US chemical distributor shares info on DarkSide ransomware data theft

bleepingcomputer.com/news/security/us-chemical-distributor-shares-info-on-darkside-ransomware-data-theft/

Sergiu Gatlan

By
Sergiu Gatlan

- July 3, 2021
- 10:00 AM
- 0

World-leading chemical distribution company Brenntag has shared additional info on what data was stolen from its network by DarkSide ransomware operators during an attack from late April 2021 that targeted its North America division.

Brenntag is the second largest in sales for North America, according to the ICIS report on the Top 100 Chemical Distributors worldwide.

The chemical distribution company is headquartered in Germany and has more than 17,000 employees worldwide at over 670 sites.

Stolen info includes SSNs, medical info, more

Brenntag confirmed the ransomware attack in an email statement sent to BleepingComputer on May 13, saying that it disconnected all impacted systems from the network after the incident was discovered to contain the threat.

However, as revealed in data breach notification letters sent to affected individuals during late June, the chemical distribution firm became aware of the attack on April 28, two days after the DarkSide operators breached its network.

"Our investigation confirmed that Brenntag systems were accessed without authorization starting on April 26, 2021, and/or that some information was taken from our system," the company said.

The data exfiltrated by the DarkSide attackers includes "social security number, date of birth, driver's license number, and select medical information."

Luckily, as Brenntag further explained, third-party cybersecurity forensic experts hired to investigate the incident found no evidence that the stolen information was misused for fraudulent purposes.

The company also asked the impacted individuals (more than 6700 according to info provided to Maine's Attorney General) to review their account statements and keep an eye on their free credit reports to detect any attempts of identity theft and fraud.

"If you find any transactions you do not recognize, contact the business or institution issuing the statement," Brenntag added.

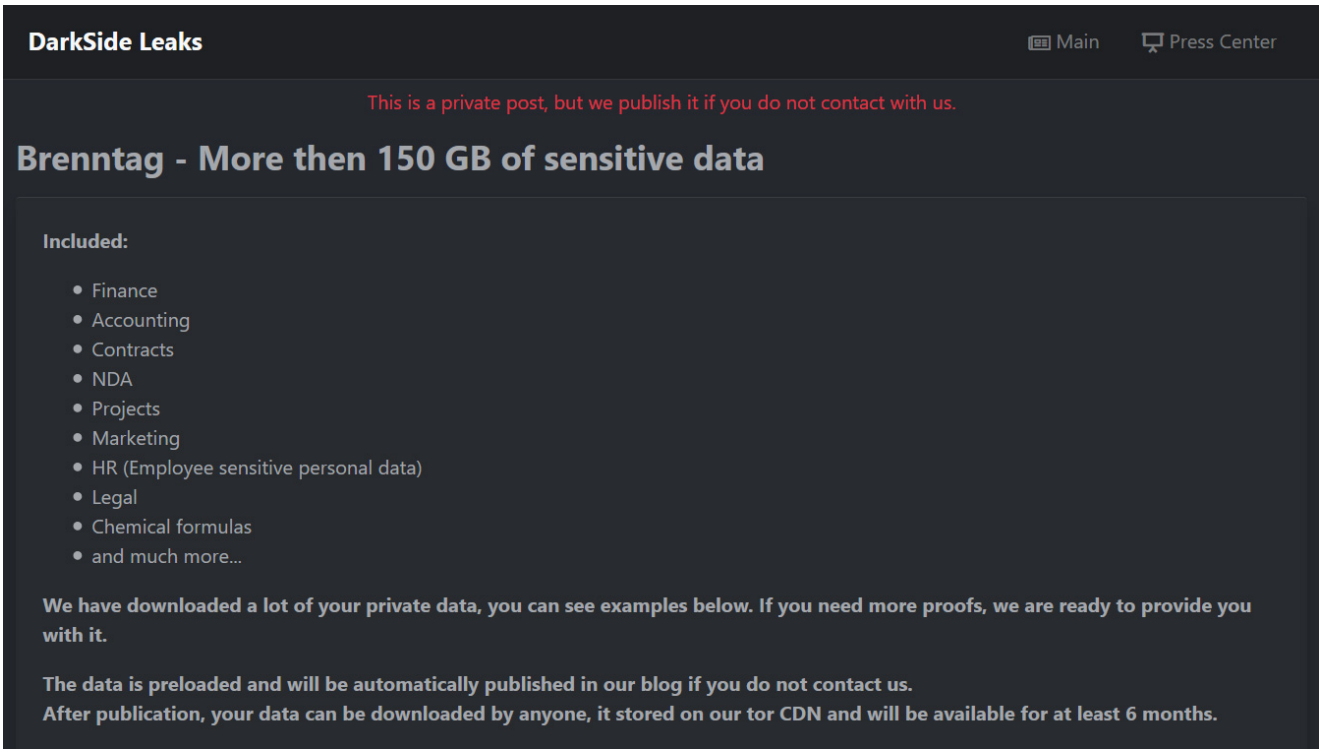
$4.4 million ransom paid to DarkSide

As BleepingComputer reported in May, the chemical distributor company paid a $4.4 million ransom to DarkSide for a decryptor and to prevent the ransomware gang from leaking the stolen data.

The ransom was negotiated down from 133.65 bitcoins (roughly $7.5 million at the time), with Brenntag having sent the $4.4 million to the attackers on May 11, as BleepingComputer was able to confirm.

After the attack, the DarkSide ransomware group claimed to have exfiltrated150GB of data while they had access to Brenntag's systems.

As proof of their claims, the threat actors also created a private data leak page with a description of the types of stolen data and screenshots of some of the files.



Private data leak page sent to Brenntag

The DarkSide affiliate who breached Brenntag's systems claimed to have gotten access to the network using stolen credentials bought from an unknown source.

This aligns with similar tactics employed by other ransomware gangs who regularly purchase stolen credentials (including Remote Desktop credentials) from dark web marketplace.

BleepingComputer reported in April that threat actors used UAS, one of the largest RDP marketplaces, to sell more than 1.3 million stolen credentials since the end of 2018.

The Darkside ransomware gang has been active since August 2020 with a focus on corporate networks and asking millions of dollars for decryptors and the promise not to release stolen data.

The ransomware group landed in the crosshairs of the US government and law enforcement after hitting Colonial Pipeline, the largest fuel pipeline in the US.

Following heightened scrutiny from law enforcement, DarkSide decided to suddenly shut down in May out of fear of being arrested.

DarkSide hit other organizations in the past, including Discount Car and Truck Rentals, Brookfield Residential, and Brazil's Eletrobras and Copel energy companies.

Related Articles:

Ransomware attack exposes data of 500,000 Chicago students

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection