

HAL (ER, UM, BAH) BITES NSA

Way back in August, the government arrested a guy named Harold Thomas Martin III, who goes by Hal. Someone leaked news of the arrest to some of a who's who list of NYT reporters – including Adam Goldman, Jo Becker, Michael Schmidt, David Sanger, Scott Shane, Matt Apuzzo, and Mark Mazzetti – who wrote what was originally a four paragraph story noting Martin is a Booz contractor and he is suspected of “taking the highly classified ‘source code’ developed by the agency to break into computer systems of adversaries like Russia, China, Iran and North Korea.” That is, the leak suggested that the FBI had found their Shadow Brokers culprit.

The story has since been updated to include, among other things, a claim from an “Administration official” that “investigators suspected that Mr. Martin might have taken the material before Mr. Snowden’s actions became public,” which is rather curious since the classified documents described in the DOJ announcement on the arrest are six 2014 documents obtained from sensitive intelligence that were found in his house and vehicle.

The complaint alleges that among the classified documents found in the search were six classified documents obtained from sensitive intelligence and produced by a government agency in 2014. These documents were produced through sensitive government sources, methods, and capabilities, which are critical to a wide variety of national security issues. The disclosure of the documents would reveal those sensitive sources, methods, and capabilities.

Martin may have started taking documents before Snowden, but if DOJ’s allegations are true, he

was able to continue even after Snowden (and would have needed to if he were actually the Shadow Broker source).

The conflicting information on this suggests that DOJ doesn't have any fucking clue what Hal Martin did yet, or why he did it. FBI was clearly trying to figure that out while someone was leaking to everyone at the NYT in terms that suggested the FBI had found the Shadow Brokers source (including the completely bullshit emphasis on Russian and Chinese targets, ignoring how many American companies have been exposed in the Shadow Brokers leak).

Or perhaps not.

The original Shadow Brokers announcement was (as Rayne's timeline lays out) on August 15. Martin was arrested on August 27. Since that time there have been two more Shadow Brokers announcements, one of little import that seems to mock Asian diction posted on PasteBin on August 28, and another bizarre self-interview posted on Medium last week. In my quick review the voice of those posts is different from the original (as is the claimed political bent). So it is possible the FBI has kept Martin's arrest secret to try to lure in someone else with further SB announcements.

Or maybe Martin just stupidly brought work home and is fucked because the NSA believes or believed he could be the source of the Shadow Brokers documents, and they need a scapegoat and he'll do fine. Good thing he is being represented by the same public defender who got Thomas Drake off with a plea deal.

Which leaves the one certainty we can take away from this thus far. Booz Allen Hamilton – which just got \$144 million in new DOD business yesterday (h/t Tim Shorrock) – needs a lot more scrutiny in its ability to keep the nation's secrets safe ... and may well need to lose a lot of business.