German tech giant Software AG down after ransomware attack

Home Innovation Security

Exclusive: The Clop ransomware gang is demanding more than $20 million from German tech firm Software AG.

Written by Catalin Cimpanu, Contributor on Oct. 9, 2020

-
-
-
-
-

software-ag-logo.png

Image: Software AG

[Software AG](#), one of the largest software companies in the world, has suffered a ransomware attack over the last weekend, and the company has not yet fully recovered from the incident.

A ransomware gang going by the name of "[Clop](#)" has breached the company's internal network on Saturday, October 3, encrypted files, and asked for more than $20 million to provide the decryption key.

Earlier today, after negotiations failed, the Clop gang published screenshots of the company's data on a website the hackers operate on the dark web (a so-called [leak site](#)).

The screenshots show employee passport and ID scans, employee emails, financial documents, and directories from the company's internal network.

saoftware-ag.png

Image: ZDNet

Software AG disclosed the incident on Monday when it revealed it was facing disruptions on its internal network "due to [a] malware attack."

The company said that services to customers, including its cloud-based services, remained unaffected and that it was not aware "of any customer information being accessed by the malware attack." This statement was recanted in a later press release two days later, when Software AG admitted to finding evidence of data theft.

The message about the attack remained on its official website homepage all week, including today.

Software AG did not return phone calls today for additional details or comments about the incident.

A copy of the ransomware binary used against Software AG was discovered earlier this week by security researcher MalwareHunterTeam. The $20+ million ransom demand is one of the largest ransom demands ever requested in a ransomware attack.

Image: supplied

The ID provided in this ransom note allows security researchers to view the online chats between the Clop gang and Software AG on a web portal managed by the ransomware group. At the time of writing, there is no evidence the German company paid the ransom demand.

clop-software-ag-chat.jpg

Image: supplied

Software AG is Germany's second-largest company with more than 10,000 enterprise customers across 70 countries. Some of the company's most recognizable customers include Fujitsu, Telefonica, Vodafone, DHL, and Airbus.

Its product line includes business infrastructure software such as database systems, enterprise service bus (ESB) frameworks, software architecture (SOA), and business process management systems (BPMS).