Trucking giant Forward Air hit by new Hades ransomware gang

bleepingcomputer.com/news/security/trucking-giant-forward-air-hit-by-new-hades-ransomware-gang/

Lawrence Abrams

By
Lawrence Abrams

- December 21, 2020
- 04:23 PM
- 0

Trucking and freight logistics company Forward Air has suffered a ransomware attack by a new ransomware gang that has impacted the company's business operations.

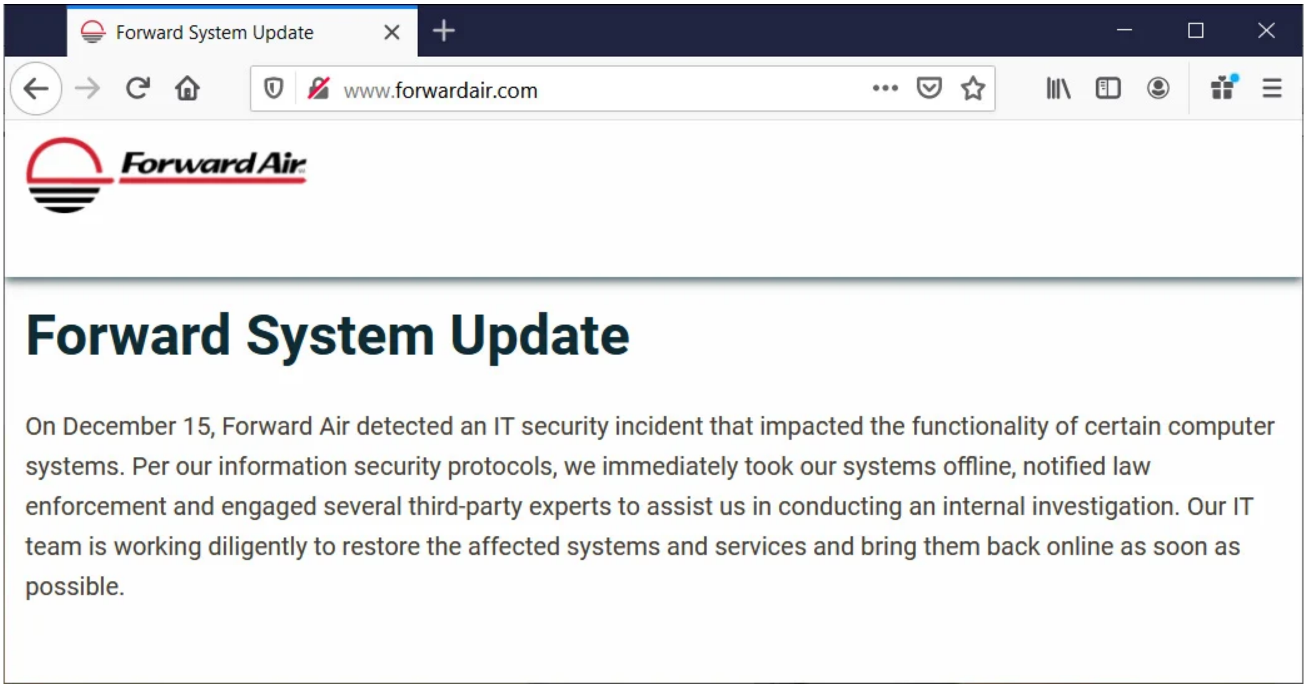
Forward Air is a leading trucking and air freight logistics company based out of Tennessee, USA. The company generated $1.4 billion in revenue for 2019 and employs over 4,300 people.

Last week, FreightWaves reported that Forward Air suffered a cyberattack that forced them to take their systems offline to prevent the attack's spread. Forward Air later confirmed this attack in a statement to BleepingComputer.

"On December 15, Forward Air detected an IT security incident that impacted the functionality of certain computer systems. Per our information security protocols, we immediately took our systems offline, notified law enforcement and engaged several third-party experts to assist us in conducting an internal investigation. Our IT team is working diligently to restore the affected systems and services and bring them back online as soon as possible," Forward Air shared in a statement to BleepingComputer.

According to FreightWaves, the attack has led to business disruption as the paperwork required to release freight from customs was stored on the shutdown systems and is not available.

At this time, Forward Air's website is down and just displays a message about the "IT security incident" and that the site is down while they restore affected systems.



Forward System Update

On December 15, Forward Air detected an IT security incident that impacted the functionality of certain computer systems. Per our information security protocols, we immediately took our systems offline, notified law enforcement and engaged several third-party experts to assist us in conducting an internal investigation. Our IT team is working diligently to restore the affected systems and services and bring them back online as soon as possible.

Forwardair.com outage
Source: BleepingComputer
If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

New Hades ransomware operation is responsible.

Sources have told BleepingComputer today that Forward Air suffered a cyberattack by a new ransomware operation known as Hades.

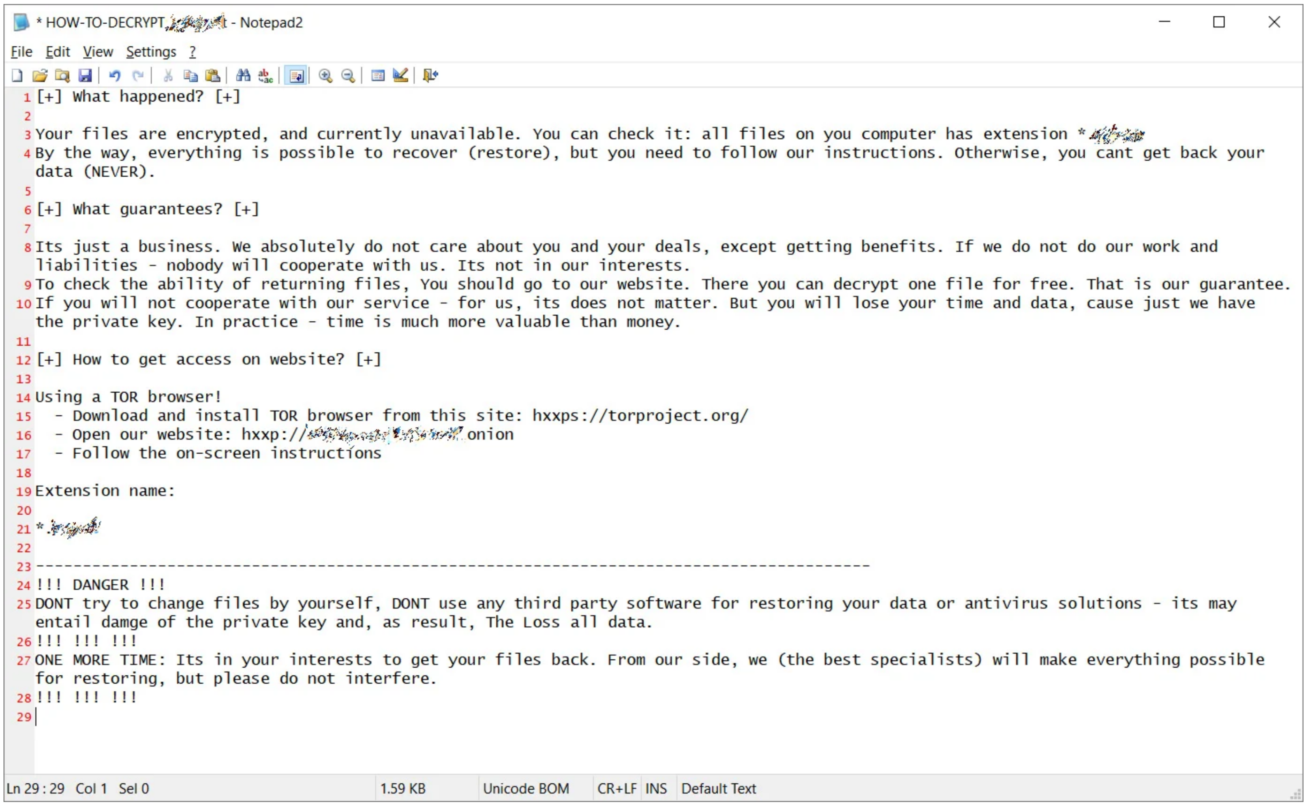
Update 12/21/20 6:37 PM EST: After we published our story, Forward Air filed a Form 8-K with the Securities and Exchange Commission disclosing that they suffered a ransomware attack.

"On December 15, 2020, Forward Air Corporation (the “Company”) detected a ransomware incident impacting its operational and information technology systems, which has caused service delays for many of its customers. Promptly upon its detection of the incident, the

Company initiated response protocols, launched an investigation and engaged the services of cybersecurity and forensics professionals. The Company has also engaged with the appropriate law enforcement authorities," the Form 8-K states.

The Hades ransomware gang behind this attack began operating about a week ago in human-operated attacks against the enterprise.

When encrypting a victim, it will create a ransom note named 'HOW-TO-DECRYPT-[extension].txt' that resembles notes used by the REvil ransomware group, as can be seen below.

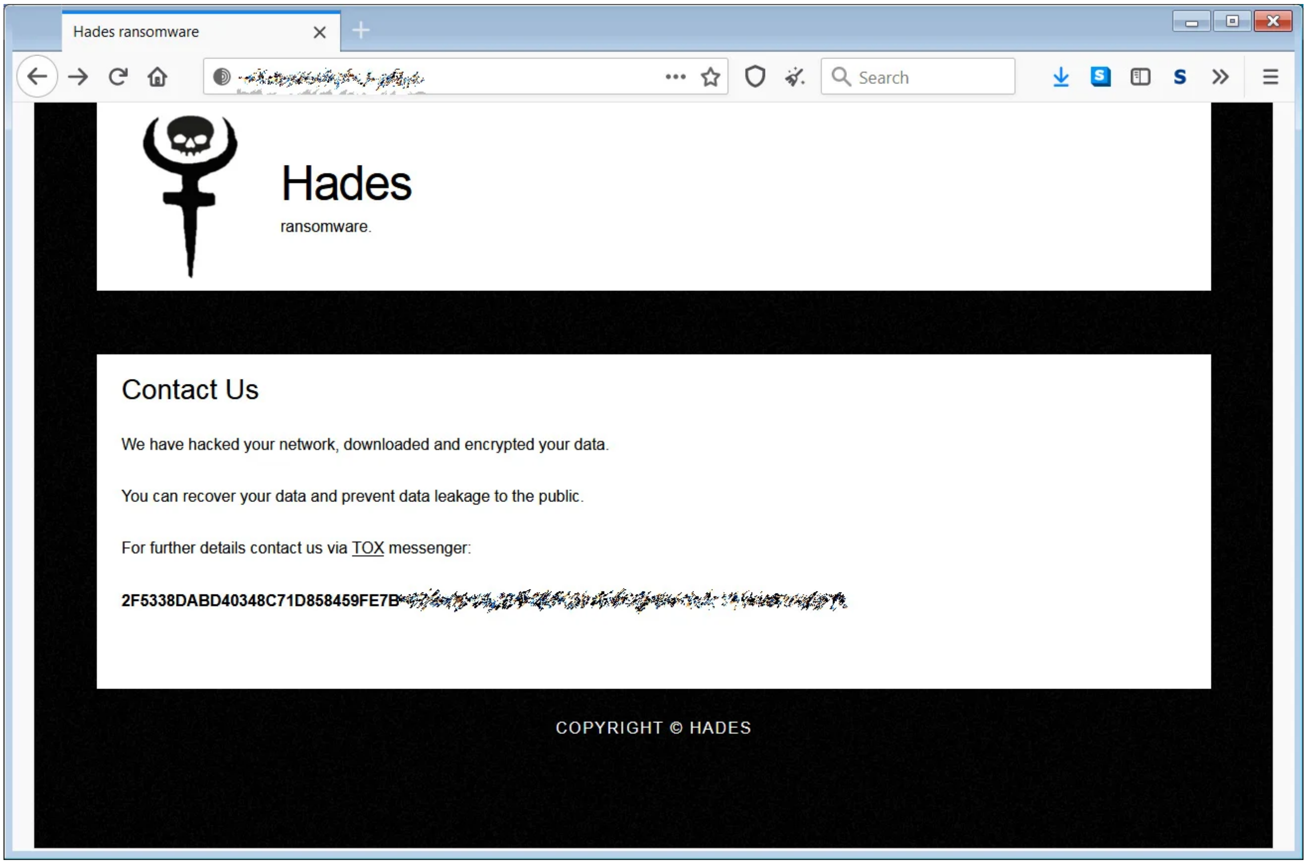

* HOW-TO-DECRYPT[redacted]t - Notepad2
File Edit View Settings ?
Ln 29 : 29 Col 1 Sel 0
1.59 KB
Unicode BOM
CR+LF INS
Default Text

```
[+] What happened? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has extension *[redacted]
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant get back your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

Using a TOR browser!
  - Download and install TOR browser from this site: hxxps://torproject.org/
  - Open our website: hxxp://[redacted] onion
  - Follow the on-screen instructions

Extension name:

*[redacted]

-----------------------------------------------------------------------------------------
!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) will make everything possible for restoring, but please do not interfere.
!!! !!! !!!
```

Hades ransom note

Source: BleepingComputer

Enclosed in the ransom notes is a Tor site URL that is unique to each victim. This URL brings you to a Tor site containing information about the attack and a Tox messenger address that victims can use to contact the attackers, which is the same for all victims.



Hades

ransomware.

Contact Us

We have hacked your network, downloaded and encrypted your data.

You can recover your data and prevent data leakage to the public.

For further details contact us via TOX messenger:

2F5338DABD40348C71D858459FE7B[redacted]

COPYRIGHT © HADES

Hades Tor site
Source: BleepingComputer
When we reached out via Tox to the ransomware actors, they were unwilling to provide any information about their attacks. They did, though, share a Twitter account whose name indicates they will use it to leak files stolen during attacks.

It is not known how much money is demanded to recover files, and a sample of the ransomware has not been found.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New 'Cheers' Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt's ransomware fight hindered by limited reporting

- Forward Air
- Hades
- Ransomware

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.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: