Baltimore ransomware attack was early attempt at data extortion, new report shows

September 25, 2020

City

Baltimore's Inner Harbor (Getty Images)

Written by Benjamin Freed
Sep 25, 2020 | STATESCOOP

The May 2019 ransomware attack against Baltimore that debilitated municipal services for weeks, cost the city government as much as to $18 million and led to the ouster of the city's chief information officer also included an early attempt by hackers pressuring a victim into paying up by threatening to publish stolen data, according to research published this week by the cybersecurity company CrowdStrike.

In a blog post Thursday, the company said that two days after the Baltimore hack was reported, the actor behind it posted a message on the dark web threatening to expose or destroy the city's compromised data, in an attempt to extort then-Mayor Bernard C. "Jack" Young into paying a ransom of about $76,000.

“Hey, Jack Young and other Baltimore leaders. In 7 June 2019 thats your dead line, well remove all of things weve had about your city and you can tell other [redacted] to help you for getting back [redacted]. This final dead line and never ever gonna back,” read the message from the actor behind the RobbinHood ransomware, which CrowdStrike calls Outlaw Spider.

Young refused to pay, but the message now sticks out as an early example of a step that’s since become typical of ransomware incidents.

“Although ineffective, the incident with the [City of Baltimore] and Outlaw Spider was the first instance observed by CrowdStrike Intelligence of data extortion to incentivize ransom payment,” the CrowdStrike blog reads.

Attempting to extort ransomware victims into paying by threatening to publish stolen files was popularized last November with the rise of Maze malware. The actors behind that ransomware pioneered the tactic of creating a publicly accessible website where victims are listed, along with samples of stolen files and threats to publish or sell full volumes of exfiltrated data unless the hackers are paid off. Other well-known ransomware actors, including those behind the REvil and DoppelPaymer malwares, have since adopted the practice. The change in tactics is natural for an enterprise that’s motivated by making as much money as possible.

“It’s continuing to evolve,” Adam Meyers, CrowdStrike’s vice president of intelligence, told StateScoop in a phone interview.

Meyers said the extortion sites are an outgrowth of the trend lines seen in ransomware over the past five or six years. As cryptocurrency ransoms became more valuable, he said, hackers changed their targets from individual victims to enterprises like corporations and government organizations — what CrowdStrike and other cybersecurity firms call “big game hunting.”

In attempting to goad victims into paying ransoms by threatening to expose potentially sensitive information, Meyers said, negotiations between hacker and victim “are commoditized.”

“These guys are financially motivated, they’re in it for the money,” he said.

Meyers said IT organizations need to continue taking many of the oft-recommended cyber hygiene steps, including regular security patching and implementing endpoint-detection tools. But he also said organizations need to invest in newer tools like “next-generation” antivirus platforms that use machine learning to detect malicious activity.

And he also said 2020 has been a good year for ransomware actors and other cybercriminals, which he credited in part to the fact that the explosion of remote-work environments brought on by the COVID-19 crisis has created many more entry points for attackers.

“We’ve seen as many attacks in the first half of 2020 as we did in all of 2019,” he said. “It’s recession proof, it’s pandemic proof.”

Meyers echoed previous findings that cybercriminals are tailoring their phishing messages to play off public health and economic crises.

“Covid’s been a boon for the threat actors because it gave them so many things to capitalize on,” he said. “Threat actors capitalize on fear or greed. Greed is powerful, but when people think they’re going to die or be out of business, now you’ve got a much more powerful tool in your quiver.”