DC police department hit by apparent extortion attack

27 April 2021

In this Monday, June 22, 2020, file photo, Metropolitan Police Department bicycle division officers stand guard after police closed the area around Lafayette Park near the White House after protesters tried to topple a statue of Andrew Jackson in the park in Washington. On Monday, April 26, 2021, the Washington, D.C., police department said that its computer network was breached, and a Russian-speaking ransomware syndicate claimed to have stolen sensitive data, including on informants, that it threatened to share with local criminal gangs unless police paid an unspecified ransom. (AP Photo/Maya Alleruzzo, File)

The Washington, D.C., police department said Monday that its computer network was breached, and a Russian-speaking ransomware syndicate claimed to have stolen sensitive data, including on informants, that it threatened to share with local criminal gangs unless police paid an unspecified ransom.

The cybercriminals posted screenshots on their dark web site supporting their claim to have stolen more than 250 gigabytes of data.

The District of Columbia's Metropolitan Police Department said in a statement that it had asked the FBI to investigate the "unauthorized access."

There was no indication that any police operations were affected, and the department did not immediately say whether it had been hit by ransomware.

The Babuk group, a relatively new ransomware gang, said on its website that it had "downloaded a sufficient amount of information from your internal networks" and gave the police three days to contact it or "we will start to contact gangs in order to drain the informants."

Screenshots it posted suggested it has data from at least four computers, including intelligence reports, information on gang conflicts, the jail census and other administrative files. One of the images, apparently of network locations accessed by the criminals, showed a text document on one computer entitled "How To Restore Your Files."

Such documents generally include instructions on how to contact the ransomware criminals, whose standard operating procedure is to exfiltrate sensitive data from networks they infiltrate as they sow malware that, once activated, encrypts data. Only after receiving payment do the criminals provide software keys that unscramble the data.

So far this year, 26 government agencies in the U.S. have been hit by ransomware, with cybercriminals releasing online data stolen from 16 of them, said ransomware analyst Brett Callow of the cybersecurity firm Emsisoft. Ransomware victims don't always pay, often preferring the arduous task of rebuilding networks from backups.

The D.C. police department said it was taking the threat seriously.

"We are aware of unauthorized access on our server. While we determine the full impact and continue to review activity, we have engaged the FBI to fully investigate this matter," the department statement said. An FBI spokeswoman had no

immediate comment.

A worsening global epidemic of ransomware attacks is considered a national security threat by many, doing tens of billions of dollars in damage. U.S. law enforcement is relatively powerless to counteract it as most of the criminals enjoy safe harbor in Russia and other nations with weak rule of law.