New Orleans latest apparent victim of Ryuk ransomware

By Benjamin Freed

Published: 2019-12-16 · Archived: 2026-04-05 16:26:11 UTC

A cyberattack last week against the New Orleans city government likely involved the ransomware known as Ryuk, based on affected files shared on the malware-analysis website VirusTotal. Colin Cowie, founder of the cybersecurity research firm Red Flare Security, was first to spot lines of code both referencing functions of New Orleans' municipal agencies and the Ryuk virus.

City officials acknowledged the attack late Friday afternoon when they declared a state of emergency and shut down more than 4,000 computers and servers across the government. New Orleans' official websites remained offline through Monday morning, and several more services were still affected. Municipal courthouses were closed Monday, and the city's Healthcare for the Homeless service was unable to see patients because workers cannot access electronic health files, according to Mayor LaToya Cantrell's office. Emergency services, including the city's 911 line, were mostly unaffected, but some agencies have opened Gmail accounts to handle non-emergency requests while the city's email server is offline.

At a press conference Saturday, New Orleans Chief Information Officer Kim LaGrue said she expects data loss to the ransomware attack to be "very minimal," which she credited to her department's relatively quick movement after detecting malicious activity on the city's network Friday morning. LaGrue's team first noticed suspicious activity at 5 a.m. Friday, and by 11 a.m. the team was shutting down systems citywide. LaGrue also said the city keeps offline backups of its files and applications.

"We've minimized data loss because part of our strategy is to always monitor for these risks," she said. "Investigating and looking for suspicious activity is something we do all the time. We are now looking to recover from a very resilient platform."

[ransomeware_map]

Click here to open the map in a larger window.

LaGrue added that the ransomware attack is under investigation by state and federal law-enforcement agencies, as well as the Louisiana National Guard.

"The forensic investigation is still in progress," she said. "There is much that we are still to learn about this attack, the mechanisms and what was significantly compromised."

While government officials have not said anything about the source of the cyberattack or how great of a ransom demand they received, third-party research pointing to Ryuk would make New Orleans the latest in a growing string of municipal governments to be attacked by the malware, which has elicited some of the largest ransomware payouts. Actors using Ryuk are known to have collected $400,000 from Jackson County, Georgia; nearly

$600,000 from Riviera Beach, Florida; $490,000 from Lake City, Florida; $130,000 from LaPorte County, Indiana; and $100,000 from the public school district in Rockville Centre, New York.

But recent research from Emsisoft, a New Zealand firm that specializes in ransomware, indicates that governments should think twice about paying for a decryption key to regain access to their files. Emsisoft's work shows that Ryuk is designed to only partially encrypt larger files to ensure it spreads quickly, which can lead the decrypter to corrupt data in some cases. "Depending on the exact file type, this may or may not cause major issues," the researchers wrote.

Ryuk was also seen in an attack last month against the state of Louisiana that prompted Gov. John Bel Edwards to issue his second emergency declaration of the year because of a cyberattack. The virus frequently works in concert with banking trojans that steal financial information and credentials from recipients of phishing emails who open malicious links. When one of the trojans, TrickBot, determines that a compromised network can be infected with ransomware, the Ryuk virus is delivered and begins encrypting files.

During the Saturday press conference, LaGrue said there is evidence last week's cyberattack began because city workers' credentials had been compromised.

"We've never confirmed any credentials were given out," LaGrue said. "But when we look at how our environment was permeated, it was through a compromise of credentials that belong to city employees."
