Trucking giant Forward Air reports ransomware data breach

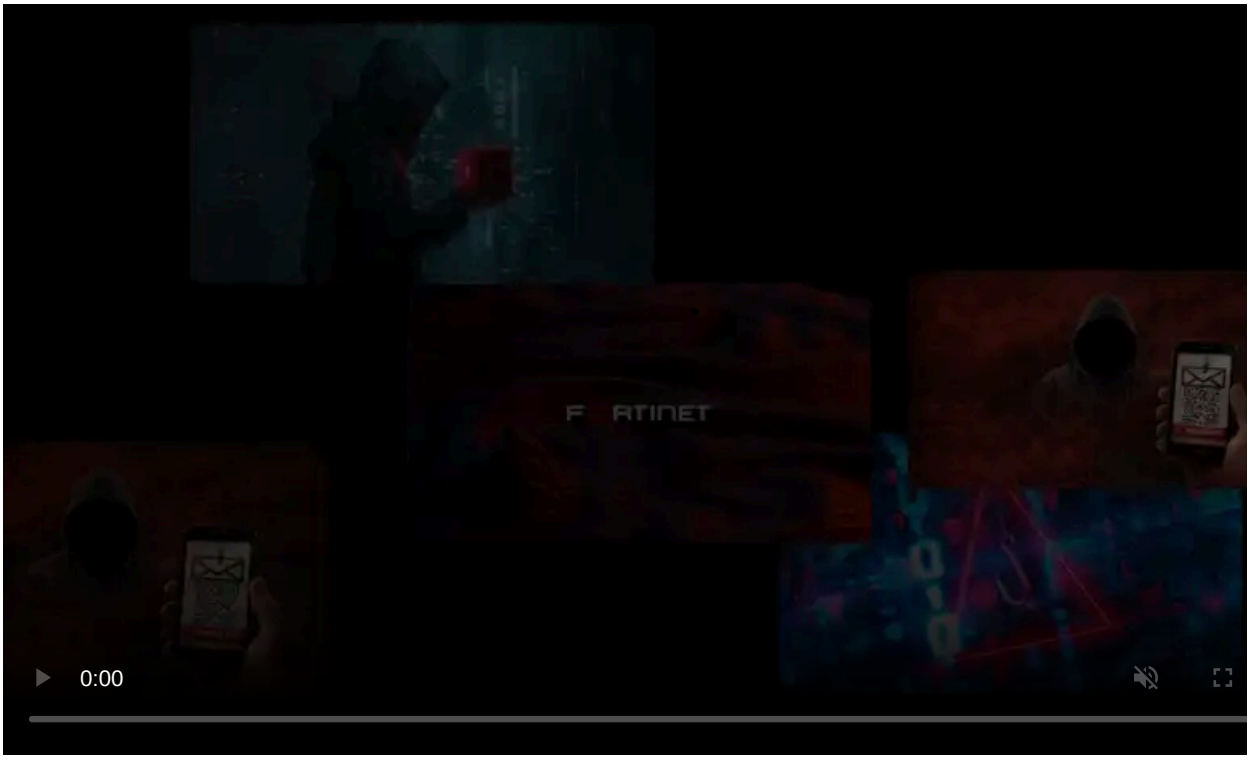
By Lawrence Abrams

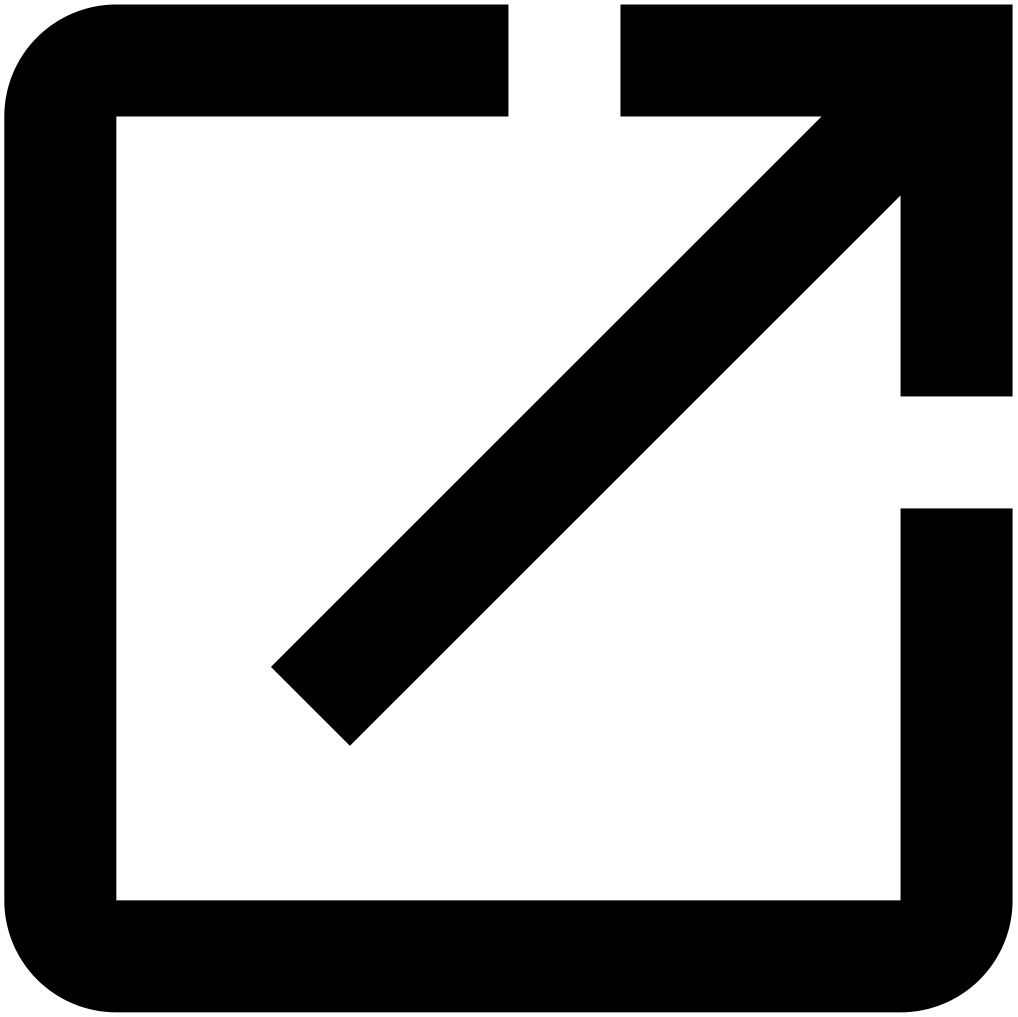
Published: 2021-09-29 · Archived: 2026-04-05 20:47:45 UTC

Trucking giant Forward Air has disclosed a data breach after a ransomware attack that allowed threat actors to access employees' personal information.

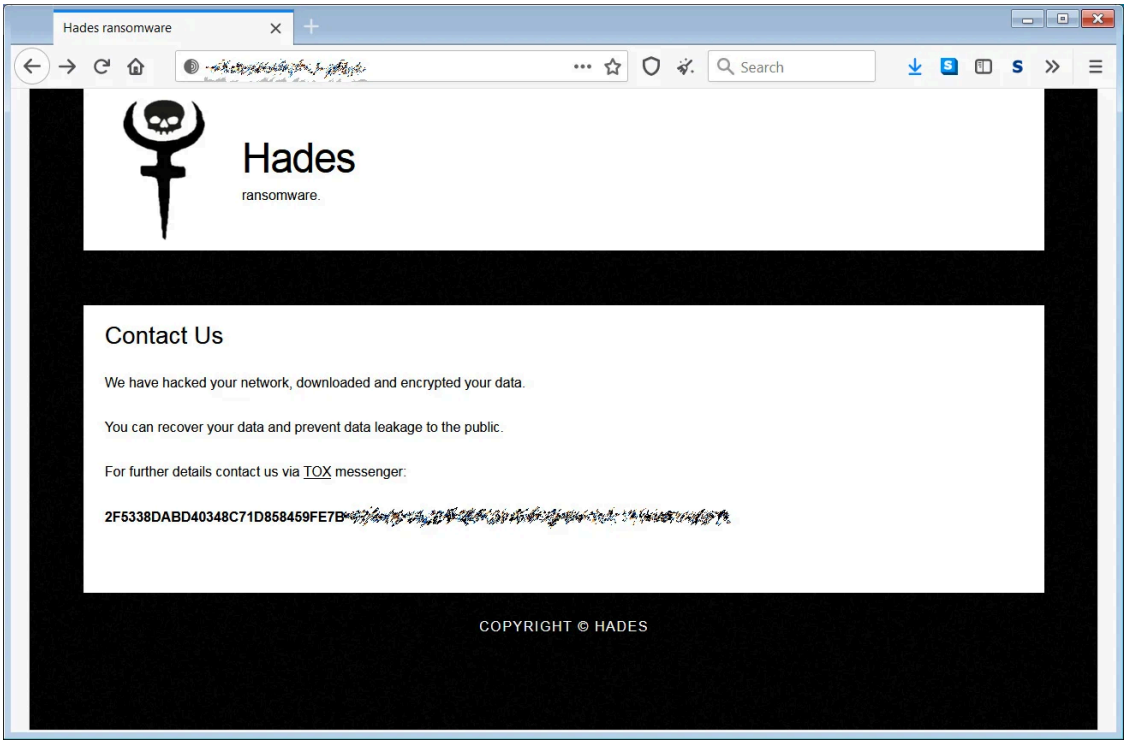
In December 2020, Forward Air suffered a ransomware attack by what was believed to be a new cybercrime gang known as Hades. This attack caused Forward Air to shut down its network, which led to business disruption and the inability to release freight for transport.

An SEC filing by Forward Air states that the company lost $7.5 million of less than load (LTL) freight revenue "primarily because of the Company's need to temporarily suspend its electronic data interfaces with its customers."


F RTINET
0:00



Researchers later revealed that this attack was likely conducted by members of the Evil Corp cybercrime gang, who routinely perform attacks under different ransomware names, such as Hades, to evade US sanctions.



At the time, BleepingComputer was contacted by multiple Forward Air employees concerned that the attack exposed their personal information.

As part of the attack, the threat actors created a Twitter account that they claimed would be used to leak data stolen from Forward Air. However, no data was ever seen leaked by the threat actors.

Forward Air discloses a data breach

Fast forward almost a year, and Forward Air is now disclosing that current and the ransomware attack exposed former employees' data.

"On December 15, 2020, Forward Air learned of suspicious activity occurring within certain company computer systems. Forward Air immediately launched an investigation to determine the nature and scope of the incident," reads a data breach notification sent to Forward Air employees.

"The investigation determined that certain Forward Air systems were accessible in November and early December 2020, and that certain data, which may have included your personal information, was potentially viewed or taken by an unknown actor."

The information that the Evil Corp threat actors potentially accessed includes employees' names, addresses, date of births, Social Security numbers, driver's license numbers, passport numbers, or bank account numbers.

While Forward Air states that there is no indication that the data has been misused, they are offering affected people a free one-year membership to the myTrueIdentity credit monitoring service.

As there is no way to determine if a threat actor has used stolen data, even if they promise not to after a ransom payment, all affected employees should assume that their data has been compromised.

This means that they should monitor their credit reports, bank statements, and be on the lookout for targeted phishing attacks.

Source: https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-reports-ransomware-data-breach/