LockBit ransomware used in attack on Ohio town's court, police department and more

By Jonathan Greig

Published: 2023-02-02 · Archived: 2026-04-05 14:16:02 UTC

The city of Mount Vernon, Ohio said its police department, municipal court and other government offices were affected by a ransomware attack that started on December 19.

On Tuesday, the city's government released a statement saying officials were made aware of an incident that began at 3 a.m. the morning of the 19th.

"The breach occurred through a remote access tool utilized by the City's information technology (IT) provider, which also affected other clients of that provider," city officials said.

"The intruder installed ransomware known as LockBit, requesting a ransom for access to certain files. The impacted departments in the City were Mount Vernon Municipal Court, the Police Department, Auditor's office and Public Works."

City experts and their IT provider, Dynamic Networks, have spent the last week working to restore all of the systems affected using backups. Vulnerable software has been removed from all of their systems, according to the statement.

The statement claims no documents with personal identifiable information were "removed, or accessed, from City systems" but officials did not respond to questions about how that could be possible considering the ransomware gang gained access to both court and police systems.

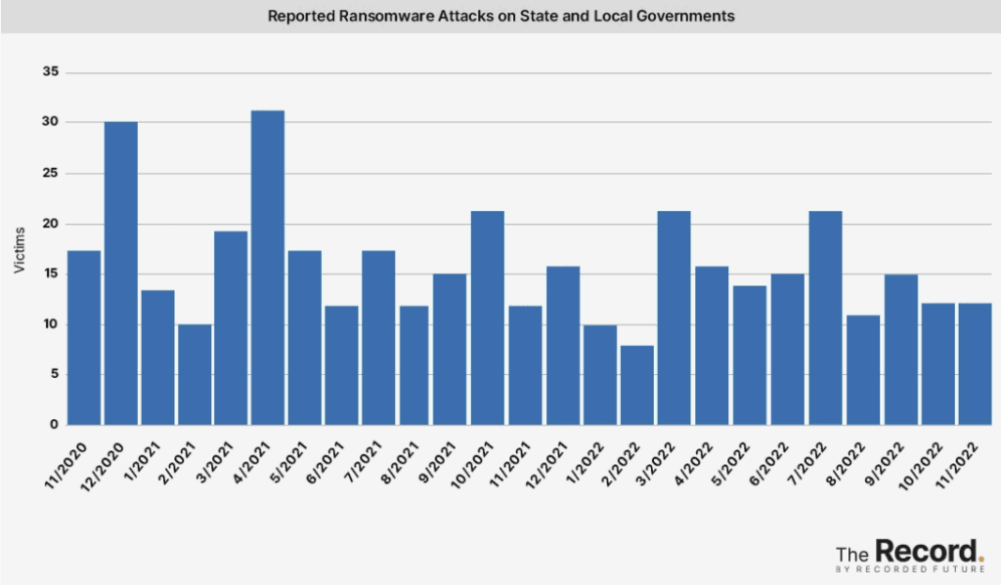
The city, which has about 17,000 residents, said it is also working with its insurance provider so they can have an independent evaluator determine whether personal information was stolen.

City officials did not respond to requests for comment about whether state or federal officials have been notified about the incident.

Jay Carey, a representative for the Ohio Department of Public Safety and the Ohio governor's office, told The Record that the city and county have not asked for assistance from state officials.

Local news outlets said the auditor's office as well as departments handling public works and cemeteries were affected by the attack.

Police officials in the city had to move to the Knox County Sheriff's Office to continue some work.



Ransomware groups have made a point of going after poorly-resourced local governments across the United States in 2022, targeting small governments in New Jersey, Colorado, Oregon, New York and several other states.

"This is part of a continuing trend of attacks against local, state and national governments," said Recorded Future ransomware expert Allan Liska.

"Recorded Future has noted 175 publicly reported attacks this year against governments, down from 2021 (196) but still a big problem."

The LockBit ransomware gang has quickly become the most prolific ransomware gang operating in 2022, launching hundreds of attacks this year on government agencies, companies and organizations around the world.

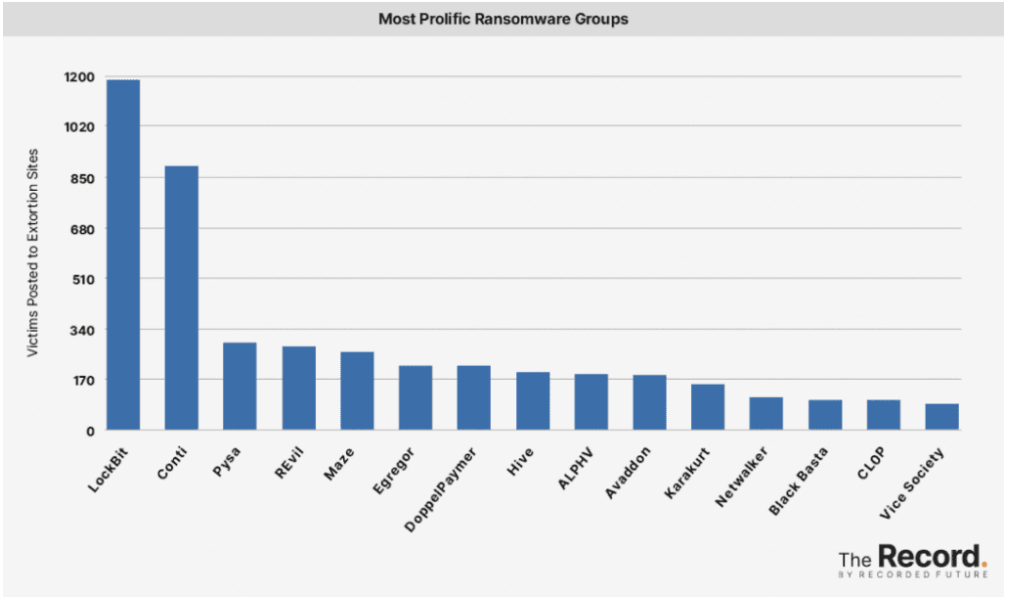
The Justice Department said the group gained prominence in January 2020 and “has become one of the most active and destructive ransomware variants in the world.”

“Since first appearing, LockBit has been deployed against at least as many as 1,000 victims in the United States and around the world. LockBit members have made at least $100 million in ransom demands and have extracted tens of millions of dollars in actual ransom payments from their victims,” the Justice Department said in November after charging a dual Russian and Canadian national for his alleged participation in the group’s attacks.

LockBit was linked to 82 attacks in August, bringing its total number of victims to 1,111, according to data collected by Recorded Future from extortion sites, government agencies, news reports, hacking forums, and other sources.

French police said the group was behind a crippling attack on a hospital about an hour south-east of Paris last month, which disrupted its medical imaging, patient admissions, and other services. About one-third of ransomware attacks targeting industrial systems in the second quarter were attributed to LockBit, according to cybersecurity firm Dragos.

The group has seen a spike in activity since June, when it launched a new version — what it calls "LockBit 3.0" — that allegedly included technical improvements and a bug bounty program that offered rewards for ways to improve the ransomware operation.



A chart tracking ransomware attacks as of December 2022.

Researchers have linked more than 1,029 attacks to LockBit since the group began its operation. The group was considered a marginal player until last year when it launched LockBit 2.0, a new version of its ransomware-as-a-service platform.

About one-third of ransomware attacks targeting industrial systems in the second quarter were attributed to LockBit, according to cybersecurity firm Dragos.

Some experts noted that the marked increase in LockBit incidents may also be due to the fact a toolkit to create DIY versions of the LockBit ransomware leaked in September. Several experts and researchers confirmed to The Record that the builder works and allows anyone to create their own ransomware based on the LockBit model.

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
