Written by **James Murphy** on June 23, 2020

Hacker Platform Publishes Potentially Sensitive Police Information

Hackers have published hundreds of thousands of documents — 269 GB — containing potentially sensitive police files from at least 200 police and FBI offices across the country. Information included in the data dump may include internal memos, e-mails, and the personal information of officers.

On Friday, the hacker platform Distributed Denial of Secrets (DDoSecrets) tweeted that they had compiled the data known as "BlueLeaks" and included a link to the breached information. The hackers claim the data goes back 24 years and comes from over 200 police departments, fusion centers, and training/support resources which were hacked by an anonymous data thief.

> RELEASE: #BlueLeaks (269 GB)
>
> Ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources. Among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.https://t.co/sWzdKc2VFc
>
> — Distributed Denial of Secrets (@DDoSecrets) June 19, 2020

The "leaked" information is apparently legitimate and connected to a massive data breach at Netsential, a Houston-based web service provider that contracts with state law-enforcement agencies across America. Reportedly, some of the data show how police agencies have been sharing information about COVID-19 and the protests and riots connected with the death of Minneapolis criminal George Floyd.

DDoSecrets fancies itself an alternative to WikiLeaks and publishes caches of previously secret information on the Internet. Although it provides "a stable platform" for the hackers and leakers, DDoSecrets claims that it doesn't do the hacking itself.

"DDoSecrets publishes materials submitted by sources both leakers and hackers. We provide a stable platform for the public to access data and an anonymity shield for sources to share it, but are uninvolved in the extrication of the data," the group tweeted.

Emma Best, a co-founder of the group, boasted that the hack is the largest of its kind.

"It's the largest public hack of American law enforcement agencies," Best claimed. "It provides the closest inside look at the state, local and federal agencies tasked with protecting the public, including government response to COVID and the BLM protests."

According to Best, the hack shows how the attitude of the various police forces informs their actions regarding the Floyd riots.

"The underlying attitudes of law enforcement is one of the things I think BlueLeaks documents really well," Best stated. "I've seen a few comments about it being unlikely to uncover gross police misconduct, but I think those somewhat miss the point, or at least equate police misconduct solely with illegal behavior. Part of what a lot of the current protests are about is what police do and have done legally."

A internal alert from the National Fusion Center Association, obtained by Internet security reporter Brian Krebs, says that hackers penetrated Netsential and stole the information sometime on or after June 19. In addition to the information about COVID-19 and the Floyd protests, the cache contains names, e-mail addresses, phone numbers, PDF documents, and images. The cache also includes a large number of text, video, CSV, and zip files. The data dump also includes bank account numbers and routing information for departments and officers.

"Our initial analysis revealed that some of these files contain highly sensitive information such as ACH routing numbers, international bank account numbers (IBANs), and other financial data as well as personally identifiable information (PII) and images of suspects listed in Requests for Information (RFIs) and other law enforcement and government agency reports."

The NFCA is concerned that bad actors including nation-states, so called "hacktivists," and cyber-criminals could use the information in the data dump to target police agencies and even individual officers since all the files are reportedly searchable by badge numbers.

Stewart Baker, a former assistant secretary of policy at the Department of Homeland Security, doesn't believe that the hack will reveal much, if anything, about police misconduct. But it is potentially dangerous to ongoing investigations and could even jeopardize police lives.

"With this volume of material, there are bound to be compromises of sensitive operations and maybe even human sources or undercover police, so I fear it will put lives at risk," Baker said. "Every organized crime operation in the country will likely have searched for their own names before law enforcement knows what's in the files, so the damage could be done quickly. I'd also be surprised if the files produce much scandal or evidence of police misconduct. That's not the kind of work fusion centers do."

Image: Thinkstock

James Murphy is a freelance journalist who writes on a variety of subjects, with a primary focus on the ongoing anthropogenic climate-change hoax and cultural issues. He can be reached at jcmurphyABR@mail.com.