ON THE TIMING OF THE NGHIA HOANG PHO PLEA

Last Friday, the guy responsible for getting a bunch of NSA hacking tools stolen from his home computer, 67-year old Nghia Hoang Pho, pled guilty to willful retention of classified information. His plea hearing was held in secret; according to the NYT which broke the story, "one courtroom official described the charges against Mr. Pho as 'super-sealed' before the hearing."

According to the information supporting his guilty plea, Pho had been bringing NSA files home for 5 years, from 2010 to 2015.

I want to note something about the timing of the plea. The actual plea deal is dated October 11. It states that "if this offer has not been accepted by October 25, 2017, it will be deemed withdrawn." The information itself was actually signed on November 29. Friday, the actual plea, was December 1.

So while there's not a substantial cooperation component in the plea deal, certainly a substantial amount of time took place in that window, enough time to cooperate.

And consider the news coverage that has happened during that period. The initial plea offer was made in the week following a big media blitz of stories blaming Pho (and through him Kaspersky) for the Russian theft of NSA tools. In the interim period between the offer and the acceptance of the plea deal, Kaspersky confirmed both verbally and then in a full incident report that his AV had found the files in question, while noting that a third party hacker had compromised Pho's machine during the period he had TAO's tools on it.

In other words, after at least an 18 month investigation, Pho finally signed a plea agreement as the media started blaming him for the compromise of these tools.

During much of that period, Harold Martin was in custody and under investigation for a similar crime: bringing a bunch of TAO tools home and putting them on his computer. Only, unlike Pho, Martin got slammed with a 20-count indictment, laying a range of files, and not just files from NSA. Indeed, the Pho plea notes,

> This Office and the Defendant agree that the Defendant's conduct could have been charged as multiple counts. This Office and the Defendant further agree that had the Defendant been convicted of additional counts, … those counts would not group with the count of conviction, and the final offense level would have increased by 5 levels.

That is, the government implicity threatened Pho to treat him as Martin had been, with a separate charge tied to the individual files he took.

Since April, Martin's docket has featured continuation after continuation that might reflect cooperation with the government.

All this leads me to believe that these two investigations may have worked in tandem. Whereas the government originally insinuated Martin had provided the files that Shadow Brokers started leaking in August 2016, the Martin cooperation may have led the government to understand the Pho compromise differently. That is, it's possible that Pho was the source for Shadow Brokers' tools (or rather, that both men were), but the government didn't come to understand that until Martin started cooperating.

It's not clear whether, between the two of them, it would account for all the files that Shadow Brokers had (nor is it clear that Shadow Brokers ever had all the files made available by one or the other of them by loading them onto their home machine). For example, it's not clear either would have had the San Antonio files at the center of the Second Source theory.

Whatever the details, the timing of the Nghia Hoang Pho plea may suggest that the government only belatedly came to understand how, by loading a bunch of TAO tools running on his Kaspersky-running computer, made the tools available to a third party hack. Certainly, that would explain why Kaspersky has a better understanding of the timing of all this than the government does.