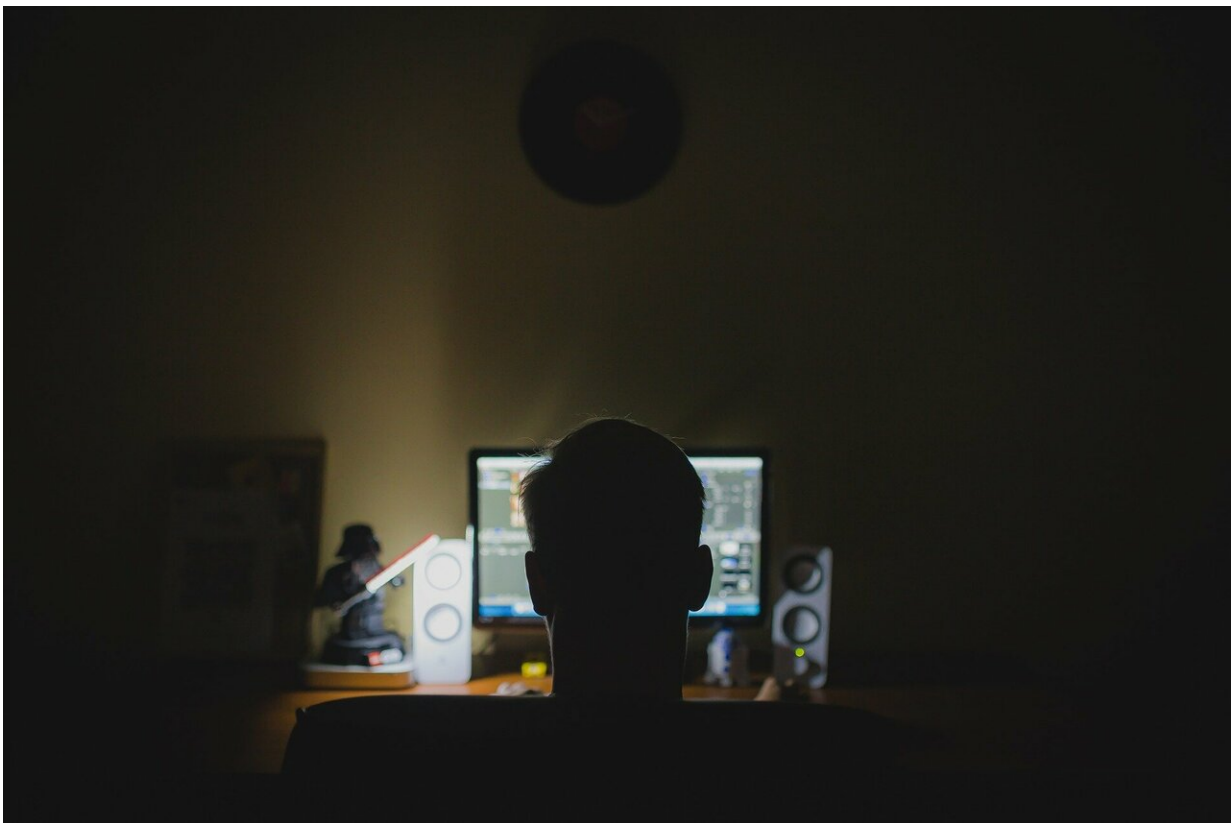


Florida city pays \$600,000 ransom to save computer records

June 19 2019, by Terry Spencer



Credit: CC0 Public Domain

A Florida city agreed to pay \$600,000 in ransom to hackers who took over its computer system, the latest in thousands of attacks worldwide aimed at extorting money from governments and businesses.

The Riviera Beach City Council voted unanimously this week to pay the hackers' demands, believing the Palm Beach suburb had no choice if it wanted to retrieve its records, which the hackers encrypted. The council already voted to spend almost \$1 million on new computers and hardware after hackers captured the [city's](#) system three weeks ago.

The hackers apparently got into the city's system when an employee clicked on an email link that allowed them to upload malware. Along with the encrypted records, the city had numerous problems including a disabled email system, employees and vendors being paid by check rather than direct deposit and 911 dispatchers being unable to enter calls into the [computer](#). The city says there was no delay in [response time](#).

Spokeswoman Rose Anne Brown said Wednesday that the city of 35,000 residents has been working with outside security consultants, who recommended the ransom be paid. She conceded there are no guarantees that once the hackers received the money they will release the records. The payment is being covered by insurance. The FBI on its website says it "doesn't support" paying off hackers, but Riviera Beach isn't alone: many [government agencies](#) and businesses do.

"We are relying on their (the consultants') advice," she said. The hackers demanded payment in the cryptocurrency bitcoin. While it is possible to trace bitcoins as they are spent, the owners of the accounts aren't necessarily known, making it a favored payment method in [ransomware attacks](#).

Numerous governments and businesses have been hit in the United States and worldwide in recent years. Baltimore refused to pay hackers \$76,000 after an attack last month. The U.S. [government](#) indicted two Iranians last year for allegedly unleashing more than 200 ransomware attacks, including against the cities of Atlanta and Newark, New Jersey. The men, who have not been arrested, received more than \$6 million in

payments and caused \$30 million in damage to computer systems, [federal prosecutors](#) have said.

The federal government last year also accused a North Korean programmer with the "WannaCry" attack that infected government, bank, factory and hospital computers in 150 countries. He is also believed to have stolen \$81 million from a Bangladesh bank. He also remains in his home country.

The FBI had no immediate comment Wednesday on the Riviera Beach attack.

Tom Holt, a Michigan State University criminal justice professor, said hackers often attack common and known vulnerabilities in computer systems. He said organizations' technology managers need to examine their systems for such flaws and teach their employees not to open suspicious email or click suspect links. The FBI says businesses also need to back up their data regularly on secure computers.

Holt said most attacks originate outside the U.S., which makes them difficult to police. He said many victims wind up like Riviera Beach: They pay their attacker because it is likely the only way to retrieve lost data.

"They might not pay the initial ransom that was suggested, but they may work with a third-party provider to negotiate the ransom down," Holt said.

He said in almost all cases, the attackers decrypt the computers after payment, allowing the victims to retrieve their data. He said the WannaCry attacks were an exception—the hackers took the money but often didn't release the data.

Some private WannaCry decryption attempts were successful.

© 2019 The Associated Press. All rights reserved.

Citation: Florida city pays \$600,000 ransom to save computer records (2019, June 19) retrieved 23 April 2024 from <https://phys.org/news/2019-06-florida-city-ransom.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.