DC Police victim of massive data leak by ransomware gang

May 13 2021, by Alan Suderman

In this April 2, 2021, file photo, Washington Metropolitan Police Department chief Robert Contee speaks during a news conference in Washington. Political hand-wringing in Washington over Russia's hacking of federal agencies and meddling in U.S. politics has mostly overshadowed a worsening digital scourge with a far broader wallop: crippling and dispiriting extortionary ransomware attacks by cybercriminal mafias. All the while, ransomware gangsters have become more brazen and cocky as they put more and more lives and livelihoods at risk. This week, one syndicate threatened to make available to local criminal

gangs data they say they stole from the Washington, D.C., metro police on informants. (AP Photo/Alex Brandon)

The police department in the nation's capital has suffered a massive leak of internal information after refusing to meet the blackmail demands of Russian-speaking ransomware syndicate. Experts say it's the worst known ransomware attack ever to hit a U.S. police department.

The gang, known as the Babuk group, released thousands of the Metropolitan Police Department's sensitive documents on the dark web Thursday. A review by The Associated Press found hundreds of police officer disciplinary files and intelligence reports that include feeds from other agencies, including the FBI and Secret Service.

Ransomware attacks have reached epidemic levels as foreign criminal gangs paralyze computer networks at state and local governments, police departments, hospitals and private companies. They demand large payments to decrypt stolen data or to prevent it from being leaked online.

A cyberattack last week shut down the Colonial Pipeline, the nation's largest fuel pipeline, prompting gas-hoarding and panic-buying in parts of the Southeast.

Brett Callow, a threat analyst and ransomware expert at the security firm Emsisoft, said the police leak ranks as "possibly the most significant ransomware incident to date" because of the risks it presents for officers and civilians.

Some of the documents include security information from other law enforcement agencies related to President Joe Biden's inauguration,

including a reference to a "source embedded" with a militia group.

One document details the steps the FBI has taken in its investigation of two pipe bombs left at the headquarters of the Democratic National Committee and the Republican National Committee before the insurrection at the U.S. Capitol on Jan. 6. That includes "big data pulls" of cell towers, and plans to "analyze purchases" of Nike shoes worn by a person of interest, the document said.

The police department did not immediately return a request for comment, but has previously said some officers' personal information was stolen.

Some of that information was previously leaked, revealing personal information of some officers taken from background checks, including details of their past drug use, finances and—in at least one incident—of past sexual abuse.

The newly released files include details of disciplinary proceedings of hundreds of officers dating back to 2004. The files often contain sensitive and embarrassing private details.

"This is going to send a shock through the law enforcement community throughout the country," said Ted Williams, a former officer at the department who is now an attorney. He's representing a retired officer whose background file was included in an earlier leak.

Williams said said having background checks and disciplinary files made public makes it difficult for officers to do their jobs.

"The more the crooks know about a law enforcement officer the more the crooks try to use that for their advantage," he said.

The Babuk group indicated this week that it wanted $4 million not to release the files, but was only offered $100,000.

The department has not said whether it made the offer. Any negotiations would reflect the complexity of the ransomware problem, with police finding themselves forced to consider making payments to criminal gangs. The FBI, which is assisting in this case, discourages ransomware payments.

The group revealed the attack last month, threatening then to leak the identities of confidential informants. The data release revealed Thursday is massive and it was not immediately clear if it included informants' names.