

The Virgin Islands Consortium

VIPD Case Files Wiped Out From Computers Following Intrusion; Hackers Demanding Ransom For Access

Crime / **Published On August 02, 2019 09:11 AM /**

Ernice Gilbert **August 02, 2019**



Were it not for hardcopies of important case files that V.I.P.D. Commissioner Nominee Trevor Velinor said the police department had saved for use as backup, an untold number of cases -- involving everything from murder to rape -- would have been lost, resulting in possibly a mass dismissal of court trials and creating a problem that would overwhelm the department.

That's because the Virgin Islands Police Department computer system has been hacked on a number of occasions over the past months, according to V.I.P.D. Public Information Officer Glen Dratte. Mr. Velinor corroborated Mr. Dratte's statement, telling The Consortium during a phone interview Thursday that he was briefed on the hackings when

he arrived in the territory.

"We've had a ransomware attack," Mr. Velinor said, adding that the ransomware attack "really impacted us" on June 11. Ransomware is a type of malware from cryptovirology (a field that studies how to use cryptography to design powerful malicious software) that threatens to publish a victim's data or perpetually block access to it unless a ransom is paid.

According to a person with knowledge of the matter, the situation has been a nightmare for officers, many of whom cannot perform basic tasks on their computers. Mr. Velinor confirmed this to be true, telling The Consortium that many computers had to be wiped clean -- losing all stored data -- and "re-imaged" to allow officers to work.

Of grave concern is the security of important case files. With many cases pending and investigations ongoing, losing access to the database where files were stored poses a massive problem for the V.I.P.D., which could lead to lawsuits. But the commissioner nominee said most of the records, along being stored on computers, were secured the traditional way as well. "I believe that many of our records are also in hardcopies, which allows us to retrieve hardcopy documentation to be able to present those as evidence," Mr. Velinor said.

The commissioner nominee said "many", meaning there could possibly be files that have been lost. And still unclear is whether hardcopy file storage was affected by Hurricanes Irma and Maria, and how effective, historically, the department has stored its hardcopy files.

The extent of the damage is far-reaching. "I was made aware to the fact that many of our computers were compromised. I was made aware that we had instructed all our users to not go on the particular server, to not go online and so therefore there was a full approach to attempt to minimize the damage. But as I said, many of the computers were already affected by the time the system administrators were alerted to the presence of a potential ransomware."

The V.I.P.D. has refused to pay the hackers the ransom demanded to unlock the system. "As you know, quite frequently when you pay the ransom it doesn't guarantee the hackers are going to provide you with the encryption key to read the encryption, and so we have not paid a ransom," said the commissioner nominee.

Mr. Velinor said some officers had access to their computer systems again, but when asked whether those officers were able to regain access to their files, he acknowledged that access was only provided after the computers were wiped clean. Some officers who had stored files on external hard drives managed to recoup at least some data.

Whether the lost files can be recouped was unclear, but Mr. Velinor said the police department would try to. "We are utilizing various sources to include the F.B.I. and others to assist with the file recovery and decoding the ransomware encryption," he said.

Recourse

The V.I.P.D. has reached out to the Federal Bureau of Investigation and other federal arms for help. It has also contacted the territory's Bureau of Information Technology for

assistance. Additionally, the police force is considering contracting an online security firm that would ascertain the safety of the V.I.P.D.'s online systems moving forward. "We will be navigating towards full service to include strengthening our system so that we are able to protect against future ransomware," Mr. Velinor said. He said the force had not secured the online security firm as of Thursday.

The police force has also started using a different domain, according to Mr. Velinor, although the name wasn't made clear. The current website is vipd.gov.vi, and the V.I.P.D. still appears to be updating it: as of July 29, a VIPD release relative to a Sunday night shooting at the Floatopia event in Frederiksted was published.