TechXplore

Ransomware gang threatens release of DC police records

May 11 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)

A Russian-speaking ransomware syndicate that stole data from the Washington, D.C., police department says negotiations over payment have broken down, with it rejecting a $100,000 payment, and it will release sensitive information that could put lives at risk if more money is not offered.

The extortion threat comes amid a separate ransomware attack on a major pipeline that's affected part of the U.S.'s fuel supply, highlighting the power of internet-savvy criminal gangs to sow mayhem from a half a world away with impunity.

The Babuk group said on its website late Monday that it would release "all the data" it stole from the Washington police department if it did not "raise the price."

"The negotiations reached a dead end, the amount we were offered does not suit us," the group said.

The department did not immediately comment and has not said whether it's negotiated any possible payment.

On Tuesday, the gang released screenshots that appear to be negotiations with the department. They show the gang asked for $4 million and received a counter-offer of $100,000. The authenticity of the screenshots could not be independently confirmed.

If true, it's an example how complex the ransomware problem is when even police find themselves forced to consider making payments to criminal gangs.

Late last month, the group said it had hacked into the network of the city's police department and threatened to leak the identities of confidential informants unless an unspecified ransom was paid. Experts said such a release could endanger the lives of the informants.

A day after the initial threat was posted, the gang tried to spur payment by leaking personal information of some police officers taken from background checks, including details of officers' past drug use, finances and—in at least one incident—of past sexual abuse.

Babuk leaked similar background files on Monday with its threat to release more, said Brett Callow, a threat analyst and ransomware expert at the security firm Emsisoft.

"This is far worse than any hack of other police departments previously," Callow said, adding that he's never seen a law enforcement agency pay a ransom before.

Ransomware gangs have been leaking sensitive data from victims for well over a year, but experts said they've not seen such aggressive new tactics used before against police departments. The cybercriminal mafias mostly operate in foreign safe havens out of the reach of Western law enforcement.

The average ransom payments last year were $310,000, up 171% from 2019, according to Palo Alto Networks.

The Biden administration has said that curbing ransomware attacks are a top priority, saying they are a threat to national security.

Citation: Ransomware gang threatens release of DC police records (2021, May 11) retrieved 23 April 2024 from https://techxplore.com/news/2021-05-ransomware-gang-threatens-dc-police.html