Ryuk Ransomware behind Attack on Florida Library System

By February 07, 2020 • Mark Harper, The News-Journal

Published: 2020-02-07 · Archived: 2026-04-05 22:31:56 UTC

(TNS) — The cyberattack that took down public-access computers at Volusia County, Fla., libraries last month involved ransomware that has elicited millions of dollars in ransom payments from governments and large businesses.

Volusia County officials say they've referred the attack to law enforcement, but would not say which agency is investigating. Emails provided in response to a public-record request indicate the library computers were infected by Ryuk ransomware. The county will not say whether it has made a ransom payment.

"Because it's under investigation, we have no comment at this time," said Kevin Captain, a county spokesman in an emailed response to a question about ransom.

Captain confirmed the county's insurance deductible is $100,000. "The county has no confirmation of cost at this time but will at a later date," Captain said.

Volusia County provided The News-Journal hundreds of pages of emails about the ransomware incident, some of it redacted because of the ongoing criminal investigation.

At 8:44 a.m. Jan. 9, Brian Whiting, director of information technology at Volusia County, wrote an email to support desk staff stating: "The Volusia County Library is currently being cyber attacked by Ryuk, an attack propagated frequently via email phishing attack."

Later that day, in another email, Whiting says the IT department has detected "a ten-fold increase in attempted attacks over the past month or so."

Twenty servers and about 600 computers were encrypted — essentially locked up — by the ransomware. The county was able to restore about 50 computers used by library staff to conduct business, such as checking books in and out, but the public-access terminals would remain down for about two weeks.

One of Volusia officials' first calls reported the incident to the Center for Internet Security's Multi-State Information Sharing and Analysis Center (MS-ISAC) in East Greenbush, New York. The Center for Internet Security is a nonprofit organization that works to safeguard private and public organizations against cyber threats.

An emergency response team from MS-ISAC got involved.

Volusia officials soon also contacted their London-based claims adjuster, CFC Underwriting, which became involved in approving expenditures on outside security firms to assist with bringing the system back. Solis Security in Austin, Texas, was also brought into the loop.

And at some point, the county notified the Department of Homeland Security about the incident, according to an email written by Andrew Krasucki of CFC Underwriting.

An email from Joshan Heer of CFC Underwriting to county officials summarized what had been found by midday Jan. 10:

Encryption of the Volusia library computers began at around 1:30 a.m. on Jan. 9, and a ransomware note had been left on a desktop by 7 that morning.

File extensions had been changed to .ryk, indicating the Ryuk ransomware. Volusia County IT staff shut down and disconnected all the computers from the county network.

"It is believed sensitive data is not at risk due to (redacted)," Heer wrote, adding that would have to be confirmed.

"Those who've used public-access computers on a network that's been hit by Ryuk probably don't have much to worry about," said Brett Callow, a threat analyst with Emsisoft, a New Zealand-based anti-malware company. "The Ryuk operators have not been known to steal data."

Cyber defense experts say Ryuk has been used in hundreds of attacks on U.S. governments and businesses since 2018, and in some cases the criminal gang of hackers responsible for the attacks have been paid handsomely.

The cost of these attacks in 2019 was estimated by Emsisoft at $7.5 billion.

At least three Florida municipalities were victimized in June 2019 alone, including:

- Riviera Beach, a Palm Beach County city of 35,000, which paid 65 bitcoins – or about $600,000 – in exchange for a decryption key from the attackers.
- Lake City in northern Florida paid about $460,000 in bitcoin to recover data and computer operations.
- Key Biscayne – a town on a barrier island near Miami – was hit and spent money trying to restore its network.

While it is unclear whether Volusia paid a ransom, Krasucki's email of Jan. 13 indicated the county might have had a way to restore its data.

"A system state backup stored on an external drive will be utilised to rebuild the active directory structure and the domain controller servers," Krasucki wrote.

Callow said Ryuk is commonly used in attacks on both the public and private sector and accounts for between 15% and 25% of all ransomware incidents.

SentinelOne, another cybersecurity firm, reported Ryuk ransomware "is largely responsible for the massive increase in ransomware payments." Where many cyber criminals demand $10,000 to remove the encryption on computer systems, Ryuk operators "demand an average of $288,000 for the release of systems."

Yet another cyber defense firm, CrowdStrike,identifies the perpetrator of Ryukas "Wizard Spider," a Russia-based criminal group.

Callow said exactly who's deploying Ryuk remains an open question.

"There's speculation that the group behind Ryuk – and it does appear to be a single group – has Russian ties, but it is just speculation. Attribution is always extremely hard," he wrote in an emailed response to questions.

"For example, some ransomware contains language exclusions and will not encrypt files if the operating system uses one of a number of specified languages – (post-Soviet) countries, Iran, etc.," he wrote. "That could indicate origin – groups not wanting to poop in their own backyards – or it could be a false flag designed to misdirect law enforcement."

Unlike other ransomware, which contain flaws in the encryption allowing security companies to create tools to recover data without needing to pay ransom, Ryuk has no such flaws, Callow said.

"The encryption is perfectly implemented and, consequently, the only way to recover data is to restore it from backups (assuming they were not deleted/encrypted during the attacks) or to pay the ransom," Callow said.
