Clop ransomware gang starts extorting MOVEit data-theft victims

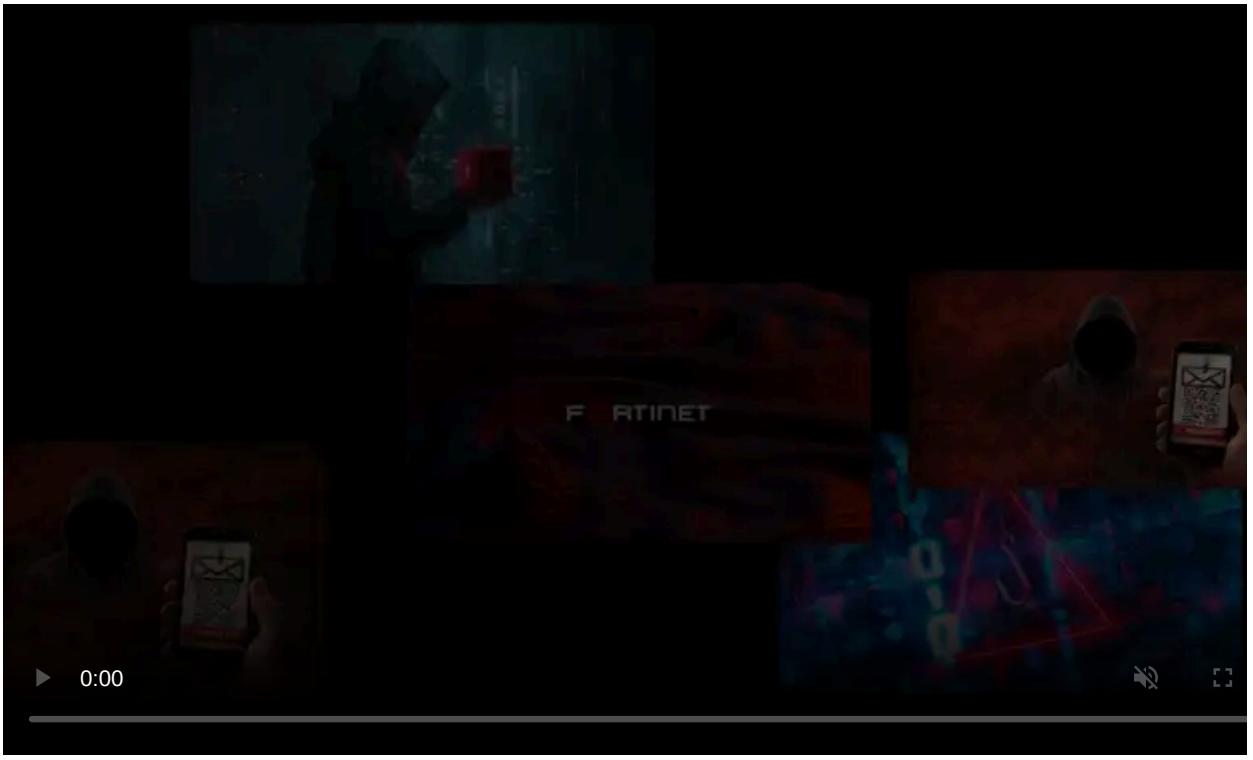
By Lawrence Abrams

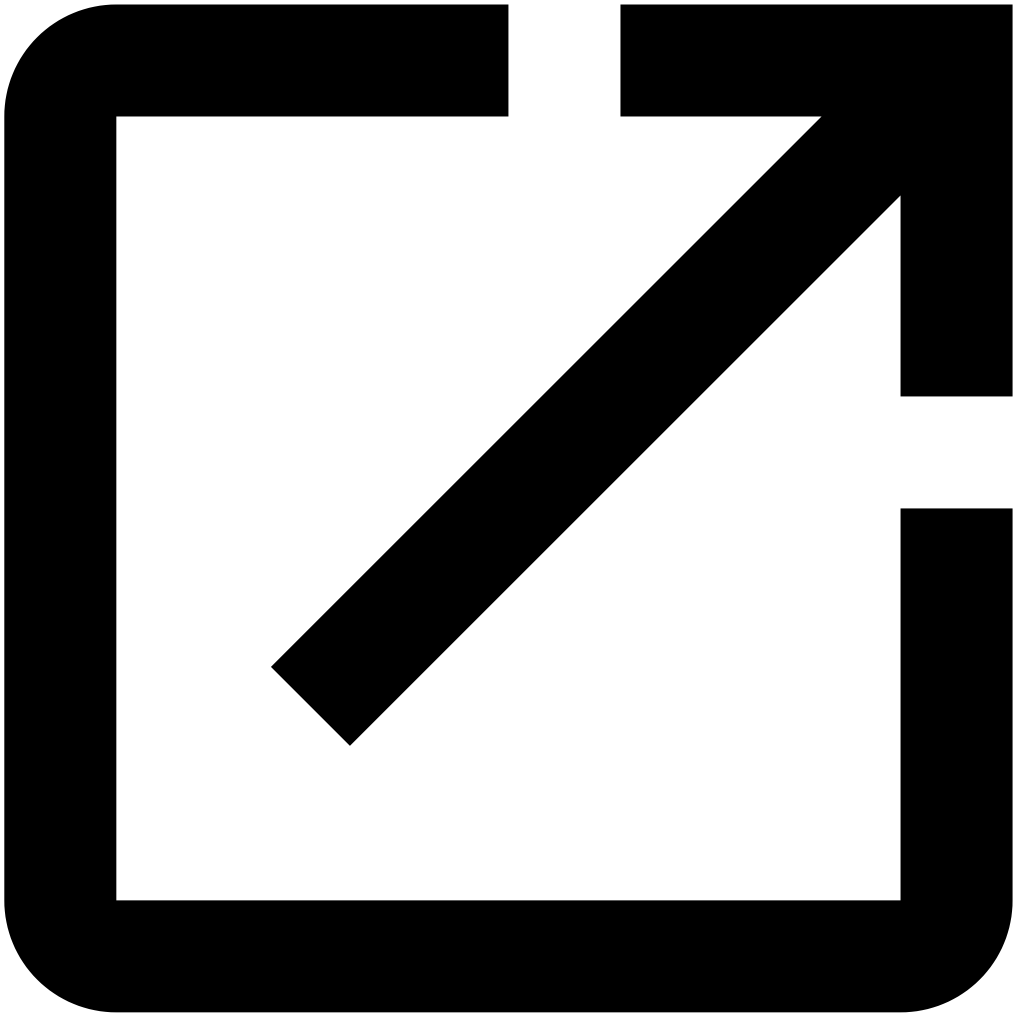
Published: 2023-06-15 · Archived: 2026-04-05 21:13:24 UTC

The Clop ransomware gang has started extorting companies impacted by the MOVEit data theft attacks, first listing the company's names on a data leak site—an often-employed tactic before public disclosure of stolen information

These entries come after the threat actors exploited a zero-day vulnerability in the MOVEit Transfer secure file transfer platform on May 27th to steal files stored on the server.

The Clop gang took responsibility for the attacks, claiming to have breached "hundreds of companies" and warning that their names would be added to a data leak site on June 14th if negotiations did not occur.


F RTINET
0:00



If an extortion demand is not paid, the threat actors say they will begin leaking stolen data on June 21st.

Clop begins extorting companies

Yesterday, the Clop threat actors listed thirteen companies on their data leak site but did not state if they were related to the MOVEit Transfer attacks or were ransomware encryption attacks.

Since then, one of the companies, Greenfield CA, has been removed, indicating the listing was either a mistake or negotiations are taking place.

Five of the listed companies, British multinational oil and gas company Shell, UnitedHealthcare Student Resources (UHSR), the University of Georgia (UGA) and University System of Georgia (USG), Heidelberger Druck, and Landal Greenparks, have since confirmed to BleepingComputer that they were impacted in varying degrees by the MOVEit attacks.

Shell said only a small number of employees and customers were impacted and Landal told BleepingComputer the threat actors accessed the names and contact information for approximately 12,000 guests.

The University System of Georgia, University of Georgia, and UnitedHealthcare Student Resources told BleepingComputer they are still investigating the attack and will disclose any breaches if discovered.

German printing company Heidelberger Druck told BleepingComputer that while they use MOVEit Transfer, their analysis indicates it did not lead to any data breach.

Putnam Investments, who is also listed on Clop's data leak site, told BleepingComputer they are looking into the matter.

While the other companies listed on Clop's site have not responded to our emails, Macnica security researcher Yutaka Sejiyama shared data with BleepingComputer confirming that they currently use the MOVEit Transfer platform or have done so in the past.

Already disclosed data breaches

Other organizations who have already disclosed MOVEit Transfer breaches include, Zellis (BBC, Boots, and Aer Lingus, Ireland's HSE through Zellis), the University of Rochester, the government of Nova Scotia, the US state of Missouri, the US state of Illinois, BORN Ontario, Ofcam, Extreme Networks, and the American Board of Internal Medicine.

In similar attacks in the past using zero-day vulnerabilities in Accellion FTA, GoAnywhere MFT, and SolarWinds Serv-U managed file transfer attacks, the threat actors demanded $10 million ransoms to prevent the leaking of data.

BleepingComputer has learned the extortion operation was not very successful in the GoAnywhere extortion attempts, with companies preferring to disclose data breaches rather than pay a ransom.

Today, CNN reported that the U.S. Cybersecurity and Infrastructure Security Agency (CISA) was working with several U.S. federal agencies had also been breached using the MOVEit zero-day vulnerability. Two U.S. Department of Energy (DOE) entities were also compromised, according to Federal News Network.

However, the Clop threat actors previously told BleepingComputer that they automatically deleted any data stolen from the government.

"I want to tell you right away that the military, children's hospitals, GOV etc like this we no to attack, and their data was erased," claimed the ransomware operation.

Unfortunately, once data is stolen, there is no way to confirm if data is actually deleted as promised, and should be assumed to be at risk.

Source: https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-starts-extorting-moveit-data-theft-victims/