

Marketing giant RRD confirms data theft in Conti ransomware attack

By Lawrence Abrams

Published: 2022-01-19 · Archived: 2026-04-05 22:26:55 UTC

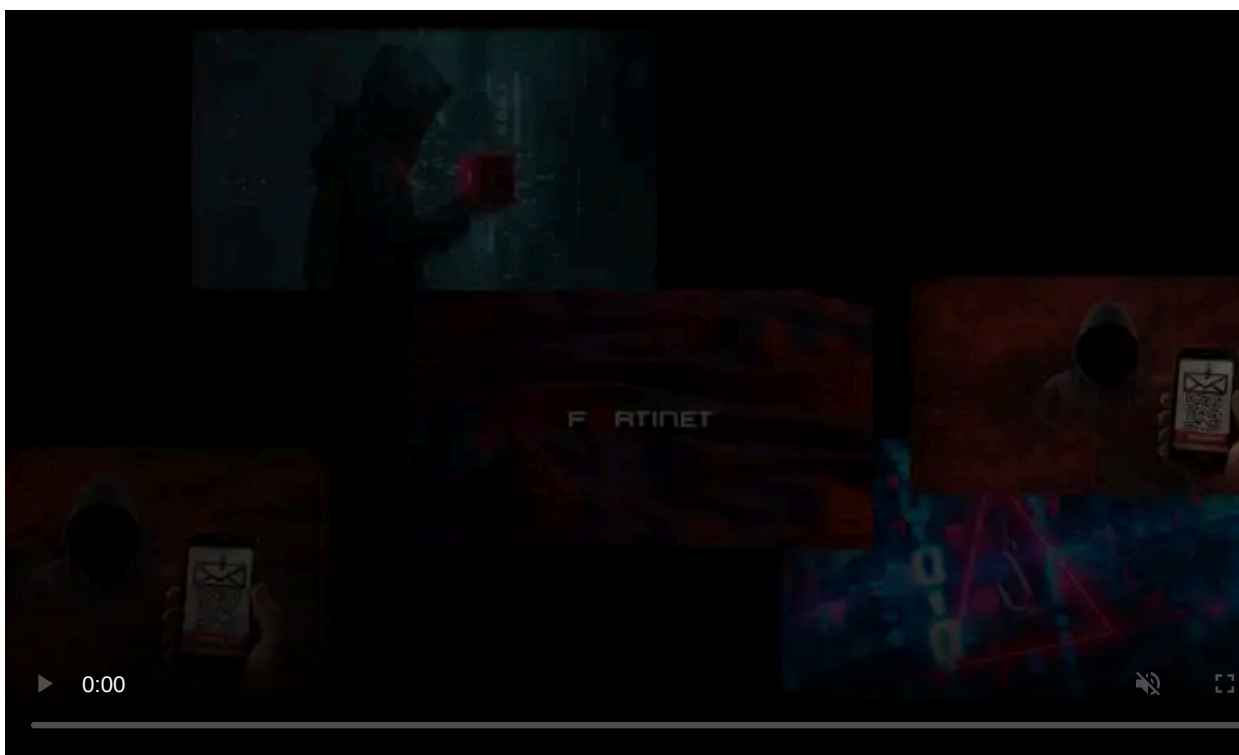


RR Donnelly has confirmed that threat actors stole data in a December cyberattack, confirmed by BleepingComputer to be a Conti ransomware attack.

RR Donnelly (RRD) is a leading integrated services company offering communications, commercial printing, and marketing to enterprise clients. The company employs 33,000 people in over 200 locations and earned \$4.93 billion in 2021.

RRD suffers a Conti ransomware attack

On December 27th, RRD filed a [Form 8-K](#) with the SEC disclosing that they suffered a "systems intrusion in its technical environment" that led to the shut down of their network to prevent the attack's spread.



Visit Advertiser website [GO TO PAGE](#)

The shut down of IT systems led to disruptions for customers, with some [unable to receive printed documents](#) required for vendor payments, disbursement checks, and motor vehicle documentation.

While RRD initially said they were not aware of any client data stolen during the attack, on January 15th, the Conti ransomware gang claimed responsibility and began leaking 2.5GB of data allegedly stolen from RRD.

However, a source told BleepingComputer that Conti soon removed the data from public view after RRD began further negotiations to prevent the release of data.

Yesterday, RRD released an additional 8-K filing confirming that data was stolen during the attack. The company also stated they are taking all appropriate measures to protect its and clients' information.

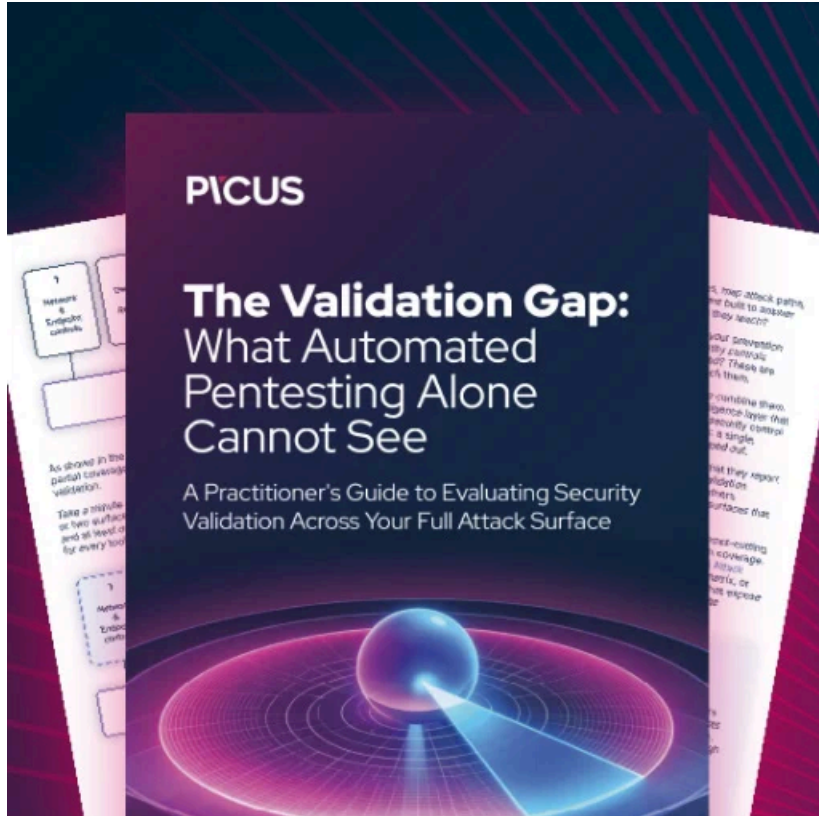
"At this time, however, the Company has become aware that certain of its corporate data was accessed and exfiltrated, the nature of which is being actively examined. Based on information known to date, the Company believes the access and exfiltration was in connection with the previously disclosed systems intrusion and not a new incident," reads the new SEC filing.

"The Company is keeping clients informed of any relevant updates on an ongoing basis and plans to take all appropriate measures to safeguard the integrity of the Company's data and clients' information."

The ransomware attack came just after announcing their definitive merger agreement to be acquired by Chatham Asset Management.

In November, the FBI released a Private Industry Notification warning that ransomware gangs commonly [time their attacks to coincide with significant financial events](#), such as mergers and acquisitions, as leverage to get victims to pay ransoms.

BleepingComputer has reached out to RRD with further questions related to the attack but did not receive a response.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/marketing-giant-rrd-confirms-data-theft-in-conti-ransomware-attack/>