Ryuk Ransomware Behind Durham, North Carolina Cyberattack

By Lawrence Abrams

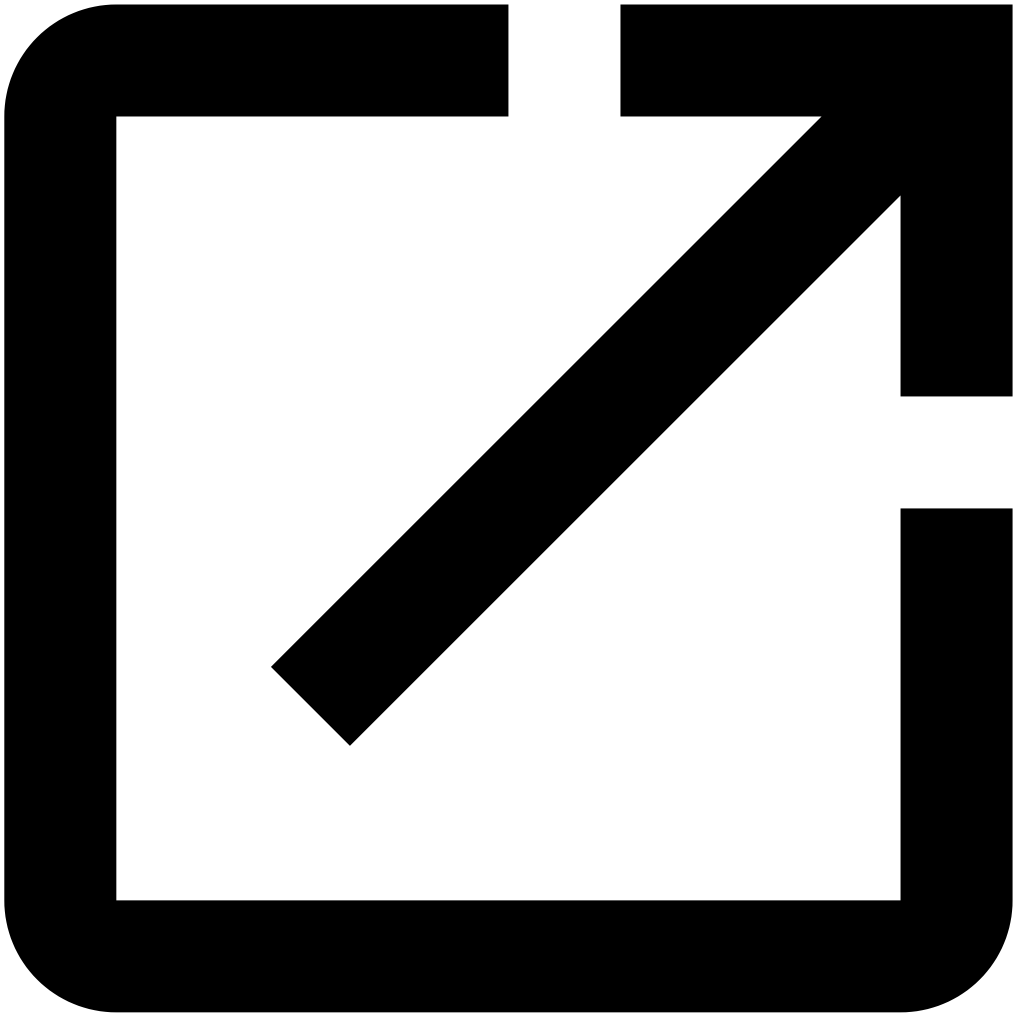
Published: 2020-03-08 · Archived: 2026-04-05 14:20:45 UTC

The City of Durham, North Carolina has shut down its network after suffering a cyberattack by the Ryuk Ransomware this weekend.

Local media reports that the city fell victim to a phishing attack that ultimately led to the deployment of the Ryuk Ransomware on their systems.

"According to the SBI, the ransomware, named Ryuk, was started by a Russian hacker group and finds its way into a network once someone opens a malicious email attachment. Once it's inside, Ryuk can spread across network servers through file shares to individual computers," reported.


DIE LINKE.
0:00



To prevent the attack from spreading throughout their network, the City of Durham has "temporarily disabled all access into the DCI Network for the Durham Police Department, the Durham Sheriff's Office and their communications center".

This has caused the city's 911 call center to shut down and for the Durham Fire Department to lose phone service. 911 calls, though, are being answered.

While they have not seen signs that data has been stolen, the city has warned that users should be on the lookout for phishing emails pretending to be from the City of Durham.

Actors were probably present on the network for weeks

The Ryuk Ransomware attacks are usually the result of a network becoming infected with the TrickBot Trojan first, which is usually installed through malicious attachments in phishing emails.

TrickBot is an information-stealing Trojan that will steal data from an infected computer and then attempt to spread laterally through the network.

After harvesting all valuable data from a network, it then proceeds to open a shell back to the Ryuk Ransomware actors who will then proceed to harvest data from the network as well and gain administrator credentials.

When done, they deploy the Ryuk Ransomware on all devices on the network to generate a large ransom, which can range from $10,000 on very small networks to millions of dollars on larger networks.

In December 2019, the Ryuk Ransomware was behind the attack on New Orleans and just recently attacked legal services giant Epiq Global, which caused them to take all of their systems offline as well to contain the infection.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
