DoppelPaymer Ransomware Launches Site to Post Victim's Data

bleepingcomputer.com/news/security/doppelpaymer-ransomware-launches-site-to-post-victims-data/

Lawrence Abrams

By
Lawrence Abrams

- February 25, 2020
- 12:01 AM
- 0

The operators of the DoppelPaymer Ransomware have launched a site that they will use to shame victims who do not pay a ransom and to publish any files that were stolen before computers were encrypted.

A new extortion method started by the Maze Ransomware is to steal files before encrypting them and then use them as leverage to get victims to pay the ransom.

If a ransom is not paid, then the ransomware operators release the stolen files on a public 'news' site to expose the victim to government fines, lawsuits, and the risk of the attack being classified as a data breach.

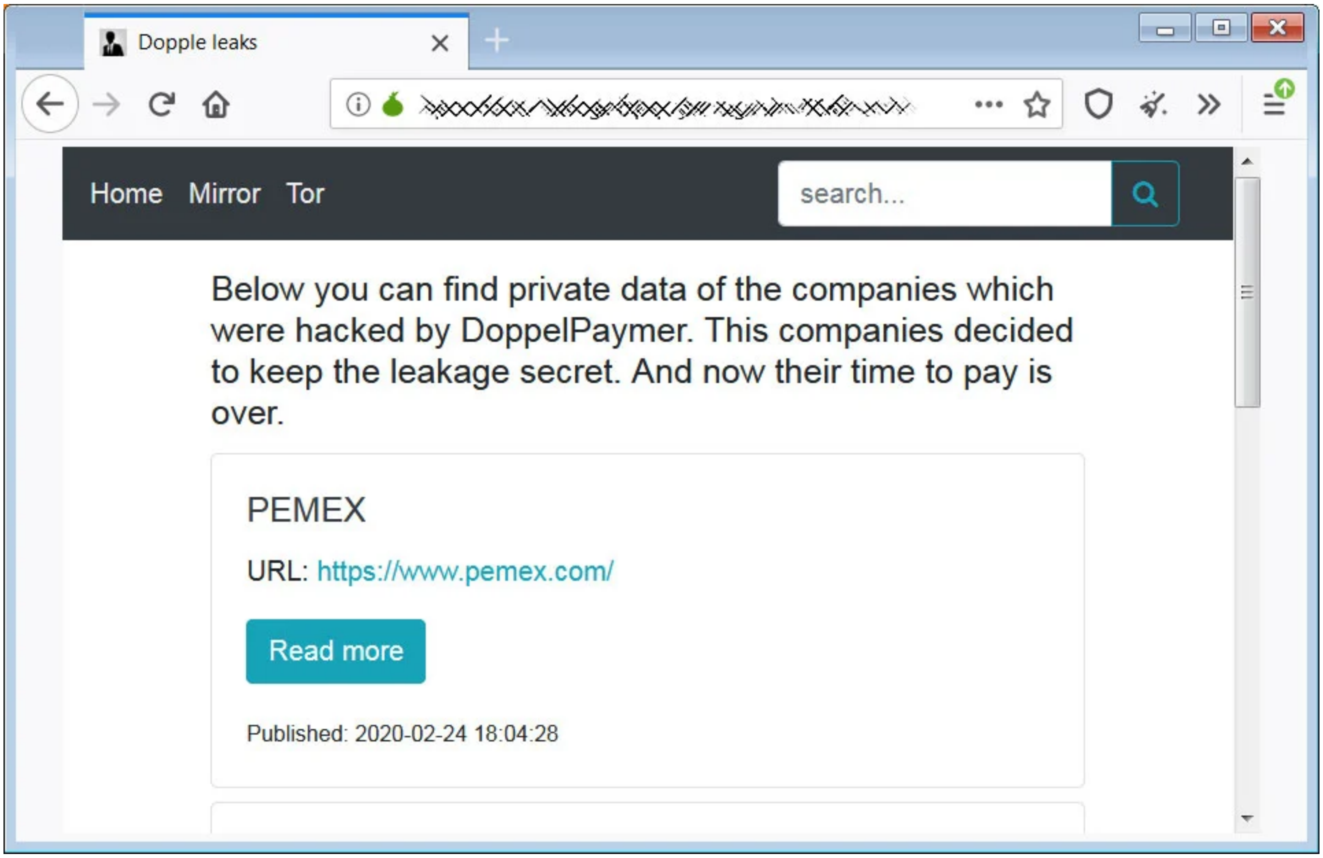
Soon after starting this tactic, other ransomware families including Sodinokibi, Nemty, and DoppelPaymer have stated that they would begin this practice as well.

DopplePaymer launches public leak site

Today, the operators of the DoppelPaymer Ransomware have followed in Maze's footsteps and launched a site called 'Dopple Leaks' that will be used to leak files and shame non-paying victims.

DoppelPaymer is an enterprise-targeting ransomware that compromises a corporate network, eventually gains access to admin credentials, and then deploys the ransomware on the network to encrypt all devices. As these attacks encrypt hundreds, if not thousands, of devices, they tend to have a huge impact on operators and the attackers demand a very large ransom.

The ransomware operators state they have created this site as a threat to victims that if they do not pay, their data and names will be leaked by the attackers.



Below you can find private data of the companies which were hacked by DoppelPaymer. This companies decided to keep the leakage secret. And now their time to pay is over.

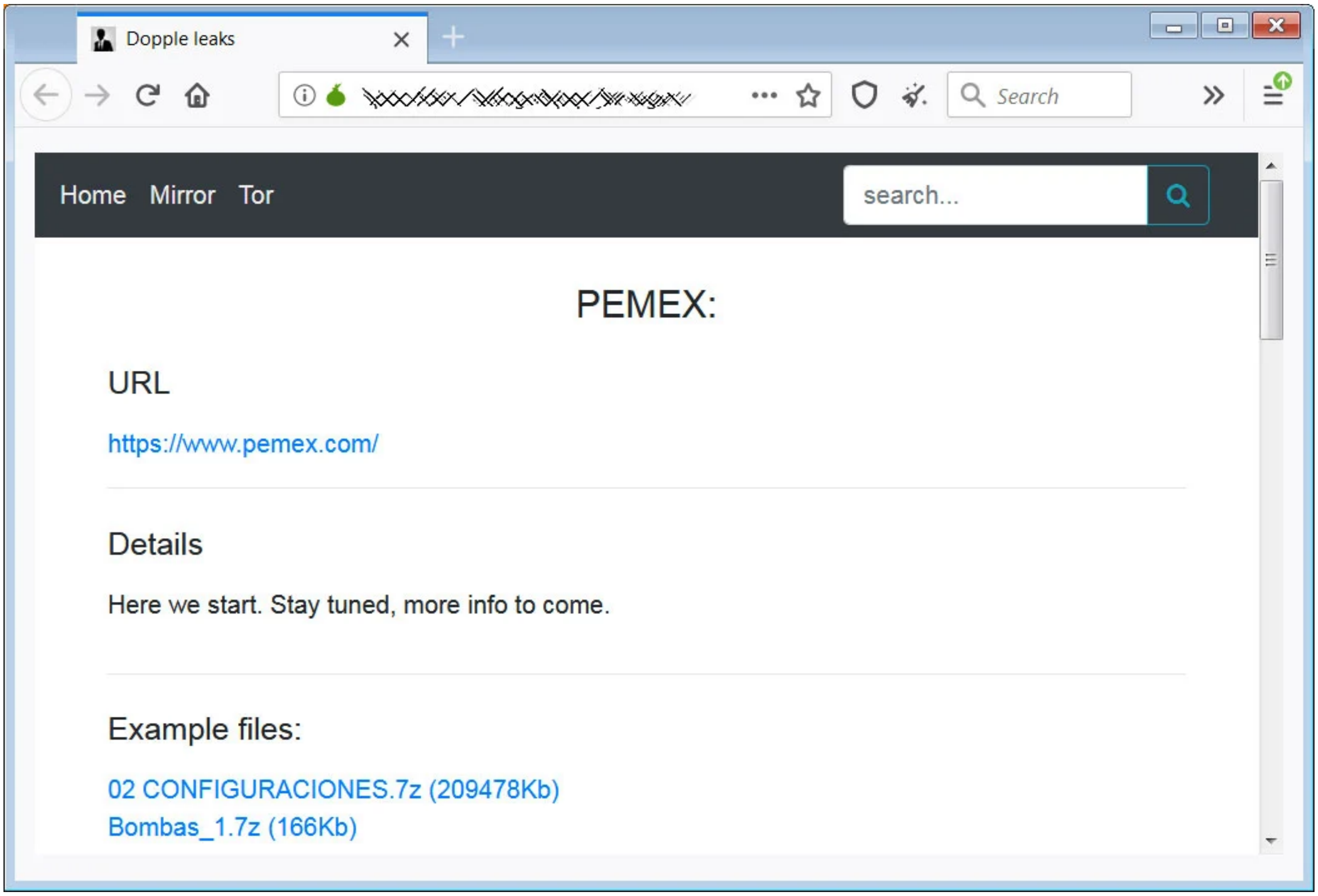
PEMEX

URL: https://www.pemex.com/

Published: 2020-02-24 18:04:28

The 'Dopple Leaks' Site

The ransomware operators have told BleepingComputer that this new site is in "test mode" and is currently being used mostly for shaming their victims and to publish a few files that were stolen from victims.



PEMEX:

URL

https://www.pemex.com/

Details

Here we start. Stay tuned, more info to come.

Example files:

02 CONFIGURACIONES.7z (209478Kb)
Bombas_1.7z (166Kb)

Pemex information on the DoppelPaymer site

Currently listed on this page are four companies that DoppelPaymer claims to have encrypted and who did not pay the ransom.

Other than Pemex, BleepingComputer will only share descriptions of the other listed companies and the demanded ransoms that were shared with us by the DoppelPaymer operators.

- A merchant account company based out of USA with a ransom amount of 15 bitcoins (~$150K).
- A French cloud hosting and enterprise telecommunications company with a ransom of 35 bitcoins (~$330K)
- A logistics & supply chain company based out of South Africa was encrypted on January 20th, 2020 with a ransom amount of 50 bitcoins (~$500K).
- Mexico's state-owned oil company Pemex was attacked by DoppelPaymer on November 10th, 2019. The attackers demanded 568 bitcoins ($4.9 million at the time) for a decryptor.

Of all the sites, DoppelPaymer told us that they only stole a large amount of "still unsorted" files from Pemex.

For the other three companies, they only stole a few files because there was "nothing interesting" or because "it was not our goal".

They stated that they do plan on performing more data exfiltration now that this site has been created.

Treat ransomware attacks like data breaches!

BleepingComputer has repeatedly stated that ransomware attacks have to be treated like data breaches.

For years, it is has been a well-known secret that ransomware attackers are looking through and stealing victim's files before encrypting computers and then threatening to release them.

It was not until recently, though, that ransomware operators have followed through with their threats.

Now that they are doing so and more ransomware operators are getting on board, companies need to be transparent about the data theft and treat these attacks like data breaches.

This is because it is not only corporate data being stolen, but also vendor and client data and the personal information of employees.

Transparency is more important now than ever and hiding these attacks is putting their employees at long-term risk as their data is exposed to identity theft and fraud.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

Quantum ransomware seen deployed in rapid network attacks

Karakurt revealed as data extortion arm of Conti cybercrime syndicate

Snap-on discloses data breach claimed by Conti ransomware gang

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.