Largest global staffing agency Randstad hit by Egregor ransomware

bleepingcomputer.com/news/security/largest-global-staffing-agency-randstad-hit-by-egregor-ransomware/

Lawrence Abrams

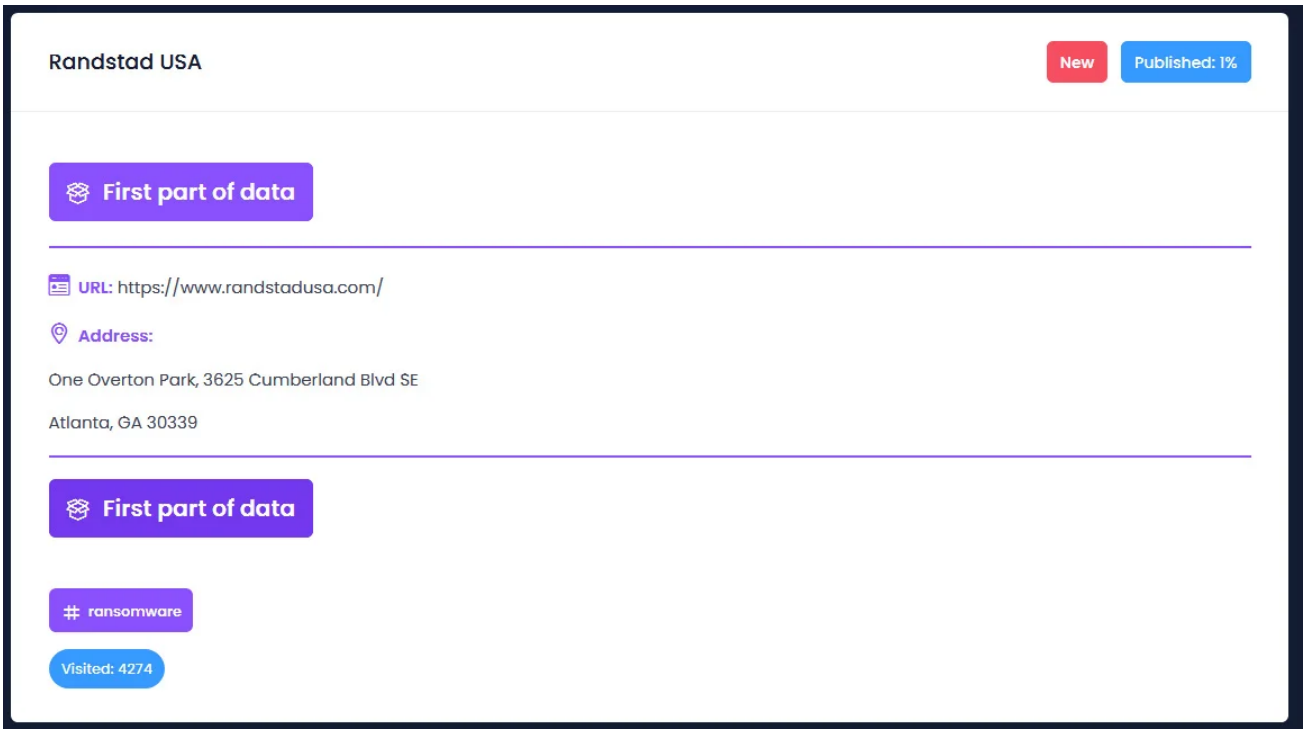
By
Lawrence Abrams

- December 4, 2020
- 10:25 AM
- 0

Staffing agency Randstad NV announced today that their network was breached by the Egregor ransomware, who stole unencrypted files during the attack.

Randstad is the world's largest staffing agency with offices in 38 markets and the owner of the well-known employment website Monster.com. Randstad employs over 38,000 people and generated €23.7 billion in revenue for 2019.

This week, the Egregor ransomware operation published what they claim is 1% of Randstad's data stolen during a recent cyberattack. This leaked data is a 32.7MB archive containing 184 files, including accounting spreadsheets, financial reports, legal documents, and other miscellaneous business documents.



Egregor ransomware data leak site

After the threat actors published their data, Randstad issued a security notification confirming that the Egregor ransomware operation attacked them.

Randstad states that only a limited number of servers were impacted and that their network and business operations continued to operate without disruption.

The company confirmed that data was stolen but is still investigating whether the personal data of clients of employees was accessed. At this time, they believe that only data related to their operations in the US, Poland, Italy, and France was stolen.

"To date, our investigation has revealed that the Egregor group obtained unauthorized and unlawful access to our global IT environment and to certain data, in particular related to our operations in the US, Poland, Italy and France," Randstad disclosed. "They have now published what is claimed to be a subset of that data. The investigation is ongoing to identify what data has been accessed, including personal data, so that we can take appropriate action with regard to identifying and notifying relevant parties,"

The Egregor ransomware operation has been extremely active over the past week, with successful attacks against Metro Vancouver's transit system TransLink and the big-box department store Kmart.

Egregor is a new organized cybercrime ransomware-as-a-service operation that partners with affiliates to compromise networks and deploy their ransomware. As part of this arrangement, affiliates earn 70% of any ransom payments they bring in, and the Egregor operators make a 30% revenue share.

The ransomware gang began operating in the middle of September 2020 after a prominent ransomware group known as Maze shut down their operation. Threat actors told BleepingComputer that many of the affiliates that worked with Maze switched to Egregor, which allowed the new operation to ramp up their attacks quickly.

Other high-profile Egregor attacks include Cencosud, Crytek, Ubisoft, and Barnes and Noble.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Costa Rica declares national emergency after Conti ransomware attacks

Quantum ransomware seen deployed in rapid network attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

- Cyberattack
- Data Exfiltration
- Egregor
- Randstad
- 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

You may also like: