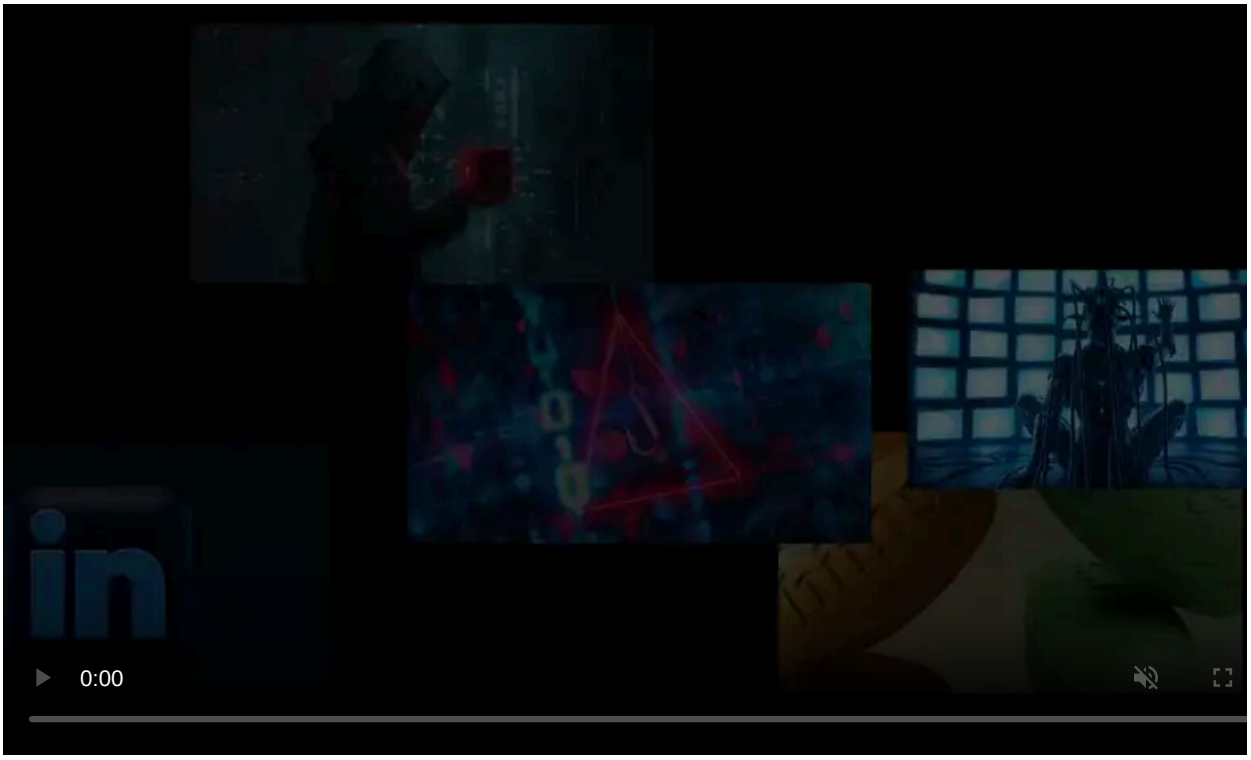
Published: 2020-01-13 · Archived: 2026-04-05 15:38:33 UTC

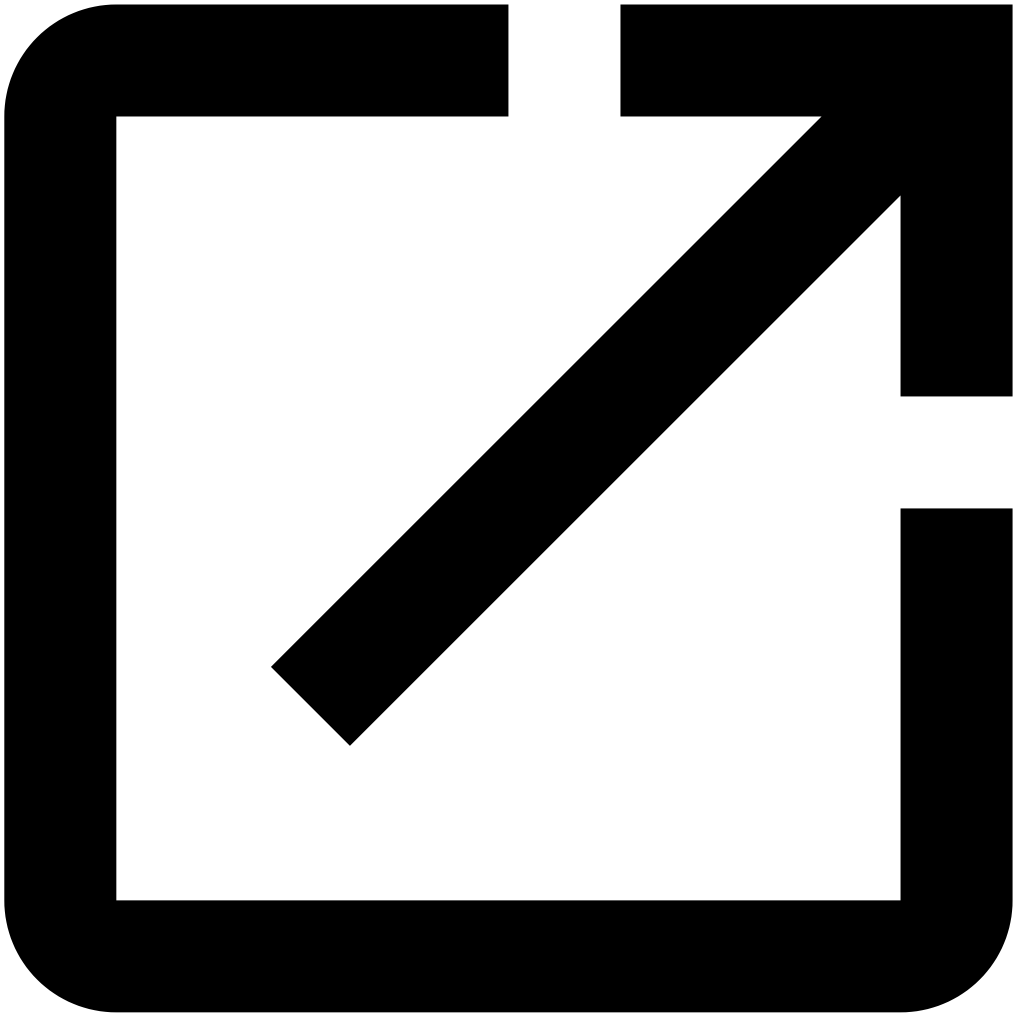


The Nemty Ransomware has outlined plans to create a blog that will be used to publish stolen data for ransomware victims who refuse to pay the ransom.

A new tactic started by the Maze Ransomware and now used by Sodinokibi is to steal files from companies before encrypting them. If a victim does not pay the ransom, then the stolen data will be leaked little-by-little until payment has been made or it has all been released.

The theory behind this is that companies may be more apt to pay a ransom if it costs less than the possible fines, data breach notification costs, loss of trade and business secrets, tarnishing of brand image, and potential lawsuits for the disclosing of personal data.


0:00

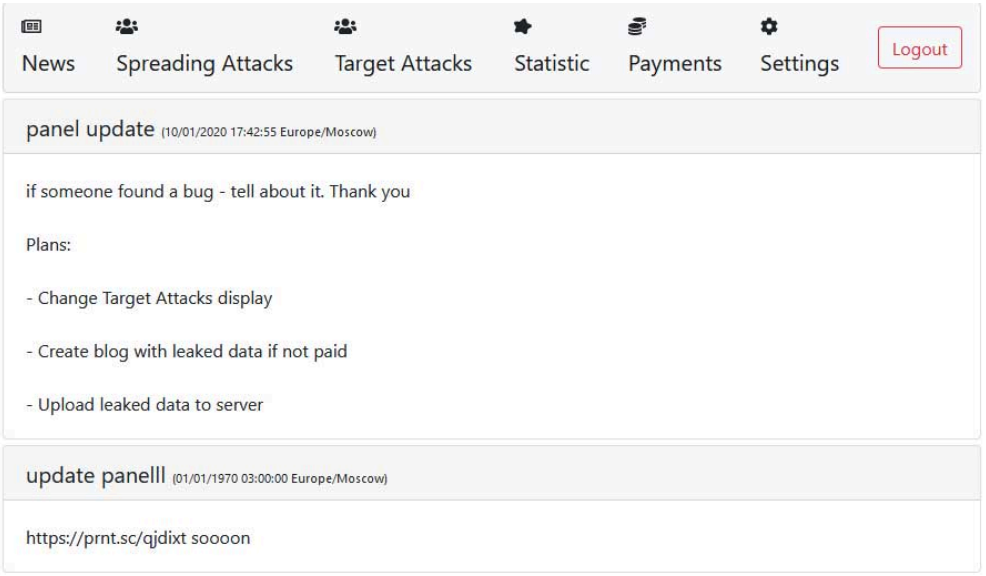


To facilitate this publishing of stolen data, the Maze operators have created a web site that they use to publish information about their non-paying victims and links to the leaked data.

Nemty plans on creating a leaked data site

In the Nemty Ransomware affiliate panel, the ransomware developers have a news feed where they post their plans, bug fixes, and upcoming changes coming to their ransomware-as-a-service.

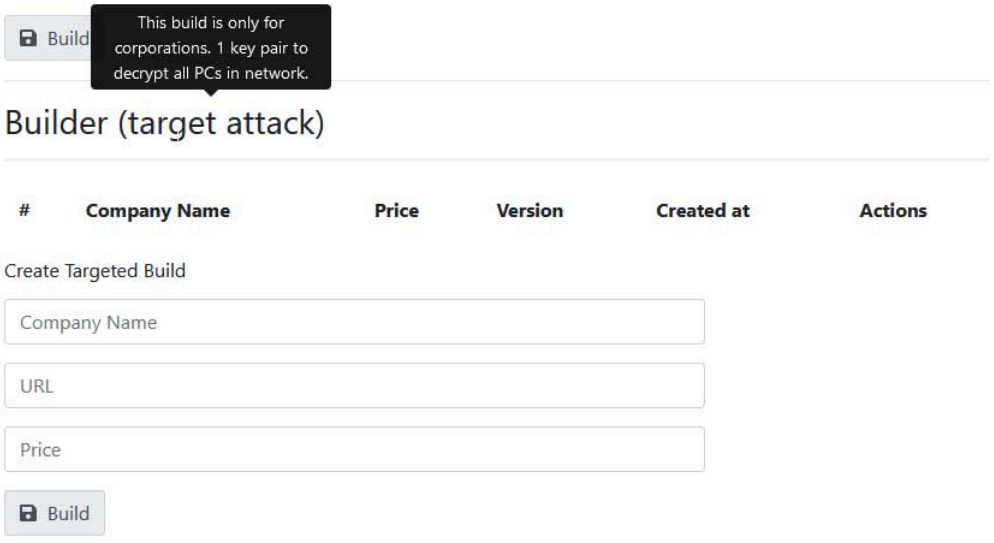
According to a recent 'News' post shared with BleepingComputer, Nemty plans to create a web site where they will leak stolen data if ransoms are not paid.



Newsfeed from Nemty Ransomware affiliate panel

Nemty is already configured for network attacks with a builder mode that is used to create executables that target an entire network rather than individual computers.

According to this mode, the created ransomware executables are "only for corporations". This means there will be one key used to decrypt all the devices in the network and victims will not be able to decrypt individual machines.



Nemty Targeted attack ransomware builder

With this functionality already in place, evolving the RaaS to incorporate data exfiltration and further extortion tactics would not be a laborious change.

If remains to see if this new extortion method is paying off for the ransomware actors, but one thing is for sure, we will continue to see more threat actors adopting this new tactic.

Even worse, this also means that these types of attacks are not only affecting the company but are causing personal and third-party information to be disclosed to unauthorized users.

While that means that victims should treat these as attacks like data breaches, from existing cases, it does not appear that they are doing so.

Source: https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data/