Shutterfly says Clop ransomware attack did not impact customer data

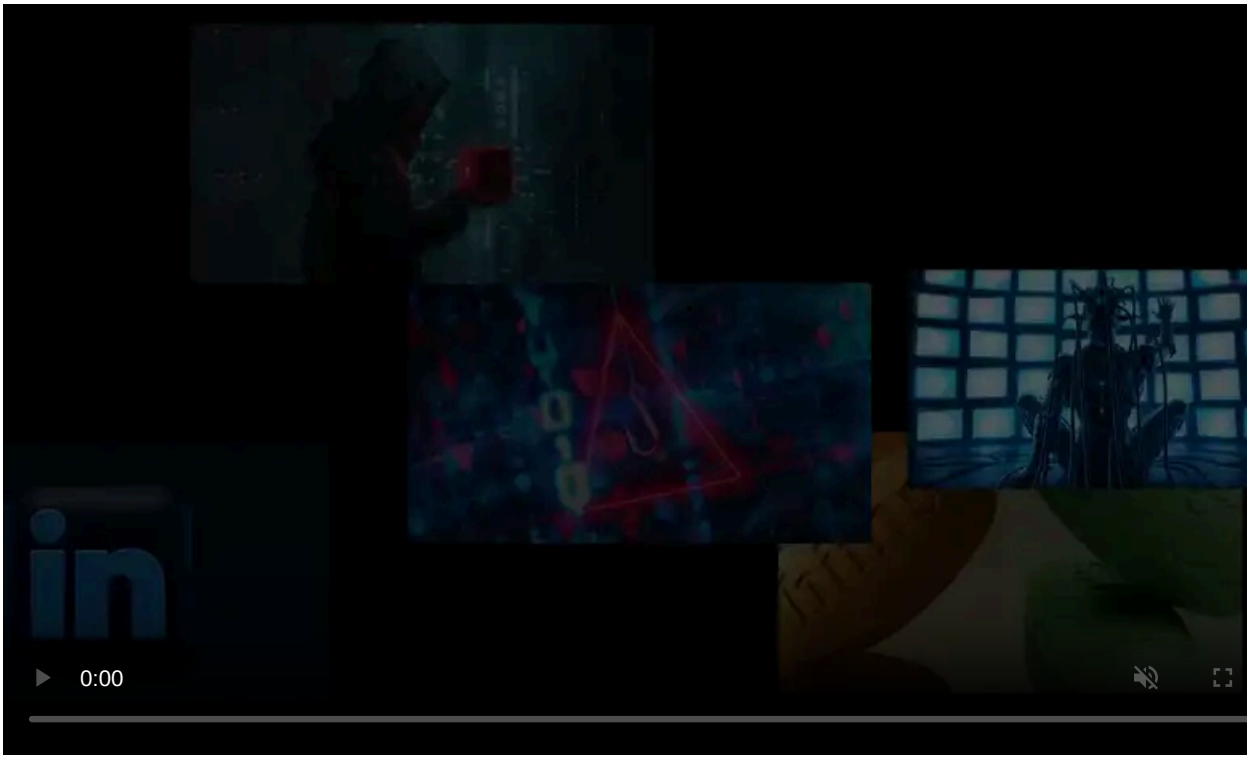
By Ax Sharma

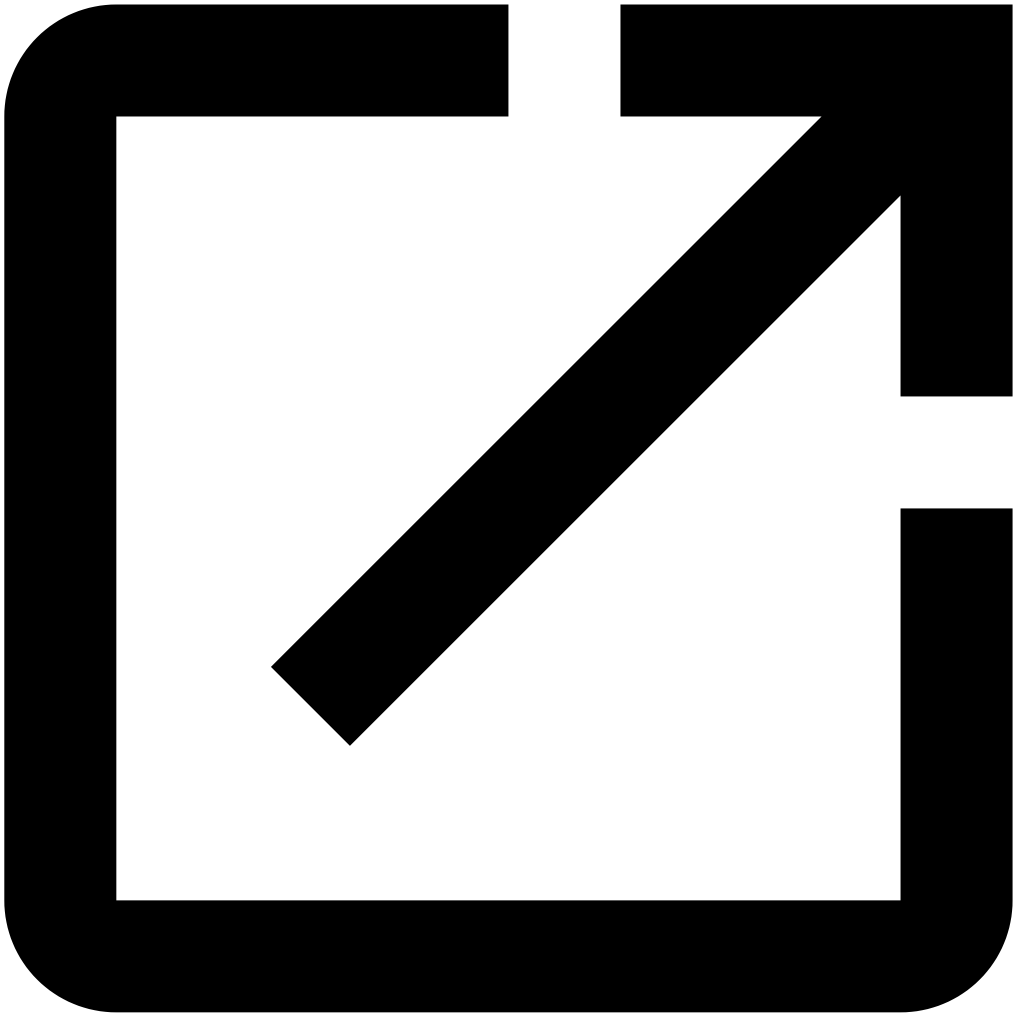
Published: 2023-07-14 · Archived: 2026-04-05 15:38:11 UTC

Shutterfly, an online retail and photography manufacturing platform, is among the latest victims hit by Clop ransomware.

Over the last few months, Clop ransomware gang has been exploiting a vulnerability in the MOVEit File Transfer utility to breach hundreds of companies to steal their data and attempt extortion against them.

Shutterfly offers photography-related services to consumers, the enterprise, and education through various brands, including Shutterfly.com, BorrowLenses, GrooveBook, Snapfish, and Lifetouch.

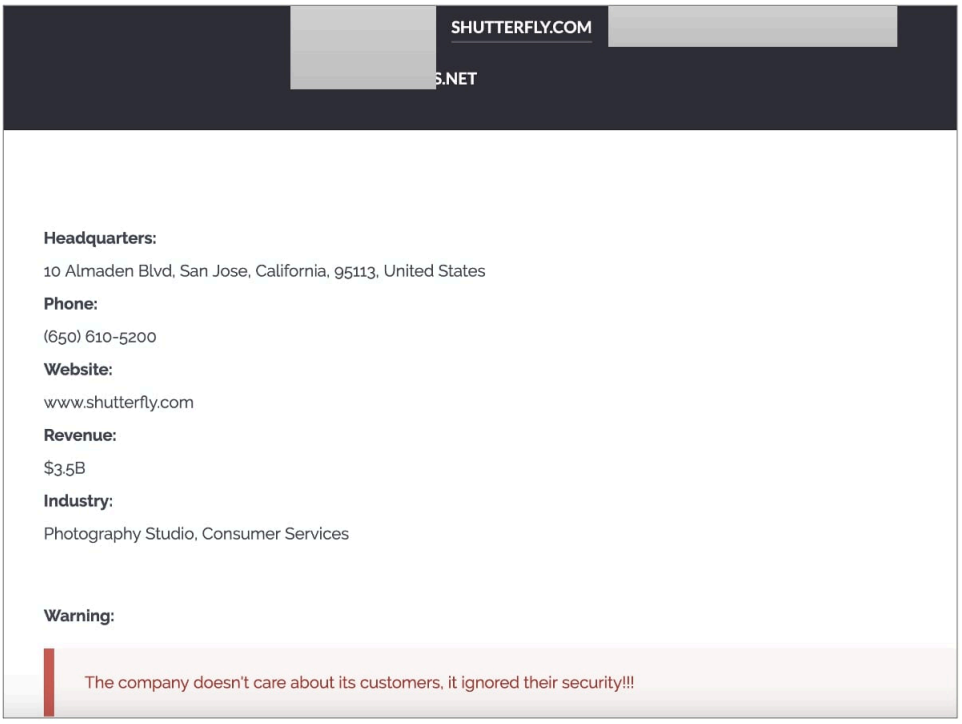

0:00



During ransomware attacks, threat actors will gain access to a corporate network and steal data and files as they spread throughout the system. Once they gain access to a Windows domain controller, and after harvesting all valuable data, they deploy their ransomware to encrypt all network devices.

Shutterfly: customer and employee data safe

This week, Clop ransomware gang published Shutterfly's name on its data leak site, among other companies it has targeted, largely via the MOVEit SQL Injection vulnerability, tracked as CVE-2023-34362.



Clop lists Shutterfly on its data leak site (BleepingComputer)

"Shutterfly can confirm that it was one of the many companies impacted by the MOVEit vulnerability. Shutterfly's enterprise business unit, Shutterfly Business Solutions (SBS), has used the MOVEit platform for some of its operations," confirmed a Shutterfly spokesperson to BleepingComputer.

"Upon learning of the vulnerability in early June, the company quickly took action, taking relevant systems offline, implementing patches provided by MOVEit, and commencing a forensics review of certain systems with the assistance of leading forensic firms."

The company did not comment on how much was the ransom demand but states that customer and employee data are safe.

"After a thorough investigation with the assistance of a leading third-party forensics firm, we have no indication that that any Shutterfly.com, Snapfish, Lifetouch nor Spoonflower consumer data nor any employee information was impacted by the MOVEit vulnerability."

In March 2022, Shutterfly had disclosed being hit by a Conti ransomware attack that occurred in December 2021. At the time of that attack, a source informed BleepingComputer that Conti had encrypted over 4,000 devices and 120 VMware ESXi servers belonging to Shutterfly.

Hundreds impacted by MOVEit vulnerabilities

In June, Clop told BleepingComputer that by exploiting this flaw, it had breached servers belonging to "hundreds of companies" to steal data, which is evident from a significant number of organizations that have thus far disclosed being breached in Clop's MOVEit hacking spree.

Some prominent names like the British multinational oil and gas company, Shell, Deutsche Bank, the University of Georgia (UGA) and University System of Georgia (USG), UnitedHealthcare Student Resources (UHSR), Heidelberger Druck, and Landal Greenparks—have since confirmed to BleepingComputer that they were impacted in the attacks.

Other organizations that have already disclosed MOVEit Transfer breaches include Zellis (and its customers BBC, Boots, Aer Lingus, and Ireland's HSE), Ofcam, the government of Nova Scotia, the US state of Missouri, the US state of Illinois, the University of Rochester, the American Board of Internal Medicine, BORN Ontario, SOVOS [1, 2], and Extreme Networks.

Earlier, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) also revealed that several U.S. federal agencies had been breached, per a CNN report. Two U.S. Department of Energy (DOE) entities were also compromised, according to Federal News Network.

In June, MOVEit Transfer customers were urged to remediate a separate SQL Injection flaw (tracked as CVE-2023-35708), PoC exploits for which had surfaced online.

Last week, MOVEit resolved yet another critical SQL Injection flaw (tracked as CVE-2023-36934) and warned customers to patch their applications.

Customers using the MOVEit File Transfer utility should ensure their instances are up to date and watch out for any new vulnerabilities that could be exploited in the wild.

BleepingComputer continues to monitor and cover incidents as well as vulnerability advisories related to the program.
