Hackers publish ExecuPharm internal data after ransomware attack | TechCrunch

By Zack Whittaker

Published: 2020-04-27 · Archived: 2026-04-05 19:25:20 UTC

U.S. pharmaceutical giant ExecuPharm has become the latest victim of data-stealing ransomware.

ExecuPharm said in a letter to the Vermont attorney general's office that it was hit by a ransomware attack on March 13, and warned that Social Security numbers, financial information, driver licenses, passport numbers and other sensitive data may have been accessed.

But TechCrunch has now learned that the ransomware group behind the attack has published the data stolen from the company's servers.

It's an increasingly popular tactic used by ransomware groups, which not only encrypts a victim's files but also exfiltrates the data and threatens to publish the data if a ransom isn't paid. This new technique was first used by Maze, a ransomware group that first started hitting targets in December. Since then, a number of new and emerging groups, including DoppelPaymer and Sodinokibi have adopted the same approach.

The data was posted to a site on the dark web associated with the CLOP ransomware group. The site contains a vast cache of data, including thousands of emails, financial and accounting records, user documents and database backups, stolen from ExecuPharm's systems.

When reached, a company executive confirmed to TechCrunch that CLOP was behind the attack.

"ExecuPharm immediately launched an investigation, alerted federal and local law enforcement authorities, retained leading cybersecurity firms to investigate the nature and scope of the incident, and notified all potentially impacted parties," said ExecuPharm operations chief David Granese.

Since the outbreak of COVID-19, some of the ransomware groups have shown mercy on medical facilities that they have pledged not to attack during the pandemic. CLOP said it too would not attack hospitals, nursing homes or charities, but said ExecuPharm would not qualify, saying that commercial pharmaceutical companies "are the only ones who benefit from the current pandemic."

Unlike some strains of ransomware, there is no known decryption tool for CLOP. Maastricht University found out the hard way after it was attacked last year. The Dutch university paid out close to $220,000 worth of cryptocurrency to decrypt its hundreds of servers.

The FBI has previously warned against paying the ransom.

> The sinkhole that saved the internet

Zack Whittaker is the security editor at TechCrunch. He also authors the weekly cybersecurity newsletter, this week in security.

He can be reached via encrypted message at zackwhittaker.1337 on Signal. You can also contact him by email, or to verify outreach, at zack.whittaker@techcrunch.com.

View Bio ›
