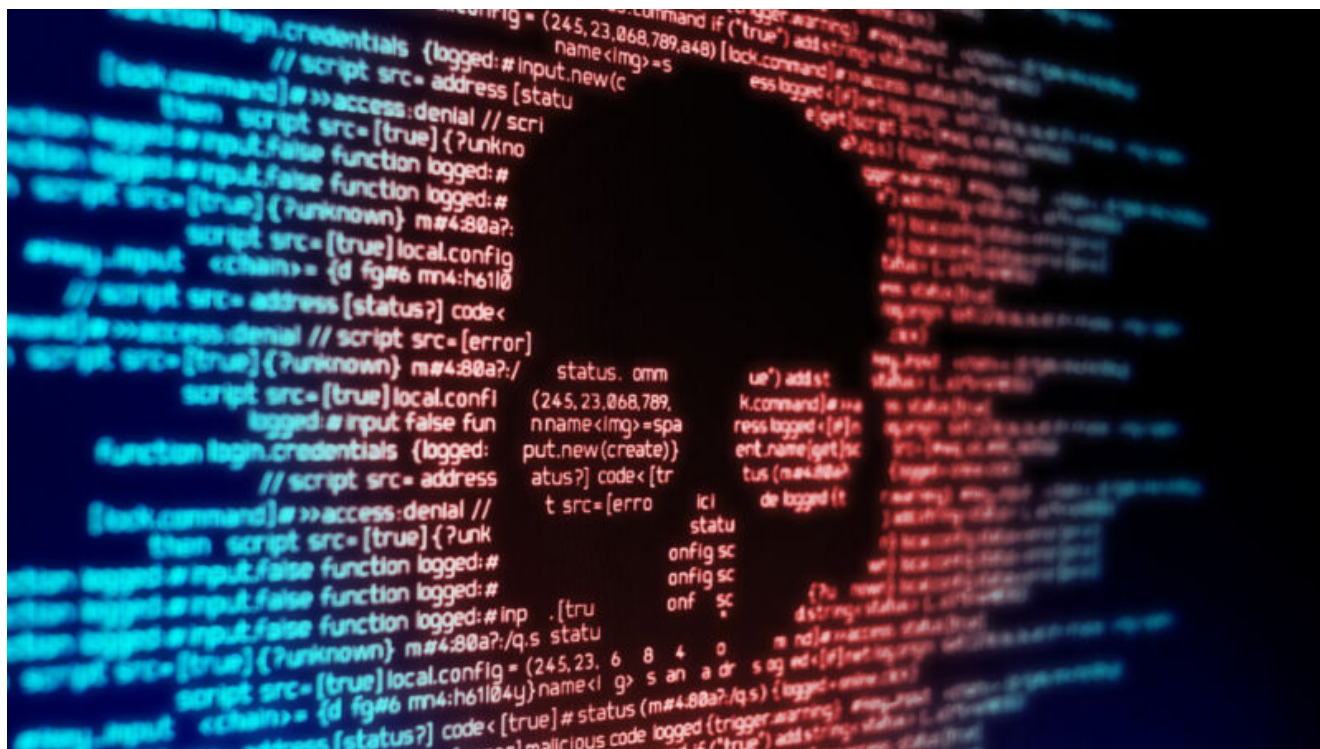


Millions of Americans' personal DMV data exposed in massive MOVEit hack



Getty Images

reader comments

58 with

As part of a massive ongoing cyberattack that exploits flaws in MOVEit file transfer software, the personal data of millions of US citizens, including those residing in Louisiana and Oregon, have been exposed to criminal organizations, according to CNN. In the wider attack, hackers targeted government agencies as well as multiple global organizations, causing a breach that extends beyond US boundaries.

While the effects of the MOVEit hack have been ongoing throughout the month of June, the most recent intrusion has hit over 3.5 million residents of Oregon and potentially over

3 million residents of Louisiana, all possessing driver's licenses or state ID cards. Information possibly compromised includes social security and driver's license numbers. This breach has prompted the respective state authorities to educate residents on preventive measures against identity fraud.

While no specific perpetrator has been officially accused by the states, federal officials have linked the comprehensive MOVEit hacking campaign to a Russian ransomware group known as Clop, which has been exploiting the same software vulnerability and demanding multimillion-dollar ransoms, as previously reported on Ars.

Both Oregon and Louisiana use MOVEit Transfer, a file-sharing tool sold by Progress Software Corp, to transfer files and data between business partners and customers. MOVEit's recently discovered vulnerability stems from a security flaw allowing for SQL injection, one of the most common types of exploits, that essentially tricks a web application into giving up confidential data or administrative system privileges.

Advertisement

In previous MOVEit attacks, the hackers have been known to gain shell access and steal data less than two hours after exploiting the MOVEit servers. The initial flaw was patched soon after it was discovered, but not before numerous organizations had their data stolen, including payroll service Zellis, the Canadian province of Nova Scotia, and UK retailer Boots. While the exploit only recently became known to security researchers, a recent report shows that Clop likely knew about the vulnerability since 2021.

Additionally, CNN reports that the hackers have accessed data from several US federal agencies, including the Department of Energy, and the data breach has also affected significant British organizations such as the BBC and British Airways. The

alleged culprits are hackers who are notorious for their multimillion-dollar ransom demands. However, as of yet, no such demands have been reported by the US or state governments.

The office of Louisiana Governor John Bel Edwards confirmed that there was no evidence suggesting that the compromised data from the Louisiana Office of Motor Vehicles was sold or released. Similarly, the hackers have not made any communication with the state government. However, Clop recently began listing names of organizations affected by the MOVEit hack in an attempt to shame them into paying ransoms.

Meanwhile, Progress Software, the US company that developed MOVEit, has identified a second vulnerability in the code that it says it is actively working to resolve. Its website also lays out steps that customers of MOVEit can take to protect their data. Even so, with a breach this far-reaching, it's likely that the fallout will continue.

<https://arstechnica.com/?p=1948548>