DoppelPaymer Ransomware Sells Victims' Data on Darknet if Not Paid

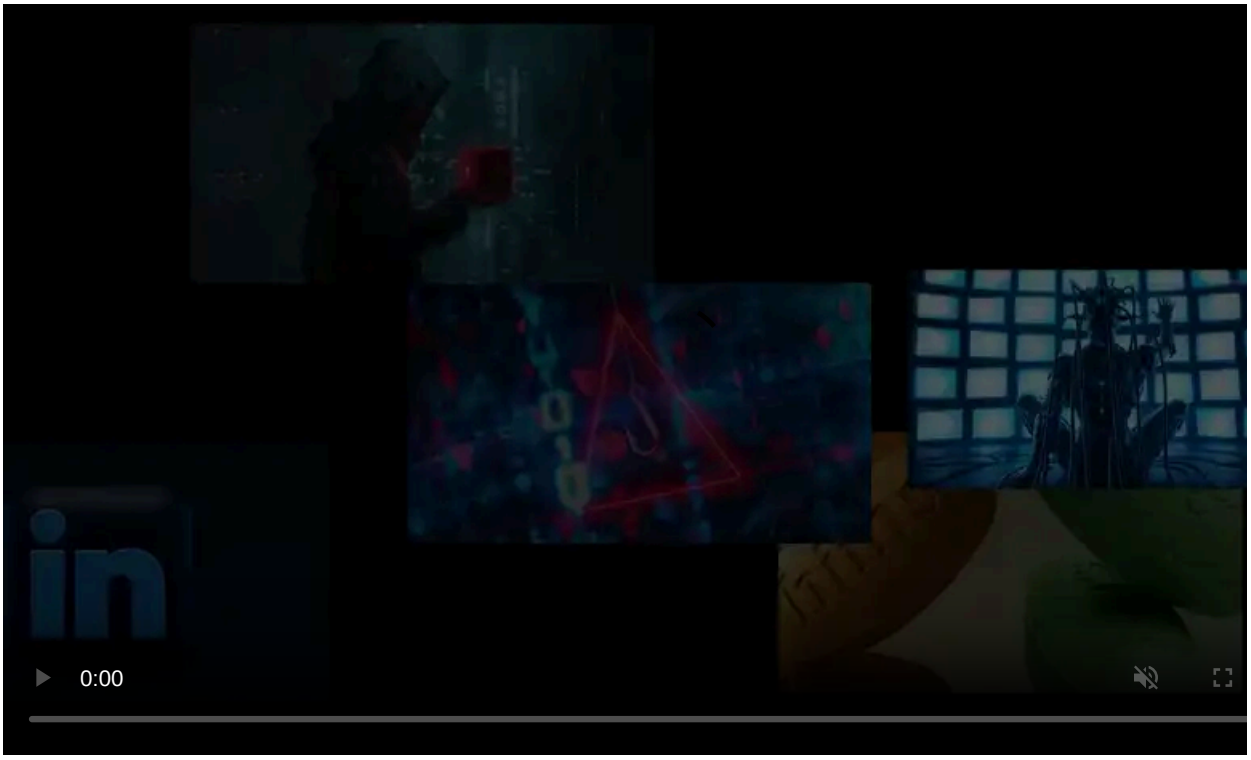
By Lawrence Abrams

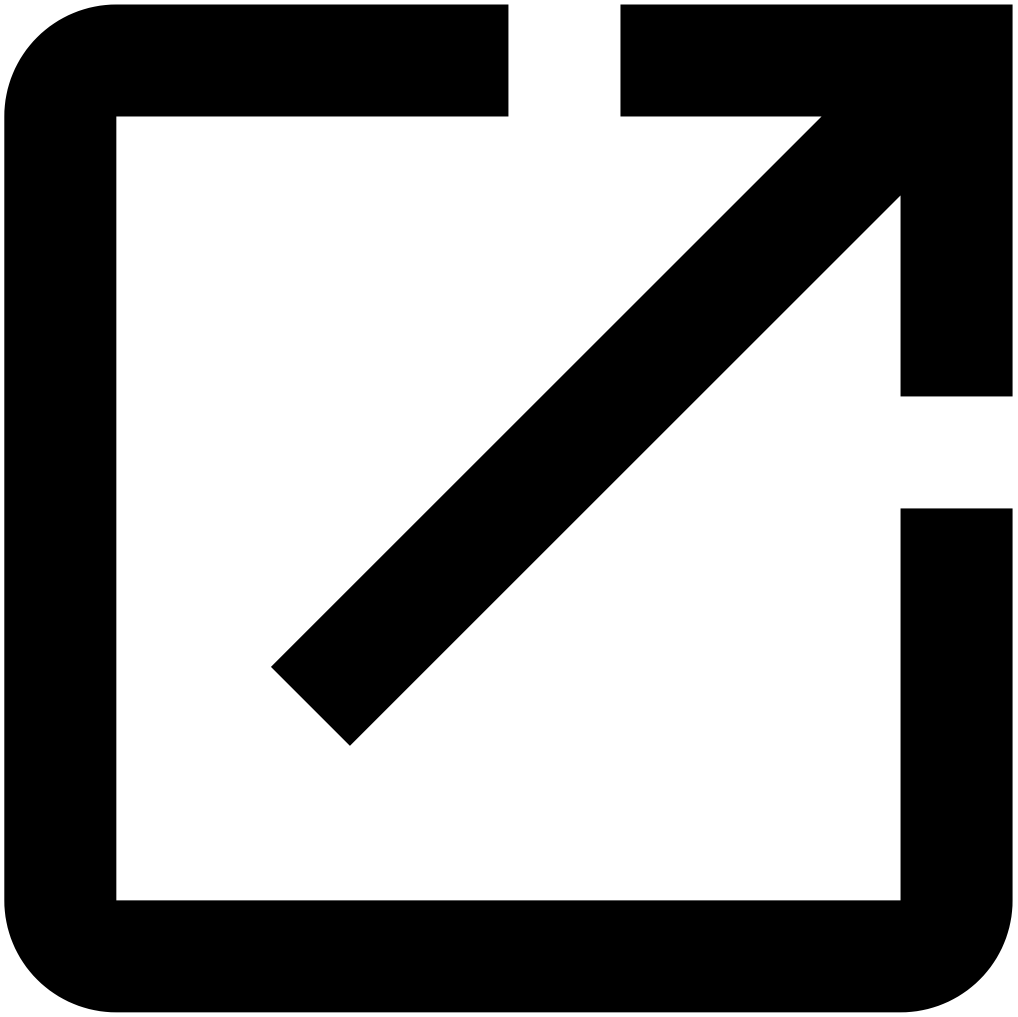
Published: 2020-02-03 · Archived: 2026-04-05 17:38:02 UTC

The DoppelPaymer Ransomware is the latest family threatening to sell or publish a victim's stolen files if they do not pay a ransom demand.

A new tactic being used by ransomware operators that perform network-wide encryption is to steal a victim's files before encrypting any devices. They then threaten to publish or sell this data if the victim does not pay the ransom.

This new tactic started in November 2019 when Maze Ransomware publicly released stolen files belonging to Allied Universal for not paying a ransom.


0:00



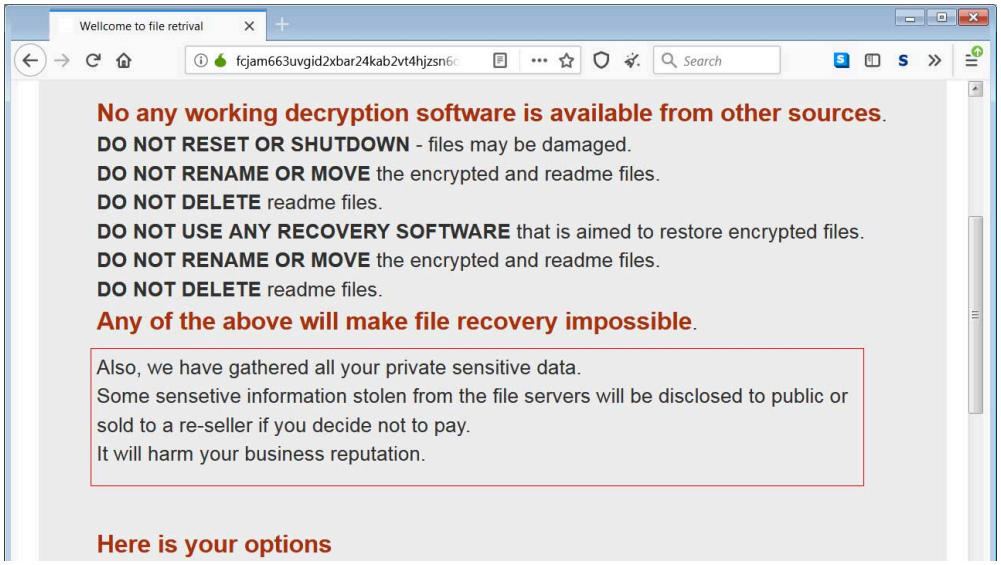
Since then, Sodinokibi/REvil published stolen data and the Nemty Ransomware announced in their RaaS affiliate panel that they would start doing it as well.

It is now DoppelPaymer's turn, who has told BleepingComputer that they have sold victim's data on the darknet in the past when they did not pay the ransom.

DoppelPaymer claims to sell victim's data

When looking at the DoppelPaymer Tor payment site, BleepingComputer noticed that they had recently started to tell victims that they have stolen their data and will to publish or sell it if a ransom is not paid.

"Also we have gathered all your private sensitive data.
Some sensetive information stolen from the file servers will be disclosed to public or sold to a re-seller if you decide not to pay.
It will harm your business reputation."



DoppelPaymer Tor Site
Red box added by BleepingComputer

In emails with the DoppelPaymer Ransomware operators, the threat actors told BleepingComputer that for almost a year they have been stealing data from their victims. They also claimed to have anonymously sold stolen files on the darknet in the past when a victim chose not to pay the ransom.

This was done to "cover some costs".

While DoppelPaymer told us that they have not publicly released stolen data as of yet, the Maze Ransomware operators have shown that doing so will increase the number of payments.

"MAZE shown the world that success rates are increased after sharing some data", DoppelPaymer told BleepingComputer.

Based on the new threats on the Tor payment site, it appears that they plan on adopting this tactic soon as well.

As proof that they are stealing data, the DoppelPaymer operators shared two Excel spreadsheets containing a list of the Windows Domain users on two networks that they compromised.

They did not, though, share any of their victim's allegedly stolen files.

Ransomware attacks are now data breaches

With ransomware operators now routinely stealing victim's data and publishing or selling it if not paid, ransomware attacks need to be classified as data breaches.

Based on the stolen data seen by BleepingComputer in recent ransomware extortion attempts, it is clear that sensitive and private information of not only businesses, but also employees, is being stolen and released.

It is now important that companies be transparent and report ransomware attacks so that all affected users, and not just the company, are protected from the leak of personal data.

DoppelPaymer begins using a new extension

Recent versions of the DoppelPaymer ransomware have also switched to a new dedicated **.doppeled** extension for encrypted files.

BleepingComputer was told by the DoppelPaymer operators that this was done to make it easier for victims to know what ransomware encrypted their network.

As DoppelPaymer is an offshoot of the BitPaymer ransomware, making this extension change makes it easier to differentiate between the two families.

Source: https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-sells-victims-data-on-darknet-if-not-paid/