Affidavit in Support of Search Warrant Application

We are requesting a search warrant on behalf of the DHS working on the case of the missing train Astrapi. This affidavit is in support of an application for a warrant authorizing the DHS team to access the email history of Pete Bishop to prove that he is Big Eat whose account is connected to Indishell.

We have reason to believe that Pete Bishop goes by the alias “Big Eat” on an online, blackhat forum frequented by the hacker organization Indishell. On the forum, he expressed knowledge in how to “cyber graffiti” a website. While planning how to vandalize the website, he revealed that he might know a way to get in touch with an insider to help bring it down. This makes sense because Pete has been working with the IT at Emory. Also, Emory has been working with Regenerative Engineering and Medicine, so Pete has the perfect “in” with the people at REM, which was later vandalized after the train went missing. Getting access into the Emory and REM databases would prove to be little challenge to him.

Because his forum posts and connection to Emory and REM, his private emails to his partners in crime would be a damning piece of evidence. Those emails would show his correspondence with his conspirators and the planning of not only attacking the websites but also recruiting their insider. This information is vitally important to linking the missing train incident with who corrupted the REM site. Because this link is so important, it is of the absolute necessity that the right protocols are taken to ensure Pete Bishop’s rights are not infringed. We are intending to take the information that comes from emails, so we will need a computer image of the email database that holds his communication with his partners in crime. This process will take place at the DHS meeting spaces in Ruston, Louisiana, so it is not necessary for us to obtain a warrant for physically searching Pete Bishop’s apartment.

This case involves Pete Bishop as the link providing the insider information that allowed Indishell to vandalize the REM and Emory websites and hack into the Astapi train. When the Astapi train was hacked, it was found that an elaborate SQL injection disabled the authentication system which allowed the hacking group to probe and map the access ports for the train. This morning, the Regenerative Engineering and Medicine IP logged in and initiated the attack on the train and subsequently the only IP able to access the train was a confirmed Indishell IP based in New Delhi, India. The hacking group was able to get past REM and Emory’s firewalls and vandalize the websites by using the insider information which they received from who we believe to be Pete Bishop.