IN MEDIA RES: THE FBI'S WANNACRY ATTRIBUTION

I've been working through the complaint charging Park Jin Hyok with a slew of hacking attributed to the Lazarus group associated with North Korea. Reading it closely has led me to be even less convinced about the government's attribution of the May 2017 WannaCry outbreak to North Korea. It's going to take me a series of posts (and some chats with actual experts on this topic) to explain why. But for now, I want to point to a really suspect move the complaint makes.

The FBI's proof that Park and Lazarus and North Korea did WannaCry consists, speaking very broadly, of proof that the first generation of the WannaCry malware shared some key elements with other attacks attributed to Lazarus, and then an argument that the subsequent two generations of WannaCry were done by the same people as the first one. While the argument consists of a range of evidence and this post vastly oversimplifies what the FBI presents, three key moves in it are:

- The earlier generations of WannaCry are not known to be publicly available
- Subjects using a known Lazarus IP address were researching how to exploit the Microsoft vulnerability in the weeks before the attack
- Both WannaCry versions 1 and 2 cashed out Bitcoin in a similar way (which the complaint doesn't describe)

For now, I'm just interested in that middle point, which the complaint describes this way:

> 221. On March 14, 2017, Microsoft released a patch for a Server Message Block (SMB) vulnerability that was identified as CVE-2017-0144 on its website, https://technet.microsoft.com/en-us/library/security/ms17-010.aspx. Microsoft attempted to remedy the vulnerability by releasing patches to versions of Microsoft Windows operating systems that Microsoft supported at the time. Patches were not initially released for older versions of Windows that were no longer supported, such as Windows XP and Windows 8.
>
> 222. The next month, on April 15, 2017, an exploit that targeted the CVE-2017-0144 vulnerability (herein the "CVE-2017-0144 exploit") was publicly released by a group calling itself the "Shadow Brokers."
>
> 223. On April 18, 2017 and April 21, 2017, a senior security analyst at private cyber security company RiskSense, Inc. ("RiskSense") posted research on that exploit on his website: https://zerosum0x0.blogspot.com.
>
> 224. On May 9, 2017, RiskSense released code on the website github.com with the stated purpose of allowing legal "white hat" penetration testers to test the CVE-2017-0144 exploit on unpatched systems. Essentially, RiskSense posted source code that its employees had reverse-engineered for the CVE-2017-0144 exploit, which cyber security researchers could then use to test vulnerabilities in client computer systems. I know based on my training and experience that penetration testers regularly seek to exploit vulnerabilities with their customers'

> consent as a proof-of-concept to demonstrate how hackers could illegally access their customers' systems.
>
> 225. On May 12, 2017, a ransomware attack called "WannaCry" (later identified as "WannaCry Version 2," as discussed below) began affecting computers around the globe.
>
> [snip]
>
> 242. Records that I have obtained show that the subjects of this investigation were monitoring the release of the CVE-2017-0144 exploit and the efforts by cyber researchers to develop the source code that was later packaged into WannaCry Version 2:
>
> a. On numerous days between March 23 and May 12, 2017, a subject using North Korean IP Address #6 visited technet.microsoft.com, the general domain where Microsoft hosted specific webpages that provide information about Microsoft products, including information on Windows vulnerabilities (including CVE-2017-0144), although the exact URL or whether the information on this particular CVE was being accessed is not known.
>
> b. On April 23, April 26, May 10, May 11, and May 12, 2017, a subject using North Korean IP Address #6 visited the blog website zerosum0x0.blogspot.com, where, on April 18, 2017 and 21, 2017, a RiskSense researcher had posted information about research into the CVE-2017-0144 exploit and progress on reverse-engineering the exploit; RiskSense subsequently released the exploit code on GitHub.com.

According to the *in media res* story told by the FBI, the following is the chronology:

> March 14: Microsoft drops a vulnerability seemingly out of the blue without publicly calling attention to it
>
> Starting on March 23: Someone using known Lazarus IP address #6 tracks Microsoft's vulnerabilities reports (note, the FBI doesn't mention whether this was typical behavior or unique for this period)
>
> April 15: Shadow Brokers releases the Eternal Blue exploit
>
> April 18 and 23: RiskSense releases a reverse engineered version of Eternal Blue
>
> Starting on April 23 and leading up to May 12: Someone using that same known Lazarus IP #6 makes a series of visits to the RiskSense site that released an exploit reverse engineered off the Shadow Brokers release
>
> May 12: A version of WannaCry spreads across the world using the RiskSense exploit

Of course, that's not how things really happened. FBI neglects to mention that on January 8, Shadow Brokers offered to auction off files that NSA knew included the SMB exploit that Microsoft issued a patch for on March 14.

Along with that important gap in the narrative, the FBI Agent who wrote the affidavit behind this complaint, Nathan Shields, is awfully coy in describing Shadow Brokers simply as "a group calling itself the 'Shadow Brokers.'" While the complaint remained sealed for three months, by June 8, 2018, when the affidavit was written, the FBI assuredly knew far more about Shadow Brokers than that it was a group with a spooky name.

As public proof, DOJ signed a plea agreement with Nghia Pho on November 29 of last year. Pho was reportedly the guy from whose home computer

some of these same files were stolen. While the publicly released plea has no cooperation agreement, the plea included a sealed supplement, which given the repeated delays in sentencing, likely did include a cooperation agreement.

Pho is due to be sentenced next Tuesday. The sentencing memos in the case remain sealed, but it's clear from the docket entry for Pho's that he's making a bid to be treated in the same way that David Petraeus and John Deutsch were — that is, to get a misdemeanor treatment and probation for bringing code word documents home to store in an unlocked desk drawer — which would be truly remarkable treatment for a guy who allegedly made NSA's hacking tools available for theft.

09/13/2018	19	SENTENCING MEMORANDUM by Nghia Hoang Pho (Attachments: # 1 Exhibit #1- Letter from Nghia Pho, # 2 Exhibit #2 - Letters in Support of Nghia Pho, # 3 Exhibit #3 - Family Photographs, # 4 Exhibit #4 - NSA Certificate, # 5 Exhibit #5 - Petraeus Materials, # 6 Exhibit #6 - Deutch Press Release)(Bonsib, Robert) (Entered: 09/13/2018)

And while it's possible that FBI Agent Shields doesn't know anything more about what the government knows about Shadow Brokers than that it has a spooky name, some of the folks who quoted in the dog-and-pony reveal of this complaint on September 6, not least Assistant Attorney General John Demers, do know whatever else the government knows about Shadow Brokers.

Including that the announcement of the sale of Eternal Blue on January 8 makes the searches on Microsoft's site before the exploit was actually released on April 15 one of the most interesting details in this chronology. There are lots of possible explanations for the fact that someone was (as the FBI's timeline suggests) searching Microsoft's website for a vulnerability before the import of it became publicly known.

But when you add the January 8 Shadow Brokers post to the timeline, it makes culprits other than North Korea far more likely than the FBI affidavit makes out.