BlackCat ransomware implicated in attack on German oil companies

zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/

Home Innovation Security Ransomware

German newspaper Handelsblatt said 233 gas stations across Germany have been affected by the incident.

Written by Jonathan Greig, Staff Writer on Feb. 2, 2022

-
-
-
-
-

An internal report from the Federal Office for Information Security (BSI) said the BlackCat ransomware group was behind the recent cyberattack on two German oil companies that is affecting hundreds of gas stations across northern Germany.

While robust passwords help you secure your valuable online accounts, hardware-based two-factor authentication takes that security to the next level.

Read now

German newspaper *Handelsblatt* managed to obtain the internal report that said Oiltanking's "systems were compromised by the BlackCat ransomware through a previously unknown gateway."

Claudia Wagner, head of communications for Oiltanking GmbH, would not confirm that BlackCat was behind the attack but said they discovered the initial cyber incident on Saturday, January 29th.

"Upon learning of the incident, we immediately took steps to enhance the security of our systems and processes and launched an investigation into the matter. We are working to solve this issue according to our contingency plans, as well as to understand the full scope of the incident. We are undertaking a thorough investigation, together with external specialists and are collaborating closely with the relevant authorities. All terminals continue to operate safely.

"Oiltanking Deutschland GmbH & Co. KG terminals are operating with limited capacity and have declared force majeure. Mabanaft Deutschland GmbH & Co. KG has also declared force majeure for the majority of its inland supply activities in Germany. All parties continue to work to restore operations to normal in all our terminals as soon as possible."

On Tuesday, Royal Dutch Shell said it was forced to reroute to different supply depots because of the issue. Handelsblatt said 233 gas stations across Germany now have to run some processes manually because of the attack.

Also: Apple, SonicWall, Internet Explorer vulnerabilities added to CISA list

Last year, US oil giant Colonial Pipeline dealt with a devastating ransomware attack that crippled its business services and left significant parts of the East Coast without access to gas for less than a week. The Darkside ransomware group was eventually named as the culprit, and some experts believe the group has rebranded multiple times to dodge law enforcement scrutiny.

Emsisoft threat analyst Brett Callow said there are links tying Darkside to another ransomware group -- BlackMatter -- which made a name for itself last summer and fall by attacking agricultural organizations.

"It's likely that BlackCat -- or ALPHV -- is a rebrand of BlackMatter, which was itself a rebrand of Darkside," Callow said. "Intel suggests that the individuals behind the operation fired their devs after the blunder which cost them -- and their affiliates -- multiple millions. New devs were recruited and they were responsible for the development of BlackCat."

Last week Palo Alto Networks' Unit 42 released a deep-dive into the BlackCat ransomware, which emerged in mid-November 2021 as an innovative ransomware-as-a-service (RaaS) group leveraging the Rust programming language and offering affiliates 80-90% of ransom payments.

BlackCat has been seen targeting both Windows and Linux systems, according to Unit 42, which added that it has observed affiliates asking for ransom amounts of up to $14 million. In some instances, affiliates have offered discounts of $9 million if the ransom is paid before the established time. They allow ransom to be paid in Bitcoin and Monero.

Unit 42 found that at least 16.7% of the groups' victims were based in Germany. Last week, Italian fashion brand Moncler was revealed to be a BlackCat victim from December.

screen-shot-2022-01-27-at-6-52-14-pm.png

Unit 42

The incident with Oiltanking follows another cyberattack on billion-dollar German logistics firm Hellmann Worldwide Logistics that took place in December.

James Carder, chief security officer at LogRhythm, said the attack on Oiltanking is a perfect example of how cyberattacks can go beyond just the targeted entity and disrupt the larger supply chain.

"In this case, the oil distributor supplies fuel to 26 companies in Germany, including Shell, which operates over 1,900 gas stations in the country," Carder said.

"While the supply of fuel has not been affected in the attack, impact remains consequential with IT systems responsible for the automation of tank loading and unloading processes, something that cannot be done manually, being forced offline for the time being. The 13 tank farms that Oiltanking operates cannot currently serve trucks, so the firm has turned to alternative methods. The economic impact of cyberattacks affecting the greater supply chain can prove to be extremely detrimental."