Chemical distributor pays $4.4 million to DarkSide ransomware

bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/

Lawrence Abrams

By
Lawrence Abrams

- May 13, 2021
- 06:24 PM
- 0

Chemical distribution company Brenntag paid a $4.4 million ransom in Bitcoin to the DarkSide ransomware gang to receive a decryptor for encrypted files and prevent the threat actors from publicly leaking stolen data.

Brenntag is a world-leading chemical distribution company headquartered in Germany but with over 17,000 employees worldwide at over 670 sites.

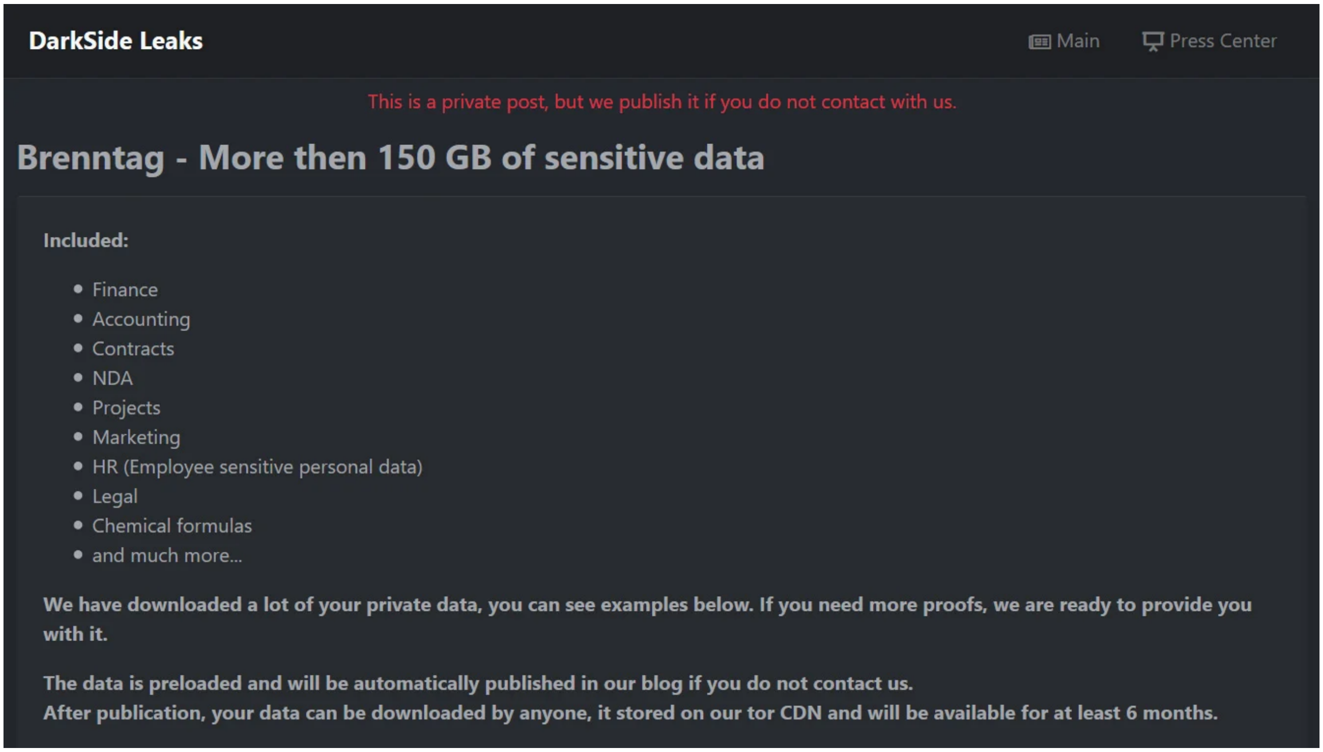
According to the ICS Top 100 Chemical Distributors report, Brenntag is the second largest in sales for North America.

Brenntag confirms cyberattack

At the beginning of May, Brenntag suffered a ransomware attack that targeted their North America division. As part of this attack, the threat actors encrypted devices on the network and stole unencrypted files.

From the information shared with BleepingComputer by an anonymous source, the DarkSide ransomware group claimed to have stolen 150GB of data during their attack.

To prove their claims, the ransomware gang created a private data leak page containing a description of the types of data that were stolen and screenshots of some of the files.



This is a private post, but we publish it if you do not contact with us.

Brenntag - More then 150 GB of sensitive data

Included:

- Finance
- Accounting
- Contracts
- NDA
- Projects
- Marketing
- HR (Employee sensitive personal data)
- Legal
- Chemical formulas
- and much more...

We have downloaded a lot of your private data, you can see examples below. If you need more proofs, we are ready to provide you with it.

The data is preloaded and will be automatically published in our blog if you do not contact us.
After publication, your data can be downloaded by anyone, it stored on our tor CDN and will be available for at least 6 months.

Private data leak page sent to Brenntag

DarkSide initially demanded a 133.65 Bitcoin ransom, valued at approximately $7.5 million at the time. However, after negotiations, BleepingComputer was told that the ransom demand was decreased to $4.4 million, which was paid two days ago.

From the bitcoin address shared with BleepingComputer, we confirmed that Brenntag sent the ransom to the attackers on May 11th.

Today, Brenntag shared a statement with BleepingComputer confirming that they suffered a security incident but did not outright state it was a ransomware attack.

"Brenntag North America is currently working to resolve a limited information security incident," Brenntag told BleepingComputer.

"As soon as we learned of this incident, we disconnected affected systems from the network to contain the threat."

"In addition, third-party cybersecurity and forensic experts were immediately engaged to help investigate. We also informed law enforcement of this incident."

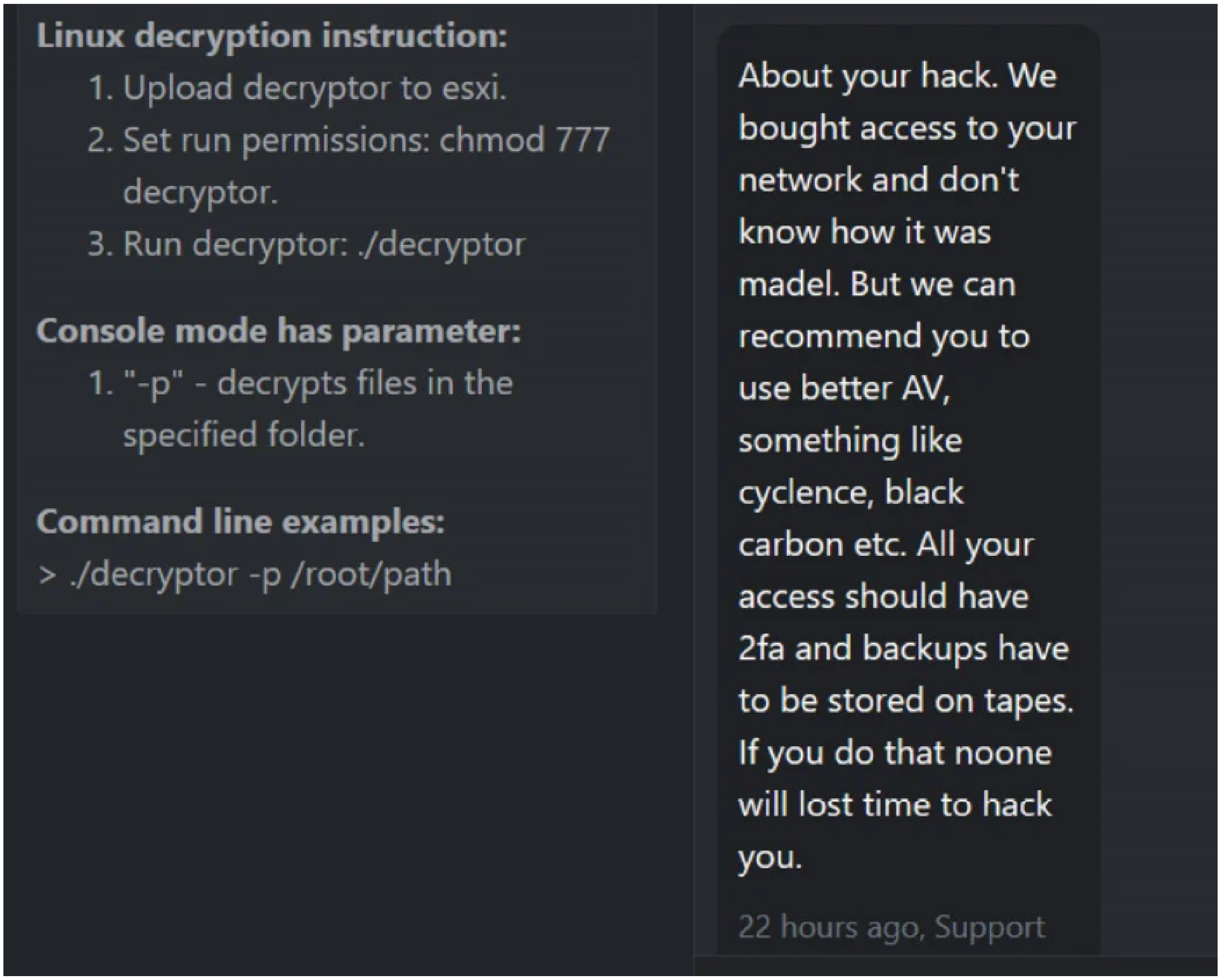
Gained access through stolen credentials

DarkSide is a Ransomware-as-a-Service (RaaS) operation, which is when the ransomware developers partner with third-party affiliates, or hackers, who are responsible for gaining access to a network and encrypting devices.

As part of this arrangement, the core DarkSide team earns 20-30% of a ransom payment, and the rest goes to the affiliate who conducted the attack.

One of the conditions for most ransomware negotiations is that the affiliate discloses how they gained access to a victim's network. This could come in the form of a multi-page security audit report or simply a simple paragraph in the Tor chat screen explaining how they gained access.

In this particular case, the DarkSide affiliate claims to have gotten access to the network after purchasing stolen credentials. However, the DarkSide affiliate does not know how the credentials were originally obtained.



Linux decryption instruction:

1. Upload decryptor to esxi.
2. Set run permissions: chmod 777 decryptor.
3. Run decryptor: ./decryptor

Console mode has parameter:

1. "-p" - decrypts files in the specified folder.

Command line examples:

```
> ./decryptor -p /root/path
```

About your hack. We bought access to your network and don't know how it was madel. But we can recommend you to use better AV, something like cyclence, black carbon etc. All your access should have 2fa and backups have to be stored on tapes. If you do that noone will lost time to hack you.

22 hours ago, Support

DarkSide says they purchase credentials for the network

Ransomware gangs and other threat actors commonly use dark web marketplace to purchase stolen credentials, especially those for Remote Desktop credentials.

Last month, BleepingComputer reported how one of the largest RDP marketplaces, UAS, suffered a breach showing that over the past three years they had access to 1.3 million stolen credentials.

While this was an expensive lesson, and unfortunately all-too-common, the attack illustrates the importance of enforcing multi-factor authentication for all logins on a network and putting all Remote Desktop servers behind a VPN.

If MFA was enabled for account logins, it is unlikely that the DarkSide affiliate would have gained access to the network.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

Ransom payment is roughly 15% of the total cost of ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

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.