LockBit claims attack on California's Department of Finance

By Ionut Ilascu

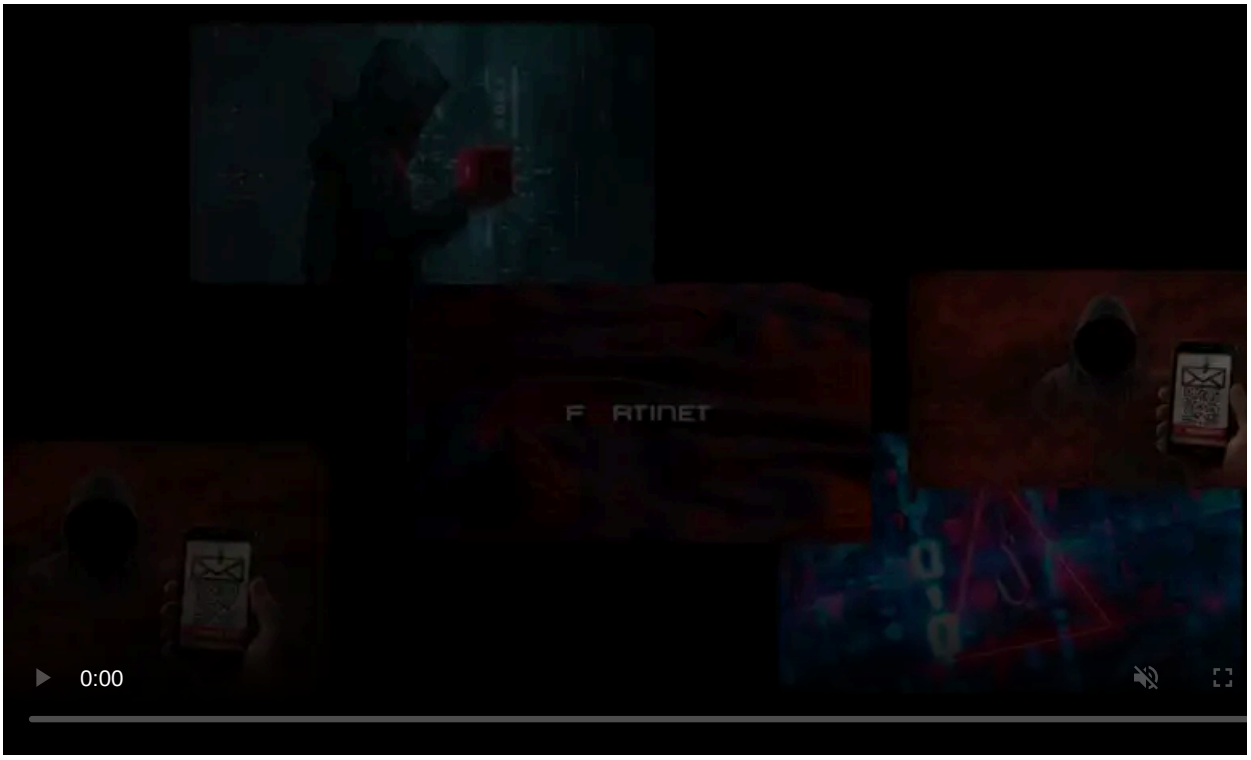
Published: 2022-12-13 · Archived: 2026-04-05 20:47:17 UTC

The Department of Finance in California has been the target of a cyberattack now claimed by the LockBit ransomware gang.

An investigation has been started by the California Cybersecurity Integration Center (Cal-CSIC), a group of state and federal agencies dedicated to protecting against cyber threats.

Ongoing investigation

California Governor’s Office of Emergency Services has confirmed that the Department of Finance has been affected by a cyber incident but did not provide too many details.


F RTINET
0:00

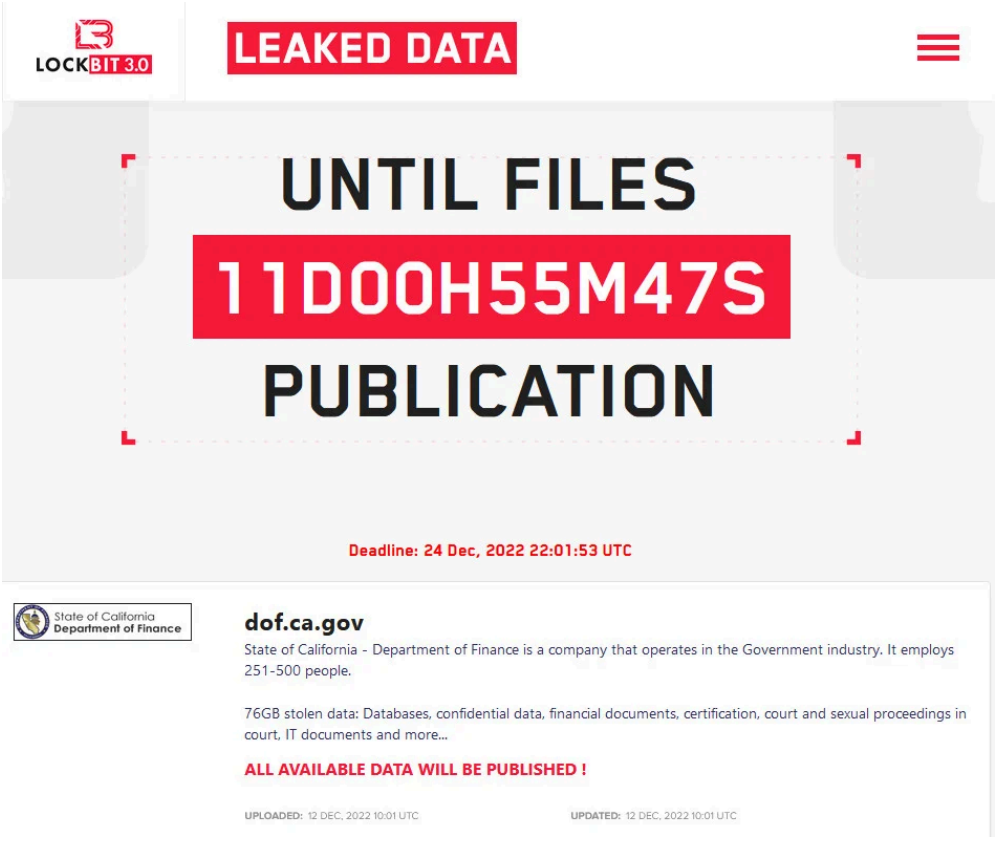
“The intrusion was proactively identified through coordination with state and federal security partners. Upon identification of this threat, digital security and online threat-hunting experts were rapidly deployed to assess the extent of the intrusion and to evaluate, contain and mitigate future vulnerabilities” - California’s Office of Emergency Services

It is unclear how much damage the hackers did or how they managed to breach the department. However, the state of California says that state funds remained unaffected by the attack.

LockBit claims 75GB of stolen files

On Monday, the LockBit ransomware gang posted on their leak site that they had breached the Department of Finance of the state of California and stole databases, confidential data, financial documents, and IT documents.

To prove their claim, the hackers published a few screenshots of files they allegedly exfiltrated from the systems of the Department of Finance in California.



source: BleepingComputer

The hackers also posted a screenshot of the directories and the number of files stored. The properties dialog shows a count of over 246,000 files in more than 114,000 folders amounting to 75.3GB of data.

LockBit’s data leak site shows a counter to get paid by December 24, threatening to publish all the files unless they get their ransom.

The builder that allows generating an encryptor and decryptor for LockBit ransomware was leaked in September by a disgruntled operator.

A week after that, a new group calling themselves BlooDy Ransomware Gang started using it in attacks against a Ukrainian entity.

In October, a 33-year-old Russian national suspected to be connected to the LockBit ransomware gang was arrested in Ontario, Canada. He is believed to have deployed the ransomware on critical infrastructure and large industrial

organizations.

At the time, Europol said that the individual is a "high-value target due to his involvement in numerous high-profile ransomware cases," demanding between €5 to €70 million from the victims.

LockBit operators are typically focusing on extorting large companies and are among the most active on the big-money ransomware scene.

Among the LockBit victims this year are automotive giant Continental, security company Entrust, and the Italian Internal Revenue Service (L'Agenzia delle Entrate).

The gang is financially driven and is the first one to introduce a bug bounty program, offering rewards of up to $1 million for vulnerabilities in their websites, locker, and new ideas to grow their operation.

Source: https://www.bleepingcomputer.com/news/security/lockbit-claims-attack-on-californias-department-of-finance/