Clop ransomware gang begins extorting GoAnywhere zero-day victims

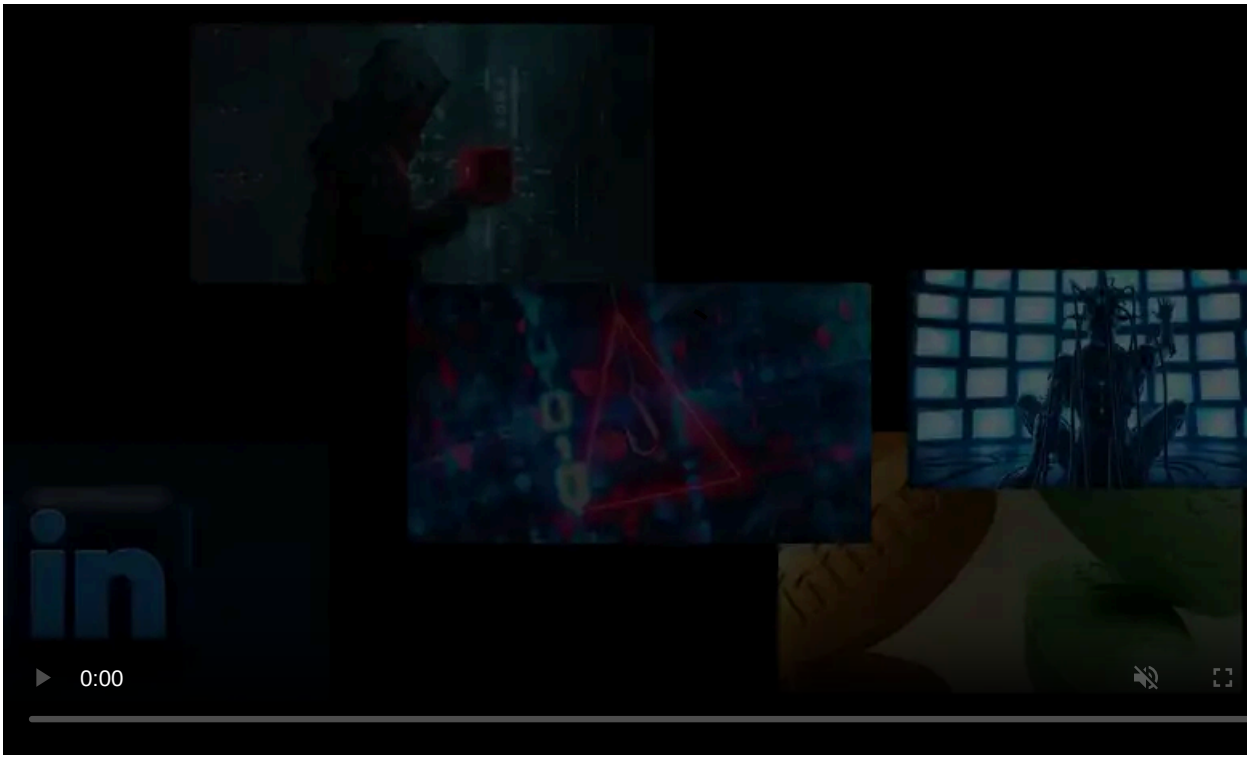
By Lawrence Abrams

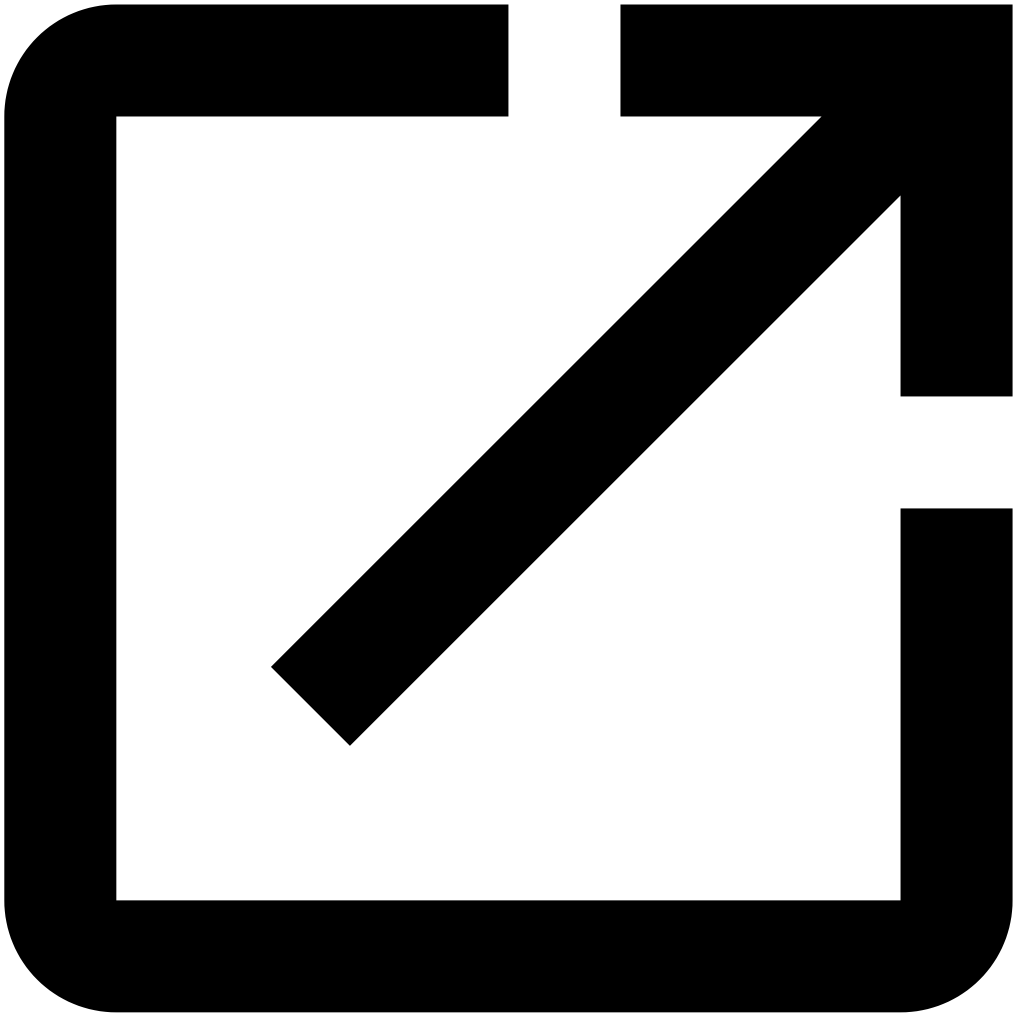
Published: 2023-03-11 · Archived: 2026-04-05 18:47:33 UTC

The Clop ransomware gang has begun extorting companies whose data was stolen using a zero-day vulnerability in the Fortra GoAnywhere MFT secure file-sharing solution.

In February, the GoAnywhere MFT file transfer solution developers warned customers that a zero-day remote code execution vulnerability was being exploited on exposed administrative consoles.

GoAnywhere is a secure web file transfer solution that allows companies to securely transfer encrypted files with their partners while keeping detailed audit logs of who accessed the files.


0:00



While no details were publicly shared on how the vulnerability was exploited, a proof-of-concept exploit was soon released, followed by a patch for the flaw.

The day after the release of the GoAnywhere patch, the Clop ransomware gang contacted BleepingComputer and said they were responsible for the attacks.

The extortion group said they used the flaw over ten days to steal data from 130 companies. At the time, BleepingComputer could not independently confirm these claims, and Fortra did not respond to our emails.

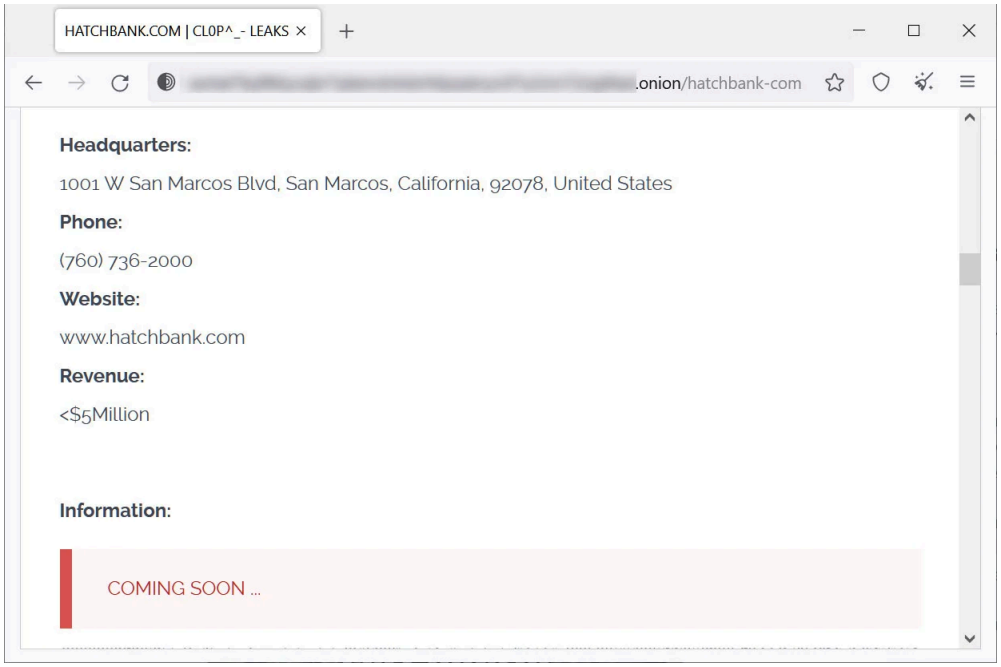
Since then, two companies, Community Health Systems (CHS) and Hatch Bank, disclosed that data was stolen in the GoAnywhere MFT attacks.

Clop begins extorting GoAnywhere customers

Last night, the Clop ransomware gang began publicly exploiting victims of the GoAnywhere attacks by adding seven new companies to their data leak site.

Only one of the victims, Hatch Bank, is publicly known to have been breached using the vulnerability. However, BleepingComputer has learned that at least two other listed companies had their data stolen using this flaw as well.

The entries on the data leak site all state that the release of data is "coming soon" but include screenshots of allegedly stolen data.



Hatch Bank listed on Clop's data leak site
Source: BleepingComputer

Furthermore, BleepingComputer has been told that victims have begun to receive ransom demands from the ransomware gang.

While it is unclear how much the threat actors are demanding, they had previously demanded $10 million in ransoms in similar attacks using an Accellion FTA zero-day vulnerability in December 2020.

During these attacks, the extortion group stole large amounts of data from nearly 100 companies worldwide, with the threat actors slowly leaking data from companies while demanding million-dollar ransoms.

Organizations that had their Accellion servers hacked include, among others, energy giant Shell, cybersecurity firm Qualys, supermarket giant Kroger, and multiple universities worldwide such as Stanford Medicine, University of Colorado,

University of Miami, University of California, and the University of Maryland Baltimore (UMB).

Source: https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-begins-extorting-goanywhere-zero-day-victims/