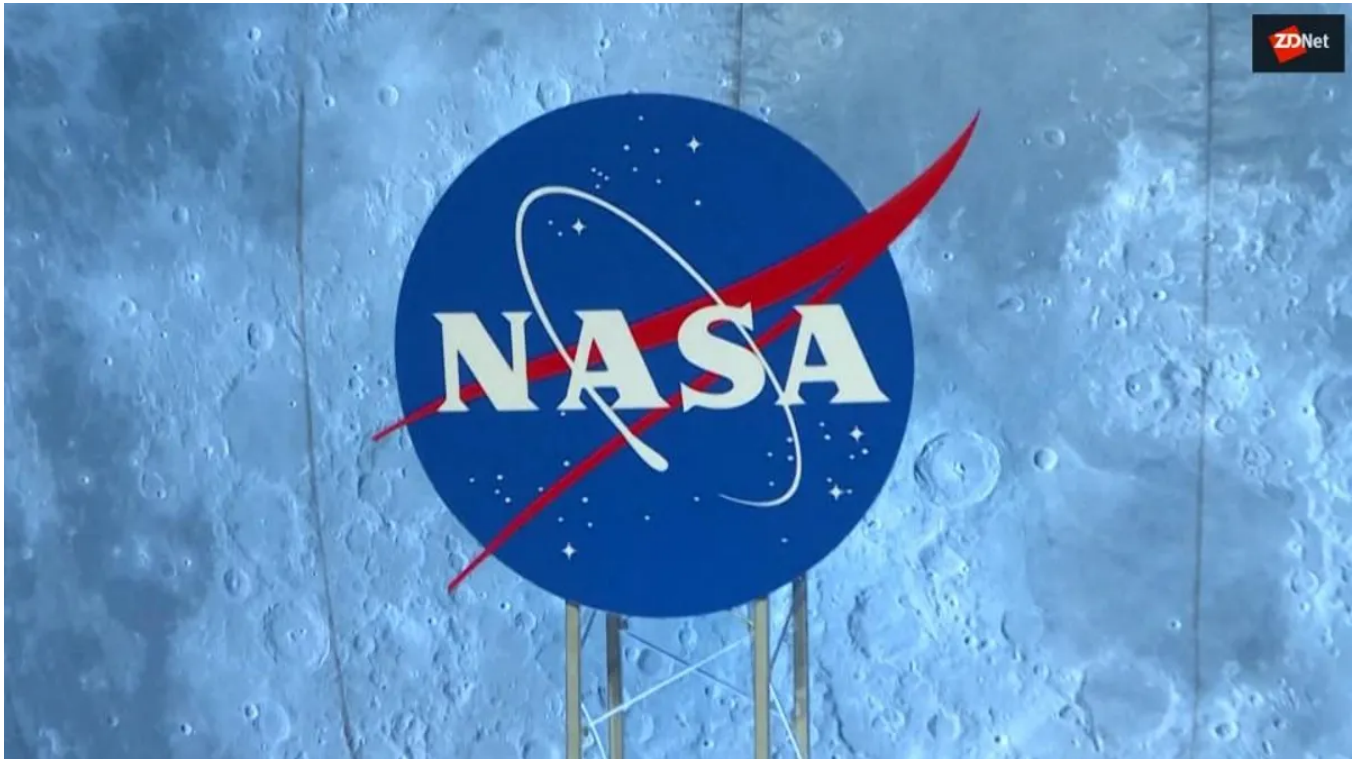


# Ransomware gang says it breached one of NASA's IT contractors

[zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/](https://zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/)



[Home Innovation Security](#)

DopplePaymer ransomware gang claims to have breached DMI, a major US IT and cybersecurity provider, and one of NASA IT contractors.



Written by [Catalin Cimpanu, Contributor](#) on June 2, 2020

- 
- 
- 
- 
-

dm-dark-web.png

Image: ZDNet

The operators of the DopplePaymer ransomware have congratulated SpaceX and NASA for [their first human-operated rocket launch](#) and then immediately announced that they infected the network of one of NASA's IT contractors.

In a blog post published today, the DopplePaymer ransomware gang said it successfully breached the network of Digital Management Inc. (DMI), a Maryland-based company that provides managed IT and cyber-security services on demand.

According to the company's press releases, DMI's customer list includes several Fortune 100 companies and many government agencies, among them NASA [1, 2].

It is unclear how deep inside DMI's network the DopplePaymer gang made it during their breach, and how many customer networks they managed to breach. Three DMI spokespersons did not answer phone calls from ZDNet seeking comment for this article.

The thing that appears to be clear is that they got their hands on NASA-related files, suggesting they breached DMI's NASA-related infrastructure.

To support their claims, the DopplePaymer operators posted 20 archive files on a dark web portal the group is operating.


 dmi-nasa.png

Image: ZDNet

The archives include everything from HR documents to project plans, as can be seen from a screenshot ZDNet took of one of the files. Employee details included in these files matched public LinkedIn records.


 dmi-forms-wfh.png

Image: ZDNet

Furthermore, the DopplePaymer gang also posted a list of 2,583 servers and workstations that hackers claim are part of DMI's internal network, and which they have encrypted and are now holding for ransom.


 dmi-machine-list.png

Image: ZDNet

The purpose of releasing all these files is for extortion. The DopplesPaymer ransomware crew is one of several ransomware gangs that operate "leak sites" where they publish data from hacked companies.

DopplesPaymer operators first share small samples like the one they shared today, and in case the victim isn't intimidated and still refuses to pay the file decryption fee, they leak all files as revenge.

Such extortion tactics have been employed since December 2019, and today, they also saw a major change when the operators of the REvil (Sodinokibi) ransomware gang added a kink in this tactic by launching an eBay-like auction site where they're selling the stolen victim data instead of giving it away for free.