Software AG IT giant hit with $23 million ransom by Clop ransomware

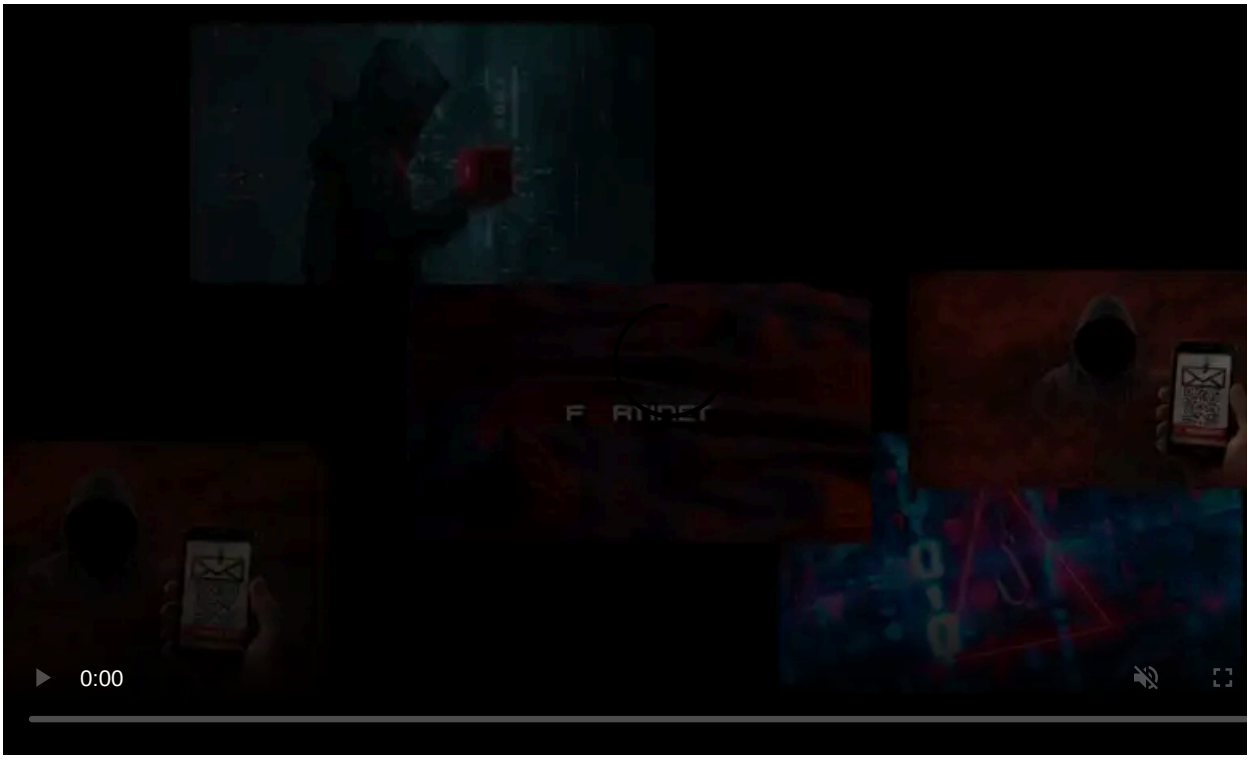
By Sergiu Gatlan

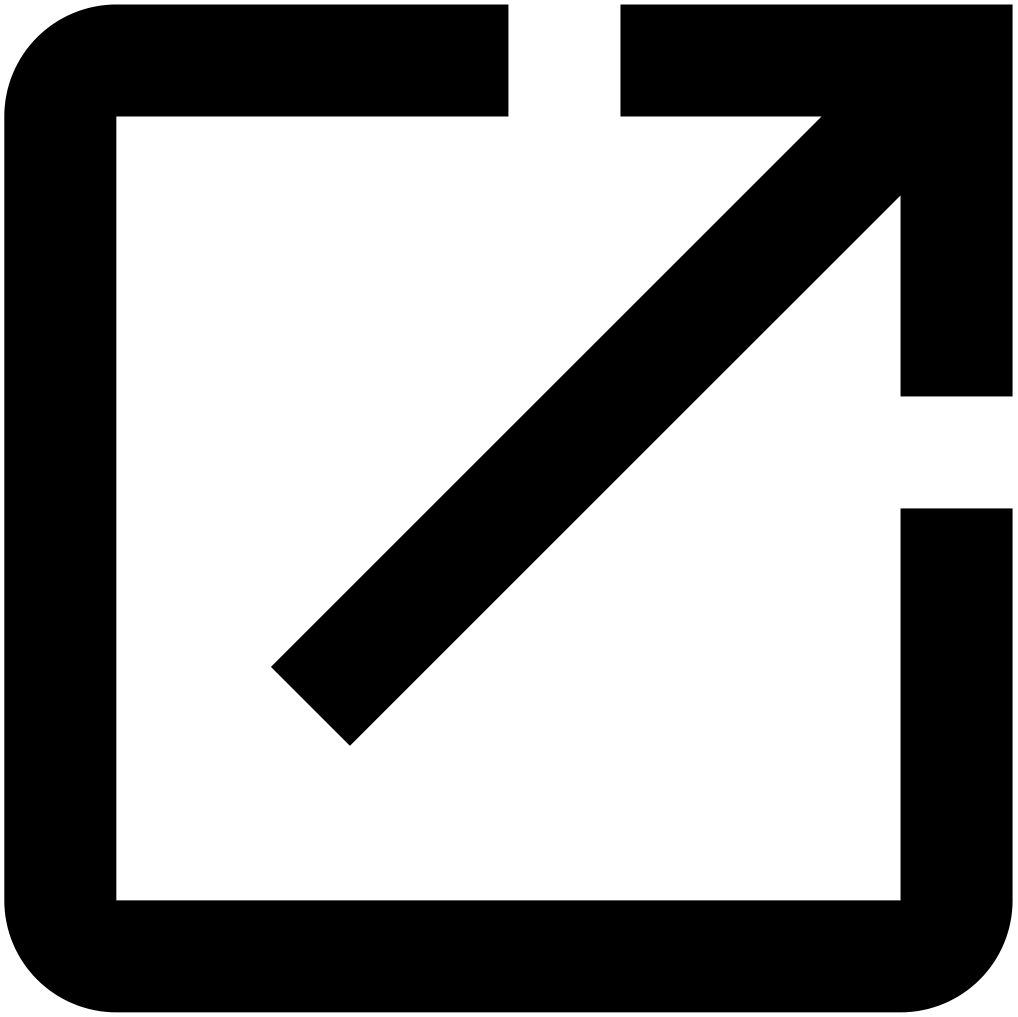
Published: 2020-10-09 · Archived: 2026-04-05 20:26:40 UTC

The Clop ransomware gang hit the network of German enterprise software giant Software AG last Saturday, asking for a ransom of $23 million after stealing employee information and company documents.

Software AG is a software company headquartered in Darmstadt, Germany, with more than 5,000 employees and operations in over 70 countries around the globe.

Software AG's customer list includes organizations from government, banking, transportation, insurance, retail, and more, Airbus, Lufthansa, DHL, Telefonica, Credit Suisse, and Continental being just a small sample of the 70% of Fortune 1000 companies that use its products.


0:00



Attack affected Software AG's internal network

"The IT infrastructure of Software AG is affected by a malware attack since the evening of 3 October 2020," says a press release issued by the company on Monday.

Software AG also says that the ransomware attack only affected its internal network while customer cloud services were unaffected.

"While services to its customers, including its cloud-based services, remain unaffected, as a result, Software AG has shut down the internal systems in a controlled manner in accordance with the company's internal security regulations," the software giant adds.

"The company is in the process of restoring its systems and data in order to resume orderly operation." Software AG added that its internal communication and helpdesk services are still affected by the attack.

In a press release published three days later, on Thursday, Software AG said that it found "first evidence that data was downloaded from Software AG's servers and employee notebooks."

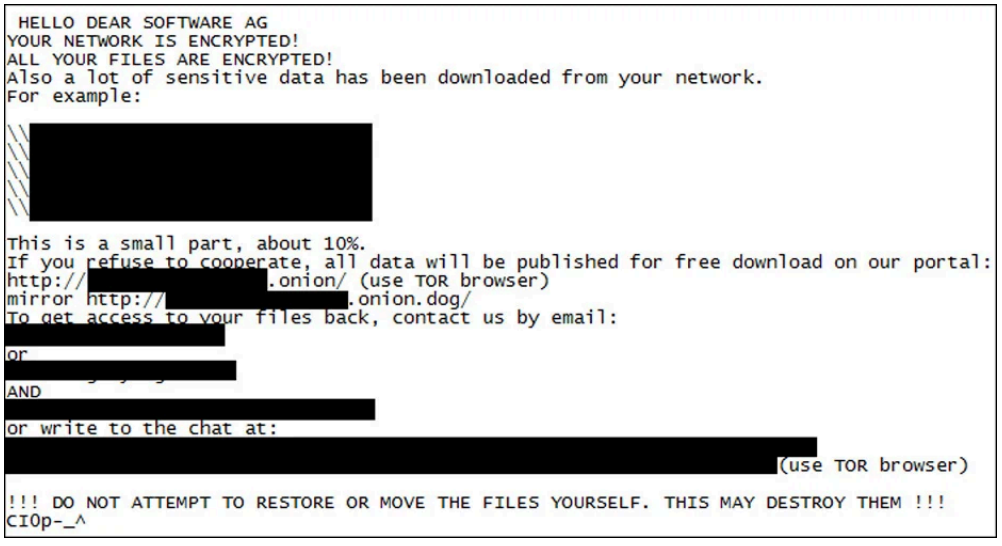
If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

Clop ransomware asks for a $23 million ransom

The company says that this was a "malware attack" and doesn't mention any details related to ransomware in its press releases.

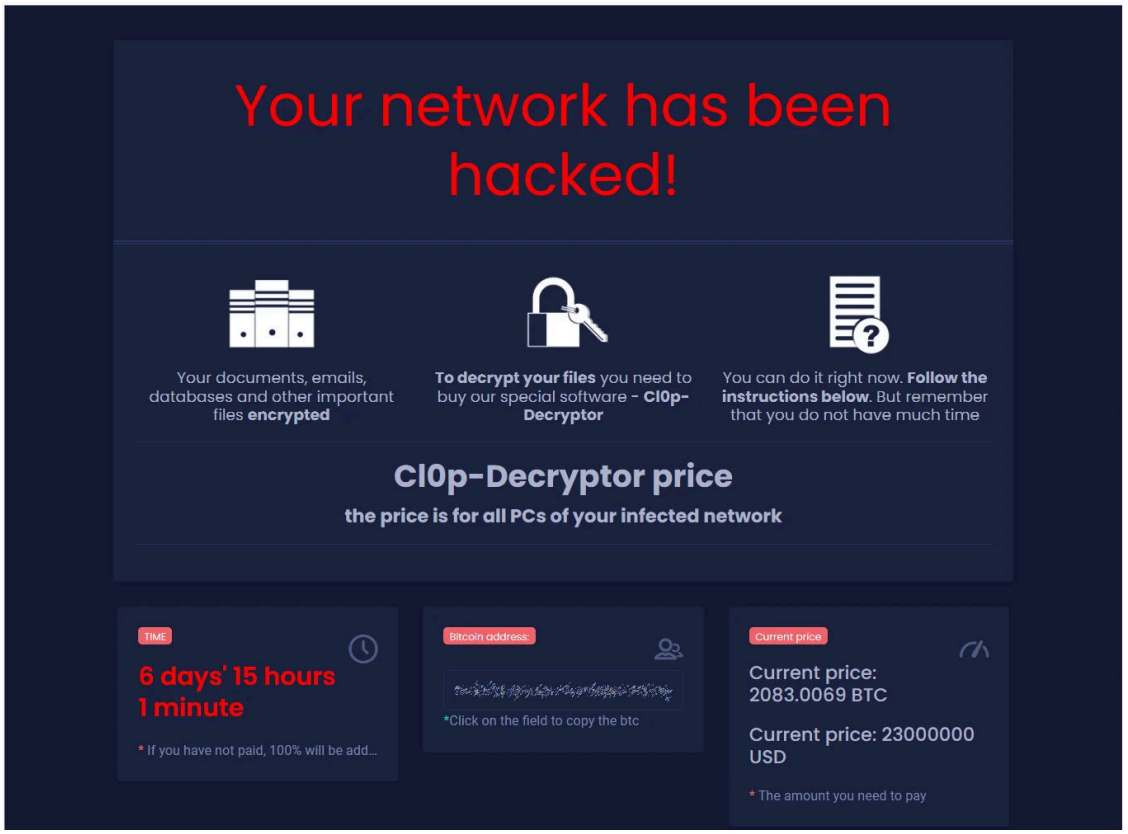
However, BleepingComputer was able to obtain the Software AG ransom note and a link to their chat on Clop's Tor payment site from security researcher MalwareHunterTeam.

MalwareHunterTeam told BleepingComputer that they gained access to this information after finding the Clop ransomware executable used in the attack on Software AG.

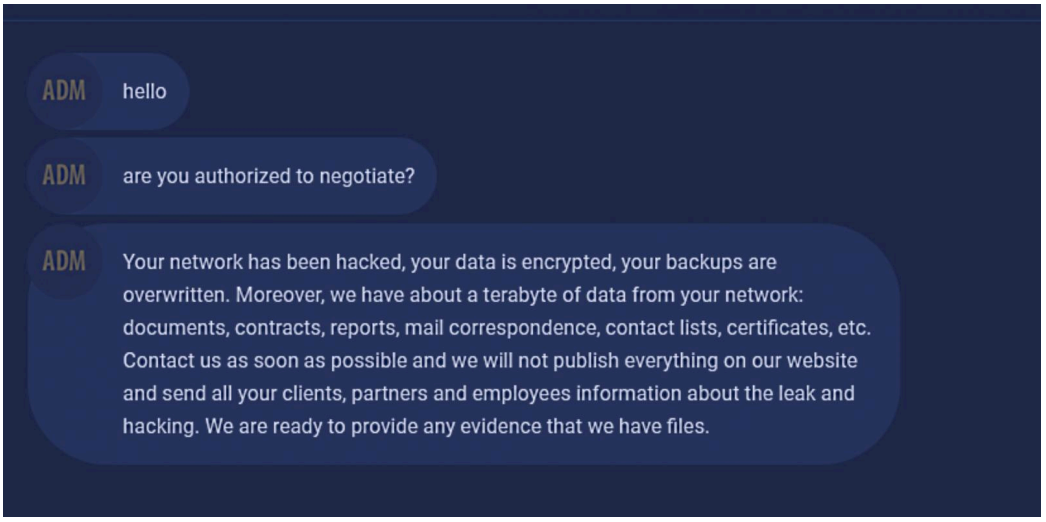


Software AG ransom note

The Tor payment site showing the Software AG ransom demand shows that the ransom asked by Clop for decrypting all encrypted computers on the company's network is $23,000,000 (or 2083,0069 BTC).



According to the chat section of Clop ransomware's leak site, the attackers were able to steal information on employees' passports, health bills, and emails, also publishing a screenshot with a folder tree containing additional info potentially stolen from Software AG.



The chat on the Software AG payment site shows the Clop actors threatening to publish the entire batch of roughly 1 TB of data they claim to have stolen from Software AG's devices including "documents, contracts, reports, mail correspondence, contact lists, certificates, etc."

Clop ransomware was also behind the attack on Maastricht University on December 23, 2019. In February, Maastricht University confirmed that it paid the 30 bitcoin ransom requested by the Clop ransomware gang.

BleepingComputer has contacted Software AG with questions related to this attack but has not heard back at this time.

Source: https://www.bleepingcomputer.com/news/security/software-ag-it-giant-hit-with-23-million-ransom-by-clop-ransomware/