Florida LAN: Someone clicks link, again, giving Key Biscayne ransomware



Enlarge / Key Biscayne, Florida, is the third Florida local government to get hit by ransomware within a month.
Alicia Vera/Bloomberg via Getty Images

reader comments

83 with 64 posters participating, including story author

Share this story

A third Florida local government has reported that it has been struck by ransomware. Key Biscayne joins Lake City as a victim of Ryuk, a form of ransomware first spotted in August of 2018. Ryuk was the final piece of what has been labeled the “Triple Threat’ attack, the other two threats being Emotet and

Trickbot malware.

While the attack on Riviera Beach, Florida, revealed last week was similar—all three cases start with a city employee clicking on an attachment in email and unleashing malware—it's not certain if that attack was also based on Ryuk.

Ryuk is targeted ransomware, originally linked to the North Korean "Lazarus" threat group, but now it appears to have been adopted by non-state criminal ransomware operators as well. It comes with a tailored ransom note that directs victims to contact the attacker via email. It has been known to lie dormant for up to a year before executing.

In Triple Threat attacks, as described in an April report by Cybereason, a malicious document uses PowerShell script to download the Emotet trojan. Emotet has been used in the past to steal banking information, but it can also be used as a "dropper" to install additional malware—in this case, the TrickBot trojan.

TrickBot is another piece of commodity malware. A modular bit of nastiness, TrickBot carries with it a number of tools for moving laterally across the network from the initial point of compromise—the computer of the person who clicked on the attachment. Those modules include password grabbers, a PowerShell-based reconnaissance tool that uses the open sourced PowerShell Empire framework, and spreader_x64.dll—a lateral movement tool based on the leaked National Security Agency EternalBlue vulnerability in Windows' Server Message Block version 1 (SMB v. 1) file sharing protocol. Spreader_x64.dll also includes the well-worn mimikatz credential-stealing tool, allowing it to harvest credentials to copy itself if it can't exploit EternalBlue.

Once TrickBot has established itself, the attackers use TrickBot to examine where their malware has landed and determine a next step. From there, they use any credentials

that have been harvested to infect other systems. In an attack examined by Cybereason, TrickBot was used to compromise a Windows domain controller, gather data on the victim's Active Directory structure, identify servers on the network, connect to them, and then infect them all with Ryuk.

Lake City, which was hit with ransomware on June 10, paid out $460,000 worth of Bitcoin to the attackers, according to City Manager Joseph Helfenberg. Paying, he told CBS4 Miami News' Hank Tester, was the cheapest option—since the city had a $10,000 deductible on its cyber insurance policy, and the insurer was paying the balance. Insurance companies have in many cases pressed for local government victims to pay ransoms to minimize their costs. Riviera Beach paid out $600,000 worth of Bitcoin to make its ransomware problem go away, for example.

But there's a small probability that Lake City could have avoided paying out to the ransomers. Brett Callow of Emsisoft told Ars, "We're actually able to decrypt Ryuk in about 5% of cases. Had they uploaded an encrypted file to ID Ransomware — which is operated by one of our team— there's a small chance they may have been able to save half a million bucks. Whether or not they actually did upload a file, I can't say."

There have been two uploads of Ryuk samples to ID Ransomware in June: one from an IP address belonging to an Internet provider in Clearwater, Florida, and another in Rockledge, Florida.

The Village of Key Biscayne is a much smaller community—Lake City has about 12.000 residents, while Key Biscayne has about 3,000. No decision has been announced by the village government yet. A special council meeting was scheduled for tonight to discuss the matter.

https://arstechnica.com/?p=1529433